Feasibility Study

Person Verification Digital Platform

07.08.2022

Feasibility Study

Group Number : 11

Title : Person Verification Digital Platform (PID 06)

Mentor : Dr. Thanuja Ambegoda

Team :

190239A - K. G. Akila Induranga

190241X - M. I. M. Ishad

190242C - W. G. Kasun Isuranga

Contributions :

- 190239A - Akila Induranga
  - Financial Feasibility
  - Risk Feasibility
  - Social / Legal Feasibility
- 190241X - Mohamed Ishad
  - Technical Feasibility
  - Resource and Time Feasibility
- 190242C - Kasun Isuranga
  - Introduction
  - Considerations

Table of Contents

1. Introduction

1.1. Overview of the Project

Currently, users need to maintain different credentials to use various services and most services use a centralized storage system to store these credentials. This project aims to mitigate these issues by introducing a service that can be used by any third-party service provider. The solutions will also feature a decentralized storage system.

1.2. Objectives of the Project

The objective of this project is to implement a software solution that can verify a person's digital identity.

1.3. The Need for the Project

Currently, a user needs to maintain quite a number of credentials for different services he uses, creating the issue of maintaining a large number of credentials for the user.

Most credentials are stored in centralized storage systems. This creates a potential security vulnerability and limits a user's control over his or her credentials.

This project uses a decentralized storage system and the ability for third-party service providers to use the implemented software system to manage authorization.

1.4. Overview of Existing Systems and Technologies

Some existing digital identity verification systems are listed below.

- uPort
- Serto Suite
- Microsoft Entra Verified ID
- Digital-Identity using ERC 725/735 (Project on GitHub)

1.5. Scope of the Project

The project can be integrated into online service providers' web applications. The library will generate a QR code and scanning the QR code using the application provided will complete the verification process with the approval of the end user.

1.6. Deliverables

A demonstration application, a cross-platform application, and an integration library will be implemented in this project.

2. Feasibility Study

2.1. Financial Feasibility

It has been observed that the proposed project can address the financial aspect of the field in the following ways.

- **Traveling cost**

  As the users don't require to be physically present at the branch offices for any verification, it reduces the cost of traveling for himself, as well as for the authorized person at the branch sometimes. Because after the implementation of such a system, most of the jobs that the authorized officer is assigned can be done remotely, making him less likely to travel to the office daily.

- **Stationary cost**

  Since the early times of verifications, record keeping has been done either on books or organized file structures, both need a significant amount of stationery items such as books, papers, pens, ink, clips, and so on. However, it is highly unlikely that a record will be inspected again once verification is done. For a simple example when a person opens a bank account, once the application is filled, verified and the account is opened, the application may not be reviewed ever again, unless there is an extreme reason for a legal issue or so.

  This product reduces the stationery cost in big amounts and even if someone wants to review back the verification, it's a few seconds away and if it is not reviewed at all, it would only be a few kilobytes.

Although the project supports reducing the cost in above-mentioned manners, nothing comes for free. It has been identified that the following additional costs will have to be met by the system in order to make the product up and running.

- **Capital**

  In order to design and implement the system, the designers, developers, and testers need to be paid and other necessary subscriptions have to be bought for the supporting APIs and other services. This is a directly seen expense, even before the system is designed.

- **Maintenance cost**

  With the changing nature of expectations and requirements, developers are tied to the product even after deploying it and handing it over. Those specifically assigned maintainers will be charging for the service they provide after the deployment and other necessary charges (such as upgrading a subscription plan for an API) also need to be covered under the maintenance.

- **Transaction fees**

  In blockchain technology, there is always a hidden fee for transactions that are benign used by the users or smart contracts, called 'Gas Fees'. The client can decide how the gas fees will be allocated in the system (eg: Introducing annual subscriptions for users, or funded by the government if the client is a government organization). Either way, this indirect cost is there as an additional cost to be paid to have the decentralized nature of the system.

2.2. Technical Feasibility

Since users with various types of operating systems are likely to use the verification platform, the development of the application needs to target all the device types such as Android, IOS, Windows, Linux, and Mac. Developing each application separately is not feasible as it needs many developers for each platform.

So, It has been decided to develop the system with a cross-platform application development framework. It is feasible to use such a framework as many of them already exist with stable versions (not in beta or alpha stages) and a large developer community.

The most popular frameworks are,

- Flutter [1]
- React Native [2]
- Xamarin [3]
- Ionic [4]

All of these are open-source frameworks that are free. (Ionic and Xamarin have some limitations on free licenses). Flutter applications have almost native application performance. And applications built using other frameworks have low performance compared to Flutter applications.

Flutter is growing popular and backed by Google. So, it receives consistent updates and a growing developer community. Third-party packages are available for additional feature integrations. So, It is technically feasible to develop the application with the Flutter framework.

The third-party integration library is planned to be developed with JavaScript since almost every system can integrate into its systems. JavaScript has a range of npm packages that can be used to develop the library easily and efficiently.

It is planned to code smart contracts in Solidity and run in the Ethereum blockchain. Truffle suite [5] is there to develop smart contracts which can be tested with local blockchain. Ethereum test networks (ex:- Ropsten, Rinkeby) are available to test the system on large scale with free ether. So, nothing has to be implemented from scratch and it is capable of being completed.

2.3. Resource and Time Feasibility

As mentioned in 2.2, applications for all platforms can be developed with one code base. So, end-user applications can be developed within time constraints. For development and support, there are enough resources online. Packages for web3.0, QR code scanning, etc. are already implemented and available. [6]

For the development of the integration library already implemented npm packages are available. [7]. So, using them appropriately greatly reduces the time to be spent on coding.

Resources are somewhat limited in the domain of blockchain as it is an emerging technology. However, enough resources are available for this project scope. Truffle suite also provides tutorials [5] for developers.

StackOverflow [8] is a great forum connecting developers all over the world. Almost all questions posted there were answered quickly.

2.4. Risk Feasibility

Considering decentralized applications, they are designed to overcome the risks that occur with Web 2.0 applications. In the personal verification aspect, it is almost perfectly verifiable using the private wallet of the user. Although, as the Web 3.0

applications are still evolving, there are the following risks and vulnerabilities identified related to the proposed product.

- **Issuing the initial credentials**

  The proposed solution will use the email address and verify the email mechanism to issue/create the verifiable credential in the decentralized blockchain and store the private key in the user's wallet. This may be risky sometimes when a hacker gets access to a person's email, creates a verifiable credential for the first time, and acts as an identity thief in the digital person verification platform.

  To prevent such identity theft vulnerabilities, Issuing of the verifiable credential has to be moderated. One feasible way of doing this is allowing only the government, or an authorized institution to issue verifiable credentials to the users. It may seem like the system is getting centralized back again, but because the credentials are stored in the blockchain, even the issuer cannot tamper with the credentials after they are given to the client, guaranteeing the ownership to the end user.

- **Recovering lost/ stolen credentials**

  Because of the immutable nature of the blockchain, and its cryptographic key security, one instance of a verifiable credential can only be owned by one user (one private key), and the ownership cannot be transferred by anyone but the owner himself. Therefore if a user lost his private key to the credentials issued to him, there is no gaining them back again.

  Maybe the authorized credentials issuing institution can issue another credential to the user, but the logs of the lost credentials can never be owned by him.

  If the private keys got stolen it is like losing the wallet with the PIN number of the credit card. But in this case, since there is no trusted party like the bank, no one can revoke the credentials. Can only be notified as stolen.

2.5. Social/Legal Feasibility

It can be identified that the following social facts determine the feasibility of the proposed product in social aspects.

- **Potential users**

  Already quite a number of people use mobile/web-based applications to get their transactions done online like e-commerce, e-channeling services, etc. This product directly addresses them to make them feel more comfortable and secure in letting their personal details out online by using cryptographic hashes and decentralized servers (nodes). Also, the service providers (verifiers - institutes that need to get the people verified) will also love to have this mechanism implemented

because it creates a trustless, transparent environment which is a great strength to compete with other businesses.

- **Familiarity with technology for the users**

  Under the hood, the product will use the Ethereum blockchain technology with smart contracts. However, end users do not require any knowledge about such technologies. The simple cross-platform application is the only thing the users need to have, and the procedure will be intuitive and informative. Also, the verifiers will also be provided with a detailed API that can be integrated into their system very easily.

- **Social resistance**

  Still, the majority of the people outside the urban areas are less likely to use digital platforms in their daily lives. The traditional pen and paper applications and signatures still play a major role in personal verification. Therefore the social resistance will always be there to such a big change. But when considering the impact that can be held upon all the people, the change seems to be feasible in advance.

The laws related to the digital world/cyberspace are still being made throughout the world.

The most known regulation is The General Data Protection Regulation (EU) (GDPR), which applies to the European Union and European Economic Area.[9]

Sri Lanka is however currently in the process of enacting legislation for the purpose of protecting personal data. The Ministry of Digital Infrastructure and Information Technology of Sri Lanka initially introduced the first draft of the Personal Data Protection Bill in 2019 and it was approved by the Cabinet of Ministers of Sri Lanka and subsequently published in the Government Gazette. [10]

According to the above-mentioned act, any operation performed on personal data including collection, storage, preservation, alteration, retrieval, disclosure, transmission, making available, etc. has to take place wholly or partly within Sri Lanka. Which still makes the decentralized applications in Sri Lanka feasible.

3. Considerations

The major considerations when implementing the project are listed below.

- Security
- Usability
- Performance
- Modularity
- Decentralized verification data storage

- Security

As the software solution is used to provide identity and personal verification services to various services (Banks) including highly sensitive services, security can be identified as the most important aspect. The personal verification data stored in the app will also be guaranteed a high degree of security.

- Usability

The verification process will be made as simple as possible to improve usability. A person with basic day to day usage of the related platforms (Computers, Smartphones, and Web browsers) will be able to effectively use the software solution.

- Performance

The software solution will be designed to perform adequately in devices with low end specifications.

- Modularity

The software will contain three major components,

1. Smart contracts system
2. The app storing the verification data
3. The library to be used to implement the provided services in a third-party application

These systems will be decoupled to a high degree. Therefore, most modifications to any of the above-mentioned systems that preserve the interface requirements will not affect the functionality of the service. As such, any component can be therefore updated separately.

- Decentralized verification data storage

The verification data will be stored in each user's wallet rather than in a central database giving the users more control over their credentials.

4. References

[1] https://flutter.dev/

[2] https://reactnative.dev/

[3] https://dotnet.microsoft.com/en-us/apps/xamarin

[4] https://ionic.io/

[5] https://trufflesuite.com/

[6] https://pub.dev/

[7] https://www.npmjs.com/

[8] https://stackoverflow.com/

[9] https://www.gov.uk/data-protection

[10]

https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=LK