FISE

FINANCIAL INTELLIGENCE SEARCH ENGINE

FISE Technologies White Paper

Authored By:

Kevin W. Hartig, CTO, FISE Technologies Inc.
kevin@fiseportal.com

M.E. ‘Nara’ Lau, CEO, FISE Technologies Inc.
nara@fiseportal.com

Date:

5 June 2023

Abstract:

This white paper describes FISE Technologies' platform, FISE Portal (fiseportal.com), and clarifies the need for a new foundational framework, one that supports the standardized development of **Self-Sovereign Identity (SSI)** applications.

There are a number of outdated and newly emerging technologies that can be used to securely host and self-manage personal data, as well as define how and when it can be shared directly between peers. Mechanisms are available to acquire, manage, and validate credentials which define the state and abilities of individuals and entities. There are also tools to create and manage decentralized IDs, decentralized storage, and cryptocurrency.

Currently, few implementations integrate these fundamental components into a unified interface, enabling individuals to securely interact with multiple applications and various types of individuals, organizations, or trusted entities. Today, non-interoperable applications with custom implementations are largely siloed and cannot interact seamlessly with each other. The solution to non-interoperability and antiquated silos utilizes, instead, a common framework. This framework facilitates user-centric, interoperable integration of applications and services, allowing users, individuals, and organizations to easily manage their digital identities and data.

The proposed framework described in this white paper includes a discussion of infrastructure components and services such as easy sign-up and on-boarding, unique decentralized ID assignment, a cryptocurrency wallet, verifiable credentials management, and access to decentralized storage. The infrastructure components and services are the cornerstones of the framework. FISE Technologies' framework integrates and interoperates these infrastructural components and services, enabling users to store and manage IDs, data, credentials, and currency.

FISE Technologies' framework integrates the components through software libraries and APIs, allowing developers to build custom applications which enable users to securely access their assets via trusted interactions defined by the individual. FISE Technologies' platform, FISE Portal, employs self-sovereign identity

principles, illuminating a new approach to identity management, user-controlled privacy, built-in security, and user-control over personal data. This white paper elaborates on FISE Technologies' proposed SSI framework, implementation, essential use cases, current challenges and limitations, and descriptions of technical components.

I. Introduction

Problem: Current challenges in managing digital identities

In order to develop tools that facilitate self-sovereign identity, users must be empowered to own and manage one or more identifiers. On a sliding scale of granularity, the most granular definition of *user* is the individual, with entity representations of the term *user* defined by sole proprietors, small businesses, corporations, consortiums, and governments.

When digital self-sovereignty is respected, enforced, and maintained at the individual user level, digital self-sovereignty will also be respected, enforced, and maintained at the entity user levels of sole proprietors, small businesses, corporations, consortiums, and governments. If individual users' digital self sovereignty are ignored, abused, or disrespected, entity users' digital self sovereignty will likewise suffer the same. The individual user is the most important building block and foundation of any entity; and by extension, is also the most important building block and foundation of any sustainable, healthy economy.

In the present day, individuals commonly possess some form of identification that establishes their identity. Digital identifiers have already gained widespread adoption for representing both individuals and entities. For instance, online accounts maintained by many people, which utilize username and password credentials, serve as a form of digital identification managed by the respective service providers.

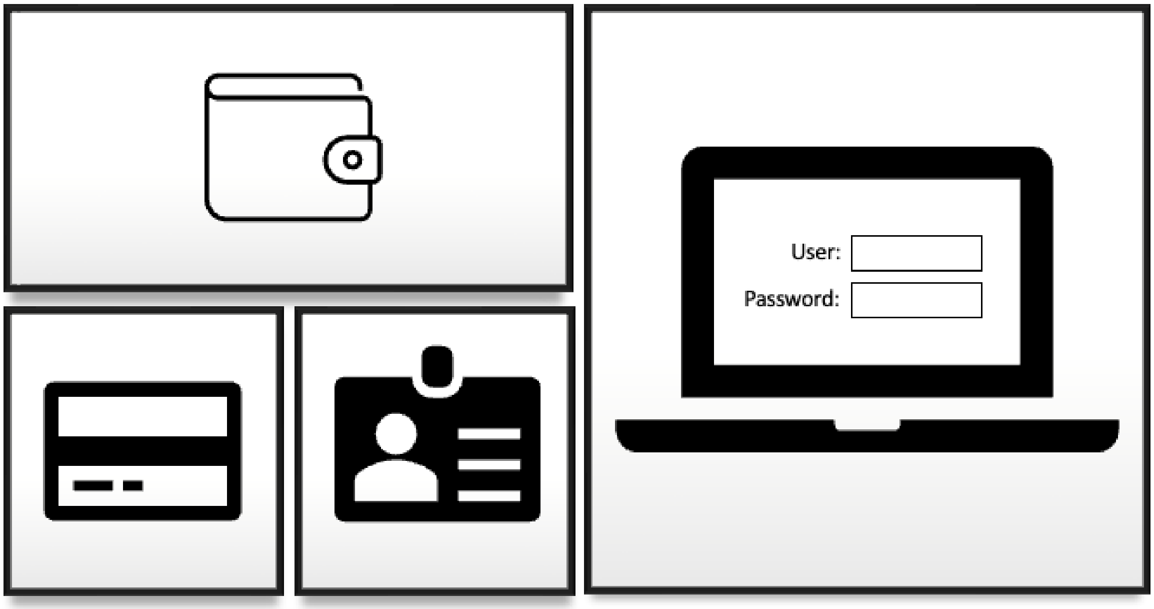

Diagram 1. Multiple Identifiers Typically Used, Physical & Online

The handling of everyone's identity in siloed data centers and siloed data storage is problematic. Current implementations of digital **identity management systems (IMS)** have a very real potential of experiencing, and have experienced the following issues:

- **Identity Theft and Fraud** - Identity theft is a crime in which someone uses another person's personal information to commit fraud or other crimes. It can have a devastating impact on the victim and is difficult to recover from. Cybercriminals are constantly finding new ways to steal personal information, making it difficult to verify the authenticated identity of users. In 2021, it was reported that identity theft affected 42 million Americans, costing $52 billion dollars, a 79% increase from the year 2020's identity theft costs at $24 billion. [1]

- **Data Breaches** - Large-scale data breaches are a major threat to digital identities. They put sensitive information at risk, such as passwords and Social Security numbers, which can be used to commit identity theft and fraud. Data breaches happen often to many types of organizations. Over 30 big data breaches were reported in 2021. Industries affected include oil & gas, motor vehicles, IT, telecom, social media, retail, healthcare, cryptocurrency, and an entire country. [2]

- **User Experience** - Users want a convenient experience when using digital services, but this can be difficult to achieve while keeping their data safe. Requiring users to create and remember multiple passwords leads to less-than-ideal practices such as using weak passwords or reusing passwords across multiple accounts. This increases the risk for hackers to gain access to their accounts. Password lists may be saved in unsecured locations that are easily compromised. Password managers provided by some companies have been known to be compromised in the past. Most often, users do not know where or what personal information is being saved or how to manage it. [3]

- **Interoperability**: Digital identities are often used across multiple platforms and systems. These federated identities may be sufficient for a few collaborating services but can create challenges for interoperability and compatibility. Federated identities only operate through a restricted set of services; and it is unclear where and how identity information is stored and how it is used. [4]

- **Regulatory Compliance**: Organizations must comply with a growing number of regulations and standards related to data privacy and security, which can make it challenging to manage digital identities compliantly, especially when regulations present potential conflicts with each other. For example, some of the current regulatory compliance standards that need to be accommodated include GDPR, KYC, CCPA, FCPA, PCI-DSS, and ISO standards.

Solution: The Need for a New Approach to Identity Management

The limitations of traditional identity management systems can be addressed by implementing a **self-sovereign identity** (**SSI**) platform. An SSI platform is a decentralized system that allows individuals to own and control their own identity, credentials, data, and currency in one place and from one context. This information can be used to prove who they are to websites, services, and applications without having to rely on a central authority intermediary for the interaction.

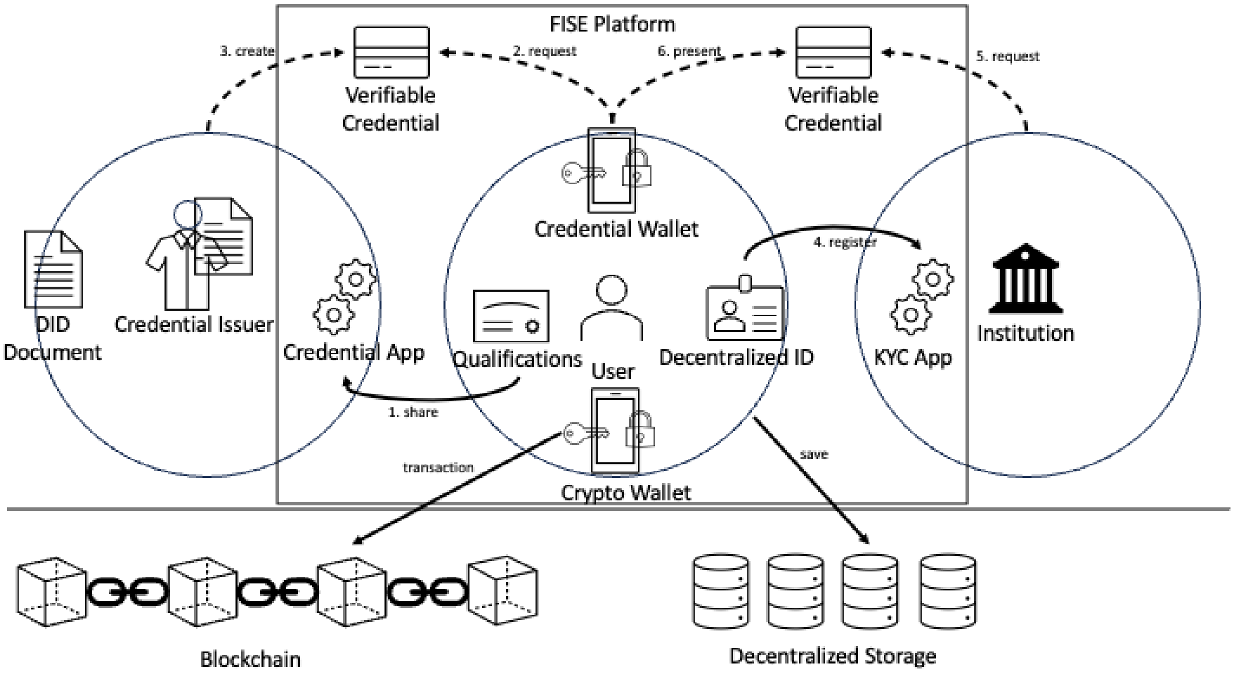

Diagram 2. FISE Platform: New Approach to Identity Management

An SSI platform addresses the limitations of traditional identity management systems in a number of ways:

- **Privacy:** User data is stored in a decentralized manner, where data is signed to indicate ownership and is encrypted which ensures that it is private and secure.
- **Security:** An SSI platform designed with built-in security measures leverages various cryptographic techniques for authentication, authorization, and data management.
- **User Control:** Users have complete control over their identity data, with options to create, access, update, and delete their data at any time.
- **Common Framework:** An SSI platform provides a common framework for building SSI based applications. This makes it easier for developers to build new applications and easier for users to manage applications they use.

- **User-friendly UI:** An SSI platform provides an easy-to-use user-interface (UI) for users to manage their identities, credentials, storage, documents, data, NFTs, and cryptocurrencies.

An SSI platform provides a more secure, private, authenticated, and user-controlled way to manage identity.

II. Problem Statement

Traditional identity management systems suffer from a number of limitations, including:

- **Privacy:** Existing solutions often rely on central authorities, which means that user data is not always private. This can lead to data breaches, identity theft, and other privacy concerns. Often, personal user data is mined and sold for profit with little or no consideration for the individual.

- **Security:** Central authorities can be a single point of failure, which means that if a central authority is breached, user data could be compromised.

- **User Control:** Users have limited control over their identity data in traditional identity management systems. This means that users cannot easily access, update, or delete their data. Some jurisdictions provide laws requiring companies that maintain personal data to abide by individuals' wishes on how to manage their data. How to make these requests is not always obvious or easy. Fulfilling user requests regarding their data and giving them actionable control over their data can be time-consuming and unclear. In some locations, users have no recourse to manage their own personal data.

- **Lack of a Common Framework:** At present, a notable gap exists in the realm of software design patterns. Specifically, no cohesive framework exists that seamlessly integrates verifiable credentials, decentralized IDs, decentralized storage, and cryptocurrency—the critical components of a unified, user-centric foundation for the development of decentralized applications, or DApps. The current user experience for users of DApps and normal (centralized) applications consists of managing their personal data across many dispersed locations for each DApp, a cumbersome and burdensome process.

- **Insufficient UIs:** Presently, the absence of a cohesive user interface hinders convenient, user-centric management of identities, credentials, storage, documents, data, NFTs, and cryptocurrencies. This lack of convenience impedes the mass adoption of digitized ownership, decentralization, and data sovereignty, as users struggle to grasp their interconnections and create a user-driven data economy. To overcome this challenge, streamlined and user-friendly interfaces are needed to consolidate these diverse elements, allowing users to effortlessly navigate and engage with their digital assets, thereby promoting equitable and incentivized data practices.

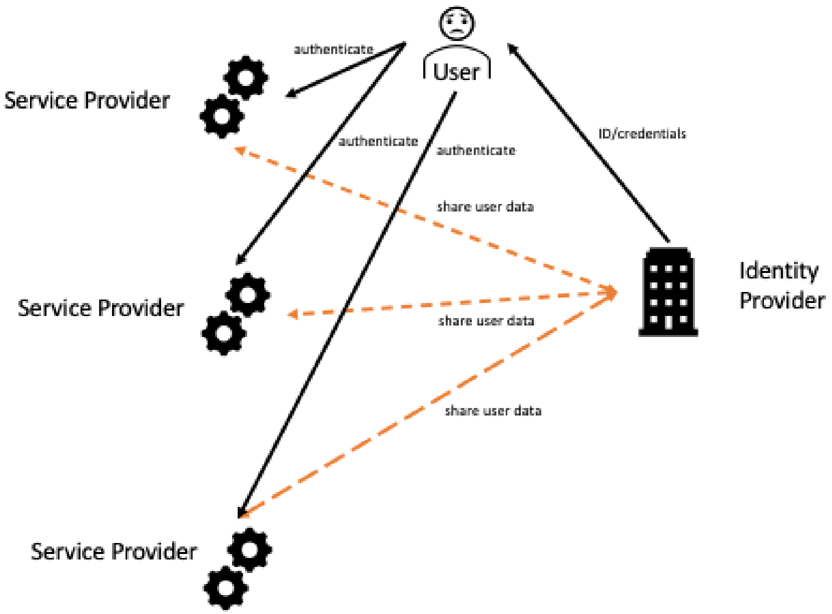

Diagram 3. Federated Identity Management. User data centrally controlled by custodian and copies scattered.

III. Solutions

SSI is a new approach to identity management that gives users control over their own identity data. SSI uses decentralized technologies such as blockchain, distributed storage, verifiable credentials, and secured identity creation technologies to manage a portfolio of data. This decentralized approach has a number of advantages over centralized IMS, including:

- **Increased Security**: SSI enhances data security by rendering user identities less susceptible to theft by criminals. This is achieved through decentralized storage of user data and the application of dynamic cryptographic techniques to encrypt the data, making it highly inaccessible to unauthorized individuals.
- **Improved Privacy**: SSI gives users more control over their personal information. Users can choose what data they share, with whom, and for how long.
- **Enhanced Portability**: SSI enables portability, making it possible for users to move their identity data between different systems. This is because SSI data is stored in a decentralized format, and is not tied to any particular system.
- **Better User Experience**: SSI is designed for ease-of-use, even for users who are not familiar with technology. User-centric control over personal identities, credentials, and secured data provides an easier way to manage an identity portfolio.

The need for new **Identity Management Systems (IMS)** using SSI technologies is clear. Current IMS lack sufficient security, often do not meet regulatory standards, and perpetuate unethical online experiences, infecting users' everyday lives with risks of identity theft, fraud, and spam.

SSI offers a number of advantages over centralized IMS, and it is the future of identity management.

- **Increased Privacy:** Users have more control over their personal data and can choose who they share it with.
- **Improved Security:** SSI platforms are designed to be more secure than traditional identity management systems.
- **Greater Convenience:** Users' SSI credentials are used and re-used to access a variety of services and applications without having to create new accounts or remember multiple passwords.
- **Enhanced Trust:** SSI platforms help build trust between users and organizations.

FISE Technologies' proposed solution combines the core SSI building blocks of decentralized IDs, decentralized storage, verifiable credentials, and cryptocurrency into a framework upon which interoperable applications can be built. The central control of personal data is shifted back to the individual for safety and security, and to facilitate the sharing of permissioned, high-quality, authenticated data between individuals and other entities.

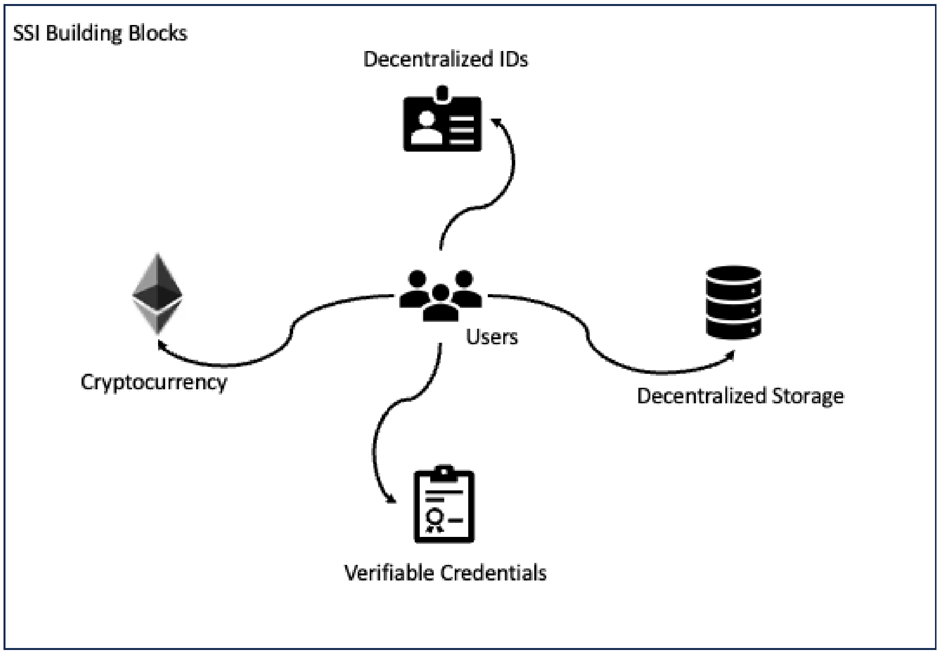

Diagram 4. Self-sovereign Identity Foundational Building Blocks

IV. What is Self-Sovereign Identity?

Definition of Self-Sovereign Identity

Self-Sovereign Identity (SSI) is an approach to digital identity that emphasizes individual control and ownership of personal data. It is a decentralized identity model that enables individuals to create and manage their own digital identities. By creating and managing their own digital identities, users can securely access digital services, verify their identity, and securely share personal information with others.

Unlike traditional identity management systems, SSI places the individual at the center of the identity model. This gives individuals control over their own data and the ability to share it on their own terms. Similarly, other entities such as **Internet of Things (IoT)** devices and **Artificially Intelligent (AI)** bots can have defined digital identities. AI and IoT data would belong to an authenticated user on FISE Technologies' SSI platform. Decentralized ownership of AI and IoT data can help mitigate behavioral risks, establish trust, accountability, and improvement metrics for owners and controllers of AI bots and IoT devices.

Key Features and Benefits of SSI by FISE Technologies

In traditional identity management systems, users rely on third parties, such as government agencies or social media platforms, to store and manage their identity data. This can lead to identity theft, data breaches, and a lack of privacy.

SSI solves these problems by giving users control over their own digital identity and data. Users create and manage their own digital identity, and users choose who has access to their data. Users have more control over their privacy and security, making it arduous for identity thieves to steal users' information.

Although a total consensus of what it means to achieve self-sovereign identity has yet to happen, a general collection of key principles listed below are generally accepted as prevailing criteria used to define SSI [5]:

1. **Existence**: Users are able to create and manage their own digital identities without relying on a third party. This means that users are able to create their own unique identifiers, store their own identity data, and control who has access to their data.

2. **Control**: Users have complete control over their digital identities and personal data. Users create, modify, and delete their own data. They are in control of managing it. Also, users are able to decide who has access to their data, and they are able to revoke access at any time. Giving users control over their data helps protect their privacy and security.

3. **Access**: Users are able to easily access their own data at any time without having to go through a third party.

4. **Transparency**: The processes and algorithms used to manage and update an identity system are transparent and understandable to users. Users easily understand how their data is being used, and they are able to make informed decisions about who has access to it. Giving users transparency helps build trust and confidence in the next digital age, where the internet connects people, things (IoT), and AI.

5. **Persistence**: Identities possess durability and persistence. Users employ their digital identity over extended periods without concerns about invalidation or obsolescence. These identities are intentionally designed to withstand the evolving digital landscape and seamlessly adapt to changes over time.

6. **Portability**: Identities are seamlessly transferred across diverse systems and networks. Users employ their digital identity across multiple services and applications, eliminating the need to create a new identity for each platform. These identities are purposefully designed for effortless portability, enabling smooth transitions between different platforms, independent of any specific service or application.

7. **Interoperability**: Digital identities are readily accessible and usable for all users. They are employed with various organizations, eliminating the need for repetitive and time-consuming verification procedures. These identities are intuitively designed, ensuring ease of use and comprehension. Importantly, they are accessible to individuals irrespective of their technical proficiency.

8. **Consent**: Users have the right to control their data. Users decide who has access to their data, and they may revoke access at any time. Users do not have to give their data away without their consent, and they do not need to worry about their data being used without their permission.

9. **Least Disclosure**: Digital identity solutions enable users to share only the necessary data. Users are solely required to share the specific data pertinent to a particular transaction, without the need to disclose any additional information even if it is available. This ensures that users maintain control over their data and share only what is essential, enhancing privacy and security by minimizing unnecessary exposure.

10. **Protection**: Data remains safeguarded against unauthorized access and interception. Users have the option to encrypt their data to prevent unauthorized parties from reading it. The authorized user retains control over the encryption process and determines who has the permission to decrypt their data. Data may be signed, attributing ownership of the content. In cases where data is copied, authorized digital signatures are necessary to ownership of the original data.

SSI is a promising new approach to digital identity that solves many of the problems associated with traditional identity systems. By giving users control over their own identity data, SSI helps to protect users' privacy and security which can decrease the odds of identity theft and hacking.

Importance of Each Component in Building a Comprehensive SSI system

SSI systems offer a number of advantages over traditional identity management systems. The most important components and their advantages include:

- **Decentralized IDs (DIDs)**: DIDs are essential for SSI systems because they allow users to own and control their own identity data. Decentralized IDs are a type of identifier that is not controlled by any single entity other than the individual who created it. DIDs are stored on a blockchain or in secured decentralized storage, which makes them tamper-proof and immutable.
- **Distributed Storage**: Distributed storage is essential for SSI systems because it allows users to store their identity data in a secure and decentralized manner. Distributed storage is a type of storage that is spread across many nodes. This increases the difficulty for hackers to attack, compromise, or steal data. It also improves reliability and resilience. For example, the IPFS distributed storage network remained functional, available, and respondent for all data even with a 60% degradation of available nodes. [6]
- **Verifiable Credentials (VCs)**: VCs are essential for SSI systems because they allow users to share their identity data with others in a secure and verifiable manner. VCs are digital documents that contain information about a user. VCs are signed by an Issuer of the credential, and are easily verified by anyone on the FISE Portal platform.

- **Cryptocurrency**: Cryptocurrency is essential for SSI systems because it is used to pay for services such as identity verification and storage. Cryptocurrency is a decentralized digital currency based on cryptographic principles, enabling secure and transparent transactions independent of central authorities.

Comparison with Traditional Identity Management Systems

Traditional identity management systems (IMS) depend on central authorities or intermediaries for identity management and verification. IMS systems employ central custodians who oversee users' personal data and data tracking. Often, custodians do not prioritize the best interests of customers or may inadvertently mishandle the data, leading to potential risks and concerns.

In contrast, SSI represents a decentralized identity model empowering individuals to establish and oversee their digital identities and user-originated data. Digital identities consist of verifiable claims related to their attributes and credentials. By adopting SSI, individuals gain enhanced control and ownership over their data, which reduces the dependence upon central authorities and intermediaries for users' data management. This decentralized approach revolutionizes the way identities are managed, placing individuals at the center of their own digital identity and data management brokering.

V. Proposed Framework Architecture and Technical Details

For a functionally secure, safe, and easy to use self-sovereign identity system to be viable, it needs to provide the mechanisms to manage decentralized identities, decentralized storage, verifiable credentials, and a wallet for currencies used in financial transactions. A corollary to this in the physical world might be a wallet or handbag. It contains items for transferring currency, proof of identification, credentials indicating memberships, and access to data in the form of handwritten notes.

In today's world, it is possible for each user to store and share personal information in digital form on users' phones, tablets, or laptops. Much of this information is also stored on centralized servers. These servers are managed and controlled by third-party corporations on users' behalf. They have access to all of the users' personal information. Users have little to no control concerning third-party corporations' access and control over their own personal data.

FISE Technologies' platform, FISE Portal, transfers ownership and control back to the user, enabling them to manage their digital identities and data. The proposed framework provides the mechanisms for users to create, manage, and potentially monetize a data portfolio.

The next section describes the core components used in the FISE Portal framework, enabling users to build and manage their own identity portfolio.

Decentralized Identities

Decentralized identity refers to an identity system where individuals have ownership and control over their own identity data, rather than relying on centralized authorities or intermediaries to manage and verify their identity. In a decentralized identity system, individuals can create and manage their own digital identities, which are based on verifiable claims about their attributes and credentials, such as their name, address, age, or educational qualifications. Decentralized identity is based on the principles of SSI, which emphasize the individual's right to control their own identity data, and the need for interoperability, privacy, and security in identity systems.

Decentralized identity has numerous benefits, including increased privacy and security, reduced risk of identity fraud, secured and authorized access to verifiable services and resources, and greater control and ownership over personal data. By enabling individuals to own and manage their own digital identities, decentralized identity systems can also reduce the reliance on central authorities and intermediaries.

Decentralized Storage

Decentralized storage is a method of storing data across a network of nodes, rather than in a centralized location managed by one or more custodial corporations. This provides several advantages over centralized storage, including:

- **Greater Security**: Decentralized storage increases the complexity for attackers attempting to access data, as they must compromise multiple nodes within the network.
- **Increased Privacy**: Decentralized storage gives users more control over their data, as they can choose who has access to it.
- **Improved Resilience**: Decentralized storage is more resilient to outages, as data is not stored in a single location.
- **Reduced Costs**: Decentralized storage can be more cost-effective than centralized storage, as costs are controlled through greater market availability of storage.

Decentralized storage systems are implemented using a variety of technologies, including **peer-to-peer (P2P)** networks, blockchain, and **Distributed Hash Tables (DHTs)**. P2P networks allow users to connect directly to each other and exchange data without the need for a central server. Blockchains are a form of distributed ledger technology facilitating secure and tamper-proof storage of data. DHTs are decentralized data structures that distribute a hash table across a network of nodes.

Decentralized storage has a number of potential applications, including:

- **Storing Personal Data**: Decentralized storage is used to store personal data, such as medical records, financial information, and contact information. This helps protect personal data from unauthorized access.
- **Storing Data for Research**: Decentralized storage is used to store data for research purposes. This helps improve the efficiency of research and makes it easier to share data between researchers.
- **Storing Data for Applications**: Decentralized storage is used to store data for applications, such as cloud computing and gaming. This helps improve the performance of applications and make them more reliable.

Decentralized storage is a promising technology with a number of potential benefits. However, it is important to note that decentralized storage is still a developing technology, and there are some challenges that need to be addressed. These challenges include:

- **Scalability**: Decentralized storage networks are continuously evolving to enhance their scalability and address the challenges associated with accommodating a large number of nodes for efficient data storage and access.
- **Security**: Decentralized storage network security needs additional reinforcement, such as that provided by FISE Technologies' built-in encryption, to mitigate risks of data exposure via cyber attacks.
- **Cost**: Although decentralized storage networks currently entail higher monetary costs compared to centralized storage networks, users can appreciate their value when considering the risks associated with identity theft, fraud, spam, and unsecured online user experiences. These risks sometimes result in significant time and monetary losses. By opting for decentralized storage networks, users gain peace of mind and enhanced data security, justifying the investment. Additionally, it is important to note that new technologies, like decentralized storage networks, typically experience a decline in monetary cost over time due to ongoing technological advancements.

Despite these challenges, decentralized storage is a promising technology with the potential to revolutionize the way data is stored. This technology is viable for building production systems today. As technology advances, decentralized storage may become widely adopted.

Verifiable Credentials

Verifiable credentials refer to a form of digital credential empowering individuals to securely and dependably share their personal information with others, including organizations, without reliance on a central authority for verification. Credentials are generated using decentralized services and undergo cryptographic verification, guaranteeing their integrity and preventing unauthorized tampering. They are used by applications in various domains such as identity verification, access control, and digital signatures, with the potential to transform how individuals handle and exchange personal information online.

Verifiable credentials provide a digital means of affirming an individual's identity, qualifications, or permissions, validating their authenticity.

A "Triangle of Trust" represents the relationship between the Issuer, Holder, and Verifier in the context of verifiable credentials, enabling secure and privacy-enhancing digital identity verification. It establishes a dynamic framework where the Holder maintains control over their credentials, relying on trusted Issuers for their validity, while Verifiers authenticate the presented credentials to confirm the claims made. [7]

- **Issuer**: Responsible for issuing verifiable credentials, ensuring their validity and integrity through digital signatures.
- **Holder**: Possesses and controls the verifiable credentials, selectively sharing them based on their needs and retaining ownership of their personal information.
- **Verifier**: Relies on trusted Issuers and cryptographic techniques to validate the authenticity and integrity of the presented verifiable credentials, confirming the claims made by the Holder.

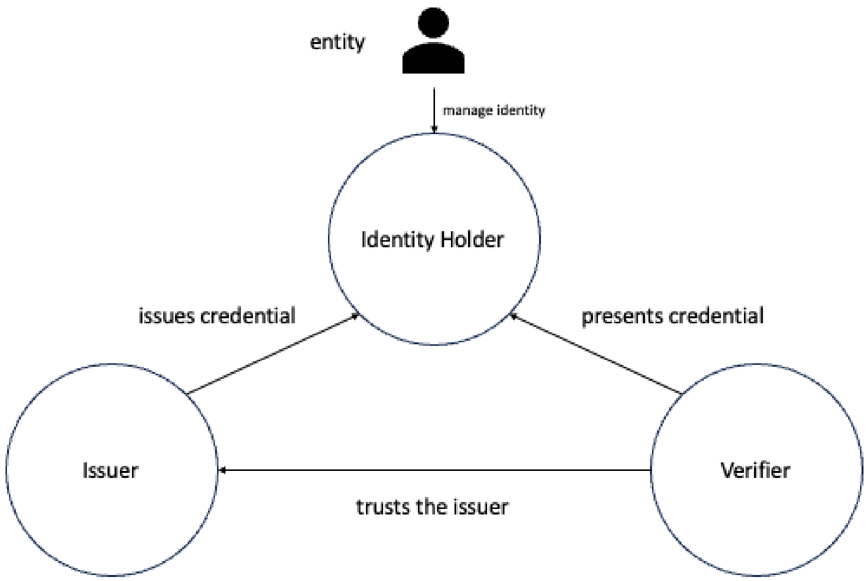

Diagram 5. Triangle of Trust

An individual acquires credentials from an Issuer, for example, a government agency or educational institution. The individual then presents these credentials to a Verifier, such as an employer or service provider, who utilizes the credentials to authenticate the individual's identity or qualifications. This streamlined process fosters trust and minimizes the necessity for repetitive exposure and analysis of sensitive personal information in order to meet identity verification standards.

Cryptocurrency Wallets

Cryptocurrency wallets are software applications designed to facilitate the storage, management, and transfer of digital assets, such as Bitcoin, Ethereum, or other cryptocurrencies. These wallets employ complex cryptographic techniques to generate public and private keys that are used to securely send and receive digital currencies utilizing various blockchains. They are capable of storing and managing multiple types of cryptocurrencies simultaneously. Cryptocurrency wallets are implemented with software that is deployed to desktop computers, mobile phones, and other hardware devices. Wallets are essential tools for managing cryptocurrency holdings, enabling transactions, and keeping track of balances. They provide users with full control over their digital assets, including cryptocurrencies and NFTs, and offer various security features, such as two-factor authentication, to prevent unauthorized access, and ensure the safety of the stored cryptocurrencies.

VI. Core Components of the FISE Technologies Framework

Explanation of each core component

Decentralized Identifiers (DIDs)

During new account registration on the FISE Portal platform, a cryptographically originated decentralized identifier (DID) is assigned to the user. DID assignment is transparent to the user and is visible in the user interface. DIDs on the FISE Portal platform follow the W3C-DID specification.

The basic decentralized identifier architecture is as follows [8]:

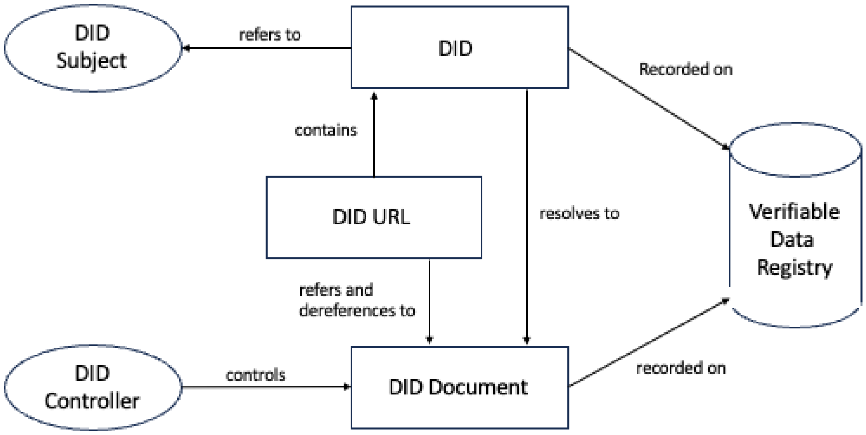

Diagram 6. Decentralized Identifier Architecture

DIDs and DID URLs

A Decentralized Identifier, or DID, is a URI composed of three parts:

- *Scheme*: the scheme is the first part of the DID and it identifies the type of DID. The current standard for DIDs is the `did:` scheme.
- *Method*: The method is the second part of a DID and it identifies the method that was used to create the DID. There are many different methods for creating DIDs, such as the **DID Method Resolution Service (DMR)** and the **Verifiable Credential Data Model (VCD)**.
- *Identifier*: The identifier is the final part of a DID. It is a unique identifier that is used to identify the specific entity that is being referred to. The identifier is a string of characters, numbers, or a combination of the two.

  Syntax:

  ```
  did:exampleMethod:123abc456def7890z
  ```

This DID uses the *scheme*, `did:`, the *method*, `exampleMethod`, and the *identifier*, `123abc456def7890z`. This DID resolves to a DID document containing information about the entity or individual identified by the DID.

DIDs are resolvable to DID documents. A DID URL extends the syntax of a basic DID to incorporate other standard URI components such as *path*, *query*, and *fragment* in order to locate a particular resource—for example, a cryptographic public key inside a DID document, or a resource external to the DID document.

DID subjects

The subject of a DID is, by definition, the entity or user identified by the DID. The DID subject might also be the DID controller. Anything can be the subject of a DID: person, group, organization, thing, or concept.

DID controllers

The controller of a DID is the entity or user (person, organization, or autonomous software) that has the capability—as defined by a DID method—to make changes to a DID document. This capability is controlled by a set of cryptographic keys automated by software acting on behalf of the controller, though it might also be controlled via other mechanisms. Note that a DID might have more than one controller, and the DID subject can be the DID controller, or one of them.

Verifiable Data Registries

In order to be resolvable to DID documents, DIDs may be recorded on an underlying system or network. A system that records DIDs and returns data necessary to produce DID documents is called a *verifiable data registry*. Examples include distributed ledgers, decentralized file systems, databases of any kind, peer-to-peer networks, and other forms of trusted data storage.

DID documents

DID documents contain information associated with a DID such as cryptographic public keys, and interactive services relevant to the DID subject.

Core Properties

A DID document serialization produces a byte stream. The properties within a DID document receive updates based on applicable operations.

DID methods

DID methods serve as the mechanism for creating, resolving, updating, and deactivating a specific type of DID and its corresponding DID document. These methods are defined through distinct specifications dedicated to each DID method.

DID resolvers and DID resolution

A DID resolver acts as a system component that receives a DID as input and generates a compliant DID document as output. This operation is known as DID resolution. Procedures for DID resolution per type of DID are outlined in corresponding DID method specifications.

DID URL dereferencers and DID URL dereferencing

The system component DID URL dereferencer takes a DID URL as input and produces a resource as output. This process is called DID URL dereferencing.

After DID creation, users use the DID to sign their owned and managed data. A DID can also represent an identification method in verifiable credentials. The EIP-2844 [9] standard introduces additional methods to the JSON-RPC, enabling signing and decrypting JOSE objects using a new did_* prefix. EIP-2884 streamlines and standardizes the process of signing and encrypting data files. Enhanced portability via compatible signing standards is now achievable with crypto wallets like MetaMask.

Distributed Storage

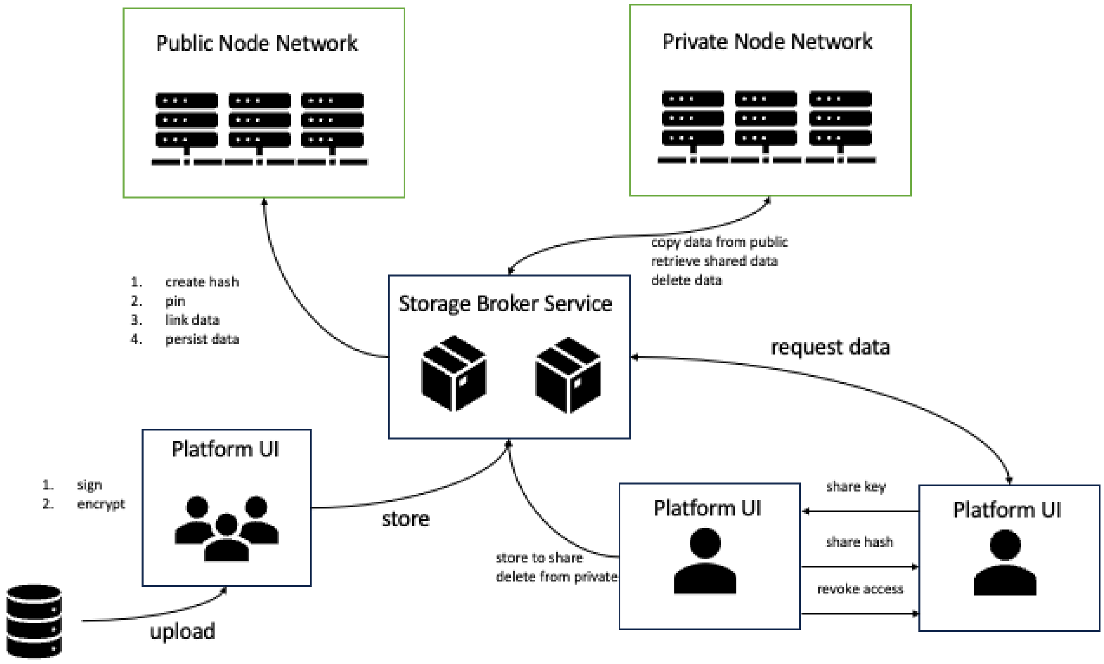

Diagram 7. Private Data Management

The main architectural components of distributed storage include these stable and secure implementations:

- **Storage Network**
  - *Public network* - the public network is composed of many nodes connected to the internet as peers and geographically distributed around the world. Users' data are stored on these nodes with file pieces linked by a directed acyclic graph (DAG). File pieces are duplicated across some nodes for redundancy and performance when accessing the data. A user may store both encrypted and unencrypted data in this network. Data may also be digitally signed. Unencrypted data is freely accessible to anyone. If the data is signed it has a unique verifiable attribution to the creator. Encrypted data is accessible to others but unencryptable unless done by the original owner storing the data.

  - *Private network* - the highly controlled private data network is not accessible by anyone, except authorized users. The private data network temporarily stores data that is shared between entities.
- **Storage Broker Service** - the storage broker service reads and writes data for storage in decentralized nodes. It creates a hash of the data to uniquely identify the data for pinning and naming. In case the content is updated and needs to be easily referenced, the service handles linking the data to solidify relationship definitions with other data.

The FISE Technologies SSI platform, FISE Portal, provides the interface tools and components needed to:

- Initially upload files into the system from local storage
- Sign the data with a unique identity defined for the owner of the data
- Encrypt the data using both a unique identity and private keys
- Send the data to be stored in decentralized storage using the storage broker service
- View data owned by the verified and authenticated user in the system
- Retrieve the data and convert to local storage if desired
- Share data with other verified and authenticated users or entities
- Revoke shared access

Sharing files in distributed storage requires some sophistication in order to keep the data private and secure, and to ensure parties can verify each other in a data-sharing transaction. The following is a basic description of how the data files are shared.

The Provider permissions access for the Receiver to view one of its files. The Provider must prove its identity to the Receiver. The Receiver is the Verifier of the Provider's identity and retrieves the content from the Provider.

Security, encryption, authentication steps below are automated on the FISE Portal back-end for users convenience. On the front end, the user experiences a simple, secure, permissioned, and intuitive application interface.

1. The Receiver generates a public/private key pair and a unique salt value. This is done automatically by the FISE Portal platform.
2. The Receiver provides their public key and salt value to the Provider.

3. The Provider creates a digital identity token from its decentralized identity (DID) assigned by the platform by encrypting the identity value with a secret key known only to the Provider.
4. The Provider generates a hash value of the encrypted identity token using the Receiver's public key, salt value, and the agreed upon check function.
5. The encrypted identity token is used to encrypt the file being shared. The file is signed using the hash value of the encrypted identity token.
6. The encrypted file is stored in the private node network, assigned a unique file hash, and that hash value is sent to the Receiver.
7. The Receiver retrieves the encrypted file through the storage broker service.
8. The Receiver reads the hash value that signs the file and uses the check function to verify that the hash is correct. The Receiver plays the role of the Verifier.
9. If correct, the Receiver decrypts the hash with its private key. If the check function fails, the Receiver knows that either the file has been compromised or that the Provider was intercepted.
10. A successfully decrypted hash can then be used to decrypt the file.

Note that the Receiver is able to view the decrypted file but is not allowed to save it to an external storage device. It is at the time the Receiver initiates viewing the file content that it is retrieved and decrypted. This is automatically done on the FISE Portal platform and requires no actions by the Receiver other than opening the file for viewing.

The Provider inputs a data and time of expiration that revokes access to a file. The file is removed from access so the Receiver can no longer access the file on the private node network. The original file, owned by the Provider, is still intact and accessible to the Provider.

Verifiable Credentials Infrastructure

The credential infrastructure is a decentralized protocol for issuing, presenting, and verifying **verifiable credentials (VCs)**. VCs are digital certificates that can be used to represent claims about an individual or organization. The infrastructure is designed to be secure, privacy-preserving, and scalable.

There are three layers in the architecture that handle credentials:

- **Application Layer**: The application layer is where applications interact with the platform to manage credentials. The application layer provides APIs that allow applications to create, manage, and use keys.
- **Network Layer**: The network layer is responsible for transferring key events between nodes. The network layer uses a peer-to-peer network supported by the platform to ensure that events are delivered reliably.
- **Storage Layer**: The storage layer is responsible for storing events. The storage layer uses a distributed storage system to ensure that events are resilient to attack. The platform provides the necessary distributed storage mechanisms.

To request a VC, a Holder creates a credential request and sends it to an Issuer. The Issuer then verifies the request and, if it is valid, issues the VC to the Holder. The Holder then presents the VC to a Verifier, who verifies its authenticity and validity.

The VC infrastructure uses a distributed ledger to store VCs. This makes it possible to verify the authenticity and validity of VCs without the need for a central authority. It also uses cryptographic techniques to protect the privacy of VC Holders. The distributed ledger itself, that holds VC credentials, is stored in decentralized storage. The distributed ledger is encrypted and private to the user within the platform. Only the user can decrypt the information for use when interacting with entities needed to share credentials. Since the credentials are encapsulated within a distributed ledger, a user can take the credentials to some other system if needed or desired. They are not tied to a specific platform implementation.

Managing the credentials requires a trust-based system that binds identities to credentials. The following components and associated functions procure a trust-based system for identity-credentialing.

- **Controller**: The controller is a user who owns an identity. The controller is responsible for managing their identity and keys.
- **Event Log**: The event log is a record of all key events that have occurred for an identity. Events include the creation, deletion, and rotation of keys used to sign credentials.

- **Public Key**: The public key is a cryptographic key that is used to verify signatures and encrypt data. The public key is associated with an identity and is used to help authenticate the controller.
- **Identifier**: The identifier is a unique identifier that is assigned to an identity. The identifier is used to reference the identity in the key event log and in other systems.

The trust-based identity system is a secure and verifiable way to manage identities. The system is based on the following principles:

- **Decentralization**: The system is decentralized, which means that there is no central authority that controls the system. This makes the system more secure and resistant to attack.
- **Verifiability**: The system uses cryptographic techniques to ensure that key events are verifiable. This means that anyone can verify that a key event has occurred.
- **Security**: The system uses a variety of security measures to protect keys and key events. This includes using strong cryptography and implementing security best practices.

Here is a general overview of how the infrastructure is used to *request*, *issue*, *present*, and *verify* a verifiable credential (VC): [10]

1. **Request a Verifiable Credential**: The Holder creates a credential request and sends it to the Issuer. The credential request includes the Holder's DID, the type of VC being requested, and the claims that the Holder wants to make.
2. **Issue a Verifiable Credential**: The Issuer verifies the credential request and, if it is valid, issues the VC to the Holder. The newly issued VC includes the Holder's DID, the claims made by the Holder, and the Issuer's signature.
3. **Verifiable Presentation of Verifiable Credential**: The Holder presents the VC to a Verifier. The Verifier verifies the VC's authenticity and validity using the Issuer's public key.
4. **Verify a Verifiable Credential**: The Verifier verifies the VC's authenticity and validity using the Issuer's public key. The Verifier can also check the VC's claims against the Holder's DID.

The verifiable credential infrastructure uses a secure, privacy-preserving, and scalable protocol for issuing, presenting, and verifying verifiable credentials. A variety of applications such as online voting, financial transactions, and access control use verifiable credential infrastructure, an essential core component of the FISE Portal platform.

Technical discussion of select components implemented in the SSI framework
(Libraries and APIs are available for developers to use and integrate with existing systems and platforms)

User Profiles

A user of the FISE Portal platform has a data profile with a minimum set of data. More user data is added by the user, which contributes to the pool of permissioned, anonymized user descriptions that can be purchased by entities or users such as marketers and advertising companies registered on FISE Portal.

The user profile data is private to the user and is anonymized by default, with options to de-anonymize before sharing with requesting entities. Profiles are represented as composable data structures. Various configurations of composable data structures provide building blocks empowering developers to rapidly construct applications atop the platform. The composable data structure is a contract defining a known structure of profile content.

A composable data structure contains anonymized user data and provides a comprehensive data solution for use cases that require searches of user profiles that meet verifiable attestation for skills, credentials, and reputation. These data structures are searchable using GraphQL [11], are portable, and can be used by a variety of applications such as social media, networking and advertising.

Credentials

Individuals and organizations (entities) are able to issue claims in the form of credentials about themselves or others that can be verified and trusted.

The Holder of a verifiable credential has the ability to control the extent of information disclosed when sharing the credential. They can set limitations on the duration of information sharing and it is possible to revoke an issued credential.

A Verifier has the authority to authenticate a credential as a genuine representation of an Issuer's claim regarding a subject. To achieve this, the Verifier establishes a connection between the Issuer's identity and the credential identifier, as well as between the subject's identity and their respective identifier mentioned in the credential. The verification information of the Issuer, including its public key, is accessible within the credential record and verifiably associated with the Issuer. The FISE Portal platform automates this process.

The claim Holder securely stores claims within a well-defined structure in a protected location. All the claims of the Holder are organized within the structure, allowing convenient retrieval of the data by authorized entities, enabling usage beyond the platform. This approach guarantees the integrity, validity, and portability of the claims.

The Holder is able to retrieve one or more credentials to present to a Verifier. The Holder selectively determines which content within the claim is shared with the Verifier.

An Issuer is able to revoke a credential and all the claims within. After revocation, the credential is no longer verifiable.

For consistency and security, only verifiable credentials using W3C standards will be handled. There is no translation or conversion of format of content between the original Issuer and Verifier. In the future, as more concrete definitions evolve and are accepted, the platform will accommodate a variety of formats.[12]

Applications

Applications developed on the FISE Portal platform facilitate seamless, user-permissioned, self-sovereign online interactions.

Applications empower users to manage their personal data securely, while also enabling the exploration of anonymized shared data from multiple individuals. By adhering to established protocols, applications act as intermediaries, facilitating the effortless exchange of verifiable credentials that serve as proof of an individual’s attribute, such as authenticating if a user is an AI bot or not an AI bot.

Leveraging distributed storage, applications provide users with encrypted storage capabilities, allowing them to securely store and retrieve their data without having to understand how to manage encryption keys.

Through applications built on the FISE Portal platform, users share these credentials or selectively disclose specific attributes of credentials with other entities. The process of verifying ownership or other relevant information is streamlined and automated into users' interactions on the FISE Portal platform.

Applications on FISE Portal seamlessly integrate non-custodial cryptocurrency wallet functions, allowing users to interact with digital assets securely, and manage their own assets while interacting with others who are also using applications on the FISE Portal platform. The platform facilitates secure and user-authenticated financial transactions for applications, fostering trust and reliability in digital interactions.

VII. User Stories

Examples of how the FISE Technologies' SSI framework can be used in various domains

Digital Education Transcripts

The registrar at TechVerse University, a cutting-edge technical institution, is responsible for maintaining the integrity, accuracy, and security of academic records. As a forward-thinking registrar, they champion an "extended transcript" concept that goes beyond traditional course grades and encompasses additional information on learner competencies. This includes not only academic achievements but also relevant work experiences and marketable non-educational skills. At the request of students, the registrar issues a digital credential that incorporates the extended transcript, providing a comprehensive representation of their qualifications. The credential may be used for a variety of scenarios including employment applications.

Finance KYC Use/Reuse

Alex wants to open a bank account. As part of the process, the bank asks her to provide two pieces of information to confirm her identity, as part of the **Know Your Customer (KYC)** check. Alex selects government-issued verifiable credentials that confirms residence at a specified address and citizenship of a specified country. The bank verifies these credentials and opens an account. The bank issues a credential to Alex which can be used to securely perform account transactions.

Alex can use the same verifiable credentials to open accounts at other banks, without having to provide the same information again, providing greater convenience. Instead, Alex uses the credential just issued by the bank. The use of verifiable credentials in this way helps enhance trust, convenience, and onboarding efficiency between banks and customers. [13]

Purchases Requiring Proof of Age

Riley goes to the Tipsy Taps liquor store to purchase a bottle of wine. They present their identity credential, which allows the liquor store owner to verify that they are of legal drinking age without disclosing their actual date of birth, address, gender, or state ID number. The checker at the liquor store accepts the credential and proof of qualification because the credential is from an Issuer that is trusted.

Data Monetization

Jordan, a user of the platform, seeks financial compensation for sharing their demographic information. Through explicit permission settings, Jordan specifies that anonymized personal demographic data can be made available exclusively to organizations conducting research using such data. Additionally, Jordan has the ability to select which personal attributes are eligible for sharing. To ensure privacy, all data is anonymized, preventing any direct association with Jordan's identity. Following data accessibility, organizations can purchase access and utilize scanning and querying functions provided by the platform. Payments made by organizations requesting data are distributed back to platform users, with a portion directed to Jordan's cryptocurrency wallet. Based on the shared information, advertising companies may utilize Jordan's Decentralized Identifier (DID) to send targeted advertisements, as determined by Jordan's specified preferences. Notably, organizations solely possess access to the DID and are unaware of Jordan's personal identity. At any point, Jordan retains the option to opt out of data sharing.

Facilitation of Job Placement

FictiveSoft, a cutting-edge software company, has posted an open position online and they are receiving thousands of applications. Jamie has applied for the job. Unlike many applicants, Jamie has attached education credentials—college degree, additional specific software training, etc. issued by known verified credential Issuers; in this case, the university attended by Jamie. FictiveSoft evaluates these credentials automatically as they receive their application. Because their materials are verifiable and verified, Jamie's application is immediately forwarded as a viable candidate.

Switching Employers

Charlie, a medical doctor in the United States, possesses a collection of verifiable credentials containing claims regarding qualifications, education, continuing education accomplishments, and board certifications. These credentials are securely stored and managed exclusively by Charlie within the platform. When presented with a job opportunity from a different health provider network, Charlie can conveniently showcase all relevant claims from their verifiable credentials to the potential employer.

Online Class Certification

In online learning systems like Massive Open Online Course (MOOC), reliable participant identification is crucial for accurate evaluation and certification. A user, Pat, engages in an online course and undergoes a test. Prior to the test, Pat was requested to submit their credentials to verify their identity. Subsequently, the system generates a verifiable credential to Pat that contains the test results, thereby facilitating a reliable record of Pat's performance. The verifiable credential is available for presentation to other requesting parties if Pat choses to allow it.

Health Diagnostic Support

Instead of having a subset of personal medical information stored at many different health providers, a user can have all medical information accessible, in whole, from their identity portfolio. When interfacing with a health care provider, a user can share the needed information with the provider securely. The user can also revoke access to this information as needed. The user is in control of the data. Also, data analytics could be done on the user's health information, orchestrated by the user to assist in tracking health conditions, and for making recommendations.

Proof of AI Bot Legitimacy

In the realm of legitimate AI bots, establishing credibility and reputation involves ensuring that all digitally produced content is appropriately attributed. Legitimacy information includes crucial details such as authorship and ownership of the entities responsible for creating the content, as well as a performance rating within a specific domain of knowledge.

Jamie seeks an AI medical bot as a collaborative tool for symptom diagnosis. The selection process involves choosing from a pool of potential bots, with the requirement of requesting verifiable credentials from each bot. In this case, Jamie is specifically seeking medical bots specializing in allergy symptoms that have been verified by renowned health institutions specializing in allergies, including Johns Hopkins, Mayo Clinic, Columbia University, and UC San Francisco. By querying for bots with credentials tied to these esteemed institutions, Jamie aims to identify the most reputable bot. Once the bot with the highest reputation rating is identified, Jamie establishes a connection to proceed with obtaining medical advice specifically related to allergies.

Benefits of using the FISE Technologies SSI framework for these use cases

- All user profile and information data is in one place owned and managed by the individual
- Social graph transcends and is usable by all applications
- Organizations may perform data mining on shared anonymized data,defined by users, to extract profiles with specific desired characteristics for targeted sales and marketing via user-controlled data permissions and payments facilitated on the FISE Portal platform
- Statistics and Machine Learning (ML) algorithms is applied to anonymized data to determine population behaviors
- User-controlled data removes reliance on centralized intermediaries and authorities

VIII. Challenges and Limitations

Slowness of Decentralized Systems

Critics argue that the reliance on decentralized technologies in SSI systems results in decreased speed and efficiency compared to traditional centralized systems. This is due to the presence of numerous distributed nodes across the internet, potentially leading to increased latency in communication and slower response times. Such limitations can pose challenges to the widespread adoption of SSI, particularly in developing countries with limited access to high-speed internet. Furthermore, the verification process in SSI systems is dependent on decentralized systems, which are currently slower compared to traditional, centralized systems. In an SSI system, verifiable credentials undergo cryptographic signing and verification by multiple parties to ensure their validity. This multi-party verification process, a critical yet ignored cyber-security measure, takes longer than traditional centralized systems that disregard such cyber-security best practices.

Despite the potential for slower processing times and increased latency in SSI systems that rely on decentralized technologies, **the benefits of increased security, privacy, and user control over personal data outweigh these potential drawbacks**.

Traditional identity systems are often centralized and rely on a single entity to store and manage user data. Despite there being Cloud technology in the implementation, a single, or a few entry points into the system creates a single point of failure vulnerable to cyber attacks and data breaches. If exploited, access to an entire large system can be shut down. **In contrast, decentralized SSI systems distribute data across a network of coordinating nodes, making them more resilient to attacks and harder to compromise**.

As decentralized technologies continue to evolve and become more efficient, the potential drawbacks of slower processing times and increased latency in SSI systems are likely to diminish. For example, the use of blockchain layer-2 scaling solutions, or swarm connection in IPFS [14] reduce latency and increase processing times for decentralized networks. Adoption of **Content Delivery Networks (CDN)** to cache data content from distributed storage significantly improves speed. This is already implemented by Fleek [15] and others. These and other innovations improve the speed, scalability, and performance, making SSI infrastructure competitive to centralized networks with regard to hosting real-time applications.

Reliance on Verifiable Credentials (VCs)

The reliance on verifiable credentials assumes that Issuers of credentials are trustworthy and reliable, which may not always be the case. It is also challenging to establish a universally accepted standard for verifiable credentials. Lack of VC standardization leads to fragmentation and lack of interoperability.

Nevertheless, FISE Portal's SSI platform will standardize foundational processes that are critical to the baseline functions of SSI systems, thereby standardizing security and trust in the credential issuance process. Verifiable credentials can be cryptographically signed, encrypted, and stored on a decentralized network of nodes, making it time-consuming and impractical for thieves to tamper with or forge.

An immutable record of credential issuance can be stored on a blockchain and ensures that only authorized Issuers can create and sign credentials. SSI systems provide mechanisms for revoking or invalidating credentials in case of compromise. This ensures that even if a credential is compromised or the Issuer is found to be untrustworthy, the credential can be quickly revoked, reducing the risk of misuse or exploitation [16].

A decentralized network of Validators and Verifiers ensures the validity of a verifiable credential (VC) by proving that multiple parties have independently verified the VC. This provides a higher degree of assurance that the credential is authentic. Records of valid or invalid verifications of an individual's credentials can be tracked to identify potential misuse, fraud, or counterfeiting of credentials.

Fear of Cryptocurrencies

Cryptocurrencies have been criticized for their volatility, lack of regulation, and association with illicit activities. These concerns are not unique to cryptocurrencies. Fiat currencies throughout history all have the same distasteful attributes. Issues are often addressed through measures such as improved regulation, and enhanced security protocols. The benefits of using cryptocurrencies in self-sovereign identity systems, such as greater security, privacy, and control, outweigh the potential risks. As more users become familiar with cryptocurrencies and their benefits, and as mathematical contracts open for review continue to evolve, the adoption of cryptocurrencies in self-sovereign identity systems is likely to increase.

Decentralized Storage

While concerns about data privacy and security with decentralized data storage are valid, it is important to remember the numerous instances of data breaches, security issues, and loss of personal data in centralized cloud systems. The Facebook Cambridge Analytica data scandal is just one prominent example [17] along with many others showing up in the media on a regular basis. Decentralized storage systems are often more resistant to data breaches and cyber-attacks, as they are less susceptible to single points of failure and are designed to provide greater control and ownership over personal data. While no system is completely foolproof, the use of decentralized storage with encryption and additional security measures provide a more secure and privacy-enhancing alternative to centralized data storage.

Ease of Use

Many of the technologies employed in a self-sovereign identity system are not familiar to an average internet user. Complexity of using these systems is a barrier to entry and adoption. Some of the difficulties users encounter while navigating a user interface for a self-sovereign identity system include:

- *Lack of familiarity with decentralized technologies*: Many users are not familiar with how decentralized technologies work, such as blockchain and distributed storage. This makes it difficult for them to understand where and how their data is stored and whether or not it is secured properly, and safe from misuse.
- *Complexity of verifiable credentials*: Verifiable credentials are a complex concept. They are digital documents that contain information about a user, which is straightforward. However, the complexity of the credential life-cycle makes it difficult for users to understand how to create, manage, and use them.
- *Lack of understanding of how to work with decentralized* IDs: Decentralized IDs are a relatively new technology, and there is a lack of understanding on how to work with them.

Much of what is now unfamiliar can become familiar and more efficient using good UI design principles. Using good design, most of the technical implementation details are encapsulated away from a user to make actions less confusing. A few of the core principles to use are:

- *Step-by-step instructions*: Step-by-step instructions are used to guide users through the process of using a self-sovereign identity platform. Wizard-based instructions, for example, show users how to obtain a new verifiable credential, how to add a verifiable credential to their self-sovereign identity portfolio, and how to share a verifiable credential with another user.
- *Clear and concise language*: The user interface uses clear and concise language to explain complex concepts. For example, the user interface avoids using jargon or technical terms that users may not be familiar with.
- *Use progressive disclosure*: Reveal more information and options as users need them. This helps reduce cognitive load and improves the user's experience.
- *Use familiar concepts*: File system management has been common for a long time in computers. The same paradigm is used in the FISE Portal platform to represent the data a user owns and manages in decentralized storage. An address book is used to manage all user-validated entities.

IX. Advantages or benefits:

These are some highlighted advantages and benefits of the proposed solution, and how they are superior to existing solutions or approaches.

Selective disclosure with verifiable credentials

In today's identity systems, when sharing personal information, too much information about a person is handed over to the requestor, despite the requestor not needing to see or use all of a user's **Personally Identifiable Information (PII)**. In addition, the requestor usually stores the PII information in a local database. This creates an undesirable copy of personal information that the user has no control over.

In the FISE Technologies platform, FISE Portal, users manage issued verifiable credentials. When sharing specific claims from a verifiable credential, users select specific attributes within the credential for presentation to a Verifier. Only information needed by a Verifier is shared. Unnecessary PII is not included. The

Verifier does not store a duplicate copy. The Verifier system or service only needs to know that at the time of interaction, a user of the system has or meets the desired qualifications.

Decentralized Datastores

Centralized databases are a common way to store data today. However, they have a number of drawbacks, including:

- *Single point of failure*: If the central server goes down, all of the data or access to all data is lost. Even if a database is clustered, it is still under the management of one controller party. If the party mismanages the database or if they decide to terminate the business, there is typically no recourse for a user to request actionable control about what is done with their personal data.
- *Security risks*: Centralized databases are a target for hackers, as they contain a large amount of sensitive PII data. Everyone relies on the party managing the PII data to provide security on their behalf.
- *Privacy concerns*: Centralized databases are used to track user activities and collect personal data, some of which may be considered PII. It is a well known, verified fact that large corporations and governments regularly track user activities and correlate these activities with users' PII data.

The FISE Technologies platform, FISE Portal, utilizes decentralized storage to address the limitations associated with centralized databases. In decentralized storage, data is distributed across a network of nodes instead of being confined to a single server or controlled isolated network managed by a single corporation. These distributed nodes are overseen by various entities. All the data stored on these nodes is encrypted, significantly increasing the difficulty for hackers to compromise and extract information. Decentralized storage also empowers users with greater control over their data, as they have direct access and full authority and autonomy over their stored information.

As decentralized storage technology matures, many centralized databases will become less and less necessary. Utilizing decentralized storage on the platform offers advantages over centralized storage, including:

- *Resilience*: Decentralized storage is more resilient to outages, as there is no single point of failure.
- *Security*: Decentralized storage is more secure, as it is more difficult for hackers to attack.
- *Privacy*: Decentralized storage offers more privacy, as users have more control over their data.

Users are in Control of Their Own Identity
With the proposed FISE Technologies platform, FISE Portal, current identity providers will no longer need to store individuals' personal information. Many cybersecurity breaches have shown plenty of evidence that centralized storage continues to be compromised, exposed, or misused by large corporations, bad insider actors, and malicious hackers. In contrast, FISE Portal's Decentralized IDs (DIDs) are stored on peered nodes in decentralized storage to ensure persistence of identity information and reliability of access. Users are able to create and manage multiple identities within the platform, providing new capabilities to share diverse aspects of a whole identity in different contexts.

Privacy Improves
The implementation of the FISE Technologies SSI platform, FISE Portal, automates encryption, digital signatures, and decentralized storage, resulting in better default privacy when compared to non-SSI, centralized web-based systems. Through data encryption for privacy, digital signatures for integrity, decentralized storage for resilience, and individual control over data sharing, the FISE Portal platform ensures that personal information remains secure, private, and under the sole control of the individual user.

X. Deployment:

Explanation of how the proposed solution can be deployed in practice.

Initially the platform will be deployed using a web front-end. This provides a platform-independent implementation for clients to use on any device supporting a web browser on any operating system, including Android OS, Apple IoS, Microsoft OS, Mac OS, and Linux. Information in a user's identity portfolio is conveniently managed on the front-end by the user. UI components on the client-side interface are responsive and self-organize according to defined styles and available screen real estate.

Users creating accounts on the platform are automatically assigned a unique decentralized ID (DID) and keys for use in identification, encrypting data, sharing data privately, and as the user's first identifier for all other verifiable credentials associated with the user. Users have the ability to manage IDs and keys; and by default, they are created automatically with no user interaction necessary. This helps with ease of use and becoming part of the SSI community.

Distributed storage is deployed across many existing public and private peered nodes utilizing libp2p protocols to find and store data files.

Both a registry of decentralized IDs and storage are maintained across a distributed network of peered nodes. The nodes are maintained by many possible organizations and individuals connected across the internet. In this manner, the resulting property of inherent trustlessness doesn't require users to trust any one party who may or may not act responsibly. This means that users can be confident that the system will operate and mitigate risk as expected (as risk and security are distributed), even if some of the participants maintaining nodes are malicious or dishonest.

A non-custodial cryptocurrency wallet, with a unique wallet address defined on the Ethereum blockchain, is issued after account signup. From FISE Portal's client-side interface, all standard wallet functions are available including send, receive, store, view balance, as well as encrypt and sign transactions.

XI. Roadmap and Future work

Once the core capabilities of the platform have solidified, future efforts will concentrate on the seamless integration of SSI applications, including DApps, which will be developed on the FISE Portal platform. More integrations will include verifiable credential Issuers interacting through the FISE Portal enterprise platform, concurrent with implementations of advanced functions such as audits.

To ensure long-term stability, FISE Technologies actively fosters collaboration with organizations whose core developments run FISE Portal's decentralized platform processes. Lastly, FISE Technologies actively pursues synergistic collaboration with organizations interested in building SSI applications such as DApps on the FISE Portal platform, aiming to continually expand the repertoire of available SSI capabilities for users.

XII. Conclusion

Self-sovereign identity (SSI) is a powerful concept enabling individuals to retain full control over their personal data and finances. It also provides mechanisms to establish provable and verifiable trust between parties. Building SSI applications requires the following foundational pillars. [18]

- **Decentralized storage**: Decentralized storage is important for SSI because it allows users to securely store their personal data on a network of computers, rather than on a single server. This makes it more difficult for anyone to access or control the data, and it also makes it more difficult for anyone to delete or modify the data.
- **Decentralized IDs**: Decentralized IDs are important for SSI because they allow users to control their own identity information. This means that users can choose what information they share with others, and they can also revoke access to their information at any time.
- **Verifiable credentials**: Verifiable credentials are important for SSI because they allow users to share their identity information with others in a secure and verifiable way. This means that users can be confident that the information they are sharing is accurate and up-to-date, and it also means that others can be confident that the information is coming from the correct person.
- **Interoperability with cryptocurrency**: Interoperability with cryptocurrency is important for SSI because it allows users to pay for services and goods without having to provide sensitive PII connected to banking or credit card information. The cryptocurrency wallet helps to protect user privacy and security, making it easier for users to participate in the digital economy.

In addition to these architectural pillars, good UI design is also important for SSI. A good UI is easy to use and understand, and it supports secure operations. A good UI helps make SSI more accessible to a wider range of users, and it helps protect user privacy and security.

The design of the FISE Technologies platform, FISE Portal, focuses on implementing core features facilitating the development of user-friendly SSI-respecting applications. The FISE Technologies platform and framework are a stable, secure, and standardized alternative to building SSI-imitation applications in custodial, centralized, siloed environments. SSI-imitation applications are marketed as decentralized or Web3+ on the front end, but lack actual decentralized back-end infrastructure and respect for users' self sovereignty over their digital identity and data.

Developers often find themselves immersed in the development of isolated SSI-imitation applications, which have failed to captivate mass user adoption. The phenomenon of one-off, disparate, non-standardized developments of SSI-imitation applications, and their corresponding failure to inspire mass adoption reveals what is missing—an SSI framework executed by FISE technologies' FISE Portal platform that enables standardization, organization, and interoperability for applications built with user-centric digital self-sovereignty in mind.

To address these critical gaps, FISE Technologies' groundbreaking platform, FISE Portal, provides the foundational infrastructure for truly decentralized SSI applications that empower and facilitate users' digital self-sovereignty. By seamlessly integrating the core SSI components of decentralized ID management, robust decentralized storage solutions, verifiable credentials, and cryptocurrency wallet, FISE Portal empowers developers to streamline the rapid deployment of cutting-edge decentralized SSI applications. Within FISE Portal's secure, non-custodial environment, access to authenticated, permissioned identity portfolios are readily available, building trust and confidence for users, corporations, and entities to explore the immense utility offered by these transformative applications.

No one has yet developed an SSI platform in a way that enables seamless collaboration among other SSI applications. Most of the existing SSI applications are built independently, leading to challenges in data sharing. This lack of interoperability poses a significant barrier to mass adoption of SSI.

FISE Technologies is building a secure, decentralized, and user-friendly SSI system that empowers individuals to take control of their personal data and finances by implementing the architectural pillars and supporting concepts described within this white paper.

The FISE Technologies platform, FISE Portal, as presented in this paper, represents a foundational, innovative advancement in SSI adoption, paving the way for seamless adaptation and unparalleled interoperability. With its comprehensive support for a multitude of SSI applications and enhanced capabilities, it revolutionizes the landscape for individuals and entities alike. By harnessing the power of the FISE Portal platform, SSI becomes effortlessly accessible to all, unlocking its true potential and ushering in a new era of limitless possibilities.

References

[1] https://www.aarp.org/money/scams-fraud/info-2022/javelin-report.html

[2] https://www.zdnet.com/article/the-biggest-data-breaches-of-2021/

[3] https://www.wired.com/story/lastpass-breach-vaults-password-managers/

[4]https://www.infoworld.com/article/2654678/the-hidden-challenges-of-federated-identity.html

[5] https://www.dock.io/post/self-sovereign-identity

[6] https://blog.ipfs.tech/2023-ipfs-unresponsive-nodes/

[7] 'A Tutorial on the Interoperability of Self-sovereign Identities'
arXiv:2208.04692v1 [cs.SE] 8 Aug 2022

[8] https://www.w3.org/TR/did-core/

[9] https://eips.ethereum.org/EIPS/eip-2844?ref=blog.ceramic.network

[10]https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/KERI_WP_2.x.web.pdf

[11] https://en.wikipedia.org/wiki/GraphQL

[12] https://identitywoman.net/wallets-cant-be-the-adapters-between-credential-formats/

[13] https://www.w3.org/TR/vc-use-cases/

[14]https://medium.com/pinata/speeding-up-ipfs-pinning-through-swarm-connections-b509b1471986

[15] https://finbold.com/review/fleek-review/

[16]https://medium.com/mattr-global/adding-support-for-revocation-of-verifiable-credentials-2342b66b0997

[17]https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

[18]https://medium.com/@kevin.hartig/building-trust-in-the-digital-age-the-foundation-of-self-sovereign-identity-e470d60effc7