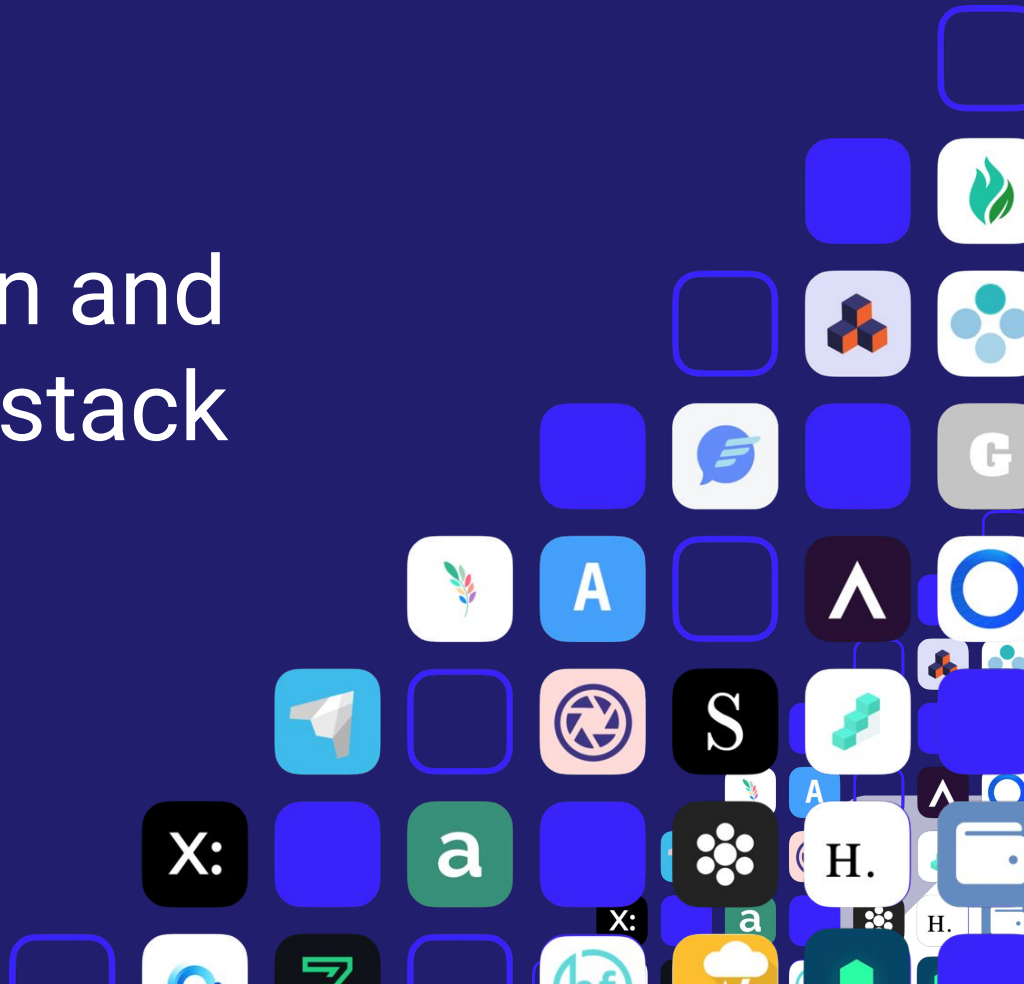
Blockstack

Decentralized Login and Storage with Blockstack

Paris P2P Festival
Ground Control
11 Jan 2020

Friedger Müffke
Engineering Partner



Blockstack

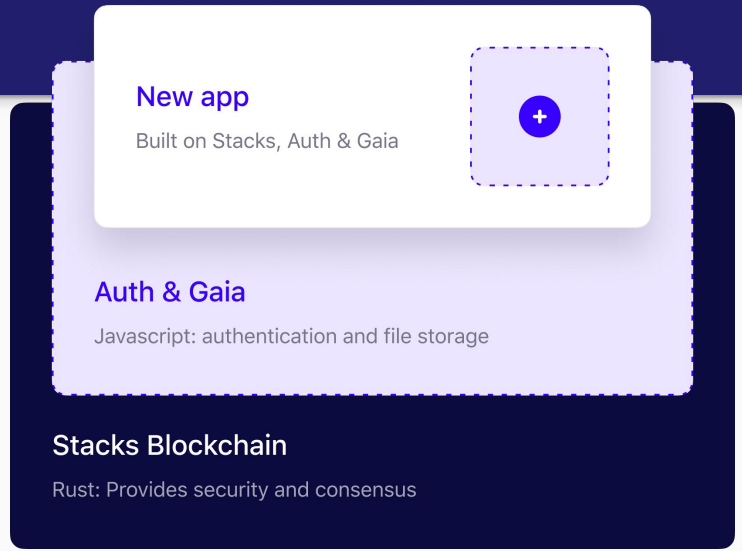
Disclaimer

Technology in new
Society not ready
No financial advice

Blockstack

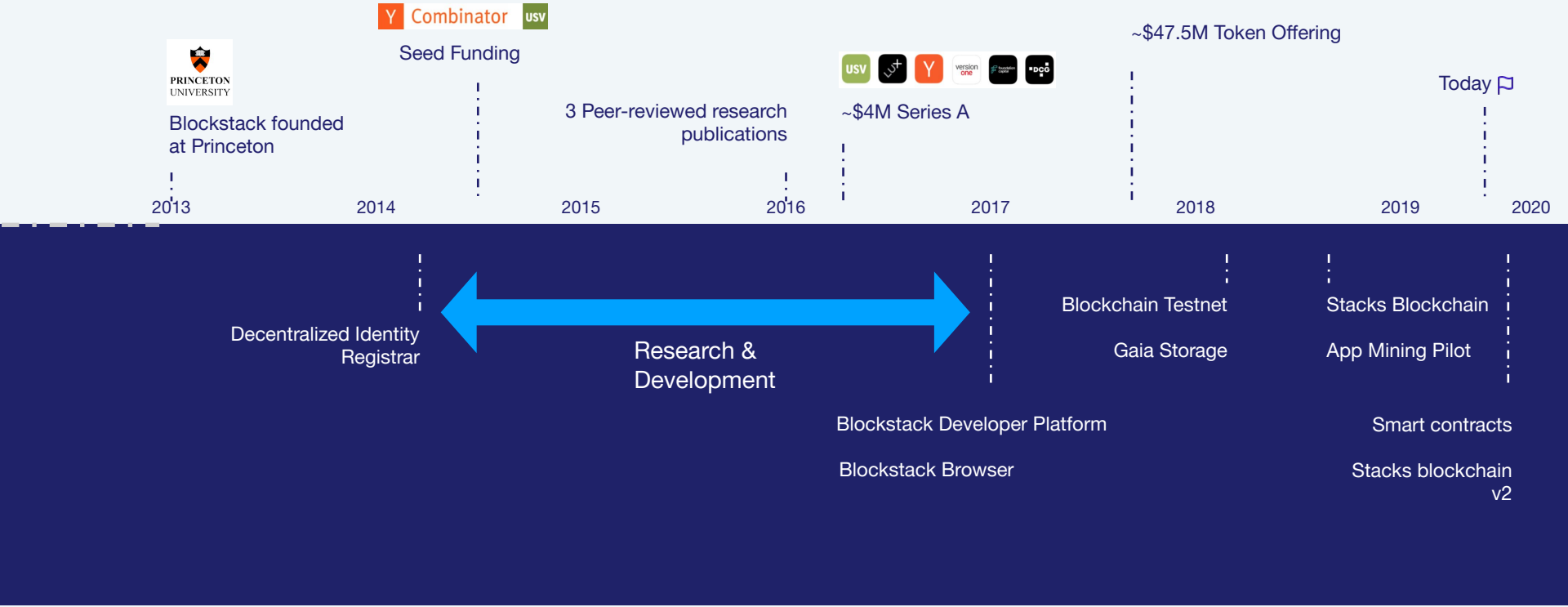
“We abstract the Blockchain complexity so app developers can focus on building great apps”

- Keep auth and smart contracts on-chain
- Keep encrypted data off-chain
- Wrap everything in an easy JavaScript API



Any javascript developer can build a Blockstack app in 1 hour. No coding language to learn.

Blockstack History



Blockstack

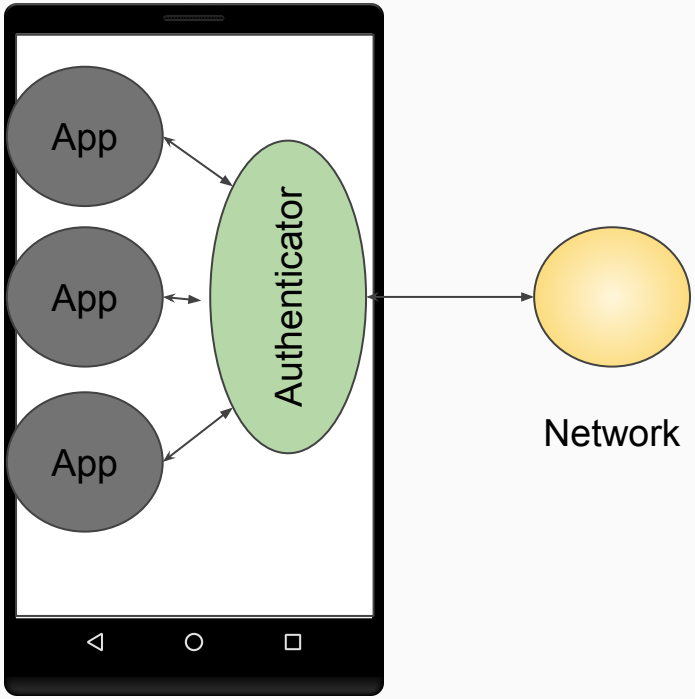
Decentralized Identity

- Self-sovereign
- Verifiable
- Person vs. profiles

Cryptographic Keys

- No more passwords
- W3C working group

Decentralized Identity - “Login”



Forget about OAuth dance!
Forget about email!

Use Decentralized Identifiers (DID)
did:*example:123456789abcdefghi*

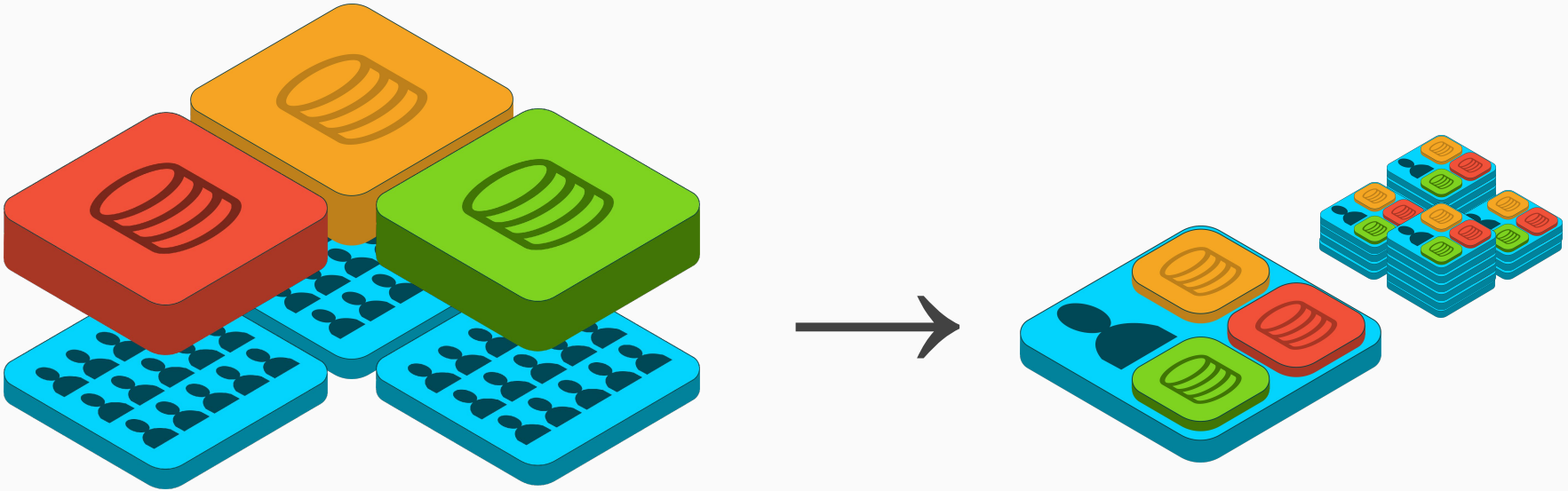
45 different DID methods
Blockstack is one of them

Decentralized Storage

- Diversity in locations
- Distributed vs. self-controlled
- Server-less apps

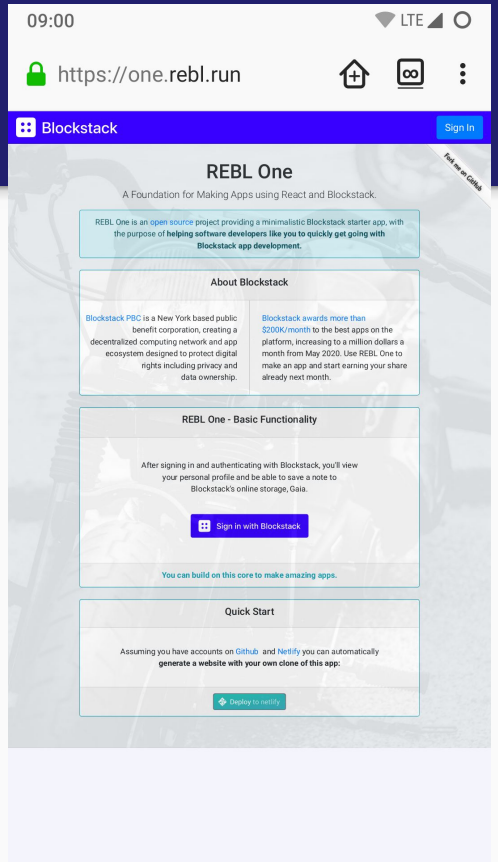
Blockstack:
Gaia protocol

Blockstack



Blockstack Starter Kit

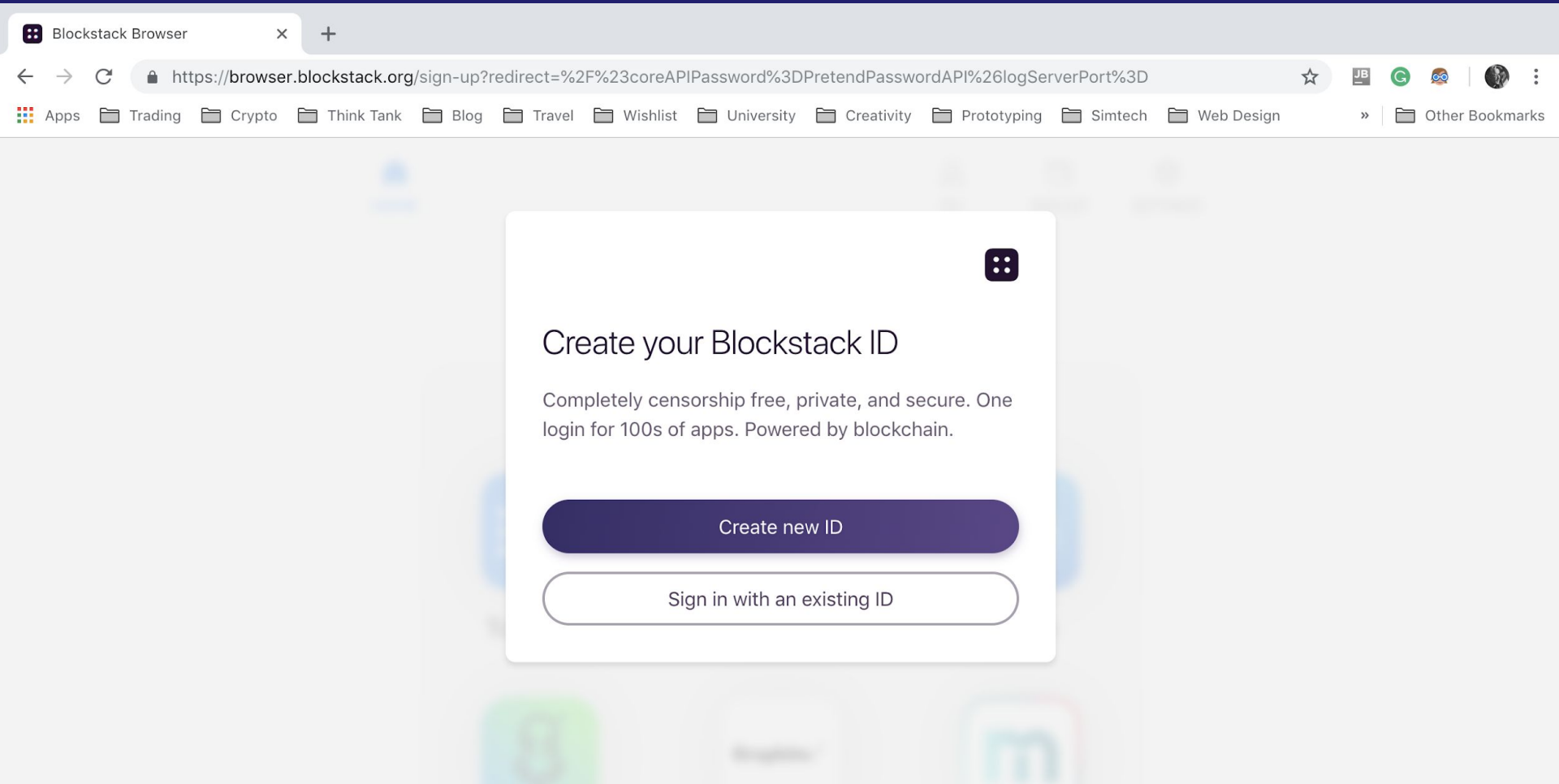
https://one.rebl.run



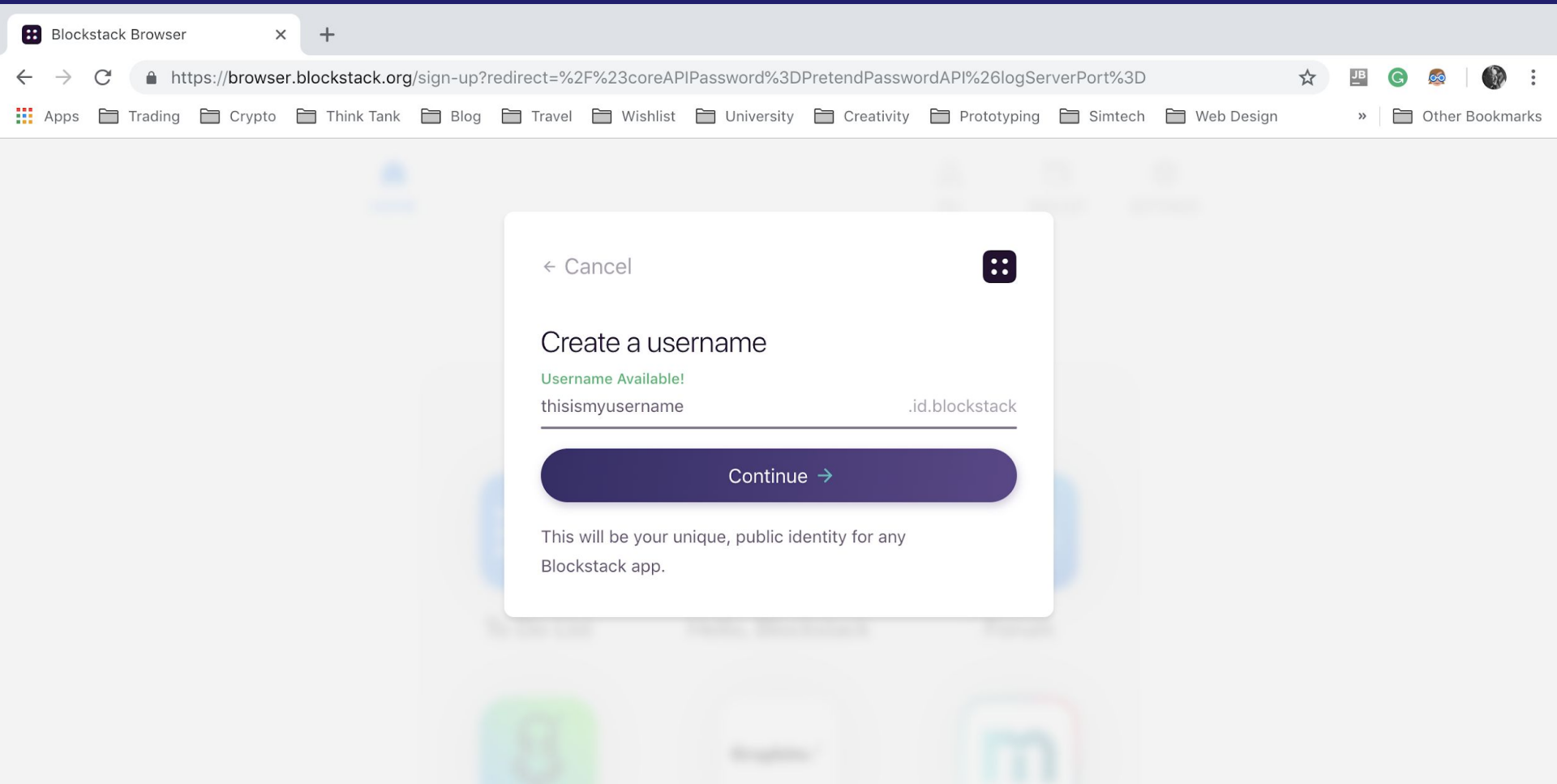
react-blockstack
blockstack.js
react.js

bootstrap

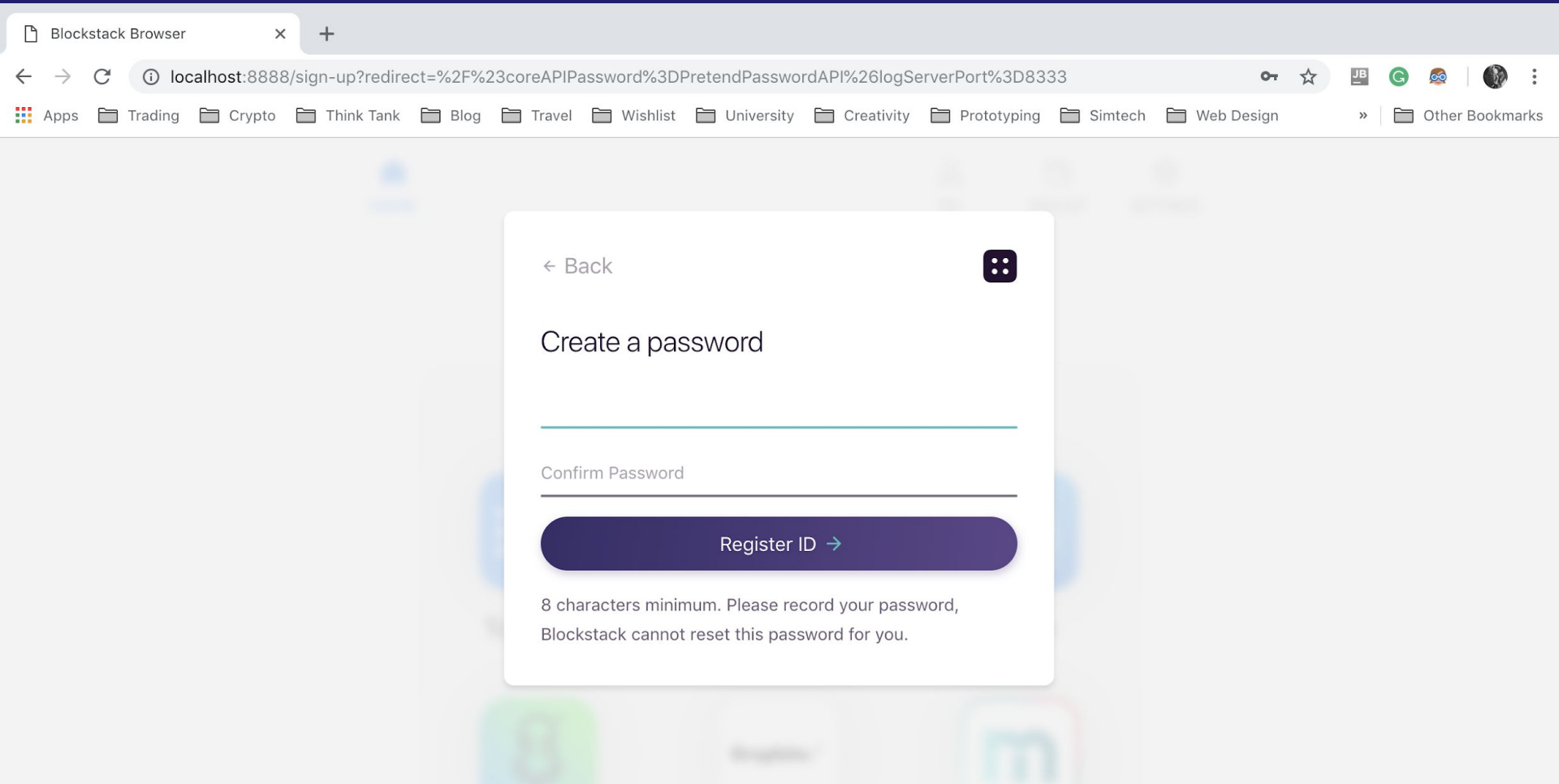
Create your username



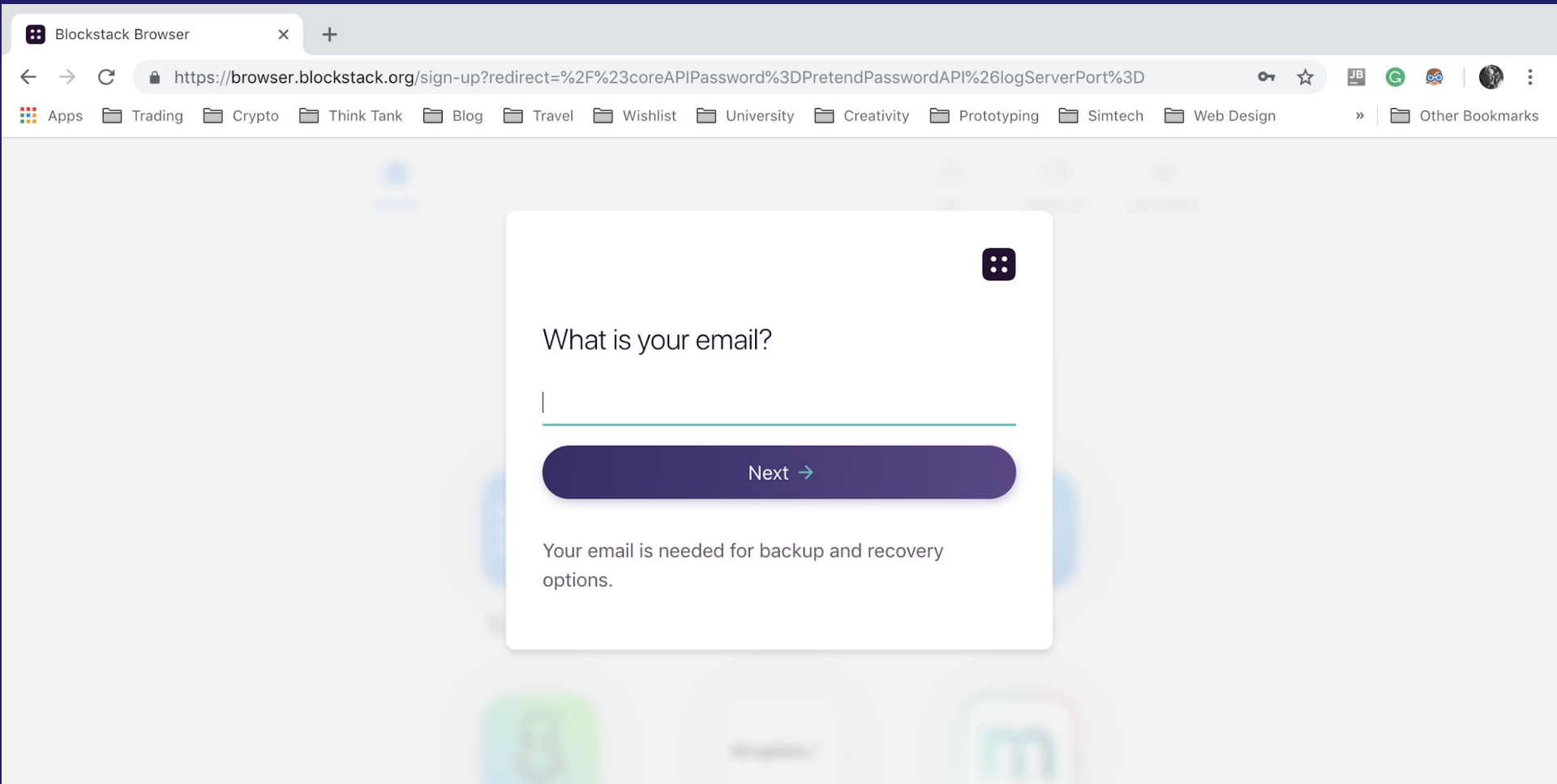
Check Availability



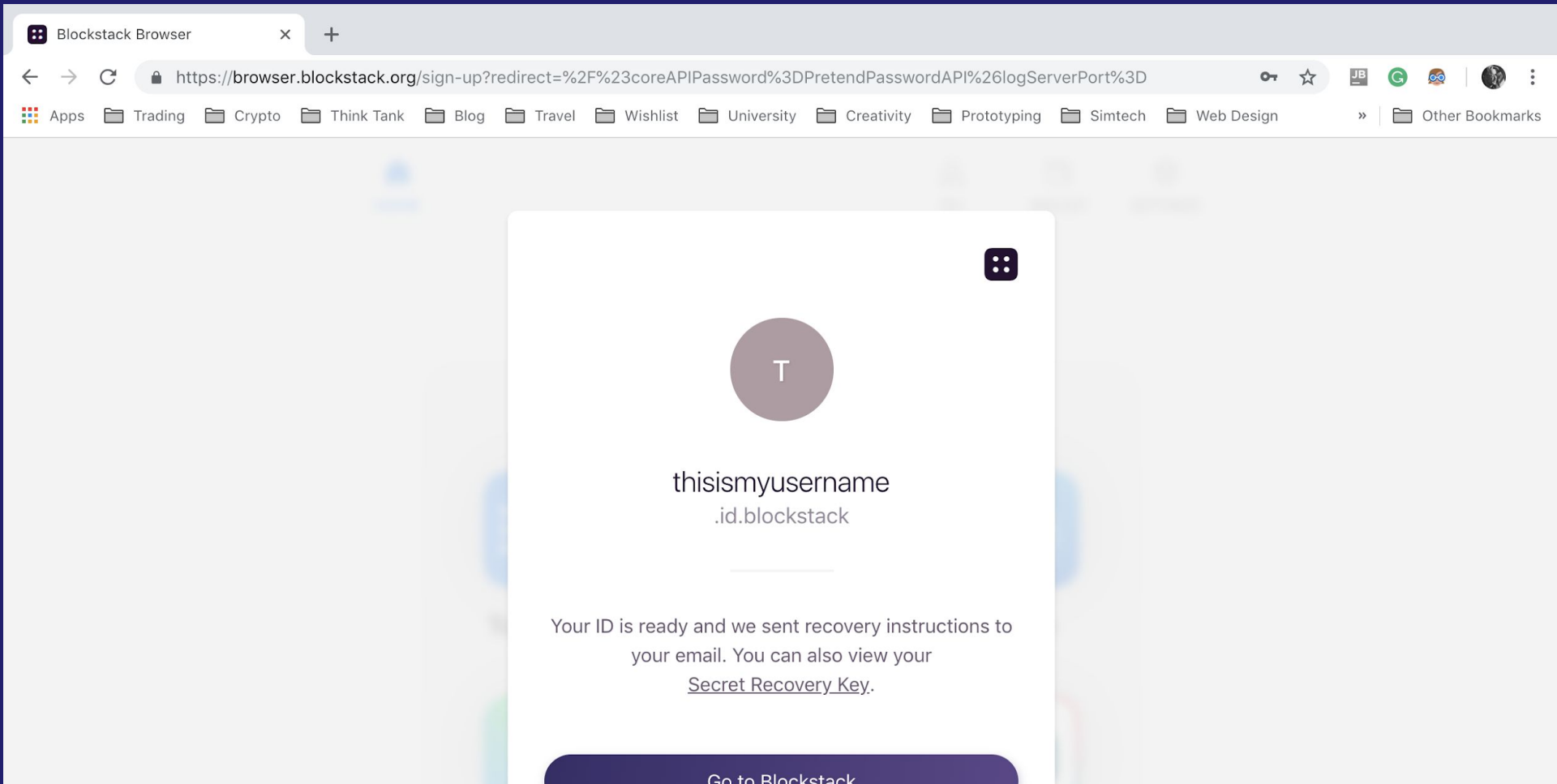
Set Password (for on-device security)



Enter email (for recovery)

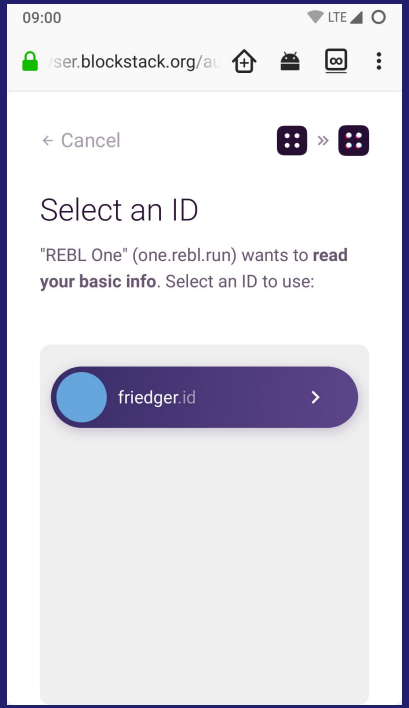


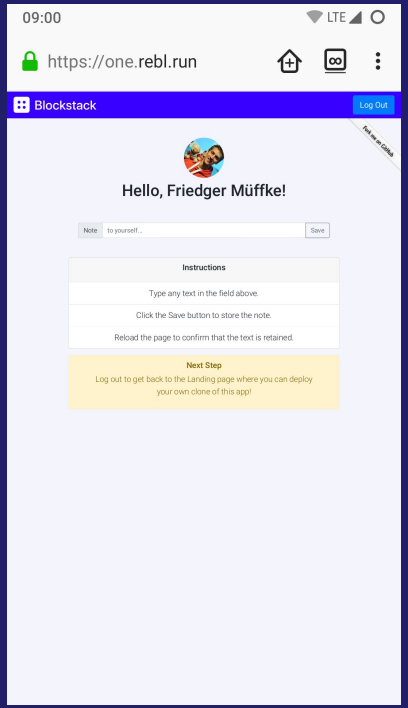
ID ready


Blockstack Browser
https://browser.blockstack.org/sign-up?redirect=%2F%23coreAPIPassword%3DPretendPasswordAPI%26logServerPort%3D
Apps
Trading
Crypto
Think Tank
Blog
Travel
Wishlist
University
Creativity
Prototyping
Simtech
Web Design
Other Bookmarks
T
thisismyusername
.id.blockstack
Your ID is ready and we sent recovery instructions to your email. You can also view your Secret Recovery Key.
Go to Blockstack

Blockstack

Blockstack Starter Kit





Blockstack

Blockstack Profile

did:stack:v0:1Mk9gNKVdeLsodtbtUssVJmJMRHaEa2hGF-67

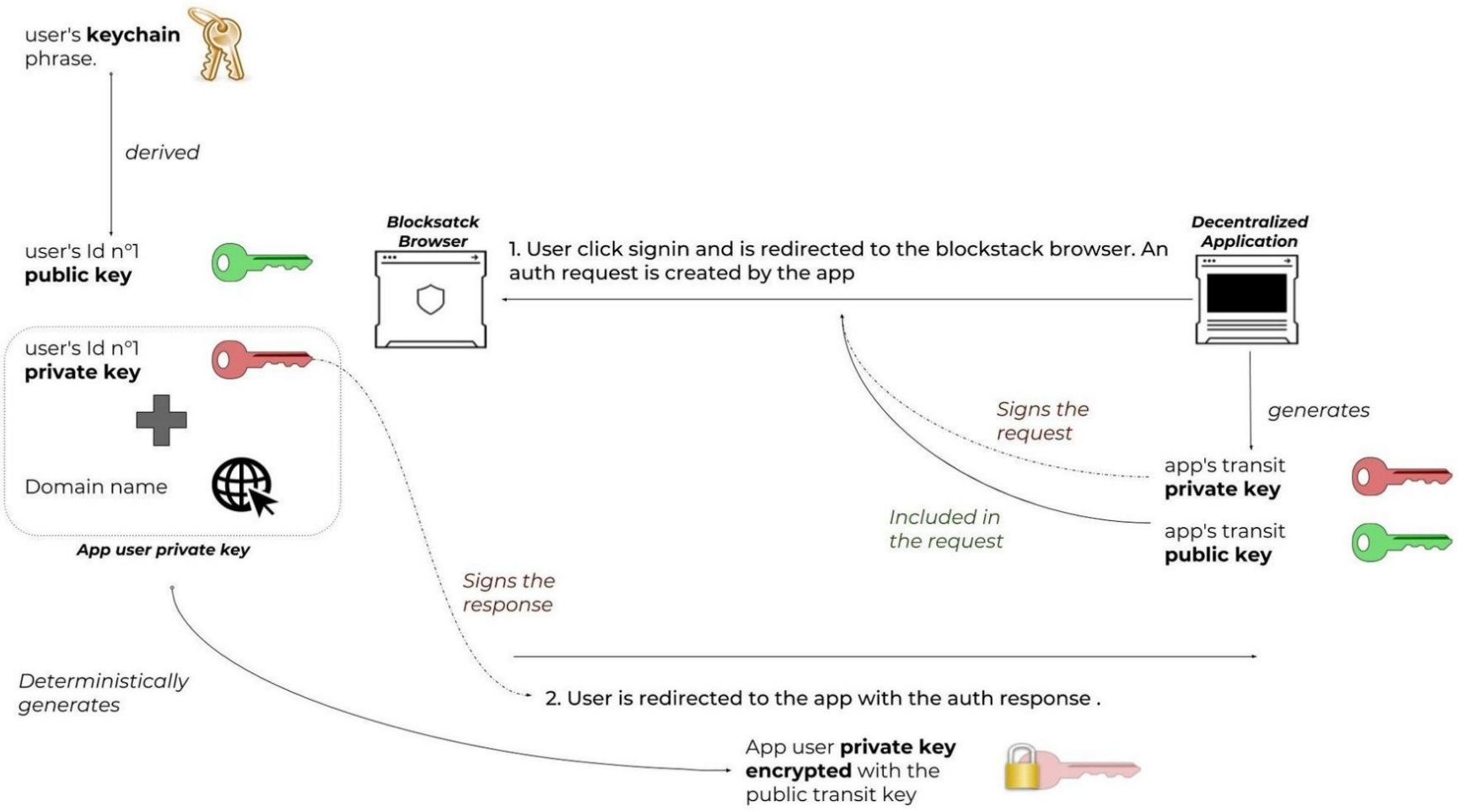
Friedger Müffke
Entredeveloper in Europe
friedger.id

https://app-center.openintents.org/u/friedger.id
https://explorer.blockstack.org/name/friedger.id
https://landr.me/friedger.id

Blockstack

Blockstack Login

```
const {signIn, person} = useBlockstack()


const userSession = new UserSession(appConfig)

userSession.redirectUserToLogin()

userSession.handleAuthResponse()
```


user's **keychain** phrase.
derived
user's Id n°1 **public key**
user's Id n°1 **private key**
Domain name
App user private key
Deterministically generates
Blocksatck Browser
1. User click signin and is redirected to the blockstack browser. An auth request is created by the app
Decentralized Application
Signs the request
generates
app's transit **private key**
Included in the request
app's transit **public key**
Signs the response
2. User is redirected to the app with the auth response .
App user **private key** **encrypted** with the public transit key

Blockstack

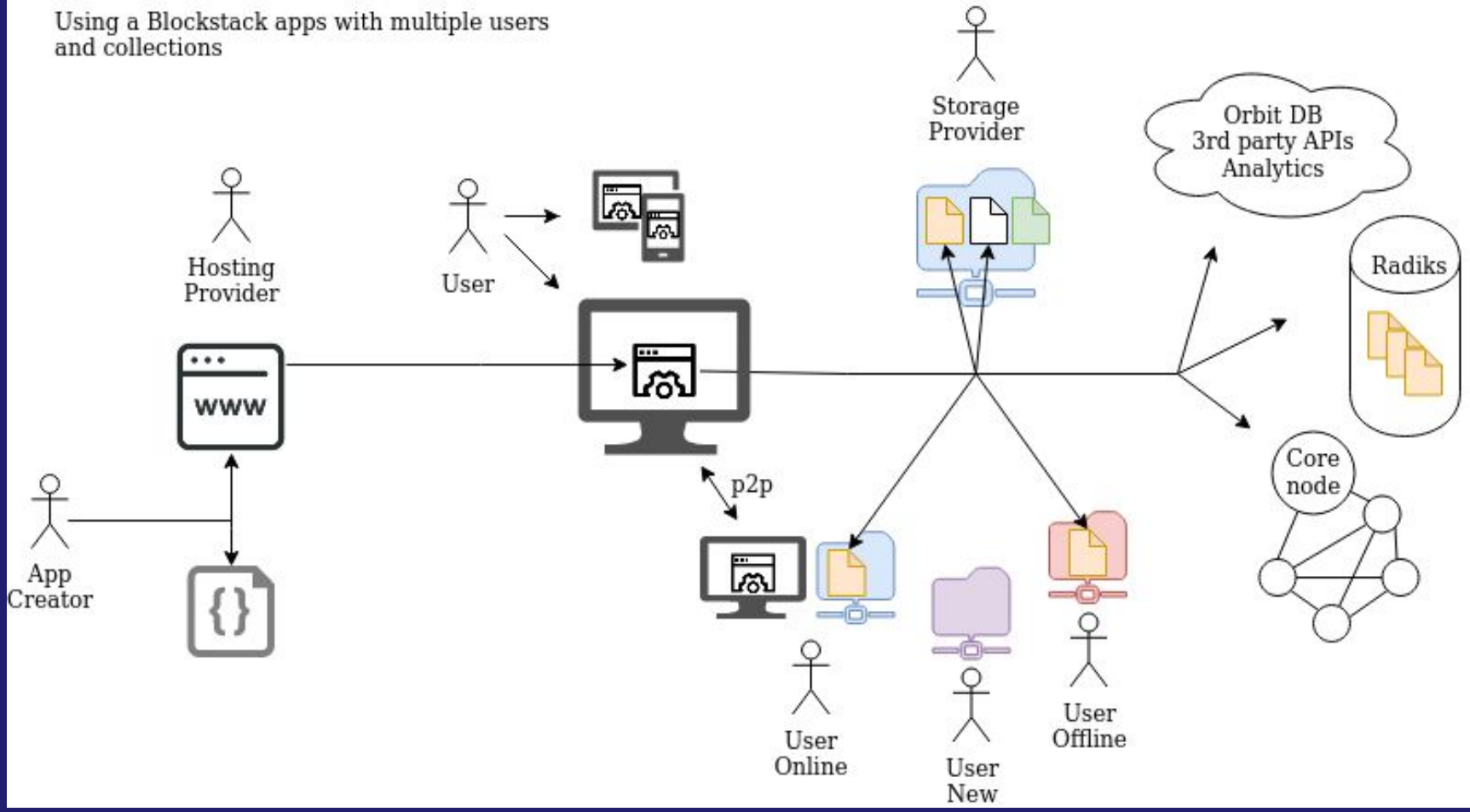
Blockstack Storage

```
const [note, setNote] = useFile(“note.txt”)
```

```
userSession.putFile(“note.txt”, note, options)

userSession.getFile(“note.txt”, options)
```

Blockstack Storage

Using a Blockstack apps with multiple users and collections

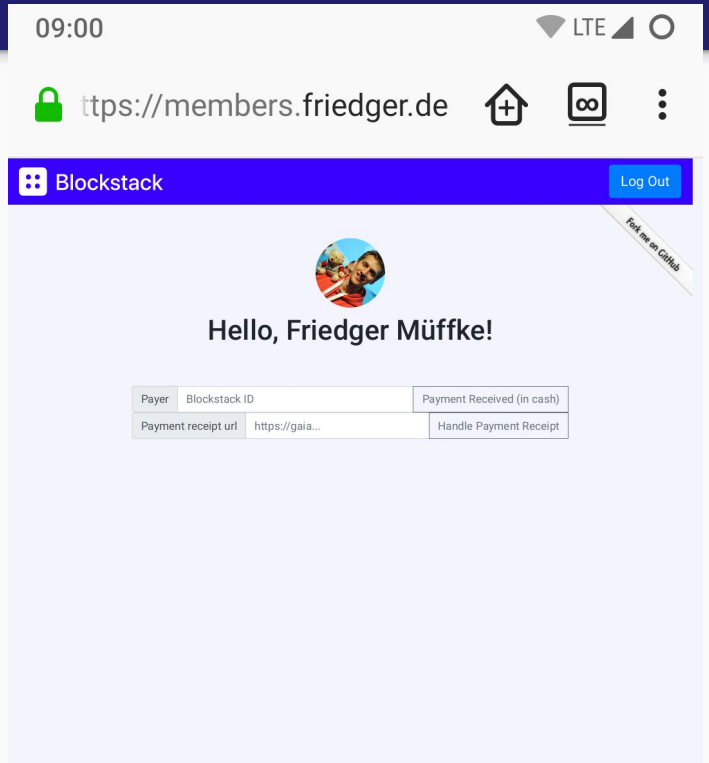


Blockstack

Membership App

1. Create + Store token
2. Fetch + Verify token

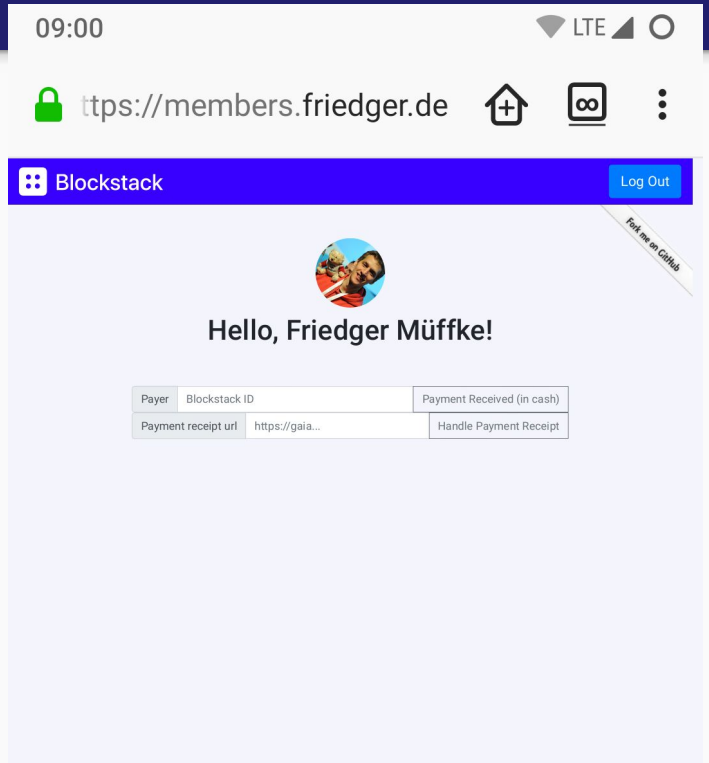
Payment Receipt Token
Membership Token



Blockstack

Membership App - Create + Store Token

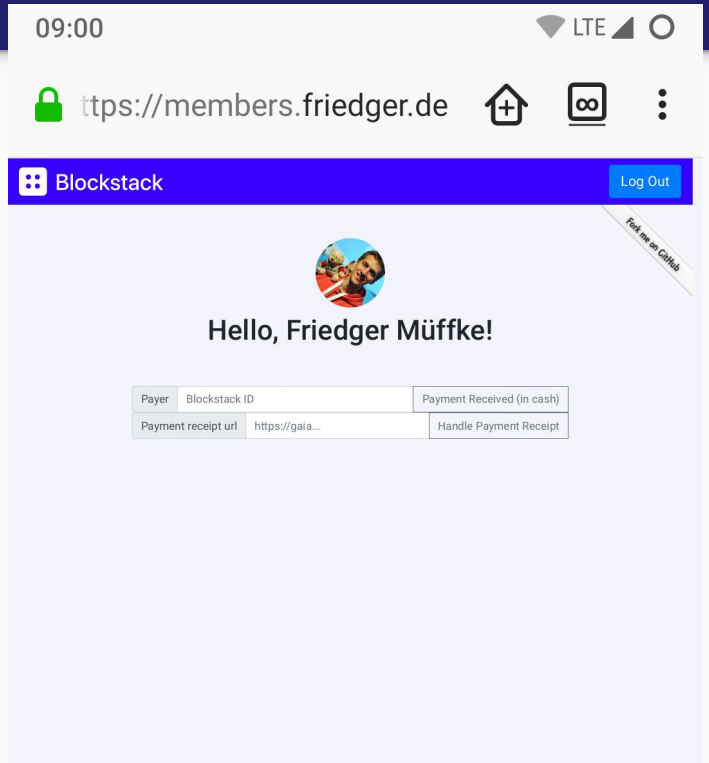
```
signProfileToken(
    claim, userData.appPrivateKey)

userSession.putFile
```



Blockstack

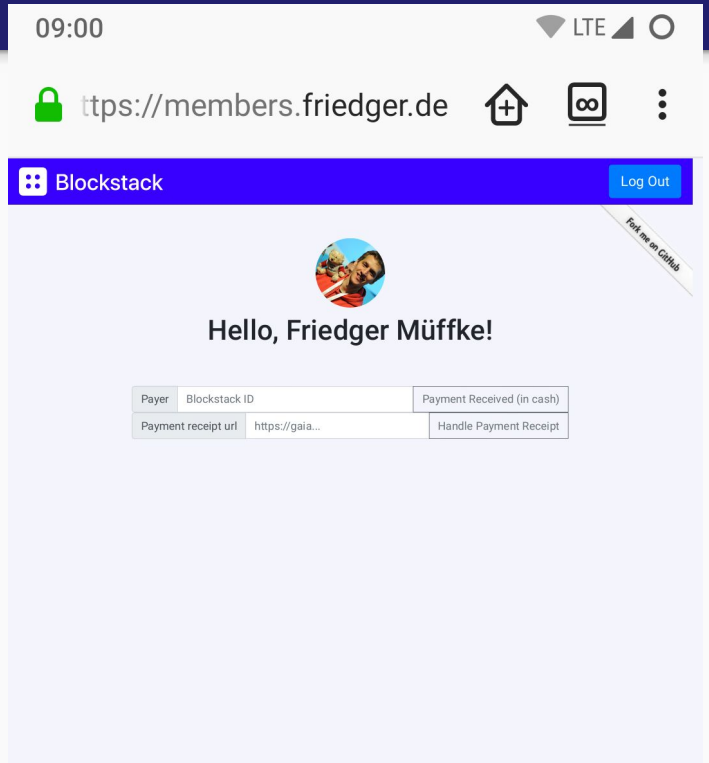
Membership App - Fetch + Verify Token

```
fetch(gaiaReadUrl)

const appPublicKey =
    publicKeyFromPrivate(
        userData.appPrivateKey)

verifyProfileToken(
    token, appPublicKey)
```



Membership App - Bonus

- Private Membership
  encrypt for member(s) only
- Members List
  store links



Blockstack

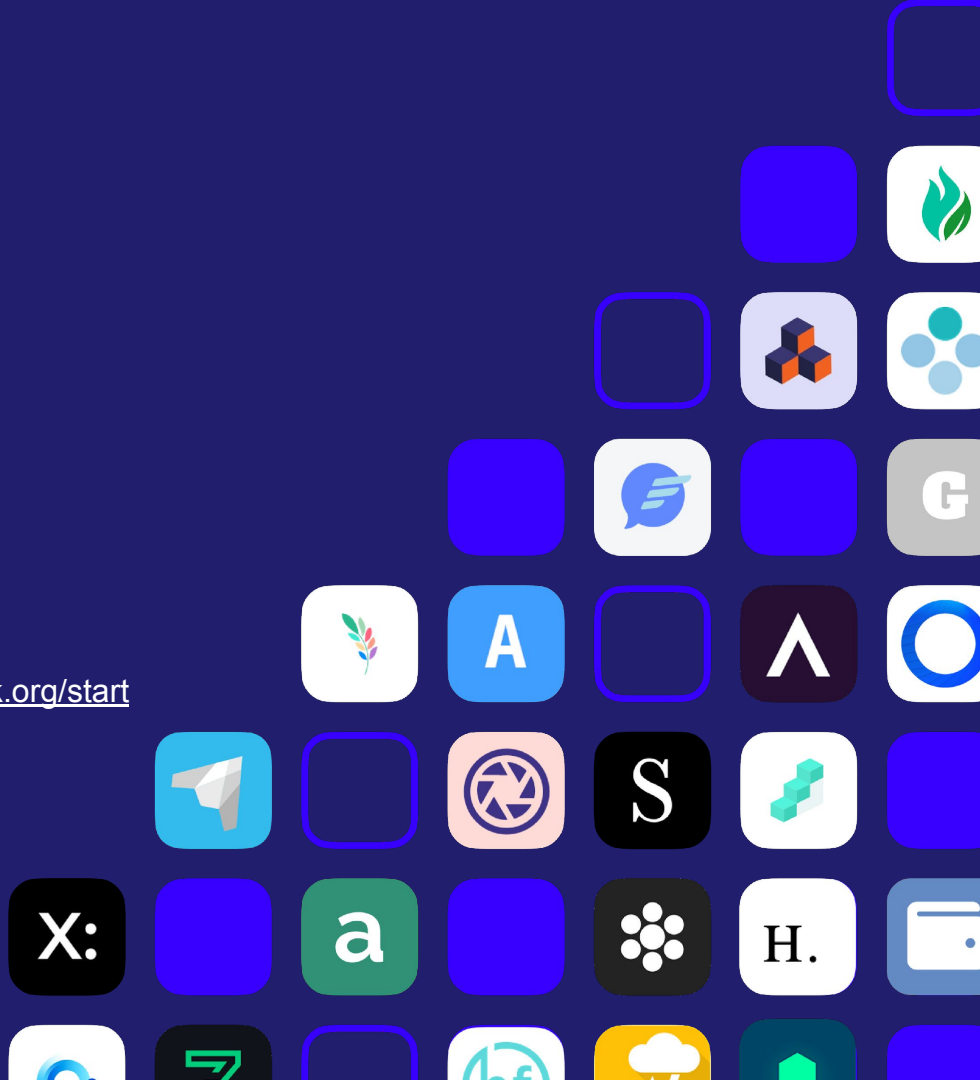
How to get involved?

Participate in our Forum → forum.blockstack.org

Join our Discord→ discord.gg/EhedcW

Contribute code → github.com/blockstack

Read the White papers → blockstack.org/papers

Host meetups, spread the word → community.blockstack.org/start

Credits to
Ludo Galabru
Xan Ditkoff