HUMANITY: A Unified Identity Protocol
Part I — Using Real-time Human Proofs to combat sybil attacks

Shlok Dharmesh Mange
shlok@0xrivendell.xyz

as of Aug 26, 2024

Abstract. The HUMANITY protocol is designed to serve as the unified identity layer for all internet applications, seamlessly integrating both on-chain and off-chain identities into a single, secure layer. HUMANITY leverages a wide range of on-chain data, including decentralized finance (DeFi) activity, recency bias, active transactions, and NFTs/tokens held. This on-chain data is complemented by real-time human proofs gathered from various hardware sources, including: ***Phones (Face ID), Laptops (Touch ID), Apple Watch, Fitbit & Apps indicating real-time activity, such as: Luma (proof of events) Strava (proof of movement)*** By combining these diverse data sources, HUMANITY provides a comprehensive and dynamic identity verification system. This system is further fortified by zero-knowledge proofs (ZKPs) submitted on-chain via an Eigenlayer Active Validated Services (AVS), ensuring privacy, security, and compliance across all applications while maintaining user anonymity and data protection. The HUMANITY protocol thus offers a robust solution for identity verification that respects user privacy, leverages cutting-edge technology, and adapts to the evolving needs of both Web3 and traditional internet applications.

1. Introduction

The rapid evolution of blockchain technology has ushered in a new era of decentralized applications (dApps) and financial services, fundamentally reshaping the digital landscape. However, this burgeoning ecosystem faces a critical challenge: the absence of a unified identity layer. This deficiency has led to a fragmented identity verification landscape, creating significant hurdles in terms of compliance, security, and user experience.

HUMANITY emerges as a revolutionary solution to these challenges, offering a unified identity protocol that seamlessly aggregates both on-chain and off-chain identity data. By doing so, HUMANITY not only simplifies the identity verification process but also significantly enhances security through the implementation of cutting-edge zero-knowledge proofs. Furthermore, HUMANITY ensures compliance with global regulatory standards, setting a new benchmark for identity management in the decentralized world.

The implications of HUMANITY's approach extend far beyond the confines of Web3. By aggregating on-chain and off-chain identities, HUMANITY positions itself as a potential replacement for centralized KYC API services, offering a more comprehensive, secure, and efficient solution for identity verification across various compliance-centric applications.

2. Problem Statement

The current identity verification landscape in the Web3 ecosystem is plagued by fragmentation and inefficiencies, presenting a significant barrier to widespread adoption and seamless user experience. Users are often required to navigate multiple wallet connection processes across different blockchain networks, manage multiple user-owned wallets, and interact with app-specific smart wallets. This redundancy not only creates friction in the user experience but also increases the risk of data breaches and identity theft.

Moreover, existing identity verification systems fail to fully capitalize on the wealth of on-chain data available. This data, which includes transaction histories, token holdings, and participation in decentralized governance, offers a rich tapestry of information that could provide a more comprehensive and nuanced view of a user's identity and activity within the ecosystem.

The lack of a unified identity protocol also severely hampers interoperability among dApps and financial services. This limitation stands in stark contrast to the promise of Web3 – a seamless, interconnected digital ecosystem where users have full control over their data and can move freely between services without repeatedly verifying their identity.

Furthermore, the challenge of ensuring compliance with diverse and often complex regulatory requirements while simultaneously maintaining user privacy remains a significant hurdle. Traditional KYC processes, which often involve the centralized storage of sensitive personal information, are ill-suited to the decentralized ethos of Web3 and pose significant security risks.

These challenges collectively create a pressing need for a solution that can:

1. Unify identity verification across multiple blockchains and applications
2. Leverage both on-chain and off-chain data for comprehensive identity proofing
3. Ensure regulatory compliance without compromising user privacy
4. Enhance security and reduce the risk of identity fraud
5. Improve user experience by streamlining identity verification processes
6. Foster greater interoperability within the Web3 ecosystem

HUMANITY aims to address these challenges head-on, providing a robust, secure, and user-centric identity solution that aligns with the decentralized principles of Web3 while meeting the stringent requirements of global regulatory standards.

3. The Need for Unified Identity in Web3

In the rapidly evolving landscape of Web3, the need for a unified identity solution has become increasingly apparent. As decentralized technologies continue to reshape industries and redefine digital interactions, the importance of secure, verifiable, and portable identity cannot be overstated. HUMANITY's unified identity protocol addresses this critical need, offering a comprehensive solution that bridges the gap between on-chain and off-chain identities.

3.1 Enhancing Security and Trust

In the decentralized world of Web3, where transactions and interactions occur without intermediaries, establishing trust is paramount. Traditional identity verification methods, rooted in centralized systems, are often inadequate in this context. HUMANITY's approach to unified identity leverages the immutability and transparency of blockchain technology, combined with the richness of off-chain data, to create a more robust and trustworthy identity ecosystem.

By aggregating multiple data points from both on-chain and off-chain sources, HUMANITY creates a multi-dimensional identity profile that is significantly more difficult to forge or manipulate. This enhanced security not only protects individual users but also strengthens the integrity of the entire Web3

3.2 Streamlining User Experience

The current fragmented state of identity verification in Web3 often results in a cumbersome user experience. Users are frequently required to undergo multiple verification processes across different platforms, leading to frustration and potential abandonment of services. HUMANITY's unified approach streamlines this process, allowing users to verify their identity once and use it across multiple platforms and services.

This seamless experience not only improves user satisfaction but also reduces barriers to entry for new users, potentially accelerating the adoption of Web3 technologies and services.

3.3 Enabling Compliance and Privacy

One of the most significant challenges in the Web3 space is balancing regulatory compliance with the principles of privacy and decentralization. HUMANITY's unified identity protocol addresses this challenge by providing a flexible framework that can adapt to various regulatory requirements without compromising user privacy.

Through the use of zero-knowledge proofs and other advanced cryptographic techniques, HUMANITY allows users to prove specific attributes of their identity without revealing unnecessary personal information. This approach ensures compliance with KYC/AML regulations while preserving the privacy-centric ethos of Web3.

3.4 Fostering Interoperability

The lack of a standardized identity layer has been a significant obstacle to achieving true interoperability in the Web3 ecosystem. HUMANITY's unified identity protocol serves as a bridge between different blockchain networks, dApps, and services, enabling seamless interaction and data portability.

This interoperability not only enhances the user experience but also opens up new possibilities for cross-platform services and applications, driving innovation and collaboration within the ecosystem.

3.5 Empowering User-Centric Data Control

In line with the principles of Web3, HUMANITY puts users in control of their identity data. Unlike traditional centralized systems where user data is often siloed and controlled by corporations, HUMANITY's approach allows users to manage and selectively share their identity information.

This user-centric model not only aligns with the ethos of decentralization but also complies with data protection regulations like GDPR, which emphasize user consent and data portability.

4. Onchain Data Utilization

HUMANITY's innovative approach to identity verification leverages the rich tapestry of on-chain data available across various blockchain networks. This data, which is inherently transparent, immutable, and verifiable, provides a dynamic and comprehensive view of a user's digital footprint within the Web3 ecosystem. By harnessing this data, HUMANITY creates a more nuanced and accurate representation of user identity, enhancing security and trust in decentralized environments.

4.1 Types of On-Chain Data Utilized

HUMANITY aggregates and analyzes a wide range of on-chain data points, including but not limited to:

1. Farcaster Activity: Interactions and engagement on the Farcaster protocol, a decentralized social media platform, provide insights into a user's social presence and influence within the Web3 community.

2. DeFi Transaction History: A user's history of interactions with decentralized finance (DeFi) protocols, including lending, borrowing, and trading activities, offers a comprehensive view of their financial behavior and creditworthiness.

3. Multiple Wallet Ownership: By linking multiple wallet addresses to a single identity, HUMANITY creates a more complete picture of a user's on-chain assets and activities across different blockchain networks.

4. ERC721 Ownership: Possession of non-fungible tokens (NFTs) can indicate participation in digital art markets, gaming ecosystems, or other blockchain-based communities, adding another layer to the user's digital identity.

5. Governance Forum Activities: Participation in decentralized autonomous organization (DAO) governance processes, including voting and proposal submissions, demonstrates a user's engagement with and commitment to specific projects or ecosystems.

6. Token Holdings and Transactions: The types and quantities of tokens held, as well as transaction patterns, can provide insights into a user's investment strategies and areas of interest within the crypto space.

7. Smart Contract Interactions: The frequency and nature of interactions with various smart contracts can indicate a user's level of engagement with different dApps and services.

4.2 Benefits of On-Chain Data Utilization

The incorporation of on-chain data into HUMANITY's identity verification process offers several key advantages:

1. Real-Time Verification: On-chain data is continuously updated, allowing for real-time identity verification and risk assessment.

2. Fraud Prevention: The immutability of blockchain data makes it extremely difficult to falsify on-chain activities, enhancing the security of the identity verification process.

3. Behavioral Insights: Analysis of on-chain activities can provide valuable insights into a user's behavior, preferences, and risk profile, enabling more tailored services and risk management strategies.

4. Cross-Chain Identity: By aggregating data from multiple blockchain networks, HUMANITY creates a comprehensive cross-chain identity that accurately represents a user's entire Web3 presence.

5. Reputation Building: Consistent positive on-chain activity can contribute to building a strong digital reputation, which can be valuable in various Web3 applications, from DeFi to decentralized marketplaces.

4.3 Data Analysis and Scoring

HUMANITY employs advanced analytics and machine learning algorithms to process and interpret on-chain data. This analysis results in a dynamic identity score that reflects a user's overall on-chain activity and trustworthiness. The scoring system takes into account factors such as:

- Longevity and consistency of on-chain activity
- Diversity of interactions across different protocols and networks
- Volume and value of transactions
- Participation in governance and community activities
- Adherence to best practices in wallet security and management

This identity score serves as a powerful tool for risk assessment, enabling dApps and financial services to make informed decisions about user access and privileges while maintaining user privacy through zero-knowledge proofs.

4.4 Privacy and Data Protection

While HUMANITY leverages public on-chain data, it does so with a strong commitment to user privacy. The protocol implements advanced cryptographic techniques, including zero-knowledge proofs, to allow users to selectively prove aspects of their on-chain identity without revealing specific transaction details or wallet addresses.

This approach ensures that users maintain control over their data while still benefiting from the enhanced trust and verification that on-chain data provides.

5. Offchain Data Integration

While on-chain data provides a wealth of information about a user's activities within the blockchain ecosystem, off-chain data is equally crucial for creating a comprehensive and legally compliant identity solution. HUMANITY's innovative approach seamlessly integrates off-chain data sources, ensuring a holistic view of user identity that meets both the technical requirements of Web3 and the regulatory standards of traditional finance.

5.1 Types of Off-Chain Data Integrated

HUMANITY incorporates a diverse range of off-chain data sources, including but not limited to:

1. Social Media Activity: Platforms like Twitter, Reddit, Google, Facebook, Uber, Strava offer valuable insights into a user's digital footprint and social influence. HUMANITY utilizes metrics which can indicate a user's credibility and reach within their network.

2. Developer Contributions: For developer-centric applications or airdrops, GitHub commit history provides a verifiable record of a user's contributions to open-source projects, demonstrating their expertise and engagement in the tech community.

3. Traditional Identity Documents: To ensure compliance with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations, HUMANITY integrates verification of government-issued identification documents such as:
   - National ID cards
   - Passports
   - Driver's licenses
   - Social Security Numbers (SSNs) or equivalent national identifiers

4. Proof of Address: Verification of physical residency through documents like utility bills or bank statements, which are often required for regulatory compliance.

5. Professional Credentials: Integration of professional licenses, certifications, or educational qualifications can add another layer of verification for specific use cases.

6. Credit Scores and Financial History: Where applicable and with user consent, traditional credit scores and financial history can be incorporated to provide a more comprehensive financial profile.

7. Biometric Data: Advanced identity verification may include biometric data such as facial recognition or fingerprint scans, always with stringent privacy protections in place.

5.2 Benefits of Off-Chain Data Integration

The incorporation of off-chain data into HUMANITY's identity protocol offers several key advantages:

1. Regulatory Compliance: By verifying traditional identity documents, HUMANITY ensures that its identity solution meets the stringent KYC and AML requirements of global financial regulations.

2. Enhanced Trust: The combination of on-chain and off-chain data creates a more complete and trustworthy identity profile, reducing the risk of fraud and increasing confidence in digital interactions.

3. Broader Applicability: The inclusion of off-chain data makes HUMANITY's identity solution valuable not only in Web3 but also in traditional Web2 applications, bridging the gap between these ecosystems.

4. Contextual Identity: Off-chain data provides context to on-chain activities, offering a more nuanced understanding of a user's identity and behavior.

5. Risk Mitigation: Access to a broader range of data points allows for more accurate risk assessment, benefiting both users and service providers in the ecosystem.

5.3 Data Verification and Integration Process

HUMANITY employs a sophisticated process for verifying and integrating off-chain data:

1. Document Verification: Advanced OCR (Optical Character Recognition) and machine learning algorithms are used to verify the authenticity of uploaded identity documents.

2. Biometric Verification: Where applicable, facial recognition technology is used to match the user to their submitted identification documents.

3. API Integrations: HUMANITY integrates with reputable third-party services for verifying social media accounts, developer contributions, and other off-chain data sources.

4. Data Normalization: Off-chain data from various sources is normalized and standardized to ensure consistency within the HUMANITY ecosystem.

5. Continuous Monitoring: The system continuously monitors and updates off-chain data to ensure the ongoing accuracy and relevance of user identities.

5.4 Privacy and Data Protection Measures

HUMANITY prioritizes user privacy and data protection in its handling of off-chain data:

1. Data Minimization: Only essential data is collected and stored, adhering to the principle of data minimization.

2. Encryption: All sensitive off-chain data is encrypted using the face id as a public-private key pair, which is then hashed using the keccak256 to create a node for the merkle root.

3. Zero-Knowledge Proofs: Similar to on-chain data, off-chain data is often verified using zero-knowledge proofs, allowing users to prove specific attributes without revealing the underlying data.

4. User Control: Users have full visibility into what off-chain data is associated with their identity and can choose which elements to share in different contexts.

5. Compliance with Data Protection Regulations: HUMANITY's data handling practices are designed to comply with global data protection regulations such as GDPR and CCPA.

By seamlessly integrating both on-chain and off-chain data, HUMANITY creates a robust, versatile, and compliant identity solution that meets the diverse needs of the evolving digital landscape while maintaining the highest standards of user privacy and data protection.

6. Zero-Knowledge Proofs and Eigenlayer AVS

At the heart of HUMANITY's innovative approach to identity verification lies the powerful combination of Zero-Knowledge Proofs (ZKPs) and Eigenlayer's Actively Validated Services (AVS).

This technological synergy enables HUMANITY to offer unprecedented levels of privacy, security, and scalability in identity management for the Web3 ecosystem and beyond.

6.1 Zero-Knowledge Proofs: Ensuring Privacy and Verifiability

Zero-Knowledge Proofs are cryptographic methods that allow one party (the prover) to prove to another party (the verifier) that a statement is true without revealing any information beyond the validity of the statement itself. In the context of HUMANITY, ZKPs play a crucial role in preserving user privacy while enabling secure identity verification.

Key Aspects of ZKP Implementation in HUMANITY:

1. Selective Disclosure: Users can prove specific attributes of their identity (e.g., age over 18, residency in a particular country) without revealing the actual data.

2. Credential Verification: ZKPs allow for the verification of credentials (e.g., educational qualifications, professional certifications) without exposing the underlying details.

3. Transaction Privacy: Users can prove their transaction history or token holdings without revealing specific transaction details or wallet addresses.

4. Scalability: ZKPs significantly reduce the amount of data that needs to be processed on-chain, enhancing the scalability of the HUMANITY protocol.

5. Compliance and Privacy Balance: ZKPs enable HUMANITY to meet regulatory compliance requirements while maintaining user privacy, a critical balance in the evolving digital landscape.

7. Security and Compliance

HUMANITY's integration of on-chain data and real-time human proofs, secured by zero-knowledge proofs (ZKPs), offers a robust solution for identity verification. This approach not only ensures a high level of security but also protects against identity fraud and data breaches. By leveraging blockchain technology and advanced cryptographic techniques, HUMANITY provides a secure and privacy-preserving identity layer for internet applications.

8. Interoperability: Bridging the Gap in Digital Identity

HUMANITY's innovative approach to identity verification serves as a cornerstone for enhanced interoperability across the digital landscape. By providing a unified identity layer, HUMANITY breaks down the silos that have long plagued both Web3 and traditional internet applications, creating a seamless ecosystem where user identities are portable, verifiable, and secure.

8.1 Cross-Platform Accessibility

With HUMANITY, users can effortlessly navigate across multiple platforms and services using a single, comprehensive identity. This eliminates the need for repetitive sign-ups and verifications, significantly reducing friction in the user experience. Whether accessing decentralized applications (dApps), financial services, or traditional web platforms, users maintain control over their identity while enjoying simplified access.

8.2 Enhanced User Experience

The interoperability facilitated by HUMANITY translates directly into an improved user experience. By eliminating the need to manage multiple identities across various platforms, users can focus on engaging with services rather than navigating complex identity verification processes. This streamlined approach not only saves time but also reduces cognitive load, making digital interactions more intuitive and user-friendly.

8.3 Fostering Web3 Adoption

HUMANITY's interoperable identity solution plays a crucial role in accelerating the adoption of Web3 technologies. By bridging the gap between traditional web services and blockchain-based applications, HUMANITY lowers the barrier to entry for new users. This seamless integration encourages exploration of decentralized services, fostering greater participation in the Web3 ecosystem.

8.4 Empowering Developers and Service Providers

For developers and service providers, HUMANITY's interoperable identity layer opens up new possibilities for innovation. By leveraging a standardized, secure identity protocol, developers can focus on creating value-added services rather than reinventing identity verification systems. This not only speeds up development cycles but also ensures a consistent and secure user experience across different applications.

8.5 Cross-Chain Compatibility

In the fragmented landscape of blockchain networks, HUMANITY serves as a unifying force. Its identity solution is designed to work across multiple blockchain ecosystems, enabling users to maintain a consistent identity regardless of the underlying blockchain technology. This cross-chain compatibility is crucial for the long-term growth and integration of the Web3 ecosystem.

By enhancing interoperability through its unified identity layer, HUMANITY is not just improving user experience and fostering adoption; it's laying the groundwork for a more connected, efficient, and user-centric digital future. As the digital landscape continues to evolve, HUMANITY's role in ensuring seamless, secure, and verifiable identity across platforms will become increasingly vital.

9. Implementation of HUMANITY

Developers and businesses looking to integrate HUMANITY into their applications will find a robust and developer-friendly ecosystem at their disposal. The protocol offers comprehensive APIs and Software Development Kits (SDKs) that streamline the integration process, allowing for seamless incorporation of HUMANITY's identity verification capabilities into existing or new applications. These tools are designed with flexibility in mind, catering to a wide range of use cases across both Web3 and traditional internet applications. The API documentation provides detailed guides, code samples, and best practices, ensuring that developers can quickly understand and implement HUMANITY's features, regardless of their familiarity with blockchain technology or zero-knowledge proofs.

At the core of HUMANITY's implementation is its unwavering commitment to privacy and security. The protocol leverages advanced zero-knowledge proofs (ZKPs) to ensure that identity data remains private and secure throughout the verification process. This means that applications can verify specific attributes of a user's identity without accessing or storing sensitive personal information. Furthermore, the integration of Eigenlayer's Actively Validated Services (AVS) provides a mechanism for ongoing verification and real-time updates to identity data. This dynamic approach ensures that the identity information remains current and reliable, adapting to changes in a user's digital footprint across various platforms and activities. By combining these cutting-edge technologies, HUMANITY offers a solution that not only simplifies identity verification but also sets new standards for privacy and security in digital interactions.

10. Adoption Strategies

To drive widespread adoption, HUMANITY is implementing a multi-faceted strategy that engages key stakeholders across various digital ecosystems. The protocol's approach focuses on demonstrating the tangible benefits of a unified identity layer, positioning HUMANITY as the standard for identity verification in both decentralized and traditional digital environments.

10. 1 Engaging Web3 Ecosystem

HUMANITY is actively collaborating with prominent players in the Web3 space, including:

- **dApp Developers**: By providing easy-to-integrate SDKs and comprehensive documentation, HUMANITY is making it simple for dApp developers to incorporate robust identity verification into their applications.
- **DeFi Platforms**: HUMANITY is partnering with decentralized finance protocols to enhance security and streamline user onboarding processes.
- **NFT Marketplaces**: Collaborations with NFT platforms are helping to verify creator identities and combat fraud in the digital art space.
- **DAOs**: HUMANITY is working with decentralized autonomous organizations to improve governance processes through verified identities.

10. 2 Bridging to Traditional Finance

HUMANITY recognizes the importance of bridging the gap between decentralized and traditional financial services. Strategies include:

- Partnerships with fintech companies to demonstrate the benefits of blockchain-based identity verification.
- Collaborations with traditional banks to explore hybrid identity solutions that meet regulatory requirements while leveraging blockchain technology.

10.3 Educating Regulatory Bodies

HUMANITY is actively engaging with regulatory bodies to:

- Demonstrate how blockchain-based identity verification can enhance security and reduce fraud.
- Collaborate on developing standards that balance innovation with consumer protection.
- Showcase how zero-knowledge proofs can address privacy concerns in digital identity verification.

10.4 User-Centric Adoption Approach

To drive user adoption, HUMANITY is focusing on:

- Developing intuitive user interfaces that simplify the identity verification process.
- Creating educational content to help users understand the benefits of a unified identity layer.
- Implementing rewards programs to incentivize early adopters and active users.

11. Future Developments

HUMANITY is committed to continuous innovation, with several exciting developments on the horizon:

11.1 Enhanced Real-Time Human Proofs

Building on its foundation of using hardware-based proofs, HUMANITY plans to expand its capabilities:

- **Advanced Biometric Integrations**: Exploring cutting-edge biometric technologies beyond facial and fingerprint recognition, potentially including gait analysis and voice recognition.
- **IoT Device Integration**: Expanding compatibility with a wider range of Internet of Things (IoT) devices to gather more diverse and reliable activity proofs.
- **AR/VR Identity Verification**: Developing solutions for identity verification in augmented and virtual reality environments.

11.2 Expanding Data Sources

HUMANITY will continue to broaden its data sources to create an even more comprehensive identity layer:

- **Social Media Analytics**: Developing more sophisticated algorithms to analyze social media activity for identity verification, while maintaining user privacy.
- **Professional Network Integration**: Exploring partnerships with professional networking platforms to incorporate career-related identity attributes.
- **Academic Credential Verification**: Collaborating with educational institutions to provide verifiable academic credentials on-chain.

11.3 Cross-Chain Interoperability

To further enhance its utility across the blockchain ecosystem, HUMANITY is focusing on:

- Developing cross-chain identity solutions that work seamlessly across multiple blockchain networks.
- Creating interoperability standards for identity verification across different blockchain protocols.

By focusing on these adoption strategies and future developments, HUMANITY aims to position itself as the leading unified identity layer for the digital world, bridging the gap between Web3 and traditional internet applications while setting new standards for privacy, security, and user empowerment in digital identity verification.

12. Conclusion

HUMANITY represents a groundbreaking advancement in digital identity verification, bridging the gap between Web3 and traditional internet applications. By seamlessly integrating on-chain data with real-time human proofs from various hardware sources, HUMANITY creates a comprehensive and dynamic identity layer that addresses the critical challenges of fragmentation and security in the digital realm. The protocol's use of zero-knowledge proofs and Eigenlayer AVS ensures that user identities remain verifiable and private while being continuously updated. As a unified identity solution, HUMANITY not only enhances interoperability across diverse digital platforms but also sets new standards for user privacy and security. With its robust adoption strategies and forward-looking development roadmap, HUMANITY is well-positioned to drive greater trust, efficiency, and innovation in both decentralized and traditional digital ecosystems, paving the way for a more connected and secure digital future.

13. References

Polygon ID: Zero Knowledge Identity for Web3
https://polygon.technology/blog/introducing-polygon-id-zero-knowledge-own-your-identity-for-web3

Web3: A decentralized societal infrastructure for Identity, Trust, Money, Data
https://ar5iv.labs.arxiv.org/html/2203.00398

Digital Identity: Assessing Web3's Building Blocks by JP Morgan
https://www.jpmorgan.com/onyx/digital-identity-web3-building-blocks

Mastering Decentralized Identity: A Pillar of Web3
https://blockworks.co/news/what-is-decentralized-identity

Using Aggregation To Solve Identity
https://workweek.com/2022/08/22/using-aggregation-in-web3-to-solve-identity/