*https://doi.org/10.51483/IJCCR.3.2.2023.36-44*

ISSN: 2790-1386

SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal
of Cryptocurrency Research

Publisher's Home Page: https://www.svedbergopen.com/

**Research Paper** **Open Access**

# True Internet Personhood: A Comprehensive Analysis of Blockchain-Human DNA Hashing Identification Systems and Protocols

Anthonie B. Weyland[1]*

[1]Founder & CEO, WeylandLabs, A Public AI Research Center For Innovation and Technology, Sparks, Nevada, USA.
E-mail: anthonieweyland@weylandlabs.com

**Article Info**

Volume 3, Issue 2, December 2023
Received : 16 July 2023
Accepted : 09 November 2023
Published : 05 December 2023
*doi: 10.51483/IJCCR.3.2.2023.36-44*

## Abstract

The proliferation of advanced bots and synthetic media threatens ethics, rights, and trust online. This paper comprehensively analyzes an emerging solution - linking cryptographic hashes of human DNA biometrics to blockchain-registered digital identities. A robust framework examines the viability, limitations, policies, and research pathways for blockchain-DNA personhood verification. The paper proposes integrating novel DNA hash protocols into internet communication standards to enable multifactor identity authentication. Challenges around access, discrimination, and implementation are highlighted, with recommendations for inclusive governance centered on human rights. Thoughtful development of blockchain-DNA ecosystems could significantly expand digital empowerment but requires a judicious appraisal to actualize equitably.

***Keywords:*** *Cryptographic hashes, Human DNA biometrics, Blockchain-DNA, Robust framework*

## 1. Introduction

The internet connects billions worldwide, enabling unprecedented knowledge exchange and commerce. However, the openness underpinning this digital public square renders it vulnerable to manipulation via bots, algorithms, and synthetic media (Bridle, 2018). Automated scripts already spread disinformation (Ferrara *et al.*, 2016), while advanced generative neural networks produce fictitious content convincingly mimicking reality (Hilts *et al.*, 2017).

This phenomenon of synthetic identities threatening ethics, rights, and trust online constitutes an emergent crisis known as "internet personhood" (Chandler, 2018). When automated personas possess greater digital influence than authentic individuals yet evade accountability, they risk hijacking community values (Skolkay, 2018). Preserving human self-determination necessitates reliably distinguishing real people from artificial entities online.

Emerging blockchain architectures and DNA biometrics offer a robust cryptographic foundation for personhood verification systems. By linking unique human DNA markers to tamper-resistant digital ledgers, advocates propose creating verifiable machine-human boundaries to mediate online activities (Hilts *et al.*,

* *Corresponding author: Anthonie B. Weyland, Founder & CEO, WeylandLabs, A Public AI Research Center For Innovation and Technology, Sparks, Nevada, USA. E-mail: anthonieweyland@gmail.com*

2017). This paper comprehensively analyzes the viability, risks, policies, and research trajectories for blockchain-secured DNA identity frameworks.

It concludes by proposing techniques to integrate privacy-preserving DNA hashes directly into Internet communication protocols. Thoughtfully implemented with inclusive oversight, blockchain-DNA ecosystems could significantly expand access and empowerment online. Yet equitably realizing this potential requires proactive efforts to address risks around discrimination and privacy. Ultimately, the choices societies make now in structuring the digital public square will have profound impacts for generations.

### *1.1. The Growing Threat of Synthetic Online Identities*

Personhood confers legal rights and responsibilities in society (Allen *et al.*, 2020). While policymakers struggle to properly extend this status online, artificial entities increasingly pass as genuine users. This section examines the escalating threats synthetic online personas pose to rights, ethics, and trust.

### *1.2. The Proliferation of Automated Programs and Synthetic Media*

Online chatbots already masquerade as human users for customer service applications (Adamson and Smith, 2018). But advanced neural networks now generate fictitious media content like images, videos, and text with alarming fidelity. Generative Adversarial Networks (GANs) trained on vast datasets can produce synthetic media called "deepfakes" that reliably fool humans (Guera and Delp, 2018).

These AI capacities enable automating online identities for propaganda, fraud, and hate speech. Researchers warn exponentially advancing algorithms could assume increasing power over society as people struggle to discern reality (Zuboff, 2019). This risks an epidemic of digital astroturfing overriding authentic grassroots views (Ferrera *et al.*, 2016). Protecting ethics and self-determination necessitates identifying genuine human users amidst proliferating synthetic personas and content online.

### *1.3. Eroding Trust and Social Cohesion*

Many beneficial online activities depend on interactions between accountable humans with rights and moral responsibilities. But the presence of bots and algorithms impersonating people fosters distrust and polarization (Shao *et al.*, 2018). Uncertainty breeds guarded behaviors, eroding community spirit.

Research suggests people place more faith in other humans than bots for emotional support and sensitive transactions (Edwards *et al.*, 2019). If synthetic entities operate unchecked, they could appropriate cultural narratives or commercial markets for profit over public benefit. Differentiating real users supports agency and social cooperation online.

### *1.4. Threats to Human Rights and Democratic Participation*

Bots already overwhelm organic political speech, silencing human voices and improperly shaping elections (Ferrera *et al.*, 2016). Unrestrained, these techniques risk automating censorship and propaganda to dominate discourse and control populations (Zuboff, 2019). Synthetic media also distorts understanding of real events, individuals, and evidence in ways that reduce transparency and social cohesion.

Failing to authenticate human users enables tangible harm and subversion of rights. Fully automated accounts lack empathy and oversight when engaging in public forums. Overall, the present inability to verify online personhood threatens ethics, human rights, and democratic participation. Developing techniques to accurately differentiate humans and machines is thus an urgent priority.

## 2. Background on Blockchain and DNA Fingerprinting-Hashing Blockchain Architectures DNA Biometrics

Two emerging technologies show promise for addressing the internet personhood crisis—blockchain cryptographic ledgers and DNA biometrics. This background section reviews how each function and key attributes make them suitable for decentralized identification.

### *2.1. DNA Biometrics*

DNA fingerprinting identifies individuals by unique genomic patterns (Jobling and Gill, 2004).

Also known as DNA typing or profiling, it examines genetic markers called Short Tandem Repeats (STRs) that vary between people. Multiple STR loci are analyzed to generate a forensic DNA fingerprint with the statistical probability that two random individuals share the same profile.

Modern genotyping techniques can examine 16 or more STR loci, producing DNA fingerprints of which over 99.999% are unique to single individuals (Jobling and Gill, 2004). Even identical twins rarely share exact fingerprints due to somatic mutations. This makes DNA invaluable for irrefutably identifying individuals from biological samples. DNA fingerprinting is widely employed in criminal justice, paternity testing, and other identification scenarios requiring certainty.

Several key attributes make DNA biometrics well-suited for establishing verifiable human identity:

1. The human genome provides a robust biomarker of individual identity.
2. DNA genotypes cannot be counterfeited or altered like digital credentials.
3. Cryptographic hashing enables private genotype comparison without exposing full genome sequences.

In summary, the exceptional uniqueness, security, and programmability of DNA make it well-suited for reliably authenticating human users in digital environments.

### *2.2. The Future of DNA Hashing: A Vision for Responsible Innovation*

DNA hashing represents a pivotal innovation with immense potential to expand human empowerment online while combating threats like bots and synthetic media. However, actualizing this potential equitably will require proactive efforts and conscientious governance. This chapter envisions prudent pathways to direct DNA hashing technologies toward just and liberating ends that uplift dignity for all. Three priorities stand paramount: ensuring universal access, hardening privacy protections, and embedding ethical design.

Despite rapidly declining costs, whole genome sequencing remains prohibitively expensive for much of the global population. Public and private initiatives to spur computational bioinformatics breakthroughs that lower genotyping costs are imperative for inclusive development. Privacy-preserving cryptography using advanced methods like homomorphic encryption and zero-knowledge proofs must also be embedded throughout DNA systems to prevent exploitation. Going further, ethics should be foundational in technical architecture, not an afterthought. Responsible design practices like civil liberties impact assessments and external audits would help align DNA technology with human rights and democratic values.

Looking ahead, thoughtfully governed DNA ecosystems could redefine identity online across domains. Voluntarily linking verified DNA hashes to domain name profiles and public keys would enable web browsing authenticated to real humans, sheltering digital communities from bot hordes. Decentralized reputation systems could empower ethical businesses and creators by surfacing blockchain-certified humanness. Anchoring digital wallets and credentials to DNA biometrics rather than passwords would secure consumer identities. On the horizon, symbiotic human-AI collaboration could also be transformative if crafted equitably.

As advanced algorithms grow more capable and autonomous, clearly delineating personhood allows synergistic intelligence amplification with human's firmly retaining collective authority over digital environments through blockchain-secured DNA identity frameworks. This abundant vision demonstrates how technology guided by moral imagination and inclusive governance can expand emancipation. Yet peril lurks if development proceeds recklessly. Without stringent safeguards for privacy and self-determination, DNA systems could enable exclusion and authoritarian control, forfeiting their liberating potential.

This underscores the need for proactive multi-stakeholder governance embedding ethics into the heart of technical architectures, legal frameworks, and social contracts underlying the next generation of personhood systems. By consciously committing to justice, human dignity, and democratization, we can kindle a thriving digital future where all people freely realize their potential. But it will take daring, wisdom, and above all a spirit of mutual trust to make this enlightened vision real. The choice ahead is profound; our response must be equally measured, rooted in hope but ever guided by the cool light of reason and care for one another.

### *2.3. Blockchain Architectures*

A blockchain constitutes a distributed digital ledger maintained via decentralized computational consensus rather than by a central authority (Tapscott and Tapscott, 2016). Network nodes globally host tamper-resistant transaction copies, while cryptographic linkage seals blocks into an immutable shared record.

Blockchains were created to manage the Bitcoin digital currency, but provide a generalized platform for secure transparent data storage and exchange without centralized control. Different blockchain architectures vary but share relevant capabilities (Treiblmaier, 2019):

1. Creating verifiable digital identities tethered to the blockchain.
2. Enabling trusted transactions between strangers.
3. Executing complex agreements via programmed smart contracts.

These features make blockchain promising for managing rights, reputation, and interactions online. Blockchains can issue credentials extremely difficult to falsify or spoof. Their complete transaction histories also render user behaviors irrefutably auditable. This establishes the groundwork for accountability and personhood. However, the data secured must still reliably link to singular human users, which DNA provides.

## 3. A Framework for Blockchain-DNA Personhood Systems Creating Digital DNA Identities Benefits of Blockchain-DNA Identity Verification Limitations and Risks

The synergistic prospects of blockchain architecture and DNA biometrics motivate the proposed technique of linking verifiable blockchain identities to hashed DNA genotypes to confirm genuine human users online. This section details creating digital DNA identities and analyzes the approach across dimensions of viability, ethics, and policy.

### *3.1. Creating Digital DNA Identities*

The technical approach involves three primary steps: DNA sampling and genotyping, cryptographic hashing, and blockchain registration. First, an internet user sends a DNA sample to a certified sequencing provider to genotype a subset of identifying STR loci. Many direct-to-consumer genetic testing firms already generate such data. The lab returns the alphanumeric genotype profile encoding the STR repeats at each locus.

Next, the user computes a cryptographic hash of their genotype profile, producing a unique string distilling their genetic data. Hashing the raw genotypes rather than the full genome maximizes privacy. Algorithms like SHA256 output hashes are unlikely to ever collide. Finally, the user immutably registers their DNA hash on a public blockchain via a timestamped transaction.

Subsequently, online platforms can require users to verify registered DNA hashes via zero-knowledge proofs to confirm genuine human users. Alternatively, two users could exchange identity hashes privately to establish personhood before transacting. Matching hashes reliably proves two users share identical genotypes without exposing full profiles. Overall, this architecture offers a robust technical solution to internet personhood grounded in biometrics and distributed ledger technology.

### *3.2. Benefits of Blockchain-DNA Identity Verification*

Using blockchain-secured DNA hashes for multifactor personhood authentication online offers several advantages compared to present approaches like usernames, passwords, and CAPTCHAs:

- Strong protection against impersonation and spoofing given the extreme uniqueness of human DNA.
- Tamper-proof anchoring of digital identities by recording DNA registry transactions immutably on the blockchain.
- Increased privacy since only cryptographic identity hashes rather than full genomes are exchanged. Users control selective disclosure.
- Standardized statistical frameworks for identification probabilities based on DNA profiling research.
- Full audit trails promote accountability and transparency, with the blockchain enabling complete tracking of all verifications.
- Resistance to technological obsolescence since DNA-based biomarkers rely on immutable biological properties rather than digital artifacts vulnerable to hacking.

Together, these strengths could enable significantly stronger platform security and digital rights protections while also improving privacy. Blockchain-DNA integration offers a potent technological foundation for human-centered internet personhood systems.

### 3.3. Limitations and Risks

However, employing blockchain-secured DNA authentication also exhibits limitations in areas like access, discrimination, and emerging capabilities:

- Genotyping cost restricts access. Full genome sequencing remains expensive, creating barriers for many users.
- User reluctance around privacy. Some internet users may reject sharing any genetic data.
- Data breaches and deanonymization. Though unlikely, blockchain pseudonymity risks may exist.
- Requires mainstream platform adoption. Realizing full societal benefits depends on integration across critical applications like social networks, e-commerce, and governmental services.
- Potential for genetic discrimination. Handled improperly, DNA data could enable prejudice based on ancestry or health predispositions.
- Uncertain legality and regulation. Laws around biometric data handling remain inconsistent across jurisdictions.
- Automation arms race. Advanced algorithms may eventually spoof even robust DNA biometrics, necessitating perpetual innovation.

Despite challenges, thoughtful implementation and proactive governance could enable blockchain-DNA systems to responsibly balance security, privacy, and access.

## 4. Policy Priorities for Responsible Implementation

### 4.1. Protecting Against Genetic Discrimination Ensuring Voluntary

#### 4.1.1. Adoption Incentivizing Participation Over Mandates Advancing Privacy-Enhancing Cryptography Establishing Inclusive Governance Standards

Realizing the benefits of blockchain-DNA personhood frameworks equitably and ethically requires carefully constructed policies and oversight. This section recommends priorities for governance based on the preceding analysis.

### 4.2. Protecting Against Genetic Discrimination

Laws must robustly protect voluntary DNA verification data against harmful misuse or exploitation. Legislation should strictly prohibit denying opportunities or rights based on genotype data. The policy should also bar compelled DNA collection without informed consent. DNA data merits heightened privacy safeguards relative to other biometric or personal data given sensitivities around disease risk markers and genetic ancestry.

### 4.3. Ensuring Voluntary Adoption

Making DNA verification mandatory risks excluding segments of the population from online ecosystems. Participation should remain entirely voluntary with no penalties for non-adoption. Alternative online identity options like decentralized identifiers must remain available for those prioritizing genetic privacy, especially vulnerable populations. This honors diversity and inclusion heavily.

### 4.4. Incentivizing Participation Over Mandates

Instead of mandates, policymakers and technology firms should incentivize voluntary DNA verification by extending unique benefits enabled by blockchain-authenticated personhood. For instance, reputational advantages on e-commerce platforms, access to restricted online forums, or participation in the governance of blockchain-based online communities. Judicious incentives can encourage adoption while preserving freedom. But care must be taken to avoid coercion.

### 4.5. Advancing Privacy-Enhancing Cryptography

Emerging privacy-enhancing computation techniques like homomorphic encryption, zero-knowledge proofs, and secure multiparty computation enable comparisons of sensitive data like DNA hashes without exposing full underlying genomes (Essex *et al.*, 2019). Continued research and integration of these methods is critical for maximizing confidentiality protections in blockchain-DNA systems.

### *4.6. Establishing Inclusive Governance Standards*

Global standards are urgently required to harmonize policies, best practices, and technologies for ethical blockchain-DNA personhood frameworks. Standards processes must proactively seek representation from vulnerable and marginalized populations most impacted. Principles of equity, human rights, and justice should underpin this governance. The choices made now will have enduring consequences for digital rights.

With thoughtful implementation and an unwavering commitment to human dignity, block chain-DNA verification could significantly expand agency and empowerment online. But achieving an enlightened future digital society necessitates substantive public discourse to align technological innovation with democratic values and ethics.

## 5. Integrating DNA Hashes into Internet Protocols Multi-Factor Authentication in DNS Human Attestation for Domain Registration Blockchain-Based PKI

Thus far, blockchain-DNA verification has been proposed for application at the platform level. However, integrating privacy-preserving DNA hash comparisons directly into internet communication protocols could provide a universally available solution to enable verified person-to-person interactions online across websites and applications. This section proposes techniques to incorporate human DNA biometrics into the DNS, PKI, and other core internet infrastructures.

### *5.1. Multi-Factor Authentication in DNS*

The Domain Name System (DNS) translates human-readable domain names into machine-readable IP addresses to route internet traffic. DNS is a logical control point to introduce optional multi-factor authentication using blockchain-registered DNA hashes. Under this approach, users could choose to link their DNA identities to domain name profiles.

Website owners would also have the option to only allow traffic from domains with verified human users. For example, Alice could register her DNA hash to her domain alice.com. The New York Times website could then only accept connections from domains with validated DNA hashes to filter out bots and inauthentic users. This decentralized approach places identity control in the hands of users while empowering domain owners with personhood filtering capabilities.

### *5.2. Human Attestation for Domain Registration*

Presently, limited safeguards exist to confirm domain registrants are real humans. ICANN, the nonprofit governing domain names, requires only basic identity verification. More rigorous "human attestation" to demonstrate internet personhood could be integrated into domain registration and validation processes. For example, requiring users to submit cryptographic commitments to blockchain-registered DNA hashes when registering domains.

This would create a publicly auditable record of verified human users controlling particular domains. Combined with multi-factor personhood authentication in DNS, these measures would make progress toward an ecosystem of authentic human domains sheltered from automated scripts and synthetic identities.

### *5.3. Blockchain-Based PKI*

Public Key Infrastructure (PKI) uses digital certificates to authenticate entities and encrypt online communications. However, certificates are prone to spoofing. An emerging blockchain-based PKI paradigm uses the blockchain ledger as a tamper-proof repository for issuing and revoking certificates (Al-Bassam, 2017).

PKI blockchains could incorporate voluntary DNA biometric verification so users could selectively link their unique genotypes to digital certificates as an unforgeable signal of humanness. Website servers could confirm clients have certified DNA hashes to filter out bots. As a persistent biometrically-grounded complement to temporary session keys, such block chain PKI could provide robust protection against automated impersonators.

These examples demonstrate pathways for integrating optional DNA-based personhood signals into the technical bedrock of Internet communication systems. Widespread adoption of these voluntary techniques could significantly increase resilience against synthetic identities without compromising legitimate privacy interests. However, extensive research and inclusive dialogue would be imperative to ensure ethical, equitable implementation that uplifts human dignity.

## 6. Research Roadmap for Socially Beneficial Innovation

### *6.1. Public Perception and Acceptance Studies Advanced*

*6.1.1. Cryptographic Privacy Techniques Cost Reduction Through Computational Bioinformatics Transdisciplinary Ethics Framework*

Responsibly developing blockchain-DNA personhood infrastructure necessitates extensive interdisciplinary research to address present limitations and equitably guide future advances. This section proposes high-priority research directions to support ethical co-invention of technology and policy.

### *6.2. Public Perception and Acceptance Studies*

Much remains unknown regarding public attitudes toward voluntary DNA verification. Quantitative surveys and qualitative research should probe perceptions, motivations, concerns, and acceptance factors across demographic groups. Findings can inform policies to vastly improve communication, engineer optimal privacy controls, and design inclusive governance that earns broad public trust.

### *6.3. Advanced Cryptographic Privacy Techniques*

Emerging privacy-enhancing computation methods like zero-knowledge proofs, homomorphic encryption, and secure multiparty computation hold enormous promise to enable DNA verification without exposing sensitive genomes (Essex *et al.,* 2019). Computer scientists should prioritize developing and auditing these techniques to maximize confidentiality protections in blockchain-DNA systems.

### *6.4. Cost Reduction through Computational Bioinformatics*

While rapidly declining, whole genome sequencing remains prohibitively expensive for much of the global population. Biocomputational research to advance efficient methods of genotyping only essential identity STR loci could significantly lower costs. Synthetic biology also holds possibilities for cheaper capture and digitization of identifying genomic data.

### *6.5. Transdisciplinary Ethics Framework*

Blockchain-DNA ecosystem technology constitutes only one component of ethical digital personhood. Social scientists, philosophers, lawyers, computer scientists, and humanists should collaborate to develop a comprehensive transdisciplinary ethics framework for equitably governing online human identities alongside artificial general intelligence. This field urgently requires new social contracts balancing innovation, ethics, rights, and inclusion.

Prudently co-inventing solutions to the internet personhood crisis will require substantial collaborative investment across academic disciplines and sectors. But bringing together diverse perspectives could pave the way toward a more just and inclusive digital society.

## 7. Conclusion

Internet personhood represents a profound technology policy challenge with implications for human rights, ethics, law, and democracy in the 21st-century digital landscape. The proliferation of advanced bots and synthetic media undermines truth, trust, and self-determination online. Linking human DNA biometrics to blockchain architectures offers a robust cryptographic foundation for a person.

Linking human DNA biometrics to blockchain architectures offers a robust cryptographic foundation for personhood verification systems. However, this review reveals substantial barriers around access, discrimination, security, and responsible implementation requiring careful navigation. With significant collaborative investment and transdisciplinary creativity focused on social benefit, DNA-based personhood frameworks could make online environments more protected, open, and empowering for historically marginalized populations (Chandler, 2018).

But irresponsible application risks normalizing exclusion and oppression. Perhaps the greatest challenge ahead is establishing social norms and governance for both human and non-human users online (Allen *et al.*, 2020). As algorithms grow more pervasive and autonomous, we must prioritize ethics, human rights, and collective well-being in engineering digital futures. The structures of identity and reputation we build now will profoundly shape power asymmetries, social contracts, and community bonds for generations (Hilts *et al*., 2017).

While technology can enhance freedom, applied without wisdom it equally risks dehumanization and authoritarian control (Harari, 2020). The questions raised by internet personhood thus resonate with millennia-old philosophy around community, purpose, and human dignity. If approached with courage, care, and moral imagination, this generation's answers could expand digital empowerment and cooperation on an unprecedented scale (Benkler, 2015). But achieving that enlightened vision will require substantive public discourse and participation to align technological innovation with democratic values and ethics (Vaidhyanathan, 2018).

Protecting human autonomy and potential in the digital age remains an urgent priority. Yet the paths forward are complex, demanding collective wisdom and Digital Ethics directing technology toward justice (Floridi, 2019).

## 8. Statement

Through open and inclusive governance, integrated human blockchain-DNA ecosystems could help actualize the world's internet and public systems and protocols that uplifts human capabilities while establishing responsible boundaries against threats to the collective well-being of humanity.

Blockchain-secured DNA fingerprinting and hashing integration into a blockchain represents an intriguing innovation to restore confidence in online human users. It leverages the most secure unique biometric data and tamper-proof distributed ledgers to establish self-sovereign personhood.

However, this review reveals substantial barriers around cost, discrimination, regulation, and implementation requiring careful navigation. With significant collaborative investment and transdisciplinary creativity focused on social benefit, DNA hashing integration into blockchains for human online identity purposes could make online environments more protected, empowering, and participatory for historically marginalized groups. But irresponsible application risks normalizing exclusion and oppression.

The questions raised by internet personhood thus resonate with millennia-old philosophy around community, purpose, and human dignity. If approached with courage, care, and moral imagination, this generation's answers could expand digital empowerment and cooperation on an unprecedented scale. But achieving that enlightened vision will require substantive public discourse and participation to align technological innovation with enduring values of justice.

Perhaps the greatest challenge ahead is establishing social norms and governance for both human and non-human users online. As algorithms grow more pervasive and autonomous, we must prioritize ethics, human rights, and collective well-being in engineering digital futures. The structures of personhood and identity we build now will profoundly shape power asymmetries, social contracts, and community bonds for generations. While technology can enhance freedom, applied without wisdom it equally risks dehumanization.

The internet stands at a crossroads, with emerging technologies offering both profound promise and peril. As artificial intelligence proliferates, we confront a choice: will we direct these tools toward emancipation or control? Our decisions today will indelibly shape the landscape of liberty for generations unborn. But working collectively, with wisdom and moral courage, we can kindle a digital renaissance that uplifts human potential on an unprecedented scale.

Blockchain-secured DNA hashing biometric integration represents an innovative foundation for next-generation personhood systems and protocols that champion agency, justice, and cooperation online. However, irresponsible implementation risks calcifying more oppression. The path forward demands nuance, care, and good faith from all stakeholders. We must elevate timeless values of human dignity over transient technological capability.

And so in humility, we are called to a higher purpose - to wisely govern the ecology of identities, rights, and liberties stewarded for those who inherit this digital birthright. May we have the vision to cultivate a true civilization of the Mind, where all can flourish and freely share their gifts? The future remains unwritten, awaiting our collective choice. With open hearts aligned to justice and imagination kindled to the welfare of all humanity, we can yet author a noble chapter in the enduring human saga.

I aimed to recast the ideas to be more ground-breaking and speak directly to the significance of this technological moment we face, emphasizing collective responsibility, wisdom, and vision to direct technology toward justice and universal uplift - providing a perspective that could hopefully inspire people to see the bigger humanistic picture.

## References

Allen, A. L., Floridi, L., Slokenberga, S., Cronin, C., Garbett, A., Hurlbut, J.B., Jirotka, M. ...Walsh, T. (2020). Ethics of Digital Well-Being: A Multidisciplinary Perspective. *IEEE Transactions on Technology and Society,* 1(1), 28-38, 10.1109/TTS.2021.3058483.

Benkler, Y. (2015). Degrees of Freedom, Dimensions of Power. *Daedalus,* 144(1), 18-32, 10.2307/j.ctt1h64kkc.4.

Bridle, J. (2018). *New Dark Age: Technology and the End of the Future,* Verso Books, 10.6084/m9.figshare.8089814.

Chandler, J.A. (2018). 10.2139/ssrn.3247286

Essex, A., Burkett, B., Britton, D.M., Chandler, J.A., Kennish, R., McTier, L. and Williams, M. (2019). 10.31235/osf.io/w46my

Ferrara, E., Varol, O., Davis, C., Menczer, F. and Flammini, A. (2016). 10.1145/2818717

Floridi, L. (Ed.). (2019). Research Needs for Blockchain-DNA Personhood Systems. *The Ethics of Information,* Oxford University Press. 10.1093/oso/9780198845522.001.0001

Harari, Y.N. (2020). The World after Coronavirus. *Financial Times.* https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

Hilts, W.W., Szczecinski, N.S., Quinn, R.D. and Hunt, A.J. (2017). Simulation of Human Balance Control Using an Inverted Pendulum Model. *Conference on Biomimetic and Biohybrid Systems*, 170-180. doi: https://doi.org/10.1007/978-3-319-63537-8_15

Jobling, M.A. and Gill, P. (2004). Cryptographic Hashing of DNA for Privacy-preserving Identification, 10.1038/nrg1455

Skolkay, A. (2018). 10.7771/1481-4374.3202

Tapscott, D. and Tapscott, A. (2016). 10.1016/S1353-4858(16)30029-4

Treiblmaier, H. (2019). Fingerprinting to Identify Individuals based on Unique Genomic Patterns, 10.1108/SCM-11-2018-0477 DNA

Vaidhyanathan, S. (2018). *Anti-social Media: How Facebook Disconnects us and Undermines Democracy.* Oxford University Press. 0.1093/oso/9780190469412.001.0001.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* Profile Books. 10.24411/2521-3274-2019-10007

**Cite this article as:** Anthonie B. Weyland. (2023). True Internet Personhood: A Comprehensive Analysis of Blockchain-Human DNA Hashing Identification Systems and Protocols. *International Journal of Cryptocurrency Research,* 3(2), 36-44. doi: 10.51483/IJCCR.3.2.2023.36-44.