Contact information

Surf: **0:714d58bfe28499c989fd8eda43e6368c0d3e908e21df690c46bfbd5c02855985**

Email:
tonsoft@protonmail.com

Forum:
https://forum.freeton.org/u/tonsoft

Project information

// Will not change after contest

GitHub:	https://github.com/tonsoft-org/alpha.browser.wallet
GitHub:	https://github.com/tonsoft-org/alpha.wallet
Site:	http://alpha.wallet.tonsoft.org/
Extension:	http://alpha.wallet.tonsoft.org/download/chrome.zip (recommended use github)

// Will change after contest

GitHub:	https://github.com/tonsoft-org/browser.wallet
GitHub:	https://github.com/tonsoft-org/wallet
Site:	http://wallet.tonsoft.org/

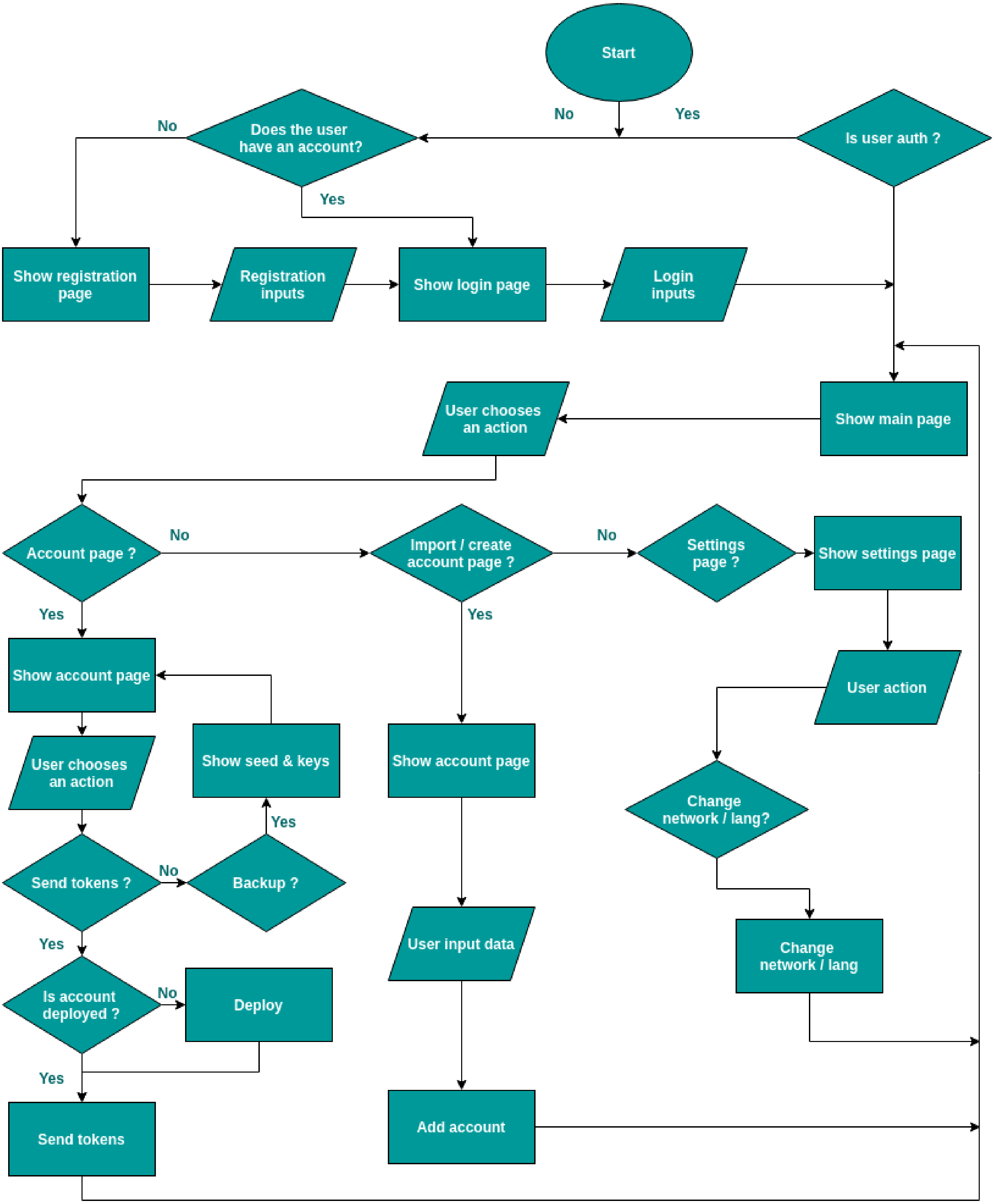
Free TON wallet as a Chrome extension

1 Introduction

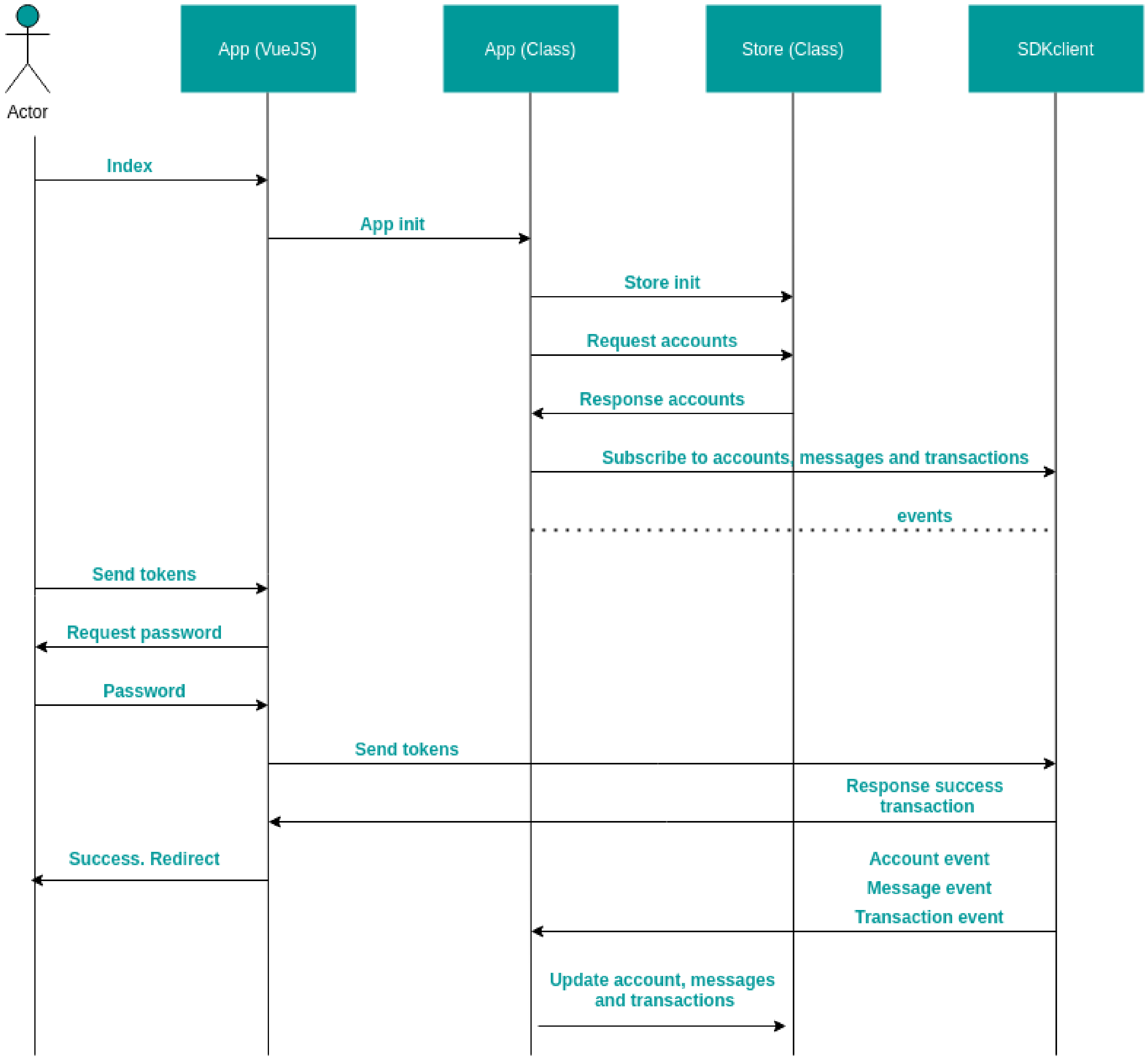
Our community is constantly evolving. There are many people in our community who don't know how to use command line, so we need to create tools that ordinary people can use. It should be an easy, fast and secure way to store and send coins. In addition, it would be great to put other useful tools in this application, for example, DeBrowser, which can interact with DeBots, or an interface with which you could manage staking.

Many people would find it convenient to perform all of these actions through a website. However, it is even better when this site can be embedded directly into your browser and always be at your fingertips. In this work, we will try to briefly describe our new application ‘Free TON wallet as a Chrome extension’.

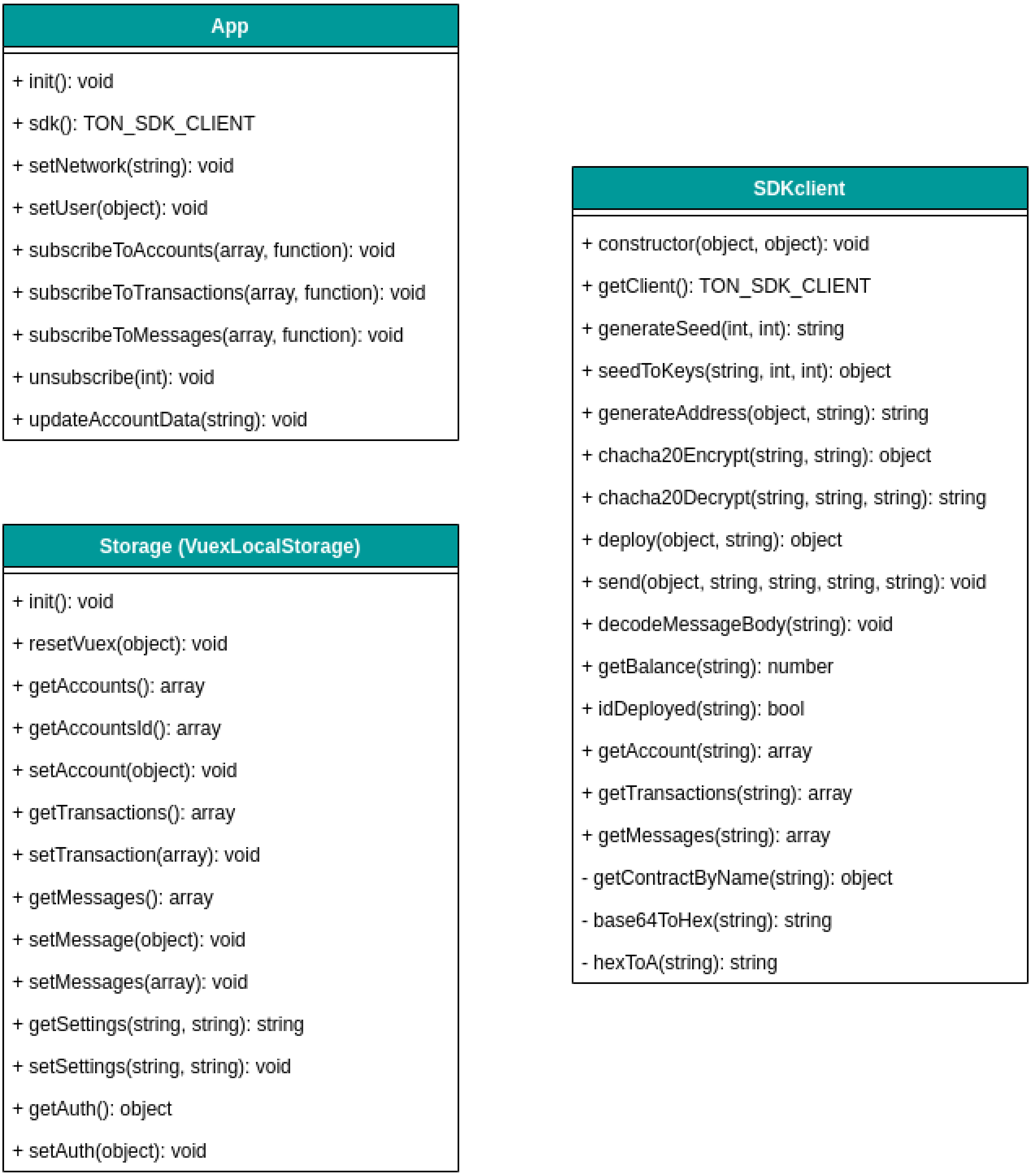
2 Application architecture (short)



Program diagram flow (simplistic)



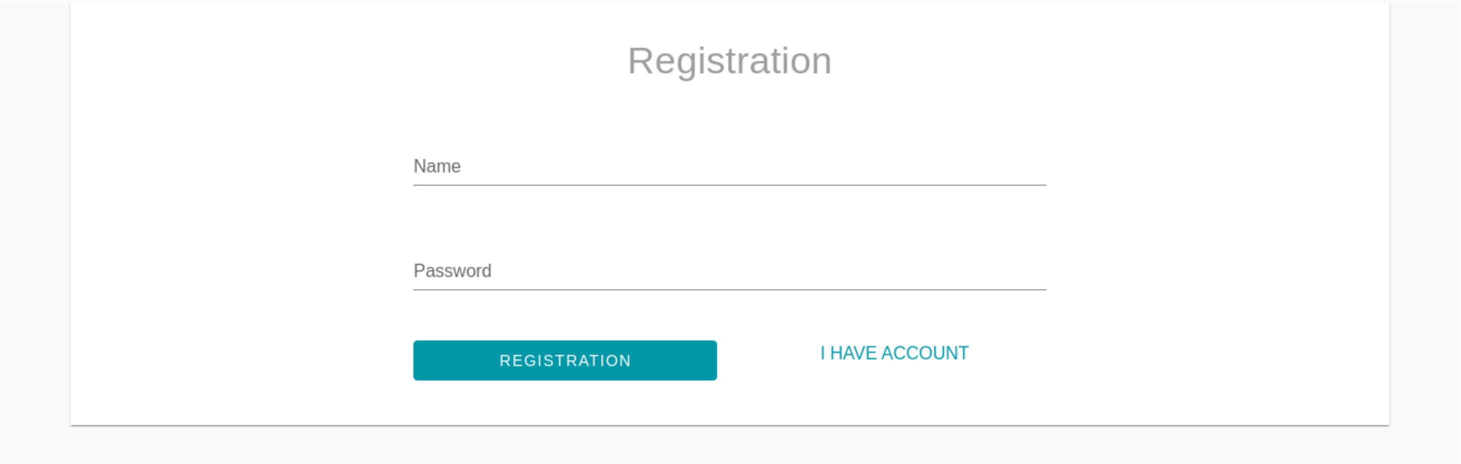
UML Diagram. Send token example.


App
+ init(): void
+ sdk(): TON_SDK_CLIENT
+ setNetwork(string): void
+ setUser(object): void
+ subscribeToAccounts(array, function): void
+ subscribeToTransactions(array, function): void
+ subscribeToMessages(array, function): void
+ unsubscribe(int): void
+ updateAccountData(string): void
Storage (VuexLocalStorage)
+ init(): void
+ resetVuex(object): void
+ getAccounts(): array
+ getAccountsId(): array
+ setAccount(object): void
+ getTransactions(): array
+ setTransaction(array): void
+ getMessages(): array
+ setMessage(object): void
+ setMessages(array): void
+ getSettings(string, string): string
+ setSettings(string, string): void
+ getAuth(): object
+ setAuth(object): void
SDKclient
+ constructor(object, object): void
+ getClient(): TON_SDK_CLIENT
+ generateSeed(int, int): string
+ seedToKeys(string, int, int): object
+ generateAddress(object, string): string
+ chacha20Encrypt(string, string): object
+ chacha20Decrypt(string, string, string): string
+ deploy(object, string): object
+ send(object, string, string, string, string): void
+ decodeMessageBody(string): void
+ getBalance(string): number
+ idDeployed(string): bool
+ getAccount(string): array
+ getTransactions(string): array
+ getMessages(string): array
- getContractByName(string): object
- base64ToHex(string): string
- hexToA(string): string

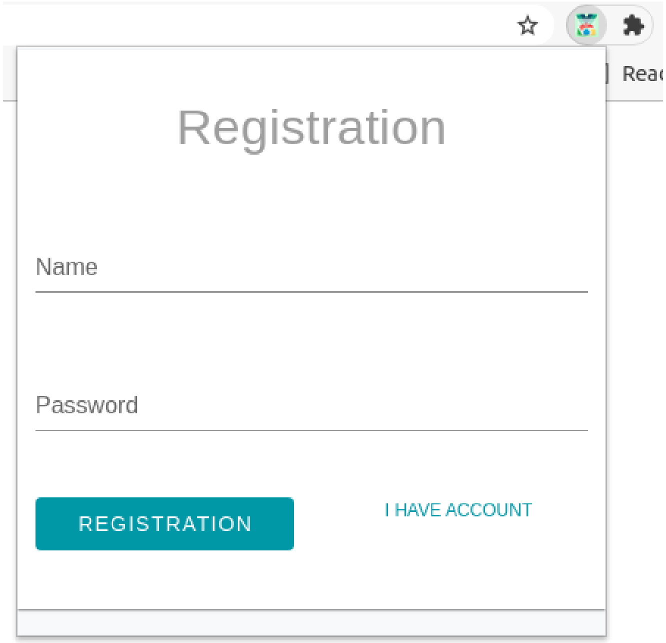
UML Diagram. Main classes.

3 Application appearance

3.1 Registration

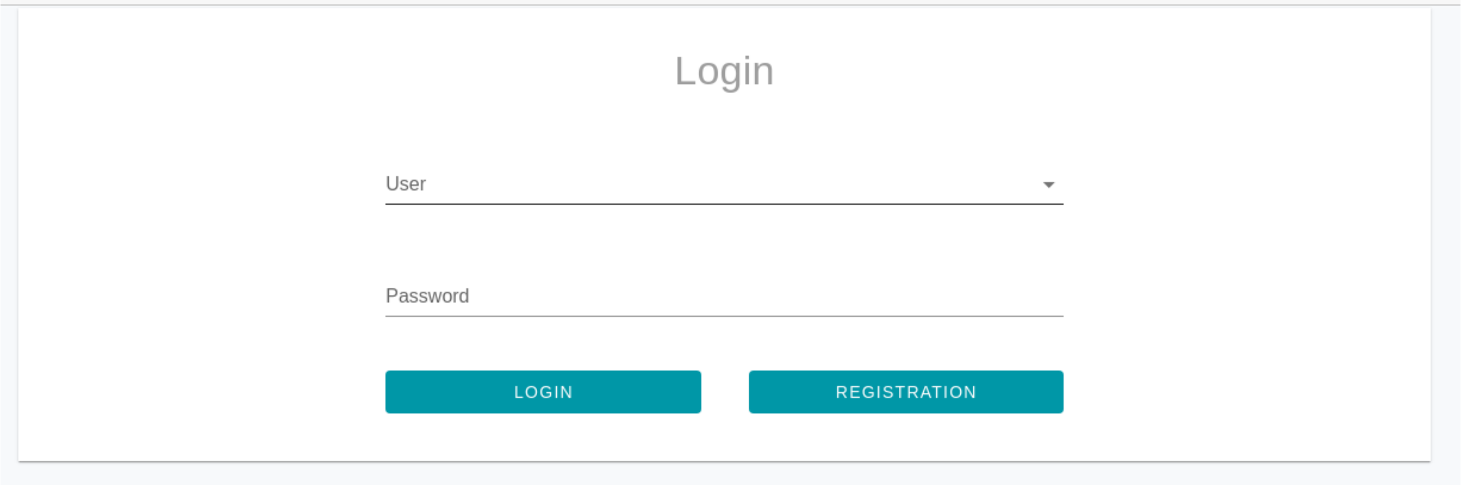


Registration. Website view.

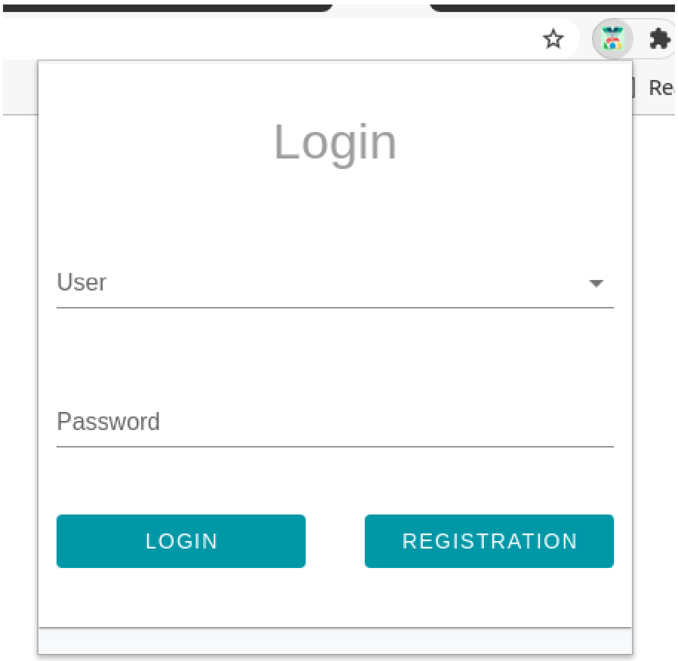


Registration. Extension view.

3.2 Login

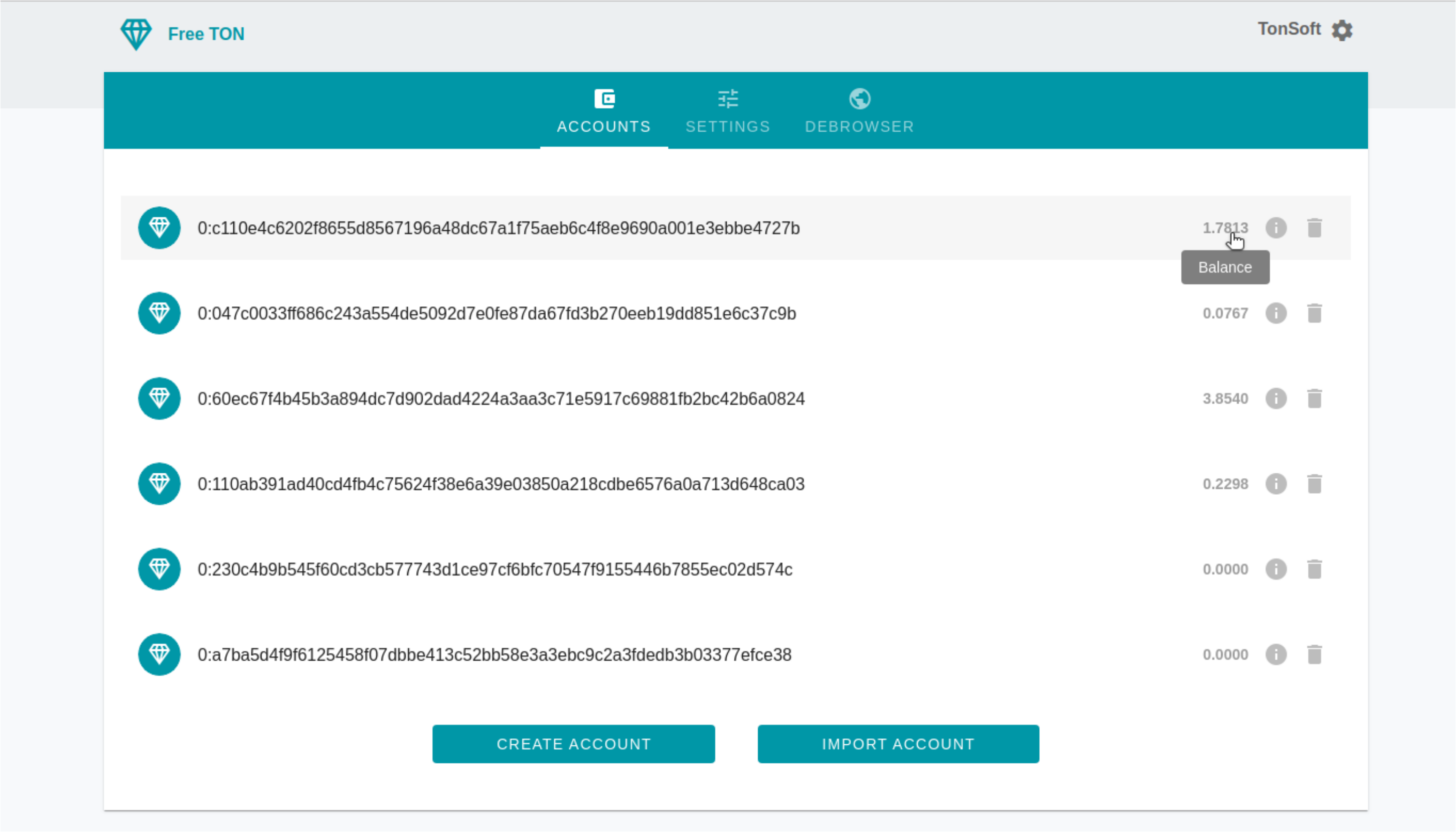


Registration. Website view.



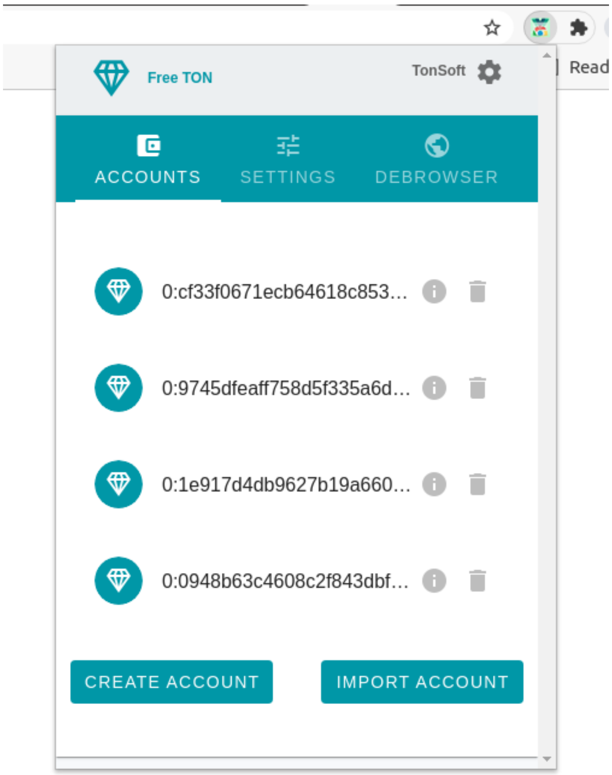
Registration. Extension view.

3.3 Main page



0:c110e4c6202f8655d8567196a48dc67a1f75aeb6c4f8e9690a001e3ebbe4727b	1.7813
0:047c0033ff686c243a554de5092d7e0fe87da67fd3b270eeb19dd851e6c37c9b	0.0767
0:60ec67f4b45b3a894dc7d902dad4224a3aa3c71e5917c69881fb2bc42b6a0824	3.8540
0:110ab391ad40cd4fb4c75624f38e6a39e03850a218cdbe6576a0a713d648ca03	0.2298
0:230c4b9b545f60cd3cb577743d1ce97cf6bfc70547f9155446b7855ec02d574c	0.0000
0:a7ba5d4f9f6125458f07dbbe413c52bb58e3a3ebc9c2a3fdedb3b03377efce38	0.0000

Main page. Website view.



0:cf33f0671ecb64618c853…

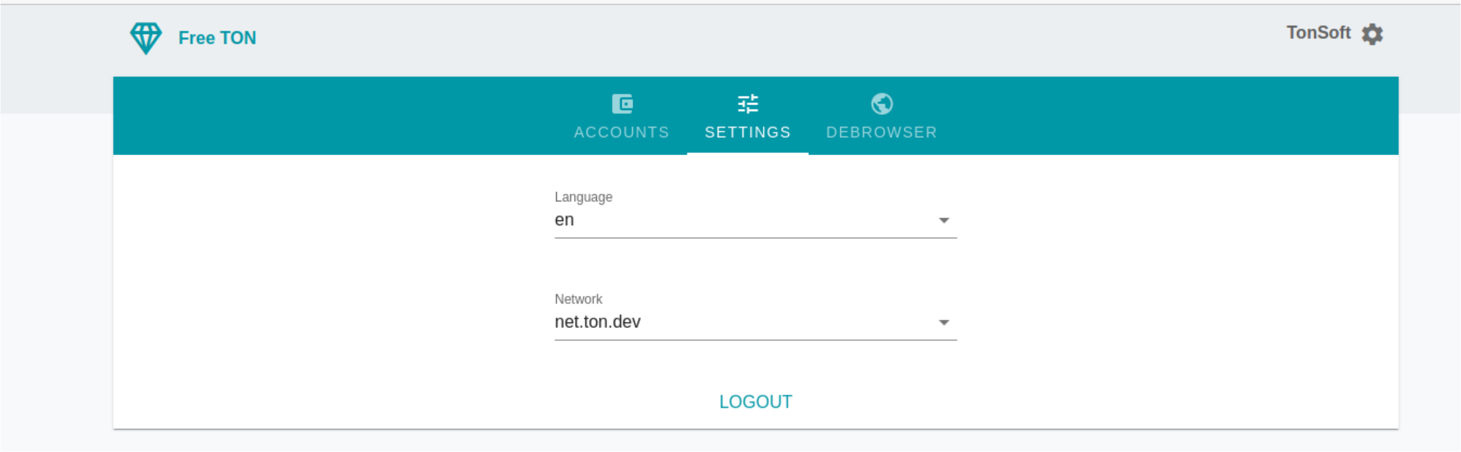
0:9745dfeaff758d5f335a6d…

0:1e917d4db9627b19a660…

0:0948b63c4608c2f843dbf…

Main page. Extension view.

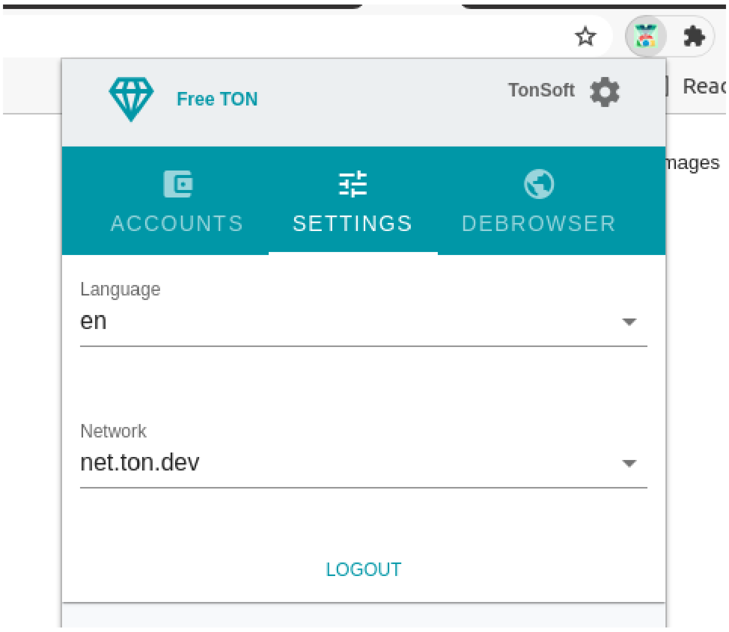
3.4 Settings



Language
en

Network
net.ton.dev

Settings page. Website view.

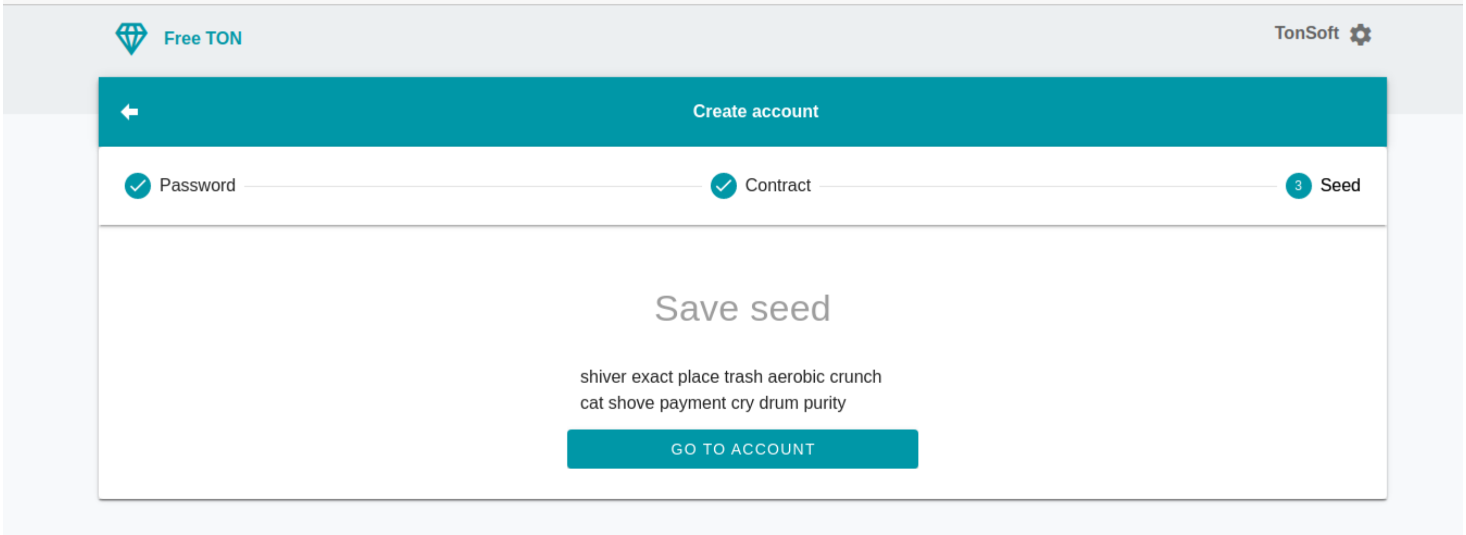


Language
en

Network
net.ton.dev

Settings page. Extension view.

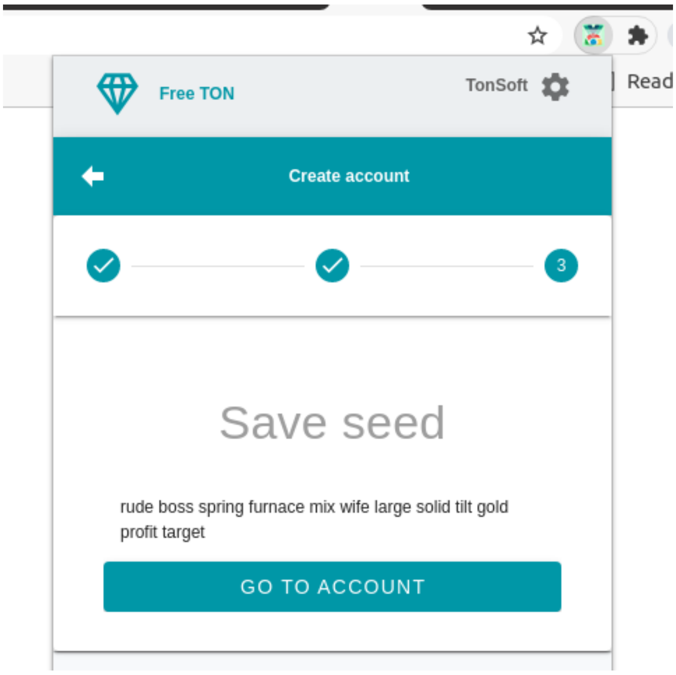
3.5 Create / import account



Save seed

shiver exact place trash aerobic crunch
cat shove payment cry drum purity

Create account page. Website view.

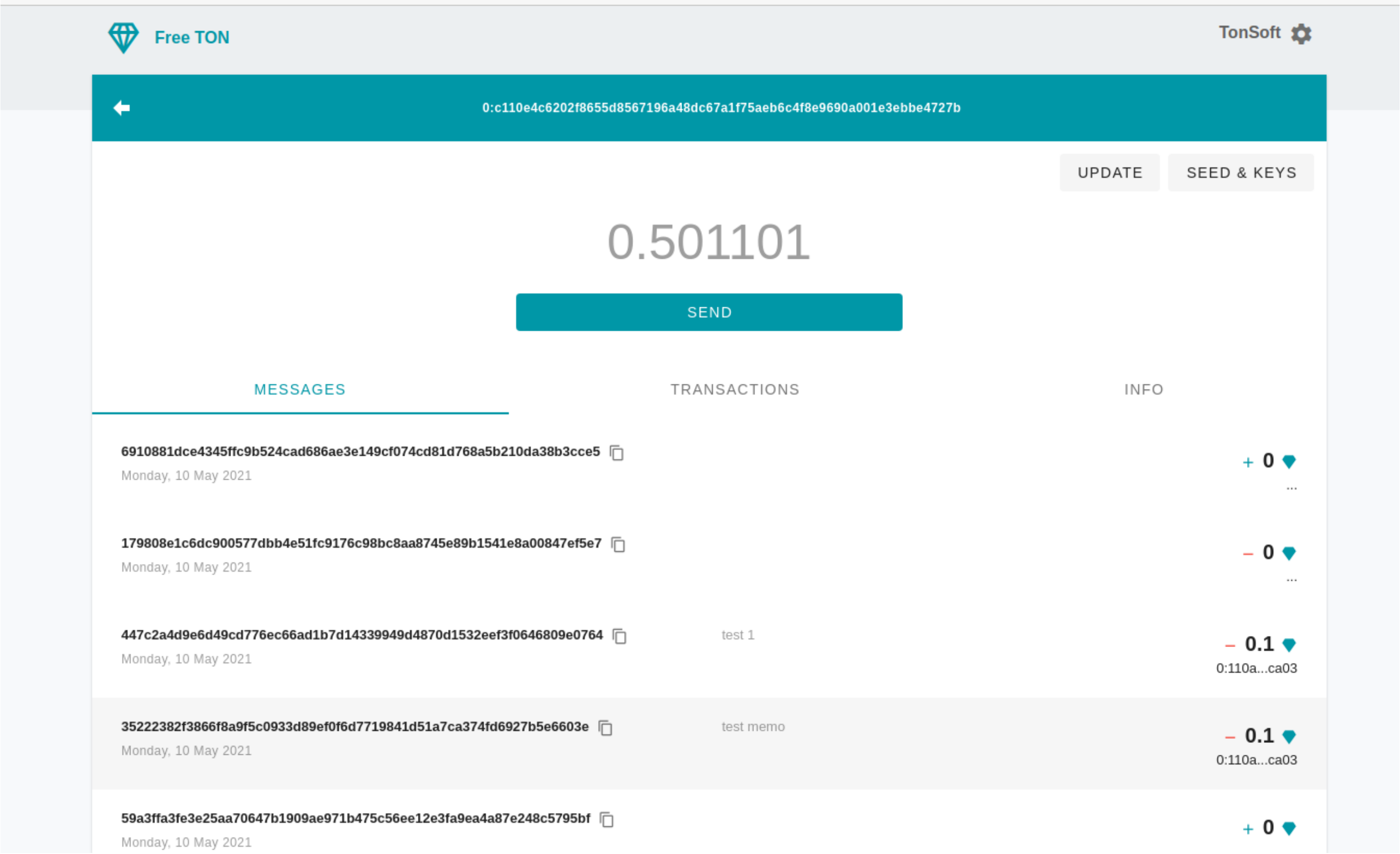


Save seed

rude boss spring furnace mix wife large solid tilt gold
profit target

Create account page. Extension view.

3.6 Account info



0:c110e4c6202f8655d8567196a48dc67a1f75aeb6c4f8e9690a001e3ebbe4727b

0.501101

6910881dce4345ffc9b524cad686ae3e149cf074cd81d768a5b210da38b3cce5
Monday, 10 May 2021
+ 0
...

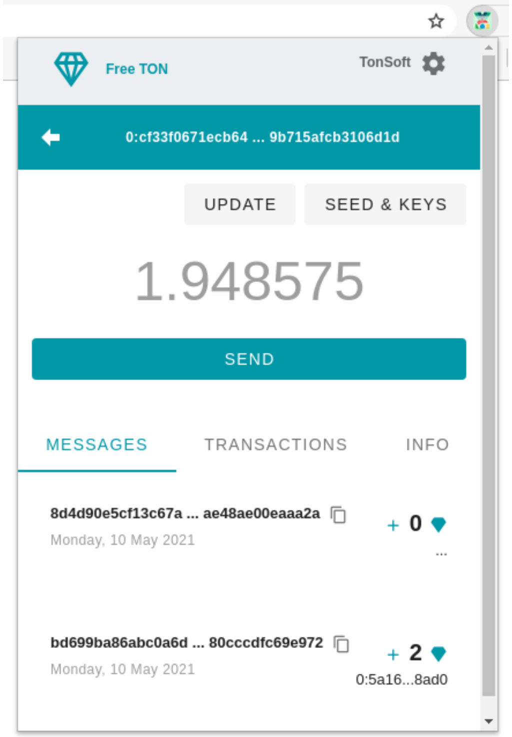
179808e1c6dc900577dbb4e51fc9176c98bc8aa8745e89b1541e8a00847ef5e7
Monday, 10 May 2021
– 0
...

447c2a4d9e6d49cd776ec66ad1b7d14339949d4870d1532eef3f0646809e0764
Monday, 10 May 2021
test 1
– 0.1
0:110a...ca03

35222382f3866f8a9f5c0933d89ef0f6d7719841d51a7ca374fd6927b5e6603e
Monday, 10 May 2021
test memo
– 0.1
0:110a...ca03

59a3ffa3fe3e25aa70647b1909ae971b475c56ee12e3fa9ea4a87e248c5795bf
Monday, 10 May 2021
+ 0

Account info page. Website view.



0:cf33f0671ecb64 ... 9b715afcb3106d1d

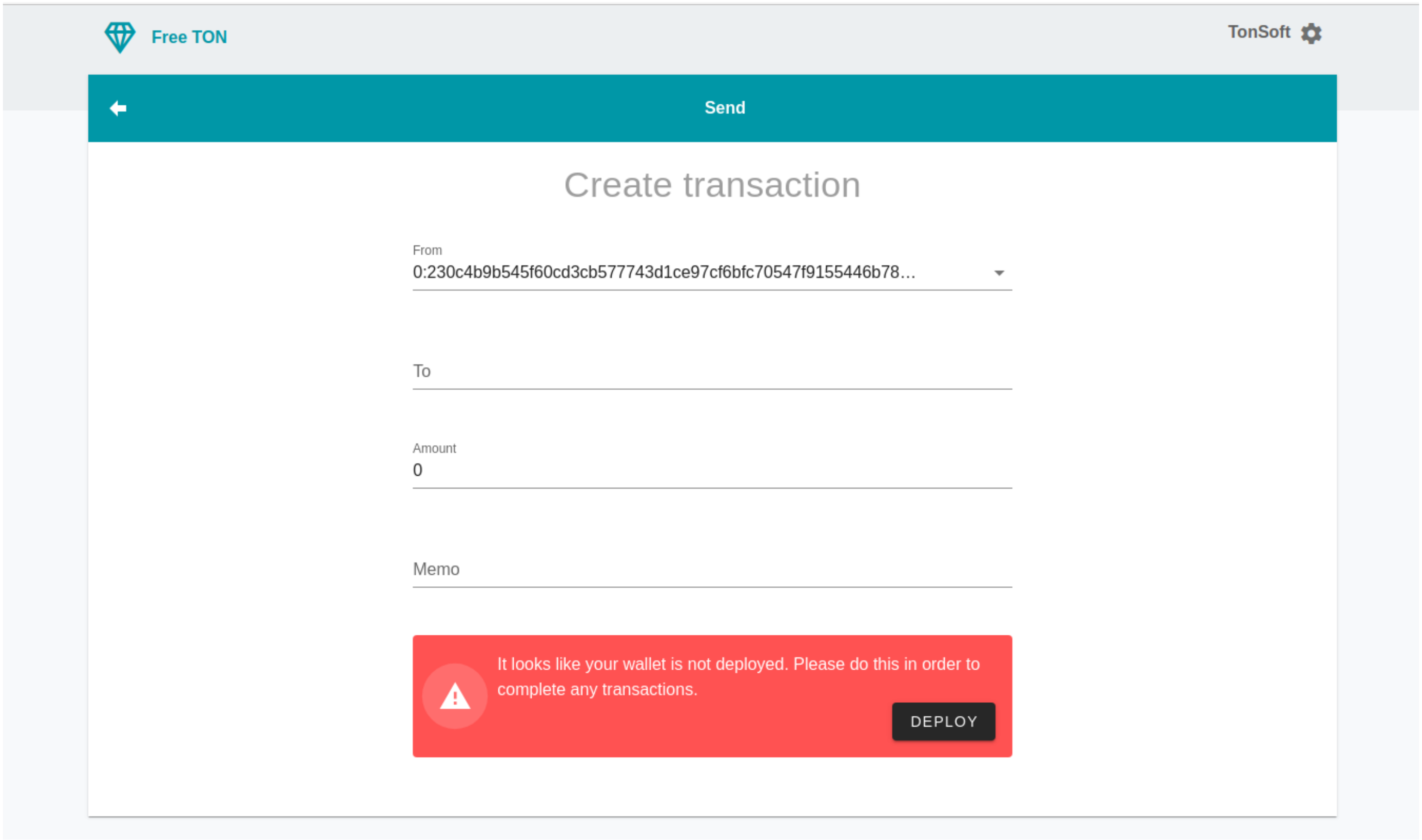
1.948575

8d4d90e5cf13c67a ... ae48ae00eaaa2a
Monday, 10 May 2021
+ 0
...

bd699ba86abc0a6d ... 80cccdfc69e972
Monday, 10 May 2021
+ 2
0:5a16...8ad0

Account info page. Extension view.

3.7 Send



Create transaction

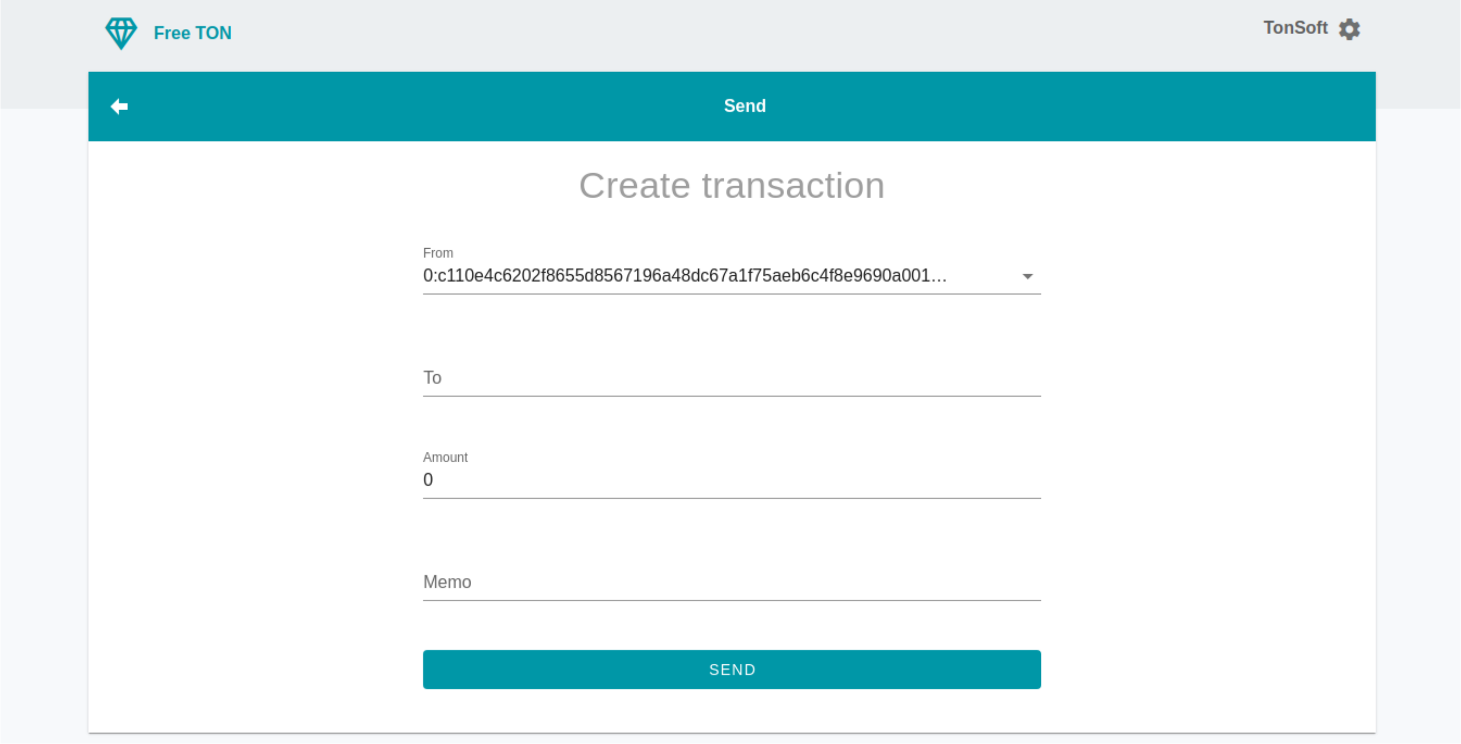
From
0:230c4b9b545f60cd3cb577743d1ce97cf6bfc70547f9155446b78…

To

Amount
0

Memo

It looks like your wallet is not deployed. Please do this in order to complete any transactions.



Create transaction

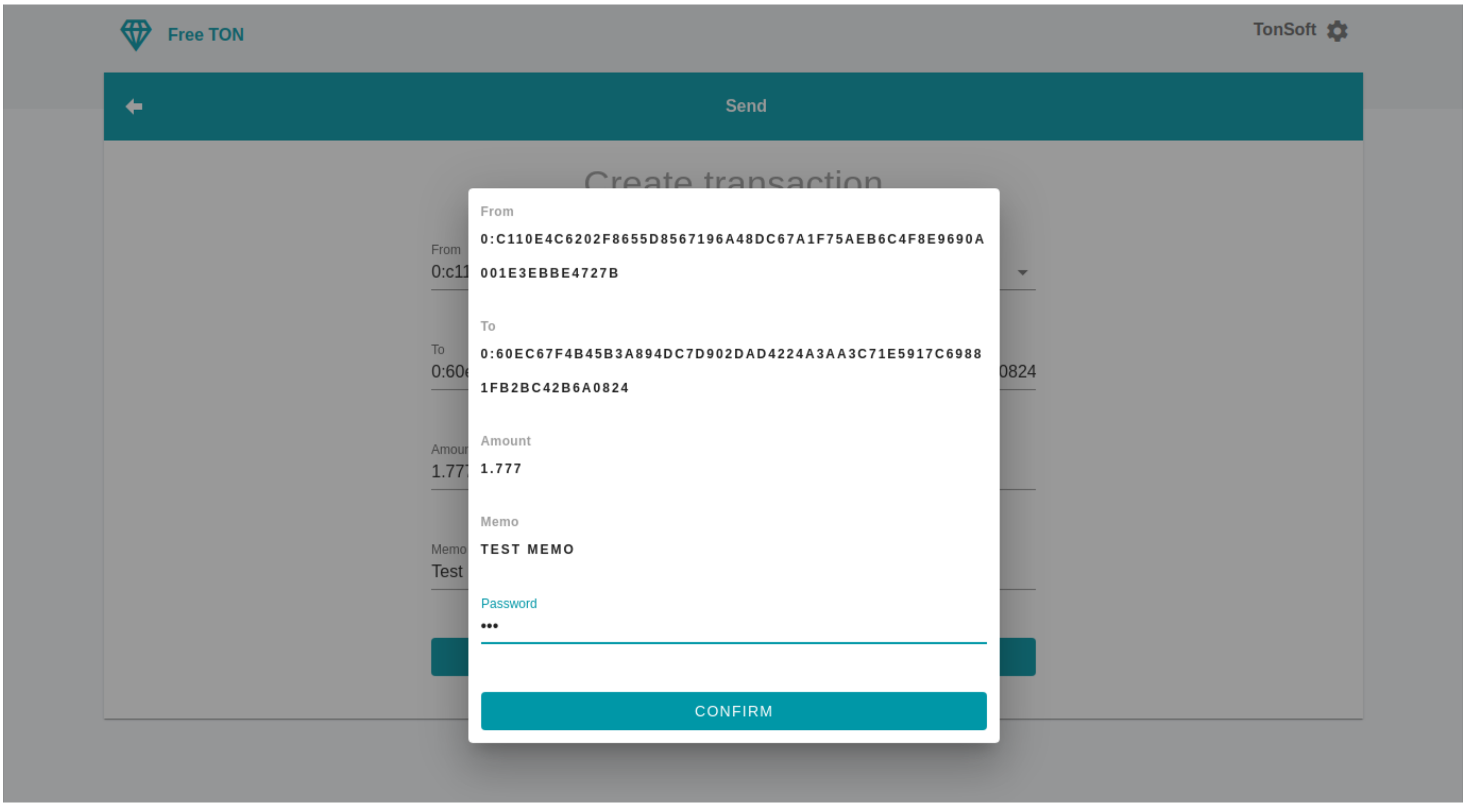
From
0:c110e4c6202f8655d8567196a48dc67a1f75aeb6c4f8e9690a001…

To

Amount
0

Memo

Send page. Website view.



Free TON

TonSoft

Send

Create transaction

From

0:C110E4C6202F8655D8567196A48DC67A1F75AEB6C4F8E9690A001E3EBBE4727B

To

0:60EC67F4B45B3A894DC7D902DAD4224A3AA3C71E5917C69881FB2BC42B6A0824

Amount

1.777

Memo

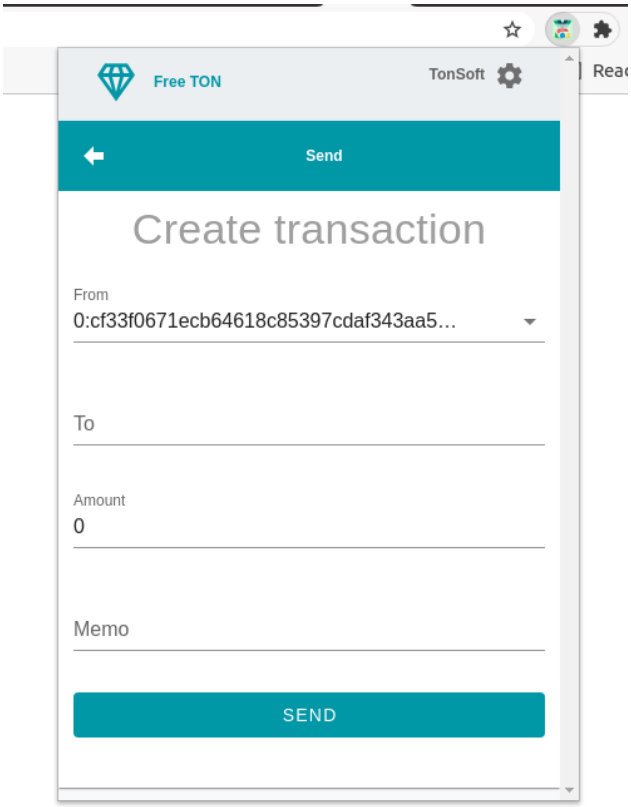
TEST MEMO

Password

•••

CONFIRM

Send page. Website view.



Free TON

TonSoft

Send

Create transaction

From

0:cf33f0671ecb64618c85397cdaf343aa5…

To

Amount

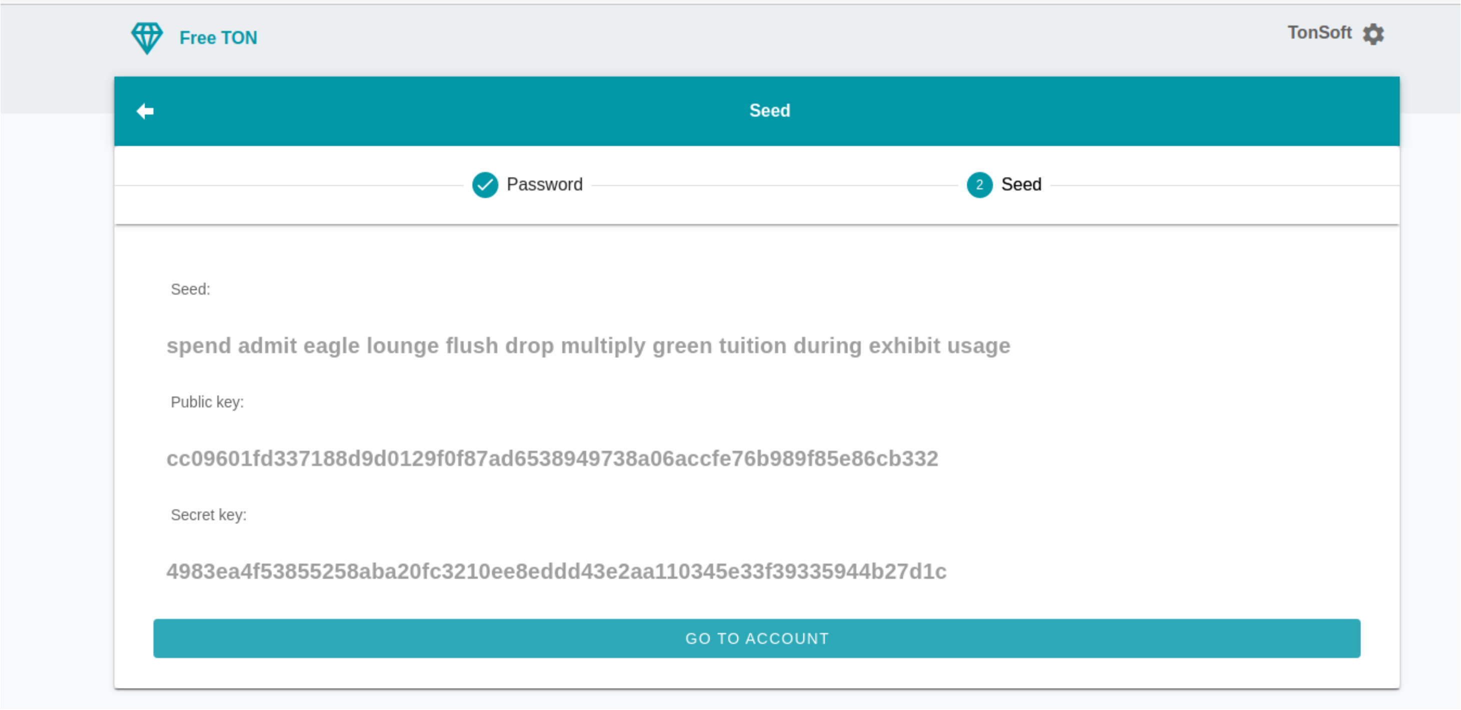
0

Memo

SEND

Send page. Extension view.

3.8 Backup



Seed:

spend admit eagle lounge flush drop multiply green tuition during exhibit usage

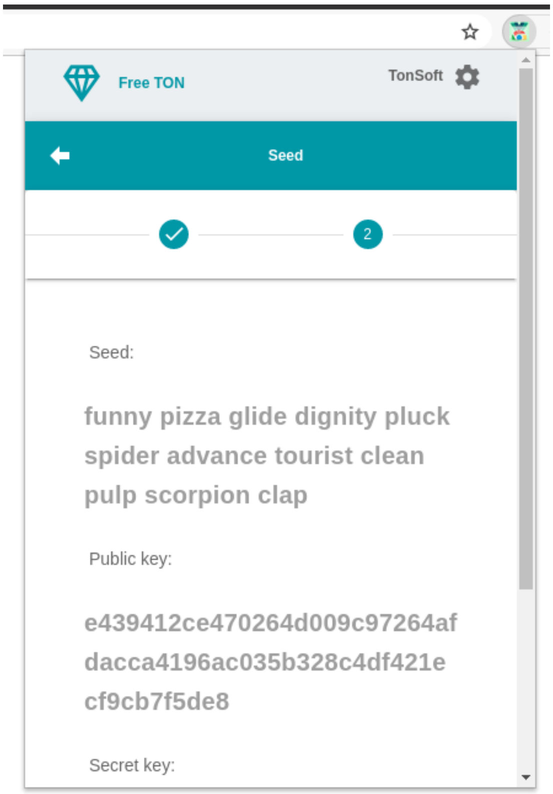
Public key:

cc09601fd337188d9d0129f0f87ad6538949738a06accfe76b989f85e86cb332

Secret key:

4983ea4f53855258aba20fc3210ee8eddd43e2aa110345e33f39335944b27d1c

Backup page. Website view.



Seed:

funny pizza glide dignity pluck
spider advance tourist clean
pulp scorpion clap

Public key:

e439412ce470264d009c97264af
dacca4196ac035b328c4df421e
cf9cb7f5de8

Secret key:

Backup page. Extension view.

Contest requirements

Generic

- ✔ **English language of the interface;**
- ✔ **Support of Google Chrome;**
- ✔ **Absence of analytical trackers (Google Analytics, Yandex Metrika, etc.);**
- ✔ **Support of mainnet and testnet(s);**
- ✔ **On-chain activity history (transactions, messages, contract interactions, etc.);**
- ✔ **Any calls that require the user’s keys must ask for the password input to decrypt them from the local storage.**

Wallet features

- ✔ **Native support of any open-sourced non-custodial Free TON wallets.**
- ✔ **Random seed phrase generation;**
- ✔ **12 or 24 words wallet initialization (based on wallet contract);**
- ✔ **Wallet seed phrase backup and restoration;**
- ✔ **Public and private keys generation, backup, and restoration;**
- ✔ **Encrypted local key storage;**
- ✔ **Password protection;**
- ✔ **Support of sending a memo with messages (or encoded payload).**

Further development

We are interested in further work on this project. There are many things to do in the next steps. For example, support for debots and debrowser, interaction with decentralized applications, improvement of the user interface, bug fixes and much more. We hope the community will enjoy our work!