Computer Science Department

The University of Hong Kong

Final Year Project 2018-19

SECURE DIGITAL WALLET DESIGN

Name: Aditya Sethi

UID: 3035240063

Supervisor: Dr. J.T.H Yuen

Background

Cryptocurrency wallets are used to access, store, send or receive our digital currencies such as Bitcoin, Ethereum, Litecoin and much more which wouldn't be possible otherwise. Cryptocurrency wallet is a software programme that stores the owners private and public key. It is a link to various blockchains in the market and it allows the users to connect to these blockchains and perform different actions like checking wallet balance, sending or receiving cryptocurrencies.

Transactions

The most basic yet the most important feature of a wallet is that it lets you send or receive cryptocurrencies apart from the security it offers to the users to carry out such transactions. It is vital to understand how the wallets work with the blockchain before we start implementing the security features. The basic features will be the same for every wallet in the market. To understand how we can secure the wallet it is critical to understand how bitcoin transactions work in the first place. Let us take Alice and Bob in this example and let Alice be the sender and bob be the receiver. Both Alice and Bob will have a pair of private and public keys. For Alice to send the bitcoins to Bob the transaction will be signed my Alice's private key. It will be later verified using Alice's public key that the transaction was signed by Alice and not by anyone else. Now one of the key problems is to prevent an attacker from stealing the private key of the owner because if the private key gets compromised then anyone can use it to sign the transactions and send money to their own addresses.

Types of wallets

Every wallet revolves around the concept of storing and using private/public keys and based on that wallets can be classified into the following five types:

1. Web
2. Mobile
3. Desktop

4. Paper
5. Hardware

Web wallet

Web wallets are hot wallets because they are always connected to the internet. These wallets can be accessed via different browsers like Chrome or Firefox. Web wallets can be categorized into two types based on where the private keys are stored. Some web wallet providers store the private keys for the user while others give full custody to the owners. Some of the popular web wallets are BitGo, BTC.com and Coin.Space.

Mobile wallets

Mobile wallets are also the most used crypto wallets in the markets right now. They are also considered to be hot wallets as they are connected to the internet. They are popular because they are mobile-based and easy to use. But before considering using a mobile wallet one must be sure about the security features of the wallet. Some of the popular mobile wallets are Mycelium and Coinmi.

Desktop Wallets

Desktop wallets are wallets that can be installed on a machine and are compatible with operating systems such as Mac, Windows, Linux. These are standalone applications. Desktops are often connected to the internet which makes them more vulnerable to malware attacks. One must take the responsibility to take the basic security measures such as installing the antivirus and configuring the firewall to prevent the system from getting compromised. Some of the popular desktop wallets are Exodus, Electrum and Bitcoin Core.

Paper Wallets

Paper wallets are an offline mechanism for storing bitcoins. Paper wallets have your private keys and public addresses printed on them. Paper wallets are more secure than desktop, web or mobile wallets as they are not connected to the internet which rules out the possibility of getting attacked by malwares. Paper wallets are secure, but one must careful about not losing them. The process of

generating a paper wallet involves printing the private keys and addresses onto a paper.

Hardware wallets

Hardware wallets are physical devices that store the private and public keys. These wallets are also known as “cold storage” wallets as they are not connected to the internet. When a user wants to carry a transaction, these wallets are momentarily connected to the hot wallets to sign the transactions and then they are disconnected. These wallets are the most secure wallets in the market. Some of the popular hardware wallets can store up to 22 cryptocurrencies. Some of the popular hardware wallet are Ledger Nano S and Trezor.

Motivation

With the advent of digital currencies there have been raising concerns about the security protocols being used to secure their use. The crypto currencies and the underlying technology blockchain is secure but the way we human interact with these technologies makes them unsecure. There have been numerous cases of people losing their crypto currencies because of their account passwords getting leaked because of their own mistake. There could be many reasons for the passwords getting leaked. Weak authentication is threat to the crypto wallet industry. People when signing up for an online account tend to click photos of their passwords and save them in their machines or email it to their accounts without knowing the repercussions. There have been cases when hackers get unauthorized access to email accounts to reset account passwords and then get access to their funds eventually. These are some of the issues that stop people from embracing these technologies that are otherwise secure.

Objective

The objective of this project can be divided into two parts. First objective will be to make a fully functional cryptocurrency wallet that will enable the users to check their crypto balance, transfer coins from one address to another. The second objective will be to make the wallet secure. To make the wallet secure there will be other features in the wallet like Two-Factor authentication. Passwords can be hacked, OTP messages sent to mobile phones can also be hacked. For Two-Factor authentication to work one must be in possession of a

physical device that generates code based on an algorithm which will be explained in more detail in the methodology section. This authentication step will make the login process secure. The wallet will be a hierarchical deterministic wallet. HD wallets make key management hassle free and more secure. HD wallets can generate all the used key pairs just form a single source often referred to as the seed. The wallet will also have multisig functionality for transaction approval. Multisig technology is explained in more detail in the methodology section.

Methodology

Components

Front-end

The front-end of the application will be implemented in Angular.js or React.js. The reason behind selecting Angular is that its component based and fast. The whole front-end of the application can be made by splitting it into several MVC components which makes it time a saving process and ensures that the code base will remain concise and clean. Angular also has two-way data binding that binds the view with the model and vice-versa.

Back-end

The back-end of the application will be implemented using Node.js and the Express.js framework. Node.js is a JavaScript runtime that allows to run JavaScript out of the browser. There are many Node.js frameworks in the market but this app will be using Express.js as it provides greater flexibility. Express integrates easily with other modules to get the desired results.

The database side of the application will be implemented using a NoSQL database. The reason behind choosing a NoSQL database is that it is less rigid as compared to other relational databases in terms of data storage techniques and thus will provide greater flexibility.

Two-Factor Authentication

Apart from the basic authentication measures like providing the username and password to login, this app will also make use two-factor authentication. The user

upon registering for a wallet will be asked to scan a QR-code using a two-factor authentication device like Google Authenticator.

Usage

1. User installs Google Authenticator on his/her phone
2. User registers for a wallet on the website
3. Upon successful registration a QR code gets displayed on the screen
4. User scans the QR code to get the secret key into the app
5. User is asked to login using the username and password
6. Upon validation of username and password user is asked to enter the code they see on the two-factor authentication device
7. Code is verified

Passwords can be hacked, OTP's sent to the mobile phones can also be sniffed but two-factor authentication requires a person to be in possession of a physical device which makes it impossible to hack unless one gets the device. This will ensure to make the wallet secure by adding an extra layer of security to the login step.

Multisignature Wallets

The wallet will use the concept of Multisignature(multisig) address to approve a bitcoin transaction. Transaction in the traditional wallet are often referred to as "single-signature transactions", because transferring fund from an address requires a single signature of the owner with the private key corresponding to the address. A hacker can retrieve or transfer all the funds if they get access to that single private key. Multisig wallets changes the way how transactions work so that such risks could be mitigated. A multisig wallet requires M-of-N signatures to approve a transaction. N is the number of people authorized to sign the transaction or in other words the number of private keys to sign the transaction and M is the required signatures. This wallet will use 2 out of 3 authorizers to sign a transaction and only then will it become a valid transaction. This multisig technology will also prevent transferring of funds by mistake and thus will make the wallet secure.

Hierarchical deterministic wallets

One of the main concerns of wallet users is key management. Hierarchical deterministic wallets allow users to generate all the private and public keys from a single point. This single point is known as a seed. Without HD wallets users must keep the records of all the key pairs separately. Managing multiple backups is error prone. HD wallets allows the user to regenerate all the key pairs just from a single backup that serves as a continuous and seamless backup. Thus, HD wallets are a step towards enhancing the security of the wallets.

Project Schedule and Milestones

Stages of software development

Requirement gathering and Preliminary Research: Understand the basic problems that the software will cater to. Understand blockchain concepts and how wallets interact with the blockchain.

Design: Get an understanding of what languages, frameworks or libraries will be needed for the different components of the system. Plan the architecture of the system and get deep understanding of how different components will interact to solve the requirements.

Development: On getting clear understanding of the system design start implementing the system.

Testing: Testing is done simultaneously with development and after the system gets developed.

Deployment: System will be deployed for actual use to a production server.

Schedule

Timeline	**Milestone**
Initial research and analysis	Sep
Design	Oct- Late Nov
Development	Late Nov-Mid Mar
Testing	Mid March
Deployment	Mid April