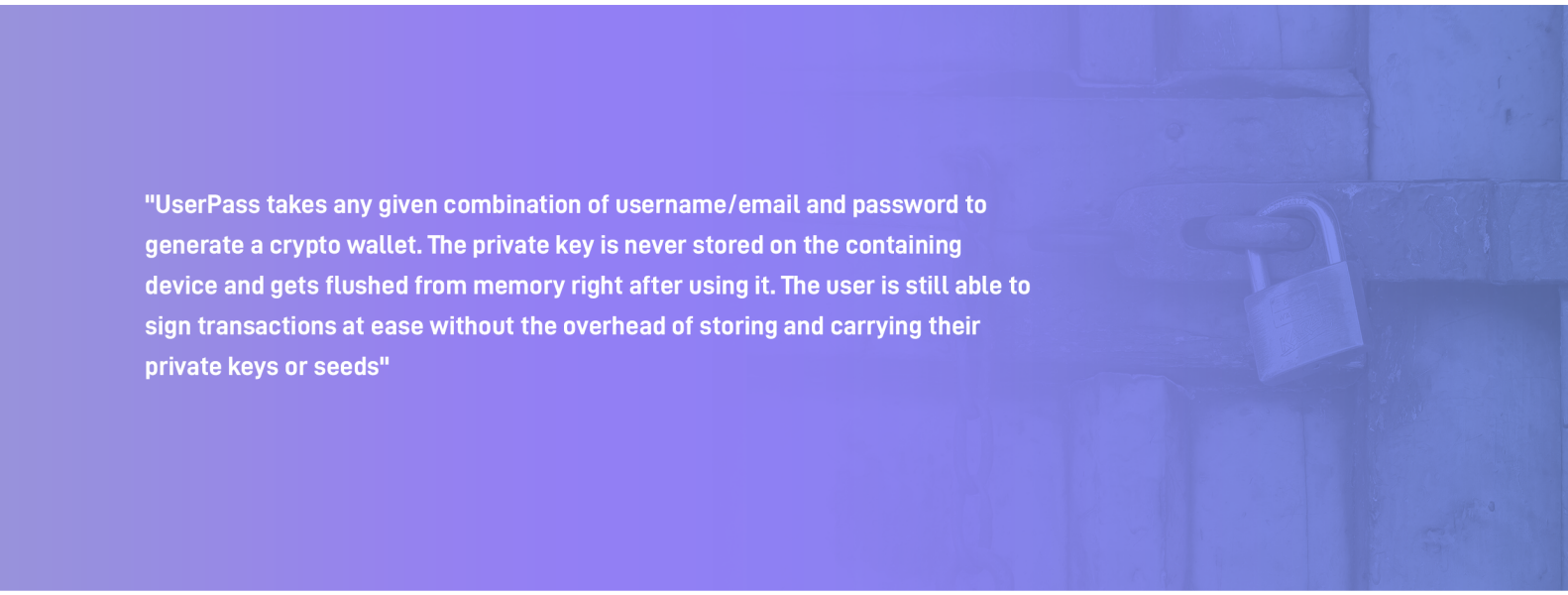
UserPass

Crypto wallet security for everyone



"UserPass takes any given combination of username/email and password to generate a crypto wallet. The private key is never stored on the containing device and gets flushed from memory right after using it. The user is still able to sign transactions at ease without the overhead of storing and carrying their private keys or seeds"

The Problem

- Existing wallet and private key generation solutions feel alineating for average users.
- Seeds, hardware wallets and their physical limitations when it comes to pop-up usage.
- Even for tech savants the storage and usage of wallets can be a burden.

The Solution

- UserPass securely derives a private key using a combination of username and password.
- It provides a familiar, known access point for average users to have access to a crypto wallet.
- For the initiated it represents an easier, volatile web wallet that can be used as a cryptocash container for day to day operations without the overhead of physical access to their private keys.

How it Works

- Making use argon2 to safely derive user-provided keys and the SHA3-Shake128 hashing function for dynamic output sizes we can deliver a secure and transversal user-friendly wallet derivation pattern.
- Thanks to the variable output length of Shake128 the resulting userpass key can be hashed into the private key of any desired format

The Roadmap

- The formal definition for the project can be found in the Github repository https://github.com/bearni95/User-Pass
- A first draft of an Ethereum volatile web wallet is on the making and will be published soon
- Future integrations in the field of self-sovereign/decentralized identities and other cryptocurrency wallets are to be discussed.

Bernat Canal - 2020