

Proof-of-Human Systems and Conditional Participation: A Scripture-First Analysis of Biometric Governance in the Age of AI

Sixbert Sangwa^{1*}

¹Open Christian University, Sacramento, California, United States

*Corresponding Author: ssangwa@openchristian.education

Article Info

Article history:

Accepted: May 19, 2026

Published: May 20, 2026

Keywords: proof of human systems, World ID and biometric verification, mark of the beast technology, Christian analysis of digital identity, AI surveillance and human verification, Revelation 13 and digital governance, conditional access and human dignity.

Copyright: ©2026 by the author(s). This article is published under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0).

Abstract

The rapid spread of proof-of-human systems in 2026 marks a decisive shift in digital governance. What began as anti-bot verification is being recast as an infrastructural answer to AI-generated fraud, agentic commerce, synthetic identity, and distrust across social, commercial, and enterprise platforms. Recent developments are especially important: World announced a major World ID protocol upgrade on April 17, 2026, described proof of human as a foundational internet layer, expanded integrations with Tinder, and presented new partnerships around AI-agent delegation, enterprise authentication, and human-in-the-loop verification (TechCrunch, 2026; Tools for Humanity, 2026; World, 2026a, 2026b, 2026c). This manuscript argues that Christians should neither dismiss these developments as neutral convenience nor collapse them simplistically into a direct identification of the mark of the beast. Scripture teaches that human dignity is grounded in the image of God rather than in machine-legible credentials, warns that end-time power systems join deception, commerce, and coerced allegiance, and forbids surrendering moral discernment to pragmatic efficiency (Gen. 1:26-28; Dan. 7:23-25; Rev. 13:16-17). Theologically, proof-of-human systems reveal a deeper anthropological temptation: to redefine personhood operationally, so that public participation depends on passing institutional verification. Analytically, the strongest current evidence supports a sober middle position. Verified facts show expanding biometric and credential-based access systems. Plausible inference suggests these systems can become preparatory architecture for more comprehensive control. Unsupported speculation begins where evidence is replaced with prophetic overreach. The church therefore needs a Scripture-first framework of discernment, resistance, and truthful witness that rejects both technocratic naivete and sensationalist panic.

How to cite:

Sangwa S. (2026). From CAPTCHA to Conditional Humanity: A Scripture-First Critique of Proof-of-Human Infrastructure in the Age of AI. Open Journal of Business Theology, 6(2). <https://doi.org/10.65655/openchristianpress.121>

1. Introduction

The most timely development within the user's recurring field of concern is the accelerating normalization of proof-of-human infrastructure. In April 2026, World framed proof of human not as a niche anti-spam feature but as an emerging

trust layer for consumer platforms, enterprise systems, and AI-agent workflows. The company reported nearly 18 million verified humans across 160 countries, described the new World ID as "full-stack proof of human," and presented integrations spanning dating, gaming, event

ticketing, enterprise communication, document signing, and agentic web activity (World, 2026a, 2026b, 2026c). TechCrunch further reported that World's AgentKit is designed to let websites verify that a real human stands behind an AI agent's purchasing decisions (TechCrunch, 2026).

This shift matters because it moves public discourse beyond familiar arguments over passwords, CAPTCHAs, and two-factor authentication. The question is no longer merely whether a user controls an account. The emerging claim is that trustworthy digital participation may increasingly require proof that an authenticated, unique, and institutionally recognized human stands behind the action. Once that principle is normalized, the gate can widen from fraud prevention to access control, ranking, economic eligibility, and delegated machine agency. Theologically, this raises a decisive question: what happens when personhood in practice becomes conditional on verification rather than acknowledged as a God-given reality?

The thesis of this manuscript is that current proof-of-human systems should be understood as morally and prophetically significant preparatory architecture, but not yet equated outright with the mark of the beast. That distinction matters. To call every biometric or identity technology "the mark" is exegetically careless and strategically weak. Yet to call these systems harmless because they promise privacy, anti-bot utility, or user empowerment is equally careless. Scripture requires a more disciplined reading: one that distinguishes verified evidence from plausible trajectory, sees governance patterns before their final form, and keeps worship, conscience, and truthful witness at the center of prophetic discernment.

The April 2026 Proof-of-Human Turn

Several verified developments justify treating this subject as unusually timely. First, World's April 17, 2026 announcement presented the new World ID as a protocol designed for "human continuity," claiming that existing security systems can authenticate accounts and devices but not the continuing presence of the same real human across interactions (World, 2026a). Second, World's developer documentation now describes a layered credential model that includes proof of human, document-backed

credentials, and selfie-based checks, all intended to provide machine-readable trust signals without disclosing the underlying personal data to relying parties (World, 2026d). Third, World's consumer rollout tied proof of human directly to social participation by expanding its Tinder integration, where users can receive a verified human badge and platform benefits after Orb-based verification (World, 2026b).

Fourth, World's April 2026 partner announcements explicitly connected proof of human to enterprise trust and the agentic web. The company described integrations or planned integrations involving Zoom, Docusign, Okta, Vercel, Browserbase, and Exa, all framed around verifying human intent, securing delegated agent action, and preserving a "human in the loop" for consequential workflows (World, 2026c). Fifth, Tools for Humanity's March 25, 2026 white paper argued that proof of human is becoming critical infrastructure for democracy, speech, fraud prevention, and agent-mediated action in a world of advanced AI, while claiming that proper implementation can avoid surveillance and protect liberty (Tools for Humanity, 2026).

These claims must be reported carefully. The verified fact is that companies are actively building proof-of-human products, partnerships, and use cases at scale. The plausible inference is that anti-bot systems are becoming a broader identity-mediated governance layer. The unsupported leap would be to declare that each product announcement already fulfills Revelation 13 in its final form. Scripture-first analysis requires patience precisely where panic is easiest.

Scripture, Personhood, and the Temptation to Reclassify the Human

Biblically, the fundamental issue is not whether machines can tell humans from bots more accurately. The deeper issue is anthropological and theological. Scripture teaches that man and woman bear the image of God by divine act, not by institutional recognition (Gen. 1:26-28; Ps. 8:4-6; Jas. 3:9). Human dignity therefore precedes every registry, credential, wallet, or biometric workflow. When public systems begin to operationalize the human primarily as a verified signal within a technical stack, they do not erase the *imago Dei* ontologically, but they do train societies to behave as if practical personhood were mediated by infrastructure.

This creates a subtle but serious category mistake. A proof-of-human credential may verify that a system believes a unique human stands behind an action, but it cannot answer the moral questions that matter most. It cannot determine truth, righteousness, repentance, justice, or worship. It cannot tell whether the authenticated human is faithful or rebellious, oppressed or manipulative, truthful or deceptive. By itself, it cannot distinguish holiness from mere legibility. Scripture repeatedly warns against reducing moral discernment to appearances, centralized procedure, or humanly impressive systems (1 Sam. 16:7; Prov. 14:12; Isa. 44:9-20).

The current proof-of-human discourse also reveals an implicit technocratic anthropology. Its controlling fear is not merely fraud but indistinguishability: the anxiety that the digital public square will become unusable unless humanity is continuously reasserted through credentialed proof. That concern is not imaginary. Synthetic media, fraud, and scalable impersonation are real problems. Yet the proposed cure can smuggle in a distorted vision of order, one in which trusted participation increasingly depends on a fusion of biometrics, cryptography, mobile devices, platform policy, and commercial governance. This is not yet the abolition of humanity, but it is a powerful rehearsal in accepting machine-mediated legitimacy as a normal condition of social life.

The Moral Logic of Conditional Humanity

Scholarly literature helps clarify why this matters. Beduschi (2019) argued that digital identity platforms may support inclusion and rights only if they also mitigate discrimination, surveillance, and exclusion risks. The same article warned that biometric and blockchain-linked identity systems can create durable privacy harms and can exclude those whose credentials fail or whose bodily features are difficult to capture reliably. A related literature on proof of personhood similarly highlights tradeoffs between Sybil resistance, privacy, equality, and governance design rather than treating technical uniqueness as a self-validating good (Berman et al., 2020).

Recent scholarship sharpens the paradox further. Condrey (2026) notes that systems designed to prove human authorship or authenticity can

require highly intimate behavioral or biometric data, creating a privacy-attestation tension rather than eliminating it. Even where privacy-preserving cryptography is employed, the moral question does not disappear. It simply moves: who defines the threshold for trusted participation, who controls the acceptable proofs, who can revoke or condition access, and what social penalties fall on those who remain outside the system?

This is where the issue becomes more than a narrow privacy debate. Once human verification becomes a requirement for higher visibility, better access, transactional trust, or delegated machine action, participation is no longer merely open. It is stratified. The logic of “one human, one action” can easily migrate from spam prevention to ranked legitimacy, from consumer convenience to preferential access, and from fraud controls to cultural expectations that the unverifiable deserve reduced trust. Sangwa (2026) has already argued, in a broader digital identity context, that identity-mediated governance can shift social participation from recognition to conditional access. Proof-of-human systems intensify that concern because they present the condition not as civil paperwork but as a morally loaded verification of one’s very humanness.

Between Denial and Sensationalism: A Disciplined Eschatological Reading

Revelation 13 does not teach that every identification system is the mark of the beast. It teaches that a beastly order binds worship, allegiance, coercion, and commerce into one integrated regime, so that participation becomes materially costly for those who refuse false loyalty (Rev. 13:16-17; 14:9-12). The mark is therefore not reducible to a neutral identifier, nor is it exhausted by the technology that may later carry it. Its heart is covenantal betrayal expressed through obedient participation in a counterfeit order.

That exegetical point cuts two ways. On the one hand, it rebukes prophetic sensationalism. A Christian who simply equates an Orb scan, a digital wallet, or a dating-app badge with the final mark moves too quickly from resemblance to fulfillment. On the other hand, the same text rebukes technocratic innocence. Revelation does not present coercive commerce as arriving without preparatory structures. Beastly power

grows through admiration, normalization, fear, and dependence long before judgment falls in its climactic form. The church therefore errs when it waits for an explicitly blasphemous label before recognizing a formative pattern.

The most defensible eschatological conclusion is this: proof-of-human infrastructure is not sufficient evidence that the final mark has arrived, but it is strong evidence that societies are being habituated to accept identity-gated participation, machine-mediated legitimacy, and delegated action anchored to recognized human principals. That matters because Revelation 13 links commerce to worship, not because commerce is spiritually neutral, but because economic systems can become instruments of allegiance management. A population already trained to accept conditional participation on ostensibly practical grounds will be easier to discipline when moral and spiritual conditions are later attached.

This middle position is stronger than both extremes. It avoids the false precision of date-setting and gadget-based prophecy claims. It also avoids the opposite error of pretending that infrastructural conditioning is irrelevant unless the final prophetic label is already stamped onto it. Scripture commends watchfulness without frenzy, discernment without gullibility, and resistance before total consolidation rather than only after it (Matt. 24:4-13; 1 Thess. 5:1-6; 1 John 4:1).

Ecclesial and Public Implications

Several implications follow. First, Christians should reject the lie that machine-verifiable status is a trustworthy moral proxy. Churches must teach that truthfulness, repentance, justice, chastity, faithfulness, and courage are not produced by stronger authentication. A technically verified person can still be an idolater, oppressor, liar, or persecutor. Second, believers should scrutinize systems that convert optional verification into practical necessity for speech, livelihood, access, and social legitimacy. The issue is not whether every anti-bot measure is evil; it is whether a society is quietly accepting a future in which ordinary participation depends on passing institutionalized proofs of acceptable personhood.

Third, the church should avoid doctrinal sloppiness. It is a mistake to declare a final prophetic fulfillment without adequate textual and factual grounding. That approach discredits true warning. Yet it is equally mistaken to silence concern by invoking privacy claims, decentralized architecture, or anti-fraud rhetoric as if these settled the matter. Tools for Humanity (2026) explicitly argues that proof of human should become foundational digital infrastructure. That claim alone warrants serious theological attention, because infrastructures shape moral habits long before they reveal their full political use.

Fourth, public ethics should insist on viable alternatives, narrow purpose limitation, refusal of coercive bundling, and protection for those excluded by design, conscience, disability, poverty, or non-participation. Even where states or companies claim to preserve privacy, Scripture requires defense of the weak and suspicion toward concentrated power that can decide who is seen, heard, trusted, or transactable (Exod. 23:6; Prov. 31:8-9; Mic. 6:8).

Finally, the church must cultivate practical noncompliance with deception at the level of formation. Christians who have already surrendered discernment to convenience, outsourced judgment to platform trust scores, and accepted credentialed access as morally normal will be poorly prepared for sharper tests. By contrast, believers who are trained to value truth over frictionless access, conscience over incentives, and fidelity over social rewards will be better positioned to recognize and resist more explicit systems of coercion when they arrive.

Conclusion

The present proof-of-human wave is one of the clearest timely signs within today's convergence of AI, surveillance, and digital governance. The relevant verified facts are plain: biometric-backed human verification is expanding from anti-bot defense into dating platforms, enterprise workflows, agent delegation, and broader trust infrastructure. Theologically, these developments matter because they press societies toward an operational reclassification of the human: not who man is before God, but who counts in practice before systems.

A Scripture-first reading does not require sensationalism to see the danger. Revelation 13 warns that beastly power fuses deception, coercion, and commerce around allegiance. Current proof-of-human systems do not yet justify an exact one-to-one identification with the final mark. They do, however, disclose preparatory logic: the normalization of conditional participation, recognized human principals, and infrastructure-mediated trust. Christians should therefore answer neither with naive adoption nor with careless prophecy, but with sober resistance, clear categories, and unwavering insistence that human dignity, moral legitimacy, and faithful witness cannot be delegated to machines or conferred by platforms.

References

- Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society*, 6(2). <https://doi.org/10.1177/2053951719855091>
- Berman, P., Fialho, F., & Howard, D. (2020). Who watches the watchmen? A review of subjective approaches for sybil-resistance in proof of personhood protocols. *Frontiers in Blockchain*, 3, Article 590171. <https://doi.org/10.3389/fbloc.2020.590171>
- Condrey, D. L. (2026). Privacy-preserving proof of human authorship via zero-knowledge process attestation. arXiv. <https://arxiv.org/abs/2603.00179>
- Sangwa, S. (2026). Digital identity, conditional access, and human dignity: A Christian policy analysis of biometric governance, surveillance infrastructure, and data justice. *Open Journal of Stigmatized Knowledge & Suppressed Discourses*, 2(2). <https://doi.org/10.65655/OpenChristianPress.2026.111>
- TechCrunch. (2026, March 17). World launches tool to verify humans behind AI shopping agents. <https://techcrunch.com/2026/03/17/world-launches-tool-to-verify-humans-behind-ai-shopping-agents/>
- Tools for Humanity. (2026, March 25). Private proof of human: Critical infrastructure for humanity in a world with advanced AI. <https://world.org/api/download?uid=private-proof-of-human>
- World. (2026a, April 17). Introducing the new World ID: Full-stack proof of human. <https://world.org/blog/announcements/world-id-full-stack-proof-of-human>
- World. (2026b, April 17). World ID: Increasing trust for online dating, gaming and event ticketing. <https://world.org/blog/announcements/online-dating-gaming-event-tickets-proof-of-human-everyday-life>
- World. (2026c, April 17). World ID for agents: Browserbase, Exa, Okta, and Vercel. <https://world.org/blog/announcements/browserbase-exa-okta-world-id-for-agents-web>
- World. (2026d). World ID overview. <https://docs.world.org/world-id/overview>