SOULVERSE

BIOMETRIC-BASED SECURE AND INTEROPERABLE SSID FOR MULTI-INDUSTRY APPLICATIONS

SHARANSH GUHA,
SOULVERSE INC

DEHRADUN,UK
MICHIGAN, USA

Table of Content

01. ABSTRACT

The essential building block of many ground-breaking applications is blockchain technology, which calls for Distributed Ledgers that are reliable and immutable and are governed by a number of authorized parties. These applications include edge/fog-enabled intelligent systems including eHealth, IIoT, and IoV, as well as cryptocurrencies, smart contracts, Self Sovereign Identity (SSI), and IoV. Researchers are paying close attention to the open-source tools Hyperledger Indy and Aries, which are supported by the Linux Foundation and have become viable solutions for integrating permissioned blockchains in SSI programmes. Some SSI applications, however, have a predetermined maximum reaction time that is in line with their business models. To meet this need, we suggest a decentralized authentication framework built on an Aries-based decentralized identity (DID) built on the permissioned blockchain of Hyperledger Indy. Also included in our strategy is private distributed storage that has been designed particularly for the SSID application.

By implementing our solution, users can authenticate and authorize themselves across multiple applications within our ecosystem without the need to repeatedly enter their credentials. This identity management solution empowers users to selectively share their identity attributes with designated service providers to access their respective services.

This whitepaper provides a ground-breaking technique for creating an interoperable Secure Service Identifier (SSID) across many chains while avoiding the requirement for mnemonic-based private keys. This new solution, which uses biometric authentication, produces the same unique PPL pair with each biometric scan, offering better security and user convenience. In order to accomplish this, Soulverse is researching and developing vital proprietary technologies using a biometric-first approach to construct an SSID infrastructure that is decentralized end-to-end, instrument independent, and super portable.

This infrastructure will be open source, allowing any Web3 product or service firm to build cost-effective and lightweight solutions. The proposed SSID has enormous promise for industries such as education, healthcare, e-commerce, tourism, and employment, since it would revolutionize how users access and interact with numerous platforms in a safe and user-friendly manner.

02. INTRODUCTION

The essential building block of many ground-breaking applications is blockchain technology, which calls for Distributed Ledgers that are reliable and immutable and are governed by a number of authorized parties. These applications include edge/fog-enabled intelligent systems including eHealth, IIoT, and IoV, as well as cryptocurrencies, smart contracts, Self Sovereign Identity (SSI). Researchers are paying close attention to the open-source tools Hyperledger Indy and Aries, which are supported by the Linux Foundation and have become viable solutions for integrating permissioned blockchains in SSI programmes. Some SSI applications, however, have a predetermined maximum reaction time that is in line with their business models. To meet this need, we suggest a decentralized authentication framework built on an Aries-based decentralized identity (DID) built on the permissioned blockchain of Hyperledger Indy. Also included in our strategy is private distributed storage that has been designed particularly for the SSID application. By implementing our solution, users can authenticate and authorize themselves across multiple applications within our ecosystem without the need to repeatedly enter their credentials. This identity management solution empowers users to selectively share their identity attributes with designated service providers to access their respective services.

Traditional internet apps frequently lack a strong identity layer, depending on usernames and passwords that are context-specific and vulnerable to security vulnerabilities such as identity theft. While global identity providers strive to improve accessibility, worries about data leaks and loss of control over private data kept on centralized systems continue. These problems are addressed by self-sovereign identification (SSI) principles, which allow users to anonymously identify themselves, verify private qualities, and retain control over their data.
While permissioned blockchains provide high levels of security and trust, they might be slower than centralized alternatives. Due to system features and limits like consensus time, transmission delays, network capacity, and miner connectivity, different permissioned blockchain implementations display differing latency measurements. As a result, academics

and practitioners encounter difficulties in determining the best blockchain architecture for their applications, demanding considerable testing and assessment.

It is critical to develop systems that are owned directly by the device owners themselves in ecosystems that demand scalable, robust, lightweight, and secure Identity and Access Management (IAM) solutions to preserve the privacy of user-data. These systems are made possible by combining consortium or public blockchains with a Self-Sovereign Identity concept (SSI).

We plan to offer a Blockchain-based IAM system that uses the SSI model to provide users with ledger-rooted IDs. Furthermore, it delves into an important aspect of blockchain technology: interoperability.

In this regard, we are focusing on developing a deployment architecture for SSI applications using Hyperledger Indy, a permissioned blockchain, and Aries.

We want to overcome latency problems and provide a scalable as well as effective solution for SSI applications by using these open-source technologies and integrating them with public ledgers like Polygon initially and expanding support to other networks eventually.

We aim to contribute to the progress of SSI applications and create a stable and efficient blockchain architecture that satisfies the needs of real-world deployments by building on the capabilities of Hyperledger Indy and supporting multiple networks/ ledgers.

03. PROBLEM

Challenges of Centralized Identity Management in the Digital World

I. Introduction

In the digital era, centralized identity solutions managed by central agencies or governments present significant challenges. This section discusses the critical issues arising from the authority these centralized entities hold over identity management.

II. Loss of Data and Digital History

- **Central Authority Control:** The centralized nature of identity management allows authorities to reject or invalidate verifiable credentials (VC), resulting in the loss of linked data. This can have severe consequences on an individual's digital history and records.

III. Dependence on Central Authorities

- **Limited Control:** Relying on central agencies for identity verification leaves individuals with limited control over their own data and digital identities.
- **Potential Bias:** Centralized control introduces the risk of biased decisions based on the authority's preferences or policies, leading to unequal treatment of individuals.

IV. Impact on Privacy and Security

- **Data Breach Vulnerability:** Centralized storage of sensitive identity information makes it an attractive target for hackers, increasing the risk of data breaches and identity theft.
- **Single Point of Failure:** If the central identity system experiences a technical failure or cyberattack, it can disrupt access to services for a large number of individuals.

V. Lack of Transparency and Trust

- **Opacity in Decision-making:** The decision-making processes of central authorities may lack transparency, leaving individuals uncertain about the criteria used to validate or reject credentials.

- **Reduced Trust:** Loss of trust in the identity system may occur when individuals perceive arbitrary decisions or lack of accountability from the central authority.

VI. Inefficiency and Delays

- **Time-Consuming Verification:** Centralized identity verification processes may involve time-consuming manual checks, leading to delays in accessing services or opportunities.
- **Redundant Data Requests:** Different entities relying on the same centralized system may request redundant information, leading to duplication and inefficiency.

VII. Potential for Misuse of Data

- **Surveillance Concerns:** Centralized identity databases hold vast amounts of personal data, raising concerns about potential surveillance and misuse of this information.
- **Data Monetization:** Centralized entities may profit from selling individuals' data without their knowledge or consent, raising ethical and privacy concerns.

VIII. Lack of Interoperability

- **Fragmented Systems:** Centralized identity systems may lack interoperability with other platforms or services, leading to a fragmented user experience.
- **Limited Accessibility:** Individuals who are part of multiple systems may face challenges accessing services across different platforms due to the lack of integration.

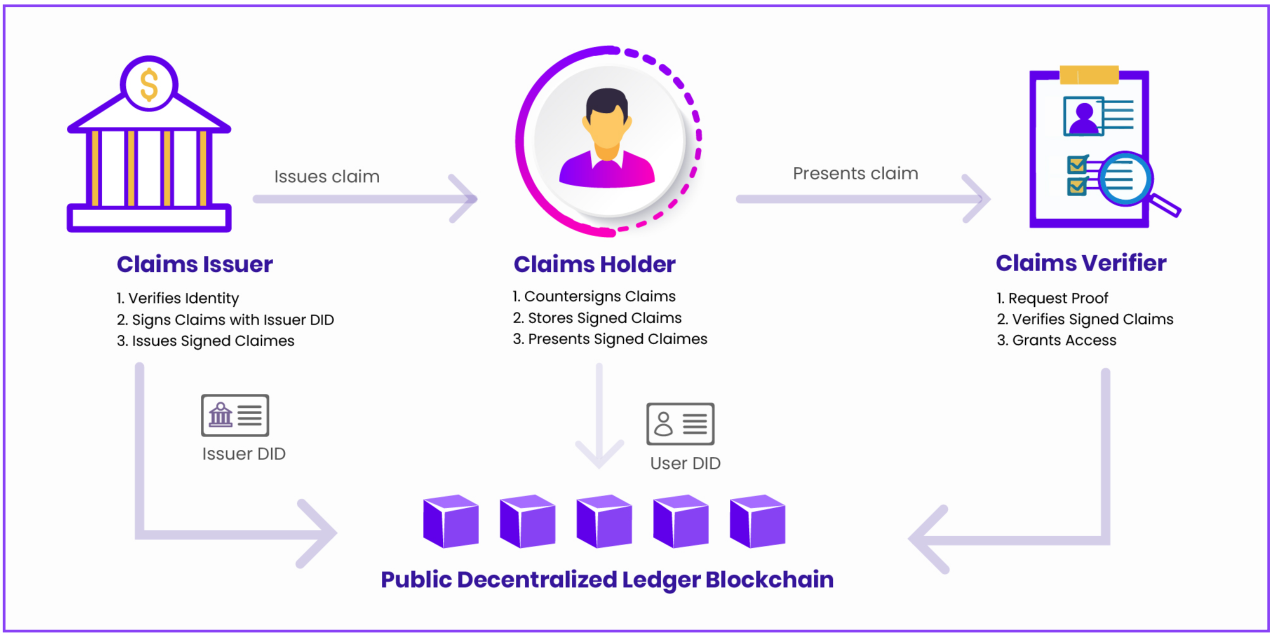
IX. Conclusion

Centralized identity management, controlled by central agencies or governments, brings forth several critical challenges in today's digital world. These issues encompass data loss, limited user control, privacy and security risks, lack of transparency and trust, inefficiency, potential data misuse, and problems with interoperability. Addressing these challenges is crucial to ensuring a secure, transparent, and user-centric approach to identity management that fosters trust and empowers individuals in the digital age.

04. SOLUTION

Self-Sovereign Identity (SSI) is a digital identifying strategy that allows individuals to take ownership of their personal data by deciding when, how, and with whom they disclose it. SSI permits the construction of “digital identity proofs” or presentations based on the individual’s personal identification traits.

Three main players are involved in the SSI schema as depicted below:



Issuer: The issuer delivers verified credentials comprising the user’s identifying characteristics. These credentials are created and signed by them.

Holder: The holder is in charge of maintaining and controlling their own credentials locally.

Verifier: The verifier must recognize and validate the user’s characteristics using verified credentials supplied by trustworthy issuers. The verifier is not required to keep any user data and is just required to validate the information. This verification is dependent on the verifier confirming the holder’s submitted credentials proof, which includes confirmed assertions. This attestation may divulge credential claim values or be a private attestation based on Zero Knowledge Proofs (ZKPs) depending on the needs.

It should be noted that the holder requires computational power, storage capacity, and communication. These features enable the holder to deliver verifiable evidence, securely store identify credentials, and engage with other system actors.

“Privacy is a shield from harm, a weapon against tyranny and an ally in struggle.”

An SSI solution includes the following components:

Credential : It is a digital certificate that provides information about the holder’s identification. The issuer is the one who issued it.
Wallet: A safe storage system for the holder’s credentials. The holder must be able to access the credentials saved in the wallet. All actors utilize the wallet to perform cryptographic operations.
Presentation: A digital proof supplied with the verifier by the holder to prove particular aspects of the holder’s identity depending on the credentials obtained.

Digital signatures are generated using algorithms for signing data so a recipient can irrefutably confirm the data was signed by a particular public key holder as the verifier is not always associated with the issuer. A private key is used in a signature algorithm to attach a digital signature to specified material. The related public key can be used to validate the signature. In the context of SSI, digital signature is used by the issuer to create verifiable credentials and by the holder to provide verifiable presentations. It is necessary to know the public keys associated with issuers and holders. While centralized databases can hold these public keys, there are worries about their integrity and availability because a third party might manipulate the keys and there could be single points of failure. Furthermore, the centralized database’s operator would have visibility into all relationships between different subjects.

The solution we propose addresses these difficulties by utilizing unique biometric technologies. This system produces a private-public key pair for each unique user upon their Soulverse application sign-in, eliminating the need to store Keys on centralized or decentralized storage. We employ Soul-ID or Decentralized Identifiers (DIDs) as unique and worldwide identifiers for persons or things participating in the process in our SSID solution. Each DID has a DID Document that defines its attributes, such as the associated public key or service endpoints for communicating with the specific DID. These components minimize the need for unneeded third-party identity suppliers, lowering security risks dramatically.
We will be utilizing Hyperledger Indy, a distributed ledger designed for decentralized identities. Our Network would be a permissioned public blockchain. It implies that everyone may utilize the blockchain, but only authorized entities can run validator nodes.

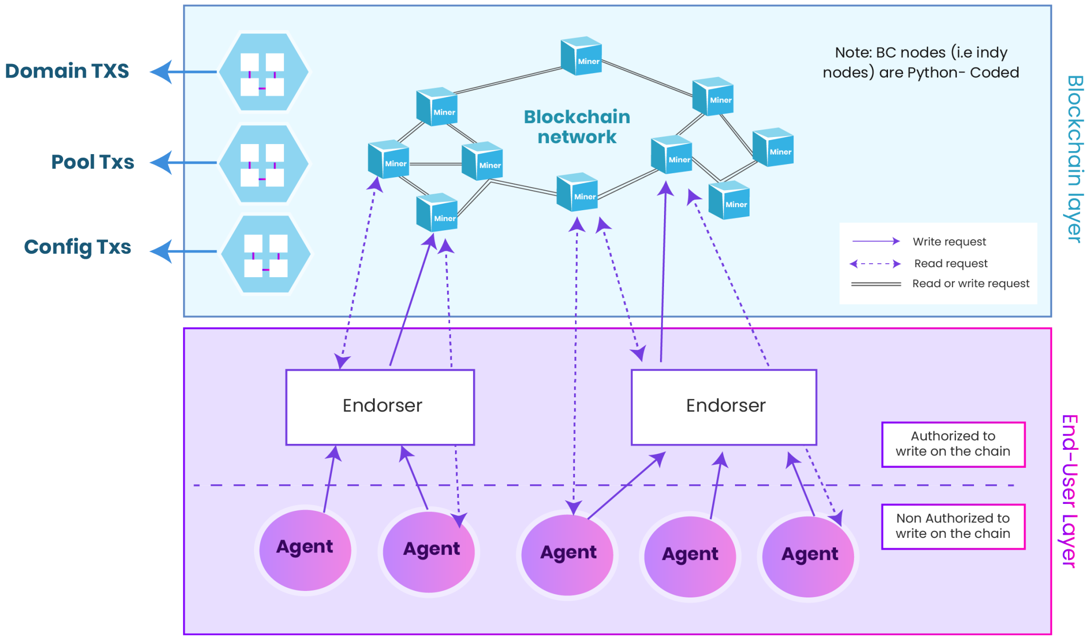
They will eventually be private, in which only selected entities may participate, as in the IBM Food Trust implementation, and permissionless, in which anybody can function as the miner validator, as in bitcoin. Contributions to the Hyperledger Indy project, which gave birth to Hyperledger Ursa and Hyperledger Aries, are critical to our design. Hyperledger Ursa is the standard cryptographic library used by all Hyperledger projects that implement cryptographic protocols like CLRSA signatures. The Hyperledger Aries protocol is used for peer-to-peer connections, wallets, communications, and key management.

We are also working on a super wallet that will allow users to store their identities (Soul-ID), all digital assets (cryptocurrencies and NFTs), and FIAT in a single location. This will be a one-stop shop for all wallet requirements. Furthermore, the Soul ID wallet will be multi-ledger interoperable, allowing users to interact with different ledgers for transactions such as identity verification, credential receipt, cryptocurrency payment, and receiving assets.

The suggested system will be a major advance over existing systems as it will be based on the AFJ protocol and will initially communicate with the Polygon ledger. Eventually a wrapper will be added to make the transactions ledger interoperable with other ledgers.

4.1 Proposed Architecture and Method

We will develop a validation architecture for deploying Indy and Aries nodes. Our approach involves an Aries agent capable of connecting to an Indy network and generating sample data (TXs) for submission. Initially, we extracted code from the Indy-SDK repository, implemented in Rust. To optimize system processing speeds, our agent utilizes a multi-threaded approach. The transactions will adhere to standard formats generated by an Aries agent, but we have developed our own agent since the existing codes in the official Aries repository only support 20 TXs/second.



For running Indy nodes on separate machines, we will design Indy node scripts suitable for individual deployment. The available modules in the official Indy repository run four nodes on a single machine, which is not production-ready. To facilitate network control by different administrators, we will incorporate Admin UI, configured to connect with the created Indy network.

All the application components we have implemented will be containerized using Docker, ensuring easy deployment for current and future projects.

All nodes will be deployed and run individually on separate virtual machines located in various regions of the Cloud Platform. Documents or Digital certificates issued are stored on distributed servers after approval from appropriate VCs.

Some key features of our solution are as follows :

4.2 SoulScan

Our own patented Biometric Scan technology offers consistent and reliable biometric scan outputs for each individual, independent of variable ambient elements like lighting, facial expressions, accessories, or age.

By utilizing advanced algorithms and procedures that enable robust and reliable biometric identification, our Biometric Scan technology overcomes these restrictions.

We are working on a method that successfully accounts for the effects of lighting conditions, facial expressions, accessories, and age differences, guaranteeing that the final biometric scan

4.3 Soul ID

Soul-ID is a one-of-a-kind identification for an entity that is not under the jurisdiction of a single entity. Individuals and organizations will be able to govern their own digital identities without relying on centralized authority.

Soul-IDs are used to identify and link network users. Each user has a unique DID that is used to establish a secure connection between their device and the network. The W3C Verifiable Credentials (VC) standard serves as the foundation for Soul-IDs.

4.4 $SoulX

The SoulX coin includes an incentive to trade digital credentials while maintaining anonymity. The SoulX token is intended to transform the Soulverse into a digital marketplace for trust by allowing digital value transfer to occur directly in-line with the exchange of verified claims and by adopting the same privacy-preserving zero-knowledge proof method.

A worldwide public utility for Self-Sovereign Identity will open up the digital credential market, creating a virtuous cycle of issuers competing on credential quality and cost. The value of verified claims may now flow directly from verifiers to issuers—or indirectly from verifiers through owners to issuers—every time a claim is traded, thanks to the SoulX token and our SSID solution.

4.5 Super Wallet

The Soul Wallet application would be a blockchain-based decentralized application (DApp). The wallet would be able to hold both self-sovereign identity (Soul-ID) and all crypto assets such as Bitcoin, Ethers, and NFTs. Furthermore, depending on the location, the wallet would be able to hold fiat currencies like USD, EUR, & GBP.

The super wallet application would be a valuable tool for users who want to manage their digital assets in a secure and decentralized way. The wallet would also be a convenient way for users to store their identity information and to use their crypto assets to make payments.

4.6 Soulogram

Eventually we will build an interoperable ecosystem where a Soulogram would be a digital avatar or embodiment of a person in virtual settings such as gaming platforms, social networking platforms, or metaverses. It functions as a customisable virtual character that users may create to look like themselves or entirely different depending on their preferences.

05. MILESTONES

5.1 PoC

In the first phase, we are planning a PoC utilizing 3rd party services for Biometric authentication, open source libraries to generate wallets, decentralized storage for document storage.

5.2 Token Launch

We plan to launch our native Token, SoulX, on Polygon.

5.3 Beta Launch

Here we plan to launch our patented Biometric scan technology and integrate it with our frameworks to support all devices with a targeted product for the Ed-Tech industry where digital certificates are issued on Chain and all other achievements of students are tracked for the future employers.

5.4 Product Launch in the Market

This will help us onboard more users through institutional partnerships and test our Product to Market fit.

5.5 Product Development and Model Training

Here we plan to train and improve the analytics engine for our patented Biometric scan technology to support human growth & change in facial features in order to still return the same vector.

Also, we plan to develop customized products for different target industries and improve the performance of the product to support more features.

06. USE CASES IN TARGET INDUSTRIES

Our SSID solution has the ability to address a number of existing issues in a variety of businesses. Here are few sectors where our SSID can make a major difference:

- **Ed-Tech :** According to the Identity Theft Resource Center (ITRC), there were 1,033 data breaches in the Ed-Tech industry in 2021, exposing the personal information of over 38 million students. The average cost of a data breach in Ed-Tech is $3.8 million. The SSID can improve security in the realm of education technology by guaranteeing that only authorized users can access educational platforms, course materials, exams, and virtual classrooms. It makes the authentication process easier for students, instructors, and administrators by removing the need for complicated passwords or numerous logins. Biometric SSID might also enable digital certifications to be generated on chain and monitor all program/course achievements on the unchangeable blockchain.

- **Healthcare :** According to the Health Information Trust Alliance (HITRUST), there were 453 data breaches in healthcare in 2021 alone, exposing the personal information of over 46 million patients. The average cost of a data breach in healthcare is $8.64 million. The SSID solution can help the healthcare industry increase security and privacy while accessing medical data, telemedicine services, and health-related platforms. Biometric authentication ensures the security of patient data, lowering the danger of unauthorized access and identity theft.

- **E-commerce :** According to the Identity Theft Resource Center (ITRC), there were 1,473 data breaches in the e-commerce industry in 2021, exposing the personal information of over 140 million customers. The average cost of a data breach in e-commerce is $3.9 million. Using the SSID, e-commerce systems may improve user security and convenience. Without the inconvenience of passwords, users may safely access their accounts, make transactions, and manage their personal information. This technology decreases the danger of fraudulent activity while still providing a consistent user experience.

- **Tourism :** According to the Ponemon Institute, the average cost of a data breach in the tourism industry is $3.8 million. The number of data breaches in the tourism industry has increased by 40% since 2018. The SSID can improve the travel experience by securely allowing travelers to plan transportation, book lodgings, and participate in tourism-related activities. It does away with the need for several registrations and passwords, allowing consumers to access a variety of tourism services with a single biometric scan.

- **Employment :** According to the Identity Theft Resource Center (ITRC), the average cost of a data breach in the employment industry is $3.7 million. The number of data breaches in the employment industry has increased by 30% since 2018. The SSID has the potential to revolutionize the recruiting process by enabling job searchers with safe and convenient authentication. It enables users to securely access job portals, submit applications, and authenticate their identities throughout the recruiting process, increasing efficiency and lowering the risk of unauthorized access.

- **Financial Services :** According to the Identity Theft Resource Center (ITRC), the average cost of a data breach in the financial services industry is $8.64 million. The number of data breaches in the financial services industry has increased by 50% since 2018. The SSID solution helps handle financial industry security challenges. Without the need of passwords, users may safely access their bank accounts, conduct transactions, and communicate with numerous financial platforms. Biometric authentication provides customers with an additional degree of security and convenience.

- **Government Services :** According to the Identity Theft Resource Center (ITRC), the average cost of a data breach in the government sector is $4.3 million. The number of data breaches in the government sector has increased by 30% since 2018. The SSID solution may be used by government entities to improve security and expedite access to public services. Citizens can safely access government systems, validate their identities, and use numerous services thanks to biometric authentication.

Overall, the biometric-based SSID solution may solve security, convenience, and user experience inadequacies in a variety of industries, including education, healthcare, e-commerce, tourism, employment, financial services, and government services.

07. BENEFITS & ADVANTAGES

The biometric-based SSID solution has various benefits and advantages, making it an appealing option for safe and seamless authentication. Here are the important benefits in detail:

1. Enhanced Security : When compared to traditional mnemonic-based private keys or passwords, biometric-based private key creation greatly improves security. Biometric data, such as fingerprints or facial recognition, is unique to each individual and difficult to copy, lowering the risk of unauthorized access, identity theft, and fraudulent activity. This strong security mechanism guarantees that only the authorized user has access to their SSID, offering more safety for sensitive data and transactions.

2. User Convenience : The biometric-based SSID eliminates the need for users to remember difficult passwords or mnemonic phrases. Instead, users may use a simple and familiar biometric scan, such as a fingerprint or face recognition, to verify their identity. This passwordless strategy improves user ease by eliminating the stress of remembering numerous credentials and lowering the danger of forgotten or hacked passwords. With a single biometric scan, users may access many platforms and services, enhancing the overall user experience.

3. Single Wallet : Users would profit from the super wallet application in a variety of ways. For starters, it would allow users to store all of their digital assets in one location. Users would be able to manage their assets and move them between platforms more easily as a result of this. The super wallet application would also be decentralized. This means that users would have complete control over their assets and that they would not be subject to the control of a central authority. Third, the super wallet application would be secure. The wallet would be protected by cryptography and it would be difficult for hackers to steal users' assets.

4. Web3 Access : The suggested solution offers a single, seamless way to access web3 platforms and services. Users may validate their identities across several chains without requiring numerous registrations or sophisticated authentication procedures. This simplified access makes it easier for consumers to interact with web3 technologies, improving user acceptance and engagement in decentralized applications, cryptocurrencies, and blockchain-based services.

5. Interoperability : The biometric-based SSID is intended to be cross-chain and platform compatible. Users can have a consistent identity and access rights across several industries, including education technology, healthcare, e-commerce, tourism, and employment. Interoperability reduces the need for users to create separate accounts and credentials for each platform, improving the user experience and lowering administrative expenses for users and service providers alike.

6. Trust & Privacy : The use of biometric data for authentication increases system confidence. Users may be certain that their identities are safely validated, alleviating fears of identity theft or fraudulent activity. Furthermore, biometric data remains with the user and does not need to be shared with service providers, protecting user privacy and avoiding the dangers associated with centralized personal data storage.

7. Future-proof Technology : Biometric-based authentication is a future-proof solution since biometric data is unique and unalterable throughout an individual's life. This guarantees that the biometric-based SSID solution may adapt and evolve in response to biometric technology improvements without jeopardizing security or needing users to alter their authentication methods.

8. Compliance and Regulation : The biometric-based SSID solution can meet security, data protection, and privacy regulations. Service providers can show compliance with applicable rules and industry standards by using standardized biometric authentication procedures and encryption practices.

The biometric-based SSID solution provides better security, user comfort, smooth web3 access, interoperability, trust and privacy, regulatory compliance, and future-proof technology. These benefits make the solution a tempting alternative for businesses looking for robust and user-friendly authentication techniques that overcome the drawbacks of traditional mnemonic-based private keys or passwords.

08. CONCLUSION

This whitepaper provides a game-changing strategy for creating a biometric-based Secure Service Identifier (SSID) that is compatible across many chains, providing better security and user convenience. The suggested system substitutes mnemonic-based private keys or passwords with biometric authentication, which generates a new private key with each biometric scan.

The biometric-based SSID solution tackles the inadequacies of existing authentication techniques while also providing a number of advantages. It improves security by taking advantage of the uniqueness and difficulty in copying biometric data. Passwordless access and seamless web3 authentication boost user comfort. Interoperability across chains guarantees that identities and access credentials are similar across industries, eliminating administrative cost for users and service providers. The benefits of a biometric-based SSID extend beyond trust and privacy, as users may be confident in safe identity verification without jeopardizing their personal biometric data. Biometric authentication's future-proof nature enables for adaptation to technological improvements. Additionally, laws can be met by using standardized protocols and encryption practices.

The proposed wallet is also a notch above the current available solutions as it will not only enable the user to store the DID but also support all digital assets. This solution will incorporate Hyperledger Indy and Polygon networks which would eventually lead to interoperability across all networks.

To summarize, the biometric-based SSID solution proposed in this whitepaper provides a safe, interoperable, and user-friendly authentication strategy. This technology solves existing inadequacies while also paving the way for the future by using biometric data and removing the requirement for mnemonic-based private keys for the wide-scale adoption of secure and seamless web3 access across industries.