Computing and Information Technology
2022

Universitatea
Politehnica
Timișoara

Walman
A Virtual Wallet Management System

Candidate: David Daniel, Pava
Coordinator: Assoc. Prof. Razvan, Bogdan

Universitatea Politehnica Timișoara

ABSTRACT

Universitatea Politehnica Timișoara

CONTENTS

1 INTRODUCTION

1.1 CONTEXT

In the last 30 years, the number of tasks that are digitalized has increased exponentially. The most important part of the security systems of these tasks is user management and authentication. The password is the most widely spread form of user authentication and thus is often the prime target of attackers that want to impersonate someone else.

According to [2], a *"systematic literature review in the area of passwords and passwords security"*, there are many problems with password security and management ranging from weak passwords and password reuse, to users writing down passwords or sending them through unsecure channels. Most of these problems according to [2] are solved by using password recommendations. A good solution to most of these problems is a password management tool. A password manager is a piece of software designed for generating and managing passwords, in this way the user can have unique, complex and safely stored password without having to remember them.

Another great method to better secure you accounts is using a two factor authentication (2FA) method. These method vary from security questions, to one time passwords (OTP) sent from the server to the user via email or SMS, to OTPs generated using specialized algorithms such as: HMAC-based One Time Password (HOTP)[3] and Time Based One Time Password (TOTP)[4].

The cryptocurrency market is another area that has seen a considerable development lately. As of May 2022, the market cap of Bitcoin is around 565 billion USD, and the market cap of Ethereum is around 214 billion USD. In the case of Bitcoin, that is more than double of what it was in 2019 (around 211 billion USD), referenced in [1]. Cryptocurrencies also offer secure and long term storage capabilities thanks to the blockchain technology. Blockchain backups, thanks to the decentralized nature of the blockchain, are very hard to be tempered with. A traditional cloud backup could be lost or inaccessible in more than one situations. The most obvious one is data loss happening as result of a cyber attack or the company simply going bankrupt. There are also situations in which the company itself can refuse to serve you anymore. They can freeze your account or just refuse to serve an entire country all-together, we have the recent example of companies like Visa and Mastercard refusing to serve russian citizens as result of political tensions. All these scenarios cannot happen in a decentralized blockchain system.

Businesses that were traditionally not online like shopping also have inversely digitalized. Nowadays most of the hypermarkets offer fidelity cards. Usually these cards are built around a unique barcode or qr code. Often it's hard to manage all your cards, so a digital storage solution to solve this issue would help the end user better manage their cards.

Considered all mentioned above, a user has to remember and manage a lot of information in order to interact with the currently available online infrastructure. A tool that could help them manage all this data better is a wallet manager.

1.2 MOTIVATION

My personal motivation for creating a wallet manager is the fact that I want to use it myself. Also I wanted for a long time to explore the state of the art in smart contract development, so this was a great occasion to do so.

I chose to create this project in the form of a mobile application since people tend to have their smartphones with them most of the time, so having a virtual wallet on your mobile device makes sense.

Another factor that motivates me is the fact that currently in the mobile application market there are almost no free and open source password management applications available. The user needs to *trust* the creators of the application with their data, not knowing how the implementation of the product is made, they have no guarantee that the data is safe.

1.3 SIMILAR PRODUCTS AVAILABLE ON THE MARKET

There are a lot of password managers available on the market. In this section we are going to try to make a comparison between some of the most popular options available.

Property	**LastPass**	**RememBear**	**KeePass**	**PassMan**	**KeyBase**
Mobile Version	Yes	Yes	No	Yes	Yes
Blockchain Storage	No	No	No	No	Yes
Price	$3/month	$6/month	Free	Free	Free
License	Proprietary	Proprietary	GPL-2.0	AGPL-3.0	BSD-3

Table 1.1: A comparison between some of the most popular password managers.

First off we have LastPass and RememBear, two very similar password managers, both having a free and a payed plan. Neither of these two is open source, so the most pressing issue regarding them is the guarantee that your data is safe. Without having the ability to see how your data is managed and stored you cannot be certain that it is secure. Also these applications do not have blockchain backups.

KeePass is probably the most popular password manager for desktop. It is free and open source, and the code was analyzed and certified by specialized organizations such as the Open Source Initiative. The biggest drawback to KeePass is the aged user interface and the missing mobile application counterpart. Nowadays a lot of the situations where a user needs access to their credentials are happening while using smartphones. Also the features are limited, KeePass doing one thing and doing it well that being password management. There are no cloud or blockchain backups, so the user needs to manager backing up and storing their password database themselves.

Similar with KeePass, PassMan is a free and open source password manager. They have a mobile version of the application, but blockchain backups are missing. Also, again, PassMan is just a password manager. It does not manage shopping cards or crypto wallets.

Last but not least there is KeyBase which is not technically a password manager. KeyBase is a blockchain, decentralized, social media application. You can store password and secure notes inside the application but from the user experience point of view, KeyBase was never designed to be a password or wallet manager. The reason why it is mentioned, is because KeyBase is implemented on the blockchain, all user data is encrypted and it's free and open source.

2 TECHNOLOGY STACK

2.1 FRONTEND

2.1.1 Flutter

Flutter is a mobile application development framework developed by Google in the Dart programming language. It was released in May 2017 and it currently is one of the most popular mobile development frameworks.

2.1.2 Dart

2.1.3 Code Generation

2.1.4 Redux

2.2 FIREBASE

2.2.1 User Management

2.2.2 Firestore

2.3 BLOCKCHAIN

2.3.1 Ethereum

2.3.2 Smart Contracts

2.3.3 Solidity

2.3.4 Test Networks

2.4 DEVELOPMENT ENVIRONMENT

3 IMPLEMENTATION

3.1 USE CASES

3.2 SYSTEM ARCHITECTURE

3.3 PASSWORD MANAGEMENT

3.4 QR AND BARCODE MANAGEMENT

3.5 OTP AUTHENTICATOR

3.5.1 HOTP

3.5.2 TOTP

3.6 CRYPTOCURRENCY WALLET

3.7 BACKUP

3.7.1 Cloud Backup

3.7.2 Blockchain Backup

3.8 SECURITY

4 TESTS

4.1 TEST PIPELINE

4.2 UNIT TESTS

4.3 WIDGET TESTS

4.4 PERFORMANCE STATISTICS

5 CONCLUSIONS

5.1 POSSIBLE IMPROVEMENTS

BIBLIOGRAPHY

[1] Brooks Allen and Sarah K Bryant. The market for cryptocurrency: How will it evolve? *Global Economy Journal*, 19(03):1950019, 2019.

[2] Viktor Taneski, Marjan Heričko, and Boštjan Brumen. Systematic overview of password security problems. *Acta Polytechnica Hungarica*, 16(3):143–165, 2019.

[3] Mountain View, David M'Raihi, Frank Hoornaert, David Naccache, Mihir Bellare, and Ohad Ranen. HOTP: An HMAC-Based One-Time Password Algorithm. RFC 4226, December 2005.

[4] Mountain View, Johan Rydell, Mingliang Pei, and Salah Machani. TOTP: Time-Based One-Time Password Algorithm. RFC 6238, May 2011.