

Blockstack

A New Internet for Decentralized Applications

Who is this guy?

- PhD candidate at Princeton University
- Worked for Blockstack since May 2015
- First engineering hire
- Background in P2P systems



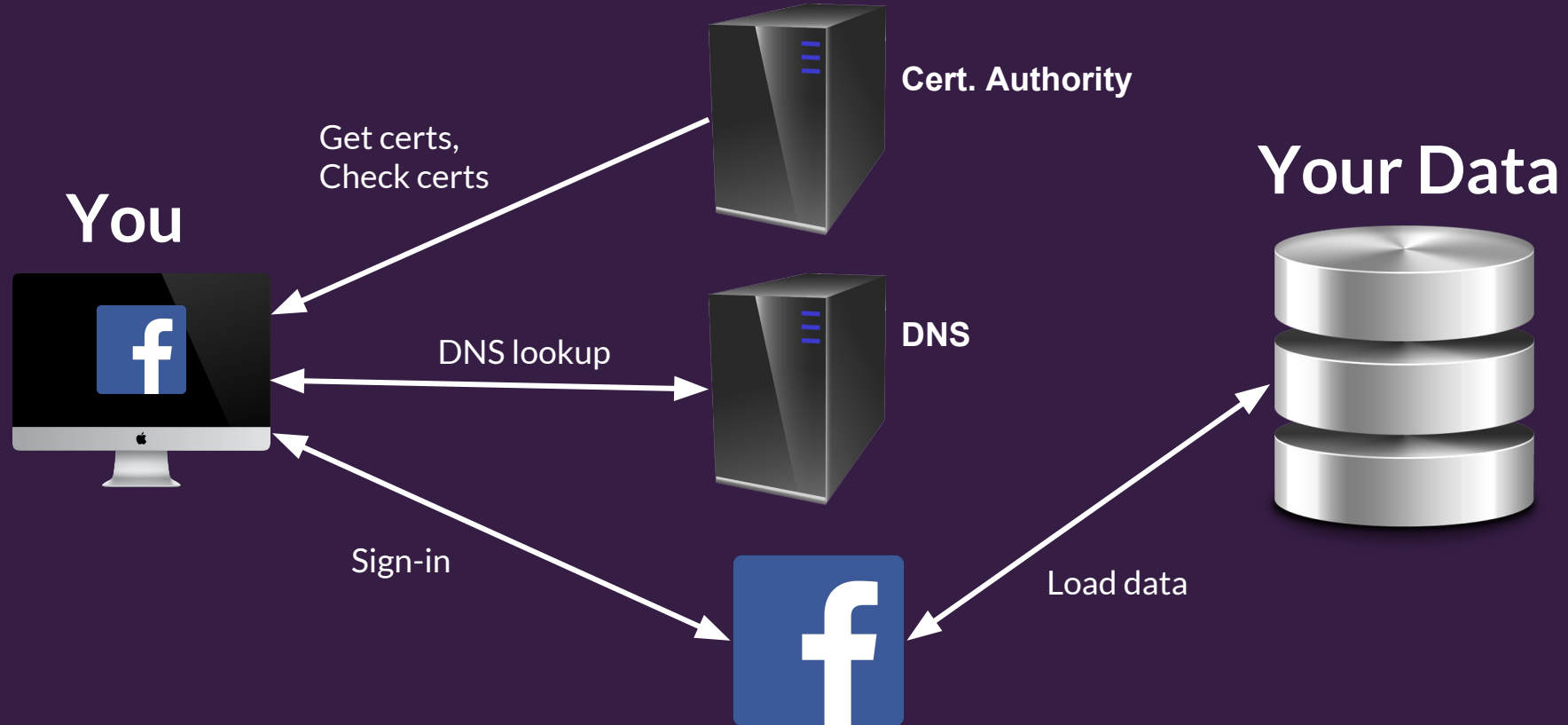
Jude Nelson ✎

jude.personal.id

ID-1Pwbo3enKDAqZq7T1SSY5T9JatuYbyonGo

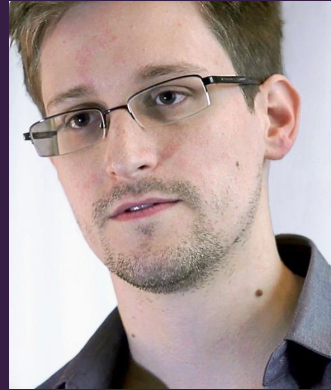
Blockstacker ✎

What Problems Are We Trying to Solve?



What Problems Are We Trying to Solve?

- Hidden trusted parties
- Single points of failure
- You are the product
- “Don’t be evil” is not good enough

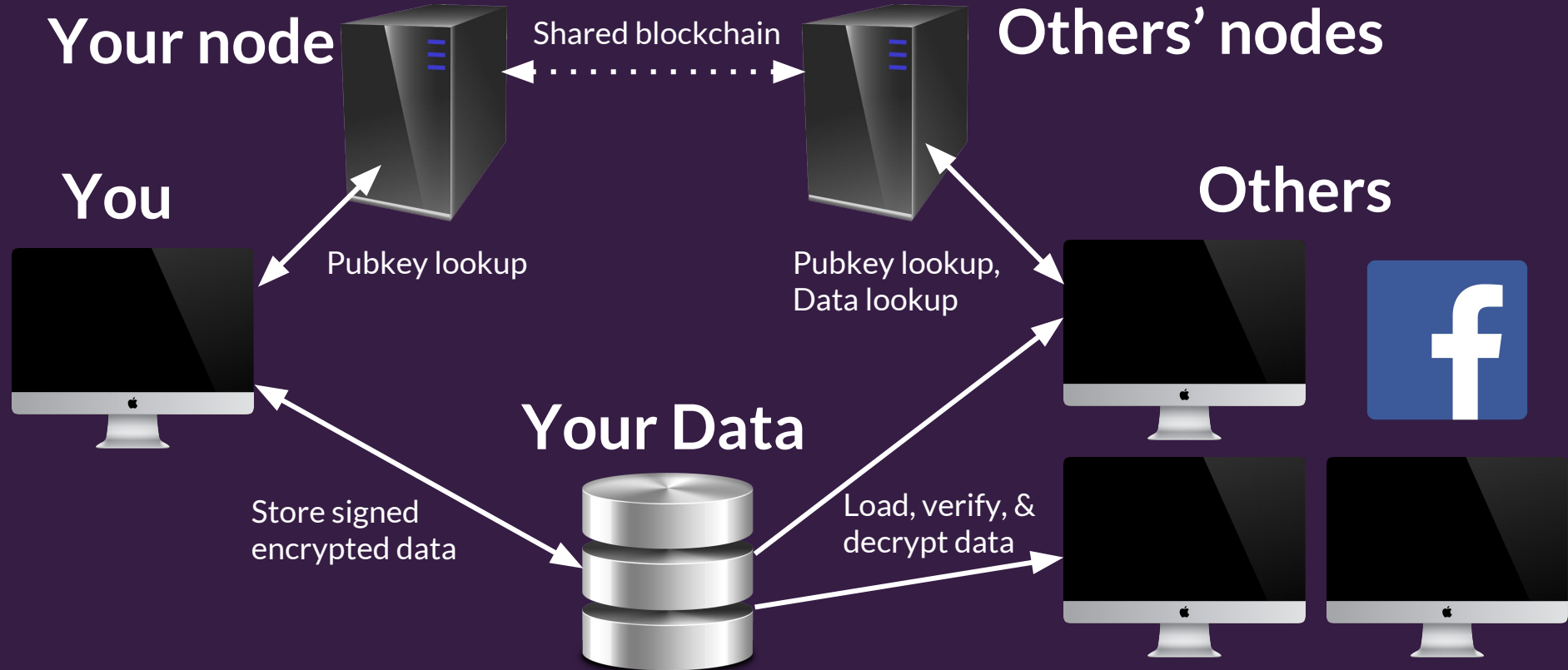


What Problems Are We Trying to Solve?

- Build “can’t be evil” applications
- Users own their identities
- Users own their data
- Apps host neither

Can we build Web apps this way? Use Blockstack!

What is Blockstack?



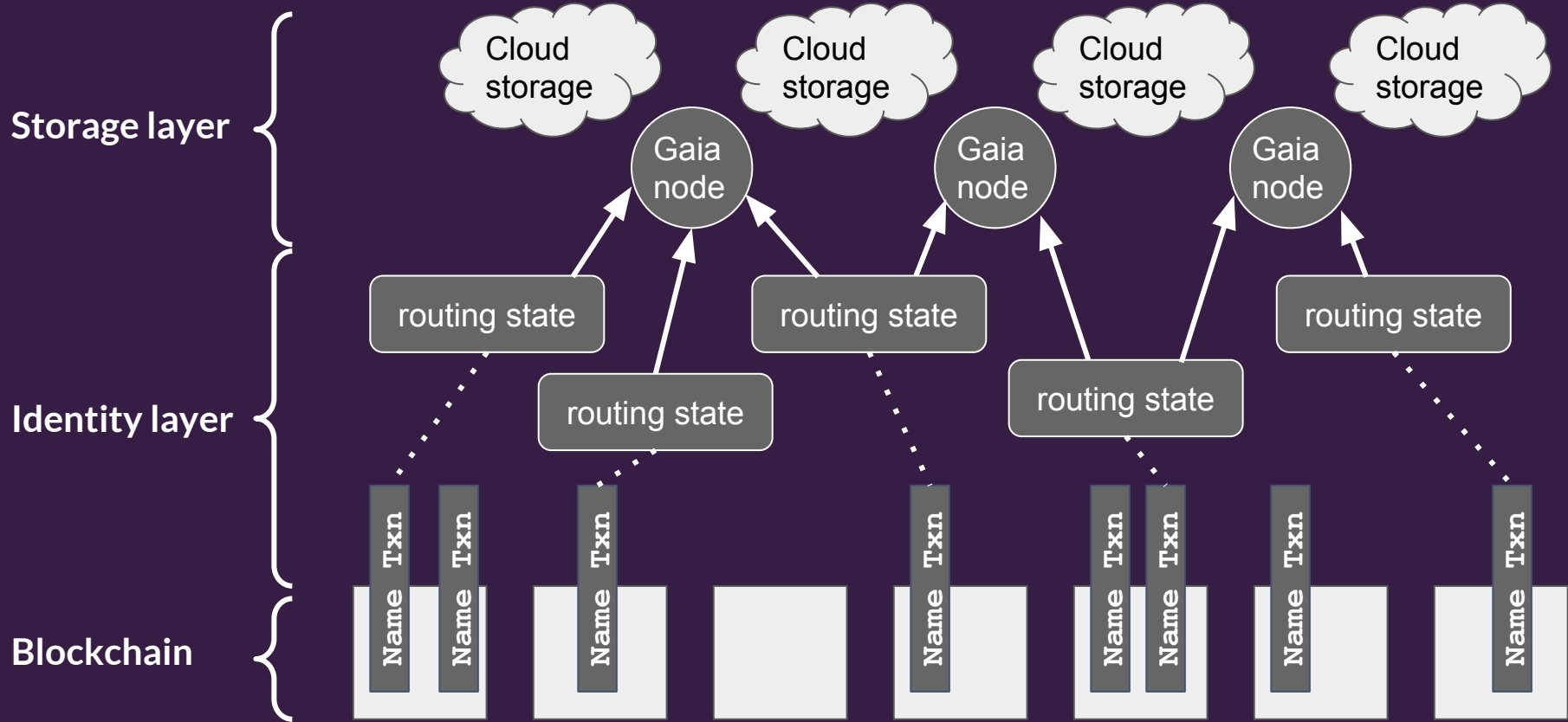
What is Blockstack?

- A new Internet for decentralized applications
- Provides core services
 - Identity
 - Storage
 - Payments
- Uses a blockchain to bootstrap

Blockstack Design Philosophy

- End-to-End Argument
 - Minimal use of a blockchain
 - Push complexity to the “edges”
- Trust-to-Trust Principle
 - Users, not servers, are the trusted endpoints

Blockstack Architecture



Blockstack Identity Layer

- Naming and PKI on a commodity blockchain
- “DNS for People”
 - Namespaces (TLDs)
 - Updates, Transfers, Renewals, Revocations
 - First-come first-serve
 - Anyone can register a name or namespace

Blockstack Identity Layer

- On-chain database log as specially-crafted TXNs

Name	Public Key Hash	Routing state hash
jude.id	16EMaNw3pkn...	b6e99200125e...
cicero.res_publica.id	1EtE77Aa5AA8et...	7e4ac75f9d79b...

- Nodes replay transactions to produce this DB
- Solves the key distribution and revocation problem

Blockstack Identity Layer

- Off-chain routing state (~40Kb/txn)
- Pointers to where your app data is hosted
- Fully replicated to all nodes via P2P network

```
$ORIGIN cicero
```

```
$TTL 3600
```

```
_file URI 10 1
```

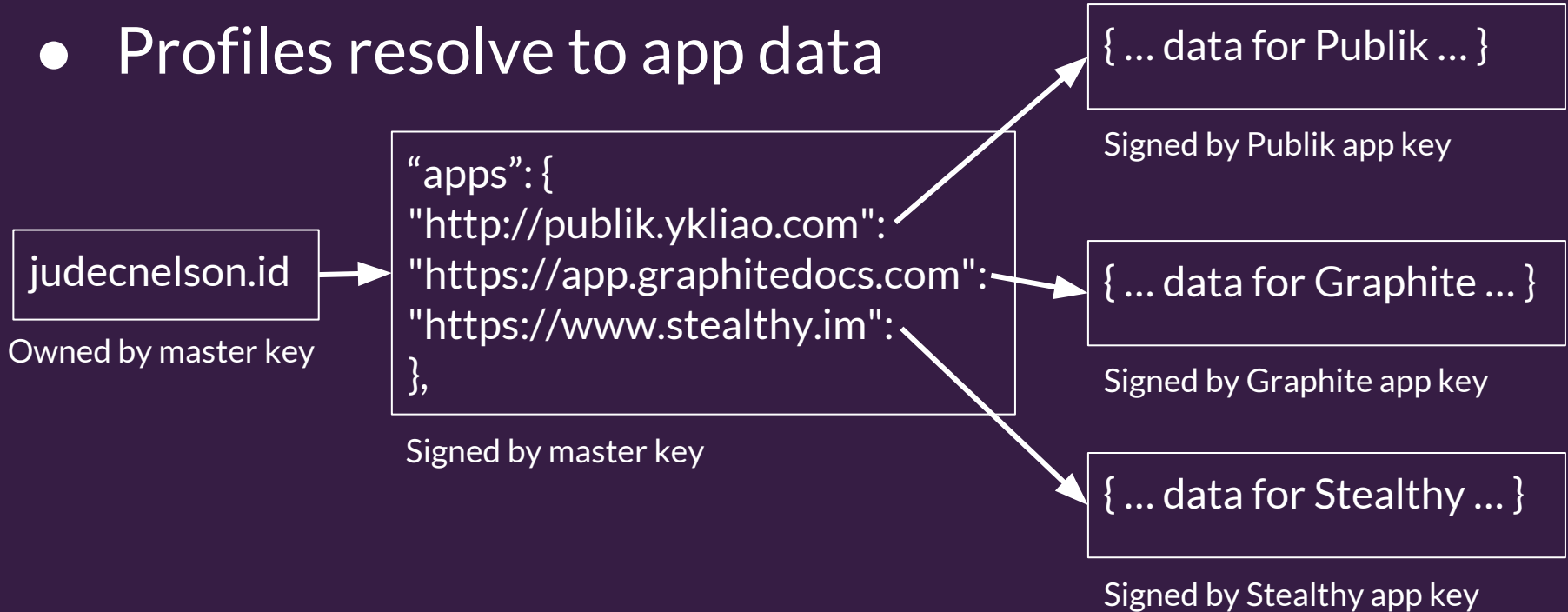
```
"https://gaia.blockstack.org/hub/1EtE77Aa5AA8etzF2irk56vvkS4v7rZ7PE"
```

Blockstack Storage Layer (Gaia)

- Reuses commodity storage systems
- Data is signed and encrypted
- User chooses which system(s) host their data
- Per-app buckets
- Per-app private keys

Blockstack Storage Layer (Gaia)

- Names resolve to profiles
- Profiles resolve to app data



Blockstack Infrastructure

- Anyone can run a Blockstack node
 - Takes ~10 GB disk, ~200MB RAM
 - Builds name DB
- <https://core.blockstack.org>
 - RESTful API endpoint
- <https://explorer.blockstack.org>
 - Profile explorer

Getting Started as a User

- Get the Blockstack Browser
 - Or go to <https://browser.blockstack.org>
- Go through on-boarding
- (Optional) buy a username with BTC
 - Required for “multiplayer” applications
 - Off-chain names are free


Building a Blockstack Dapp

- Runs in your Web browser
- Built like a normal Web app
- Uses blockstack.js to access Blockstack network
- User runs the Blockstack Browser
 - Identity wallet
 - SSO endpoint
 - URLs to trusted Blockstack node(s)

Building a Blockstack Dapp

Login with Blockstack

Sign In Request



The app "Graphite" located at <https://app.graphitedocs.com> wants to:

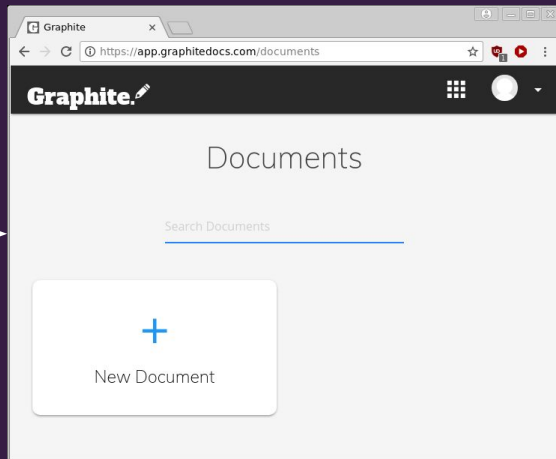
Read your basic info ⓘ
Publish data stored for this app ⓘ

Choose a Blockstack ID to sign in with.

jude.personal.id ▼

APPROVE

DENY



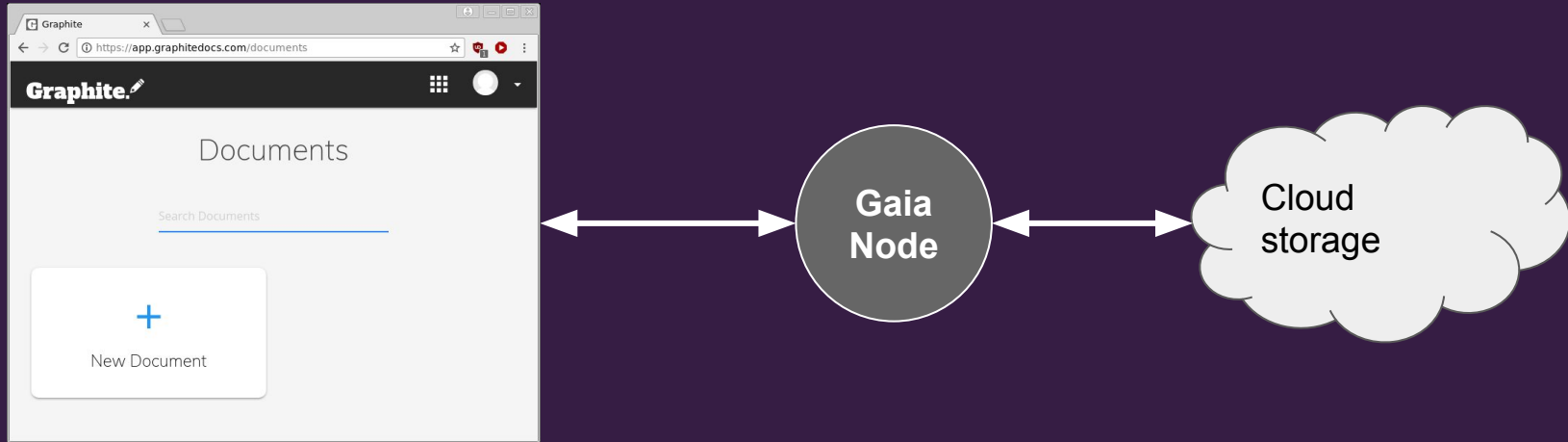
Building a Blockstack Dapp: Identity

- `redirectToSignIn(): void`
- `handlePendingSignIn(): Promise(profile)`
- `loadUserData(): profile`
- `lookupProfile(): Promise(profile)`

<https://blockstack.github.io/blockstack.js/>

Building a Blockstack Dapp: Storage

- `getFile(path, options): Promise(data)`
- `putFile(path, data, options): Promise(bool)`



Example Dapps Today

Name	Description
Graphite	Encrypted Google Suite
Dotpodcast	Podcast player and catalog without middlemen
Misthos	Github where developers share future project revenues
Bellweathr	Business analytics without 3rd parties (revenue positive!)
Coins	Encrypted cryptocurrency portfolio
Stealthy.im	Encrypted chat
Blockstagram	Encrypted Instagram

Project Technical Roadmap

- iOS/Android SDKs
- Off-chain names
- App-specific tokens
- STACKs blockchain

Core infrastructure is GPLv3; ancillary tools are MIT

Business Roadmap

- Blockstack Signature Fund
- App bounties
- Public app directories
- We're hiring!

Demo!

Thank You!

<https://blockstack.org>

<https://github.com/blockstack>

Blockstack vs Ethereum/EOS (with ENS, Swarm, IPFS)

- Names are enumerable
- Names are human-readable
- Names can live on- or off-chain
- Business logic runs off-chain
- Portable across blockchains
- User chooses where data is hosted
- Reads and writes are much more reliable

Off-chain Name Registration

- jude.personal.id, cicero.res_publica.id
- DB log is stored in an on-chain name's routing state
- Have same safety properties as on-chain names
 - Only the owner can update, transfer, revoke
- Require on-chain name to propagate signed ops
- Cheap---only \$0.005 when running at full capacity