Tiered Privacy: Restoring Trust in the Digital Age

A Decentralized Framework for Identity and Authenticity Online

https://github.com/keeplist-io/keeplist-TPIF

Michael Deeb
Layout: OpenAI o1
Writing Assistance: OpenAI Chat-GPT4o
Round 1 Editing: Gemini Experimental 1206
Round 2 Editing: Gemini 2.0 Flash Thinking Experimental 01-21

Keeplist.io
TealWolf Consulting
Civic Tech DC

Washington, DC
deeb@keeplist.io

Abstract

Tiered Privacy and Identity Verification Framework (TPIF), a decentralized identity solution empowering users to verify their authenticity across five clear, flexible tiers—from fully anonymous to fully transparent—using advanced cryptographic techniques and minimal personal data exposure.

Executive Summary

This paper introduces the Tiered Privacy and Identity Framework (TPIF),a decentralized identity solution empowering users to verify their authenticity across five clear, flexible tiers—from fully anonymous to fully transparent—using advanced cryptographic techniques and minimal personal data exposure.

TPIF offers a fundamentally new approach to online identity, one that prioritizes user privacy, security, and control, while simultaneously enabling the trust and accountability necessary for a thriving digital ecosystem. By moving beyond the limitations of traditional all-or-nothing identity systems, TPIF provides a flexible and adaptable framework that can meet the diverse needs of individuals, platforms, and organizations.

TPIF's core innovations – the tiered privacy model, the universal Proof-of-Personhood VC, the consortium-governed permissioned blockchain, and the strategic use of advanced cryptography (including Zero-Knowledge Proofs, Secure Multi-Party Computation, and Fully Homomorphic Encryption) – combine to create a system that is both powerful and privacy-respecting. The FHE-protected audit log, in particular, represents a significant step forward in ensuring long-term privacy and auditability without compromising on either.

TPIF is not just a theoretical concept; it's a blueprint for a more trustworthy and user-centric digital future. It addresses the critical challenges of disinformation, online abuse, and data breaches while empowering individuals to participate in the digital world on their own terms. The framework's open and collaborative nature, combined with its strong technical foundation, positions TPIF as a potential cornerstone for the next generation of online identity systems. The time for a more privacy-respecting and secure internet is now, and TPIF provides a viable path towards that future.

This framework aims to:

1. **Preserve Online Freedom**
   Keep the internet accessible, decentralized, and equitable.
2. **Build Trust Without Compromise**
   Use cryptographic proofs to verify authenticity without revealing sensitive data.
3. **Raise the Cost of Abuse**
   Make automated manipulation significantly more difficult and expensive.
4. **Support Context-Specific Verification**
   Provide understood and flexible tiers of identification that fit different situations and user preferences.
5. **Enable Secure Anonymous Communication**
   In compromised political environments, users can prove their authenticity without exposing their identities or risking retaliation.

These core principles are the building blocks of a more trustworthy and user-centric digital future.

1. Background: The Problem with Identity on Today’s Internet

The Rise of Bots and Fake Accounts

Today, nearly half of all internet activity comes from automated sources—bots—with over 30% being malicious (Imperva, 2024). Fake product reviews flood platforms like Amazon, where counterfeit goods and dishonest sellers manipulate consumers daily (CT Insider, 2022; NY Times). The digital spaces we rely on for information, commerce, and social connection have become increasingly unreliable, forcing us to question who or what we can truly trust online.

Why "Authenticity" Is Failing Online

Attempts to confirm authenticity online have produced mixed results at best. Social media verification programs, for instance, often provide a false sense of security. Bad actors routinely exploit inconsistent verification policies to amplify misinformation, while platforms themselves sometimes blur the lines between genuine verification and paid endorsements. For example, Twitter's once-respected "blue checkmark" shifted overnight from indicating trustworthiness to simply identifying paid subscribers. Such confusion weakens trust and deepens the digital identity crisis.

Lessons from Centralized Approaches: The Worldcoin Experiment

Consider the recent experience of Worldcoin—a widely publicized digital identity system built around biometric iris scans. Although it promised universal access and resistance to bots, Worldcoin highlighted critical problems inherent to centralized identity approaches. The reliance on expensive, limited, and specialized hardware created barriers, particularly disadvantaging rural or underserved populations. And financial incentives encouraged vulnerable individuals to share sensitive biometric data, raising ethical and privacy concerns.

Even with promises of privacy safeguards, Worldcoin's centralized collection of biometric data has led to global scrutiny, regulatory pushback, and concerns about potential misuse (CNIL, 2018; Mijic & Ramachandran, 2023). Most importantly, Worldcoin demonstrated the fundamental risk of centralizing identity within a single company, making millions of users dependent on one entity's policies and motivations. The lesson is clear: centralized identity models pose serious risks to user privacy, security, and autonomy.

Why Current Digital Identity Solutions Fall Short

Traditional Identity Systems: Centralized and Vulnerable

Traditional approaches—typically managed by corporations or governments—store vast amounts of sensitive personal data. This centralization makes these databases prime targets for breaches, surveillance, and identity theft. In an era of sophisticated AI-driven misinformation, such systems simply cannot guarantee privacy or protection.

Decentralized Identity (DID): Empowering Users, with Limits

Decentralized Identity emerged to put control back in users' hands. At its core, DID provides digital identities managed entirely by individuals, without a central authority. Think of it as a digital passport you fully own, offering greater privacy. Yet, DID's actual effectiveness depends heavily on how it's implemented—particularly how carefully user privacy is maintained.

Verifiable Credentials: Sharing Only What's Needed

Complementing DID, Verifiable Credentials (VCs) allow users to securely prove aspects of their identity—such as age, nationality, or qualifications—without revealing unnecessary personal information. Like showing only your birth date at a bar instead of handing over your entire

driver’s license, VCs offer precise and privacy-focused digital interactions, and consequently, are a critical building block.

Self-Sovereign Identity: Putting Users Fully in Charge

Self-Sovereign Identity (SSI) pushes these ideas further, emphasizing complete user control. With SSI, you alone decide what personal data to share, with whom, and under which conditions. SSI prioritizes autonomy, privacy, and flexibility, shifting power away from centralized systems and returning it to the individual—exactly the direction needed for trust online.

Proof of Personhood: Verifying Humans without Losing Privacy

To combat fake accounts and AI-driven bots, "Proof of Personhood" (PoP) methods emerged to verify genuine human users. Approaches range from biometric scans—like those used by Worldcoin—to networks where users confirm each other's authenticity. Each method offers trade-offs between privacy, ease of access, and effectiveness. The ideal PoP method balances privacy and accuracy without imposing risks or unnecessary hurdles on users.

Blockchain’s Transparency Problem

Public blockchains, praised widely for transparency, are ironically problematic for identity verification. While transparency works well for tracking transactions, it becomes dangerous when applied to personal identities, potentially exposing sensitive user data. Moreover, public blockchains often have unpredictable costs and limited scalability, making them unsuitable for widespread identity solutions.

Ethical, Legal, and Inclusive Identity

Creating a successful digital identity system isn’t purely technical—it also means addressing ethical, legal, and accessibility challenges. Regulations like GDPR in Europe and HIPAA in the U.S. prioritize minimal data use, user consent, and secure management. Any identity system must inherently align with these values, safeguarding privacy at every step.

Accessibility is equally essential. A truly effective identity framework should bridge digital divides, ensuring privacy and secure identities are available to everyone, regardless of technical availability or political alignments. TPIF prioritizes usability by abstracting complex cryptographic key management behind intuitive client apps, ensuring that all users—even those without technical expertise—can securely control and recover their identities.

2. Problem Statement: The Urgent Need for Trust

The erosion of trust online is driven by widespread in-authentic behavior, privacy compromises in centralized identity systems, and the inherent risks of centralization itself. This crisis urgently requires a decentralized solution that prioritizes user privacy, autonomy, and authenticity. For this to be feasible and adopted, the solution needs to be compatible with the core principles of

an open and free internet and seamlessly integrated into everyone's shared understanding of the internet.

3. Technical Framework: Balancing Privacy and Trust

Tiered Privacy and Identity Framework (TPIF) addresses the erosion of online trust by creating a marketplace for authenticity, where users decide the level of verification that best suits their needs, from fully anonymous to fully public, but verifiably authentic. By creating shared definitions and frameworks, users can have confidence in the authenticity across services and an intuitive understanding of the differences between different types of authenticity.

4.1 TPIF's Approach to Key Technologies

TPIF builds upon established concepts like Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and Self-Sovereign Identity (SSI), but integrates them in a novel way to create a flexible, privacy-preserving system. TPIF's core innovations lie in *how* it uses these technologies to achieve its tiered structure.

- **Tiered DIDs:** Unlike traditional DID approaches, TPIF's DIDs support a *spectrum* of association with real-world identity. This ranges from completely unlinkable anonymous DIDs (for maximum privacy) to pseudonymous DIDs with verifiable links to real-world credentials (for regulated contexts), and finally to publicly linked DIDs (for full transparency). This tiered approach to DID usage is central to TPIF's flexibility.

  Unlike existing DID frameworks such as Hyperledger Indy (focused mainly on verifiable credentials) or Microsoft ION (focused primarily on public decentralized identifiers), TPIF uniquely integrates flexible, graded identity privacy directly into DID usage.

- **VCs and Trusted Issuance:** TPIF leverages VCs extensively, but within a *hierarchical Certificate Authority (CA) structure*. This ensures the trustworthiness and integrity of credentials while enabling efficient revocation. TPIF consortium acts as the root of trust, delegating authority to specialized CAs for different credential types. This structured approach to VC issuance and management is crucial for scalability and reliability.

- **Universal Proof-of-Personhood:** A key differentiator of TPIF is the requirement of a CA-issued *Proof-of-Personhood (PoP) VC for all users*. This establishes a baseline of human authenticity across *all* tiers, combating bots and Sybil attacks, even in anonymous contexts. The PoP VC is obtained through a privacy-respecting process and its existence can be proven without revealing identifying information.

- **Graded Self-Sovereignty:** TPIF embraces the *principles* of SSI (user control and data minimization), but recognizes that complete self-sovereignty isn't always practical or desirable. TPIF offers *graded* self-sovereignty, allowing users to choose the level of

identity verification appropriate for each interaction, balancing privacy with the need for accountability in certain contexts.

- **Permissioned Blockchain and Consortium Governance:** TPIF utilizes a custom *permissioned blockchain* governed by a consortium of trusted organizations. This approach addresses the privacy concerns associated with public blockchains, while still providing a tamper-proof and auditable record for DIDs, public keys, and smart contract interactions. Blockchain frameworks designed for decentralized identity, such as *Hyperledger Indy*, are particularly well-suited for building out this consortium-based infrastructure.

- **Advanced Cryptography for Privacy:** TPIF goes beyond basic digital signatures, incorporating:

    - **Zero-Knowledge Proofs (ZKPs):** ZKPs allow you to prove something is true without revealing any other information. Imagine proving you're old enough to enter a bar without showing your ID or revealing your birthdate – that's the power of ZKPs. TPIF uses ZKPs extensively to enable private attribute verification (El-Hajj et al., 2022; Goldreich et al., 1991).
    - **Secure Multi-Party Computation (MPC):** MPC is like a group of people solving a puzzle together without anyone seeing the other people's pieces. In TPIF, MPC allows multiple Verification Oracles to collaboratively verify credentials and attributes without any single oracle gaining access to all the data. This distributes trust and enhances privacy (Yao, 1982).
    - **Fully Homomorphic Encryption (FHE):** FHE is like performing calculations on a locked box without ever opening it. Thanks to recent advancements, FHE is becoming practical, allowing TPIF to perform computations on encrypted data without decryption (Gentry, 2009). This opens up possibilities for privacy-preserving data analysis and attribute verification, even on sensitive information.
    - **Onion Routing (via a Mix Network)**: Provides network-level anonymity, ensuring that a user's location or identifying network details aren't exposed (Chaum, 1985).

In essence, TPIF combines and adapts existing technologies in a novel way to create a tiered identity system that balances the often-competing goals of privacy, security, and usability. The framework's use of universal PoP VC, CA hierarchy, tiered DIDs, consortium-based blockchain infrastructure, and strategic use of advanced cryptography are key differentiators. The following sections detail how these technologies are applied within each specific tier.

4.2 TPIF System Architecture: A High-Level Overview

TPIF is built upon a decentralized, multi-layered architecture designed to provide flexible privacy options and verifiable authenticity. This architecture integrates the key technologies

described previously, creating a user-centric system for managing digital identities and interactions.

The key components are:

- **User Client:** The user's primary interface with TPIF. This is a user-controlled application (e.g., a browser extension, mobile app, or desktop application) that securely manages the user's DIDs, private keys, and Verifiable Credentials (VCs). The client is responsible for:
    - Generating and managing DIDs.
    - Storing and managing VCs (including the PoP VC).
    - Creating Zero-Knowledge Proofs (ZKPs).
    - Constructing onion-encrypted messages for communication through the Mix Network.
    - Interacting with Relying Parties and Verification Oracles.
    - Managing user consent for data disclosure.
- **Relying Parties (Websites/Applications):** The services that users wish to access using their TPIF identities. Relying parties:
    - Specify their identity verification requirements (which tier, which attributes).
    - Receive verification results from the Verification Oracles.
    - Grant access to users based on successful verification.
- **TPIF Blockchain:** A permissioned blockchain, maintained by a consortium of trusted organizations, serves as a public, yet privacy-respecting, bulletin board. It stores:
    - Decentralized Identifiers (DIDs).
    - Public Keys.
    - Smart Contracts that govern the verification process and manage the consortium.
    - **Privacy-Preserving Audit Log Checkpoints:** Instead of storing the full audit log on-chain (which could reveal patterns over time), TPIF uses a novel approach:
        - The detailed audit log is stored off-chain and distributed among Verification Oracles.
        - Periodically, these Oracles use Secure Multi-Party Computation (MPC) and Fully Homomorphic Encryption (FHE) to collaboratively compute a cryptographic hash of the combined log entries without revealing the data itself.
        - Only this THE-computed hash – a tamper-proof commitment – is stored on the blockchain. This ensures auditability without compromising privacy.

    This approach balances transparency and accountability with strong user privacy.

- **Mix Network:** A dynamically configured network of mix nodes provides onion routing. This:
    - Obfuscates the communication between the User Client, Relying Parties, and Verification Oracles.
    - Protects user privacy by making it difficult to track their online activities or link them to their IP address.
    - Employs a reputation system (managed by a smart contract on the TPIF blockchain) to incentivize good behavior and deter malicious nodes.

- **Verification Oracles:** A pool of nodes within the TPIF consortium that collaboratively perform verification computations. They:
    - Are randomly selected for each verification session (using a secure lottery mechanism on the blockchain).
    - Use Secure Multi-Party Computation (MPC) to verify credentials and attributes without any single oracle gaining access to all the data.
    - Produce a digitally signed verification result, which is sent to the Relying Party.
    - A threshold number of oracles are required to cooperate to produce a valid result, preventing collusion and single points of failure.

- **Certificate Authorities (CAs):** A hierarchical CA structure, managed by the TPIF consortium (and potentially including external trusted CAs), is responsible for:
    - Issuing Verifiable Credentials (VCs), including the crucial Proof-of-Personhood (PoP) VC.
    - Managing the revocation of VCs.
    - Ensuring the trustworthiness and integrity of the credentials used within the system.

- **IPFS (InterPlanetary File System):** IPFS provides decentralized storage for user data and serves as a way to further obfuscate the origin of user data. All data stored on IPFS is encrypted using user-controlled keys.

4.3 The TPIF Privacy-Preserving Login Protocol

TPIF's core functionality is enabled by a novel privacy-preserving login protocol. This protocol, detailed in Section 5, allows users to seamlessly authenticate to relying parties while maintaining control over their personal information. The protocol leverages the components described above, orchestrating their interactions to achieve secure and flexible authentication across the different privacy tiers. It combines DIDs, VCs, ZKPs, MPC, and onion routing to achieve its privacy and security goals.

The following sections describe the individual privacy tiers and how they utilize this architecture to provide a spectrum of identity verification options.

4.4 Understanding the Tiers: A Spectrum of Choice, Governed by the Community

The Tiered Privacy Model is the heart of TPIF, offering a spectrum of authenticity rather than a rigid hierarchy. TPIF offers five distinct privacy tiers, enabling users to match their identity verification level to specific contexts and needs. Each tier balances anonymity, privacy, and authenticity uniquely. These tiers are intended to be managed by the consortium, ensuring transparency, consistency, and a balance of interests. This community governance ensures the system remains user-centric and adapts to the evolving digital landscape.

Each tier offers a distinct range of privacy and verification, creating a flexible system that adapts to countless online contexts.

4.4.1 Tier 1: Anonymous but Authentic – Free, Secure Foundation

What it is

Tier 1 is the foundation: complete, cryptographically-guaranteed anonymity. It's your digital birthright: the right to participate online anonymously, but with the assurance that you're interacting with other real human beings. It's free, universal, and the starting point for everyone.

Think of it like

Walking into a public square and joining a conversation. You don't need to announce your name or show ID, but you – and everyone else – can be confident that you are all real people, not automated voices. Tier 1 provides that same foundational assurance online.

Applications

- True Freedom of Speech: Participate in online discussions, express your opinions, and engage in debates without fear of censorship or reprisal, knowing your identity is protected.
- Secure Whistleblowing: Report wrongdoing or share sensitive information anonymously and securely, with the assurance that your submission is verified as human.
- Unbiased Feedback: Provide honest opinions and reviews without your identity influencing the reception of your feedback.
- Combating Disinformation: Help create a more trustworthy online environment by reducing the impact of botnets and automated manipulation, fostering genuine human interaction.
- Exploring Sensitive Topics: Be able to research and get support, knowing you are completely anonymous.

Key Limitation

Tier 1 is strictly limited to proving your humanity. You cannot use Tier 1 to verify any specific attributes about yourself. This keeps Tier 1 simple, secure, and focused on its core purpose.

Value

Tier 1 offers a powerful combination: uncompromising anonymity with the essential assurance of human authenticity. It’s a free and universal foundation for a more trustworthy internet, reducing noise, fostering genuine interaction, and empowering free speech. It's not just about hiding your identity; it's about reclaiming the internet for real people.

4.4.2 Tier 2: Anonymous but Unique – Proving What You Have, Not Who You Are

What it is

Tier 2 builds on Tier 1 by adding session-based uniqueness and the ability to anonymously prove the validity of external credentials. You remain completely anonymous, but the system ensures you are a unique individual for a given limited session, and you can optionally prove you possess certain valid tokens – like a digital driver's license, a student ID, or a professional membership – without revealing the contents of those tokens. It's about proving what you have, not who you are.

How it works

You possess digitally signed tokens issued by trusted authorities (governments, universities, organizations). Using Fully Homomorphic Encryption (FHE) or Zero-Knowledge Proofs (ZKPs), you can prove to a platform that:

- Your token is valid (issued by a legitimate authority).
- Your token possesses certain properties (e.g., "type = driver's license," "status = active").

All of this is done without TPIF or the platform ever seeing the actual token data. Your privacy is protected by cryptography.

Think of it like

Using a single-use, anonymous hashed token to enter a fairground. The token guarantees you can enter only once, but once you're inside (or once you leave), the token is no longer relevant, and there's no record of who used it. It was simply about ensuring fair entry, one token per person.

Applications:

- Online Polls and Voting: Guaranteeing "one person, one vote" without requiring registration or revealing voter identities. The system ensures uniqueness for the duration of the poll, but doesn't track voters afterward.
- Limited-Time Offers and Trials: Preventing users from claiming multiple free trials or abusing promotional offers, without creating permanent user profiles. The uniqueness is tied to the offer itself, not a persistent user identity.
- Anonymous Giveaways and Contests: Ensuring fair participation by limiting entries to one per person, while maintaining complete anonymity.

- One-Time Anonymous Access: Providing access to a resource or service (e.g., a single download, a temporary chat room) with the guarantee of unique access, without requiring long-term registration. (e.g. Temporary email accounts, url shorteners).

Key Limitation

Like Tier 1, Tier 2 is strictly limited in what it can prove. It's about uniqueness only, and the validity of *credentials*, not any other attributes.

Value

Tier 2 provides fairness and integrity for anonymous interactions that require unique participation. It prevents manipulation and abuse without creating persistent identities or tracking users over time. It's the perfect solution for situations where you need to ensure "one person, one action," but where ongoing tracking is unnecessary and undesirable. The anonymity is absolute and session-based.

4.4.3 Tier 3: Pseudonymous Presence – Building Reputation, Protecting Identity

What it is

Tier 3 allows you to establish a unique pseudonymous presence, creating a persistent identity tied to a specific platform or service, without revealing your real-world identity. Build reputation, engage in communities, and conduct transactions with greater trust, all while maintaining your privacy.

Think of it like

Having a respected username on a marketplace or online community – a consistent persona that others can recognize and trust, without knowing your real name or personal details.

Applications:

- Online Marketplaces and Commerce: Build buyer/seller reputations, facilitate secure transactions, and foster trust in online marketplaces.
- Subscription Services and Platforms: Manage accounts, access content, and engage with services pseudonymously.
- Online Communities and Forums: Establish a consistent presence, build relationships, and contribute to communities with a recognizable pseudonym.

Value

Tier 3 bridges the gap between anonymity and accountability, enabling users to build lasting connections and engage in meaningful interactions while protecting their real-world identity.

4.4.4 Tier 4: Moderated Identity – Verified Credentials, Controlled Disclosure

What it is

Tier 4 involves verification by trusted third-party organizations. This provides a higher level of assurance, often necessary for regulated environments or situations requiring verified credentials. Crucially, you still control what information is disclosed and to whom.

Think of it like

A doctor proving they are the specific holder of a particular medical license (identified by its unique license number) on an online healthcare platform, without revealing their full name or address to the platform itself.

Applications

- Regulated Professions: Doctors, lawyers, accountants, etc., proving they hold specific licenses without revealing their full identities to every online platform they use.
- High-Value Transactions: Proving ownership of a specific asset (e.g., a digital title, a domain name) without revealing all personal details to the counterparty.
- Secure Access Control: Granting access to resources or services based on possession of a specific, unique credential (e.g., a building access card, a membership card) without full identity disclosure.
- Decentralized KYC/AML: Meeting regulatory requirements in a privacy-preserving way by proving the link to verified identity documents without exposing the full document content to every service.

Value

Provides a high level of identity assurance without requiring full public disclosure. It enables strong, verifiable links between online pseudonyms and real-world credentials, facilitating trust in situations where anonymity is not sufficient, but full transparency is undesirable.

4.4.5 Tier 5: Public Identity – Transparency and Accountability

What it is

Tier 5 represents full transparency. Your real-world identity is publicly linked to your online actions. This is reserved for situations where maximum accountability and public trust are paramount, such as for public figures or in high-stakes public roles.

Think of it like

Having a publicly verified social media account as a journalist, politician, or public organization – signaling authenticity and embracing full transparency.

Applications

- Public Figure Verification: Ensure authenticity for journalists, politicians, celebrities, and organizations, combating impersonation and misinformation.

- High-Accountability Roles: Establish transparency and accountability for individuals in positions of public trust.
- Critical Infrastructure and Security: Verify identities in systems requiring the highest levels of security and accountability.

Value

Provides complete transparency and accountability, essential for specific roles and contexts where public trust and verifiable identity are paramount. It's the digital equivalent of operating under your real name in the public sphere.

4.5 The Power of Choice: A Digital World Tailored to You

The Tiered Privacy Model isn't just about technology; it's about empowering users. It’s about creating a digital world where:

Users are in control: Choose the level of verification that fits their needs and your context.

Privacy is respected: Share only what's necessary, minimizing data exposure and maximizing their anonymity when desired.

Trust is earned: Build trust and reputation at their own pace, on their own terms.

The internet is more trustworthy for everyone: Reduce spam, bots, and disinformation, fostering more genuine and meaningful online interactions.

5. TPIF Privacy-Preserving Login Protocol

This section details the core protocol enabling privacy-preserving login within TPIF. This protocol allows users to authenticate to websites and applications without revealing unnecessary personal information, leveraging a decentralized architecture and advanced cryptographic techniques to achieve "eventual privacy" and mitigate the risks of large-scale surveillance and individual targeting. The design builds upon the foundational principles of Self-Sovereign Identity (SSI), Decentralized Identifiers (DIDs), and Verifiable Credentials (VCs) while incorporating novel mechanisms for enhanced privacy and resistance to deanonymization.

5.1. Design Goals:

The protocol is designed to achieve the following goals:

- **Strong Practical Privacy:** Render it computationally infeasible for adversaries to routinely monitor a user's login activity across different services over time.
- **Decentralized Verification:** Eliminate reliance on any single centralized authority for identity verification.

- **Data Minimization:** Disclose only the *minimum* necessary information required by the relying party (website/application).
- **User Control:** Empower users with complete control over their digital identities and the release of their personal data.
- **Eventual Privacy:** Obfuscate the details of login events over time, making long-term tracking impractical.
- **Usability:** Provide a seamless and intuitive user experience, abstracting away the underlying cryptographic complexity.
- **Scalability:** Support a large and growing ecosystem of users, relying parties, and verification services.
- **Interoperability:** Adhere to relevant W3C standards (DIDs and VCs) to ensure compatibility with other identity systems.

5.2. System Components:

The protocol involves the following key components:

- **User Client:** A client-side application (e.g., browser extension, mobile app) that securely manages the user's DIDs, private keys, Verifiable Credentials, and interacts with the TPIF network. This client is responsible for generating Zero-Knowledge Proofs (ZKPs) and managing secure communication channels.
- **Relying Party (Website/Application):** The service that the user wishes to authenticate to. The Relying Party specifies its identity verification requirements.
- **TPIF Blockchain:** A permissioned blockchain, utilizing Tendermint for Byzantine Fault Tolerant (BFT) consensus, maintained by a consortium of trusted organizations. This blockchain serves as a public bulletin board for DIDs, public keys, and smart contracts that govern the verification process.
- **Mix Network:** A dynamically configured network of mix nodes that provide onion routing to obfuscate the communication between the user client, the Relying Party, and the Verification Oracles. This network utilizes techniques inspired by Tor, but is specifically tailored for TPIF login protocol, incorporating a decentralized reputation system managed by a smart contract on TPIF blockchain. Dummy traffic is generated to enhance anonymity set sizes.
- **Verification Oracles:** A pool of nodes within the TPIF consortium that collaboratively perform the verification computations using Secure Multi-Party Computation (MPC). Oracles are randomly selected for each verification session, and a threshold number is required to cooperate to produce a valid result. This approach builds upon the principles of distributed trust found in systems like Hyperledger Indy, but with a stronger emphasis on privacy through MPC.
- **IPFS (InterPlanetary File System):** A decentralized storage network used for storing any user data that cannot be efficiently verified solely through VCs and ZKPs. All data stored on IPFS is encrypted using user-controlled keys, with access granted selectively and temporarily via threshold encryption.

5.3. Protocol Flow (Step-by-Step):

1. **Login Initiation:** The user initiates the login process by selecting the "Login with TPIF" option on the Relying Party's website.

2. **Session and Request Preparation:**

    - The user's TPIF client generates a cryptographically random `SessionID` and its corresponding hash, `SessionIDHash`.
    - The Relying Party transmits a login request to the client, specifying:
        - Its own DID (to receive the verification result).
        - A list of required Verifiable Credentials (e.g., proof of age, proof of membership).
        - A list of acceptable credential issuers.

3. **Mix Network Route Selection:** The client selects a random path through the mix network, consisting of *N* mix nodes (e.g., *N*=5). The selection algorithm prioritizes nodes with high reputation scores (as recorded on the TPIF blockchain) and diverse geographical distribution.

4. **Onion-Encrypted Request Construction:** The client constructs an onion-encrypted message. Each layer is encrypted with the public key of a mix node, starting with the *last* node in the route and working backward. The innermost layer contains:

    - `SessionID`
    - Relying Party DID
    - List of Required Credentials
    - A randomly generated one-time pad for symmetric encryption

5. **Request Routing (via Mix Network):** The client sends the onion-encrypted message to the first mix node. Each mix node decrypts its layer and forwards the remaining message to the next node in the route, adding a random delay to mitigate timing analysis.

6. **Final Mix Node Processing:** The final mix node receives the decrypted innermost layer. It then interacts with a smart contract on the TPIF blockchain, calling the `requestVerification` function and providing the `SessionIDHash` and the list of Required Credentials.

7. **Verification Oracle Selection (Smart Contract):** The `requestVerification` smart contract, inspired by secure lottery mechanisms, randomly selects *M* Verification Oracles

(e.g., *M*=7) from the eligible pool, prioritizing those with high reputation scores. The contract returns the DIDs of the selected Oracles to the final mix node.

8. **Client-Side Credential Processing and ZKP Generation:**

    - The final mix node securely transmits the list of selected Oracle DIDs and the Required Credentials back to the user's client, utilizing the one-time pad for symmetric encryption and reversing the mix network path for communication.
    - The client selects the appropriate VCs from its local storage.
    - For each required credential attribute, the client generates a Zero-Knowledge Proof (ZKP). For simple attributes (e.g., age verification), efficient zk-SNARKs (specifically, Groth16) are employed. For more complex predicates or when setup trust is a primary concern, zk-STARKs are utilized.
    - If necessary, the client prepares encrypted access to data stored on IPFS. A new, temporary symmetric key is generated, the *minimal required data* is encrypted with this key, and the key itself is encrypted using a *threshold public key* derived from the Verification Oracles' public keys. This leverages a Distributed Key Generation (DKG) protocol performed by the Oracles in advance.

9. **Verification Request to Oracles (via Mix Network):** The client constructs another onion-encrypted message, routed through the mix network (either the same path or a new, randomly selected path), destined for the selected Verification Oracles. The innermost layer contains:

    - `SessionID`
    - Generated ZKPs
    - (If applicable) Encrypted data from IPFS and the corresponding encrypted temporary key.
    - The public keys associated with the presented VCs.

10. **Secure Multi-Party Computation (MPC) Verification:** The Verification Oracles receive the request via the mix network and initiate an MPC protocol. Within the secure computation:

    - The signatures on the presented VCs are verified against the provided issuer public keys.
    - The ZKPs are verified, proving the required attributes without revealing the underlying data.
    - If necessary, the Oracles collaboratively decrypt the temporary key (using their private key shares) and access the encrypted data from IPFS. No single Oracle ever gains access to the unencrypted key or data.
    - The Oracles perform the validation logic specified by the Relying Party's requirements.
    - The Oracles compute an aggregated, boolean verification result: `isValid`.

- The result is digitally signed using a threshold signature scheme (e.g., a threshold ECDSA based on Gennaro-Goldfeder or Lindell-Pinkas).

11. **Result Delivery:** The MPC protocol outputs the signed `isValid` result, encrypted with the Relying Party's public key (obtained from its DID), and sends it to the Relying Party's DID on the TPIF blockchain. A separate, minimal confirmation (containing only the `SessionID`) is sent to the user's client, potentially via the mix network, to indicate the completion of the verification process.

12. **Relying Party Decryption and Access:** The Relying Party receives the encrypted verification result, decrypts it, and grants access to the user if `isValid` is true.

13. **Session Cleanup:** All temporary data associated with the session (SessionID, mix network routes, temporary keys) is securely deleted from the client, mix nodes, and Verification Oracles.

14. **Audit Log Entry Creation:**

    - **Each Verification Oracle that participated in the MPC verification creates an encrypted log entry for the event.** This entry includes:
        - A timestamp.
        - The `SessionIDHash`.
        - The Relying Party's DID.
        - The user's DID (pseudonymized, except in Tier 5).
        - A summary of the verification request (e.g., which attributes/credentials were verified, but *not* the actual attribute values).
        - `isValid` result
        - This log entry is encrypted using a key shared among the Verification Oracles (or a key specific to the oracle, with the key itself managed through a distributed key management scheme).

15. **Off-Chain Log Storage:**

    - **Each Verification Oracle stores its encrypted log entry fragment. These fragments are distributed across the Oracles, ensuring no single point of failure or compromise.** This could involve:
        - Shamir's Secret Sharing: The log entry is split into shares, and each Oracle holds a share. A threshold number of shares are required to reconstruct the entry.
        - A Distributed Hash Table (DHT): The log entries are stored on a DHT, with redundancy and access control.
        - (Optional) Encrypted storage on IPFS.

16. **Periodic FHE Hash Commitment (Off-Chain, via MPC):**

    - At predefined intervals (e.g., every hour, every day), the Verification Oracles initiate an MPC protocol.
    - Within this MPC, each Oracle contributes its encrypted log entry fragments for the relevant period.
    - Using Fully Homomorphic Encryption (FHE), the Oracles collaboratively compute a cryptographic hash of the *combined* log entries, without ever decrypting the individual entries.
    - The resulting FHE-computed hash is a short, fixed-size "fingerprint" of the audit log for that period.

17. **On-Chain Hash Recording:**

    - The FHE-computed hash is published to the TPIF blockchain via a smart contract. This hash serves as a tamper-proof commitment to the off-chain audit log.

6. Benefits of TPIF: A Transformative Approach

TPIF offers significant advantages over existing identity systems, addressing critical challenges and creating a more trustworthy and user-centric digital environment. The benefits are transformative for all stakeholders:

- **For Users:**
    - **Enhanced Privacy:** Granular control over identity data, with options ranging from complete anonymity (with proof of personhood) to selective disclosure.
    - **Greater Security:** Reduced risk of identity theft, fraud, and online abuse.
    - **Empowerment:** True control over their digital identities and online interactions.
    - **Digital Inclusion:** Safer and more equitable participation in the digital world, especially for marginalized groups.
- **For Platforms (Social Media, Online Services):**
    - **Increased Trust:** Verified identities enhance platform credibility and user trust.
    - **Improved Content Quality:** Algorithms can prioritize content from verified human users, reducing the impact of bots and disinformation.
    - **Safer Environments:** More effective content moderation and reduced spam/abuse.
    - **Enhanced Engagement:** A more trustworthy environment fosters greater user participation and interaction.
- **For Governments and Organizations:**

- **Secure and Efficient Verification:** Streamlined identity verification processes for services, reducing costs and improving efficiency.
- **Enhanced Cybersecurity:** Reduced risk of data breaches and improved resilience.
- **Privacy-Preserving Data Sharing:** Facilitates secure and compliant data sharing across borders.
- **Stronger Governance:** A foundation for more trustworthy and privacy-respecting digital governance.

TPIF's tiered approach, combined with its advanced cryptographic underpinnings, delivers a unique combination of privacy, security, and usability, addressing the limitations of both centralized and fully decentralized identity systems.

7. Call to Action and Future Vision

TPIF presents a pragmatic and adaptable solution to the pressing challenges of online identity and trust. It offers a path towards a digital future where privacy is respected, users are empowered, and interactions are secure and accountable. TPIF's tiered approach, built upon a foundation of strong cryptography and decentralized governance, provides a flexible framework for a wide range of applications, from anonymous online forums to regulated financial transactions.

We invite developers, researchers, organizations, and individuals to join us in building this future. TPIF is envisioned as an open-source, community-driven project. Your contributions, feedback, and participation are essential to its success.

Key next steps for TPIF include:

- **Prototype Development:** Building working prototypes of the core TPIF components.
- **Consortium Formation:** Establishing the initial consortium of trusted organizations.
- **Community Building:** Engaging with the broader digital identity community.
- **Rigorous Testing:** Conducting extensive security audits and performance benchmarking.
- **Further Research:** Exploring advancements in cryptography and decentralized technologies.

TPIF is more than just a technical framework; it's a vision for a more equitable and trustworthy digital ecosystem. By working together, we can make this vision a reality. A more detailed technical paper will follow, providing further specifications and implementation details.

11. References

Allen, C. (2016). The Path to Self-Sovereign Identity. https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/The-Path-to-Self-Sovereign-Identity.md

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., … Yellick, J. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. Proceedings of the Thirteenth EuroSys Conference. https://doi.org/10.1145/3190508.3190538

Ben-Sasson, E., Chiesa, A., Genkin, D., Tromer, E., & Virza, M. (2013). SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge. Cryptology ePrint Archive, Paper 2013/507. https://eprint.iacr.org/2013/507

Ben-Sasson, E., Bentov, I., Horesh, Y., & Riabzev, M. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. IEEE Symposium on Security and Privacy. https://doi.org/10.1109/SP.2014.36

BrightID. (n.d.). BrightID. Retrieved March 24, 2025, from https://www.brightid.org/

Buterin, V. (2023, July 24). What do I think about biometric proof of personhood? Vitalik Buterin's website. https://vitalik.ca/general/2023/07/24/biometricproofofpersonhood.html

Camenisch, J., & Lysyanskaya, A. (2001). An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. EUROCRYPT. https://doi.org/10.1007/3-540-44987-6_8

Chaum, D. (1985). Security without identification: Transaction systems to make big brother obsolete. Communications of the ACM, 28(10), 1030-1044. https://doi.org/10.1145/4372.4373

Cheon, J. H., Kim, A., Kim, M., & Song, Y. (2017). Homomorphic encryption for arithmetic of approximate numbers. Advances in cryptology–CRYPTO 2017: 37th annual international cryptology conference, Santa Barbara, CA, USA, August 20–24, 2017, proceedings, part III 37. Springer, Cham, 409-437.

CNIL. (2018, September 6). Solutions for a responsible use of the blockchain in the context of personal data. https://www.cnil.fr/en/first-elements-analysis-cnil

CT Insider. (2022). Amazon fake reviews: How to spot them and what CT is doing about it. https://www.ctinsider.com/politics/article/amazon-fake-reviews-connecticut-17632471.php

El-Hajj, M. I., Fadlallah, C., Chamoun, M., & Serhrouchni, A. (2022). A Survey of Zero-Knowledge Proofs: Advancements and Applications in Blockchain Technology. 2022 International Conference on Cyber Security and Resilience (CSR), 1-10. https://doi.org/10.1109/CSR54659.2022.9850286

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The Rise of Social Bots. Communications of the ACM. https://doi.org/10.1145/2818717

GAO. (2018). INTELLECTUAL PROPERTY -Agencies Can Improve Efforts to Address Risks Posed by Changing Counterfeits Market. GAO-22-106029. https://www.gao.gov/assets/gao-18-216.pdf

Gentry, C. (2009). Fully Homomorphic Encryption Using Ideal Lattices. Proceedings of the 41st Annual ACM Symposium on Theory of Computing. https://doi.org/10.1145/1536414.1536440

Goldreich, O., Micali, S., & Wigderson, A. (1991). Proofs that Yield Nothing but Their Validity. Journal of the ACM. https://doi.org/10.1145/103418.103439

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). Digital identity guidelines (NIST Special Publication 800-63-3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-3

Hyperledger Indy. (2019). AnonCreds Specification. Hyperledger. https://hyperledger.github.io/anoncreds-spec/

Imperva. (2024) 2024 Bad Bot Report. https://www.imperva.com/resources/resource-library/reports/2024-bad-bot-report/

IPFS. (2024). (Assuming IPFS has a general homepage or whitepaper that could be cited, insert relevant citation here. If not a formal citation, consider removing '(IPFS, 2024)' recommendation).

Kim, J., Bakhtiari, S., Chen, H., Darup, D., Kim, M., Lee, E., Nalla, S., Puranik, N., Rahimi, A., Rathee, D., Sakzad, A., Shrestha, R., & Wang, X. (2024). Cheddar: A Swift Fully Homomorphic Encryption Library for CUDA GPUs. https://arxiv.org/pdf/2407.13055

Kleros. (n.d.). Proof of Humanity - A Decentralized Human Verification System for Web3. Retrieved March 24, 2025, from https://poh.eth.limo/

Lundkvist, P. (2022). ID.me's Proof-of-Personhood Problem. Idenitity.com https://www.identity.com/id-mes-proof-of-personhood-problem/

Mijic, M., & Ramachandran, L. (2023, August 3). Kenya suspends Worldcoin over privacy concerns; Europe investigating. CoinDesk. https://www.coindesk.com/policy/2023/08/02/kenya-suspends-worldcoin-over-privacy-concerns-europe-investigating/

NY Times. How to Spot Fake Amazon Reviews and Other Online Shopping Scams. https://www.nytimes.com/wirecutter/blog/amazon-counterfeit-fake-products/

Open Identity Exchange. (2021). Self-Sovereign Identity and GDPR: OIX White Paper May 2021. https://www.openidentityexchange.org/file-download/download/public/167

Perkins Coie, LLP. (2018). Legal Considerations for Blockchain-Based Identity Systems. https://www.perkinscoie.com/en/news-insights/legal-considerations-for-blockchain-based-identity-systems.html

Preukschat, A., & Reed, D. (2021). Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials. Manning Publications.

Rao, S. (2019, August 28). A Deep Dive into STARKs vs SNARKs. ConsenSys. https://consensys.net/blog/blockchain-explained/a-deep-dive-into-starks-vs-snarks/

Shuting Ada Wang, Min-Seok Pang & Paul A. Pavlou (2018). Cure or Poison? Identity Verification and the Spread of Fake News on Social Media. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3249479

Sovrin Foundation. (2018). Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust. https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

Tools for Humanity. (2023). World ID: Technical Overview. Worldcoin. https://worldcoin.org/whitepaper-world-id

W3C. (2022). Decentralized Identifiers (DIDs) v1.0. https://www.w3.org/TR/did-core/

W3C. (2022). Verifiable Credentials Data Model v1.1. https://www.w3.org/TR/vc-data-model/

World Bank. (2018). ID4D Identification Assurance Framework. https://documents1.worldbank.org/curated/en/395571543521237173/pdf/ID4D-Identification-Assurance-Framework-v2-0.pdf

Yao, A. C. (1982). Protocols for Secure Computations. 23rd Annual Symposium on Foundations of Computer Science. https://doi.org/10.1109/SFCS.1982.38

Zavodny, J., Schuchard, M., Peebles, R., Knysz, M., & Shankar, A. (2014). Cirrus: A system for scalable, always-on identity and access management. 2014 IEEE 34th International Conference on Distributed Computing Systems Workshops, 105-110. https://doi.org/10.1109/ICDCSW.2014.27