Public Respect Protocol (PRP) White Paper

The World's First Decentralised Reputation Economy

***Token**: PR (Public Respect)*

***Network**: Polygon*

***Application**: https://publicrespect.app*

***Website**: https://publicrespect.com*

***Contact**: info@publicrespect.com*

***Document Version**: 1.0*

***Security Standard**: ECDSA Signature Verification*

***Governance Model**: 10-Vote Consensus Jury*

1. Introduction and Abstract

Human society has always operated on the foundation of reputation, yet the architecture of the internet failed to create a native system for trust, accountability, and measurement. While the digital world has achieved unprecedented scale for communication, it has simultaneously created a vacuum where influence is rewarded without integrity and visibility exists without responsibility. On modern platforms, value flows without verification, and "social capital" is often nothing more than a superficial metric.

The Public Respect Protocol (PRP) introduces a new primitive to the digital world: cryptographically verifiable, community-enforced respect as an economic signal. This protocol transforms human behavior—honesty, contribution, judgment, and participation—into a measurable, on-chain asset class. PRP does not monetize attention, reward virality, or sell influence. Instead, it creates an economy where respect itself becomes capital—earned through action, validated by community consensus, and settled transparently on the blockchain. Through decentralized governance and real human verification, PRP establishes reputation as a scarce, earned, and defensible resource.

Key Principles:

- Verifiable Trust: PRP provides the first cryptographically secured reputation layer.

- Behavior as Capital: Human integrity is transformed into a measurable asset.

- Decentralized Settlement: Respect is settled on-chain, free from corporate control.

- Economic Enforcement: Reputation is backed by real value and community consensus.

By treating respect as capital—earned through action, validated by community consensus, and settled on the Polygon blockchain—PRP establishes a trust layer that is scarce, defensible, and globally interoperable.

2. The Problem: Reputation Has No Native Economy

Every digital system today relies on reputation—from hiring and governance to moderation and trust—yet reputation remains fundamentally broken. Current systems are fragmented across isolated platforms, making it impossible to verify a user's global standing. Furthermore, these systems are centrally controlled and easily manipulated; likes can be bought, followers can be faked, and reviews can be gamed.

Modern platforms monetize attention rather than trust. Because there is no universal, trust-minimized reputation layer, there is no inherent cost to dishonesty and no tangible reward for long-term integrity. When reputation is platform-bound and non-transferable, the user loses their history the moment they leave a service. This lack of a native currency for reputation means the internet lacks a persistent and economically meaningful layer of accountability.

Core Issues:

- Fragmentation: Reputation is currently locked in silos and non-transferable.

- Manipulation: Existing trust signals (likes/followers) are easily faked or bought.

- Centralization: Platforms can delete or alter reputation at their own discretion.

- Costlessness: There is currently no economic penalty for being dishonest online.

- Zero-Cost Signaling: "Likes" and "Follows" are free to generate, leading to bot-driven manipulation and sybil attacks.

- Absence of Penalty: There is no financial or social cost for dishonesty or harassment beyond localized platform bans.

3. The Core Insight: Reputation Behaves Like Money

Reputation only becomes truly valuable when it is both costly to earn and costly to lose. In the physical world, reputation compounds over time, trust unlocks unique opportunities, and high credibility lowers the friction of doing business. Conversely, bad behavior carries a real-world cost.

PRP formalizes this reality by treating reputation as an economic primitive governed by transparent rules instead of platform-specific algorithms. It is not a mere "social score" or a badge of honor; it is a settlement layer for human behavior. By anchoring reputation to economic signals, the protocol ensures that respect requires risk, validation requires community judgment, and value follows behavior rather than popularity.

Key Concepts:

- Costly Signaling: Value is derived from the difficulty of earning and keeping it.

- Economic Primitive: Reputation is treated as a foundational rule-based system.

- Settlement Layer: PRP acts as the final judge for human behavior on-chain.

- Risk-Based Trust: True respect requires participants to have "skin in the game."

4. Core Economic Units and Conversion

The PRP economy operates on a dual-token/point system to balance social interaction with financial liquidity:

- Respect Points (RP): The atomic unit of reputation. These are whole integers representing a user's total accumulated social capital.

- PR Currency: The withdrawable, liquid utility token. This acts as the bridge between social reputation and real-world value.

The Conversion Metric:

1,000,000 Respect Points = 1 PR Currency

5. What is the PR Token?

PR (Public Respect) is the native utility token that powers the entire ecosystem. It functions as the anchor that ties abstract reputation to real economic consequences. It is intentionally designed as a utility tool for protocol operation rather than a speculative asset or a yield-bearing token.

The PR token is required to unlock withdrawals, participate in governance, and prove real usage of the system. It prevents "zero-cost abuse" because users must have skin in the game to interact with the protocol's higher functions. PR cannot be printed endlessly or auto-generated by the system; once the initial distribution concludes, the token exists only through peer-to-peer exchange, ensuring that market demand grows alongside the usage of the protocol.

Token Features:

- Utility Focus: PR is designed for protocol operation, not mere speculation.

- Access Asset: Required for withdrawals, governance, and high-integrity actions.

- Fixed Supply: Cannot be printed or inflated by administrators. Hard cap of 30,000,000 tokens with zero inflation.

- Anti-Abuse Anchor: Prevents bots and bad actors by creating economic friction.

- Deflationary Pressure: Includes a configurable burnPercent (defaulting to 20%) during withdrawals, where this percentage of tokens is permanently destroyed.

The token is used for withdrawals, purchases, and as the ultimate settlement unit for validated reputation.

6. What is the Public Respect Protocol (PRP)?

PRP is the underlying rule engine and "social operating system" that dictates how respect is issued, how disputes are resolved, and how value is distributed. It replaces the subjective and often biased moderation of centralized platforms with deterministic, economic accountability.

Every rule within the protocol is explicit and every outcome is auditable on-chain. By moving away from "trusting the platform" and moving toward trusting mathematics and aligned incentives, PRP ensures a neutral environment. The protocol operates without administrative discretion, meaning that no single entity can override the collective judgment of the community or manipulate the outcomes of the reputation economy.

Protocol Attributes:

- Rule Engine: A deterministic system for issuing and validating respect.
- Auditability: Every transaction and dispute is recorded transparently on-chain.
- Neutrality: Replaces biased platform moderators with objective mathematics.
- Zero Discretion: No admin can override the consensus of the protocol rules.

7. The Public Respect App

The Public Respect App serves as the living interface for the protocol. It is a non-custodial, mobile or desktop-first gateway that allows humans to manage their wallet-based identities. Through the app, users can earn respect through meaningful interactions, challenge or validate the behavior of others, and vote on "social truth."

Crucially, the app does not custody user funds or control the outcomes of transactions. It merely executes the logic defined by the protocol. It renders the underlying on-chain data into a usable social experience, allowing users to track their reputation history and convert their earned standing into economic value within the guidelines of the system.

App Features:

- User Gateway: The primary interface for interacting with the reputation economy.
- Non-Custodial: The app does not hold user funds or control user identities.
- Interactive Governance: Allows for voting on social truths and validating behavior.
- Protocol Execution: The app serves as a renderer for protocol-level data.
- UI/UX Design: Dark Mode implemented for all components using a dark gray/black palette (1a1a1a). Mobile-First WalletConnect with 1-second delayed guidance for mobile users. Respect Graph: A cumulative line chart on every profile visualizing reputation growth over time.

8. Identity and Ownership

PRP utilizes cryptographic wallets for authentication rather than traditional emails or passwords. This creates a paradigm of identity without centralized ownership. Each profile represents a persistent on-chain identity that houses a cumulative history of a user's behavior.

Because the history is tied to the wallet and recorded on the Polygon network, a user’s reputation cannot be reset by simply creating a new account. This continuity of identity ensures that a user’s economic footprint and social history follow them everywhere, creating a sense of permanent accountability that is absent in the anonymous or semi-anonymous "throwaway" culture of the current web.

Identity Features:

- Wallet-Based: Authentication via cryptography instead of centralized emails.
- Persistence: Reputation history is permanent and follows the wallet.
- Accountability: Users cannot simply "reset" their history with a new account.
- User Sovereignty: Identity and reputation belong to the user, not the app.

Authentication Flow:

- Request: User sends wallet address to /api/auth/request-message.

- Challenge: Backend generates a unique random string.

- Sign: User signs the message via their wallet (MetaMask, WalletConnect).

- Verify: Backend uses eth-account to verify the signature.

- Token: A JWT (JSON Web Token) is issued, containing the wallet address and expiration.

9. Respect as a Costly Signal: The Pledge System

In the Public Respect Protocol, giving respect is never a free or impulsive action. Every time a user grants respect to another, they must provide a 12% pledge which is temporarily locked until the transaction is finalized by community judgment.

This pledge system serves as the core anti-spam mechanism of the protocol. It introduces economic friction that forces sincerity of intent. If a user attempts to game the system through empty praise or malicious attacks, they risk losing their pledge. This ensures that every respect action recorded on the protocol carries weight and represents a genuine, considered opinion backed by capital.

Pledge Mechanics:

- 12% Pledge: A mandatory temporary lock of funds for every respect action.
- Economic Friction: Prevents impulsive behavior and mass-spamming of likes.
- Integrity Anchor: Ensures every signal has a tangible cost attached to it.
- Risk vs. Reward: Givers must stand by their judgment with financial backing.

Calculation Logic:

- Pledge (P): Fixed at 12% of the respect amount (R).

- Total Initial Cost for Giver: |R| + P.

10. Community as the Court: Distributed Governance

To prevent collusion and the concentration of power, PRP replaces centralized moderators with a distributed jury of peers. No respect transaction is finalized until it has passed through a community voting process. This requires a minimum of 10 independent votes and a majority consensus to settle.

Voters are not merely expressing an opinion; they are performing a service for the protocol and are rewarded for their participation. This turns governance from an ignored burden into an active earning activity. By rewarding honest arbitration, the protocol ensures that "truth" is decided by those with aligned incentives rather than those with the most political power or platform influence.

Governance Details:

- Decentralized Jury: Reputation actions are finalized by 10+ independent peers.

- Consensus Settlement: Truth is determined by majority community agreement (6+ / 10 votes for approval or rejection).

- Incentivized Voting: Participants are paid to maintain system integrity.

- Anti-Collusion: Removes power from central authorities and spreads it to the crowd.

- Anonymity Protocol: To prevent social retaliation, the Sender's identity is hidden during the voting process, while the Receiver remains visible for character assessment.

- Finality Requirement: Exactly 10 votes are required for a transaction to exit the "Pending" state.

11. Incentive Geometry and Economic Flow

The protocol is designed as a behaviorally optimized system where honest actors are rewarded and bad actors are penalized. When a transaction is approved by the community, the receiver gains validated respect, the giver receives their pledge back along with a bonus, and the voters earn fees for their labor.

If a transaction is rejected, the respect does not transfer, penalties are applied to the parties involved, and the voters are still compensated for their work in protecting the system. This creates a "long-term honesty equilibrium" where the most profitable path for any participant is to act with integrity.

Approval Distribution (Majority Consensus: 10 Approvals):

- Voter Pool (Vp): 10% of the Pledge.
- Receiver Gains: R - Vp.
- Giver Gains: P + (0.20 × |R|) (Deposit returned + 20% bonus).
- Each Voter Gains: Vp / 10.

Rejection Distribution (Majority Consensus: 10 Rejections):

- Receiver Gains: 2% of the Pledge (Small compensation for false targeting).
- Giver Loses: Vp (10% of the Pledge is forfeited to voters).
- Giver Penalty: P + 10% (lose extra 10% (given to voters) + pledge will be lost as penalty).
- Each Voter Gains: Vp / 10.

Overall Dynamics:

- Reward Loop: Honest givers, receivers, and voters all gain from valid actions.
- Deterrence: Rejections result in financial penalties for bad behavior.
- Non-Zero Sum: The system rewards cooperation and integrity.
- Self-Correction: The economy naturally pushes out bad actors through penalties.

12. Verification: Protecting the Economy

A critical pillar of the protocol is the requirement for manual human verification before withdrawals are permitted. While the protocol is decentralized, it is not dehumanized. This intentional step ensures that one human corresponds to one reputation and prevents automated bots from draining the economy.

Verification ensures that social proof exists beyond the protocol's code. By requiring a real person to stand behind their on-chain reputation, PRP protects its value from "extraction attacks" and ensures that the economic rewards of the system are flowing to real contributors rather than sybil networks.

Verification Process:

- Manual Verification: Required for all value withdrawals to ensure human presence.
- Anti-Bot: Prevents automated scripts from extracting value from the protocol.
- One Human, One Identity: Anchors digital reputation to real-world existence.
- System Integrity: Protects the liquidity and value of the PR token.
- Lifecycle: Link Confirmation (User locks social links like Facebook, Twitter in profile); Bio Verification (User places PRP profile URL in external bios); Manual Review (Admins check bios); Status Update (Approval grants "Verified" badge and enables withdrawals).

13. Behavioral Security: The Red Flag and Ban Mechanism

The system can "Ban" users for suspicious activity or fraudulent verification attempts. Banned users are marked with a prominent RED FLAGGED badge and placed in Read-Only Mode, disabling all economic actions including giving respect, voting, or withdrawing PR. This permanent visual warning serves as a systemic deterrent against bad behavior.

Security Features:

- Read-Only Mode: Banned users can view content but are blocked from actions.

- Visual Deterrence: Profiles display a "RED FLAGGED" banner and X-icons.

- Admin Control: Bans can be verified manual from backend.

14. Technical Architecture: PublicRespect.sol on Polygon

The protocol is powered by a robust Solidity smart contract designed for security and scalability on the Polygon network. The contract implements an ERC20-compatible token with advanced administrative and security controls. This technical foundation ensures that reputation data is permanent, transparent, and free from centralized censorship.

ECDSA Signature-Based Minting and Security:

- To prevent unauthorized supply inflation, the contract implements signature-based minting.

- Withdrawals are validated off-chain and executed on-chain using ECDSA (Elliptic Curve Digital Signature Algorithm) signatures.

- The backend contacts a dedicated signer service to facilitate this cryptographic proof.

-

Financial Security: Withdrawal Signatures:

- Request: Verified user requests withdrawal.

- Validation: Backend checks verification_status and withdrawable_balance.

- Signing: Backend generates ECDSA signature.

- Execution: User provides signature to Smart Contract on Polygon to release funds.

Operational Security:

- Daily limits: dailyLimit (default 5000 PR/day) and maxWithdrawPerTx to prevent mass extraction.

- On-Chain Proof: Every respect action is cryptographically auditable.

- Trust less Security: No custodial risk or central administrator override.

15. API Integration and Data Settlement Flow

The application architecture utilizes a FastAPI backend to manage high-frequency social interactions before they are finalized on-chain. Dedicated backend handles data persistence.

Primary API Endpoints:

- POST /api/respect/give: Initiates transaction, calculates pledge, deducts points.

- POST /api/respect/vote/{id}: Records vote, triggers distribution if 10-vote threshold met.

- GET /api/activity-logs: Returns 100 most recent activities.

- POST /api/withdraw: Initiates on-chain withdrawal via signer service.

- Authentication: Message-based wallet verification.

- Reputation Management: Profile creation, updates, respect issuance.

- Governance: Fetching pending transactions and recording votes.

- Activity Logs: Real-time tracking of protocol events.

Database Schema: Backend Collections:

- Profiles: wallet_address, username, respect_points, withdrawable_balance, verification_status, is_banned.

- Respect Transactions: from_wallet, to_wallet, pledge_amount, approvals/rejections arrays.

- Activity Logs: Timestamped events.

- Manual Reviews: Verification requests for admin auditing.

16. Tokenomics and Market Scarcity

The PR token features a fixed maximum supply of 30,000,000 tokens with no mechanism for inflation, hidden minting, or future issuance. This permanent scarcity is a fundamental design choice.

The distribution logic is structured so that early users can purchase PR directly, while later participants must acquire it from the open market. As the protocol grows and more users require PR to unlock their earned reputation or participate in governance, the fixed supply meets increasing demand. This creates structural scarcity where PR becomes a valuable access asset for anyone wishing to participate in the reputation economy.

Tokenomics Details:

- Hard Cap: Fixed supply of 30 million PR with zero inflation.

- Market-Driven: Late adopters must buy from the existing peer-to-peer market.

- Deflationary Pressure: High demand for a static supply increases utility value; 20% burn on withdrawals.

- No Hidden Reserves: Transparent distribution with no administrative minting.

- Utility Status: PR conveys no equity or profit rights; it is for access only.

17. Fear of Loss (FOL) vs. Hype

Unlike many blockchain projects that rely on the "Fear of Missing Out" (FOMO) and speculative hype cycles, PRP is driven by the "Fear of Loss." In this system, inactivity can lead to a reduction in influence, and dishonesty results in direct financial loss.

Users are incentivized to stay engaged and maintain their integrity not just because of potential future rewards, but because walking away or acting poorly has immediate and tangible consequences. Reputation decay in PRP is social and economic, ensuring that the community remains active and vigilant.

Motivational Framework:

- Active Engagement: Inactivity leads to a decay in protocol influence.
- Tangible Consequences: Bad behavior results in direct economic loss.
- Sustainable Motivation: Users stay for the value they have already built.
- Anti-Hype: Built on long-term behavioral mechanics rather than trends.

18. Roadmap and Future Applications

The evolution of PRP is divided into four distinct phases. Phase I establishes the foundation with the core app and the Genesis Race. Phase II introduces liquidity through decentralized exchange (DEX) trading. Phase III develops the internal economy, including peer-to-peer PR renting and marketplace mechanics. Finally, Phase IV builds financial bridges, including fiat integration and real-world payments.

The long-term vision for PRP is to serve as the infrastructure layer for trust across the internet. Potential use cases include decentralized hiring, DAO governance weighting, social trust verification, and digital citizenship primitives. PRP is designed to outlive digital trends by providing a permanent solution to the problem of human trust.

Phased Roadmap:

- Phase I: Core infrastructure, app launch, and Genesis Race.

- Phase II: Market discovery and DEX liquidity.

- Phase III: Advanced internal P2P economies and PR renting; expanding into Reputation NFTs, Staking Systems, and Group/Organization reputation pools.

- Phase IV: Real-world financial bridges and fiat integration.

Infrastructure Goal: To become the universal trust layer for all DAOs and digital platforms.

Security, Transparency, and Legal Standing

PRP operates through verified smart contracts on the Polygon network, providing on-chain proof for every single action. There is no custodial risk and no admin override, meaning that trust is replaced by verification.

From a legal positioning standpoint, PR is a utility token. It conveys no equity, no ownership, and no rights to profits. It represents nothing more than access, participation, and utility within the Public Respect Protocol. It is the trust layer of the decentralized world, admitting and encoding the rules that have always governed human interaction.

Final Notes:

- Protocol Permanence: Designed to be the immutable trust layer of the web.