ByHuman:
Verifying Human Creativity in a Decentralized World

Abstract

With the increasing ability of artificial intelligence (AI) to create complex digital content, it is becoming increasingly difficult to distinguish between human and machine works. ByHuman provides a decentralized solution for verifying human authorship based on blockchain technology - specifically Ethereum and the Ethereum Name Service (ENS) while protecting user privacy. Through self-sovereign ENS domains and a community-driven verification process, creators can establish their unique, human-verified identity. Cryptographic signatures and smart contracts ensure that digital works are tamper-proof and verifiably linked to their human creators. Compared to biometric or centralized approaches, ByHuman offers a privacy-friendly and ethically sound alternative. This solution promotes transparency, gives individuals control over their data and emphasizes the value of human creativity in an AI-driven world.

Introduction

Today, artificial intelligence can generate deceptively real-sounding text, music and images. It is becoming increasingly difficult for readers, listeners or clients to trace the origin of digital content is a work actually created by a human or by an AI? Interest groups are already warning that the authenticity of creative works must be ensured in markets flooded with AI. Interest groups are already looking for ways to certify human works.

Proof-of-By-Human is a concept that aims to clearly verify that a human being is behind a digital action or content. However, previous approaches for such proof of identity have significant weaknesses. Biometric approaches, for example, attempt to assign each person a unique digital ID using biometric iris scans. However, this approach may lead to data protection concerns and official intervention - supervisory authorities in Europe could force such organizations to delete

the collected biometric data due to GDPR violations. Unethical side effects may also occur: In countries of the global South, people could be financially lured into giving away their iris scans, for example, and a black market could even emerge where verified IDs are traded for a few dollars. Such problems undermine the trustworthiness of these solutions. Other projects such as rely on manual verification (video uploads and two-way vouching) or social graphs to identify unique individuals. Although such alternatives bypass mass biometric data collection, they often require the disclosure of personal information (photo/video) and are so far only widespread in niche markets.

ByHuman takes a new approach to bridge the gap between trust and privacy. The concept makes it possible to prove human authorship of AI-generated content. ByHuman relies on realizable token interactions in the Ethereum ecosystem instead of centralized registries or biometric scanners. At its core, ENS (Ethereum Name Service) domains will serve as identity anchors, combined with cryptographic signatures and smart contracts to provide tamper-proof, privacy-friendly proof of human identity. This white paper explains the technical, social and ethical foundations of ByHuman, describes how it works using concrete application examples and compares the model with existing solutions.

Verification of human identity on the web3

The challenge of distinguishing genuine human identities from bots or multiple accounts (Sybil attacks) online is nothing new. In the Web3 context - i.e. blockchain and decentralized platforms- various proof-of-personhood methods have been tested:

- Biometric methods: Biometric approaches such as iris scans are centralized, violate privacy and are vulnerable to regulation.

- Social and community-driven methods: Community-based methods are more privacy-friendly, but are often costly and difficult to scale.

- Hybrid approaches and experimental solutions: Some newer approaches attempt to use zero-knowledge proofs to confirm a unique person based on government IDs or cell phone contracts, for example, without disclosing the details. Others are discussing Turing tests for users (CAPTCHAs or similar) - but this remains a cat-and-mouse game with

increasingly powerful AIs. Established Web2 platforms also recognize the problem: Twitter (now X) introduced paid verifications to keep bots out, and forums are discussing the labeling of AI-free content. However, these isolated solutions are proprietary or centralized and not interoperable.

To summarize, an ideal proof-of-human mechanism should have the following characteristics:

- Decentralized: no dependence on a single company or device; the system should be built on open protocols (e.g. Ethereum) and operated collaboratively.

- Privacy: No biometric mass data collection and no compulsion to disclose real-world identities. Users should be able to remain pseudonymous if they wish - only the fact that they are human yes/no should be verified.

- Sybil resistance: High hurdles against multiple registrations of the same person in order to maintain the value of a unique identity. At the same time, the effort for legitimate users should remain manageable (user-friendly, no prohibitively complicated procedures).

- Verifiability: It must be possible for third parties to clearly verify the "verified person" status, e.g. cryptographically or on-chain, so that it can be used automatically (e.g. in apps or content platforms). Ideally, the authorship of content can also be unequivocally linked to such an identity.

- Incentives: In order to create a network effect, participants should be rewarded - be it through access to certain platform benefits, financial incentives (tokens) or intangible values such as increased reputation and trust for verified creators.

These criteria form the benchmark against which ByHuman will be measured as a new concept. In the next section, we explain the objective and core idea of ByHuman before diving into the technical design.

Objective and basic principle of ByHuman

ByHuman (from "by human" in the sense of "created by a human") is a proposal for an alternative proof-of-human system aimed at all those who want to be perceived as human on the web. The aim is to make human authorship verifiable and visible - without compromising the privacy of authors or having to rely on centralized authorities. ByHuman is intended to enable authors, developers, artists, musicians, designers, users, etc. to provide their digital works or posts with proof that a real human mind is behind the creation and not a generative AI. At the same time, each proof should be designed in such a way that it is forgery-proof (i.e. cryptographically verifiable) and can be checked decentrally.

The core idea is based on four basic principles:

1. Self-sovereign identity via ENS domain: Each participant receives a unique Ethereum-based identity in the form of an ENS domain (Ethereum Name Service). ENS domains already function as Web3 usernames and portable digital identities. ByHuman uses this proven system by reserving special domain names such as ByHuman01.eth, human02.eth, ... human1000.eth as identity anchors. Each such domain represents exactly one verified human identity and belongs entirely to the respective user by means of a private wallet key (self-sovereignty). ENS names are uncomplicated and user-friendly-instead of long cryptic addresses, a simple name can be memorized and used across platforms. This makes them the ideal basis for a human identity network that is anchored to Web3 but can be used across the entire Internet.

2. Decentralized verification process without central registration: Instead of a central registration authority or biometric verification, ByHuman relies on a community-driven process to ensure that each person can only obtain one ByHuman domain. A combination of social verification and economic incentives is planned: New applicants for a ByHuman###.eth domain must, for example, be confirmed (vouched) by already verified members and pay a small security deposit. This deposit is refunded as soon as the identity is established, but serves as a safeguard against fraud - if someone tries to create multiple identities, they can be exposed by challenges and would lose their deposit (similar to a security deposit principle). The use of zero-knowledge proofs or external decentralized identity networks as optional additional factors is also conceivable: for example, a user could prove that they were recognized as unique in a BrightID meeting

without disclosing details and present this certificate at the domain claim. The important thing is: No one has to send personal data or biometric features to a central location. Verification is peer-to-peer and cryptographically secured. This means that ByHuman remains ethically compliant and data protection-friendly without sacrificing the rigor required for Sybil resistance. As a result, a Sybil-proof list of human ENS identities is built similar to a membership list - except that this list exists on Ethereum in the form of registered domains/tokens and can be viewed and verified by everyone.

3. Proof-of-Creation through cryptographic signatures: Once a user is equipped with a ByHuman identity, they can now sign digital content to prove their authorship. Every interaction in which creative content is created or published can be countersigned with the private key of the user's own ENS domain. In concrete terms, this means that the author calculates a unique fingerprint (hash) of their work - be it a text document, a code snippet, a piece of music as a file or a graphic image - and creates a digital signature of this hash with their wallet key. This signature can then be attached or linked wherever the work appears (e.g. at the end of a blog post, in the README of a GitHub repository or in the metadata of a music file). Anyone who wants to check the work can now verify whether the signature belongs to a verified human identity. This can be done by checking the signature with the public key of the specified ByHuman###.eth domain - which is possible without an intermediary thanks to of the decentralized ENS registry and Ethereum cryptography. If the signature is correct, it is proven: This work was controlled by the person behind ByHuman###.eth. Since each ByHuman domain is clearly assigned to a real person, human authorship is thus proven. Technically speaking, ByHuman thus provides proof of origin (proof of creation): Content is provided with a timestamp and an author ID. In the event of a dispute (e.g. accusations of plagiarism), it can be shown beyond doubt who registered/signed a particular work first - blockchain timestamping makes this possible. As an alternative or supplement to pure signing, creators could also emboss their work in the form of a token. For example, an artist could issue an NFT directly from their personal address, whereby authenticity is also clearly anchored to the original creator. Soulbound tokens (SBTs) are particularly suitable for proof-of-creation: The creator binds a non-transferable token to their identity address that contains or references certain metadata of the work . Research in the Web3 area has outlined SBTs as a suitable means of recording the origin and ownership of digital works. For example, photographers could store their images as SBTs in their own "soul" (wallet) to prevent

deepfakes, or publicists could publish important statements as SBTs in order to have a reliable track record of their real statements in retrospect. The user is free to decide which variant (signature, NFT or SBT) is preferred in each individual case - what they all have in common is that a cryptographic proof of human authorship is created that cannot be imitated by an AI.

4. Integrations and user-friendliness: One of ByHuman's main focuses is practical usability. The system should fit seamlessly into standard workflows. Thanks to ENS and Ethereum keys, login via wallet is already possible in many apps today (Sign-In with Ethereum) - a standard method in which users authenticate off-chain services by signing a message. ByHuman can dock here: For example, in future an author could log into their blog account with Ethereum and allow the platform to check whether their wallet has a ByHuman.eth domain. This would allow a "verified human" badge to be displayed in the profile or next to posts. The same applies to developer platforms (e.g. GitHub), where you can sign commits with the ENS key or store the ByHuman ID in your profile in order to be recognized as a real developer. The use of ENS as an identity anchor guarantees interoperability - the same identity can be used in different contexts without having to create new accounts everywhere. Thanks to open interfaces (smart contracts and open ENS records), ByHuman can be integrated directly with Web3 apps and with Web2 apps via bridges (APIs or verification services). In short: an adequate solution will only be successful if it is easy to use. ByHuman therefore relies on already established UX patterns (wallet signatures, username domains) instead of exotic hardware or cumbersome checks.

Taken together, ByHuman fulfills the requirements outlined above: It is decentralized (built on Ethereum), preserves privacy (no personalized data in the system, pseudonymity possible), offers Sybil protection (one person - one domain, through community check and economic protection), is clearly verifiable (signatures and on-chain records) and creates motivation to participate through the benefits as well as possible token incentives. The technical design of this concept is described in more detail below.

Technical concept and implementation

In this section, we look at the technical building blocks of ByHuman in detail: from the use of ENS domains and smart contract interactions to security and data protection mechanisms.

Architecture overview and identity anchors (ENS domains)

The foundation of ByHuman is the Ethereum blockchain as a trust-minimized platform. All important processes - registering identities, issuing verification tokens, etc. - are carried out either directly on-chain or with on-chain anchored authenticity. With its global community of participants, immutability of data and smart contract capability, Ethereum offers ideal conditions for building an independent identity system.

Identity anchor: Each verified identity corresponds to a unique ENS domain, e.g. ByHuman09.eth. ENS (Ethereum Name Service) is a decentralized naming system on Ethereum that maps human-readable names to wallet addresses and other information. ENS- domains are owned by the person who controls the associated private key - no third party can take them away or censor them. In ByHuman, the ENS domain serves as the primary key for the identity. It enables a human identity to be represented consistently in different contexts (as a user name, signature verifier, profile, etc.). The name itself - such as ByHuman09.eth - already signals membership in the "ByHuman network". Any number of such domains can be provided for in the concept (beyond ByHuman1000.eth) to enable scaling for millions of users, but without abandoning the "one person - one name" rule.

Registration of a new identity: The allocation of a ByHuman###.eth domain takes place via Smart Contract. A special ByHuman registrar contract manages the list of available identity domains. If a user wants to join the network, they go through the following steps (simplified):

1. Application: the user initiates a request in the DApp frontend and selects one of the free ID names (e.g. the next free number). His wallet creates a transaction to the ByHuman registrar contract, which includes a small deposit (security amount in ETH or a ByHuman-owned token). At the same time, they can attach optional references - e.g. the addresses of already verified friends who want to vouch for them, or a proof of BrightID, etc. This data is collected off-chain and transmitted to the contract (e.g. as an IPFS link or event).

2. Verification phase: The application is made public for a certain period of time (e.g. in a pending state on-chain or on an associated page). During this time, already verified ByHuman members can interact: At least N existing members must submit a vouching signature via transaction to confirm that they believe the new candidate to be genuine. (N could be 1 or 2 initially and later increased depending on the network size). At the same time, all members have the right to raise an objection if they suspect fraud - for this they could trigger a challenge in which they themselves provide a counter-deposit and state a reason (e.g. "Identity X appears to be a duplicate of Y"). A challenge would trigger an arbitration procedure (conceivably via a decentralized court such as Kleros or by majority decision of the community), which would decide whether the application is valid in a serious case. Successful challenges lead to the rejection of the application; the challenger then receives part of the applicant's deposit as a reward (incentive to uncover Sybil attempts), the rest goes to a treasury for system development. If no valid challenge is received and sufficient vouchers have been collected, verification is successful.

3. Assignment: The contract finalizes the registration, assigns the desired ByHuman###.eth ENS domain to the user (the contract functions here similarly to the ENS Auction Registrar, which transfers the domain to the user) and marks the identity as verified. The deposit is refunded to the user (minus any small fees) or - depending on the economic model - transferred to a staking mechanism where the user keeps it tied up as long as he is in the system (as ongoing security). After successful registration, a soulbound NFT representing participation in the ByHuman network could be automatically minted to the address. This NFT is non-transferable (to prevent identity trading) and can carry simple metadata such as the date of verification, possibly the user's pseudonym, etc. It serves as on-chain proof of participation. It serves as on-chain proof that the address is a verified human identity - queryable for other smart contracts.

The entire process takes place transparently on the blockchain, but without personal data having to be disclosed at any point. Neither a real name nor a photo or biometric scan is required - the system relies on social graphs and economic sanctions to make fraud unattractive. Individual privacy is preserved as only pseudonymous identifiers (ENS name, wallet address) and hashes/proofs are exchanged. These mechanisms are comparable to existing decentralized identity registers, but tailored for maximum user-friendliness and minimum data footprint. Even

the ENS profile can remain anonymous - those who wish can voluntarily enter social media handles or an email, which would be possible via ENS Text Records, but is not mandatory. (ENS even offers a "Verified Personhood" badge function, where you can validate your identity via a partner service such as Dentity. However, ByHuman goes one step further and creates a standalone solution that makes such external KYC services unnecessary).

Proof of creation: signing and proving content

Once a person has received their ByHuman identity, they can provide proof of authorship for any digital content. The focus here is on the process of signing content, which has already been described. Technically, there are two main ways of doing this, which can be combined depending on the use case:

- Off-chain signature with on-chain verification: This is the most straightforward method. The user creates a hash of the content locally (e.g. in their authoring software or with a wallet tool) and signs it. The signature (a character string) can then be inserted at the end of a text, for example, or attached to a piece of music as a separate .sig file. A recipient of the content who wants to check the authenticity can calculate the hash of the work themselves and check the signature using the public key of the specified ENS domain. This verification only requires ENS and Ethereum access (the domain's public key can be obtained indirectly from the signature and address, as Ethereum uses ECDSA). Tools could automate this verification - one can imagine browser extensions that display a check mark for a blog article if the signature is valid and comes from a ByHuman ID. Off-chain signatures have the advantage that there are no transaction costs for the creator as long as they only pass on the proof data off-chain. The disadvantage is that with pure off-chain solutions, the time and sequence of publications are more difficult to prove (however, the signed hash can also be stored on a public ledger such as a GitHub Gist or in Arweave, for example, in order to have a timestamp).

- On-chain hash and tokenization: If a unique proof of time is required, the creator can also register the hash of its content on-chain. ByHuman could provide a simple proof-of-creation smart contract: The user sends a transaction with the hash (e.g. IPFS content ID of the work or SHA256 of the text) to the contract; the contract stores the hash together with the sender address and the timestamp of the block time in a log. This creates an unalterable time record of when this account declared content X. Subsequent disputes

about priority (who created something first) can thus be resolved objectively. Alternatively or additionally, the contract could issue the user with an NFT/SBT that references the content . For example, when creating a digital artwork, an artist would immediately mint an NFT that is linked to their ByHuman.eth address - this NFT is initially purely a certificate and not intended for sale. However, it proves authorship and, if necessary, can later be converted into an actual marketing NFT or transferred with a buyer (depending on the desired business model). Soulbound certificates can also represent series (e.g. an SBT that says "This photo belongs to the SummerCollection2025 by photographer XY and is one of 5 authentic works in it" - such a statement could be embedded in the token signed by the creator). The ledger of record concept - i.e. a public log of their publications kept by the creators themselves - creates a traceable history of all official content of a creator in the long term.

It should be as easy as possible for the end user (reader, viewer, listener, recipient) to check all this evidence. Ideally, platforms should recognize the ByHuman verification and visualize it. For example, Medium.com could mark an article with a "ByHuman Authored - Verified by ByHuman" symbol if the author is logged in and verified accordingly. In other cases, there could be a simple online tool or browser plugin where you upload a text or file and receive confirmation that a valid ByHuman hash is registered on the chain.

Important: ByHuman does not guarantee the quality of the content or the complete absence of AI help. A text marked as "human" could well have been created with AI assistance (grammar check, suggestions) - however, a human being vouches for it with their identity and takes responsibility. It is therefore less about technically blocking AI-generated content and more about creating transparency and making human creativity visible again. Unsigned content could have been circulated anonymously by an AI, while signed content is guaranteed to have come from an identifiable human author. This additional layer of provenance information is likely to become crucial in many contexts, be it in science, journalism or art.

Security, anti-counterfeiting and privacy

ByHuman is designed so that it does not store any sensitive personal data centrally. The only relevant data that appears on-chain are ENS domain entries, wallet addresses, cryptographic hashes and any social links (vouchers), but these are pseudonymous. This ensures that high data

protection standards are maintained - no real names, addresses, iris images or similar are passed through the system. Even the vouching members normally only know: "Wallet X vouches for wallet Y".

Tamper-proof: The use of digital signatures and the blockchain as the source of truth makes ByHuman tamper-proof from the ground up. It is almost impossible to forge someone else's identity, as you would need their private key to do so. An AI cannot simply "pretend" - either it cryptographically compromises the account (which is virtually impossible with sufficient key length), or it has no valid proof. Content signed with a specific ByHuman ID can only originate from the person who has access to the corresponding wallet. This means that ByHuman has a much stronger evidential value than, for example, embedded digital watermarks or AI detection algorithms, which always contain uncertainties. The comparison with biometric procedures is also interesting in this respect: while biometric procedures promise to handle biometric data securely, ByHuman does not require such trust - the security and deletion of sensitive data does not even arise, as such data is never recorded. A worst-case scenario with biometric systems is that a user loses their unique identifier or it is misused - as we all know, you can't get a new eye if the iris hash has been compromised. With ByHuman, on the other hand, a user whose wallet has been hacked could lose their identity, but would theoretically be able to obtain a new one via community processes (whereby the old one would be blocked). Recoverability and human control remain a given, as no immutable physical characteristics are involved.

Sybil resistance and protection against abuse: The planned vouching and challenge system is intended to actively prevent multiple identities. Of course, no solution can 100% rule out the possibility of clever fraudsters trying to fool the system (e.g. by a group colluding to confirm each other's phantom identities). However, the combination of social proof and economic punishment makes it very unattractive: every verified user risks their status and possibly financial losses if they support false claims. In addition, by analyzing the graphs (connections who has vouched for whom), conspicuous behavior can be identified - e.g. a cluster where the same few wallets always verify each other. Such cases could be automatically flagged for closer scrutiny. A robust governance model - perhaps in the form of a ByHuman DAO - could set rules for when identities are revoked (e.g. if duplicate accounts are discovered, or if someone is abusing the system for spam/purposes that harm the community). All this is to ensure that the statement "Person X is a human being and is represented exactly once in the system" remains valid.

Privacy and anonymity: As mentioned, users are free to choose how much of themselves they reveal. Some people will want to openly associate their ByHuman domain with their real identity to strengthen their brand (e.g. a well-known author might list ByHuman007.eth as their Verifier ID on their profiles). Others may wish to work under a pseudonym - this is also possible as long as the original verification was done by trusted parties. ByHuman makes a conscious distinction between verification and identification: it confirms that someone is a unique person, but not necessarily who that person is in the civil sense. This principle of pseudonymous reputation has proven itself in online communities and is even strengthened by blockchain technology - you can build up a history of achievements and trust characteristics without showing your passport. However, should a participant voluntarily disclose their identity at some point (e.g. to enforce copyright claims), they can do so - the ByHuman domain can be enriched with clear profile information (ENS allows the storage of e.g. Twitter, Github, website etc. in the name profile). The key point is that the user retains control. Unlike central ID solutions, where you have to hope that the operators don't leak or misuse anything, ByHuman guarantees maximum sovereignty over your own data.

Comparison: ByHuman and biometric solutions at a glance

In order to clearly define the characteristics of ByHuman once again, Table 1 compares the most important features with a biometric approach. It shows how ByHuman is designed as an ethically justifiable, decentralized model that avoids many of the disadvantages of the biometric method.

Criterion	Biometric solution	ByHuman (ENS identity)
Identity principle	One-time biometric scan using proprietary hardware (Orb); a unique personal ID is derived from this.	One-time registration of an ENS domain (e.g. ByHuman123.eth) per person; unique crypto ID based on wallet key, no physical characteristics.
Data protection	Captures highly sensitive biometric data (e.g. iris image); users must trust that hashes are deleted securely and according to promise. Stored in	No biometric or personal raw data required. Pseudonymous identities on blockchain; stored information limited to hashes and signatures. By using ZK evidence (optional),

	central database, vulnerable to misuse if compromised.	off-chain checks could be carried out without disclosing content.
Decentralization	Relies on a centrally developed and controlled hardware stack (orbs) and an organization that operates it.	Built entirely on decentralized infrastructure (Ethereum, ENS). Anyone can participate in the verification process (community vouchers) Smart contracts are open source and the registry is publicly auditable No dependence on proprietary hardware or individual companies.
Accessibility	Requires physical presence at an orb scanner. Distribution of orbs mainly in some cities; many regions underserved.	Only requires internet and a smartphone/computer with wallet. Globally accessible - registration and verification online. No special hardware; even rural or sanctioned areas can participate as long as Ethereum is accessible.
Ethics & acceptance	Vulnerable to regulation - e.g. temporary bans in Europe due to GDPR violations	Clear focus on privacy and voluntariness. No personal data -> compliant with data protection laws. Higher level of trust from the tech community thanks to decentralization and open source approach Ethically harmless, as no one has to disclose sensitive information. Could find wider acceptance among creatives who value their authorship and institutions that want to prove a verified "by-human touch".

Table 1: Comparison of features of a biometric solution vs. ByHuman.

As Table 1 shows, ByHuman represents a paradigm shift away from hardware-dependent biometrics towards a social-technical network approach on existing blockchain infrastructure. The concept is ethically cleaner, as it does not exploit sensitive physical characteristics, and at the same time more flexible in its application, as it is directly interlinked with the digital creative industry.

Integration into Web3 and Web2 platforms

It is crucial for the success of ByHuman that the proof that "humans created this work" is simple and widely usable. The following section outlines some typical application scenarios and what integration might look like. The spectrum ranges from pure Web3 applications to classic Web2 platforms:

- Open Source Code (GitHub): Let's imagine a developer contributing to an open source project. To ensure that his contributions are not made by bots, he can sign his commits with his ENS key. GitHub already supports verified signatures (PGP/GPG); in the future, it could also accept Ethereum signatures. A browser extension or a GitHub Action Workflow could be used to mark which commits originate from ByHuman-verified developers. The user could store their ByHuman###.eth domain in their GitHub profile (via keybase verification or by including a signature block in their README profile). This increases trust in the code quality, as everyone can see: this contributor is a unique human with a verifiable identity, not an automated bot account.

- Blogging and online journalism (e.g. Medium, Mirror): On a blog platform, the author logs in with their Ethereum wallet (Sign-In with Ethereum, already supported natively by Mirror.xyz, for example). The platform recognizes from the wallet that a ByHuman domain exists and has been verified. In the editor, the author can click on "Sign article", whereupon the article content is automatically hashed and signed by the wallet. When publishing, Medium saves this signature hash as the metadata of the post (or references the on-chain proof-of-creation ID). Readers will then see a note next to the article such as "Authorship Verified: ByHuman157.eth (ByHuman)". A reader or fact-checker can click on the details if required and will see, for example "Signed on [date] by the verified identity ByHuman157.eth. Verifiable via Ethereum." - possibly with a link to a verification tool. Such an integration would place a minimal burden on the author (connect wallet once, the rest is done automatically) and have maximum effect, as the information is transparent for every reader.

- Music and audio (e.g. SoundCloud): A music producer uploads a new track. When exporting from his audio workstation, he could register a fingerprint of the song on the blockchain via a plugin (e.g. as a hash in ByHuman's contract or as an NFT). SoundCloud could enter into a partnership so that artists can enter their ByHuman ENS in their profile. When uploading, SoundCloud reads the blockchain: if a matching hash entry is found, or if the artist signs the track file, the release is marked as "ByHuman Verified". In the event of a dispute (e.g. if someone else has released the same track as an AI remix), the artist can present their original timestamp and signature as proof. For listeners, it is immediately clear that this song comes directly from a verified artist - which will be a valuable

distinguishing feature, especially in times of AI-generated music (keyword: AI clones of artists' voices).

- Design and digital art (Behance, DeviantArt, NFT marketplaces): Visual works can be treated similarly. Platforms like Behance could introduce a feature where designers link their uploads to a blockchain ID. DeviantArt is already working on AI detection and warning systems for unauthorized AI use of artworks - ByHuman could complement this by providing certified "human art" profiles. On NFT marketplaces, the situation is Web3-native anyway: Here, ByHuman could simply serve as an additional filter - buyers could set to only see NFTs that have been minted by verified ByHuman accounts (e.g. to filter out AI bulk goods).

- Social media and forums: In classic social networks (Twitter/X, Reddit, StackExchange), ByHuman could be used indirectly. For example, a Twitter user could have their .ByHuman.eth name in their profile; a browser extension or an unofficial verification bot account could then add a small symbol to posts from such users. Elon Musk has announced that he wants to make all human users on X recognizable - ByHuman would offer an open solution that is effective across platforms instead of being owned by a single company. The same applies to forums: a plugin for common forum software that allows users to log in via an Ethereum wallet and gives them a "ByHuman" badge would be conceivable. This would curb bot and troll accounts.

Table 2 below provides an overview of how exemplary platforms could integrate ByHuman and the immediate benefits this would bring:

Platform/area	**Integration**	**Benefit**
Open source code (GitHub)	Developers sign commits with their ByHuman key; GitHub or a plug-in checks the signature and displays a verified badge in the repo.	Increased trust in contributions - code from verified human developers recognizable, less risk from bot accounts.
Blog/Article (Medium)	Authors log in via Sign-In with Ethereum and link their ENS name. When publishing, a content hash is automatically registered or	Readers can immediately see that the text comes from a real person (not completely AI-generated). Increases credibility and authority of articles, especially in journalism and research.

	signed on-chain. Medium displays a "ByHuman" seal on the article.	
Music (SoundCloud)	Artists store their ByHuman ENS in their profile. When a song is uploaded, the audio track is hashed and signed by the ByHuman app; e.g. SoundCloud saves the signature receipt.	Listeners see a human creator notice on the track. The artist has a verifiable timestamp of their original, which protects them from plagiarism or AI copies. Music fans can specifically support human-created music.

Table 2: Examples of ByHuman integration in popular platforms and applications.

These integration examples show that ByHuman does not exist in isolation, but can serve as an infrastructure building block for a more human digital world. The hurdles for implementation are lower than they might seem - many building blocks (ENS, Ethereum login, NFT interfaces) already exist and only need to be combined in a targeted manner. It will be crucial to create sufficient awareness and enter into partnerships with platforms so that the ByHuman certificate becomes a recognized quality feature. This is where incentive models and a clever publishing strategy come into play.

Monetization and incentive models

For ByHuman to be accepted by users and sustained in the long term, it needs meaningful incentives. Two questions arise: "What do individuals gain from participating?" and "How is the system financially self-sustaining?". Some possible models, which can also be combined, are discussed below.

1. Direct token incentives (crypto UBI or rewards) are not necessary, as ByHuman is aimed at content creators. Users are primarily interested in recognition and protection of their own work.

2. Reputation and visibility: In creative industries, reputation is worth money. A ByHuman certificate can help a person find fans, clients or buyers more easily because there is trust. For example, an online marketplace for freelance work (copywriters, designers, programmers) could give preference to verified ByHuman accounts - companies looking for quality in the age of AI content would rather hire someone who can prove their identity and authorship. This is indirect monetization: those who are verified get competitive

advantages. ByHuman could encourage such behavior by entering into partnerships with platforms. A verification badge on portals such as Upwork, Fiverr or similar for ByHuman members would be conceivable. Or a "ByHuman Marketplace" list on a ByHuman website, where all verified people are listed - a kind of directory that customers can search specifically for "real" content creators. This network effect - the more good people are verified, the more demand, the more people want to be verified - is a strong driver and requires marketing and persuasion above all.

3. Community governance and staking: Another incentive for users - especially tech-savvy ones - can be co-creation. If ByHuman is organized as a DAO, verified users can, for example, automatically become members of the DAO and vote on important parameters (e.g. deposit amount, approval of new partner platforms, etc.). This increases identification with the project. Staking mechanisms could be introduced in which, for example, vouching members deposit a certain amount in a bond and are rewarded for this over time as long as no abuses occur. A kind of "Identity Curators" program: those who actively contribute to gaining new honest members (through vouchers) and thus grow the network receive recognition points or token rewards. Conversely, they lose a stake if they wave fraudsters through. This creates a self-regulating system in which the participants' incentives are aligned with the integrity of the network.

4. Monetization for creators through protected content: Finally, individuals themselves benefit financially from the fact that their works are protected. If they can prove that they are the creator of successful content, they can more easily claim compensation in the event of copycats or unintentional AI training use. The extent to which AI-generated works are eligible for copyright protection is currently the subject of legal debate - the tendency is to give priority to genuine human creations. ByHuman provides exactly the evidence that an author needs to show in case of doubt: "I as a human created this work, here is the digital fingerprint with date and signature." This legal certainty argument is worth hard cash for professional content producers, as it better protects their intellectual property.

Overall, ByHuman creates an ecosystem in which real people can express their creativity and be rewarded for it - be it in the form of higher visibility, direct tokens or simply the trust that their brand enjoys. On the other hand, consumers or AI systems could even pay to use verified content in the future. Imagine news portals that only accept ByHuman-tagged articles as sources

(because they know they weren't invented by a bot). A paywall could prioritize content from real people or provide it with a premium. While such developments are still some way in the future, they show the potential: human authenticity is itself becoming a currency. ByHuman wants to coin this currency - literally and figuratively.

Social and ethical implications

The introduction of a system like ByHuman also raises questions beyond technology. Overall, however, the social and ethical benefits are clear:

- Strengthening human creativity: in an age where AI generators spit out masses of average content, ByHuman can help highlight the value of original human creation. It creates a two-tier division - but a meaningful one: responsible human authorship vs. anonymous generic content. This gives genuine writers, artists and thinkers a distinguishing feature that enhances the value of their work. For the audience, it means the chance to consciously choose content with a human fingerprint when authenticity is desired.

- Transparency and finding the truth: Fake news and deepfakes are serious problems. If, for example, only verified people were allowed to participate in social networks, this would be too restrictive. But ByHuman can at least add a verified layer: Statements that come with an identified reputation could be weighted differently than completely anonymous posts. Anyone spreading false news under their ByHuman ID risks their reputation (and the loss of their verified identity if the community intervenes). Overall, this promotes a culture of responsibility in the digital space. At the same time, anonymous freedom of expression remains possible - ByHuman is voluntary. It does not force anyone to reveal their identity if they do not want to. It only offers the option of underpinning one's own credibility.

- Inclusivity vs. new digital divide: A potential risk with such systems is that they could exclude people who do not have access to technology. ByHuman strives to keep the threshold as low as possible (all that is needed is internet access and a simple smartphone to use the wallet). Nevertheless, initiatives need to be launched to get less tech-savvy people on board - for example, workshops for creative people on how to digitally sign

their work. The impression must not be created that you have to be a blockchain expert to be considered a real artist. ByHuman should be seen as a tool that stays in the background, similar to SSL certificates on the web: People perceive them as a seal of approval, without knowing every technical detail. Education and usability are essential here, so that no new digital divide is created between verified "tech-savvy" creators and those who shy away from so-called new territory.

- Privacy and self-determination: From an ethical point of view, ByHuman has a clear advantage over biometric solutions because it respects the self-determination of participants. Where biometric solutions implicitly ask users to "Trust us with your unique biometric features", ByHuman says: "Keep your secrets; we believe you even if your peers confirm you." This principle ties in with the idea of self-sovereign identity (SSI), which is propagated in many future-oriented digital identity concepts. The user decides when to reveal what about themselves. ByHuman provides the infrastructure to verify certain claims (e.g. "I am a unique person" or "I created this and that") without having to reveal who you are in a civic sense or what you look like. This promotes freedom and reduces opportunities for discrimination - in an anonymized form, it's the content that counts, not the person. If someone decides to give up their pseudonymity and link the ByHuman verification to their real identity (e.g. a prominent author who proudly displays their verification certificate), this is also voluntary and controlled.

- Potential for abuse: Of course, one must also be vigilant that ByHuman is not misused. For example, a regime could try to make ByHuman identities mandatory in order to monitor all citizens online. This is countered by the decentralized nature - no government controls the system. Moreover, coercion would be counterproductive, as ByHuman can always be circumvented by simply acting without a certificate (but then with less trust). Another scenario: Could AI operators themselves try to obtain ByHuman IDs at some point in order to give their bots a "human mask"? It would be possible, for example, for an AI to grab a stolen or purchased verified wallet and sign it. Similar to social media account theft, such cases would fall into the area of classic cybercrime and could be detected and sanctioned by the community (e.g. identity revocation if the rightful owner reports the theft). ByHuman therefore does not create a new threat area, but rather adds a layer of protection: the authenticity check, where previously blind trust or complicated evidence was required.

To summarize, ByHuman fits in well with values that are demanded in technology ethics and politics: Transparency, privacy, decentralization and empowerment of the individual. It can be a useful tool for maintaining the balance between rapidly advancing AI and human control. It will be important to strictly adhere to these values during implementation - e.g. through open governance, public audits of smart contracts and collaboration with civil society groups.

Conclusion

ByHuman is a new type of whitepaper concept for Proof of ByHuman, which is intended for use in the digital economy in particular. It combines proven Web3 technologies - above all Ethereum and ENS - with a community-based verification process to establish unique, human digital accounts. These ByHuman.eth identities can be used to cryptographically sign content of any kind and prove its human authorship. Unlike biometric approaches, ByHuman fully preserves user privacy and relies on decentralization and open source. This minimizes ethical concerns and lowers the barriers to broad acceptance.

Technically, the concept is designed in such a way that it can already be implemented today: the Ethereum infrastructure offers all the basic functions required, from wallet-based logins to NFT/SBT issuance and global availability. Finally, it should be emphasized that ByHuman is not a panacea - AI generation in itself is nothing illegitimate. Rather, ByHuman provides a toolset to put freedom of choice and trust back into people's hands: One can recognize where a human is directly responsible, and where possibly not. This additional meta-information will become increasingly valuable as AI becomes more pervasive in all areas of life. ByHuman is thus positioning itself at the cutting edge, at the interface of blockchain, AI and digital society.

ByHuman is more than a technical tool - it is a step towards a digital world in which human creativity takes center stage again, supported by the power of decentralization.