Toronto Metropolitan University

Framework for Quantum Identity Wallet

By

Javaid Iqbal Zahid *, Dr. Alex Ferworn* and Dr. Fatima Hussain*

* Toronto Metropolitan University (Formerly, Ryerson University) Toronto, Canada

Agenda

- Introduction
- Objectives
- Proposed Quantum Identity Framework
- Implementation and Testbed
- Conclusion
- Q&A

Introduction

"The Internet was built without and identity layer. The Internet was built without a way to know who and what you are connecting to. This limits what we can do with it and exposes us to growing dangers. If we do nothing, we will face rapidly proliferating episodes of theft and deception that will cumulatively erode public trust in Internet."

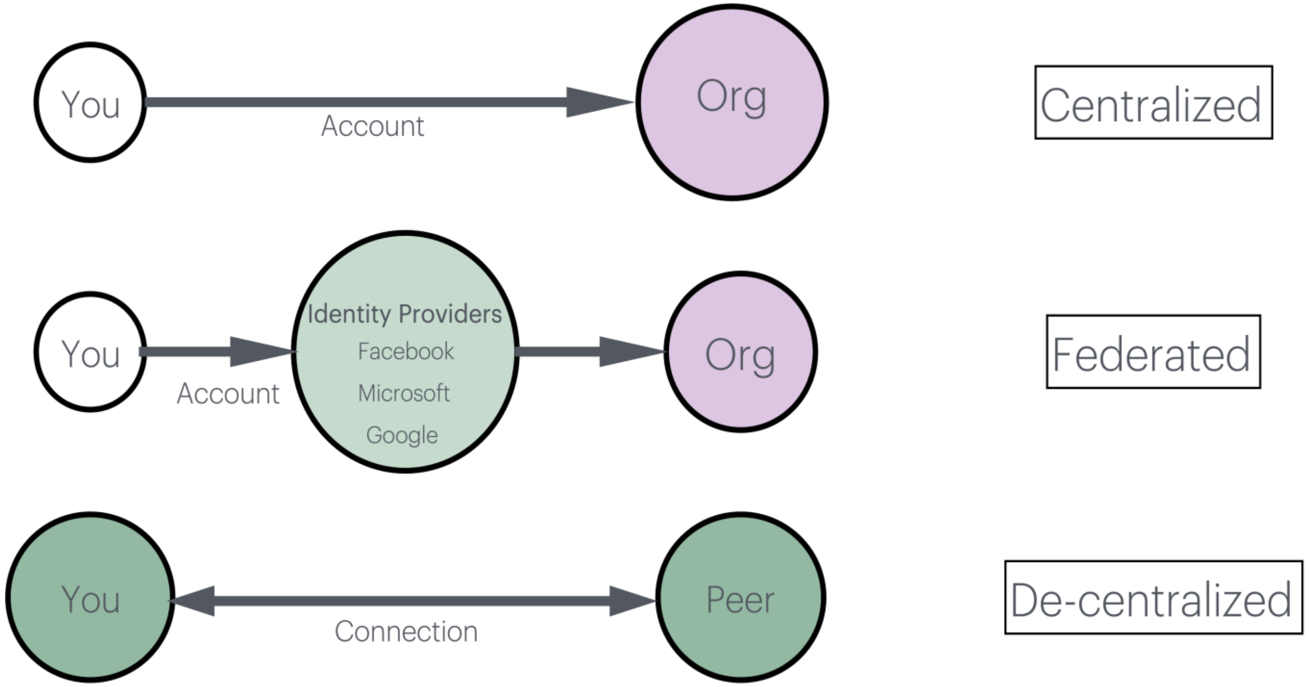
Kim Cameron — Microsoft
"The Laws of Identity", 2005 Identity Web log

Introduction (Models of Identity)

Centralized model is the commonly used model where you register an account with a website, service or application.

Federated model uses an identity service provider, called IDP (for example, Microsoft, Facebook, Google, etc.

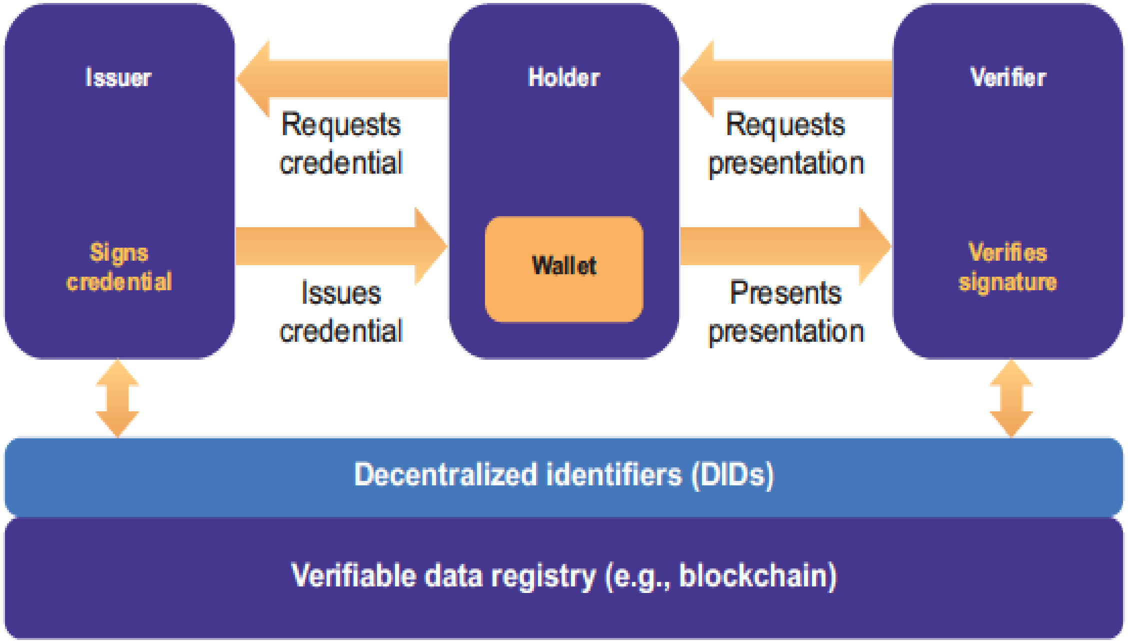
Decentralized model is a peer-to-peer network conceptualized from blockchain technology. Gives self control to each individual entity about its own identity information .



Source: Reference [1]

Introduction (roles of entities)

In SSI peer-to-peer network, three kinds of entities are involved: an issuer who provides identity information to a user (holder), for example, passport, Photo ID, birth certificate, etc. the user presents his/her identity information to a service provider when requested. A decentralized ledger can store DIDs of each entity in a verifiable data registry.

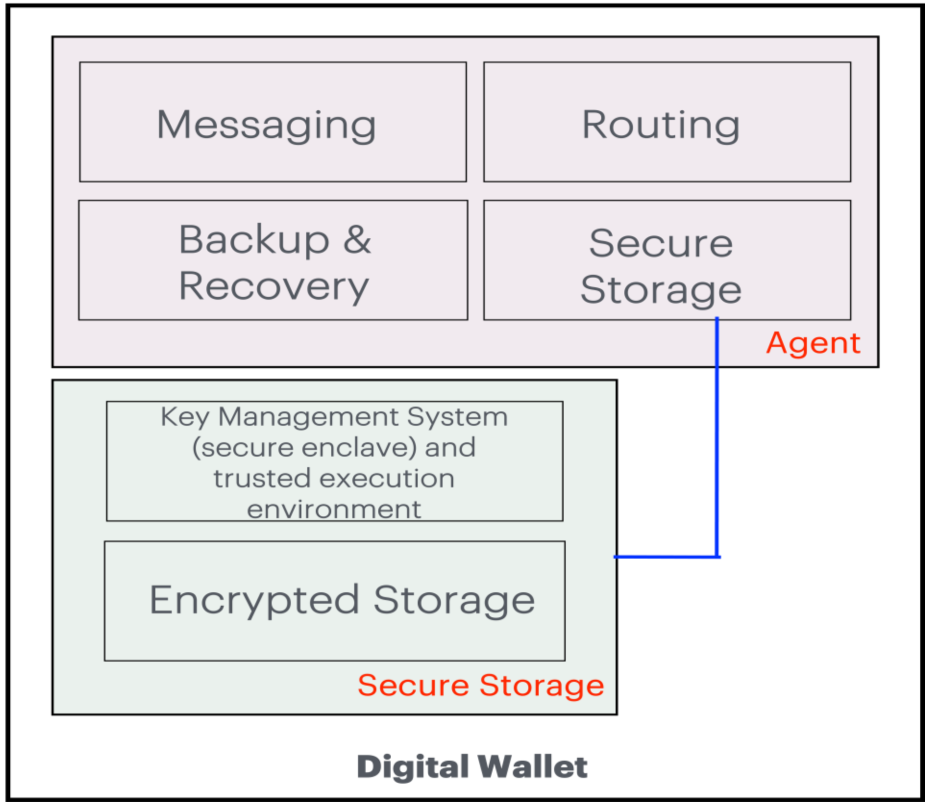


Source: Reference [1]

Role of Wallet and Agent

The digital wallet in an SSI ecosystem has pivotal role as it contains identification information, called verifiable credentials (VCs). It is equivalent our physical wallet. VCs are the digital equivalent of physical credentials that we carry in our physical wallets. VCs must be secured against theft or prying eyes. Wallet also contains cryptographic keys.

Digital agent is an application software enables secure communication between peers for presenting VCs to other peer agents.



Source: Reference [1]

Objectives

- The primary objective of proposed research on quantum digital identity wallet (QDIW) is to design an architecture and reference framework for promoting trusted digital identities that user can present to service providers, still exercising self-control on their private information. To achieve this, utilize the principles of quantum information processing [*2*]

- Self-sovereignty is provided by the SSI recommendation itself. However, the security is provided using public-key cryptography which is under treat from emerging quantum computing [*4*].

Specific Objectives

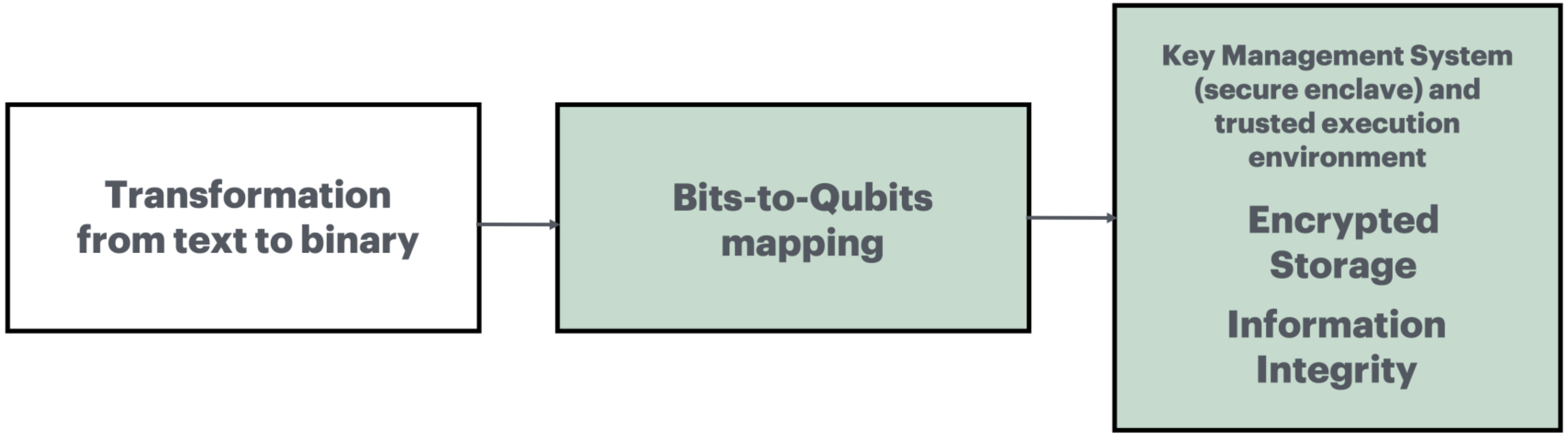
- Explore and examine proposals on digital identity wallets from national/international bodies with a view to draw technical and operational requirements of digital wallets.

- Develop architectural framework with use cases for prototyping the QDIW that will help in achieving self-control, security, and privacy

Proposed Quantum Identity Framework

We propose the following:

1. Create a structure of verifiable credentials (VCs).
2. Convert the structure into classical information units (bits).
3. Map the classical bits to quantum bits (qubits).
4. Develop a process (a set of quantum algorithms) to secure a store the qubits.
5. Develop a procedure to securely exchange VCs in a peer-to-peer connection.



Transformation from text to binary

Bits-to-Qubits mapping

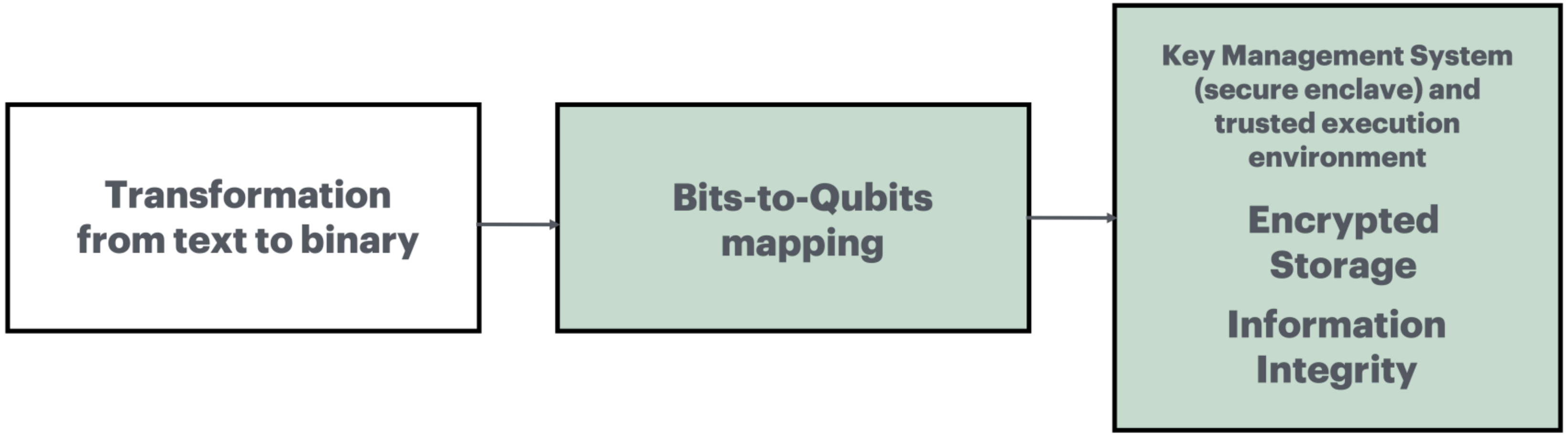
Key Management System (secure enclave) and trusted execution environment

Encrypted Storage

Information Integrity

Implementation and Testbed

We intend to develop a software application for realizing a prototype based on the proposal outlined in previous slide. In that, we will be using a development framework from IBM which is based on Python/Qiskit along with their cloud-based quantum computing hardware platform available publicly. The top-level view is shown in the figure below:


Transformation from text to binary
Bits-to-Qubits mapping
Key Management System (secure enclave) and trusted execution environment
Encrypted Storage
Information Integrity

Action Plan

Objectives	Description
Literature review on SSI	Comprehensive review of existing literature on SSI schemes (strengths and weaknesses), and quantum computing.
Identification and evaluation of relevant technologies	Selecting relevant and suitable quantum computing, communication, and cryptography approaches to implement the prototype of SSI
Development of a proof of concept (PoC)	Design and implementation of a prototype to prove the viability of QDIW framework.
Analysis of results from PoC	Analyzing effectiveness of our architecture based on the results from PoC
Assessment of social impact	Assessing the impact of technology on data privacy, protection of individual rights and other consequences

Conclusion

SSI, as a distributed and peer-to-peer network, provides a new model for identification and verification of entities on the Internet to provide/avail various services. Verifiable credentials (VCs), digital wallets and agents, decentralized identifiers (DIDs), verifiable data registries, and appropriate governing framework form the SSI ecosystem. However, vulnerability of public-key cryptography to quantum attacks makes the current implementations useless. Hence, an early research to enhance the security of private information is the call of the day. Our proposal is a step towards achieving this goal. In our proposal, we provide a framework for implementing a secure digital wallet that stores verifiable credentials using principles of quantum computing.

References

[1] A. Preukschat and D. Reed, Self-Sovereign Identity. Manning PublishingCo., 2021.

[2] M. A. Nielsen and I. L. Chuang, Quantum Computing and Quantum Information. Cambridge University Press, 2010.

[3] A. S. R. L. Rivest and L. Adleman, “A method for obtaining digital signatures and public key cryptosystem,” in Communications of the ACM, vol. 21, no. 2, 1978, pp. 120–126.

[4] P. W. Shor, “Polynomial-time algorithm for prime factorization and discrete logarithms on a quantum computer,” in SIAM Journal in Computing, vol. 26, no. 5, October 1997, pp. 1488-1509

Q&A

Thank you!