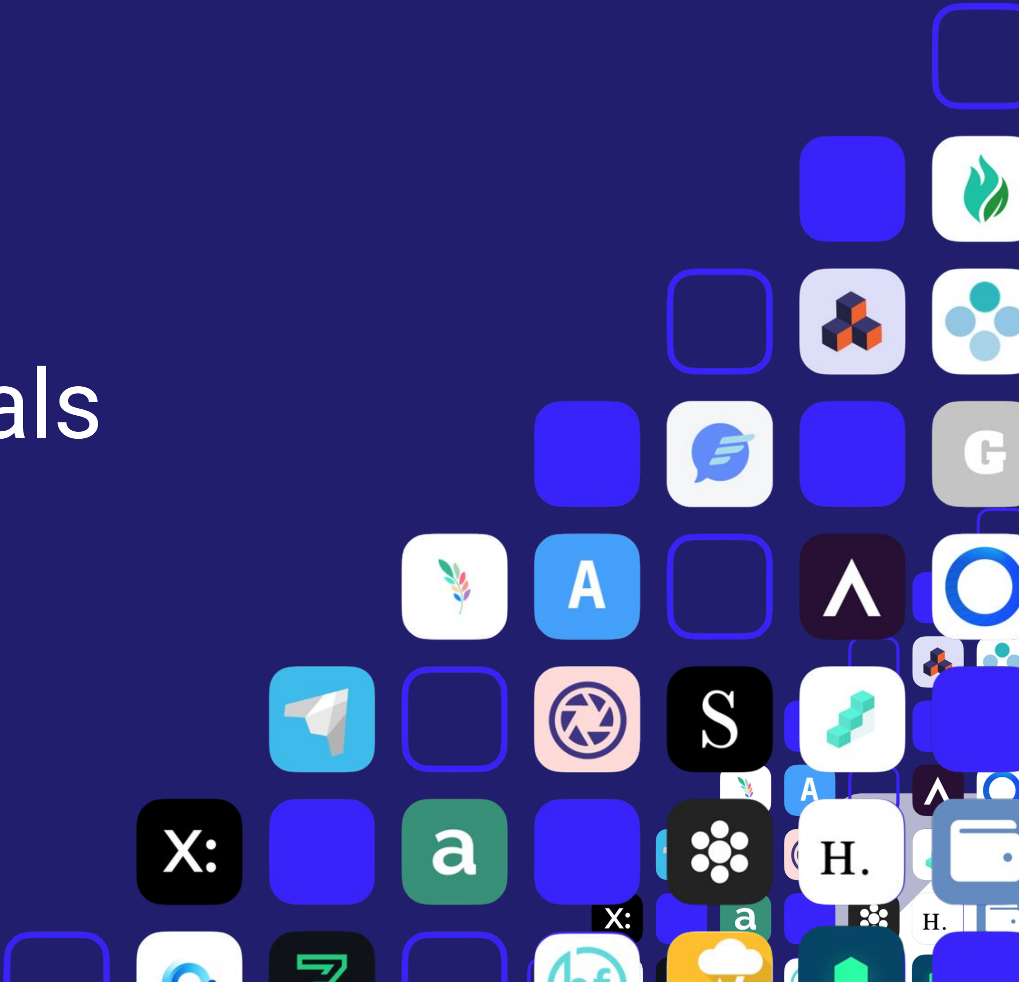
Blockstack

Blockstack and Verifiable Credentials

Paris P2P Festival
Ground Control
10 Jan 2020

Friedger Müffke
Engineering Partner



Disclaimer

Technology in new

Society not ready

No financial advice

Decentralized Identity

Decentralized Identity

- Self-sovereign
- Verifiable

Decentralized Identity

- Self-sovereign
- Verifiable
- Person vs. profiles

Decentralized Identity

- Self-sovereign
- Verifiable
- Person vs. profiles

Cryptographic Keys

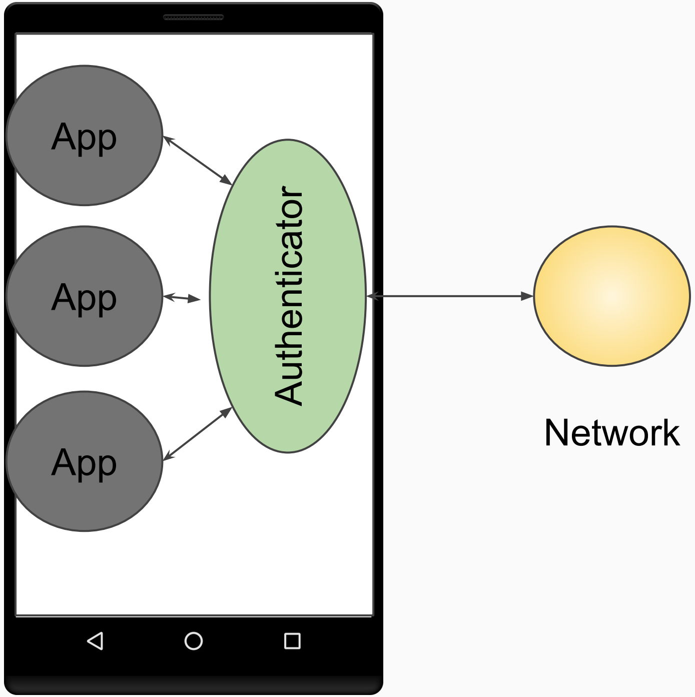
Decentralized Identity

- Self-sovereign
- Verifiable
- Person vs. profiles

- No more passwords
- W3C working group

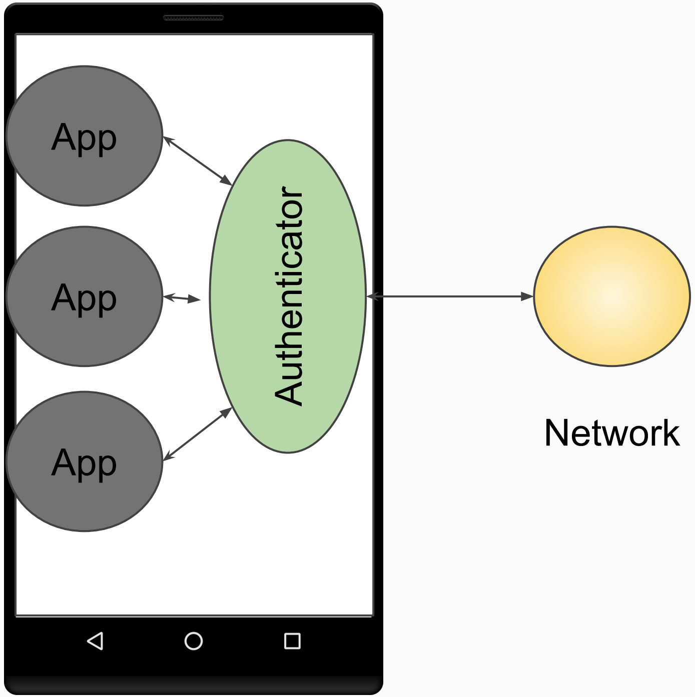
Cryptographic Keys

Decentralized Identity - “Login”



Forget about OAuth dance!
Forget about email!

Decentralized Identity - “Login”

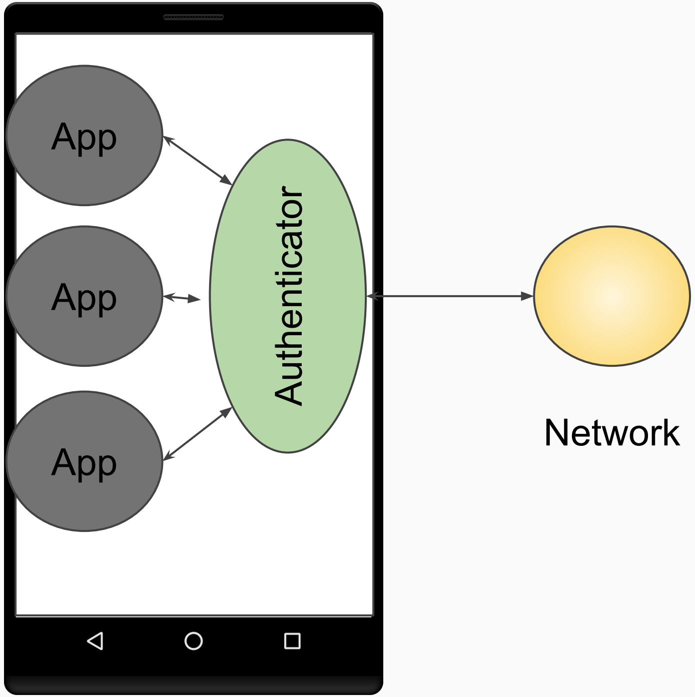


Forget about OAuth dance!
Forget about email!

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

45 different DID methods

Decentralized Identity - “Login”



Forget about OAuth dance!
Forget about email!

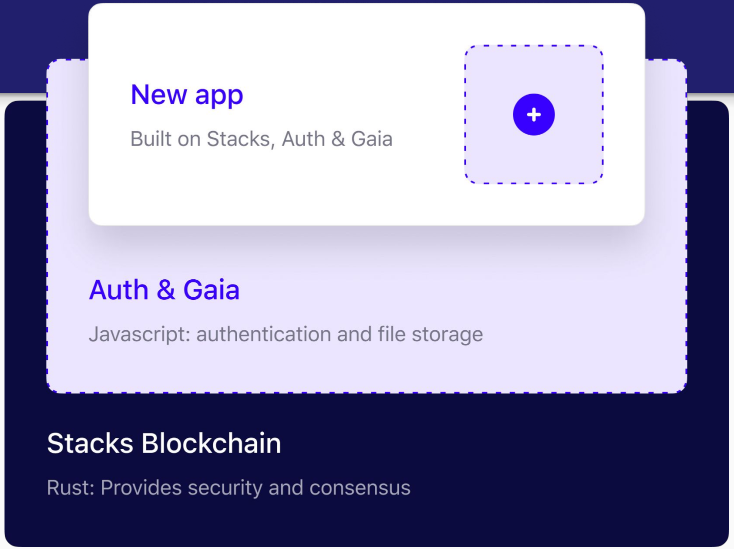
Use Decentralized Identifiers (DID)
did:*example:123456789abcdefghi*

45 different DID methods
Blockstack is one of them

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



New app

Built on Stacks, Auth & Gaia

Auth & Gaia

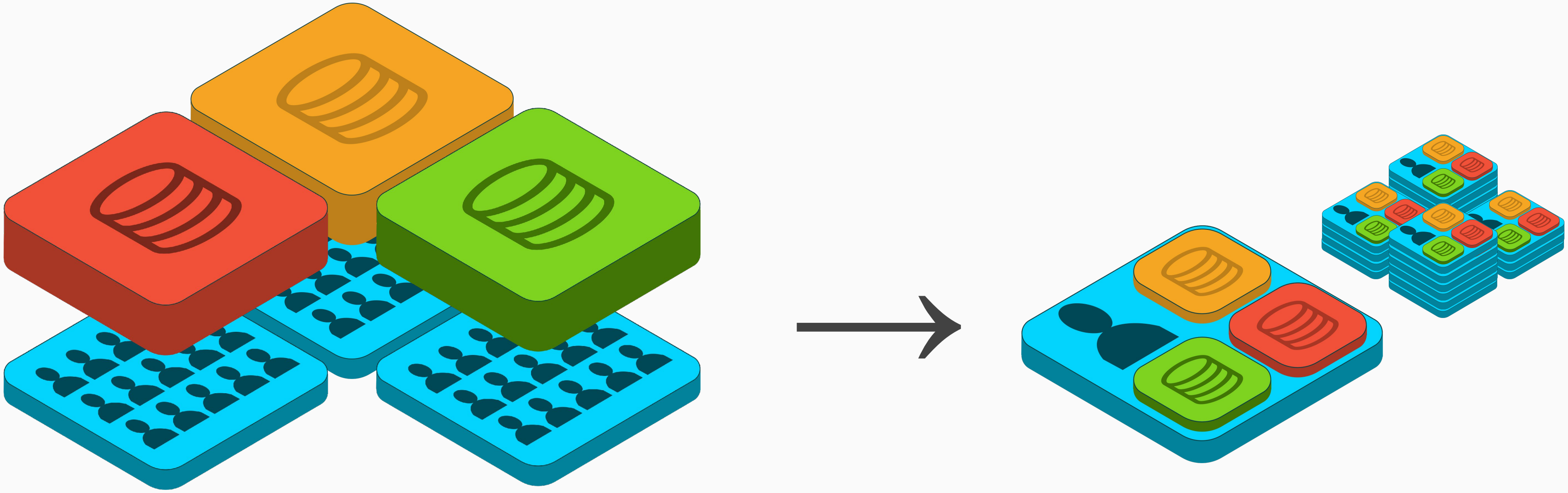
Javascript: authentication and file storage

Stacks Blockchain

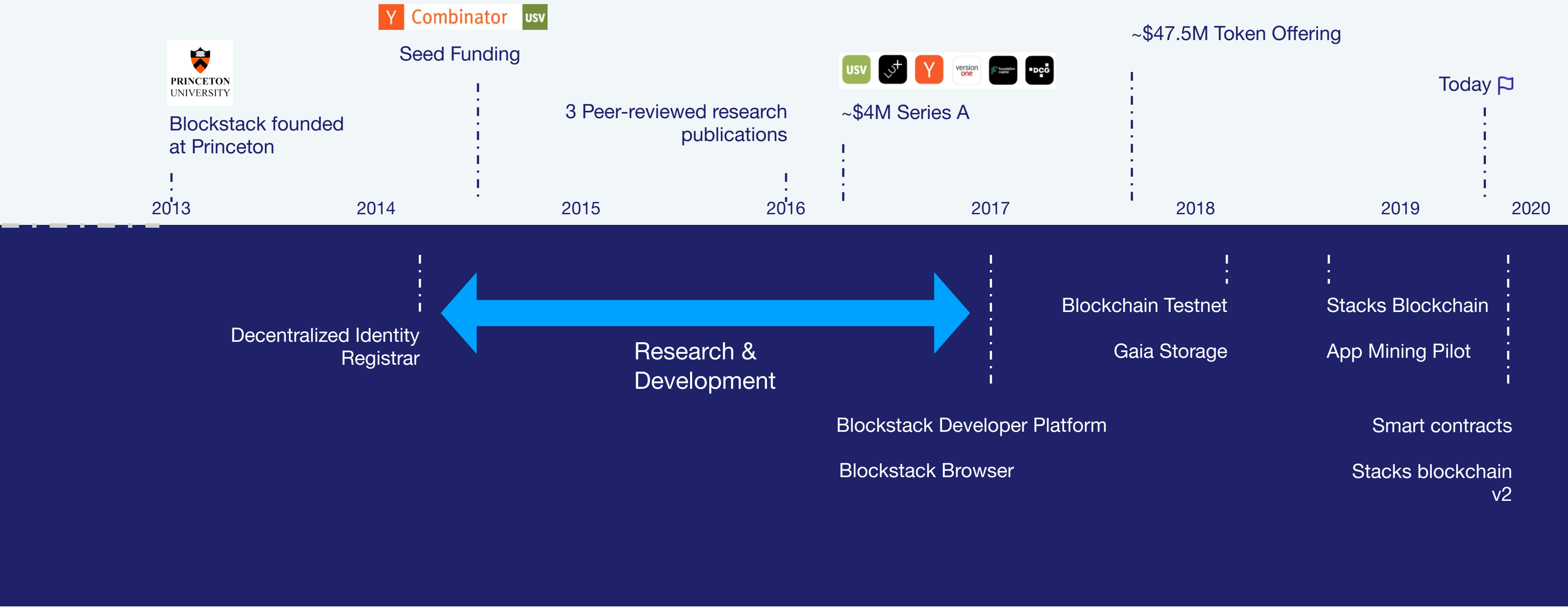
Rust: Provides security and consensus

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

Blockstack



Blockstack History



PRINCETON UNIVERSITY

Blockstack founded at Princeton

Y Combinator USV

Seed Funding

3 Peer-reviewed research publications

USV Y version one DCG

~$4M Series A

~$47.5M Token Offering

Today

2013 2014 2015 2016 2017 2018 2019 2020

Decentralized Identity Registrar

Research & Development

Blockstack Developer Platform

Blockstack Browser

Blockchain Testnet

Gaia Storage

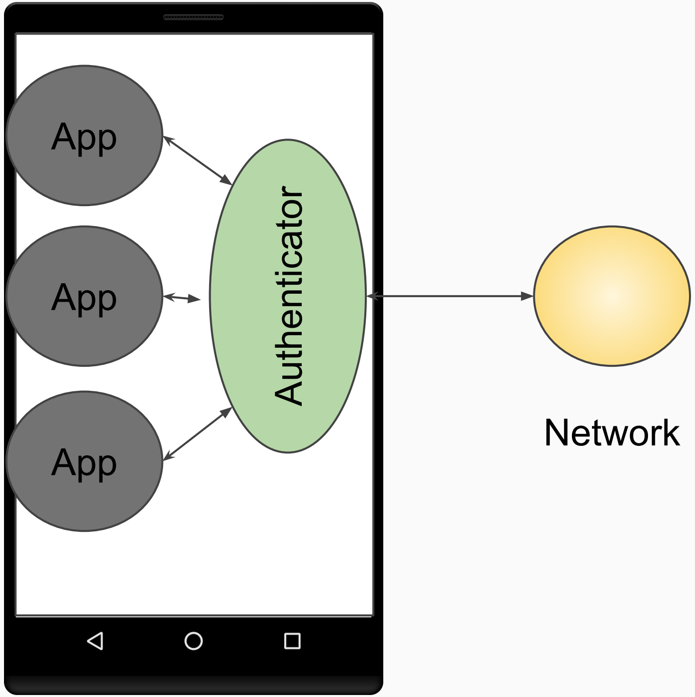
Stacks Blockchain

App Mining Pilot

Smart contracts

Stacks blockchain v2

Decentralized Identity - “Login”

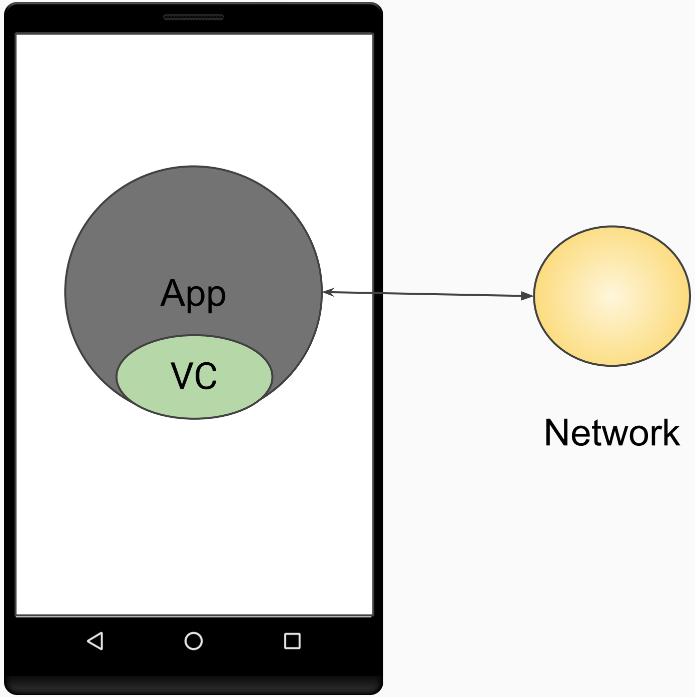


Forget about OAuth dance!
Forget about email!

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

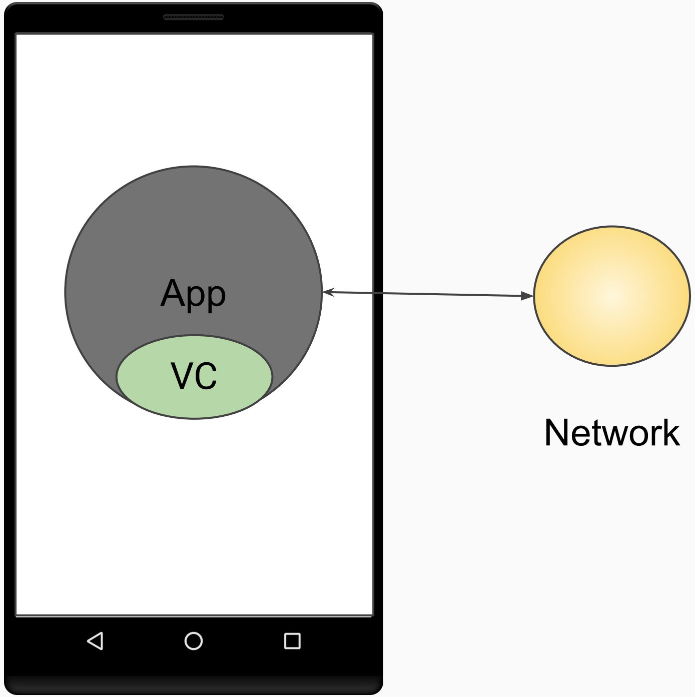
45 different DID methods
Blockstack is one of them

Verifiable Credentials (Claims)



Proof of ownership of key
App acts on behalf of the user

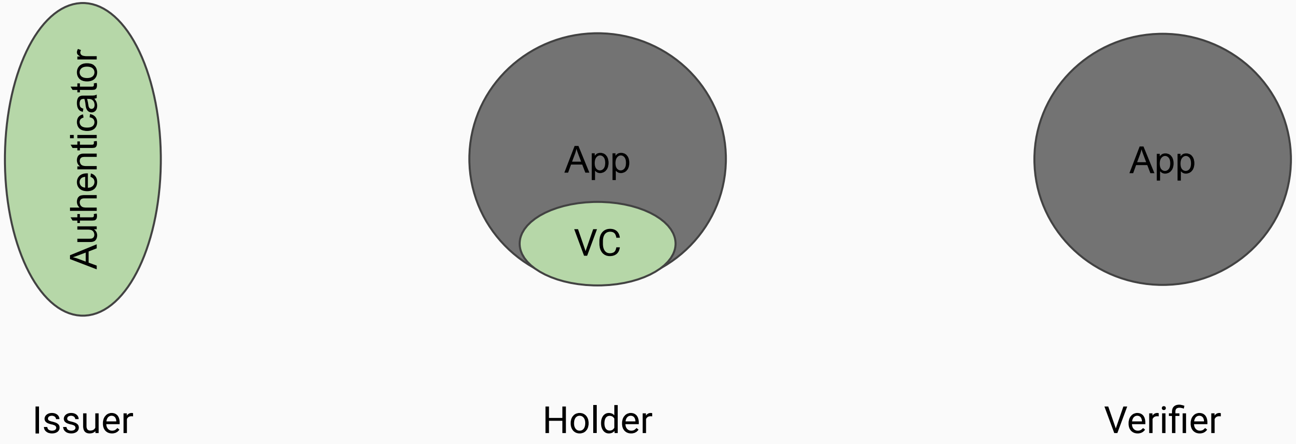
Verifiable Credentials (Claims)



Proof of ownership of key
App acts on behalf of the user

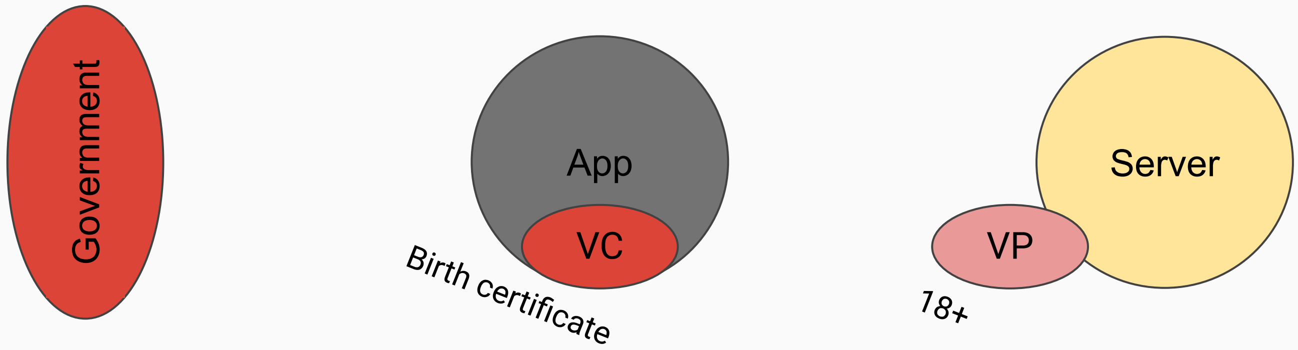
Example:
Retrieve my profile picture

Verifiable Credentials (Claims)



Blockstack

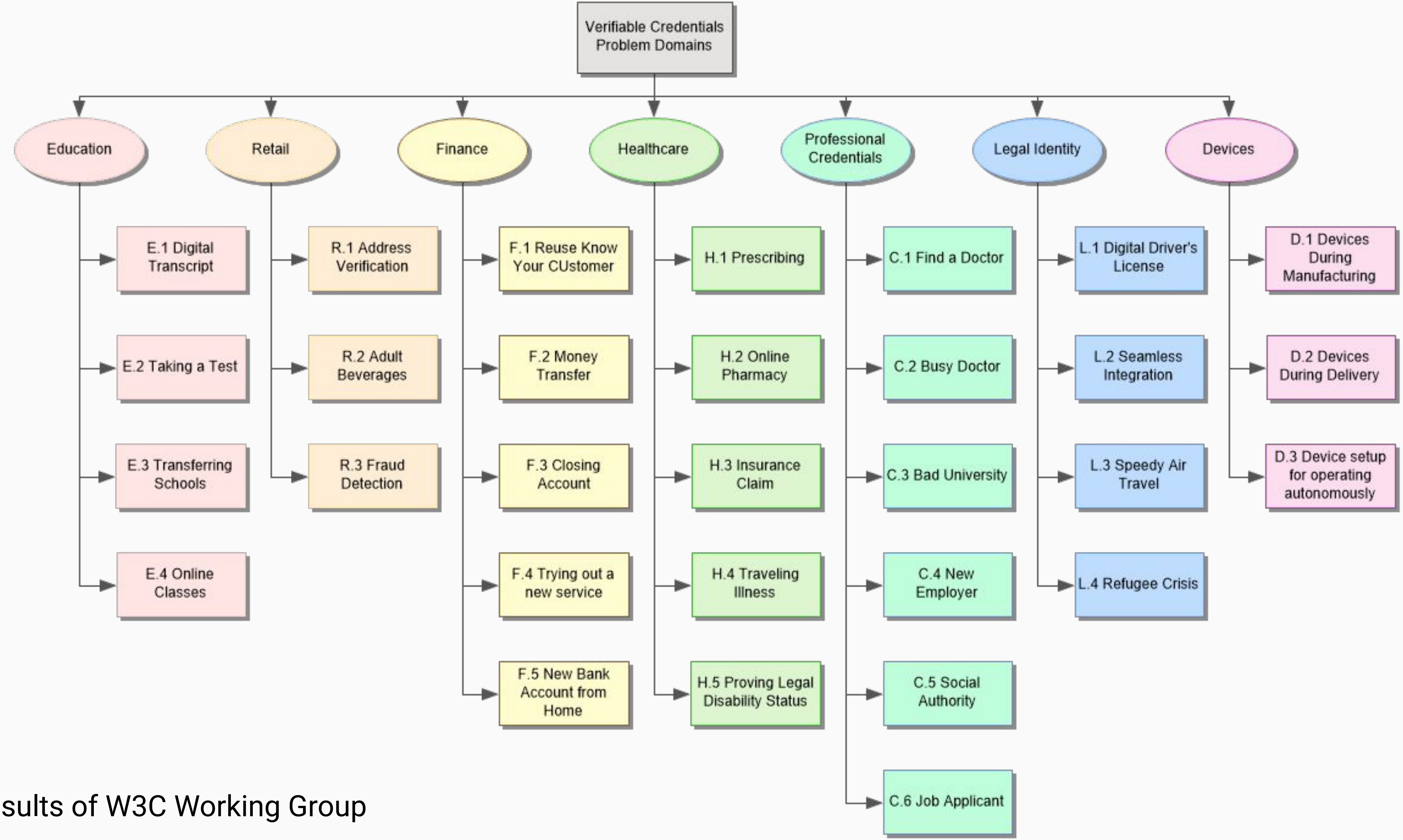
Verifiable Credentials (Claims)



Issuer

Holder

Verifier



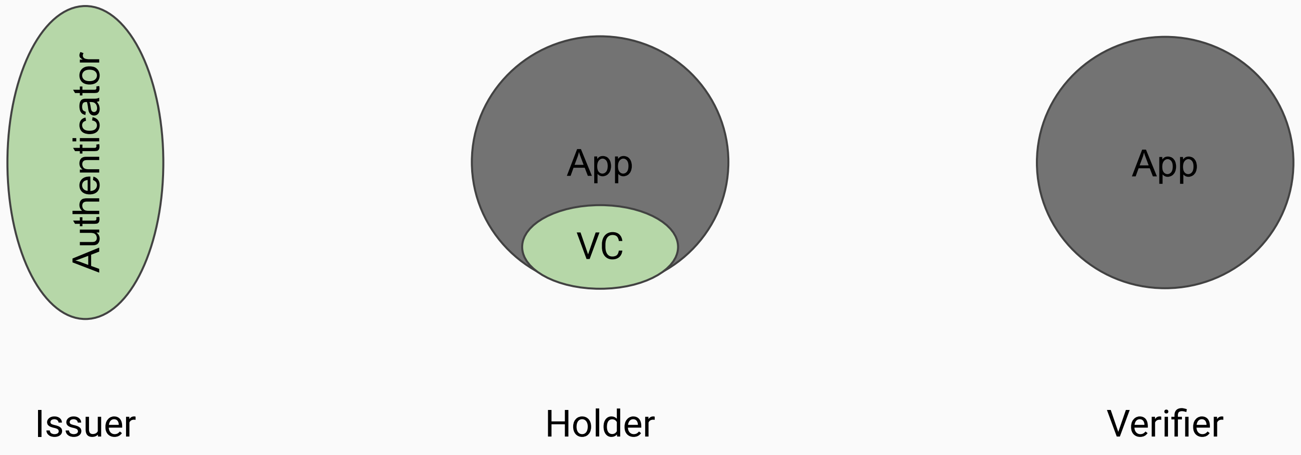
Verifiable Credentials Problem Domains

- Education
  - E.1 Digital Transcript
  - E.2 Taking a Test
  - E.3 Transferring Schools
  - E.4 Online Classes
- Retail
  - R.1 Address Verification
  - R.2 Adult Beverages
  - R.3 Fraud Detection
- Finance
  - F.1 Reuse Know Your CUstomer
  - F.2 Money Transfer
  - F.3 Closing Account
  - F.4 Trying out a new service
  - F.5 New Bank Account from Home
- Healthcare
  - H.1 Prescribing
  - H.2 Online Pharmacy
  - H.3 Insurance Claim
  - H.4 Traveling Illness
  - H.5 Proving Legal Disability Status
- Professional Credentials
  - C.1 Find a Doctor
  - C.2 Busy Doctor
  - C.3 Bad University
  - C.4 New Employer
  - C.5 Social Authority
  - C.6 Job Applicant
- Legal Identity
  - L.1 Digital Driver's License
  - L.2 Seamless Integration
  - L.3 Speedy Air Travel
  - L.4 Refugee Crisis
- Devices
  - D.1 Devices During Manufacturing
  - D.2 Devices During Delivery
  - D.3 Device setup for operating autonomously

Results of W3C Working Group

Blockstack

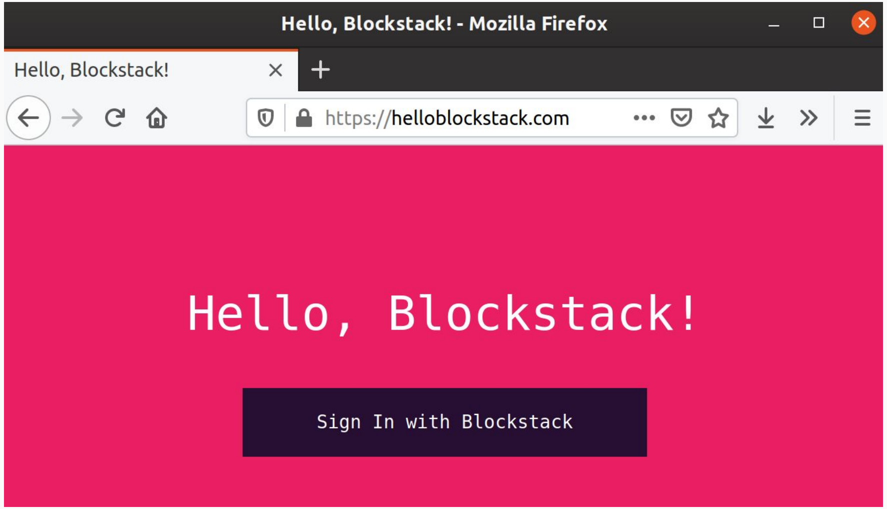
Verifiable Credentials (Claims)



Blockstack

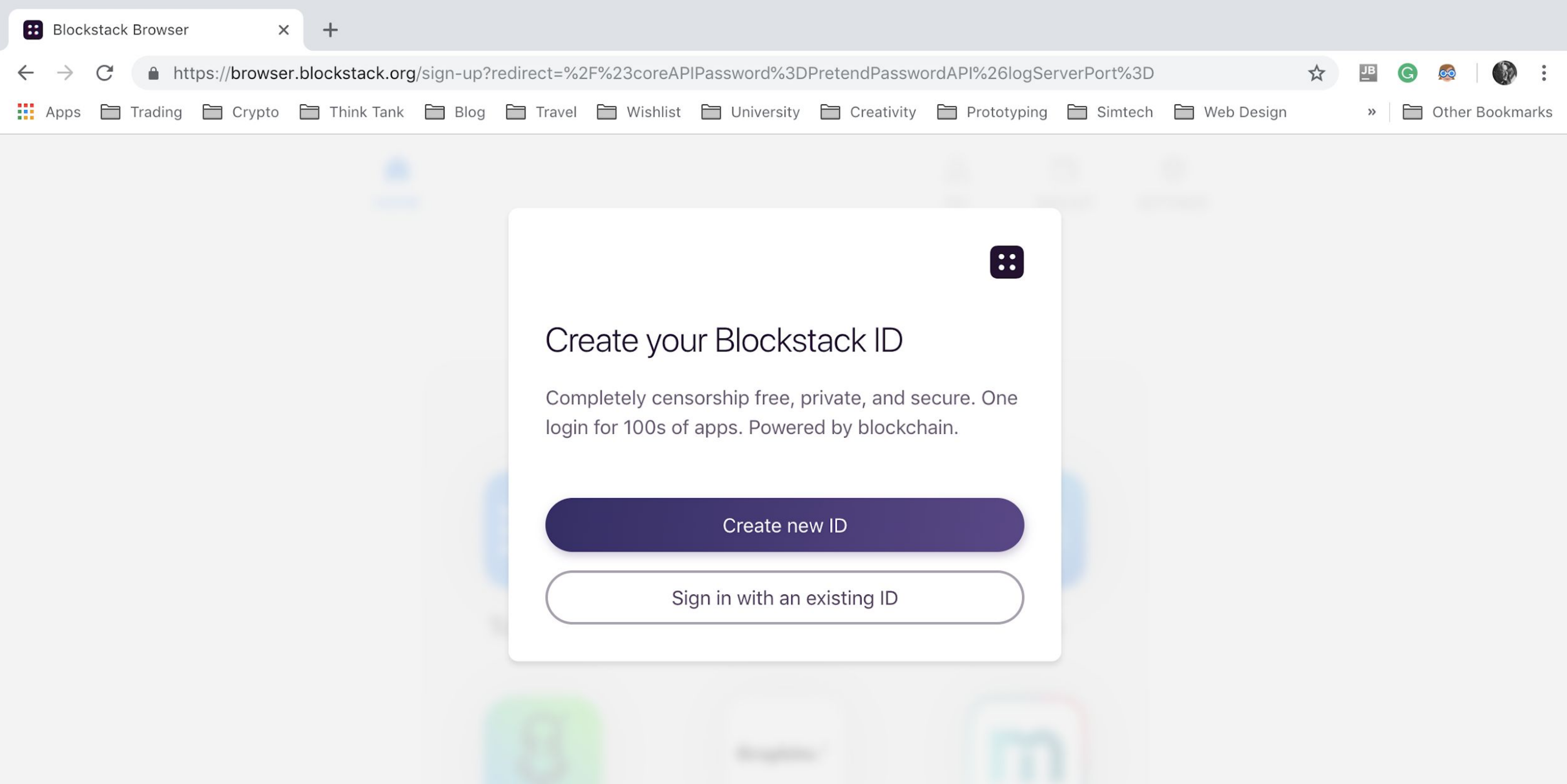
Verifiable Credentials (Claims) - Demo

https://helloblockstack.com



Hello, Blockstack! - Mozilla Firefox

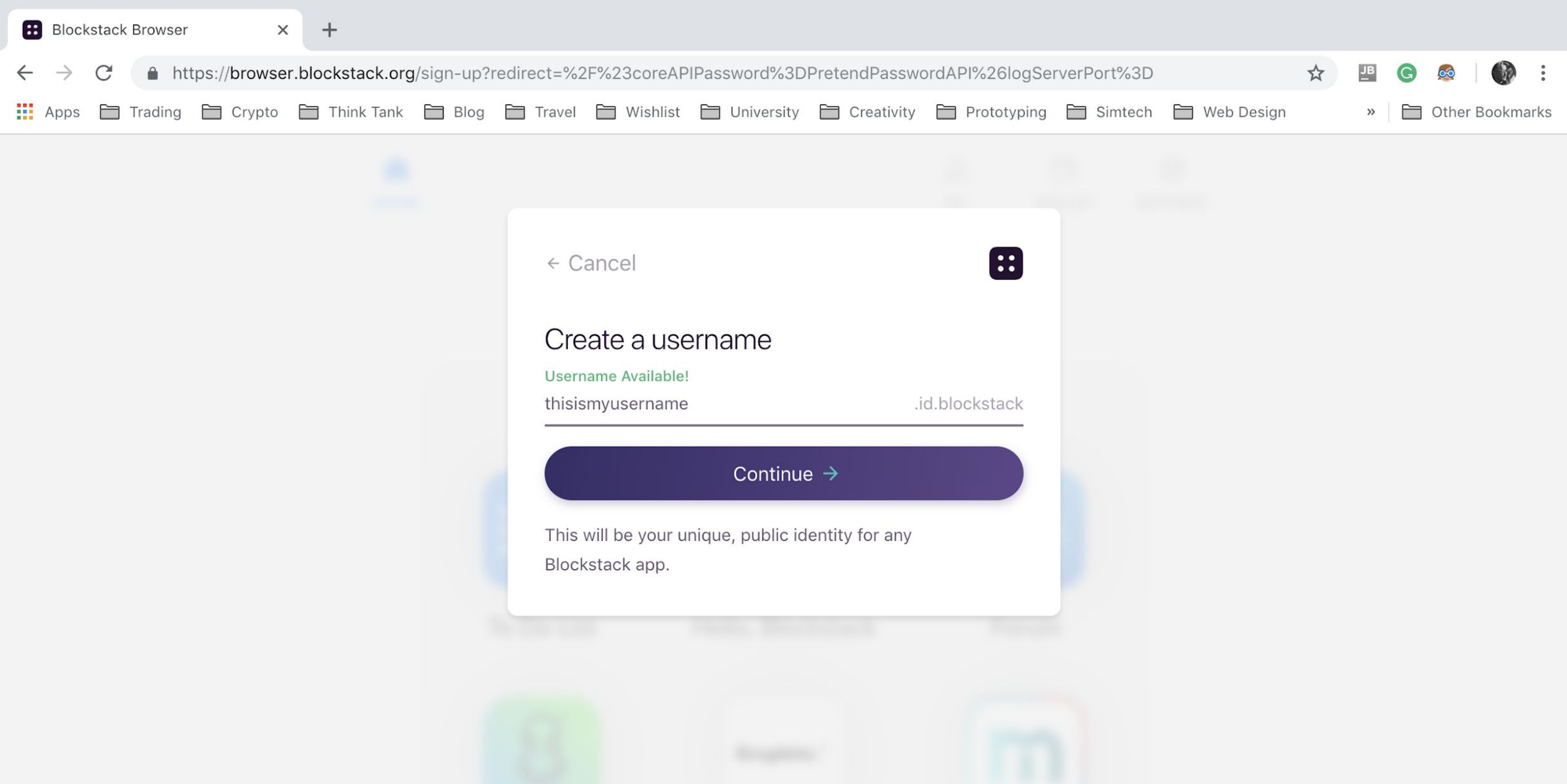
Create your username



Create your Blockstack ID

Completely censorship free, private, and secure. One login for 100s of apps. Powered by blockchain.

Check Availability



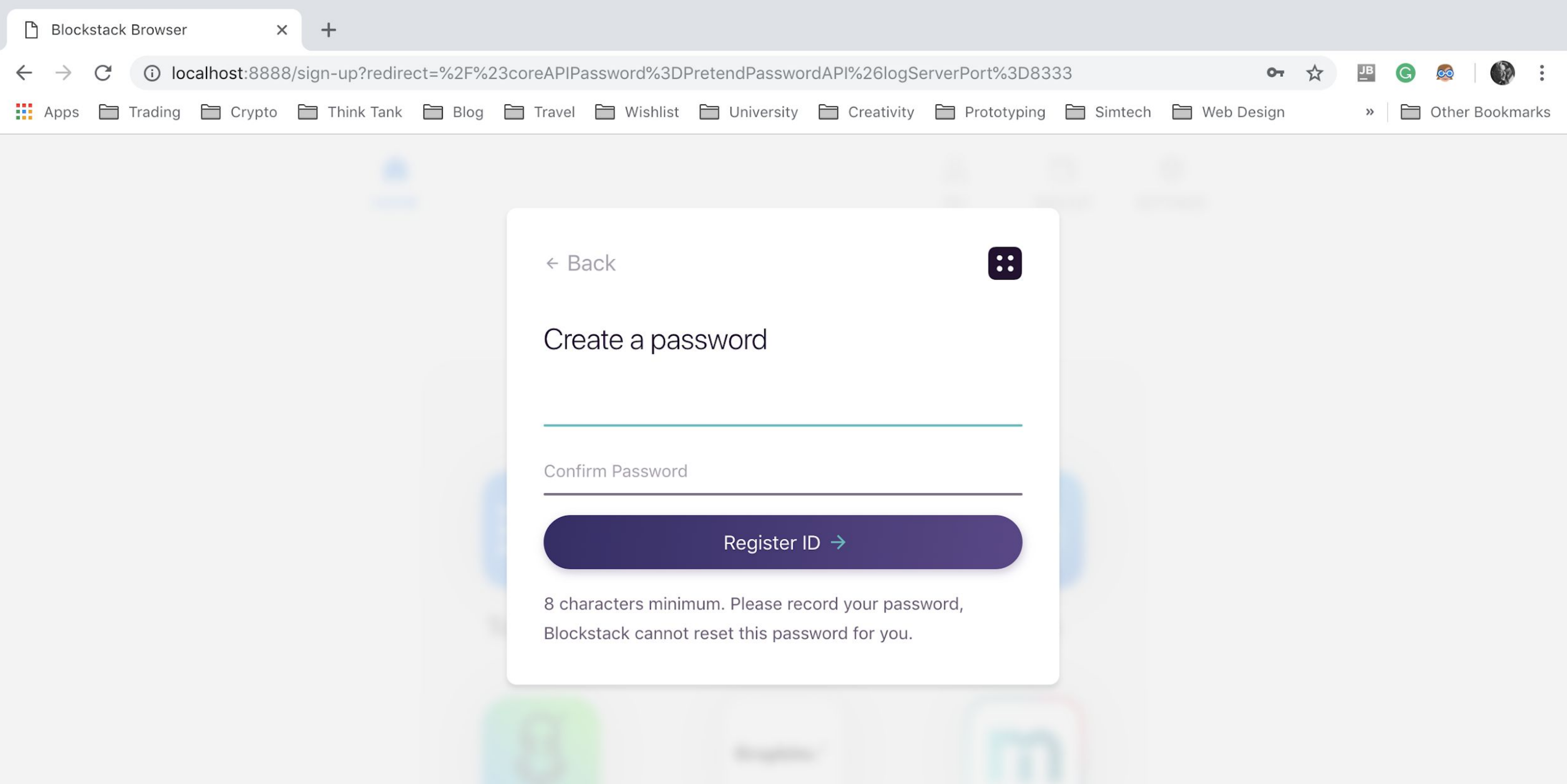
Create a username

Username Available!

thisismyusername .id.blockstack

This will be your unique, public identity for any Blockstack app.

Set Password (for on-device security)

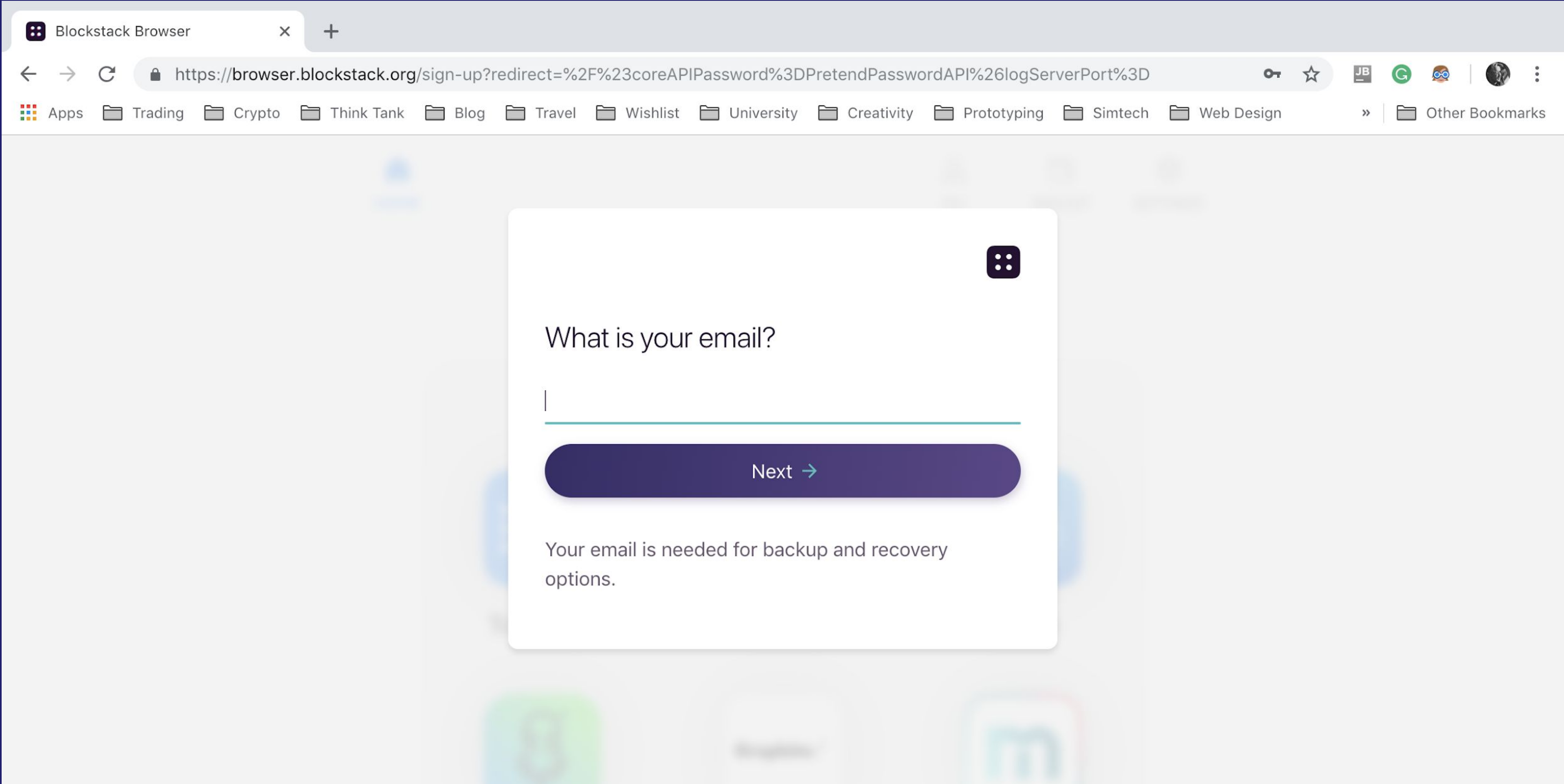


Create a password

Confirm Password

8 characters minimum. Please record your password, Blockstack cannot reset this password for you.

Enter email (for recovery)

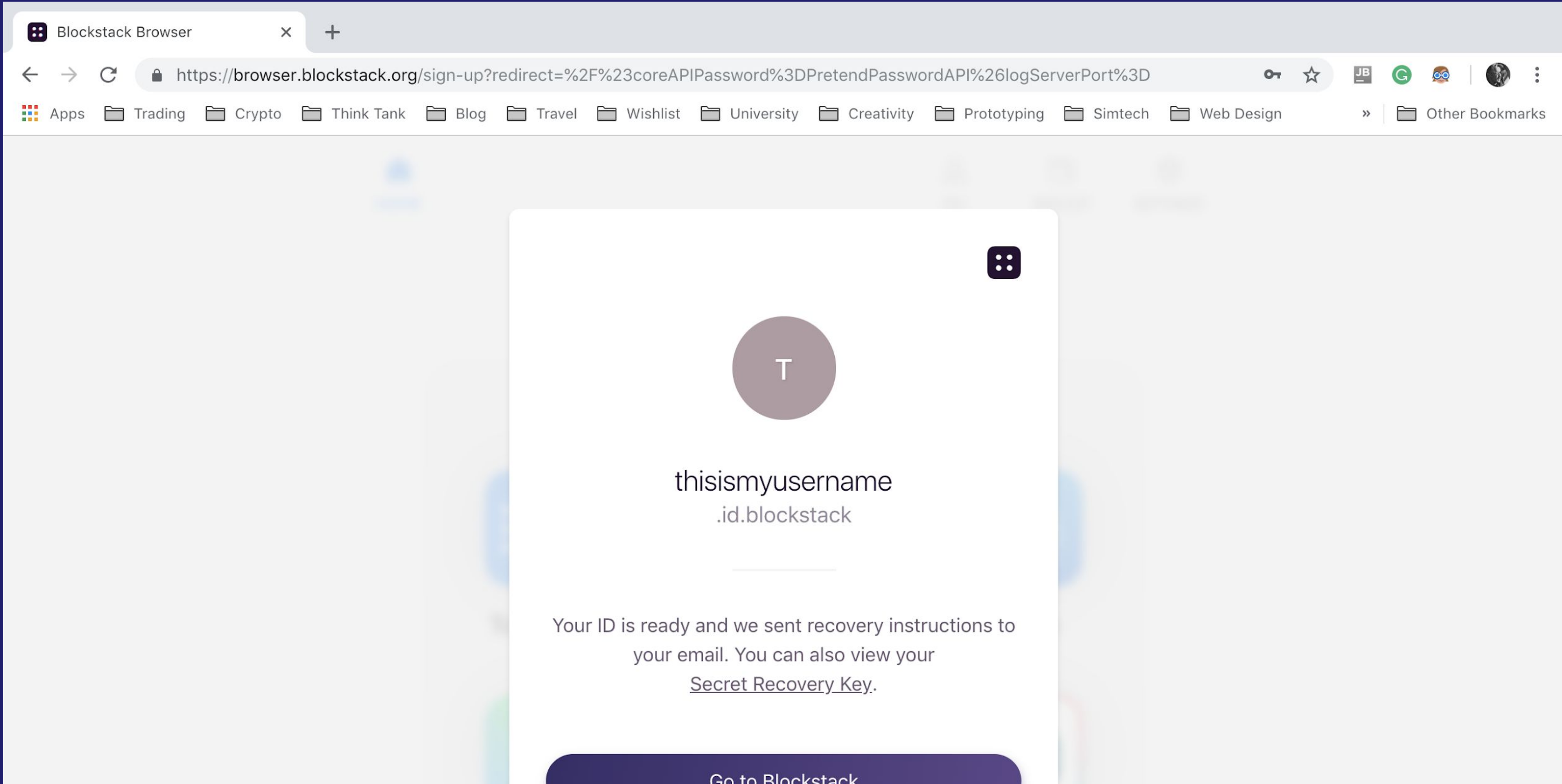


What is your email?

Next →

Your email is needed for backup and recovery options.

ID ready

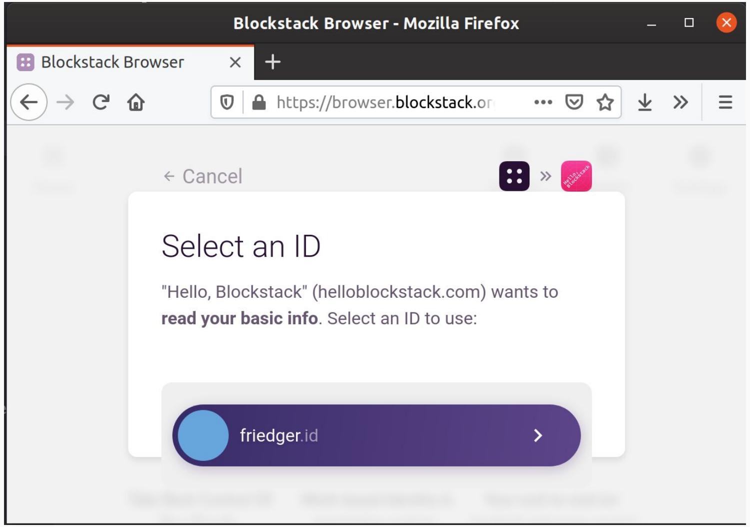


thisismyusername
.id.blockstack

Your ID is ready and we sent recovery instructions to your email. You can also view your Secret Recovery Key.

Blockstack

Verifiable Credentials (Claims) - Demo



Blockstack Browser - Mozilla Firefox

Blockstack Browser

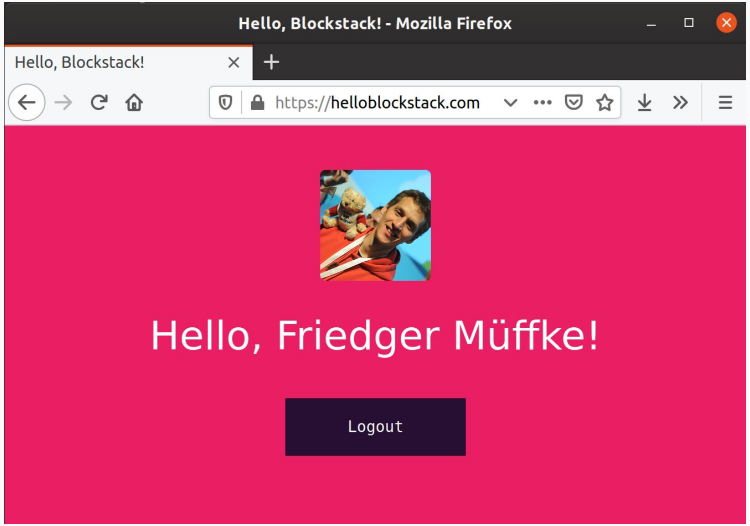
https://browser.blockstack.or

← Cancel

Select an ID

"Hello, Blockstack" (helloblockstack.com) wants to **read your basic info**. Select an ID to use:

friedger.id



Hello, Blockstack! - Mozilla Firefox

Hello, Blockstack!

https://helloblockstack.com

Hello, Friedger Müffke!

Verifiable Credentials

1. Authenticator creates authentication token
    - Token contains profile url
    - Signed by the user’s key
2. App receives token
3. App verifies token
    - Retrieves profile
    - Loads profile image

Verifiable Credentials

1. Authenticator creates authentication token

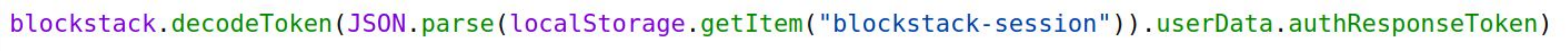
   Token contains profile url

   Signed by the user’s key

2. App receives token
3. App verifies token

   Retrieves profile

   Loads profile image



```
blockstack.decodeToken(JSON.parse(localStorage.getItem("blockstack-session")).userData.authResponseToken)
```

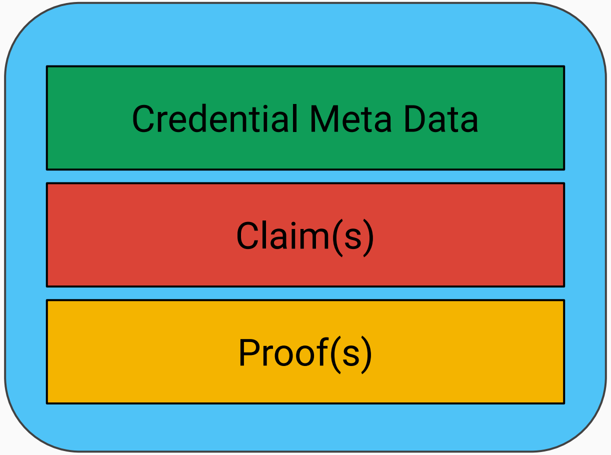
Blockstack Profile

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

Verifiable Credentials - Spec

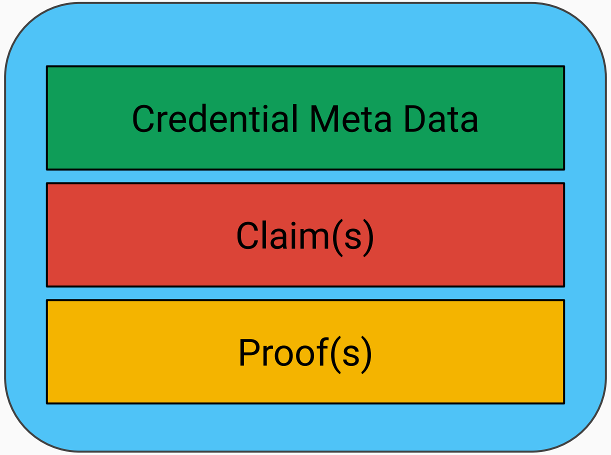


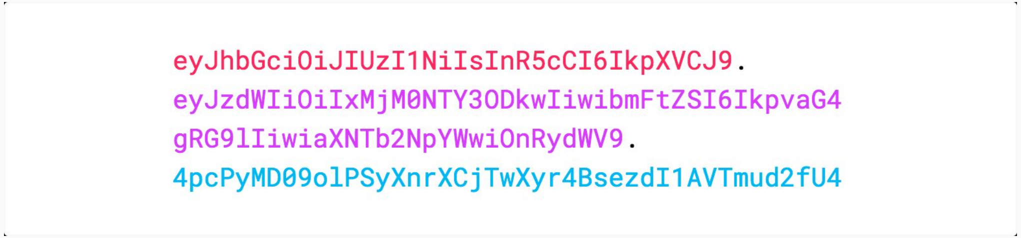
```
{
 "@context": [
   "https://www.w3.org/2018/credentials/v1",
   "https://www.w3.org/2018/credentials/examples/v1"
  ],
 "id": "http://example.edu/credentials/1872",
 "type": ["VerifiableCredential", "AlumniCredential"],
 "issuer": "https://example.edu/issuers/565049",
 "issuanceDate": "2010-01-01T19:73:24Z",
 "credentialSubject": {
   "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
   "alumniOf": {
     "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
     "name": [{
       "value": "Example University",
       "lang": "en"
     }, {
       "value": "Exemple d'Université",
       "lang": "fr"
     }]
   }
  },
  "proof": {
   "type": "RsaSignature2018",
   "created": "2017-06-18T21:19:10Z",
   "proofPurpose": "assertionMethod",
   "verificationMethod": "https://example.edu/issuers/keys/1",
   "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5X
     sITJX1CxPCT8yAV-TVkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-WUc
     X16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G_zS245-kronKb78cPN25DGlcTwLtj
     PAYuNzVBAh4vGHSrQyHUdBBPM"
  }
}
```

```
"type": [
   "VerifiableCredential",
   "AlumniCredential"
]
```

```
"type":
   "RsaSignature2018"
```

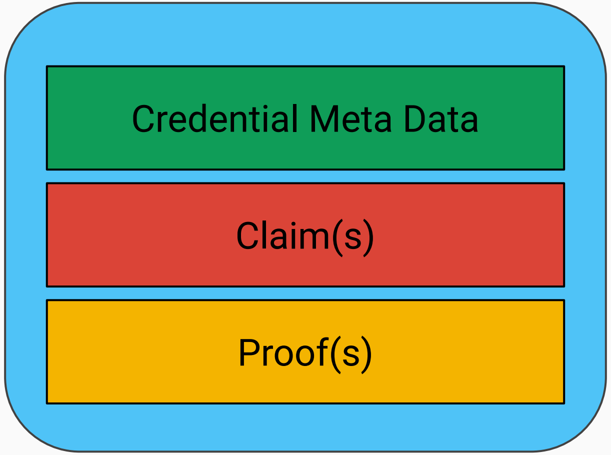
Verifiable Credentials - JWT





```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4
gRG9lIiwiaXNTb2NpYWwiOnRydWV9.
4pcPyMD09olPSyXnrXCjTwXyr4BsezdI1AVTmud2fU4
```

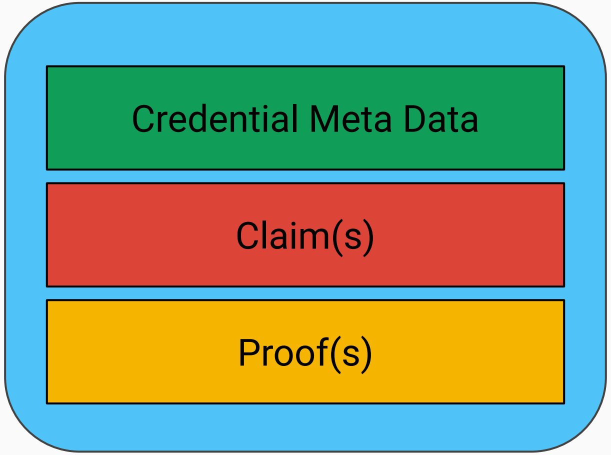
Verifiable Credentials - JWT



Requires additional knowledge/context

ES256K algorithm (bitcoin, ethereum, blockstack)
did-jwt (javascript library)

Verifiable Credentials - JWT



Requires additional knowledge/context

ES256K algorithm (bitcoin, ethereum, blockstack)
did-jwt (javascript library)

WORKSHOP
Saturday 17:30

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