uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain

Nitin Naik¹ and Paul Jenkins²

¹School of Informatics and Digital Engineering, Aston University, United Kingdom
²Cardiff School of Technologies, Cardiff Metropolitan University, United Kingdom

Email: n.naik1@aston.ac.uk and pjenkins2@cardiffmet.ac.uk

Abstract—Managing identity across an ever-growing digital services landscape has become one of the most challenging tasks for security experts. Over the years, several Identity Management (IDM) systems were introduced and adopted to tackle with the growing demand of an identity. In this series, a recently emerging IDM system is Self-Sovereign Identity (SSI) which offers greater control and access to users regarding their identity. This distinctive feature of the SSI IDM system represents a major development towards the availability of sovereign identity to users. uPort is an emerging open-source identity management system providing sovereign identity to users, organisations, and other entities. As an emerging identity management system, it requires meticulous analysis of its architecture, working, operational services, efficiency, advantages and limitations. Therefore, this paper contributes towards achieving all of these objectives. Firstly, it presents the architecture and working of the uPort identity management system. Secondly, it develops a Decentralized Application (DApp) to demonstrate and evaluate its operational services and efficiency. Finally, based on the developed DApp and experimental analysis, it presents the advantages and limitations of the uPort identity management system.

Index Terms—Self-Sovereign Identity; SSI; Identity Management System; IDM; uPort; Decentralized App; DApp; Decentralized IDentifier; DID; Verifiable Credential; Distributed Ledger; Blockchain; Ethereum; User-Centric Data Platform.

I. INTRODUCTION

A digital identity is a set of attributes used to identify a particular user in order to gain access to resources and services in the digital world. This identity management process has been organised using a dedicated system called Identity Management (IDM), which is continuously evolving to fulfil the requirements of this domain. Originally, Centralised IDM systems reliant on a central authority were designed to provide services to small and closed environments [1]. This IDM was generally limited to an organisation and requires a separate identity for each organisation [2]. In this IDM, there was no inter-organisation accessibility available for the global interconnection, which led to the development of a new IDM model called Federated IDM system [3], wherein, an IDentity Provider (IDP) was responsible for managing an identity to provide single sign-on for many organisations by establishing the trust relationship [4]. However, this IDM system had some issues such as the control of an identity was still not with the user and the user details were stored at the identity provider [5]. This led to the development of a user-centric identity management system called Self-Sovereign IDM system, which replaced the traditional central authority with a distributed ledger and offered overall control of an identity and its related data to the user.

The uPort system is an open-source identity management system for providing self-sovereign identity to users, organisations, and entities. A uPort identity is a simple smart contract on Ethereum blockchain for digital representation of a user, organisation, or entity in order to make assertions relating to their identity when interacting with other smart contracts on-chain or off-chain [6]. This capability to make claims about themselves, without relying on centralized identity providers, fulfils the biggest requirement of a self-sovereign identity. A smart contract is a piece of code that resides at a specific address on the Ethereum blockchain and runs to control valuable items such as Ethereum currency ETH or other digital assets [7], [8].

In public key cryptography based identity management systems, public keys are used to represent identities and the ownership of an identity is determined by possession of the private key that controls the public key. The principal concern with this system is that the loss of a private key means the loss of an identity. The uPort system resolves this cryptographic key management issue using blockchain as an identity certification authority where a smart contract represents the digital identity of a user. These smart contracts can be controlled by other smart contracts, therefore, they can be utilised to recover user’s keys [6].

The uPort identity management system is still evolving as a self-sovereign identity platform and offers several identity services. As an emerging identity management system, it requires meticulous analysis of its architecture, working operational services, efficiency, advantages and limitations. Therefore, this paper contributes to these aims by examining all of these objectives. Firstly, it presents the architecture and working of the uPort identity management system. Secondly, it develops a Decentralized Application (DApp) to demonstrate and evaluate its operational services and efficiency through
three underlying IDM operations: login/connecting with uPort Mobile App, creating and issuing credentials, and requesting and verifying credentials. Finally, based on the developed DApp and experimental analysis, it present the advantages and limitations of the uPort identity management system.

The rest of the paper is structured as follows: Section II explains about self-sovereign identity. Section III explains components and working of uPort identity management system. Section IV presents the development of a DApp for uPort to demonstrate and evaluate their operational services and efficiency. Section V presents the analysis of operational services and efficiency of uPort identity management system. Section VI presents advantages and limitations of uPort identity management system. Section VII presents the summary of the paper and related future work.

II. BACKGROUND: SELF-SOVEREIGN IDENTITY (SSI)

Self-sovereign identity (SSI) is a sovereign, enduring and portable identity for any person, organization, or body, that allows its owner to access all relevant digital services by utilising verifiable credentials linked to the identity in a privacy-preserving manner. The ecosystem of self-sovereign identity is illustrated in Fig. 1. It has three main roles Issuer, Holder and Verifier. An issuer creates and issues credentials to a holder. A holder receives credentials from an issuer, retains it and when it is required, it shares credentials with a verifier. A verifier receives and verifies credentials presented by a holder. This self-sovereign identity is an emerging model of an identity which offers several essential features for a sovereign identity without dependence on any external administrative authority:

- An identity owner should be the sole owner of the identity with full control over its use and attributes.
- An identity owner should be able to decide the type of identity data used to define their identity.
- An identity owner should be able to perform all the operations related to its identity and personal data or assign control of such functions on its behalf.
- An identity owner should be able to use its identity as long as it wishes and its identity cannot be revoked or removed by anyone else.

Self-sovereign identity is unique from preceding identity models in a way that it employs new standards such as Decentralized IDentifier (DID) and Verifiable Credentials (VC) based on blockchain/distributed ledger to create a cryptographically verifiable digital identity that is fully governed by its owner [9], [10].

From the beginning of the identity management technology, there has not been a universally unique identifier which could be used as a standard interoperable identifier, consequently, each employer or service provider had been required to create their own. Circumventing this issue, SSI has offered a universally unique identifier called Decentralized IDentifier (DID). The DID is a permanent, universally unique identifier and cannot be taken away from its owner who owns the associated private key, which is completely different from other ephemeral identifiers such as a mobile number, IP address and domain name [9]. Only public DIDs alongside some other public credentials selected by DID owners could be stored on the blockchain/distributed ledger (or off-blockchain/off-ledger) in the form a DID document. This does not include private DIDs and identity related personal and confidential data and therefore, these are not stored on the blockchain alternatively it is maintained on the storage (e.g., digital wallet) of an identity owner or agent. The DID document is normally governed by the identity owner through holding its associated private key.

A claim is an assertion made relating to any entity. A credential is a group of claims used by any entity to prove their identity. A Verifiable Credential (VC) is verifiable through a signature or evidence supplied by an issuer who has either issued the VC or can confirm its correctness. A VC is used to represent similar information on the Web to that of a physical credential in the real world. The verifiable credentials should be linked with an identity through its unique identifier such as a DID.

Self-sovereign identity allows identity owners to control their identity related confidential data and retain on storage owned or controlled by them. Generally, this data is stored in a digital wallet, which is analogous to a physical wallet which keeps all digital credentials as physical entities, however, digital credentials in the digital wallet are digitally signed, verifiable credentials and much faster to issue and verify than their physical counterparts. This means a user can control what to share with other organisations. The user can share an entire credential, part of a credential (known as claim), or Zero-Knowledge Proofs (ZKPs) acquired from a credential [1]. The encrypted and persistent connection is established to transmit digital credentials securely and privately. The trust relationship between organisation and user is maintained through blockchain (see Fig. 1). The verifier verifies the digital signatures on received credentials using an underlying blockchain.

III. uPORT OPEN-SOURCE IDENTITY MANAGEMENT SYSTEM

uPort is an open-source framework for delivering a decentralized identity for a self-sovereign identity [11]. It is based on the public permissionless blockchain Ethereum and utilises its smart contracts [12]. A smart contract is a program written to automatically observe, accomplish and implement an agreement. Employing this framework, users can securely publish their identity including transferring their credentials, sign transactions and control their keys and data. A uPort
identity can be created for users, organisations, and other resources. The identity is completely owned and governed by the owner of that identity and not by the third-party. Additionally, all identity related personal and confidential data is held by the owner in their digital wallet thus, information releases are kept to a minimum [13]. The components and working of the uPort identity management system are as follows [6], [12], [14]:

A. Components of uPort

There are several components in the uPort identity management system. Here some of the most important components (see Fig. 2) are explained:

1) Smart Contract Components:

   **Controller Contract:** It is the overall control logic with the functionality of controlling the access to the proxy contract. Furthermore, it allows the user to reclaim their identity if the user loses their mobile and private key. It maintains a list of recovery delegates (e.g. selected family members, friends or institutions) who can assist the user to regain their uPort identity.

   **Proxy Contract:** It is the permanent identifier of a user linked with the private key of the user, therefore, it allows the user to replace their private key without affecting their permanent identity.

   **Registry Contract:** It offers a cryptographic link between a uPort identifier and its data attributes or profile data stored off-blockchain (e.g. InterPlanetary File System (IPFS)). IPFS is a peer-to-peer protocol for storing and retrieving data on a distributed file system. The proxy contract can only update the Registry contract.

2) Server Components:

   **Chasqui:** The Message Server manages all aspects of communications with any decentralized app and mobile app.

   **Sensui:** The Gas Fuelling Server avoids the requirement of a new Ethereum user to purchase Ether and paying fees to use the network. It pays the gas fees for the new user allowing them to create a new uPort account instantly.

   **Infura Ethereum RPC:** This Infura API provides a standard RPC interface to allow uPort to communicate with the Ethereum network.

   **Infura IPFS:** This Infura API provides a standard interface to allow uPort to communicate with the IPFS network.

B. Working of uPort

In the uPort identity management system, any user/app can interact with any application contract for identity related information. However, this process involves two main contracts a proxy contract which is a universal and permanent identifier for a user, and a controller contract which is the main controlling program. The app interacts with the proxy contract through the controller contract which passes a request to the corresponding application, the smart contract. As a permanent identifier on the ledger, the proxy contract interacts with all application contracts and creates a layer between user’s private key (in the digital wallet) and application contracts. uPort requires standard RPC interface provided by Infura to communicate with the Ethereum network. A user can send a transaction without having any Ether in their sending account, by sending it to the Sensui server which then supplies adequate Ether to pay the transaction fee. The uPort identity related data attributes or profile data can be stored off-ledger (e.g. IPFS, Dropbox, OneDrive, GoogleDrive). This can be accomplished by establishing a cryptographic link to an external data structure using a registry contract. However, the registry contract can only be updated by the proxy contract. This requires Infura IPFS interface for uPort to communicate with the IPFS network. This working of uPort identity management system is shown in Fig. 3.

IV. DEVELOPMENT OF A DAPP FOR uPORT IDENTITY MANAGEMENT SYSTEM TO DEMONSTRATE AND EVALUATE ITS OPERATIONAL SERVICES AND EFFICIENCY

To demonstrate and evaluate the operational services and efficiency of the uPort identity management system, a DApp called MyDApp was developed to interact with the uPort Mobile App [15]. Utilising this developed MyDApp, three underlying IDM operations were performed: login/connecting with uPort Mobile App, creating and issuing credentials, and
requesting and verifying credentials. Thus, analysing several operational aspects related to the uPort identity management system and uPort Mobile App. In the first login operation, MyDApp generates a QR Code and the uPort Mobile App scans this code to connect with MyDApp as shown in Fig. 4. Once MyDApp is connected with uPort Mobile App, MyDApp generates a credential and sends it to uPort Mobile App, when the credential is accepted then it is stored in the Digital Wallet on the mobile device as shown in Fig. 5. This is one of the enhancements in SSI where all credentials are stored in the Digital Wallet on the users device. This MyDApp is used for both purposes creating and issuing credential, and requesting and verifying credential. Therefore, using MyDApp, the credential can be sent to the verifier for its verification to obtain its services, which is demonstrated here as shown in Fig. 6. In summary, the three important IDM operations were performed using MyDApp to reflect and analyse the actual results based on experiments.

V. ANALYSING OPERATIONAL SERVICES AND EFFICIENCY OF uPORT IDENTITY MANAGEMENT SYSTEM

Based on the MyDApp experiments and empirical evidence, this section analyses the operational services and efficiency of the uPort identity management system to present its effectiveness and limitations. Table I illustrates an analysis of uPort system based on several important features related to identity management [10], [16], [17], [18]. The uPort identity management system is an open-source identity management system for offering decentralized self-sovereign identity which is built on public permissionless Ethereum blockchain. Presently, Ethereum blockchain is using a Proof of Work (PoW) consensus algorithm Ethash, which is not a very effective consensus algorithm, however, the upcoming Ethereum 2.0 will replace the PoW consensus algorithm with a more effective Proof of Stake (PoS) consensus algorithm. This analysis shows that uPort identity management system offers several important features related to identity and its management such as sovereignty, access control, storage control, recovery management, security, privacy, safeguard, user-friendliness, and cost-effectiveness, however, it offers no or limited support for several important commercial features such as availability, transparency, portability, interoperability, and governance in order to establish it as a commercial and successful SSI system [19]. As SSI is an emerging IDM model and uPort is an emerging identity management system, therefore, the successful implementation of these commercial and operational features require the development and adaptation of a set of common protocols and standards provided by standard organisations such as the Decentralized Identity Foundation (DIF), the World Wide Web Consortium (W3C) and the Organisation for the Advancement of Structured Information Standards (OASIS) [19]. Presently, the scalability feature is one of the important implementation issues for uPort, currently being resolved by employing various design optimisation techniques to fulfil the growing demands of sovereign identity globally.

VI. ADVANTAGES AND LIMITATIONS OF uPORT IDENTITY MANAGEMENT SYSTEM

After analysing operational services and efficiency of the uPort identity management system, this section will discuss some of the most common advantages and limitations of this uPort identity management system.

A. Advantages of uPort Identity Management System

The uPort identity management system is one of the first user-centric and open-source identity management system for self-sovereign identity, which offers several advantages:

- The joining process of uPort network is easy and frictionless and user can create multiple uPort identity without any cost.
- It offers user-centric sovereign identity with full control of its user.
- It offers password-less authentication and single sign-on functionality.
<table>
<thead>
<tr>
<th><strong>Operational Services and Efficiency</strong></th>
<th><strong>uPort Identity Management System</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Type</td>
<td>It is an open-source identity management system for offering decentralized self-sovereign identity.</td>
</tr>
<tr>
<td>Blockchain Type</td>
<td>It is built on Ethereum blockchain which is a public permission-less ledger for smart contracts. Smart contracts are utilised for decentralized self-sovereign identity.</td>
</tr>
<tr>
<td>Consensus Algorithm</td>
<td>Presently Ethereum blockchain is using a Proof of Work (PoW) consensus algorithm built specifically for the Ethereum blockchain called Ethash. The Ethash PoW algorithm introduces the property of Memory Hardness to the Ethereum blockchain. However, Ethereum 2.0 will use a Proof of Stake (PoS) consensus algorithm (e.g., Casper).</td>
</tr>
<tr>
<td>Identity Data</td>
<td>It allows user to store identity related personally identifiable information on the storage owned or controlled by the identity owner.</td>
</tr>
<tr>
<td>Access Control</td>
<td>It offers full control of identity and identity related personally identifiable information to its owner.</td>
</tr>
<tr>
<td>Tokenisation Process</td>
<td>It utilizes Ether as Gas within the Ethereum ecosystem.</td>
</tr>
<tr>
<td>Recovery Management</td>
<td>It offers social recovery method, where, Recovery Delegates (e.g. selected family members, friends or institutions) are nominated by an identity owner, who can assist the identity owner to regain its uPort identity.</td>
</tr>
<tr>
<td>Security</td>
<td>It requires credentials and biometry for controlling identity through blockchain. Users can securely publish their identity including transfer their credentials, sign transactions and control their keys and data.</td>
</tr>
<tr>
<td>Privacy and Consent</td>
<td>It is a Privacy Preserving. Users do not need to disclose personal data in order to create uPort identifiers for low value accounts. It uses various methods to minimize the correlation of a user’s on-chain smart contract interactions between different DApps.</td>
</tr>
<tr>
<td>Safeguard</td>
<td>It protects users’ right to privacy.</td>
</tr>
<tr>
<td>Scripting / Programming Language</td>
<td>Its underlying languages are: Solidity, C++, Python, Go, Rust, Scala.</td>
</tr>
<tr>
<td>User-Friendliness</td>
<td>It is based on a simple design architecture and easy to use mobile app. At present it has no provision of a Guardian/Agent.</td>
</tr>
<tr>
<td>Availability</td>
<td>It is available to all users through the use of smart-phones and offers a simple mobile app to manage their identity.</td>
</tr>
<tr>
<td>Transparency</td>
<td>It is based on open standards and open source projects.</td>
</tr>
<tr>
<td>Portability</td>
<td>It is limited, however, uPort is using several open standards to make it portable, e.g., Verifiable Credential (VC) and Decentralized IDentifier (DID).</td>
</tr>
<tr>
<td>Interoperability</td>
<td>Presently it is evolving, therefore, it requires a further alignment with other similar identity management systems.</td>
</tr>
<tr>
<td>Scalability</td>
<td>It is limited. At present, the public Ethereum blockchain can process nearly 15 transactions per second. It is resolving this by avoiding creation of multiple smart contracts on the blockchain and letting users to create Ethereum key pair.</td>
</tr>
<tr>
<td>Cost-Effectiveness</td>
<td>Presently identity is free for users, however, all transactions have an inherent cost. It introduces additional costs, as the public Ethereum blockchain requires expensive computational activity and Gas fees in order to add new transactions to the ledger.</td>
</tr>
<tr>
<td>Operational Efficiency</td>
<td>In this MyDApp based experiment, it performed satisfactorily, however, it is evolving and network load is increasing rapidly.</td>
</tr>
<tr>
<td>Governance</td>
<td>Presently it does not have a governance model.</td>
</tr>
<tr>
<td>Applications</td>
<td>Zug stadt/Government eServices; PWC; TrueProfile; LACChain; Onfido; ALASTRIA.</td>
</tr>
</tbody>
</table>
It offers easy-to-use data management and control functionality, where user stores, controls, and shares identity data.

The uPort Registry is a shared contract, however, the identity data stored by each identity is solely controlled by the uPort identity itself, which makes it impossible to censor or block.

It offers simplified user-centric key management functionality, where users hold their private keys at their devices and use social recovery methods by assigning recovery delegates of their choices.

It offers a user-friendly mobile app and interaction with blockchain apps.

It mostly complies with General Data Protection Regulation (GDPR) and privacy-preserving policy [20].

It offers uPort SDK to integrate uPort identity operations into mobile apps.

The uPort identity management system is an open-source identity management system and the code is open-source for anyone to use.

### B. Limitations of uPort Identity Management System

As uPort identity management system offers greater control and access to users for their identity on their mobile devices, however, this comes with some complexities and risks. Additionally, it is evolving therefore, the current uPort identity management system has some inherent limitations which may be overcome in future version. Here some of the limitations of the current uPort identity management system are:

- The private key that controls a uPort identity is stored only on the user’s mobile device and if it is compromised then identity and its related personal and confidential information could be compromised.
- The authentication process on the user’s mobile device is not completely secure.
- Recovery delegates could be at risk and become the subject of attack vectors as their own identity is connected to the user’s identity and may be traced on blockchain.
- The current Proof of Work (PoW) consensus algorithm Ethash for underlying Ethereum blockchain is not the most efficient algorithm. However, upcoming Ethereum 2.0 will replace this existing algorithm with an efficient Proof of Stake (PoS) consensus algorithm.
- Organisation’s own uPort network could be different in terms of services.
- Smart contracts are smaller in size with limited capacity.
- The identity attributes are encrypted, however, the analysis of their meta-data in JSON structure might provide some indications.
- The uPort identity management system offers limited portability, interoperability and scalability.
- Number of public repositories for the uPort identity management system are still limited.
- The uPort identity management system asserts that its basic identity management system will always be free to users, however, all transactions have involved an inherent cost.

### VII. Conclusion

This paper presented an in-depth assessment of an emerging uPort open-source identity management system. It performed an analysis of the architecture, working, operational services, efficiency, advantages and limitations of uPort identity management system. It demonstrated and evaluated uPort operational services and efficiency through the development of a DApp and experimental analysis. Finally, it presented the advantages and limitations of the uPort identity management system. In future, the security and privacy aspects of uPort identity management system would be analysed in detail. Furthermore, it is worthwhile performing comparative analysis of uPort identity management system with some other emerging SSI systems.

### REFERENCES


