Reinventing Identity: A ParallelChain Initiative

JESSIE CHAN, IAN HUANG
PARALLELCHAIN LAB

Introduction

We live in an era where digital interactions are as significant as, and in fact often overlap with, physical ones. In such a world, the concept of identity must evolve to encompass the various aspects of an individual's existence, both online and offline. ParallelChain is well positioned to bring this evolved concept of identity to reality. By leveraging pioneering blockchain and artificial intelligence (AI) technologies, ParallelChain provides the blockchain platform for a thriving community to build identity solutions and applications that will change our everyday experience.

What is Identity?

The concept of identity is multifaceted, necessitating both philosophical inquiry and tangible data. To navigate the discussions and solutions presented by ParallelChain in this paper, it is crucial to first define 'identity'.

Subjective identity refers to the social and psychological aspects of who we are, encompassing personal beliefs, values, and experiences. Subjective identity is not easily quantified or captured – and is not easily represented by the concrete data and binary code of digital systems.

Objective identity, on the other hand, refers to the more verifiable aspects of an individual's identity. This includes name, date of birth, ID numbers, biometrics, and other personal data that can be documented, verified, and, crucially, digitised. In the context of web2 and emerging web3 paradigms, objective identity is what digital

systems, governments, and corporations interact with and utilise. In fact, it has become a token of its own, enabling users' transactions and access to services. It is the aspect of identity that can be and has been monetised, protected, and, unfortunately, stolen.

Integrating Subjective and Objective Identity

In the rapid digitalisation of our economy and day-to-day life, the line between subjective identity and objective identity is blurred. ParallelChain recognises the importance of bridging these two aspects of identity, particularly in modern digital ecosystems envisioned by initiatives like Soulbound Tokens [1]proposed by Vitalik Buterin.

The Dual Dimensions of Identity in Business Contexts

ParallelChain envisions that in the business realm, the objective and subjective aspects of identity can be complementary while serving distinct purposes. Businesses can leverage the synergy between objective and subjective identities to strengthen regulatory compliance and enhance customer relationships.

Objective identity, encompassing verifiable personal data, is the cornerstone of compliance frameworks like Know Your Customer[2] (KYC). For highly regulated industries such as banking and finance, verifying the objective identity of customers is essential for preventing fraud, money laundering, and other illicit activities. However, the reliance on objective identity alone is not without its challenges. Despite advances in technology, objective identifiers can be falsified, stolen, or duplicated. This vulnerability underscores the need for additional layers of verification and the potential value of incorporating subjective identity data. For instance, subjective identity data can enhance security and combat Sybil attacks[3], where one individual creates multiple identities (fake accounts) to manipulate a system or network. Unlike objective data, subjective experiences and behaviours are difficult to replicate or falsify, making them a potent tool for verifying the authenticity of user interactions.

Contrary to the fixed and formal nature of objective identity, subjective identity encompasses personal preferences, relationships, and experiences. This web3 big data, encompassing users' preferences, hobbies, and online behaviour patterns, is

[1] The concept of soulbound token was first mentioned by Ethereum co-founder Vitalik Buterin in a blog post in January 2022.
[2] Know Your Customer (KYC) is the process of verifying the identity of (new) customers.
[3] Sybil attack is a type of security threat in which an attacker creates multiple fake identities.

invaluable to businesses aiming to understand their customers better and tailor their services accordingly.

An Approach Combining Objective and Subjective Identities

The future of business, particularly in highly regulated sectors, will depend on the ability to seamlessly integrate the different facets of identity into a holistic framework. This integrated approach not only augments the existing objective data, but also transforms the approach to identity verification, making it more intelligent and reflective of the real person behind the profile. This makes it significantly more difficult for malicious actors to create fake identities.

Bridging Online and Offline Identities

ParallelChain advocates for a holistic approach to identity, one that recognises the essence of an individual spans beyond the binary confines of online and offline or subjective and objective data. ParallelChain does not dictate the terms of this integration, but provides the enabling tools and a secure environment for the community to safely explore new identity paradigms. To this end, ParallelChain identifies a unique blend of blockchain and artificial intelligence (AI) technologies, which will be discussed in this paper.

Anti-Spoofing – Biometrics That Speak Truth

Biometrics, such as facial features, fingerprints, and voice, are the de facto identification credential in digital systems. They offer a unique, user-specific key that is inherently more secure than traditional methods such as passwords.

However, the security provided by biometrics, while superior, is not infallible. Sophisticated spoofing[4] techniques, such as synthetic reproductions deepfake videos capable of deceiving even human judgement, present new challenges. While many biometric systems incorporate anti-spoofing measures to combat these threats, these systems mostly rely on 'active liveness detection[5]' which requires users to perform actions like blinking or head-turning to prove their presence. Such an approach not only works at the expense of user experience, but it gives the users an illusion of safety while the reality is the opposite—these systems are easily spoofed.

In response, ParallelChain has developed an advanced passive anti-spoofing face verification system. This system integrates a suite of AI models capable of *passively*

[4] Spoofing is a type of presentation attack aimed at bypassing security.
[5] Active liveness detection is an anti-spoofing method that requires end-users' active interaction, such as by opening their mouth or turning their head, to prove their physical presence in front of the camera.

distinguishing whether the given input (i.e. the face) is captured in-person or is a 2D (image, video) or 3D (mask) spoof. All this is done without requiring any active interaction from the user.

Moving Beyond Seed Phrases

Currently, web3 interactions largely rely on seed phrases for authentication and account recovery, which is user-unfriendly (hassle to manage) and unreliable (easily lost or stolen). Furthermore, this method ties a user to a specific blockchain and complicates interactions across different ecosystems.

ParallelChain's passive face anti-spoofing user authentication is a novel approach that creates a seamless cross-chain experience. Users' biometrically-verified identity — and/or their biometrically-generated non-fungible token — is generated on ParallelChain Mainnet, serving as a universal key across multiple ecosystems.

However, maintaining user anonymity or pseudonymity presents a challenge when integrating biometric data. Our systems must ensure that biometric authentication does not publicly expose users' on-chain activities to real-world entities unless the user explicitly permits it or when it is required by law.

There are several ways to address this challenge, among which leveraging edge[6] AI and Decentralised Identifiers (DIDs) are particularly notable. Both approaches offer unique benefits: edge AI fully embraces the non-custodial principle and self-sovereignty by processing data directly on the user's device, while DIDs enhance decentralisation and interoperability through standardisation. ParallelChain currently leans towards the former, but remains open to integrating DIDs and other technologies in later phases of ecosystem development.

Edge AI – Identity Management on the Go

Edge AI, which refers to the deployment of AI directly on users' devices rather than in centralised servers, has been a pivotal element in ParallelChain Lab's research & development. In the context of ParallelChain-based identity management, edge AI refers to immediate, on-device processing of biometric data in identity authentication and management when interacting with web3 services, digital wallets, and dapps. For instance, users of a decentralised messaging app want to ensure that they are communicating with the intended person. So, before initiating a chat, users biometrically authenticate each other on the spot through edge AI, and the data does not leave the user's device. Another example is an NFT marketplace that implements

[6] Edge computing refers to the concept of computing as close as possible to where data is created.

edge AI for identity verification. The marketplace can confirm users' or artists' identities locally and securely attach their verified digital signatures to the NFTs to ensure authenticity and ownership.

Challenges remain, particularly around biological twins, device compatibility, regulatory compliance, and data monetisation (the ecosystem may still be inclined towards monetising user data). However, ParallelChain already has the foundational technologies needed to make edge AI identity management a reality, and these technologies continue to evolve rapidly.

Trustless Identity Document Authentication for Web3

Unlike traditional identity systems where identity documents (IDs) are verified by trusted third parties, decentralised platforms demand a trustless system where users can securely prove the authenticity and ownership of IDs. The following points depict the key characteristics of the document verification framework and system to be implemented on ParallelChain Mainnet, purpose-built for addressing the challenges and requirements of decentralised platforms.

Global ID Support

The system supports global passports and more than 100 types of ID documents, catering to a worldwide user base and accommodating the global nature of web3.

Fake Passport / ID Detection

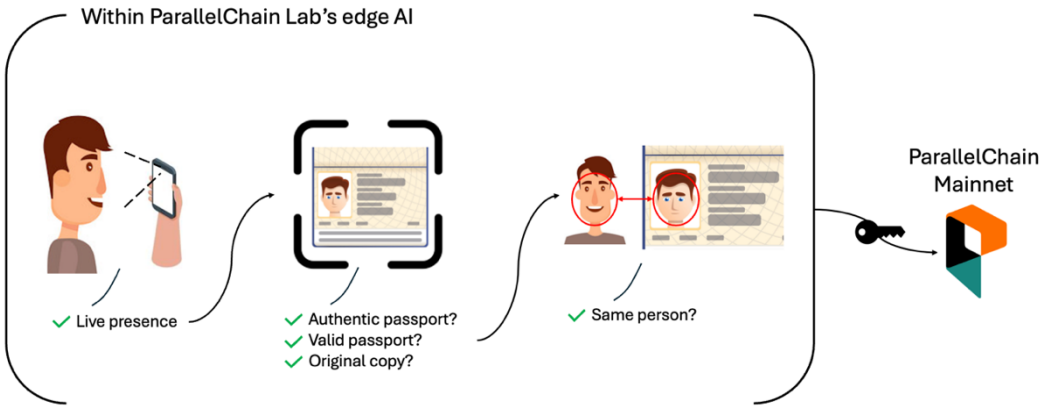
Incorporating advanced detection capabilities for fake passports and IDs is crucial. The system is adept at identifying counterfeit documents, to protect users and platforms from fraudulent activities.

Document Anti-Spoofing

At the core of our system is a state-of-the-art document anti-spoofing model. This model rigorously assesses the legitimacy of IDs to confirm they are authentic, original copies.

Ownership Verification

Extending beyond mere document legitimacy, our system also verifies that the ID belongs to the user through a dual-verification process where the ID photo is compared against the live image of the user.



Decentralised, Privacy-Preserving Verification

A crucial aspect of the system is a decentralised verification process. This allows users to prove the validity of their IDs without revealing their personal information or relying on a single verifying entity. This could involve creating a decentralised network of trusted validators or – our current preference – employing privacy technologies such as Zero-Knowledge Proof (ZKP) and edge AI. For instance, a decentralised exchange (DEX) can determine if a user complies with jurisdictional requirements by receiving a binary response regarding the presence in a restricted jurisdiction – without the DEX ever accessing or learning about the user's actual citizenship.

These characteristics collectively form the backbone of a robust, web3-native document verification framework that aims to achieve both verifiability and user privacy. Furthermore, it balances regulatory compliance and user anonymity when needed.

PRFC Token Standard – The Unbreakable Bond of Identity Tokens

A challenge confronting identity systems today is their capacity to honour the complexity and fluidity of subjective identity. This demands a nuanced approach, one that encapsulates the richness of human experience without compromising privacy or security. ParallelChain's goal is to provide solutions grounded in frameworks that emphasise the multifaceted nature of individuals, combining their daily experiences and interactions with verifiable attributes.

Drawing inspiration from the visionary concept of Soulbound Tokens, ParallelChain has embarked on developing an identity-focused PRFC [7] token standard for ParallelChain Mainnet. This token standard is designed to encapsulate both objective data (such as biometric information, legal identification numbers, and official documents) and subjective attributes (including personal achievements, social affiliations, and interaction histories). This dual representation ensures a comprehensive digital identity that remains true to the user's real-world persona, shifting from static, one-dimensional identifiers to dynamic, multi-dimensional tokens that reflect the real-world complexity of individual identities.

Five principles central to the PRFC identity token standard are:

- *Security*: protection against attacks such as deepfakes, replay, forgery, etc.
- *Privacy and verifiability*: data minimisation and user consent
- *Representation*: user's right to self-representation and autonomy over choosing what to share and with whom
- *Updateability*: allowing for addition and modification while maintaining the historical integrity and authenticity of the token
- *Interoperability*: an identity that can seamlessly interact with various platforms, whether they are based on web2 architectures or web3 frameworks

Zero-Knowledge Proof (ZKP): The Art Of Sharing Nothing

As mentioned, ParallelChain aims to empower the paradigm shift from the traditional trust-based identity verification relying on attestations by trusted third parties, to cryptographic methods that offer definitive proof while maintaining user privacy. Central to this transformation is the implementation of Zero-Knowledge Proof[8] (ZKP).

In the context of ParallelChain, ZKP offers an ideal solution for creating a trustless system of identity verification that respects user privacy. It allows one party (the prover) to prove to another party (the verifier) that a certain identity attribute — such as age or nationality — is true, without revealing any information beyond the validity of the statement itself. In practice, ZKP within ParallelChain Mainnet can be applied in various scenarios. For instance, users can prove that they are above 18 years old to access certain decentralised finance (DeFi) services without revealing their birth date; individuals can prove that they graduated from an institution

[7] PRFC stands for ParallelChain Request for Comments, which defines a set of rules for how the tokens of a particular token standard should be created, issued, and deployed.
[8] Zero-Knowledge Proof is a method by which one party can prove to another party that a given statement is true, without conveying to the verifier any information beyond the mere fact of the statement's truth.

without sharing their education certificate which contains irrelevant private information; users can prove that they are not from a restricted jurisdiction without disclosing their citizenship.

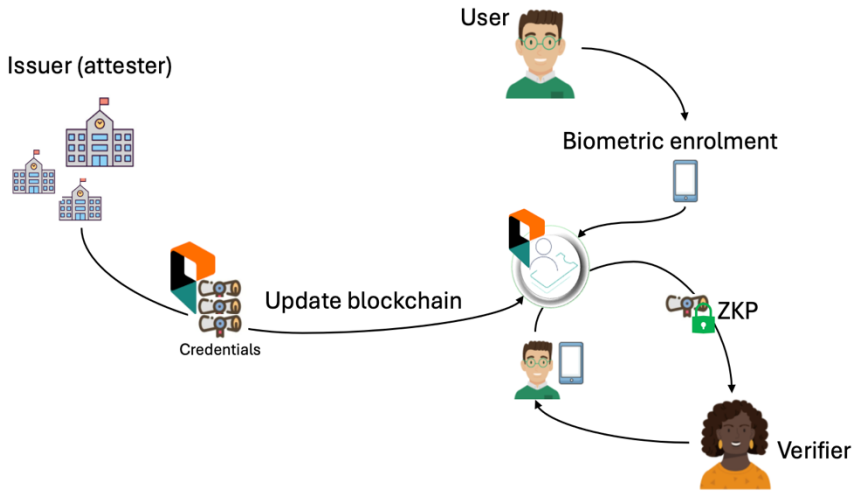
ParallelChain is committed to advancing the field of ZKP and focusing efforts on various ZKP frameworks to facilitate different use cases and performance requirements, including zk-STARKs, which is well-suited for scalable operations where numerous identity verifications can occur simultaneously.

Issuance and Verification of Identity and Credentials on ParallelChain

The following points describe the intended approach to the backbone of ParallelChain's identity infrastructure: issuance and verification of identity and credentials.

Creation of Identity – A Biometrically-Tied Identity Token

The user begins by enrolling his biometrics through a mobile application. Upon successful biometric enrolment, a non-fungible PRFC identity token anchored to the biometric data is generated on ParallelChain Mainnet. The token provides a secure and portable means of identity verification across various applications on ParallelChain, and other platforms in the future.



Issuance of Credentials

A credential issuer, such as an education institution, digitally signs, thus attesting to, the attributes associated with an individual, creating what is known as PRFC credential tokens on ParallelChain Mainnet. Verifiers, such as an employer who

wants to validate whether a candidate completed a Bachelor's degree in Computer Science from a specific university in 2023, can verify an individual's credentials by accessing the cryptographically hashed versions of the credentials.

Integration of Credentials into Digital Identity

Once a user's identity is established, they can integrate credentials into their 'profiles' on ParallelChain. Recognising that different scenarios may require different verification solutions, ParallelChain facilitates various approaches.

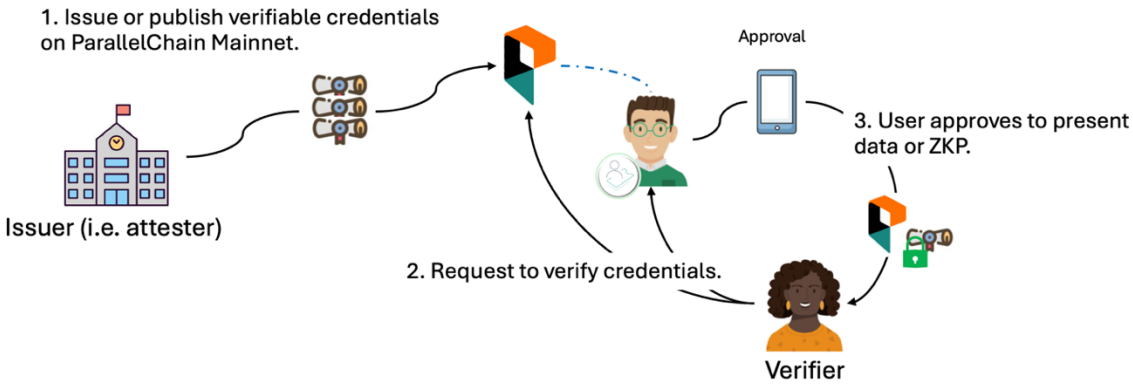
One approach is to issue *PRFC credential tokens* representing specific attributes, which are then stored in the user's identity wallet (i.e. profile). This method allows for a flexible and modular system where new credentials can be added or revoked easily. This approach is also well-suited for applications where users are likely to accumulate a range of credentials over time, such as certifications in continuous education or professional development. The ability to issue distinct credential tokens on ParallelChain makes it easier for users to manage specific credentials as needed.

Another approach entails *updating the PRFC identity token* to reflect new credentials and verifications. This involves modifying the token's data to include new attributes or proof of certain qualifications. This framework is more suited for static attributes that are expected to remain constant, such as date of birth. Another scenario where this framework is advantageous involves tracking and verifying changes over time, where the history of changes is critical. For instance, the history of a user's passport numbers, including both expired and current numbers, can be crucial for Anti-Money Laundering (AML) purposes.

Verification of Credentials

When an individual needs to prove the validity of certain ParallelChain-based credentials to a verifier, the verifier can use ZKPs to verify the credentials. For instance, if an individual wants to assert their active full-time employment status, they can generate ZKPs of the relevant attributes without revealing excessive information such as job position, salary value, etc.

ParallelChain recognises the need for diverse use cases and confidentiality requirements. This is why ParallelChain allows for various verification pathways: directly between the verifier and the credential owner (i.e. the entity being verified), and indirectly between the verifier and the credential issuer (i.e. attester).



XPLL – ParallelChain's Native Token

XPLL, the utility token native to ParallelChain, plays a multifaceted role within the identity ecosystem, extending beyond transaction facilitation to encompass monetisation of own identity, governance of the system, and incentivisation.

Transaction Fees for Credential Issuance and Verification

XPLL is used to facilitate transaction fees on ParallelChain Mainnet, in the context of this paper, it facilitates operations related to the creation and update of identities as well as the issuance and verification of credentials. Whenever a user's identity needs to be verified or a new credential is issued, XPLL is utilised to compensate for the computational resources required for these processes. This ensures that the network remains efficient and secure, while also incentivising participation and proper resource allocation by the nodes supporting the network.

Identity Monetisation and Access to Premium Features

XPLL can act as a key to unlocking premium services and features within the platform, this can include advanced verification, additional privacy protection, or priority processing. While the PRFC identity token functions as a digital 'passport' for users to access applications on ParallelChain, XPLL facilitates nuanced transactions, such as permissions for accessing (verifying) identity data.

This setup introduces a dynamic and user-centric model for identity management and monetisation, enabling users not just to determine the terms under which their identity data is accessed and used, but also to benefit from its value. It marks a shift away from traditional models, where large corporations profit extensively from user data, ParallelChain aims to redistribute the value derived from personal data, ensuring that individuals receive their fair share of their data contribution in the digital economy.

Incentivisation and Reward Mechanisms

The ParallelChain ecosystem leverages XPLL to incentivise positive behaviours and contributions, such as participating in network security through operating a node or contributing to community governance. For credential verifiers and issuers, XPLL can also serve as a reward for maintaining high standards of accuracy and reliability, thus ensuring the overall trustworthiness of the identity system.

Governance and Decentralised Decision-Making

XPLL is instrumental in the governance of the ParallelChain ecosystem, holders can participate in decision-making processes, influencing the development and operational aspects of the identity system. This includes voting on updates, policy changes, and the integration of new features or technologies, ensuring that the development and evolution of the identity system reflect the collective interest of the community — the users.

Interoperability, Connecting ParallelChain to the Worlds

It is extremely important that the identity systems developed on ParallelChain Mainnet can interact with other systems. This principle ensures that ParallelChain-based credentials transcend boundaries, enabling users to leverage a single, unified identity across different environments, and empowering ParallelChain-based identities to be universally recognised and utilised. This section outlines the various approaches ParallelChain plans to explore to achieve this vision.

Bridges

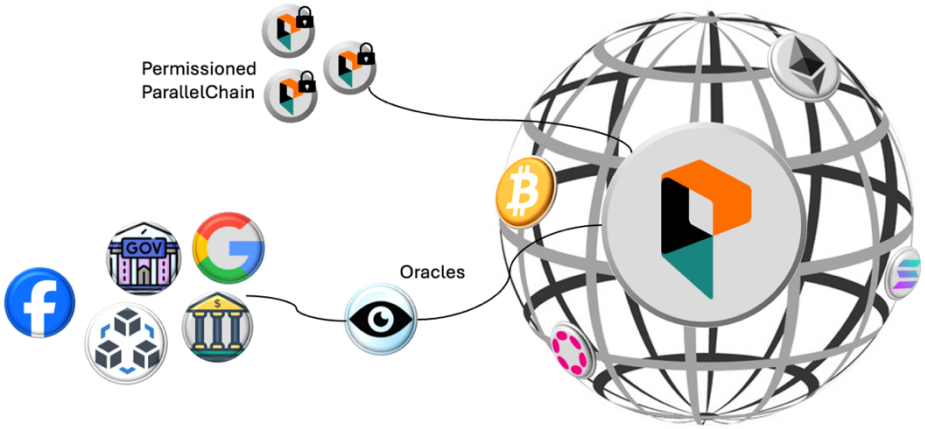
Blockchain bridges serve as connectors that allow the transfer of information and assets between different ecosystems. The types of bridges vary in their design, functionality, and purpose, serving different use cases, such as cross-chain data verification, asset liquidity and portability, etc. In ParallelChain's context, bridges

aim to i) facilitate the recognition and validation of ParallelChain-based identities on external blockchain networks, and ii) enrich ParallelChain-based identities.

For instance, Alice owns an identity on ParallelChain and wants to update or add environmental-related credentials for her contribution to a tree-planting initiative that ran on Ethereum. These credentials exist on Ethereum. Alice generates ZKPs for her credentials, and the bridge communicates her proofs to the ParallelChain-based credential issuance platform. The platform, in turn, verifies the authenticity of the proofs against its subset requirements.

Oracle Protocols

Blockchain oracle protocols act like messengers that gather and check information from data providers, including a wide range of blockchain networks — including permissioned ParallelChain which serves applications that have specific regulatory or organisational requirements to follow, and off-chain sources such as APIs, the internet, government databases, etc. In ParallelChain's context, oracle protocols have three main purposes: to collect important external data needed for a more comprehensive check of someone's identity; to enable smart contracts on ParallelChain to respond to events happening in the real world; and to allow external systems to use ParallelChain's verification services.



Real-World Applications and Impact

The identity infrastructure powered by ParallelChain has far-reaching implications across sectors. In certain sectors, complete user anonymity or ZKP-based verification may not be commercially desired or does not align with regulatory compliance requirements. The composability of the PRFC identity token standard allows for the

development of purpose-built applications, catering to the nuanced demands of such use cases.

The points below explore the tangible impacts and real-world applications of the identity solutions to be built on ParallelChain.

Enhanced Onboarding and KYC for Web2

Web2 service onboarding and KYC processes are known to be slow and cumbersome, relying on manual checks and data entry, leading to high user drop-off rates. The necessity for repeated processes across different platforms exacerbates user frustration.

By using ParallelChain's interoperable identity system integrated with automated verification and passive anti-spoofing security measures, onboarding time and friction are significantly reduced, minimising user drop-off rates and enhancing user satisfaction.

Crypto and Digital Assets Banking

Traditional financial institutions struggle to integrate cryptocurrency and digital assets services due to the complexity of bridging blockchain and traditional banking systems and ensuring compliance across diverse asset types.

ParallelChain enables seamless integration of crypto and traditional banking services by providing a unified identity framework. With PRFC identity tokens, banks can link customers' online and offline identities and monitor transactions across asset types to facilitate fraud prevention and regulatory compliance.

For instance, Alice wishes to invest in digital assets through her bank account. Using ParallelChain, the bank can seamlessly link Alice's existing profile with her ParallelChain digital wallet, allowing her transactions, across both fiat and crypto, to be monitored consistently under one identity framework, ensuring compliance and security without hindering her user experience.

Decentralised Finance (DeFi) Compliance

DeFi platforms operate in a regulatory grey area, lacking clear KYC and anti-money laundering (AML) frameworks. This exposes them to potential regulatory penalties and undermines user trust.

ParallelChain prepares DeFi platforms for this eventuality by equipping them with tools for regulatory compliance, particularly KYC, without compromising the ethos of decentralisation.

For instance, a DEX facing regulatory requirements to implement KYC can leverage ParallelChain's identity verification mechanisms to enable users to prove their identity through ZKP-based verification. This ensures privacy and security while meeting regulatory requirements, all within a decentralised framework.

Decentralised Social Media

Current decentralised social media platforms face challenges in establishing user trust and accountability without infringing on privacy.

By implementing ParallelChain's identity solutions, accounts with identity tokens attached can be ZKP-verified to confirm authenticity without revealing personal information. As a result, decentralised social media platforms can reduce spam, fake profiles, and malicious activities. This enhances user trust and safety and allows for verified but anonymous interactions and content sharing.

Healthcare

The healthcare sector struggles with fragmented data systems, leading to inefficiencies and privacy concerns during patient data exchange between medical service providers.

ParallelChain's secure and interoperable identity tokens allow for controlled and consent-based sharing of health records between medical service providers. Furthermore, edge AI ensures that sensitive data processing occurs locally on devices, enhancing data security and patient privacy.

E-Government and Public Services

Public services typically suffer from inefficiencies and data silos within various departments and agencies. This leads to a disjointed experience for citizens, who find themselves navigating a labyrinth of bureaucracy, repeatedly submitting the same information and documents for different services. This redundancy not only burdens users but also contributes to further data inconsistencies.

By tokenising citizen identity on ParallelChain, authorities establish an identity system where citizens can prove their eligibility for services or benefits without going through repetitive processes. The benefits extend to private sector interactions. For instance, senior citizens can prove their eligibility for elderly discounts without disclosing specific personal information such as their exact age or identity details.

Background Checks

Current methods for performing background checks and verifying educational credentials are slow, manual, and rely heavily on verification services provided by

agencies. Furthermore, these processes require sharing sensitive personal information with third parties, raising data privacy and security concerns.

Through the use of cryptographic techniques, specifically ZKPs, ParallelChain enables verification to occur directly between the individual and the requesting party (e.g. an employer or another educational institution) without sharing more than what is necessary. In addition, ParallelChain offers a comprehensive platform for different verifications, from employment history to educational credentials.

These real-world applications illustrate ParallelChain's role in transforming how trust is formed, assured, and experienced. As regulatory landscapes evolve and digital interactions become increasingly central to our lives, the importance of such advanced identity solutions will only continue to grow.

Conclusion

ParallelChain's endeavour to construct this identity infrastructure is a collective journey. It requires the active involvement and collaboration of all stakeholders of the ecosystem, innovators, developers, policymakers, and users alike. The path laid out by ParallelChain underscores the vital importance of open standards, user engagement, and collaborative innovation in crafting an inclusive, effective, and respectful identity system. This paper serves as a clarion call to join forces, as our vision can only be realised through the concerted efforts of all of us working towards a common goal.