Abstract

The Sybil problem — one entity creating multiple fake identities — has consumed decentralized identity research for over two decades. Solutions range from iris biometrics (Worldcoin) to trust graphs (BrightID) to video-based proof (Proof of Humanity), each adding cryptographic and computational complexity while introducing new attack surfaces. This paper proposes that the Sybil problem was solved by physics before computers existed: one body cannot occupy two locations simultaneously. A protocol requiring all participants on Earth to be physically co-present in groups of four or more during a single synchronized 60-minute window, four times per year, achieves 100% Sybil resistance through the constraint of embodiment. No biometrics. No graph analysis. No challenge mechanisms. The cost of this system — forced human connection — is reframed not as overhead but as its primary output.

Keywords: Sybil resistance, proof of personhood, physical attestation, co-presence, decentralized identity, BLE mesh, mandatory voting

1. Introduction

In 2002, John Douceur formalized the Sybil attack: in any system where identity is cheap, one adversary can create arbitrarily many identities and overwhelm honest participants (Douceur, 2002). Two decades of research followed, producing increasingly sophisticated defenses — all of which share a common flaw: they try to solve a physical problem with digital tools.

A human body is a physical object. It occupies one location at one time. No amount of private keys, zero-knowledge proofs, or neural network classifiers can create a second body. The entire Sybil problem reduces to a single question: **were you physically there?**

This paper presents a protocol that asks exactly that question, nothing more, and achieves what no cryptographic scheme has: complete Sybil resistance with zero false positives, zero surveillance, and zero specialized hardware.

---

2. The Failure of Digital Sybil Resistance

2.1 Biometric Approaches

Worldcoin's Orb scans the iris to create a unique biometric hash (Worldcoin Foundation, 2023). Problems:

- Requires specialized hardware ($5,000+ per Orb)
- Creates a biometric database — the exact surveillance infrastructure sovereign identity seeks to eliminate
- Iris scans can be spoofed with high-resolution images (Czajka & Bowyer, 2018)
- Cultural resistance: populations with histories of state surveillance (most of humanity) will not voluntarily scan their eyes
- Single point of failure: compromise the Orb, compromise the system

2.2 Trust Graph Approaches

BrightID builds social trust graphs where existing verified humans vouch for new ones (BrightID, 2020). Problems:

- Graph analysis can identify clusters but cannot prove absence of Sybils
- Sufficiently large coordinated groups can bootstrap fake subgraphs
- Requires continuous online presence and social graph maintenance
- Graph topology leaks social information

2.3 Challenge-Response Approaches

Proof of Humanity requires video submissions reviewed by a decentralized court (Proof of Humanity, 2021). Problems:

- Deepfakes undermine video attestation (Chesney & Citron, 2019)
- Decentralized courts create governance overhead
- Time-consuming for participants
- Disputes create adversarial dynamics

2.4 Economic Approaches

Staking mechanisms require deposits that are slashed for misbehavior. Problems:

- Wealth determines participation — the opposite of universal identity
- Well-funded adversaries absorb slashing costs
- Does not prove personhood, only capital

2.5 The Common Flaw

All digital approaches attempt to verify a physical fact (this is a unique human body) through non-physical channels. They are, fundamentally, trying to prove that matter exists using only information. This is why they fail. The answer is not better information — it is direct observation of matter.

---

3. The Protocol

3.1 Specification

1. Frequency: 4 times per year (quarterly)

2. Window: One global 60-minute window, synchronized to UTC
3. Minimum group size: 4 persons
4. Presence requirement: All members physically co-present for the full 60 minutes
5. Attestation: Each member's device (BLE-enabled) continuously broadcasts and records presence
6. Sign-off: At window close, all present members confirm the head count
7. Result: Each confirmed member receives a proof-of-presence attestation valid for the quarter

3.2 Why These Parameters

Why 4 per year? Frequent enough to maintain identity liveness. Infrequent enough to not be burdensome. Aligns with natural quarterly rhythms. Comparable to existing civic obligations (tax filing, voting in Australia).

Why 60 minutes? Long enough that a person cannot transit between two verification groups in the same window. Long enough that meaningful social interaction occurs. Short enough that it is not an imposition. Average human walking speed is 5 km/h; in 60 minutes, maximum displacement is 5 km, making simultaneous presence in two groups physically impossible for any groups separated by more than ~2.5 km.

Why 4 people minimum? Prevents trivial collusion (2-person mutual attestation). Creates a social dynamic where deception requires coordinating multiple humans willing to risk their own identity. 3 others besides yourself = majority cannot be you.

Why global synchronization? This is the critical design decision. If verification windows are flexible, one body can attend multiple groups at different times. Global synchronization makes this physically impossible. Fred cannot be in Sydney and also in Brisbane during the same 60 minutes. His body is the constraint.

3.3 The Vouch Chain

The protocol layers on an existing vouch system:

- Each person is vouched into the network by existing members
- If you don't show up for a count, your token goes dormant
- If someone you vouched for doesn't show up, your trust score degrades

- Repeated absences by your vouchees = your token goes dormant too

This creates **accountability through the vouch chain.** You don't vouch casually. You vouch for people you'll actually check on. "My vouchee is sick" is not an excuse — it's a signal to go to them. Press the emergency button on the mesh. Three people come to your door. Head count happens at your kitchen table.

3.4 Failure Modes and Recovery

Sick? Your neighbors come to you. The emergency mesh exists for exactly this. The system converts every inability into more human contact.

Offline? The BLE attestation records locally with timestamps and cryptographic signatures. When connectivity returns, the attestation syncs. The signatures prove co-presence during the window regardless of internet availability.

Remote location? Satellite BLE relay or delayed sync. The attestation is the timestamp plus the co-signed presence proof. It doesn't require real-time connectivity — just real-time co-presence.

Natural disaster? Grace period. The system knows when an entire region goes dark. Tokens in affected areas remain active until the next verification window.

---

4. Security Analysis

4.1 Sybil Cost

To create one fake identity, an attacker needs:

- 3 real, verified humans willing to attest to the fake identity's presence
- Those 3 humans must be physically present for 60 minutes, 4 times per year
- Those 3 humans risk their own identity tokens if the fake is detected

- The fake identity must never need to be present simultaneously with the attacker's real identity (impossible — they share a body)

Cost per Sybil identity: 3 corrupted humans × 4 hours/year × their own identity risk. This does not scale. Creating 1,000 Sybils requires 3,000 corrupted real humans, each staking their own identity.

4.2 Comparison to Existing Systems

SYSTEM	COST PER SYBIL	HARDWARE	SURVEILLANCE	SCALABLE ATTACK?
Worldcoin	One spoofed iris scan	$5,000 Orb	Biometric DB	Yes (manufactured scans)
BrightID	Social engineering	Phone	Social graph	Yes (fake subgraphs)
Proof of Humanity	One deepfake video	Camera	Video DB	Yes (improving deepfakes)
Staking	Capital deposit	None	Financial	Yes (well-funded adversary)
Co-Presence	3 corrupted humans/quarter	Any BLE device	None	No

4.3 The Physics Guarantee

Every digital Sybil defense has an information-theoretic attack: better fakes, more capital, larger coordinated groups operating asynchronously. Co-presence has a **physical guarantee:** the laws of physics prevent one body from occupying two locations simultaneously. This is not a cryptographic assumption. It is not a game-theoretic equilibrium. It is a property of matter.

No technology currently exists or is theoretically possible that allows a human body to be in two places at once. The security of this protocol is therefore not contingent on computational hardness, economic rationality, or honest majorities. It is contingent on physics.

5. The Social Output

5.1 Forced Connection

The protocol requires humans to be in physical proximity for one hour, four times per year. This is framed as a cost. It is the product.

Modern urban life is characterized by social isolation. In Australia, 1 in 4 adults report loneliness (Australian Institute of Health and Welfare, 2021). In the US, the Surgeon General declared loneliness an epidemic (Murthy, 2023). People live in apartments without knowing their neighbors' names. They order food without speaking to another human. They die without anyone noticing for days — which is precisely the problem the canary ripple system addresses (see (Applebee & Combe, 2026, "*Wanted Attention for Unwanted Results*")).

The co-presence protocol does not solve loneliness as a side effect. It makes loneliness structurally impossible. Four times a year, you must stand in a room with at least three other humans. You must stay for an hour. You will talk. You will learn names. You will, despite yourself, form connections.

5.2 Ritual

Every human society has synchronized collective rituals: religious services, harvest festivals, national holidays, sports events. These rituals serve no economic purpose. They exist because humans need to periodically affirm collective existence.

The verification window is a global ritual. 8 billion people, four times a year, stopping what they're doing to stand with their neighbors and say: *we are here.* The purpose is identity verification. The function is communion.

5.3 Precedent: Mandatory Voting

Australia has required citizens to vote since 1924 — 102 years of "show up and be counted" (Australian Electoral Commission). Turnout consistently exceeds 90%. The fine for not voting is $20. The cultural norm is near-universal compliance. Australians do not experience mandatory voting as oppression. They experience it as civic life.

The co-presence protocol asks less: no ballot, no political knowledge required. Just be there. Be counted. Confirm the count.

---

6. Implementation

6.1 BLE Continuous Presence

Each participant's device broadcasts a BLE beacon during the 60-minute window. Devices record all other beacons received, creating a presence log: "I saw device A, B, C continuously from T_0 to T_0+60min."

At window close, each device presents its presence log. All participants cross-sign the consolidated head count. The signed attestation is: "Devices A, B, C, D were continuously co-present from [UTC timestamp] to [UTC timestamp + 60 min]. Signed: A, B, C, D."

6.2 Anti-Relay

To prevent relay attacks (broadcasting someone's BLE beacon from a remote location), the protocol uses proximity-bound attestation:

- BLE signal strength (RSSI) must indicate 90% compliance with a $20 fine. This protocol's consequence is losing your identity token — access to voting, transactions, and the mesh network. The incentive is orders of magnitude stronger.

"This doesn't scale to 8 billion people."

It scales perfectly. Each group is 4+ people. 8 billion ÷ 4 = 2 billion groups, all operating simultaneously, requiring zero central coordination. The protocol is embarrassingly parallel.

"What about time zones?"

One UTC window. It's midnight in some places, noon in others. Australia already votes on a Saturday. This is one hour. Set an alarm.

---

8. Conclusion

The Sybil problem is not a computer science problem. It is a physics problem that computer science tried to solve with the wrong tools. One body, one location, one hour, four times per year. The protocol is simple enough to explain to a child, robust enough to resist any known attack, and produces — as its primary output, not its side effect — the forced human connection that modern society has engineered away.

Be in the same room at the same time. That's the whole paper.

Series Context

This paper is part of the OMXUS Research Series.

Direct dependencies:

- (Applebee & Combe, 2026, "*Wanted Attention for Unwanted Results*") (Community Emergency & Policing) — the BLE mesh and emergency response system that carries the co-presence attestation and handles "I can't make it" cases
- (Applebee & Combe, 2026, "*Swiss Direct Democracy*") (Swiss Direct Democracy) — 178 years of "show up and decide things together" as precedent
- (Applebee & Combe, 2026, "*Democratic Voting Mechanisms*") (Quadratic Voting) — what you vote on once your identity is verified

This paper proves:

- Conclusion 5 (Direct Democracy) — verified identity enables direct participation without representatives
- Conclusion 4 (Community Emergency Response) — the emergency mesh is the infrastructure for both safety and verification
- Conclusion 16 (Crime Not Inevitable) — a society where everyone knows their neighbors is a society with less crime

Convergence: If community response works ((Applebee & Combe, 2026, "*Wanted Attention for Unwanted Results*")), and direct democracy works ((Applebee & Combe, 2026, "*Swiss Direct Democracy*")), then the only missing piece is identity verification. This paper closes that gap without surveillance, without biometrics, and without any technology more complex than a Bluetooth radio and a clock.

See also: (Applebee & Combe, 2026, "*Trust-First Governance*") (Trust-First Governance), (Applebee & Combe, 2026, "*Two Monkey Theory*") (Two Monkey Theory)

References

Australian Electoral Commission. (2024). Compulsory voting. https://www.aec.gov.au/voting/compulsory_voting.htm

Australian Institute of Health and Welfare. (2021). Social isolation and loneliness. AIHW.

BrightID. (2020). BrightID: A decentralized proof of uniqueness. https://www.brightid.org

Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107, 1753–1820.

Czajka, A., & Bowyer, K. W. (2018). Presentation attack detection for iris recognition. Computer Vision and Image Understanding, 176–177, 1–13.

Douceur, J. R. (2002). The Sybil attack. In Peer-to-Peer Systems: First International Workshop (IPTPS 2002), pp. 251–260. Springer.

Murthy, V. H. (2023). Our epidemic of loneliness and isolation: The U.S. Surgeon General's advisory on the healing effects of social connection and community. U.S. Department of Health and Human Services.

Proof of Humanity. (2021). Proof of Humanity: A system combining webs of trust with reverse Turing tests. https://www.proofofhumanity.id

Worldcoin Foundation. (2023). Worldcoin whitepaper. https://whitepaper.worldcoin.org