

Building a New Internet with Blockstack

by Muneeb Ali

Twitter:

@muneeb

Blockchains 101

Blockchains 101

Let's design a new currency...



Blockchains 101

Let's design a new currency...



Muneeb Ali

10 coins

Brian Kernighan

10 coins



Blockchains 101

Let's design a new currency...



Muneeb Ali

10 coins

Brian Kernighan

10 coins

Paul Krugman

0 coins



Blockchains 101

Let's design a new currency...



Muneeb Ali

10 coins



Brian Kernighan

10 coins

Paul Krugman

0 coins

**Muneeb —> Krugman 2 coins
(unconfirmed)**



Blockchains 101

Let's design a new currency...



Muneeb Ali

8 coins



Brian Kernighan

10 coins

Paul Krugman

2 coins

**Muneeb —> Krugman 2 coins
(confirmed)**



Blockchains 101



Muneeb Ali

8 coins



Paul Krugman

2 coins

**Muneeb → Krugman 2 coins
(confirmed)**

Bill Gates

0 coins



Brian Kernighan

10 coins



Blockchains 101



Muneeb Ali

8 coins

Brian Kernighan

10 coins

Paul Krugman

2 coins



**Muneeb → Krugman 2 coins
(confirmed)**

Bill Gates

0 coins

**Muneeb → Bill 2 coins
(unconfirmed)**



Blockchains 101

Need a consensus algorithm ...

Consensus susceptible to Sybils

- All consensus protocols based on membership...
 - ... assume independent failures ...
 - ... which implies strong notion of identity
- “Sybil attack” (p2p literature ~2002)
 - Idea: one entity can create many “identities” in system
 - Typical defense: 1 IP address = 1 identity
 - Problem: IP addresses aren’t difficult / expensive to get,
esp. in world of botnets & cloud services

Consensus based on “Work”

- Rather than “count” IP addresses, bitcoin “counts” the amount of CPU time / electricity that is expended

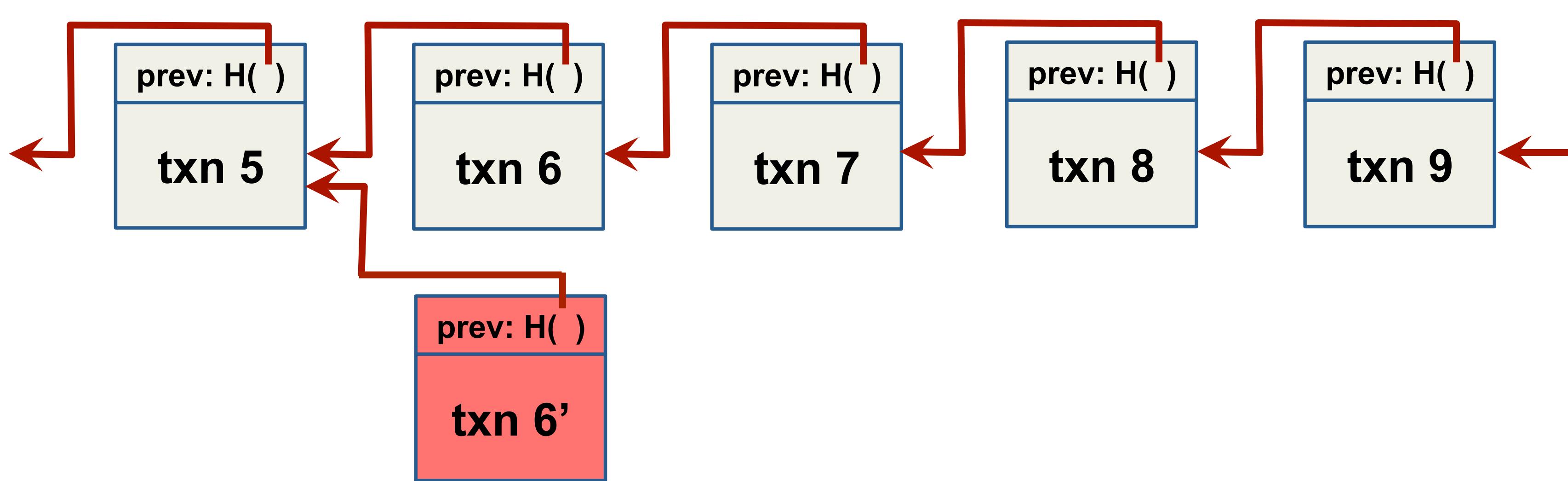
“The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.”

- Satoshi Nakamoto

- Proof-of-work: Cryptographic “proof” that certain amount of CPU work was performed

Key idea: Chain length requires work

- Generating a new block requires “proof of work”



- “Correct” nodes accept longest chain
- Creating fork requires rate of malicious work $>>$ rate of correct
- So, the older the block, the “safer” it is from being deleted

How Blockchains Work

How Blockchains Work



Blockchain

- It's a file!
- Append-only global log
- Every node on the network has a consistent copy

How Blockchains Work

- Private-public key pairs

```
>>> from pybitcoin import BitcoinPrivateKey  
>>> priv = BitcoinPrivateKey()  
>>> priv.to_hex()  
'91149ee24f1ee9a6f42c3dd64c2287781c8c57a6e8e929c80976e586d5322a3d'
```

How Blockchains Work

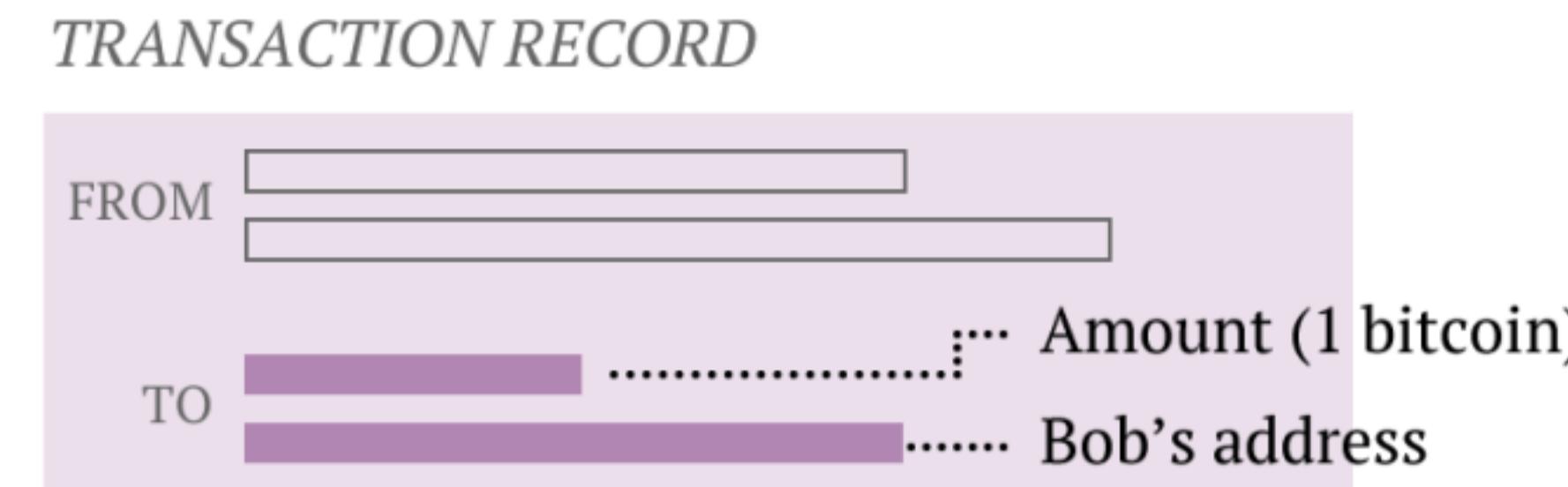
- Private-public key pairs
- Bitcoin address = deterministic from pubkey

```
>>> pub = priv.public_key()  
>>> pub.to_hex()  
'042c6b7e6da7633c8f226891cc7fa8e5ec84f8eacc792a46786efc869a408d29539a5e6f8de3f71c0014e8ea71691c
```

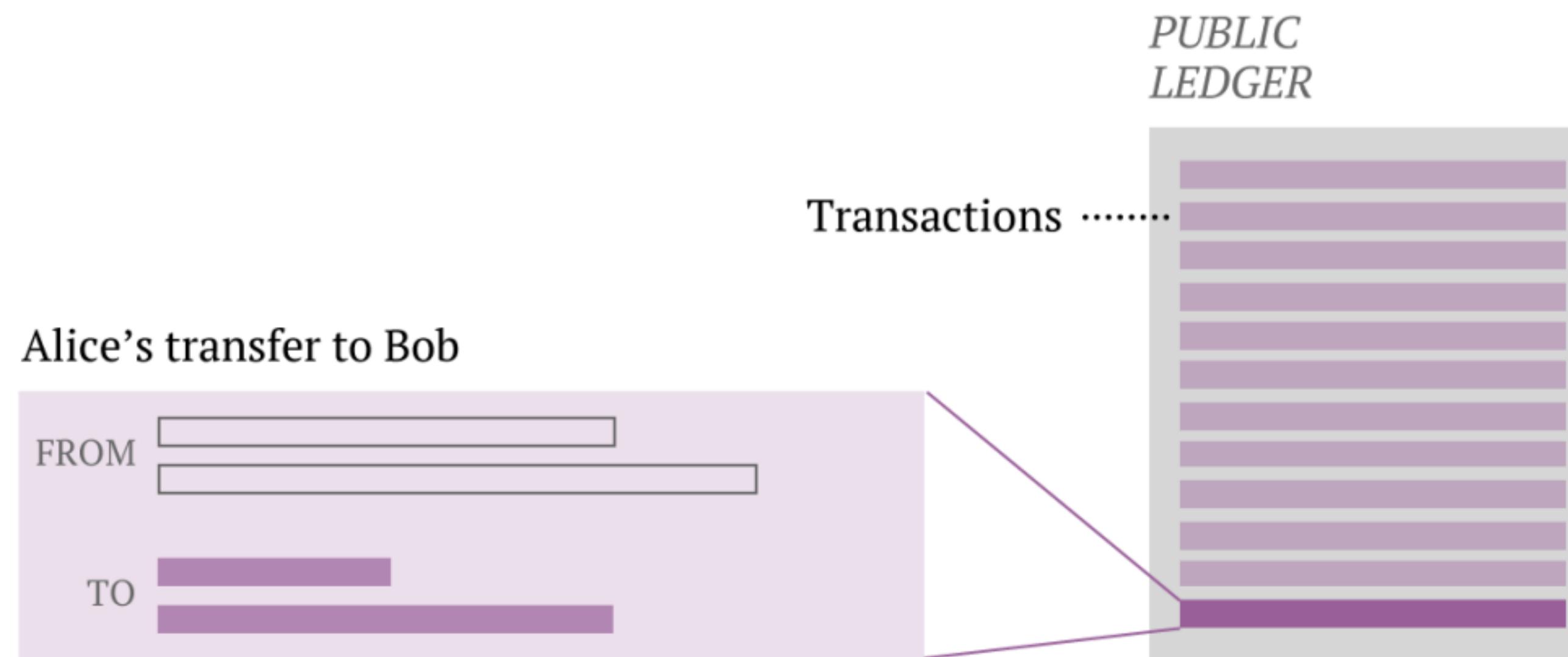
```
>>> pub.address()  
'13mtgVARiB1HiRyCHnKTi6rEwyje5TYKBW'
```

How Blockchains Work

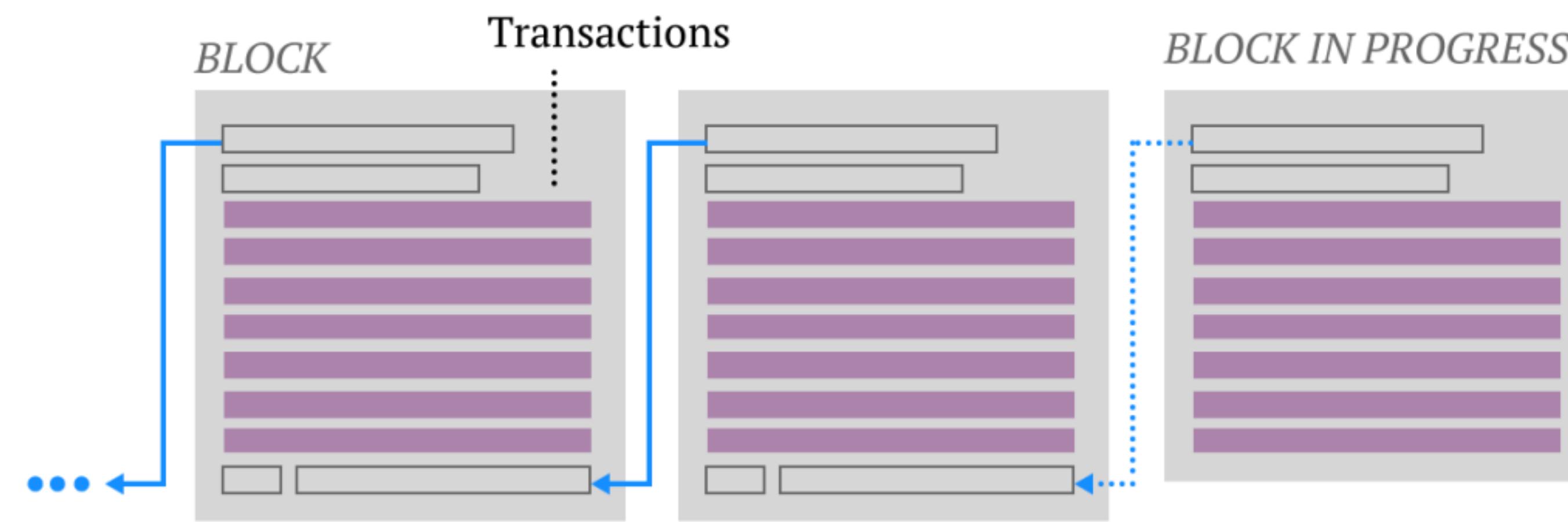
- No such thing as a “bitcoin”. Only inputs and outputs
- 21 million total bitcoins (fixed)
- 50 BTC minted each block, halved to 25 BTC



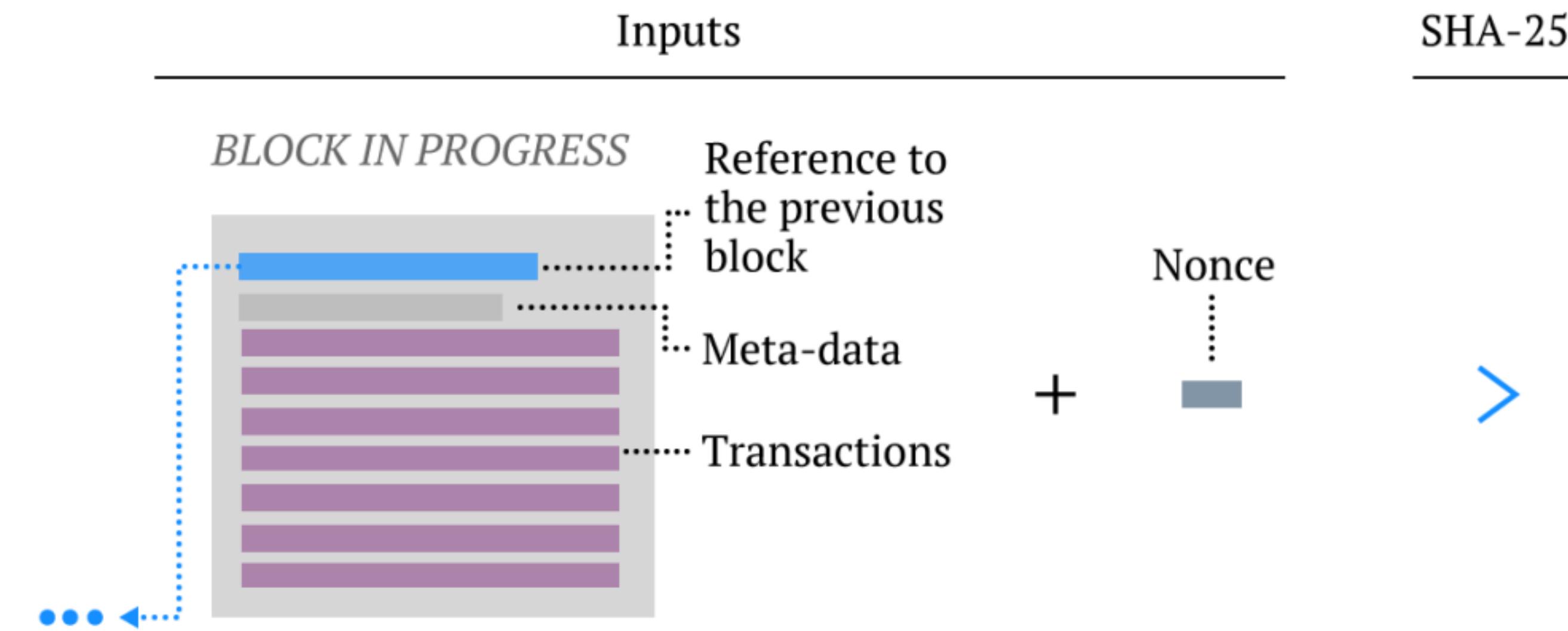
How Blockchains Work



How Blockchains Work

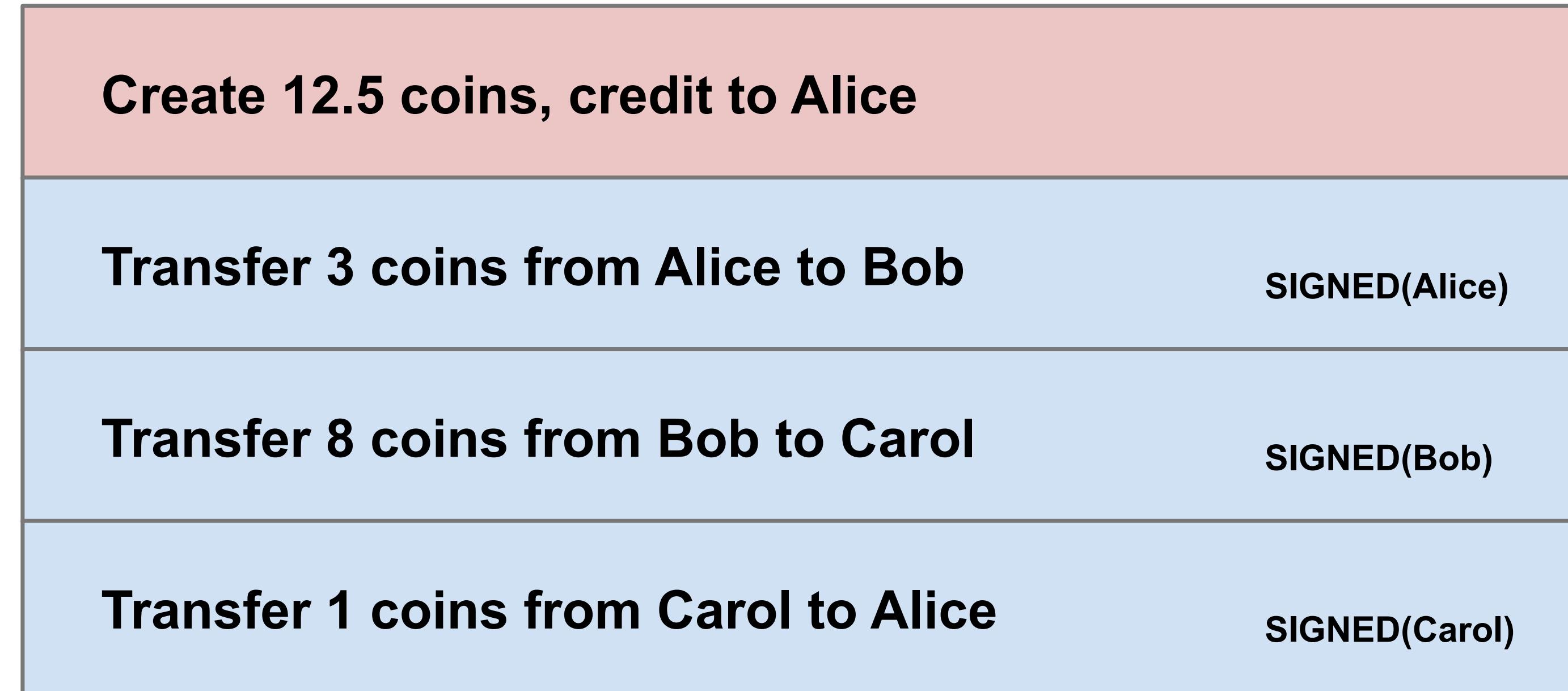


Bitcoin's Proof-of-work



000009ff7ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284add200126d9069

Bitcoin's Transaction Format



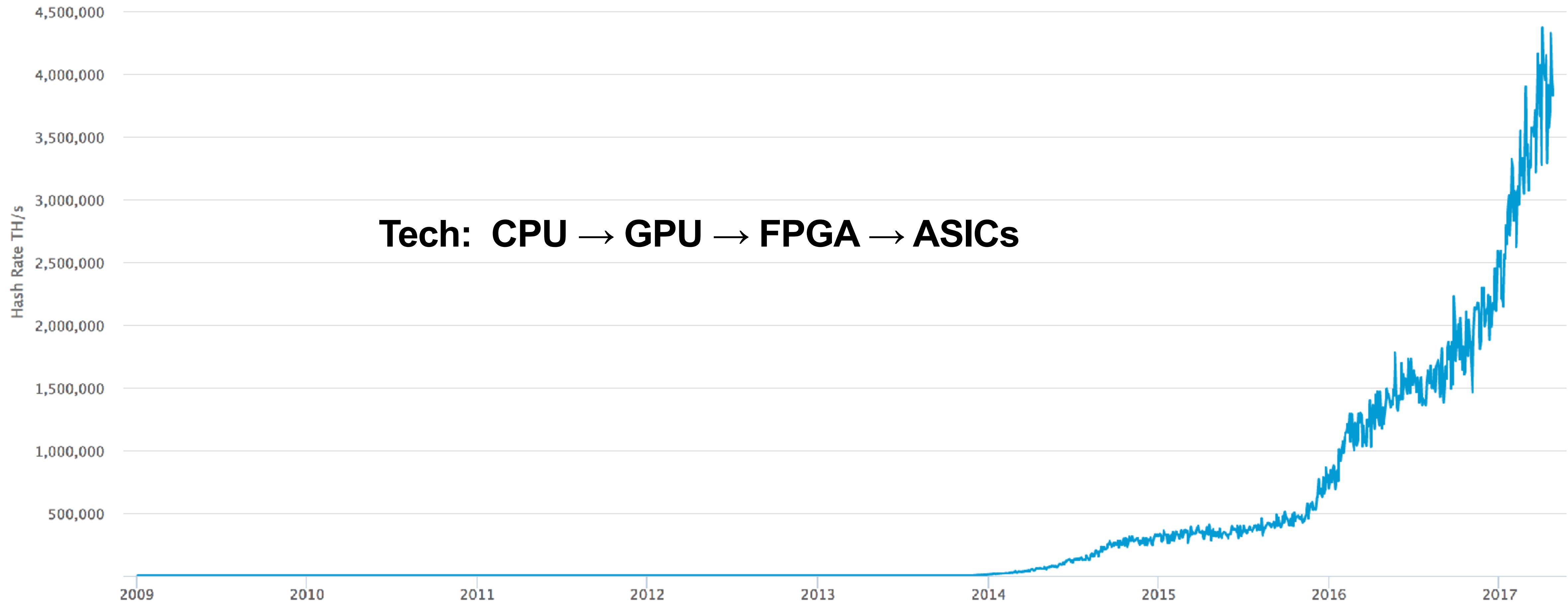
How do you determine if Alice has balance?
Scan backwards to time 0 !

Bitcoin's Transaction Format

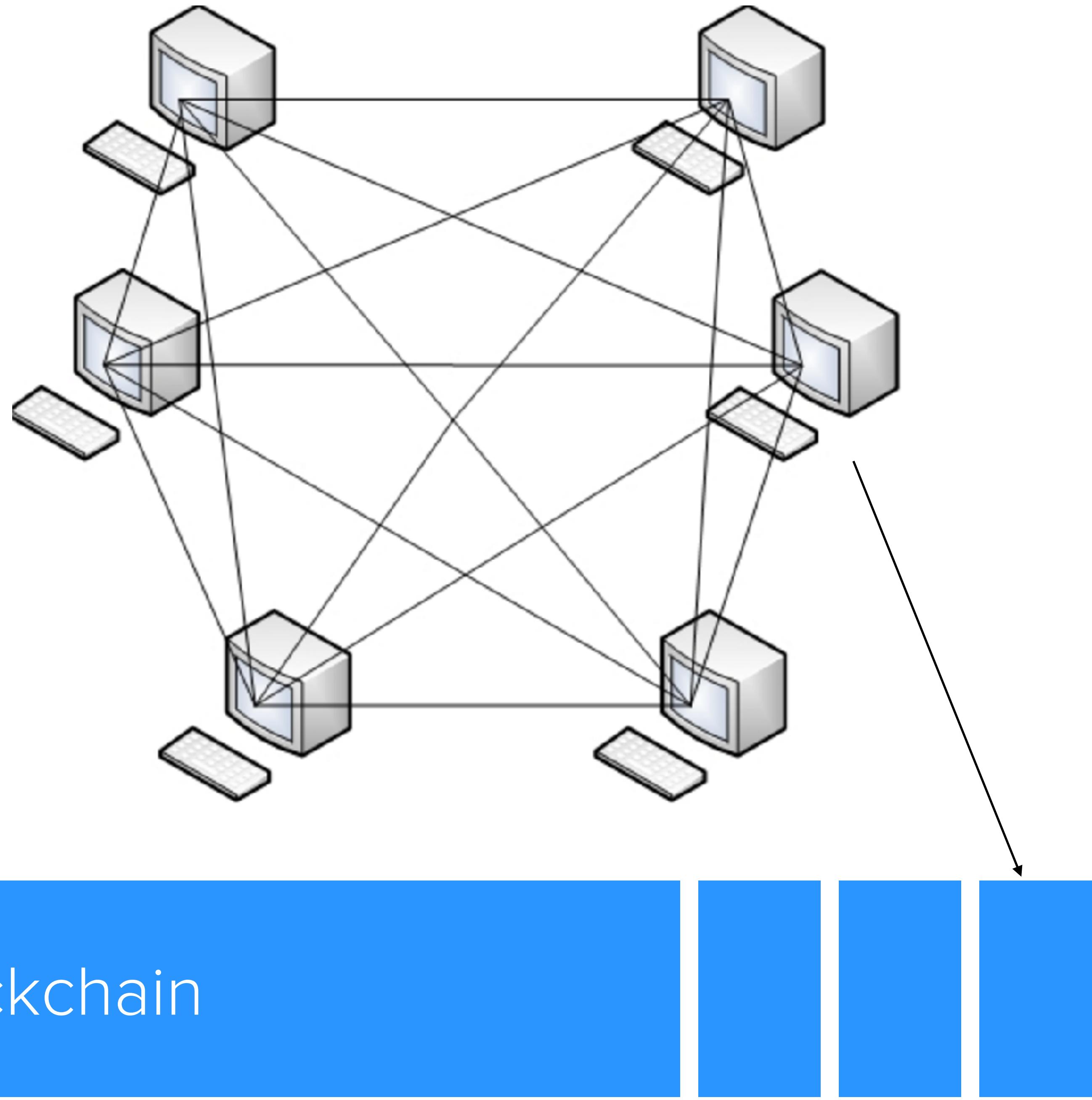
Inputs:	\emptyset	<i>// Coinbase reward</i>
Outputs:	$25.0 \rightarrow PK_{Alice}$	
Inputs:	$H(\text{prevtxn}, 0)$	<i>// 25 BTC from Alice</i>
Outputs:	$25.0 \rightarrow PK_{Bob}$	SIGNED(Alice)
Inputs:	$H(\text{prevtxn}, 0)$	<i>// 25 BTC From Alice</i>
Outputs:	$5.0 \rightarrow PK_{Bob}, 20.0 \rightarrow PK_{Alice}$	SIGNED(Alice)
Inputs:	$H(\text{prevtxn1}, 1), H(\text{prevtxn2}, 0)$	<i>// 10+5 BTC</i>
Outputs:	$14.9 \rightarrow PK_{Bob}$	SIGNED(Alice)

- Unspent portion of inputs is “transaction fee” to miner
- In fact, “outputs” are stack-based scripts
- 1 Block = 1MB max

Bitcoin's Hash Rate



Bitcoin's P2P Network





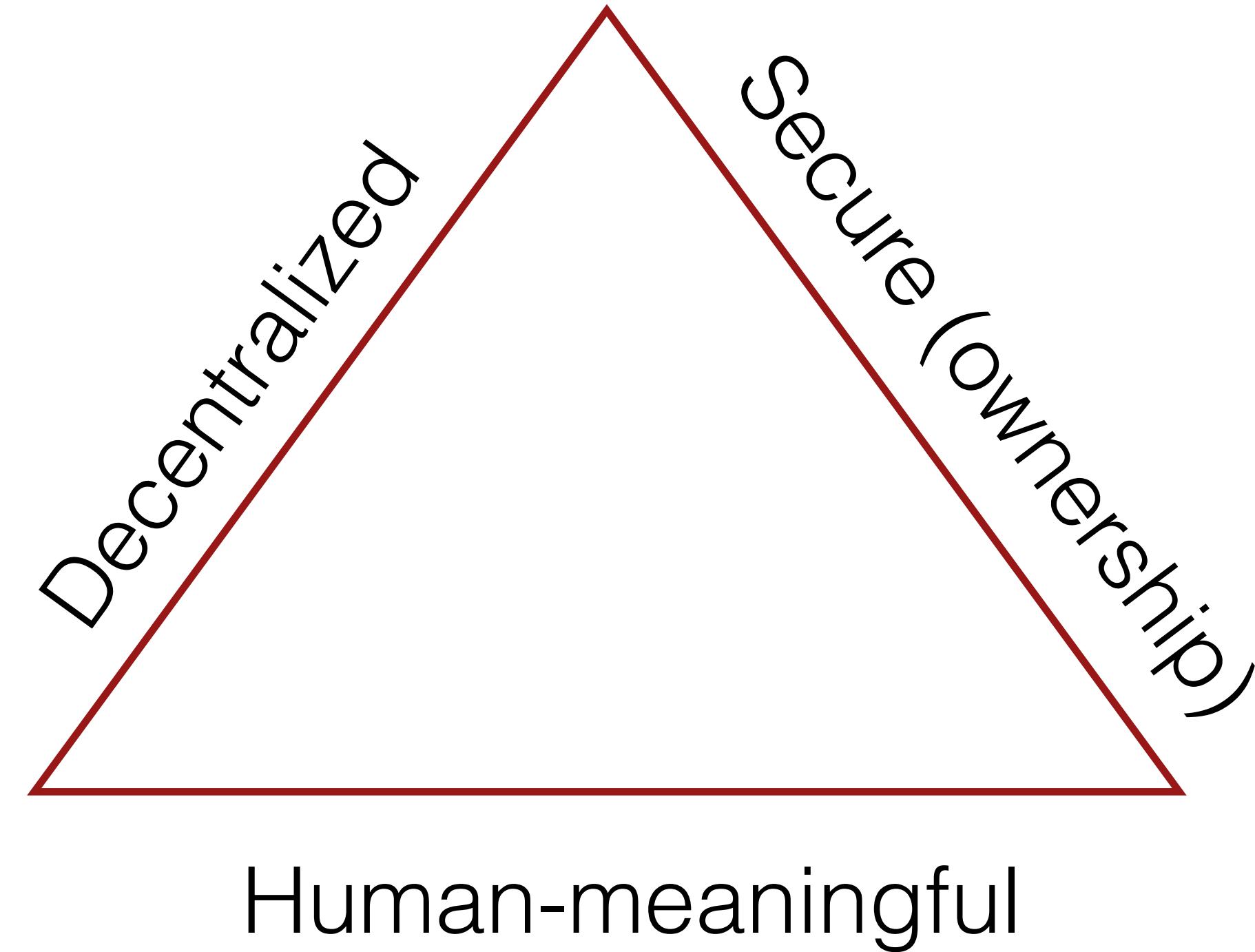
Building Systems using Blockchains

Bootstrapping Trust using Blockchains

- Blockchains can serve as decentralized PKI.
- All “accounts” already have private/public keypairs.
- Deployed nodes serve as lookup servers.
- Strong financial incentive for keeping the network secure

But can we build DNS?

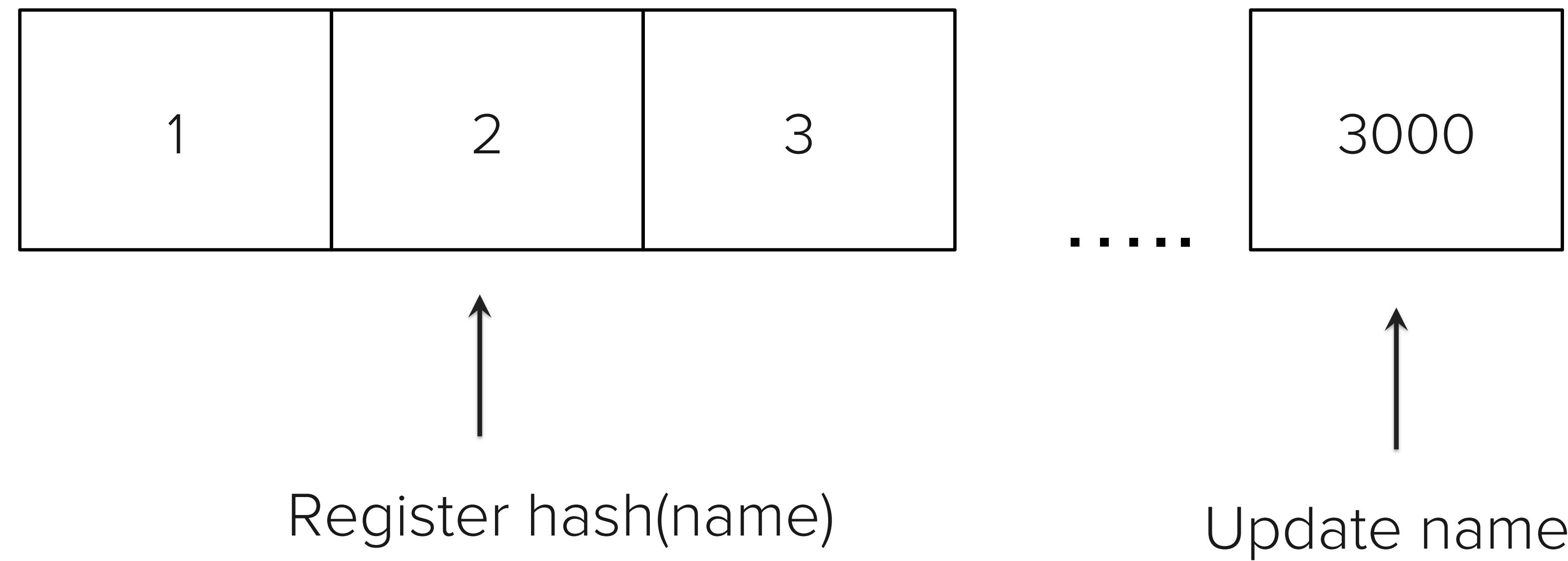
Zooko's Triangle



- Long hash is secure & decentralized e.g., 1Hdsfd34fDdgeTe...
- Twitter handle is human-meaningful & secure e.g., @muneeb

Blockchains can give all three! (e.g., Namecoin)

Naming System on a Blockchain:



Design Limitations

- Blockchains are horrible for data & compute
- P2P networks are horrible for performance

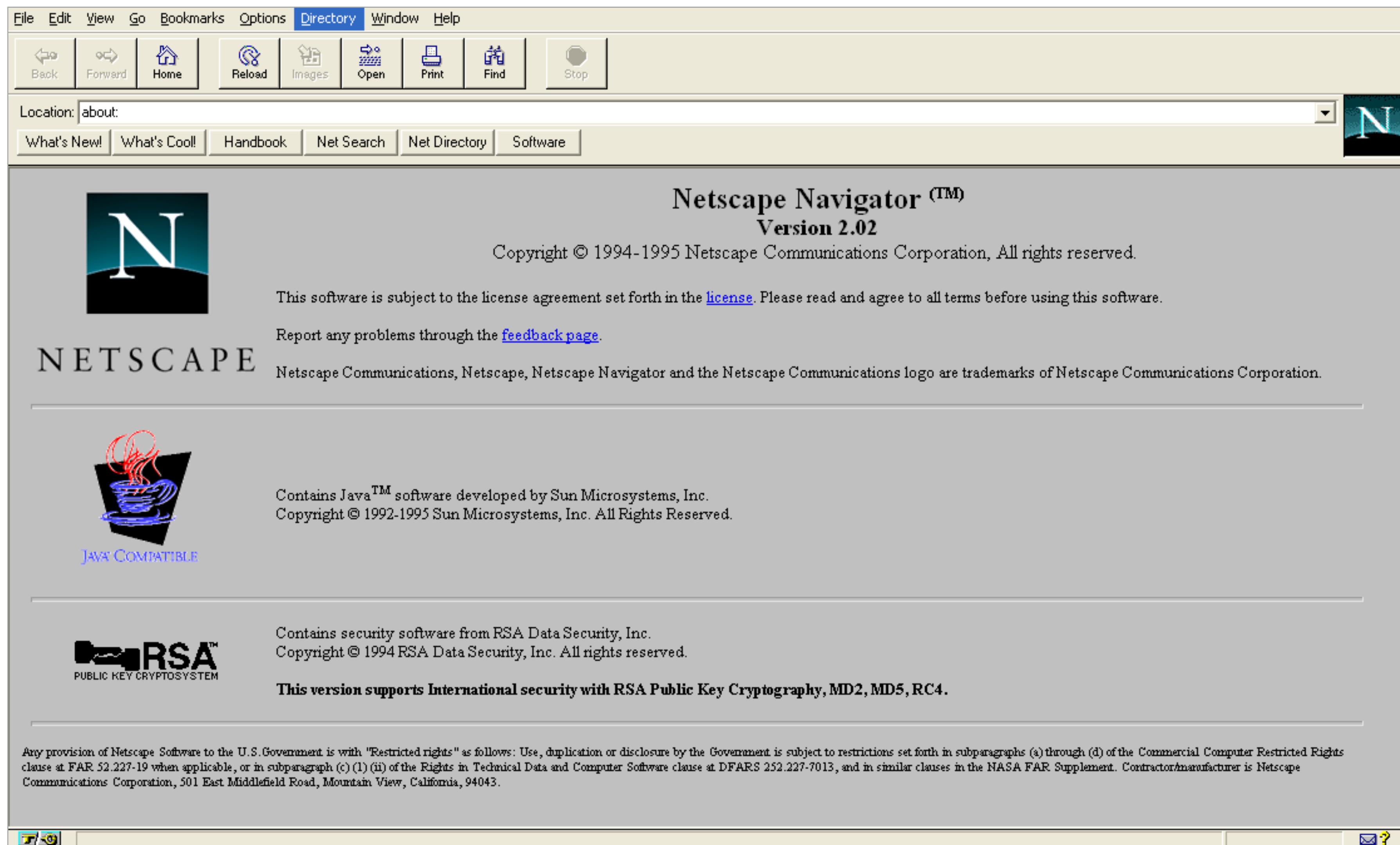
Communication Channels



Bootstrapping trust in distributed systems ...



Building a New Internet



The Internet



chrome

facebook

VeriSign®

Time
Warner
Cable®

Akamai

ICANN

The Internet



chrome

TURKTRUST

Google

#1 **Blind Trust**

We trust parties we don't even know exist.

The Internet



chrome



chrome

#2 No Ownership

Big companies, not users, own the data.

Traditional internet: end-to-end design

New internet: trust-to-trust design

Payments

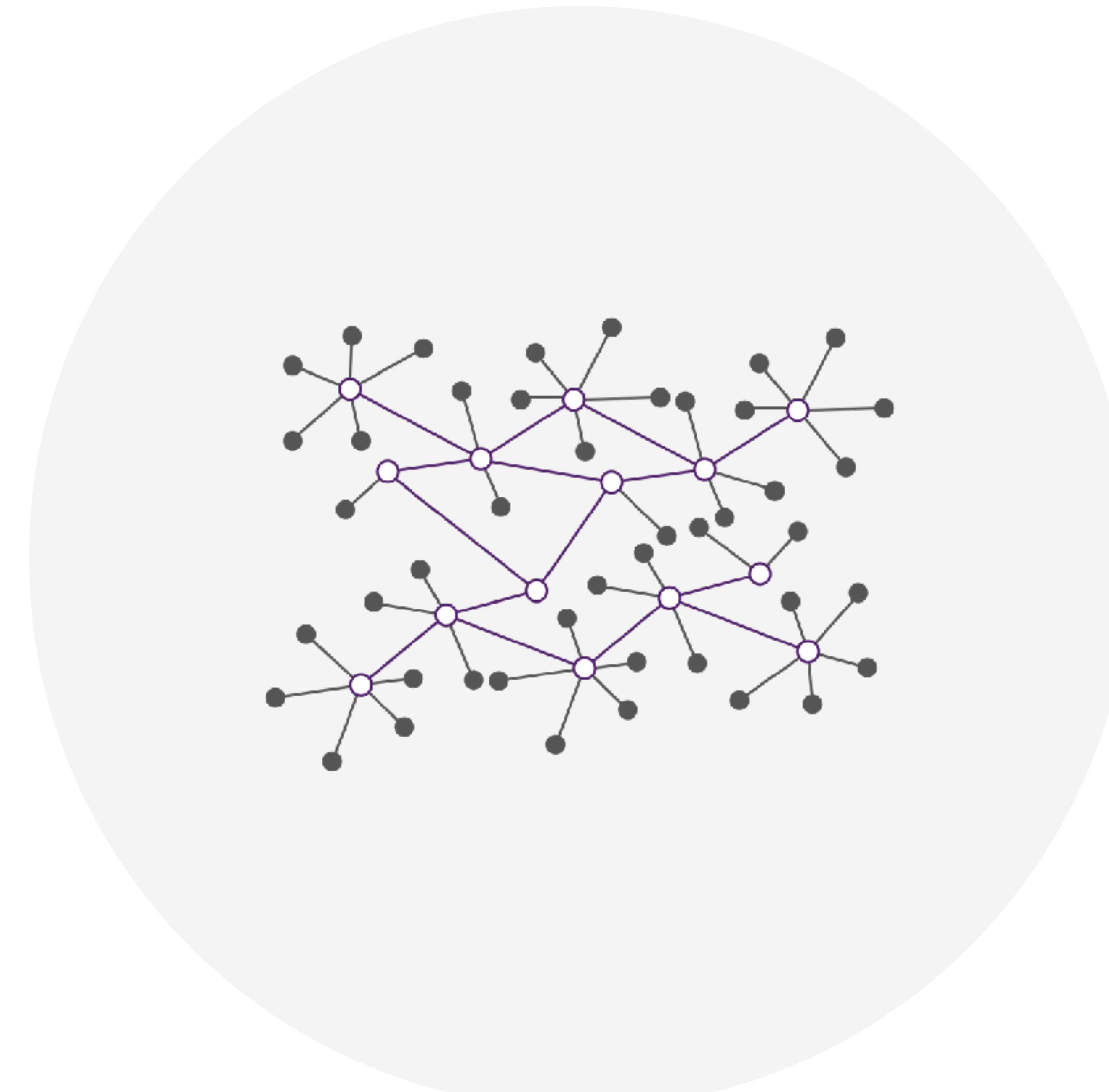


chrome



chrome

Payments



How to use this new network?

91148ee24f1ee9a6f42c3dd64c2287781c8c57a6e8e929c8097e586d5322a3d

Payments → Banks (Citibank)

Internet → Data Banks (Facebook)



Personas

REGISTER IMPORT

Thomas Middleditch
thomasthemd.id

Tom Middleditch
tommyinthemiddle.id

Tom Middleditch
tmiddleditchvalley.id

Search for people, apps and more...

Home Account

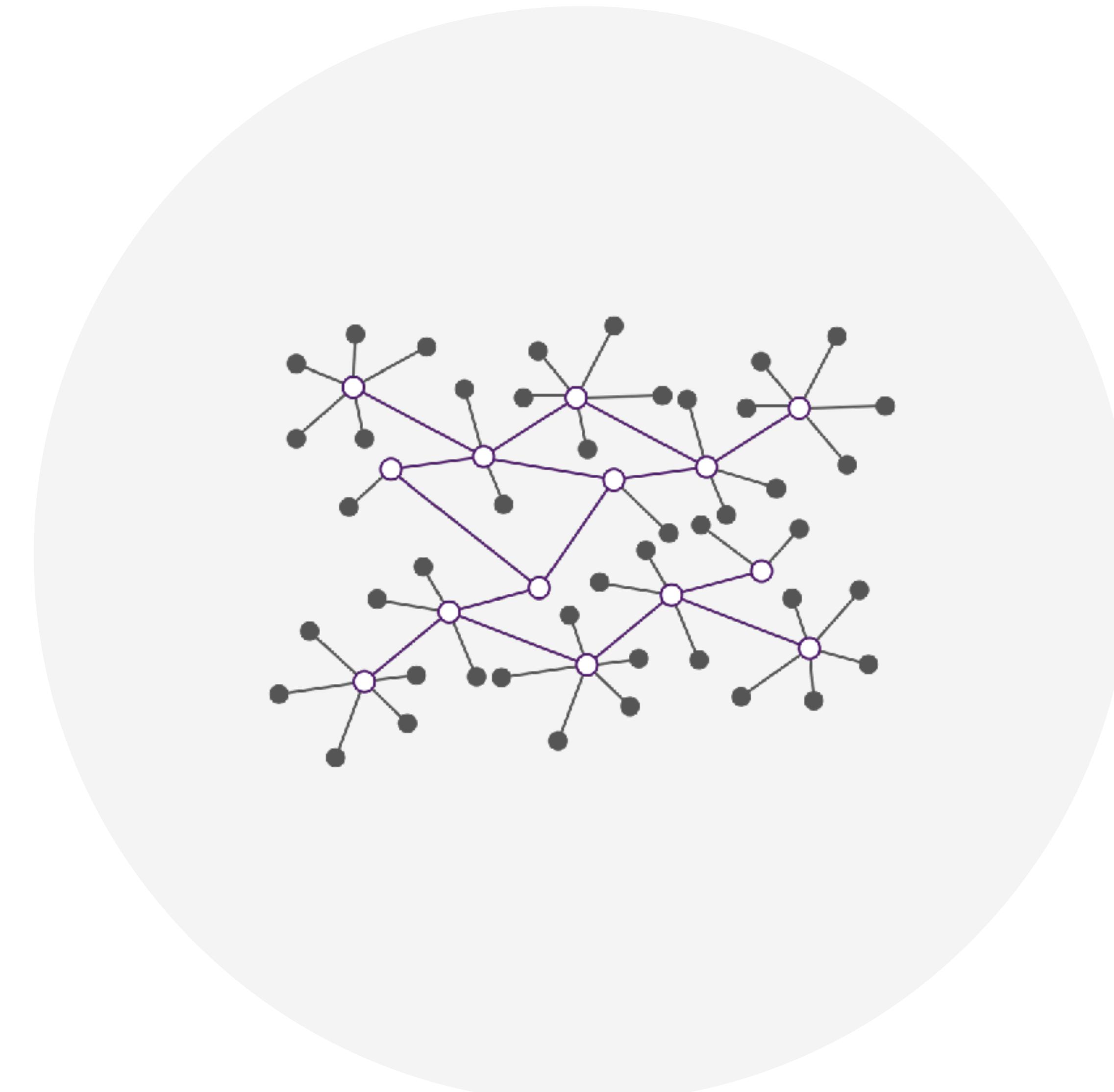
blockstack

Browse the decentralized internet

The Blockstack browser is the world's first browser that enables you to browse the decentralized internet

Login with Blockstack

The New Internet



Q werner.id

Home Account

Personas

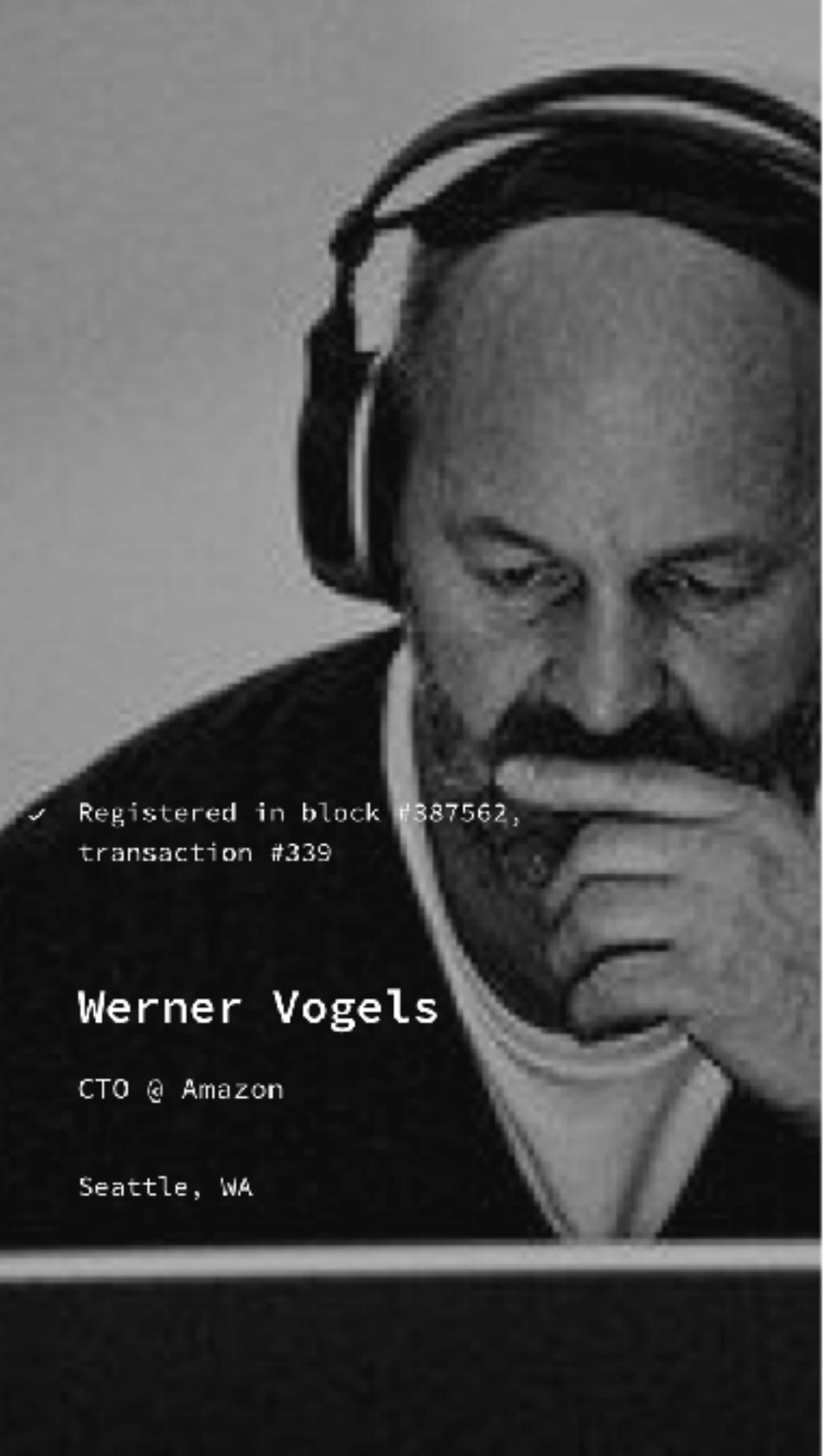
REGISTER IMPORT

Thomas Middleditch
thomasthemd.id

Tom Middleditch
tommyinthemiddle.id

Tom Middleditch
tmiddleditchvalley.id

✓ Registered in block #387562,
transaction #339

Werner Vogels
CTO @ Amazon
Seattle, WA

✓ f wernervogels
✓ t @werner
✓ o wv

Connections

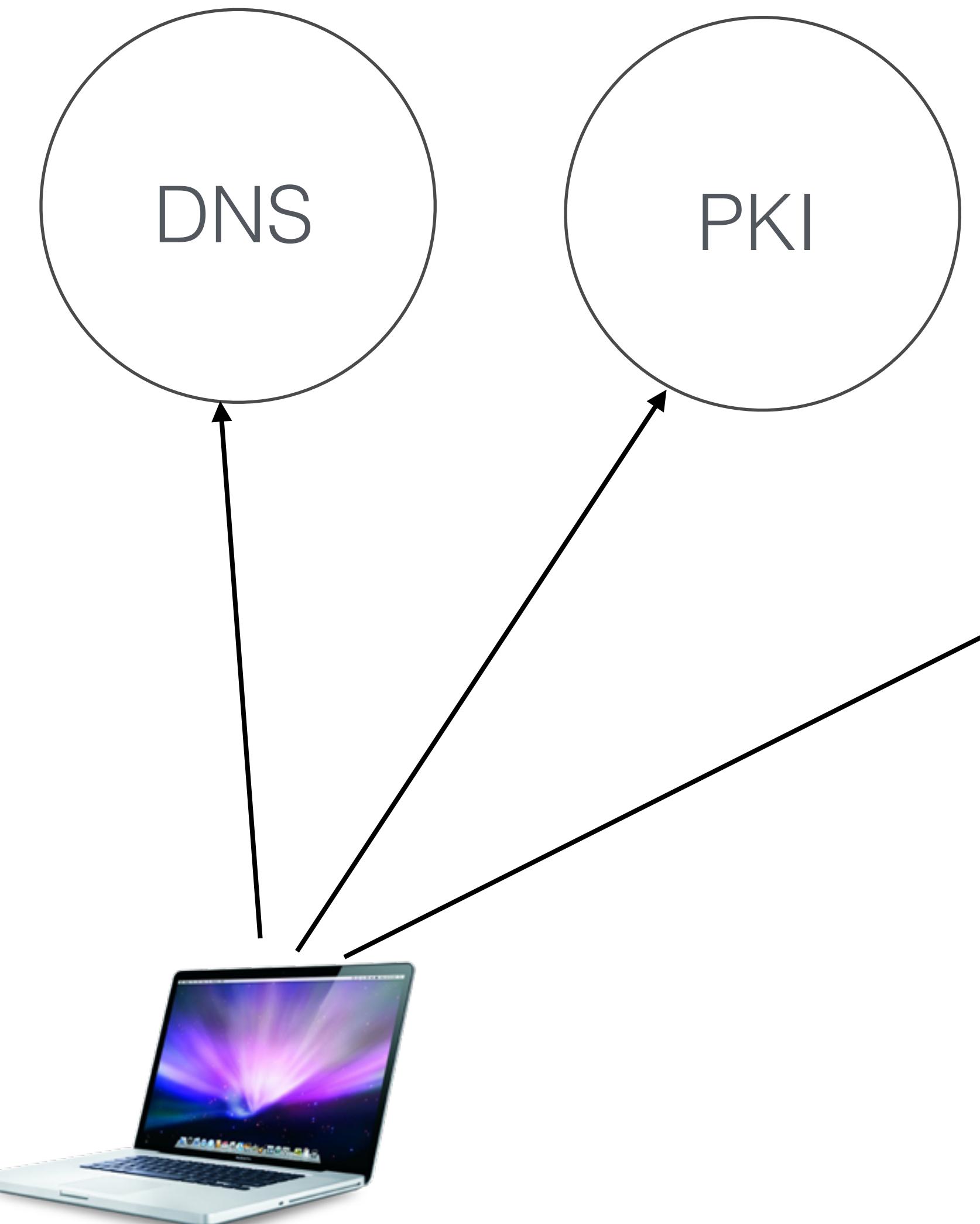
The New Internet



werner.id

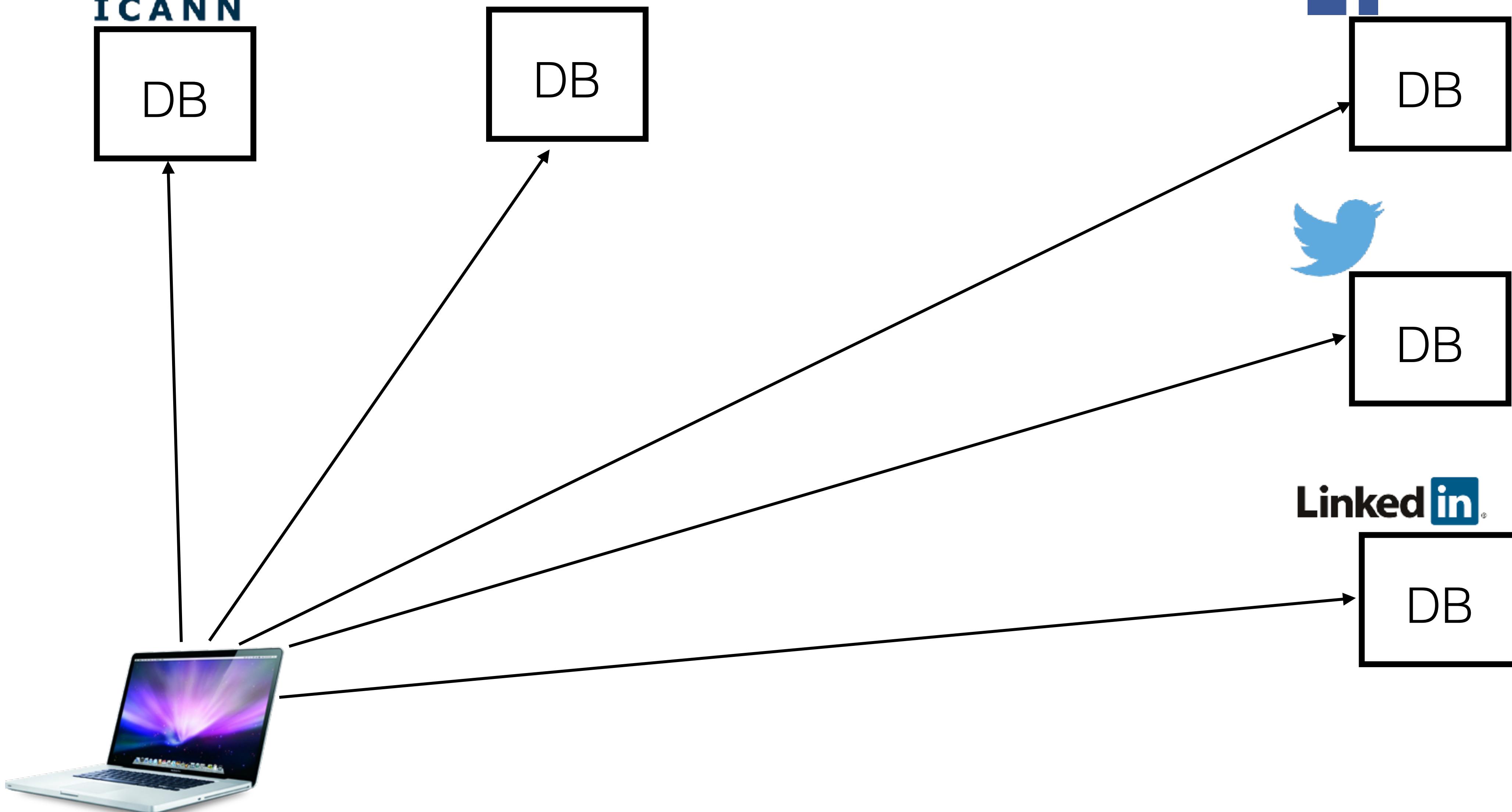
muneeb.id

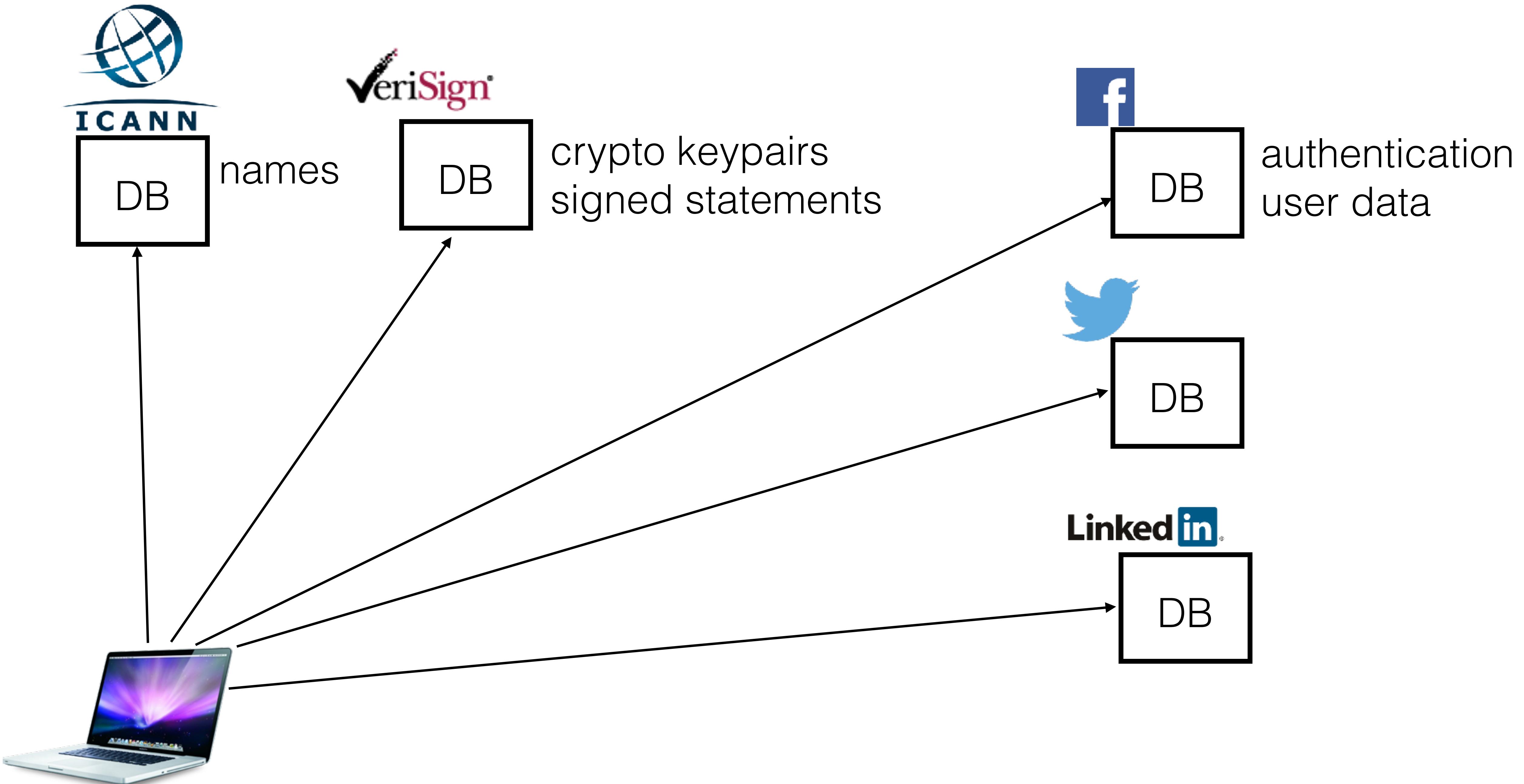






VeriSign





A Global Database

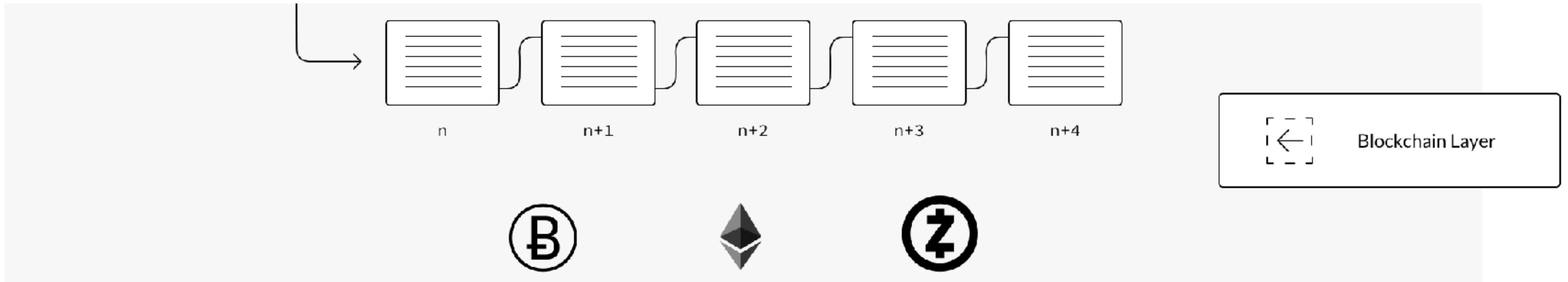
A Global Database

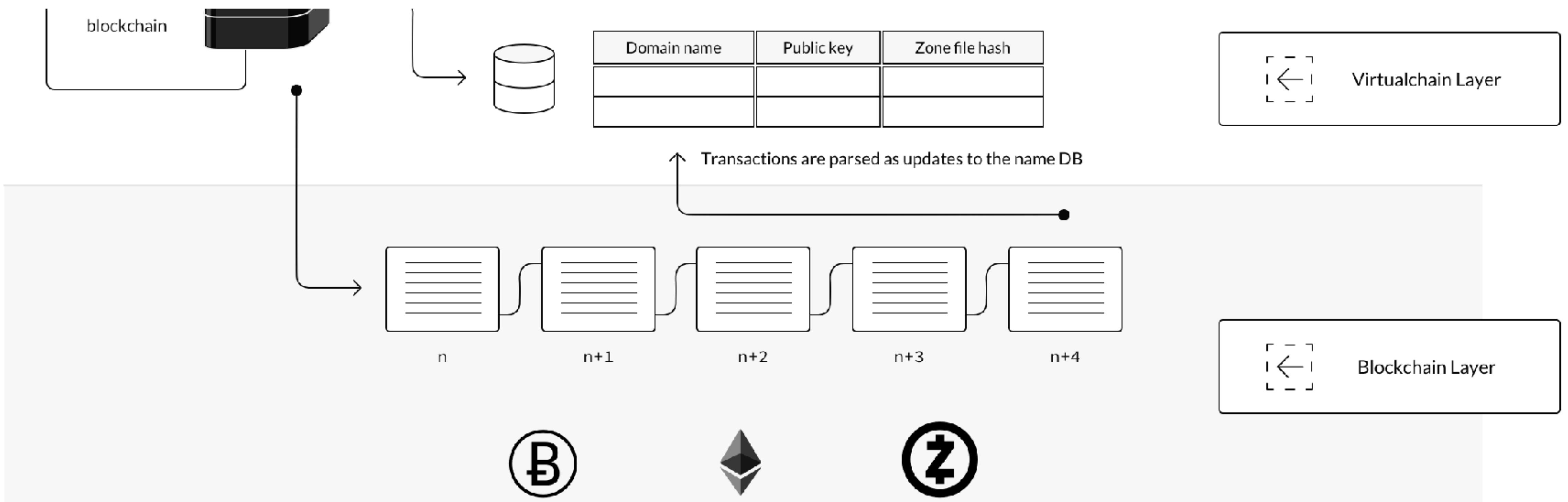
1. names
2. crypto keypairs
3. signed statements
4. authentication
5. user data

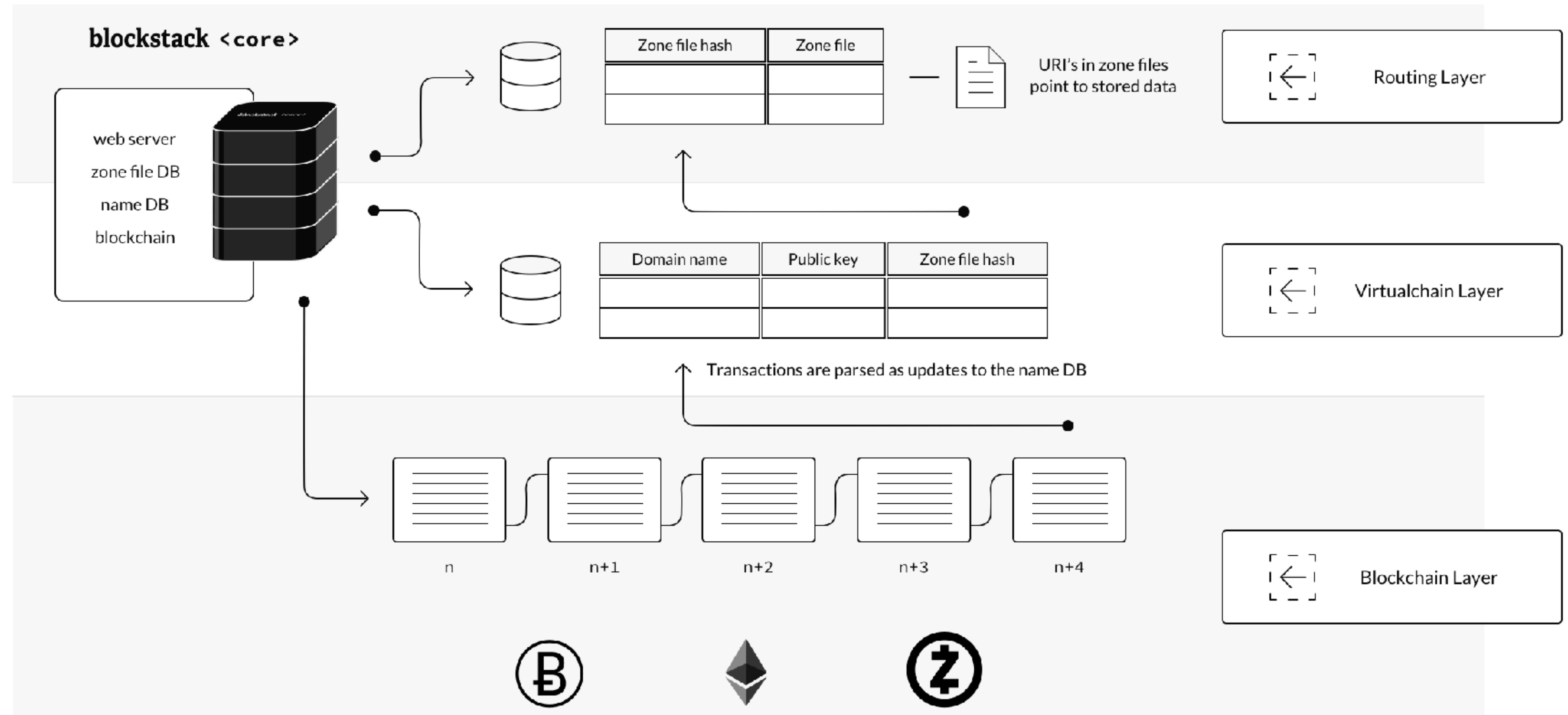
	data		
	muneeb.id		
	ryan.id		
	werner.id		

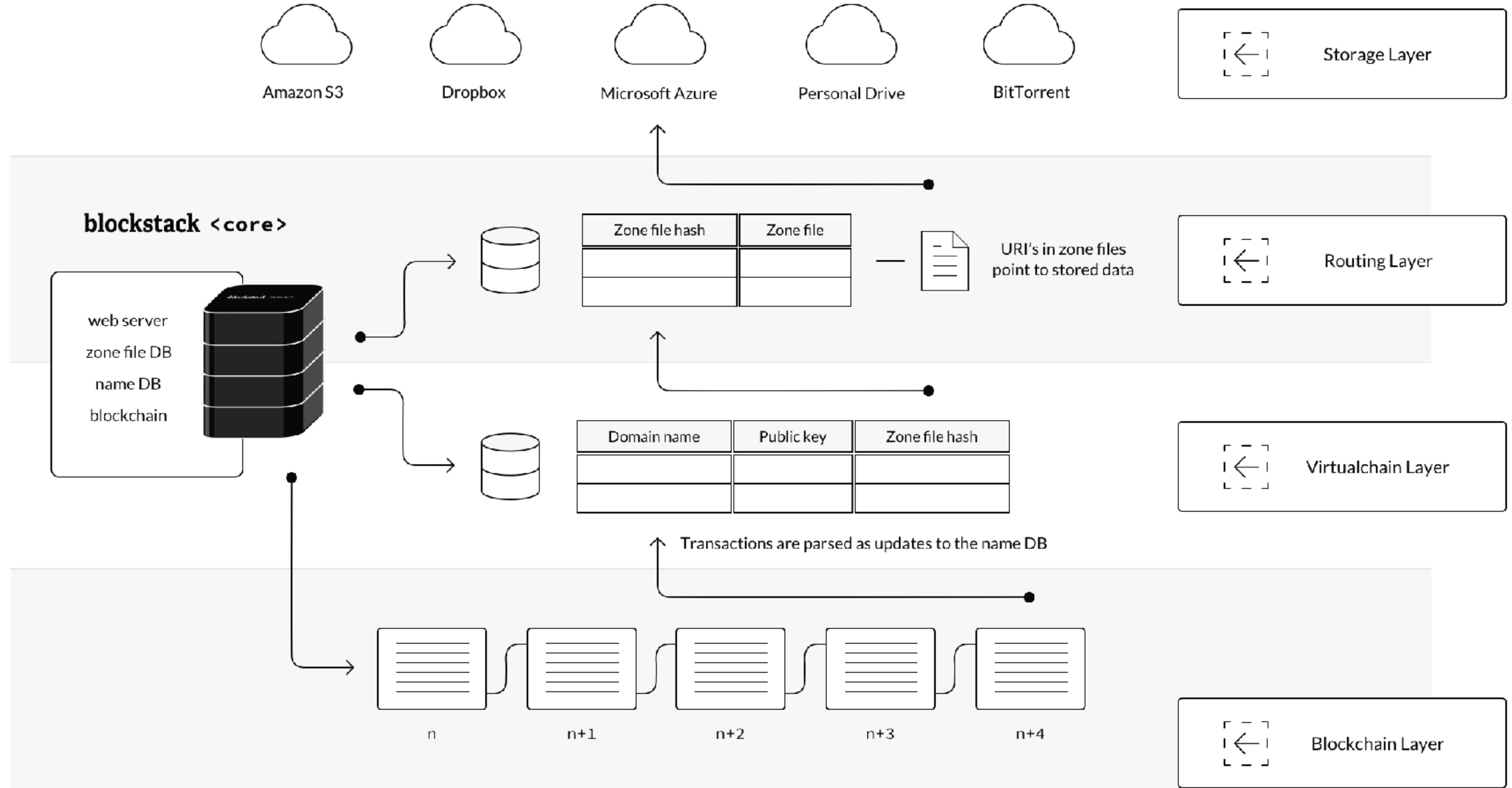


How Blockstack works







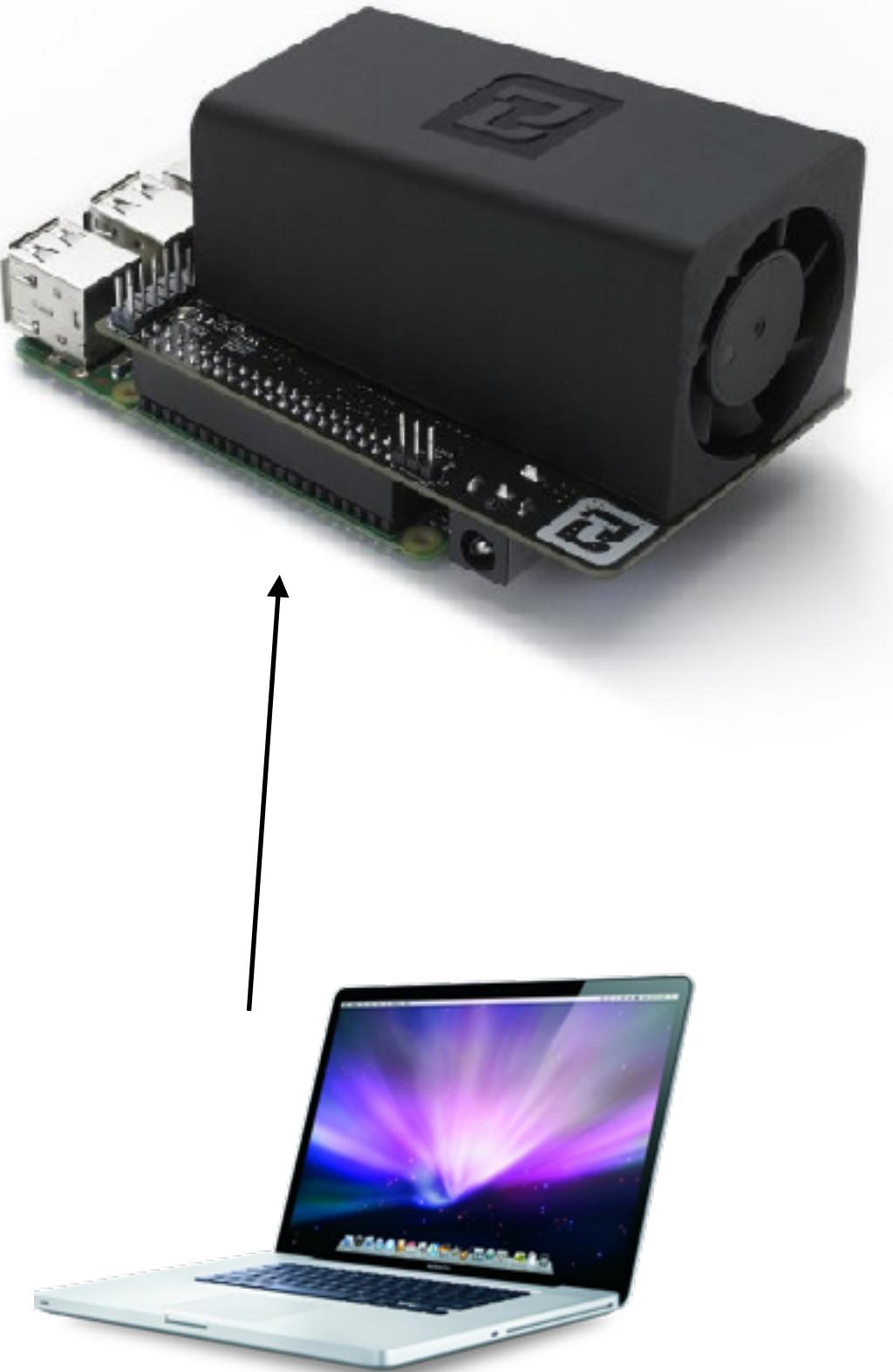
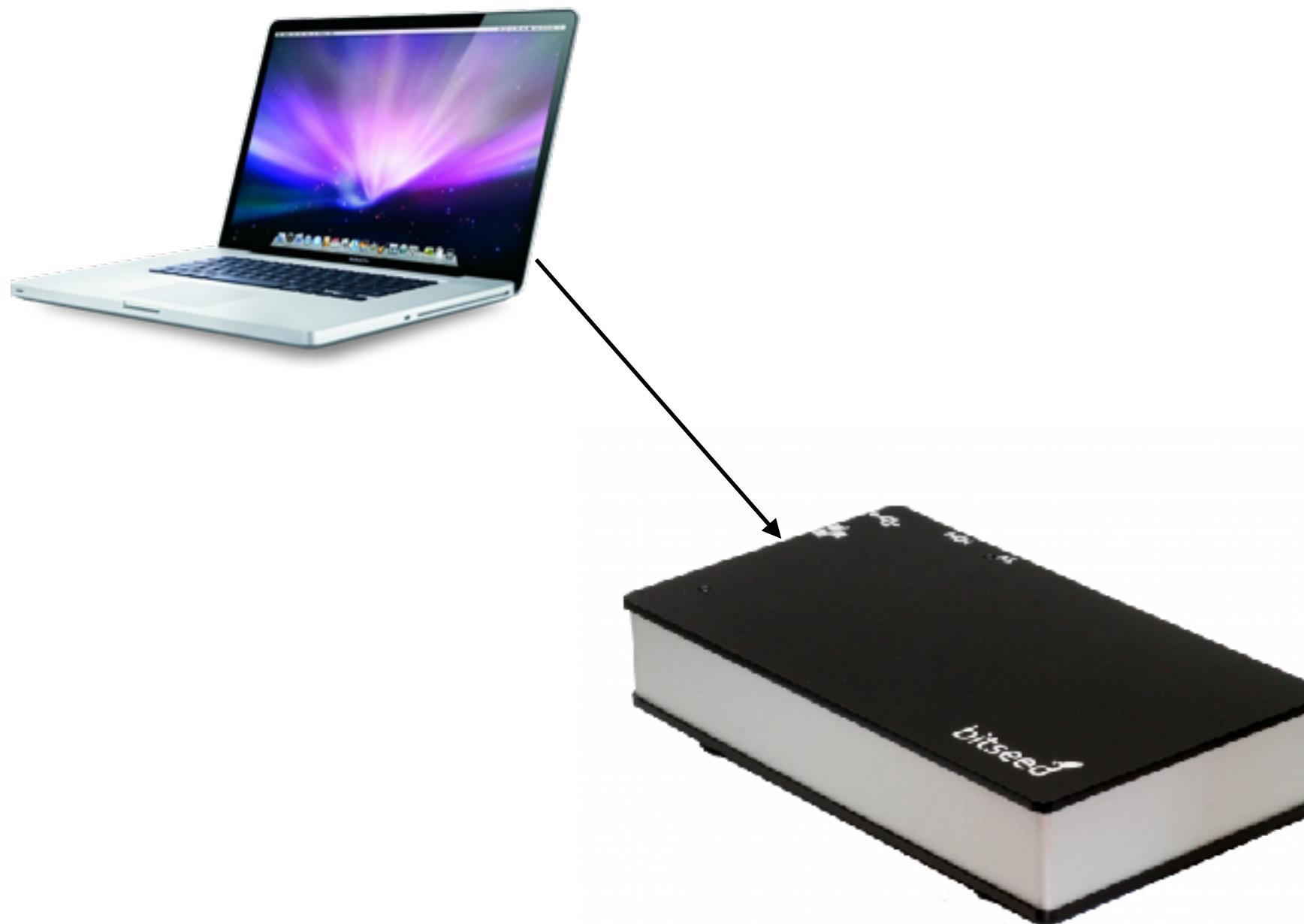


Example Zone File:

```
$ORIGIN werner.id
$TTL 3600
_http._tcp URI 10 1 http://54.231.237.47/werner.id
```

Security on the new Internet

Can ask for consensus hash from friends



Project Status



Werner Vogels

+werner

following 0

CTO @ Amazon

Seattle, WA · <http://smile.amazon.com>

Werner · proof

wernervogels · proof

wv · proof

B L O C K S T A C K

Names

Blocks

Status

Search for name, block, transaction or address

sandromarques.id

Owner [15YxdQosAFNUk4FPQPifqJqdHd5igmEkNV](#)

History

BLOCK #453386

NAME_TRANSFER

BLOCK #453343

NAME_UPDATE

BLOCK #453331

NAME_REGISTRATION

BLOCK #453323

NAME_PREORDER

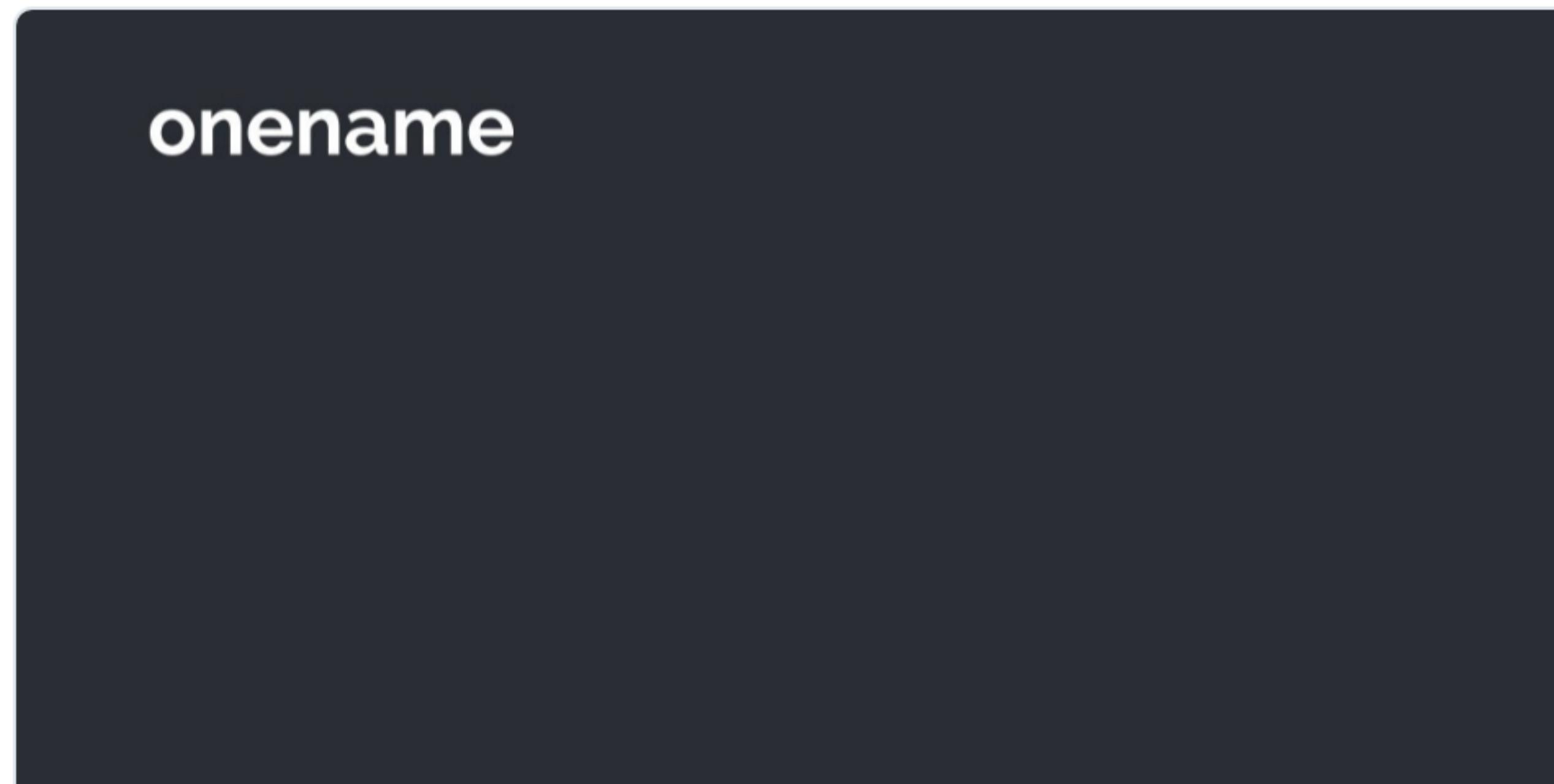


Tim Berners-Lee
@timberners_lee

Follow

Verifying that +timblee is my blockchain ID. onename.com/timblee

4:50 PM - 8 Jun 2016



+timblee on Onename

-

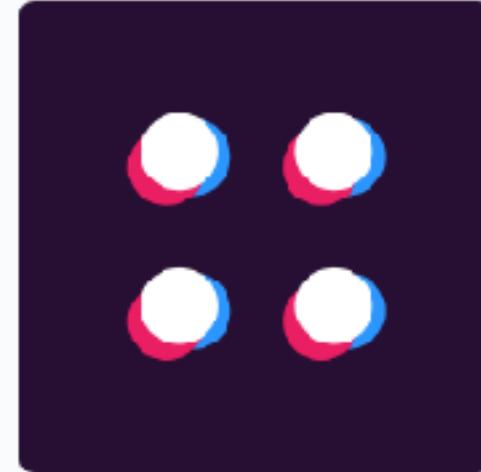
onename.com



188



376



Blockstack

A new decentralized internet

<https://blockstack.org>

Repositories

People 8

Teams 6

Projects 0

Settings

Pinned repositories

[Customize pinned repositories](#)

blockstack

Blockstack documentation and protocol specs

627 77

blockstack-core

The reference implementation of Blockstack

Python 702 96

blockstack-portal

The Blockstack Browser Portal

JavaScript 73 16

blockstack.js

The Blockstack JS library for identity and auth

HTML 189 51

blockstack.org

The Blockstack website

JavaScript 26 25

blockstack-explorer

A block explorer for Blockstack

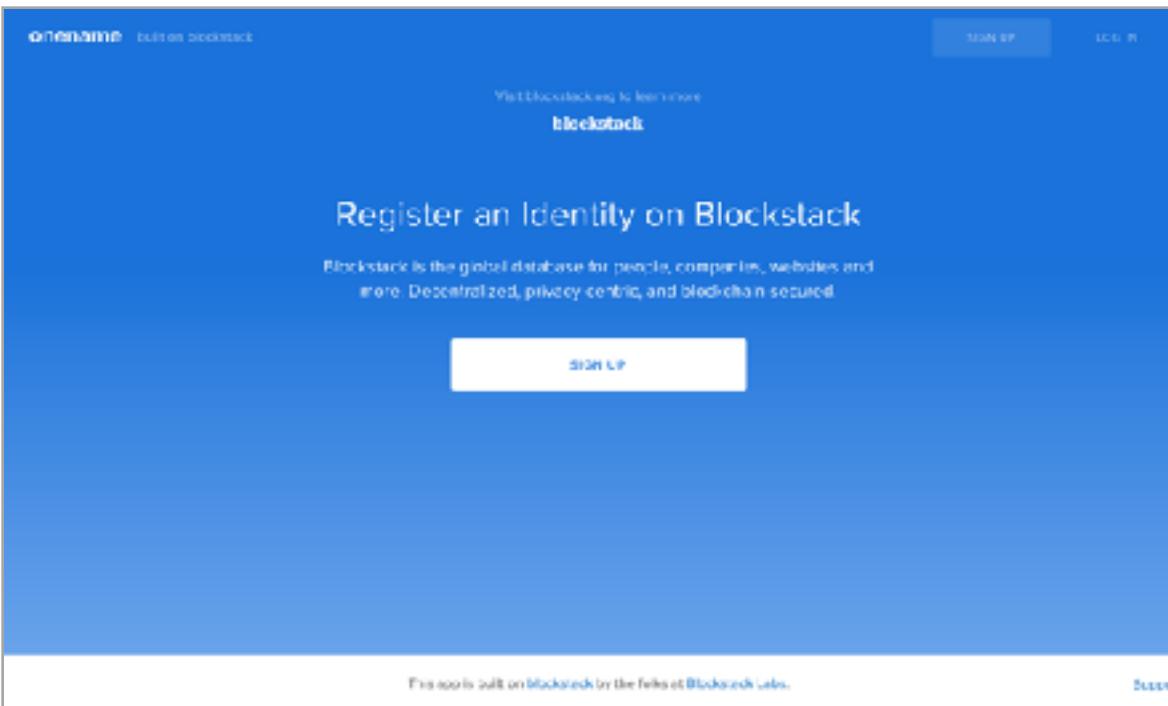
JavaScript 14 10

We launched several key Blockstack clients

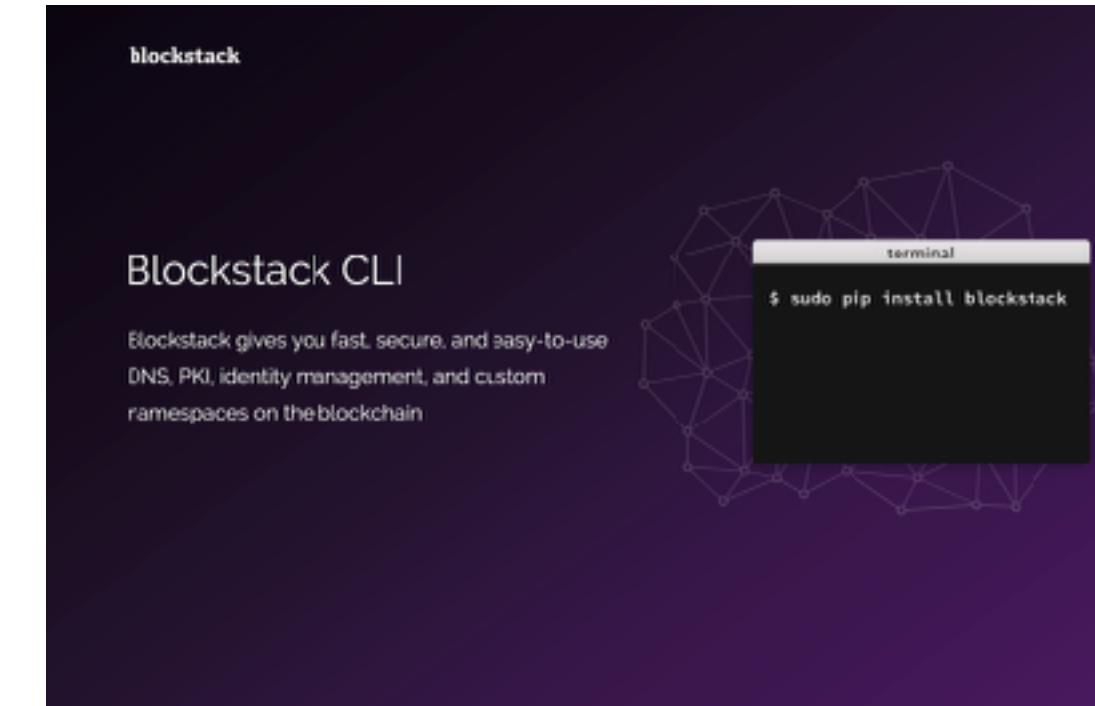


blockstack

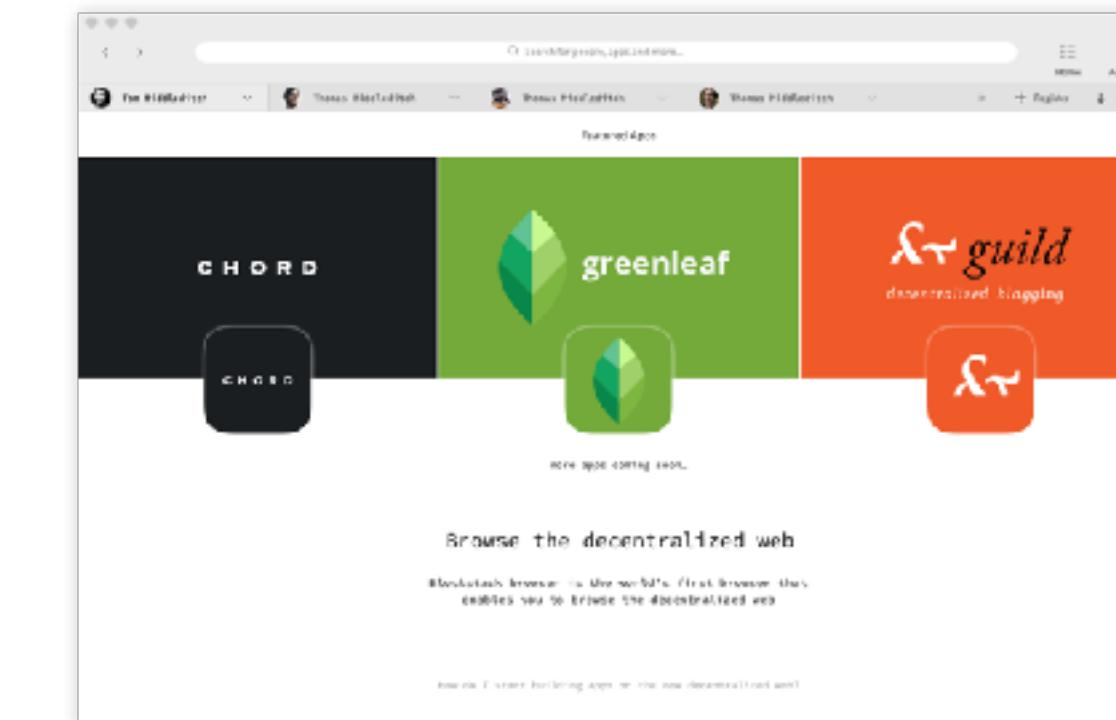
Onename
Web App



Blockstack
Command-line Interface



Blockstack
Browser

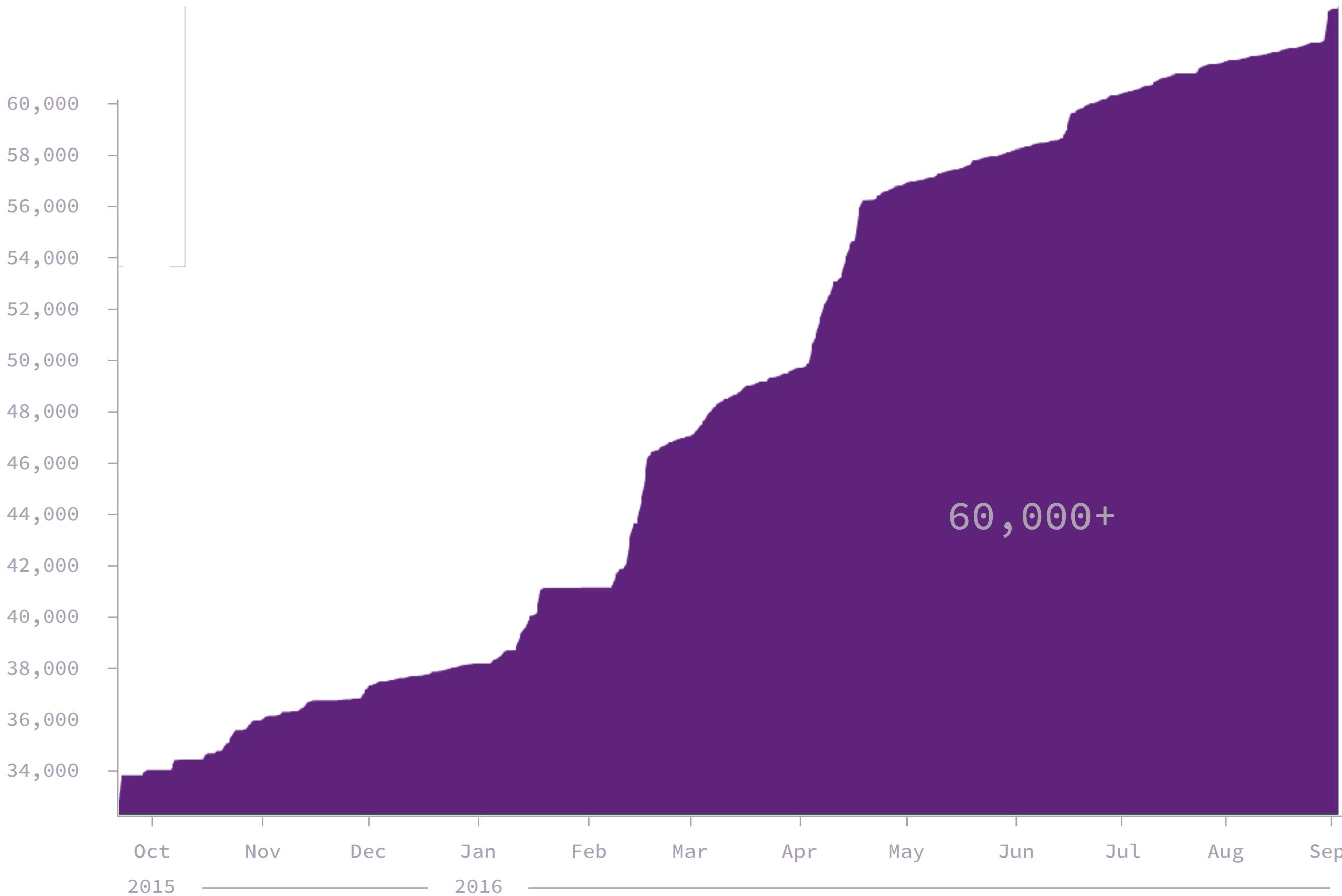


```
$ blockstack lookup fredwilson.id
```

You should get a response like this:

```
{
  "data_record": {
    "name": "Fred Wilson",
    "bio": "I am a VC",
    "website": "http://avc.com"
    ...
  }
}
```

Registrations in the .id namespace



There are developer meetups around the world



5,469
members

17
Meetups

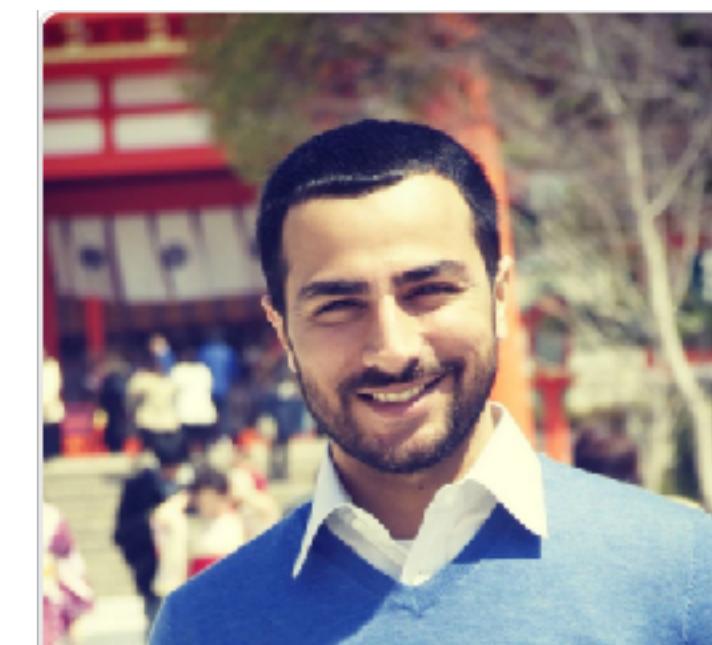
Advisors



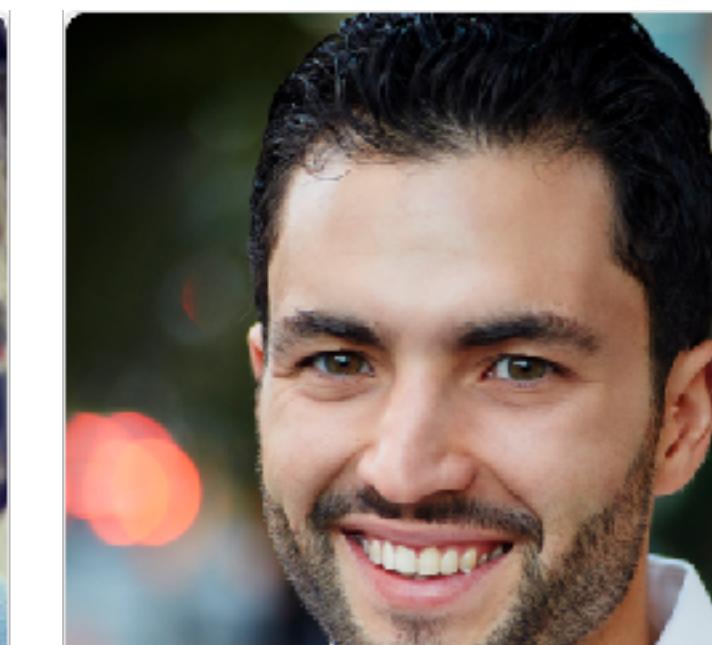
+judecn
Jude Nelson



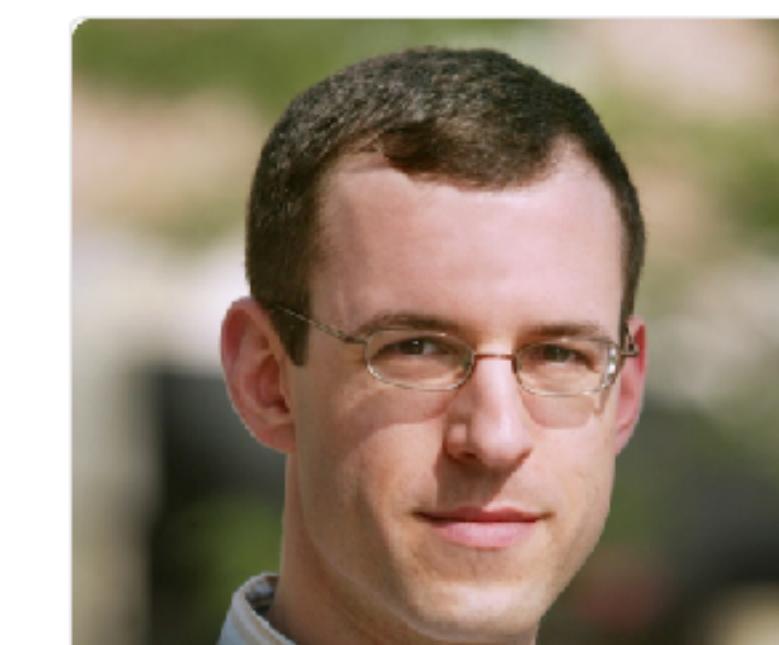
+guylepage3
Guy Lepage



+muneeb
Muneeb Ali



+ryan
Ryan Shea



+mfreed
Mike Freedman



+jp
JP Singh

plus open-source contributors and 3000+ community members



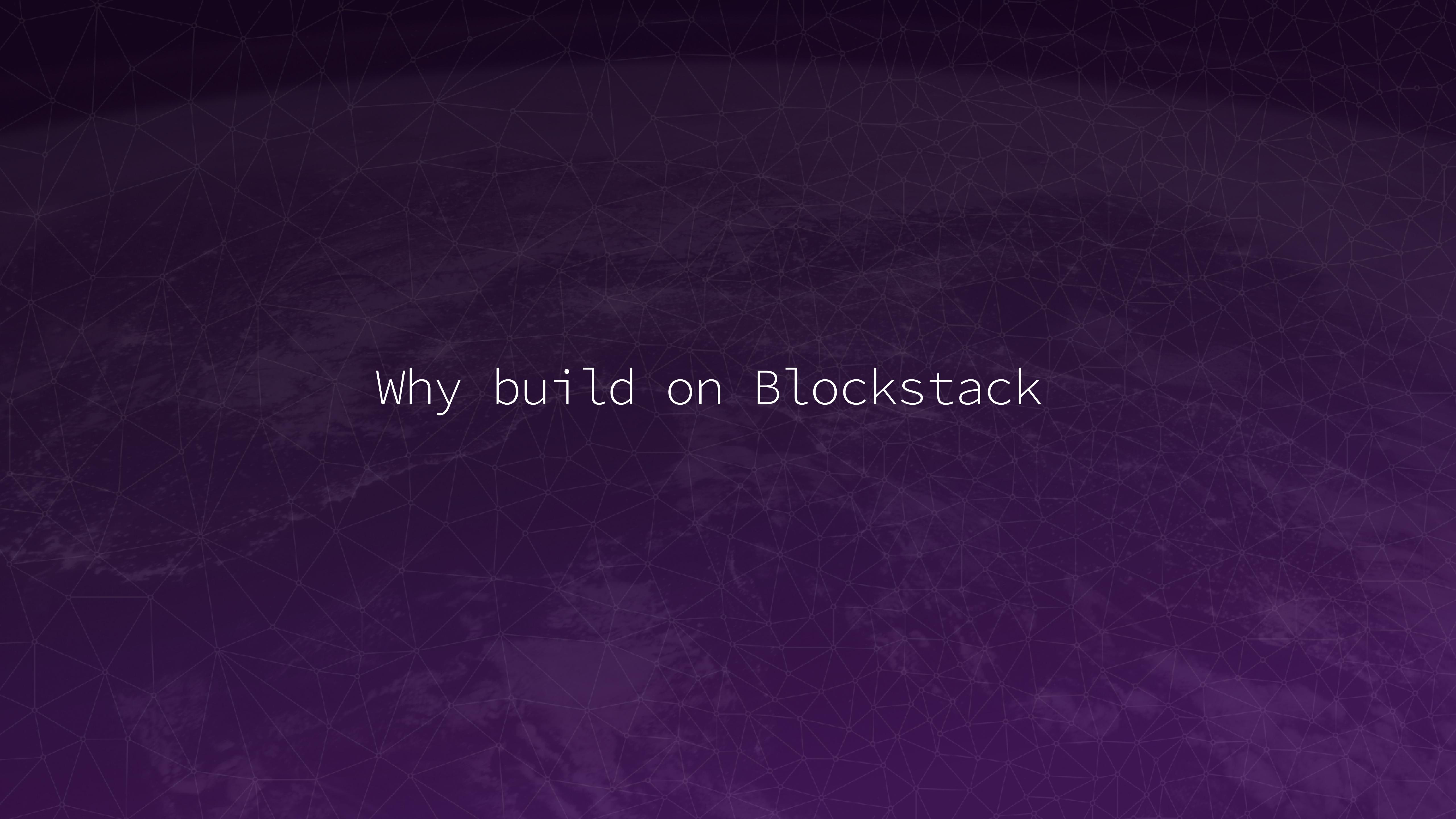
Larry Salibra



Patrick Stanley



Aaron Blankstein

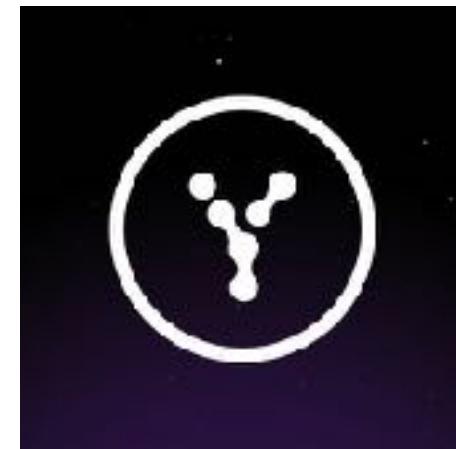


Why build on Blockstack

Organizations building on Blockstack range from startups to academic institutions to large enterprises



OpenBazaar



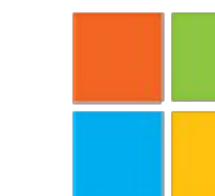
CONSENSYS



DemocracyOS

anyshare

consent



Microsoft



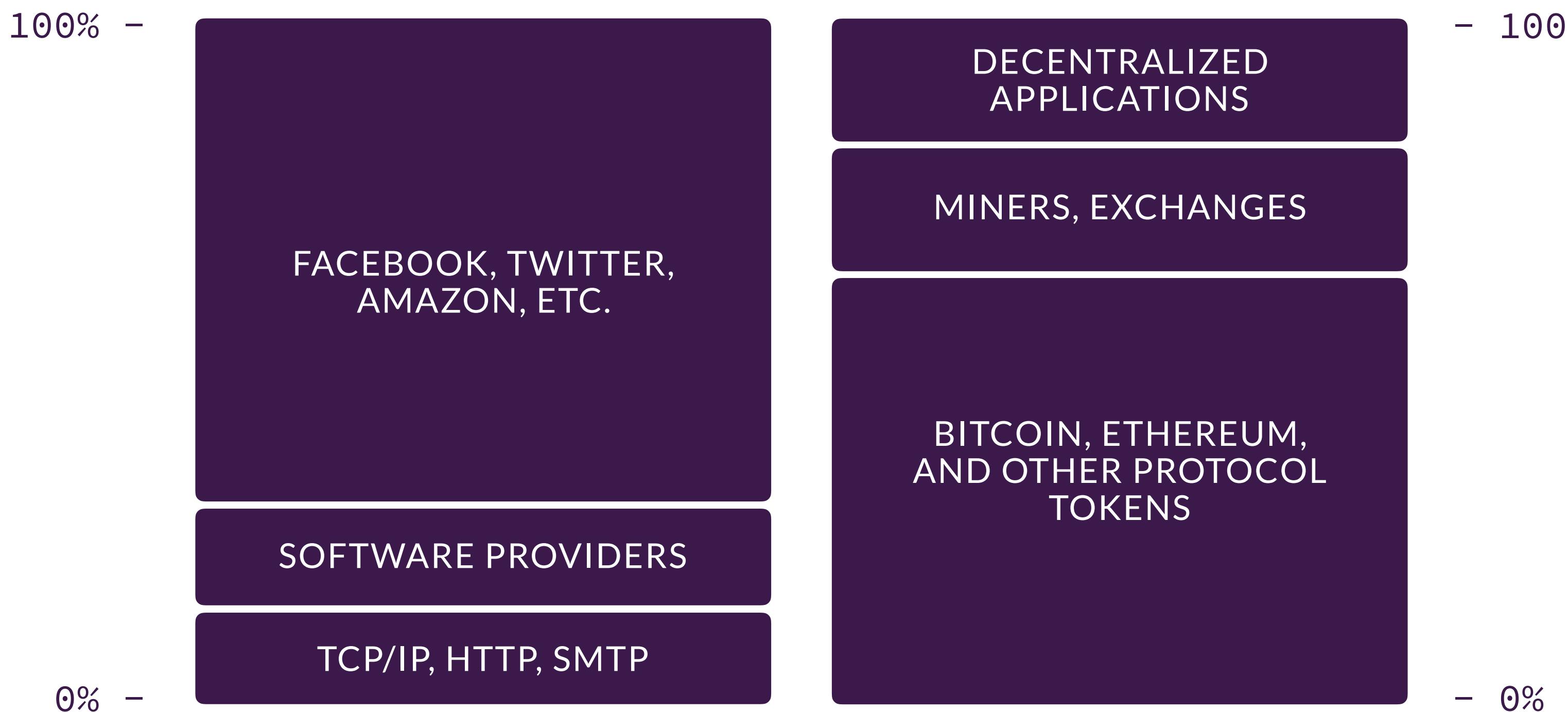
OpenCloud

Serverless Computing

- Push computing to client-side (JS apps)
- Little to no infrastructure to manage
- New business models

```
import blockstack from 'blockstack'
let user = blockstack.loginUser()
user.get("photos")
```

Thesis: value capture will move down the software stack



More info: <https://www.usv.com/blog/fat-protocols>

In the real world, we have property rights.

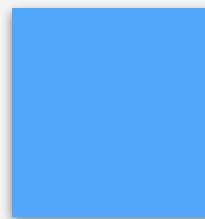


The New Internet



 **blockstack**

werner.id



muneeb.id



 **blockstack**

Old Internet

#1 Blind Trust

#2 No Ownership

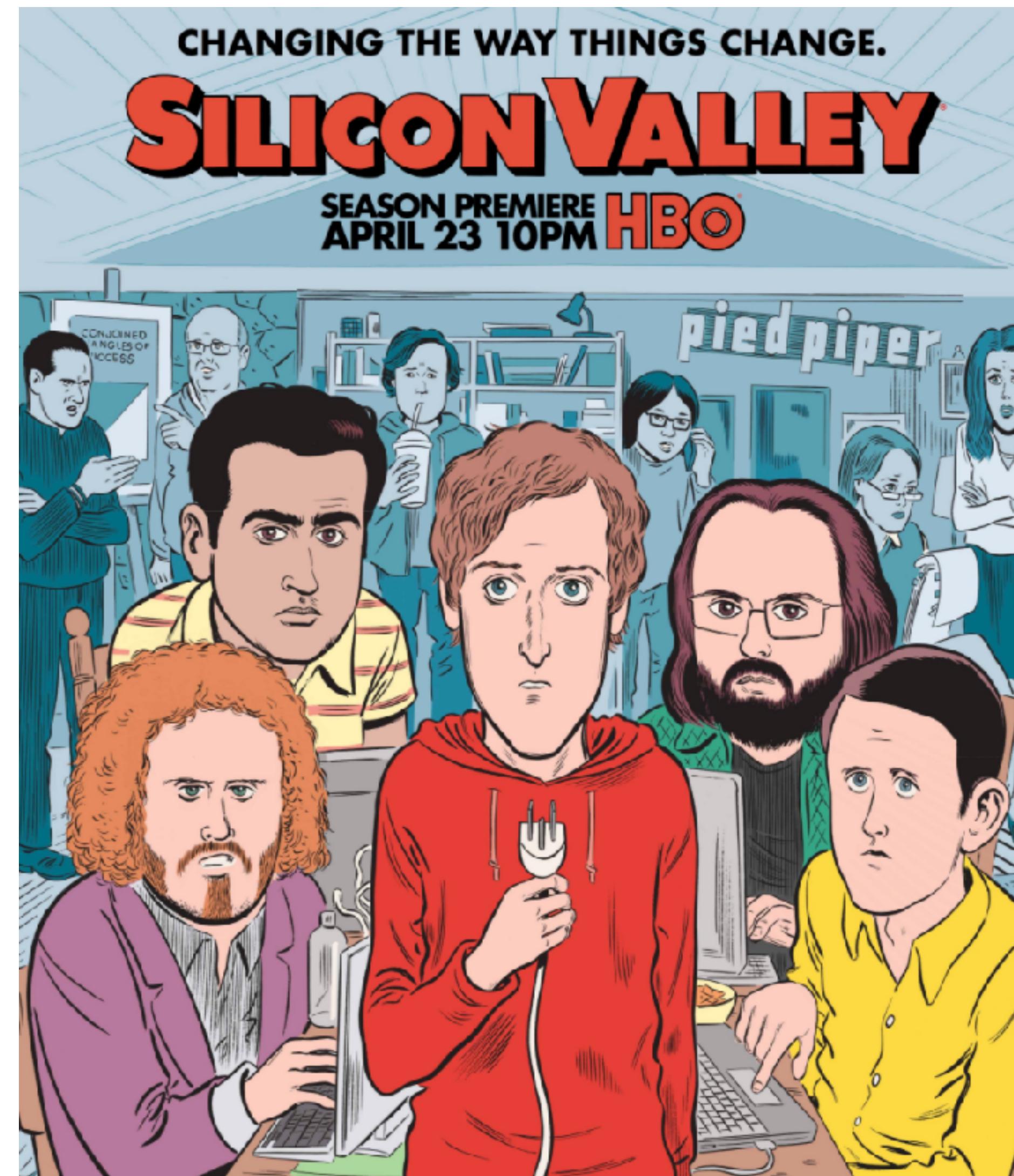
New Internet

#1 ~~Blind Trust~~

#2 ~~No~~ Ownership

Let's build a new decentralized Internet!

**Let's build a new decentralized Internet!
(as featured on the Silicon Valley show)**



Thank you

Twitter:

@muneeb

@blockstackorg

More Info:

Website: blockstack.org

Code: github.com/blockstack

Paper: blockstack.org/papers

Talks: blockstack.org/videos