Free TON Wallet

Originally, **Free TON Wallet** project was started by #137 Contest - Free TON Web Browser Extension.

Along research phase our team made decision to develop a cross platform application to archive best user experience, due most of people around the World use several platforms same time.

Right now we take a focus to fulfill Chrome Extension and Web-based versions with all necessary features. Build for Mobile and Desktop versions we plans to configure after code freeze.

Find us

- Website - http://freeton-wallet.org/
- Telegram Updates
- Google Group
- GitHub

Installation

Binary Releases of the wallet application available in our GitHub repostiry https://github.com/freeton-wallet/wallet/releases.

There are good reason to verify signature:

```
gpg --verify freeton-wallet-chrome-extenstion.zip.asc
```

To install Chrome Extention from ZIP binary archive follow this manual.

Publishing an extension to the extension stores is planned for near future.

References

- #137 Contest Free TON wallet as a Chrome extension. PDF: Stage 1 (a local copy).

Updates

2021-06-08 Chrome Extension Dry-Run

Another good news 🈂. We have success with first dry-run the application as Chrome-Extension. We are planning to publish the application into Web Stores in few days...

2021-06-07 Beta Release

Today we are published our Beta version of Web Wallet. Checkout 🈂 https://app.freeton-wallet.org

2021-06-07 Community Presentation

Google Slides

|

Text Version

Our Team

Originally, the project was started by Max Anurin and Anatoliy Vasilev just for fun.

Along with investigating phase and initial development there a few other people have joined as researchers and advisors. These people are involved in TON technical details. They are extremely interested in the project and the TON ecosystem.

These guys are waiting for the initial setup of the project to start their own contribution to growth the project.

Principles

We classically follow three common principles:

- Security

- Usability

- Upgrowth

SECURITY

Security is the most important principle. Our users have to trust the application and our team. Also, we, as vendor, have to protect our users from potential fund losses by incorrect usage of the application and TON ecosystem.

From a newbie user perspective, there are a lot of hard-to-understand terms, features, etc... We want to help our users to get involved in the TON ecosystem as simply as possible. For the case we defined user guidelines like Glossary, Common Attack Vectors, Safety Checklist and Source/Binary signing.

From a security perspective, we chose Type Safety Dart-based technical stack to prevent potential fund losses via bugs. In our opinion, Dart will help us to stay at a quality code base along with the upgrowth contribution of junior developers. We plan to develop new features while our JS-based competitors fix issues. Dart/Flutter grows in software development, the same as crypto grows in classical assets model.

Public visible CI/CD is hard criteria to distribute such software. We are on it via GitHub Actions. End-users may (and have to) check sources related to use binary distribution.

USABILITY

Usability makes our users happy! So it is an important principle too.

Chosen UI framework Flutter is solving most of desires:

- Expressive and Flexible UI

- Native Performance

- Material Design

Another bonus is cross platform codebase. Currently, it is pretty good to share the same user experience across mobile and desktop platforms. It makes a user free to switch between platforms with zero-learning dependency.

CI/CD is an usability friend. The users obtain releases and notifications as soon as possible.

UPGROWTH

Upgrowth is the main intention of the core team.

Our main idea is to provide a project ecosystem and the right technical stack to be able to contribute as easily as possible. This idea has to make it possible to make low-cost development to grow the project.

We spent time setting up a project ecosystem. This is like heart-beat for the project in counter front to phrase "give someone or something a bad name" or russian analog "▯▯▯ ▯▯▯ ▯▯▯▯▯▯ ▯▯▯▯▯▯▯▯▯▯▯▯, ▯▯▯▯ ▯▯▯▯▯ ▯▯ ▯▯▯▯▯▯▯▯▯▯▯". Right now we have a starting point to grow the project.

Summary

☺ We Are Born!

Core team still working on Contribution Guidelines, CI/CD Configuration, Knowledge Docs, Setup Public Relations, etc...

If you have any questions we are happy to answer them!

Be in touch:

- Ask any questions in our Telegram and Google Group channels
- Subscribe our Telegram Updates Channel

YouTube Video Cast

I

Browser Extension

Chrome

1. Download desired version of binaries `freeton-wallet-chrome-extenstion.zip` and corresponding signature `freeton-wallet-chrome-extenstion.zip.asc` from https://github.com/freeton-wallet/wallet/releases

2. Verify signature, to prevent maleware injection

   ```
   gpg --verify freeton-wallet-chrome-extenstion.zip.asc
   ```

3. Switch your Chrome Extenstions into `Developer mode`. See for official documentation for details.

   a. Navigate to chrome://extensions

   b. Turn ON development mode toggle.

4. Use button `Load unpacked` to upload ZIP binaries

5. Use Free TON Wallet extension

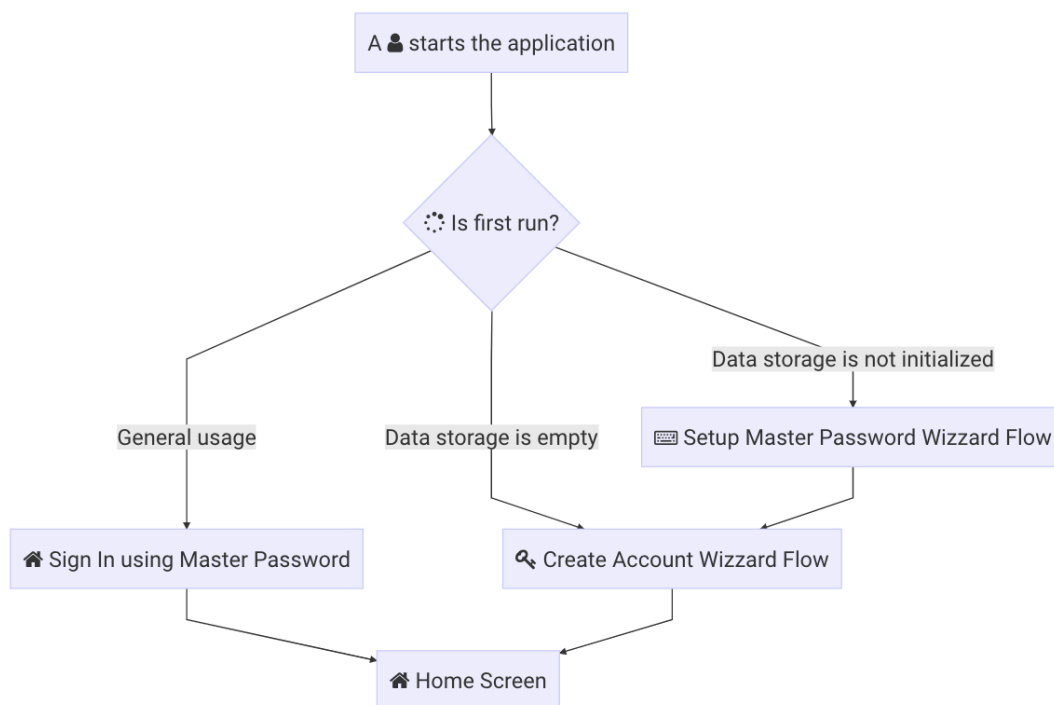## Firefox

TBD

Safari

TBD

# Roadmap

Use Cases

Launch the application

At launch time the application check data storage and detect necessity of wizzard flow.

For example, at first launch, the application make wizzard for Master Password and create a first account.

```
                    A 👤 starts the application
                              │
                              ▼
                        ◆ Is first run?

    General usage      Data storage is empty    Data storage is not initialized
                                                ⌨ Setup Master Password Wizzard Flow

  🏠 Sign In using Master Password    🔑 Create Account Wizzard Flow

                    🏠 Home Screen
```

Use Cases

Create Account Wizzard
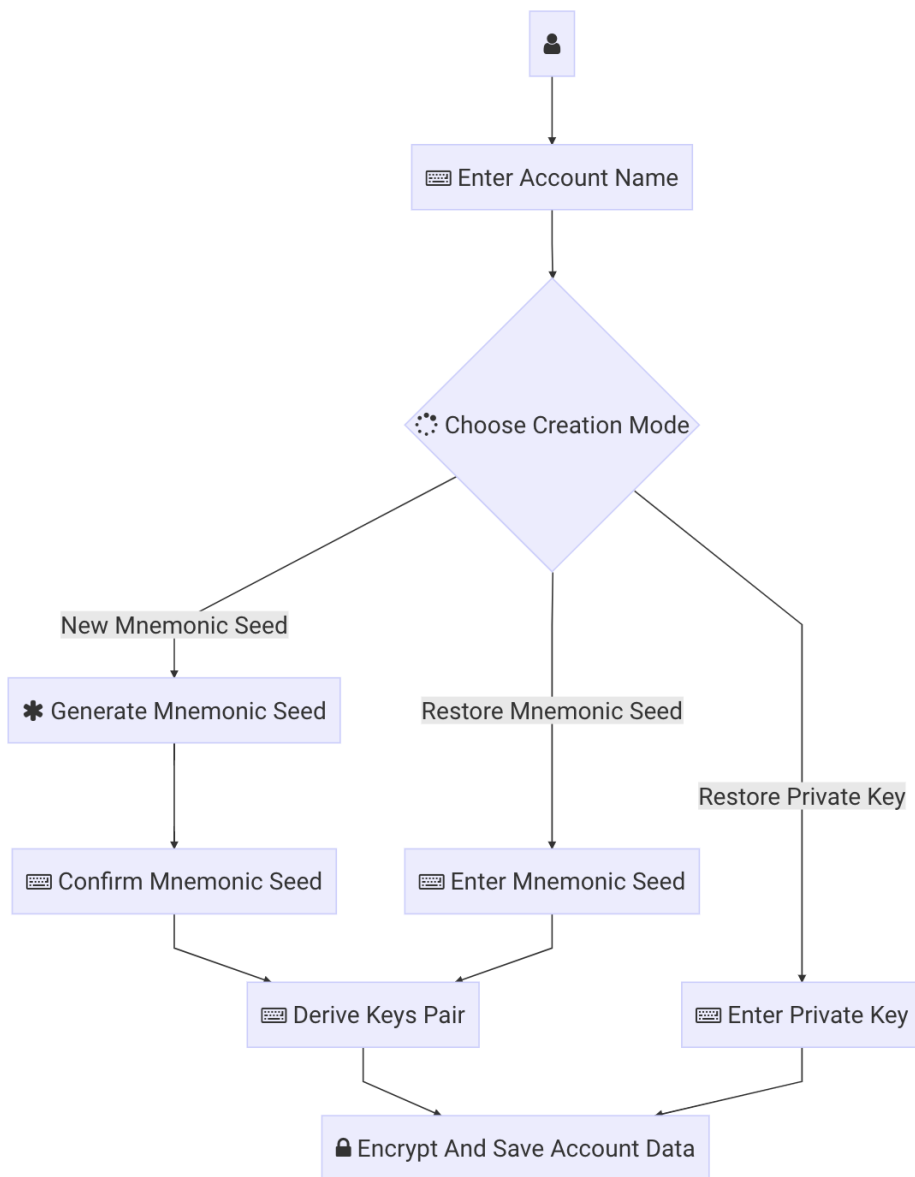
Use Cases

Deploy Wallet Contract

A new account is required a Wallet Contract to be deployed. So after account creation, a user have to deploy one of contract.
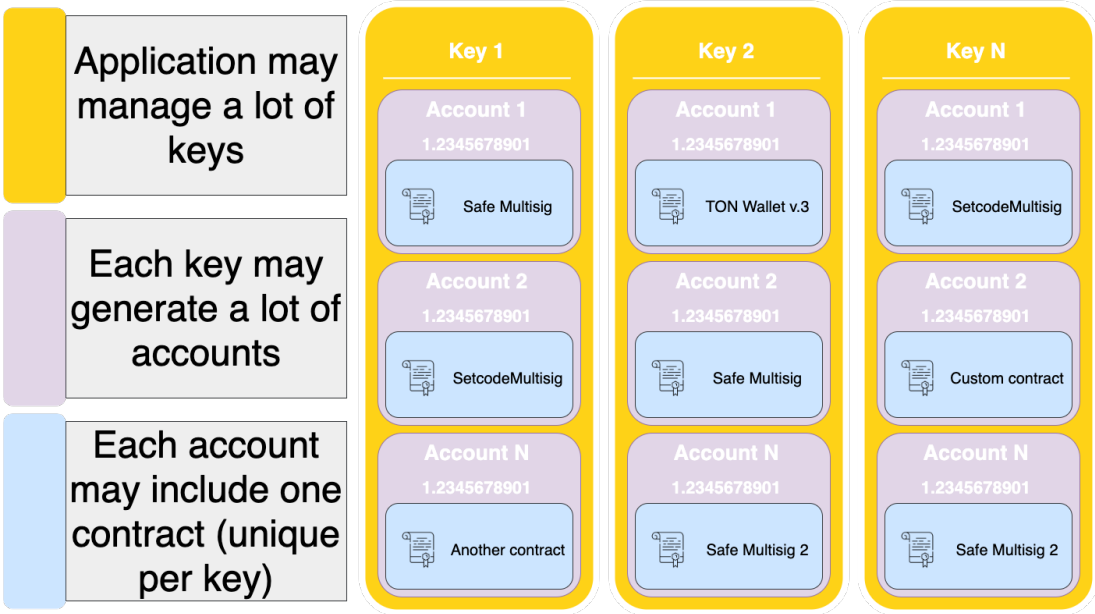
TBD

Technical Stack

- Wallet Application is written in Flutter/Dart
    - Web platform:
        - Free TON Blockchain communication via official TON Javascript Web SDK with own interop facace library
        - Data Storage in browser LocalStorage
        - Sensetive data encryption via AES-CBC (with PKCS7 padding)
        - Password derivation using PBKDF2
        - Using Extension Manifest V2
    - Mobile platform - Not impelmented yet
    - Desktop platform - Not impelmented yet
- Documentation generated by MkDocs

Software Architecture

Application Objects Composition
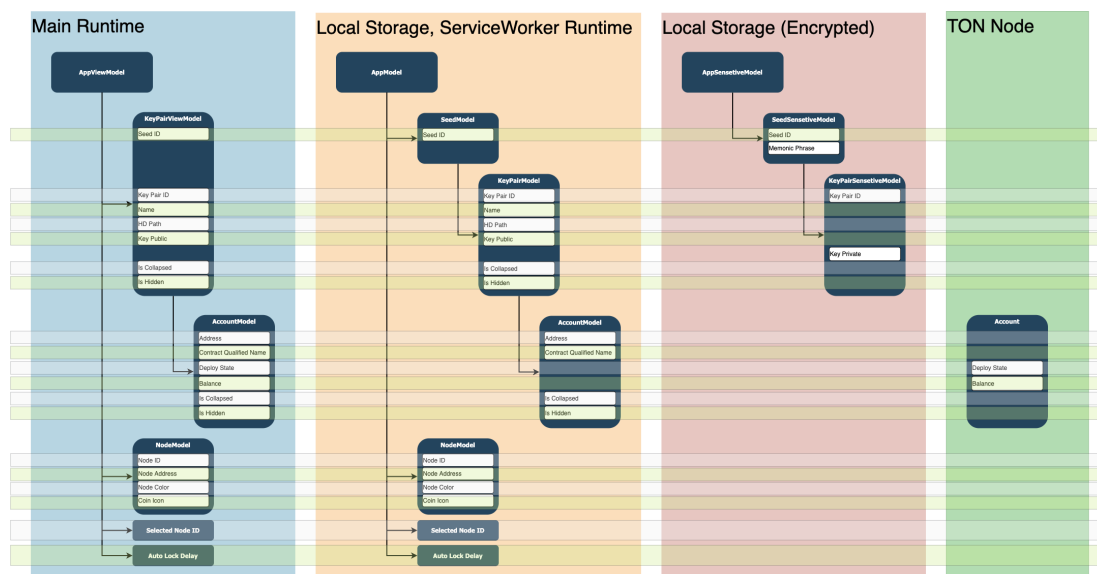
Free TON Wallet

Application Objects Composition

		Key 1	Key 2	Key N
Application may manage a lot of keys		**Account 1** 1.2345678901 — Safe Multisig	**Account 1** 1.2345678901 — TON Wallet v.3	**Account 1** 1.2345678901 — SetcodeMultisig
Each key may generate a lot of accounts		**Account 2** 1.2345678901 — SetcodeMultisig	**Account 2** 1.2345678901 — Safe Multisig	**Account 2** 1.2345678901 — Custom contract
Each account may include one contract (unique per key)		**Account N** 1.2345678901 — Another contract	**Account N** 1.2345678901 — Safe Multisig 2	**Account N** 1.2345678901 — Safe Multisig 2

See Glossary in a Technical Paper to understand terms key, account, contract...

Components View

Web/Extension Application
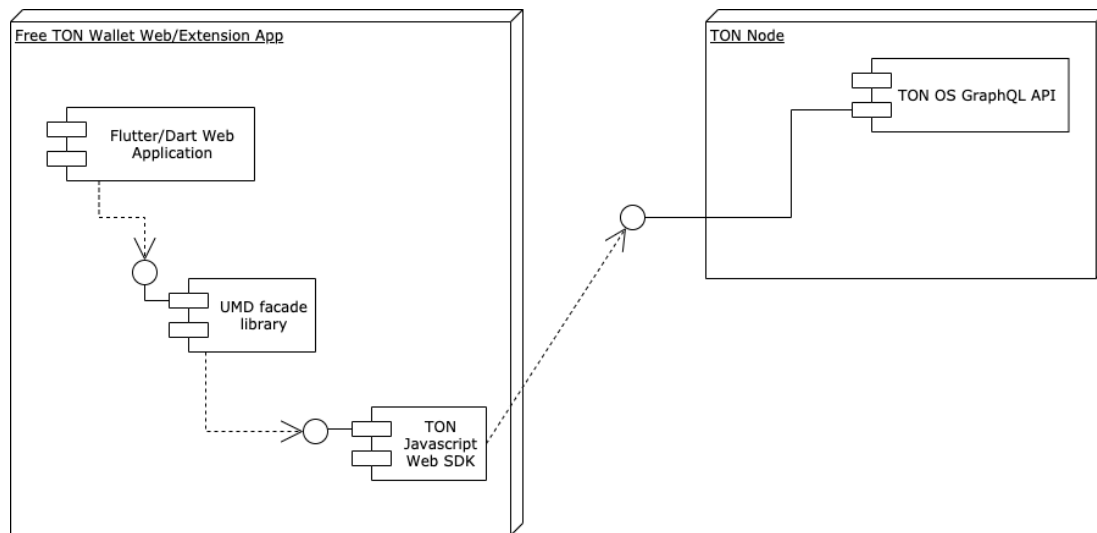
Data Relation

Change Log

2021-03-21

- Start the project

Glossary

H

HDPATH

For example Free TON use value `m/44'/396'/0'/0`.

Defines a logical hierarchy for deterministic wallets. Level 2 of the hierarchy describes a coin type in use.

Originally was desined for Bitcoin as BIP-0044.

See also:

- BIP-0044
- SLIP-0044 : Registered coin types for BIP-0044

M

Mnemonic Seed

Mnemonic phrase, **mnemonic seed**, or **seed** phrase are defined as a secret group of words that represent a wallet. When used in sequence they allow access to the cryptocurrencies stored within. **"Mnemonic"** just means a memory aid such as rhymes, abbreviations and songs that help you remember something else.

Safety Warning Do not take photos or screenshots. Other apps can get access to them. Write everything down on paper and store it in a safe place.

See also:

- Seed phrase
- Mnemonic phrase

W

Wallet

A word **Wallet** is a little bit abstract thing. Different applications have different meaing of the terms.

We use the word **Wallet** to define crypto wallet on the blockchain (smart contract).

Like a:

- TON wallets

- SafeMultisig

- SetCodeMultisig