Nullproof

NullProof

The Role-Based Access Protocol for Web3

Verifiable Onchain Credentials × AI-Based Identity

White paper

Version 1 — August 2025

Index

1. Introduction

The Identity Paradox in Web3

Web3, by its very nature, champions decentralization — removing intermediaries, empowering individuals, and creating open ecosystems. Yet, when it comes to verifying identity and legitimacy, the space remains paradoxically dependent on centralized platforms, manual attestations, and opaque reputation systems.

Whether you're a founder looking to join an incubator DAO, an investor exploring early-stage protocols, or a contributor proving your merit across GitHub or governance forums, there's no unified, trustless method to establish who you are — or more importantly, what you've done.

This fragmented approach to identity is not only inefficient but restricts access, slows onboarding, and excludes high-potential users who lack "visible credentials" but possess real contributions.

NullProof: ZK-Native Role Verification

NullProof is redefining access in Web3 by introducing a privacy-preserving, zero-knowledge-based role verification protocol.

We combine:

- On-chain activity (wallet behaviors, protocol interactions),
- Off-chain data (social scores, GitHub repos, funding records), and
- AI-based scoring models

…to create a verifiable role identity for every user — whether you're a founder, contributor, or investor.

Using zk-SNARKs, we generate proofs of identity roles without ever revealing the underlying data. This ensures full privacy, interoperability, and on-chain verifiability — enabling dApps, DAOs, and protocols to gate access, distribute incentives, or govern participation based on what you've done, not just what you claim.

2. The Access Crisis in Web3

Web3 promised a new paradigm — one where anyone, anywhere, could participate in decentralized ecosystems. Yet, beneath this promise lies a fundamental flaw: while wallets are pseudonymous by design, access in Web3 is not.

Identity Without Context

Wallet addresses — the backbone of user interaction in blockchain applications — offer little more than a string of alphanumeric characters. They carry no context, no reputation, no provable background about the person behind them.

As a result, protocols and platforms are left to guess:

- Is this user a real contributor, or a Sybil attacker farming airdrops?

- Is this wallet owned by a credible investor, or just another fundless address?

- Is this participant a proven founder, or someone impersonating one?

This uncertainty is breaking the trust layer needed to scale Web3 coordination.

DAO Participation Is Risky

DAOs face this crisis daily. Without verifiable proof of identity or contribution:

- Governance proposals are influenced by unvetted wallets.

- Funding decisions often fall prey to clout-based favoritism.

- Early access opportunities are gamed by botnets and mercenaries.

Protocols often resort to centralized KYC, Discord screenshots, manual GitHub checks — defeating the very ethos of decentralization.

Broken Onboarding in Web3

The onboarding journey — into token launches, grants, accelerators, or protocol roles — remains manual, opaque, and trust-based. We rely on:

- Subjective referrals
- Discord applications
- Twitter clout

This is unsustainable, especially as Web3 matures into multi-billion dollar ecosystems.

3. Our Vision: Access, Not Assumptions

At the heart of Web3 lies a core principle — permissionless participation. But true permissionlessness cannot exist without credible, decentralized access control. Today, too much of the Web3 ecosystem runs on assumptions, not verifiable identity:

- A Twitter bio says "Founder" — we assume it's true.
- A wallet holds a few tokens — we assume it's legitimate.
- A GitHub handle is linked — we assume it's the real contributor.

NullProof Envisions a Better Future

We believe that credibility shouldn't come at the cost of privacy, and identity shouldn't require doxxing. That's why NullProof is built on a different foundation — verifiable roles, not unverifiable claims.

In our vision:

- Identity isn't exposed — it's cryptographically proven.
  Users retain privacy while still demonstrating provable legitimacy through zero-knowledge proofs.
- Credentials aren't bought — they're earned.
  Roles like *Contributor*, *Investor*, or *Founder* are assigned based on transparent, on-chain and off-chain metrics — not just self-claims.
- Access isn't gated by clout — it's enabled by merit.
  Whether you want to join a DAO, apply for a grant, or participate in governance, you're evaluated by what you've done, not who you know.

Credibility Without Compromise

NullProof is building the infrastructure to make this future real — where:

- AI models analyze behavioral signals across data layers.
- zk-SNARKs ensure user privacy while generating trustless credentials.
- Verifiable Credentials (VCs) empower users to control and present their identity anywhere across the decentralized web.

We're not here to replace Web3 identity.
We're here to upgrade it — from trust-based access to proof-based credibility.

4. The NullProof Protocol

NullProof is a modular, interoperable protocol designed to verify roles without compromising user privacy. It provides a new way for users to prove who they are and what they've done, without ever revealing sensitive personal information.

At its core, NullProof brings together zero-knowledge cryptography, decentralized identifiers, and AI-driven scoring to enable programmable access based on verifiable, earned credentials.

Key Capabilities of NullProof

Generate zk-Proofs of Role & Reputation
Users can create zero-knowledge proofs that attest to their status as a *founder*, *contributor*, or *investor* — backed by a scoring model that processes both on-chain and off-chain data. These proofs are:

- Privacy-preserving
- Non-transferable
- Verifiable on-chain

Issue Verifiable Credentials (VCs)
NullProof supports the generation of W3C-compliant Verifiable Credentials based on user activity from:

- GitHub repositories
- Social graphs
- DAO voting and governance
- On-chain interactions (wallet behavior, funding activity)

Mint Access Badges with ERC-20 Tokens
Once verified, users can mint unique identity badges (e.g. "Verified Founder" or "Top Contributor") by paying in AGT, the protocol's native ERC-20 utility token. These badges are:

- Role-bound
- Non-fungible
- Required for unlocking certain gated dApp experiences

Cross-App Interoperability
NullProof is built for seamless integration with partner dApps and DAOs. Once users generate a zk-proof and mint a credential, they can:

- Log in to participating dApps
- Join gated Telegram or Discord communities
- Claim access to airdrops, bounties, and exclusive events
- Participate in role-based governance

5. Key Platform Features

NullProof is more than a protocol — it's a complete identity infrastructure that reimagines access, reputation, and role verification in Web3. Each core feature is purpose-built to deliver verifiability, privacy, and utility, leveraging the latest in AI and cryptography.

AI-Driven Role Assessment

NullProof employs a custom-trained AI/ML engine to evaluate both on-chain and off-chain behavior. This model assigns dynamic reputation scores that help determine a user's most likely role — whether they are a Founder, Contributor, or Investor — based on provable activity such as:

- GitHub contributions
- Investment transactions
- DAO participation
- Community engagement

This allows the platform to move away from static, self-claimed roles and toward merit-based, data-driven identity classification.

ZK-Proof Credentialing

At the heart of NullProof lies zero-knowledge cryptography, which allows users to prove their credentials without revealing the raw data. Users generate zk-proofs that attest to:

- Contribution history
- Investment activity
- Founder status

These proofs are verifiable on-chain and can be used across dApps, enabling seamless, trustless access control while preserving user privacy.

NFT Badge Minting

Once verified, users can mint role-based badges — soulbound NFTs that represent their earned identity on-chain. These badges are:

- Non-transferable (SBTs)
- Tied to verified credentials
- Used to unlock access to DAOs, token-gated events, or specialized dashboards

Users pay for badge minting using AGT, NullProof's native ERC-20 utility token — creating an economic layer on top of identity.

Verifiable Credentials (VC) Integration

NullProof supports the W3C Verifiable Credential standard, allowing users to generate, own, and present cryptographically signed credentials based on:

- GitHub repositories
- Twitter handles
- Discord community roles
- DAO governance records

These VCs can be stored locally or through a DID (Decentralized Identifier), and shared with dApps or DAOs as proof of legitimacy — without revealing sensitive personal information.

On-Chain / Off-Chain Analytics Engine

NullProof integrates a powerful analytics engine that fetches, parses, and correlates:

- On-chain data: wallet transactions, protocol interactions, DAO votes
- Off-chain data: GitHub activity, forum presence, social engagement

This hybrid engine forms the foundation of role scoring and zk-proof generation. It ensures that all data driving credentialing is transparent, tamper-resistant, and cryptographically verifiable.

Together, these features form the backbone of a trustless identity stack that's built for the next generation of decentralized ecosystems.

6. Market Opportunity

The decentralized web is at an inflection point — as billions of dollars flow through DAOs, protocols, and tokenized networks, identity and access control have become mission-critical. Yet, traditional methods of verification — from centralized KYC to social handles — are fundamentally misaligned with the ethos of Web3.

This disconnect creates an enormous opportunity: the infrastructure to support decentralized, verifiable identity.

Web3 Identity Market: $30B+ by 2030

Analysts project the Web3 identity market to surpass $30 billion by 2030, fueled by:

- Decentralized finance (DeFi) requiring Sybil-resistant reputation
- DAOs managing billions in treasury needing role-based permissions
- On-chain credentials unlocking everything from credit to community access

As protocols evolve, identity becomes the gateway to value, governance, and coordination.

Rise of AI + DID-Based Identity Systems

With the rise of decentralized identifiers (DIDs) and AI-powered reputation models, new frameworks are emerging to:

- Contextualize user actions
- Classify roles based on provable contribution
- Enable logic-based identity that adapts in real time

NullProof sits at the convergence of these trends — bringing AI to identity, and privacy to reputation.

7. Competitive Landscape

As identity continues to evolve in Web3, several projects have emerged to tackle elements of the identity stack — from naming systems to social graphs to reputation scores. However, most existing solutions lack programmable, verifiable access control and do not utilize zero-knowledge (ZK) cryptography to ensure privacy.

NullProof is uniquely positioned in this landscape as a ZK-native access protocol with AI-based role scoring, offering a more complete, secure, and composable identity layer.

Project	Primary Focus	Zk-Native	Role scoring
ENS	Human-Readable Names	No	No
Gitcoin	Identity Reputation	No	Partial
Lens Protocol	Decentralized social graph	No	No
NullProof	Zk-Based access control	Yes	Yes

Strategic Advantage of NullProof

Unlike point solutions, NullProof is built as a complete, modular access framework:

- ZK-native from the ground up
- Real-time scoring with AI
- Integrates GitHub, social, DAO, and on-chain activity
- Exports role-based credentials for any Web3 app

This positions NullProof as the infrastructure layer for access in the decentralized identity economy.

8. Tokenomics & DAO

At the core of the NullProof protocol lies AGT, a native ERC-20 utility token designed to power the role-based access and governance ecosystem. Unlike traditional utility tokens, AGT is directly tied to verifiable identity and earned credentials, making it an integral part of user engagement, governance, and protocol expansion.

🔹 Token Name: AGT

🔹 Type: ERC-20 (Ethereum, Sepolia/Testnet-compatible)

Utility of AGT Token

AGT is the fuel that enables participants in the NullProof ecosystem to interact with protocol features in a permissionless, verifiable, and incentivized manner. Its use cases are tightly coupled with role-based access and identity verification:

1. Role Badge Minting

Users who generate valid ZK-proofs of their contributions or credentials can mint soulbound role badges (e.g., Founder, Contributor, Investor) by paying a small fee in AGT.
 This creates a proof-of-participation trail and discourages fake or spammed role claims.

2. Contributor Incentives

DAO contributors, developers, and community participants can earn AGT tokens through:

- Submitting pull requests or code
- Creating verified content or community guides
- Participating in DAO governance, research, or audits

This makes AGT a mechanism for attribution and reward tied to meaningful identity-driven engagement.

3. Access Gating

AGT can be used as a gating layer to unlock:

- Partner dApps
- Token-gated communities
- Special dashboards, analytics, or data APIs

By coupling identity + access, NullProof ensures utility = earned permission, not just token possession.

4. DAO Participation

AGT token holders form the backbone of the protocol's governance. They can:

- Propose changes to scoring algorithms

- Vote on new badge categories
- Approve integrations with third-party dApps
- Allocate treasury funds for grants and ecosystem development

DAO Voting

NullProof is governed by a community-owned DAO, where AGT holders vote on all major protocol-level decisions. The DAO governs:

- Feature Releases: Should a new verification method be added (e.g., proof of event attendance, podcast guesting)?
- Badge Eligibility Criteria: Who qualifies as a founder? What GitHub reputation threshold defines a contributor?
- Treasury Disbursement: What projects or community efforts receive funding?

Governance is executed using on-chain voting smart contracts, ensuring transparency, immutability, and decentralization.

9. Go-To-Market Strategy

Bringing a novel, privacy-preserving access protocol like NullProof to market requires more than a launch — it demands a strategic entry into high-signal, identity-sensitive Web3 ecosystems. Our go-to-market (GTM) approach is designed to validate the protocol with real users, demonstrate utility across key use cases, and build early network effects with credibility-focused partners.

1. Strategic Launch: Hack2Launch by Dcodeblock

We're launching NullProof's MVP at Hack2Launch, one of the premier hackathons hosted by Dcodeblock, a key player in the developer-first Web3 ecosystem.

- Community Reach: Hundreds of builders, early-stage startups, and investors
- Live Use Cases: NullProof will be deployed as a trust layer in hackathon teams' applications
- Developer Feedback Loop: Real-time testing, bug bounty challenges, and idea validation

This event positions NullProof in front of high-intent, high-utility users from Day 1.

2. Partnerships with Early-Stage DAOs

DAOs are among the biggest beneficiaries of verifiable, zero-knowledge role access.

We'll onboard small to mid-sized DAOs who face:

- Bot spam in proposal voting
- Difficulty filtering real contributors
- Poor contributor attribution models

These DAOs will use NullProof to:

- Gate governance access
- Issue contributor badges
- Analyze on/off-chain reputation for roles

3. Onboarding Founders, Contributors, and VCs

Our immediate onboarding focus includes:

- Founders who need verifiable profiles to pitch VCs
- Contributors seeking to prove their portfolio across ecosystems
- Investors desiring identity-based access to gated launches or deal flow

By targeting this core triangle of Web3 actors, we build both demand and credibility for our role verification system.

These stakeholders will get access to:

- Identity badge minting
- Custom dashboards showing verifiable contributions
- Privileged access to gated product and DAO launches

4. SDK for Third-Party Protocols

To accelerate adoption, NullProof will release a lightweight, modular SDK that can be integrated into any:

- dApp
- Governance platform
- Credential system
- Reputation protocol

The SDK will allow developers to:

- Request zk-proofs from NullProof identities
- Read user badges and access roles
- Define gating logic in minutes

This modularity turns NullProof into a plug-and-play layer for trust, making access programmable across the decentralized web.

10. Roadmap

NullProof is built to evolve — from a zero-knowledge verification tool into the infrastructure backbone of access, identity, and trust across Web3 ecosystems. Our roadmap is designed to align product maturity with ecosystem readiness, ensuring that each phase of the journey introduces tangible value to our users, developers, and partners.

Q3 2025 — MVP & Virtuals Launch

Milestone: MVP Ready for Demo & Use

- First working version of the NullProof protocol
- Verification for Founders, Contributors, and Investors via ZK-proofs
- Basic badge minting enabled with AGT token
- Hosted on Sepolia Testnet and deployed to Ethereum Mainnet

Virtuals Demo Day

- Live launch at Hack2Launch by Dcodeblock
- Initial DAO integrations & feedback loop with early contributors

Q4 2025 — DAO & Governance Rollout

Governance Module Launch

- On-chain voting for badge types, eligibility scores, and protocol upgrades
- Community can propose and vote using AGT tokens

Partnership Integrations Begin

- Collaborative onboards with DAOs and dApps focused on reputation, credentials, or gated access
- Begin integration with grant platforms, incubators, and developer communities

Community Building Campaigns

- Launch of ambassador, bounty, and contributor programs
- AGT incentive pools for early adopters and ecosystem testers

Q1 2026 — SDK, API, & Custom Badge Layer

SDK for Developers

- Plug-and-play SDK to embed NullProof verification and badge gating in third-party dApps
- GitHub repo, examples, and support documentation included

API Suite for Protocol Access

- REST + GraphQL APIs for integrating verification, roles, and badges
- Identity scoring endpoints with optional off-chain data

Custom Badges Marketplace

- Allow dApps and DAOs to mint custom role badges for their ecosystem
- Payable in AGT, with DAO-curated templates and listing guidelines

Mobile Integration (Phase I)

- React Native support for mobile dApps and Web3 wallets
- In-app badge verification via QR and link-based proofs

Q2 2026 — Expansion Layer: Mentorship + Cross-Chain

Mentorship & Role Networking Layer

- Enable verified contributors/founders to join mentorship communities
- AI-based matching for guidance, teaming, and hiring based on badge history

Cross-Chain ZK Proofs

- Integrate ZK-verifiable credentials for Solana, Polygon, Optimism, and BSV chains
- Expand DID verification across L2s and multi-chain ecosystems

Proof Interoperability Standards

- Collaborate with DID, ZK, and VC ecosystems to enable shared identity proof standards
- Proposals for EIP/ERC status around ZK-role proofs

11. Team

Sharath Kariyappa - Founder & Lead Blockchain Developer

Professional Background:

- Currently serving as Software Development Engineer at Timechain Labs
- Extensive experience in blockchain development and Web3 technologies
- Lead developer for Neucron Wallet
- Deep expertise in smart contract development and DeFi protocols

Technical Expertise:

- **Blockchain Development**: Solidity, Web3.js, Ethers.js, Smart Contract Security
- **Full-Stack Development**: React, Node.js, TypeScript, Python
- **AI/ML Integration**: Machine learning model integration in blockchain applications
- **System Architecture**: Scalable distributed systems and microservices
- **Security**: Zero-knowledge proofs, cryptographic protocols, and secure system design