blockstack

Blockstack: A Global Naming and Storage System Secured by Blockchains

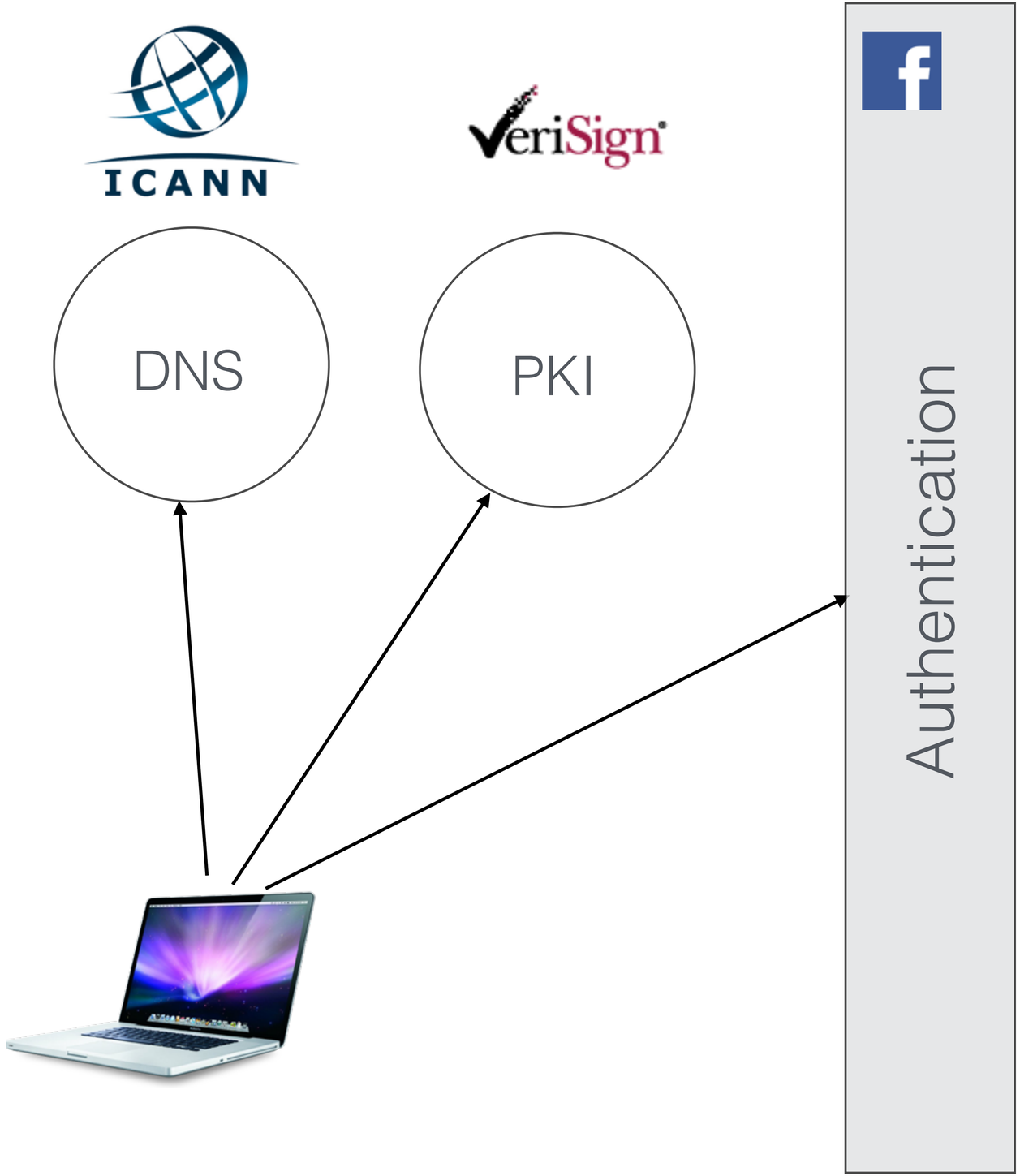
Muneeb Ali, Jude Nelson, Ryan Shea, and Michael Freedman

Blockstack Labs and Princeton University

Outline

— Problem
— Background on blockchains
— Lessons from production deployment
— Design of Blockstack
— Performance results & future work

Problem



facebook

Centralized
User Data

Decentralized
DNS +PKI

Decentralized Auth

Decentralized
User Data

Background

How Blockchains Work

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)	

How Blockchains Work

We need a distributed ledger
(blockchain)

How Blockchains Work

— It’s a file!

— Append-only global log

— Every node on the network has a consistent copy

General Challenges with Blockchains:

— Storage limitations (blockchain bloat)

— Introducing new features (hard fork)

— Slow writes

— Endless ledger problem

Blockchain DNS + PKI

Werner Vogels

+werner

following 0

CTO @ Amazon

Seattle, WA · http://smile.amazon.com

Werner · proof

wernervogels · proof

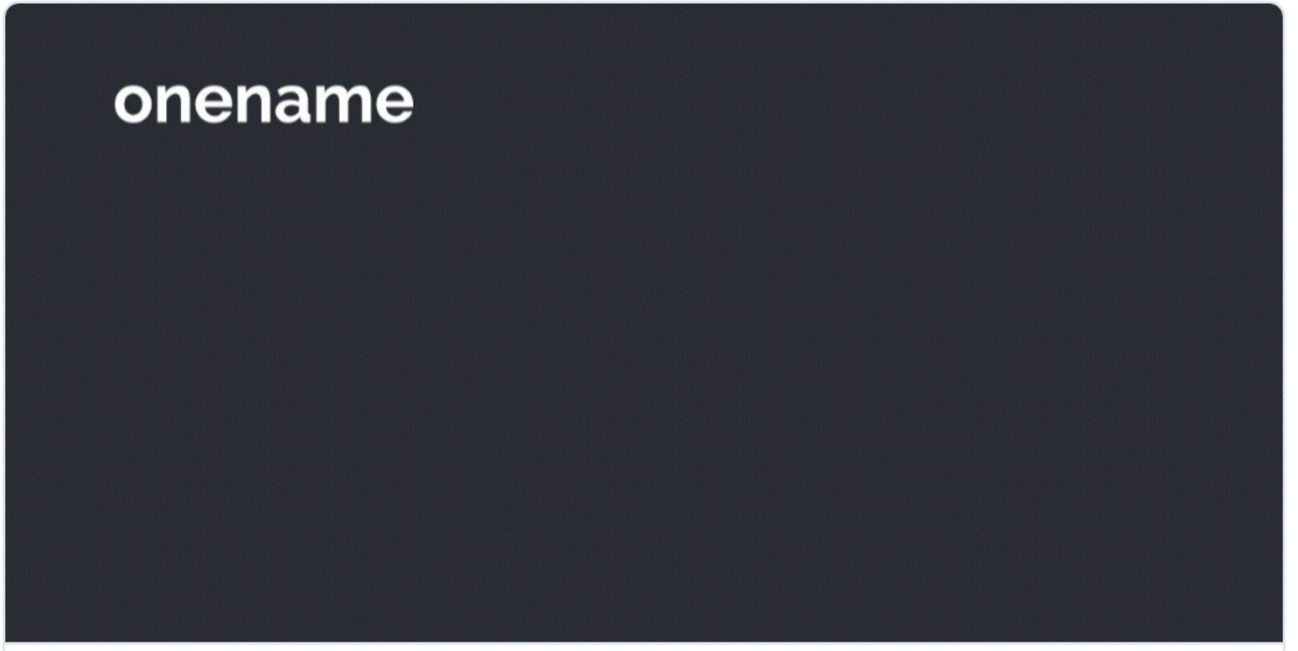
wv · proof

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

2015-02-28 20:28:46	220006	f4fa7479fc...	OP_NAME_UPDATE	{"website": "http://smile.amazon.com", "bio": "CTO @ Amazon", "github": {"username": "wv", "proof": {"url": "https://gist.github.com/wv/2427b5a69aec5524ca67"}}, "name": {"formatted": "Werner Vogels"}, "twitter": {"username": "Werner", "proof": {"url": "https://twitter.com/Werner/status/571698777297321985"}}, "cover": {"url": "https://s3.amazonaws.com/dx3/werner"}, "bitcoin": {}, "next": "i/werner-1"}
2015-02-27 20:34:17	219910	0e5037d25f...	OP_NAME_UPDATE	{"website": "http://smile.amazon.com", "bio": "CTO @ Amazon", "name": {"formatted": "Werner Vogels"}, "twitter": {"username": "Werner"}, "cover": {"url": "https://s3.amazonaws.com/dx3/werner"}, "bitcoin": {}, "location": {"formatted": "Seattle, WA"}, "v": "0.2", "avatar": {"url": "https://s3.amazonaws.com/kd4/werner"}}
2014-07-14 06:30:59	186807	918e306bb5...	OP_NAME_NEW	c40f99f8ee5da0f03d3ecf4e3ce013a91bd3efec

Lessons from Namecoin

Production system on Namecoin:

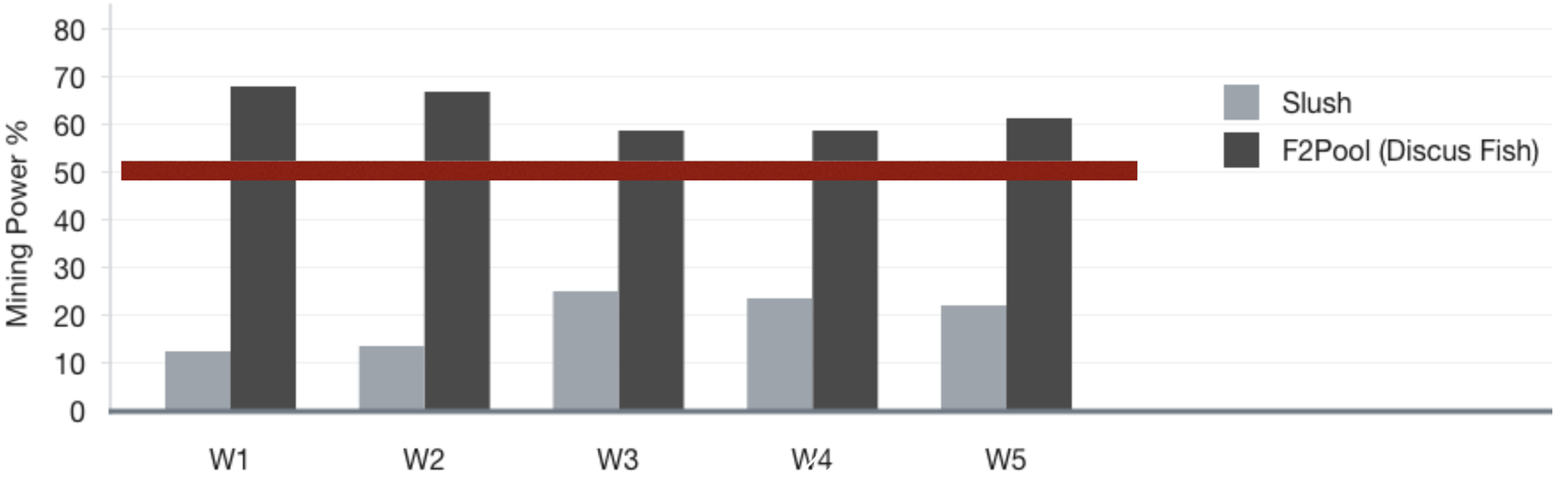
— Used u/ namespace

— Live between March 2014 and August 2015

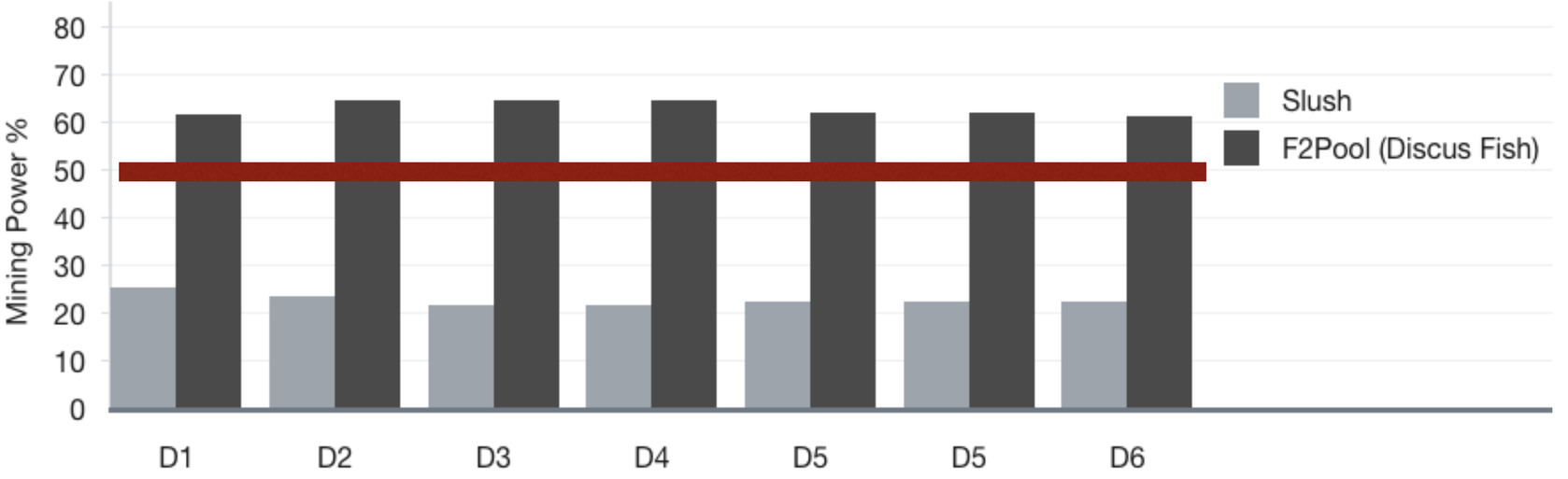
— 33,000 registrations

— Over 200,000 transactions

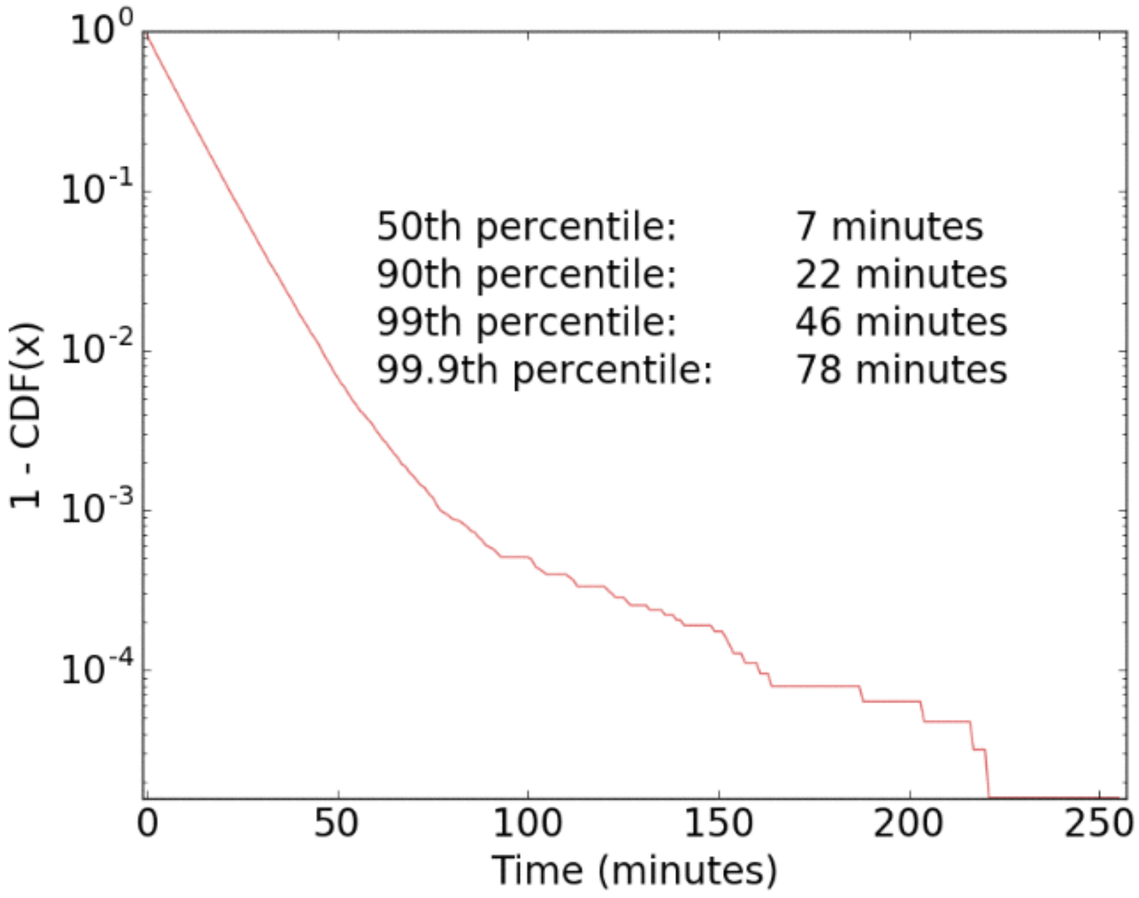
Weekly Distribution *(7/27 – 8/30)*



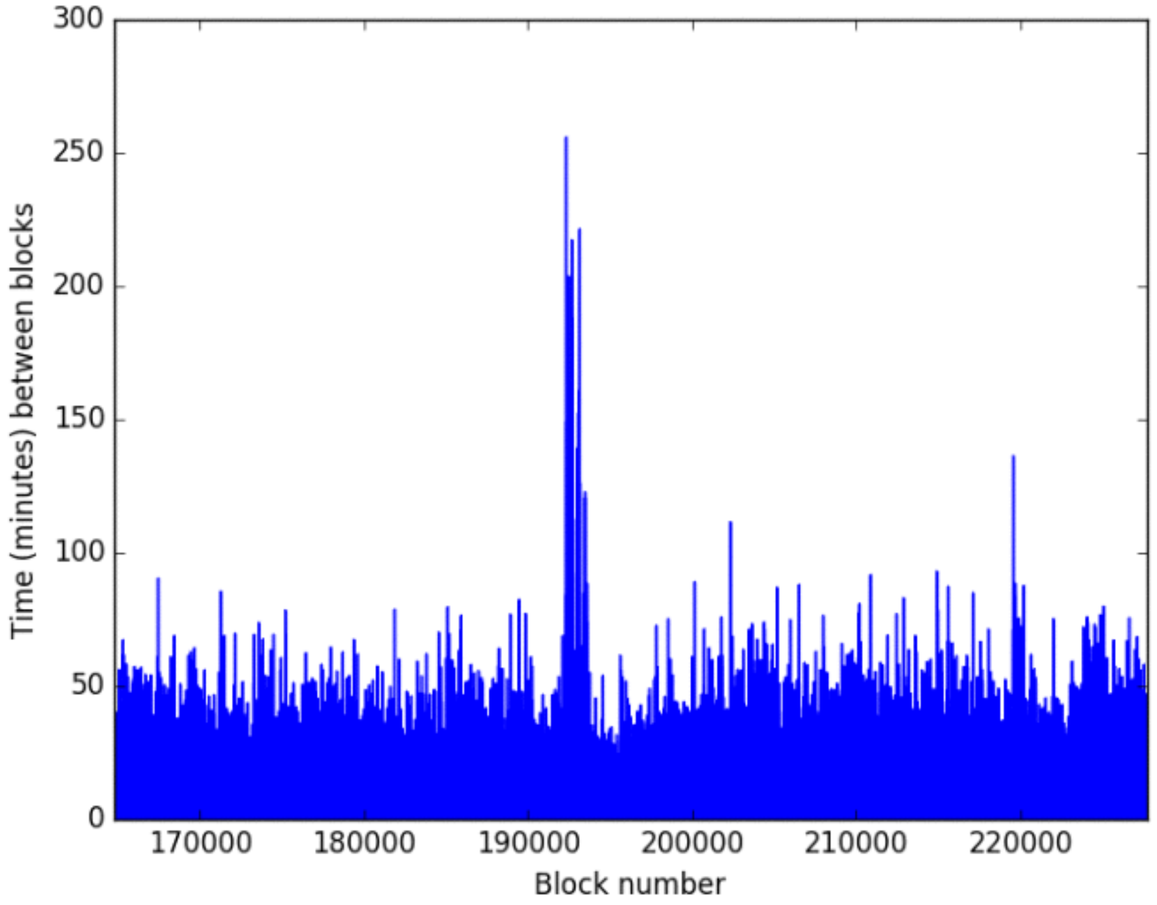
Daily Distribution *(8/24 – 8/30)*



Network latency:



(a) CCDF of network latency (03/14 – 04/15)



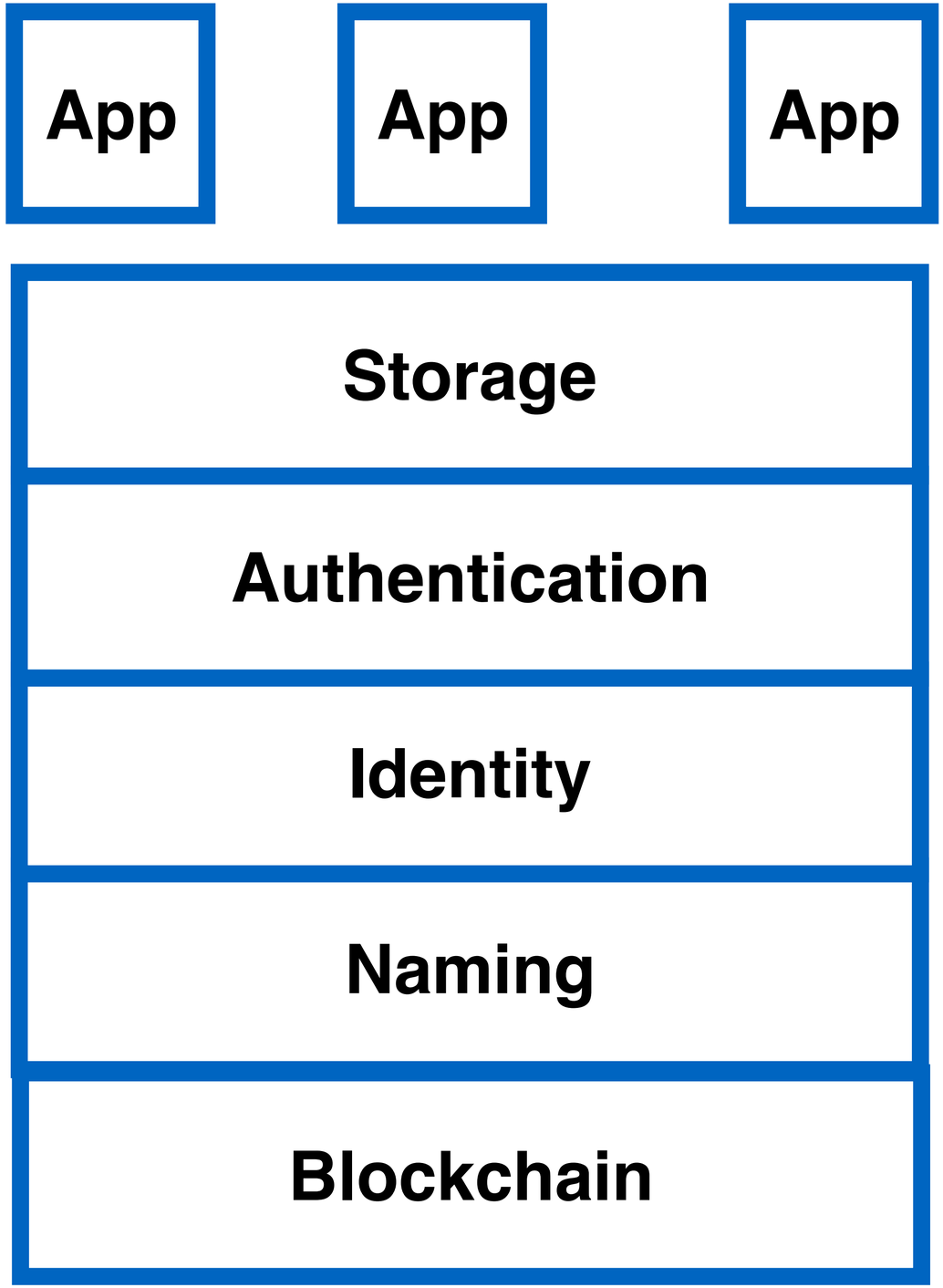
(b) Network latency per new block (03/14 – 04/15)

Design of Blockstack

“Security Box”

Follow David Clark’s trust-to-trust principle

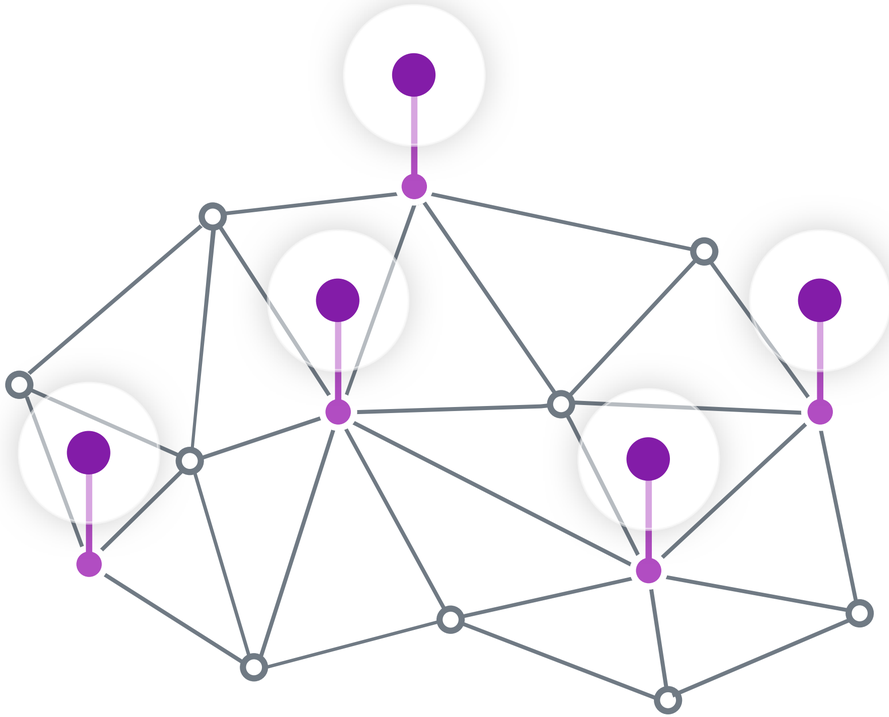
blockstack

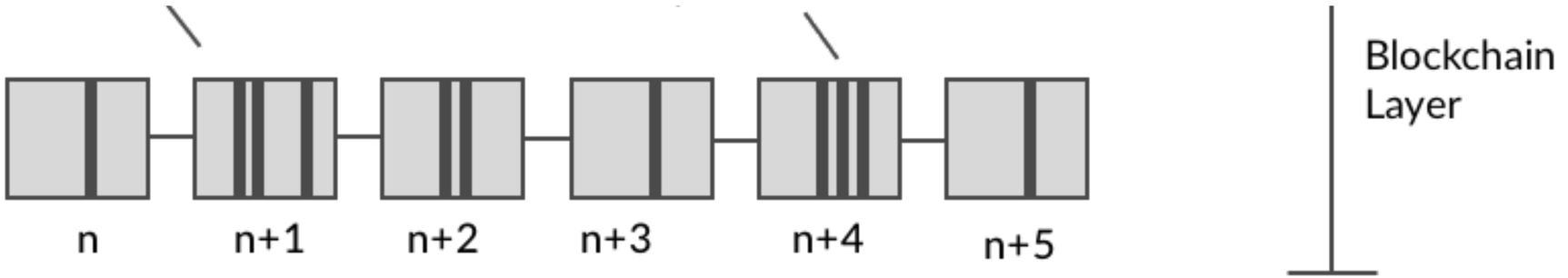

App
App
App
Storage
Authentication
Identity
Naming
Blockchain

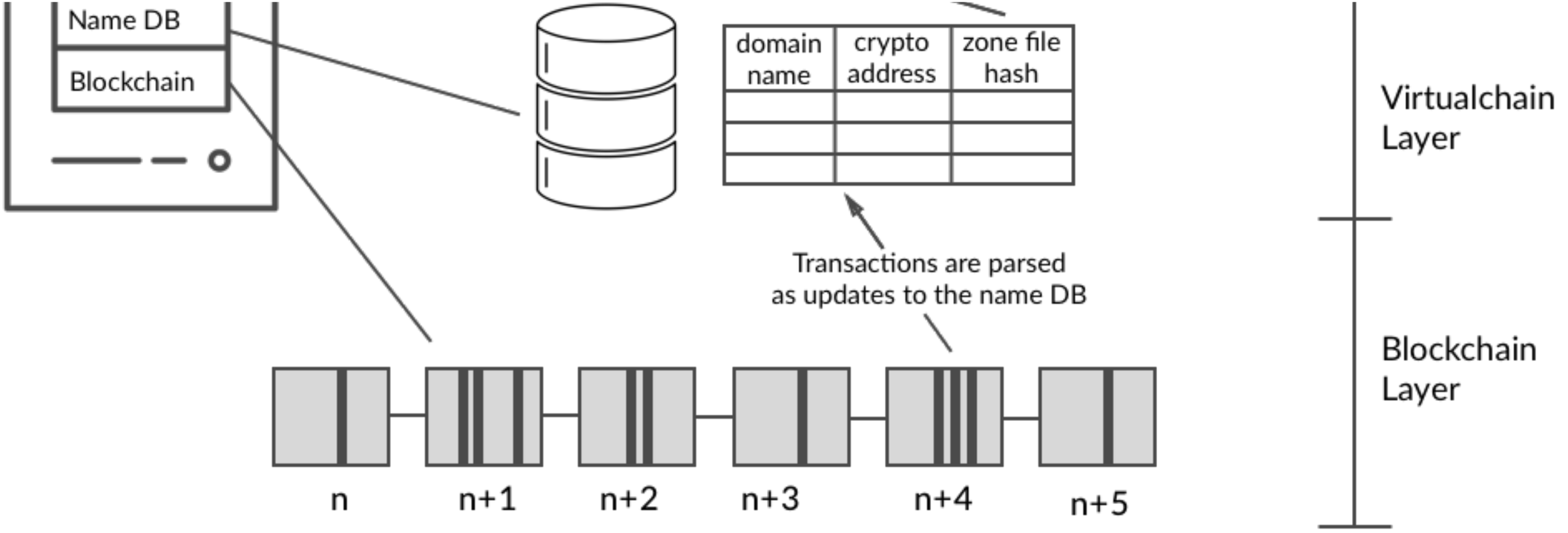
blockstack

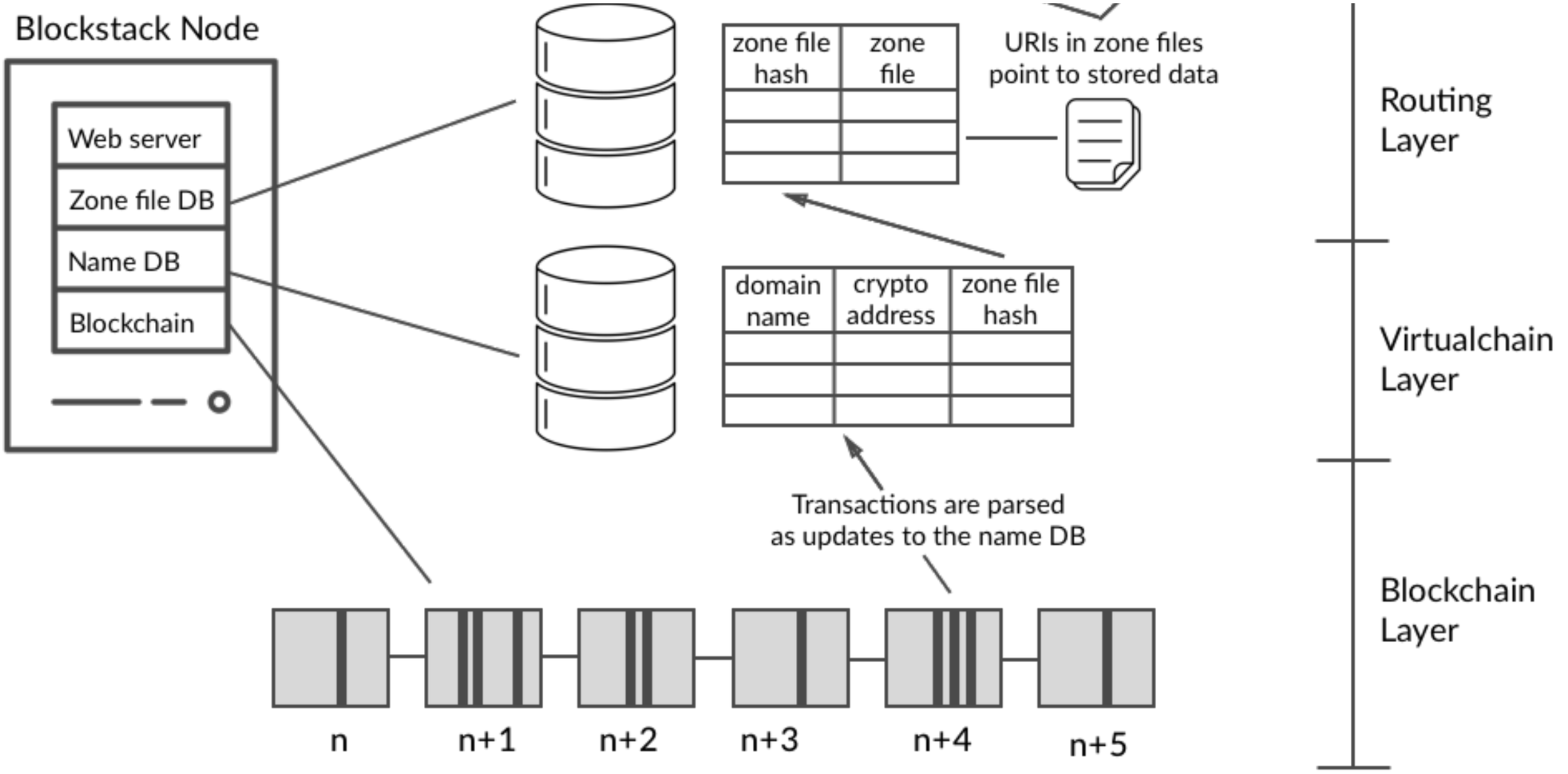
Blockstack Network

- bitcoin node (bitcoind)
- blockstack server
- bitcoind peer connection
- rpc connection to bitcoind



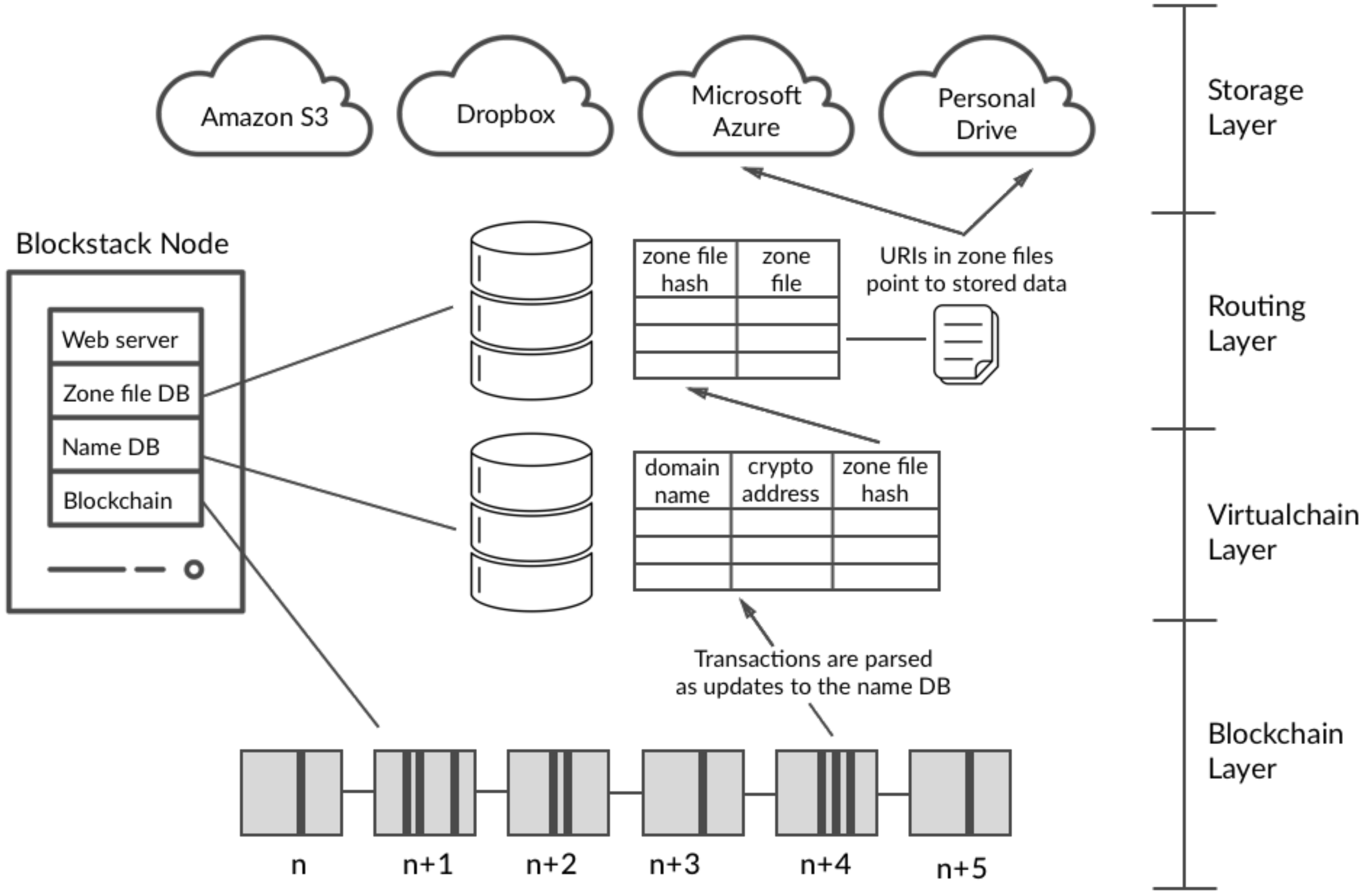

n
n+1
n+2
n+3
n+4
n+5
Blockchain
Layer


Name DB
Blockchain
domain name
crypto address
zone file hash
Transactions are parsed as updates to the name DB
n
n+1
n+2
n+3
n+4
n+5
Virtualchain Layer
Blockchain Layer


Blockstack Node
Web server
Zone file DB
Name DB
Blockchain
zone file hash
zone file
URIs in zone files point to stored data
domain name
crypto address
zone file hash
Transactions are parsed as updates to the name DB
n
n+1
n+2
n+3
n+4
n+5
Routing Layer
Virtualchain Layer
Blockchain Layer

Example Zone File:

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


Amazon S3
Dropbox
Microsoft Azure
Personal Drive
Storage Layer
Blockstack Node
Web server
Zone file DB
Name DB
Blockchain
zone file hash
zone file
URIs in zone files point to stored data
Routing Layer
domain name
crypto address
zone file hash
Virtualchain Layer
Transactions are parsed as updates to the name DB
Blockchain Layer
n
n+1
n+2
n+3
n+4
n+5

Lessons from Production Use:

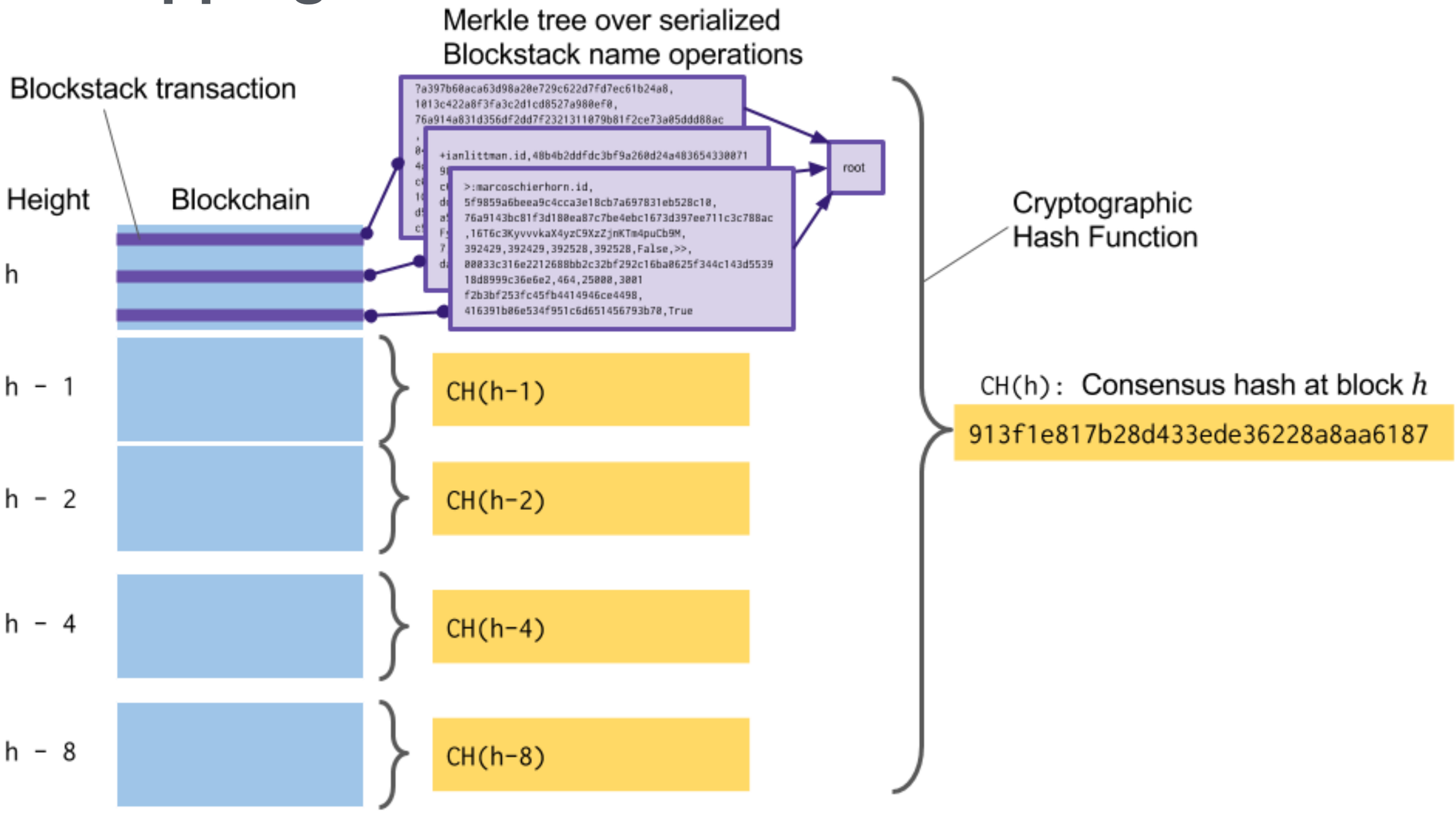
— Security issues —> Need most secure blockchain (migrate)

— Storage limitations (blockchain bloat) —> Unlimited data

— Introducing new features (hard fork) —> Virtualchain

— Slow writes —> Get operations off blockchain path

Fast Bootstrapping:

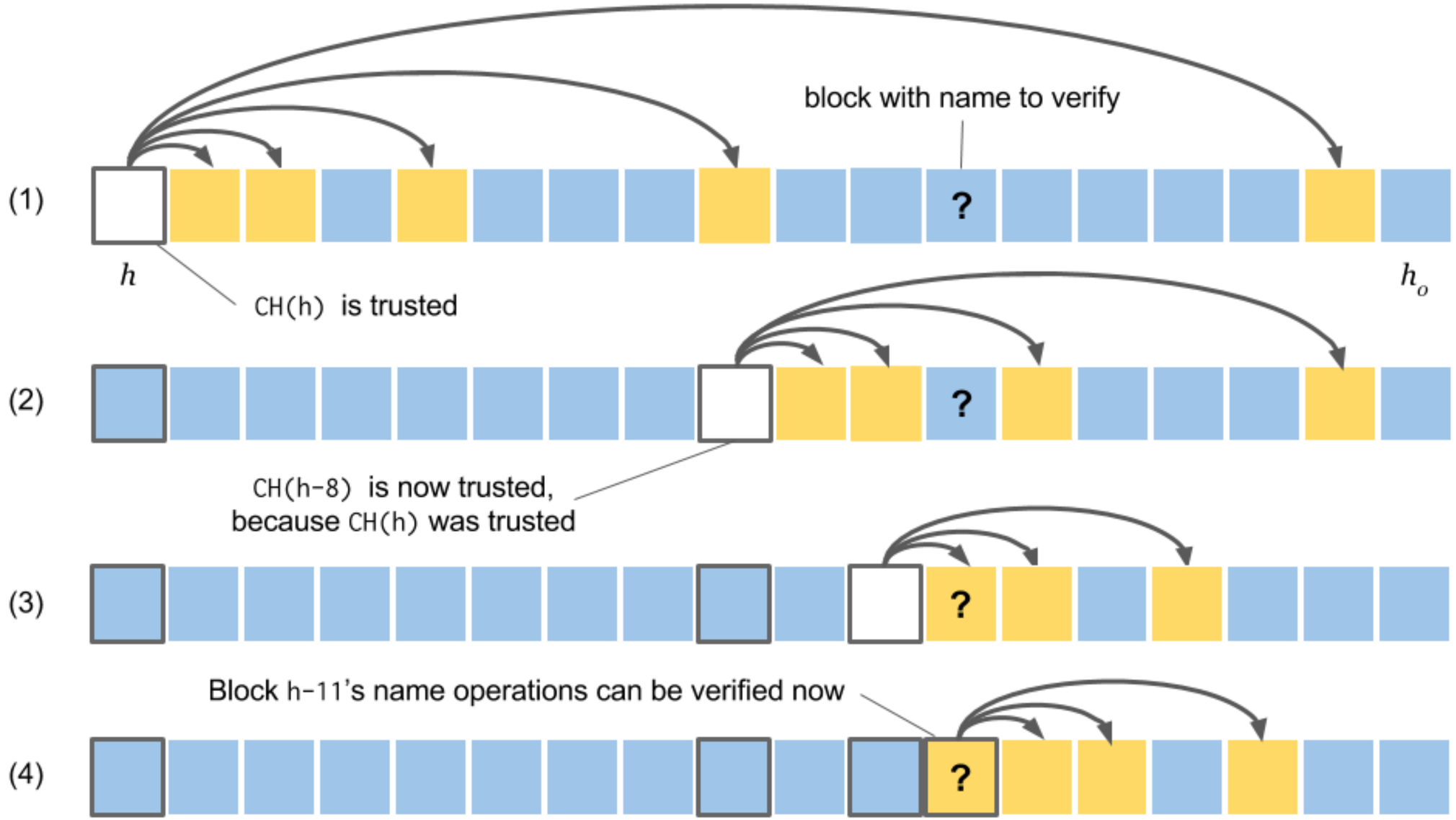


(1) Records are organized into a Merkle tree (2) whose root is fed into the consensus hash, (3) along with a geometric series of prior consensus hashes

Secure Internet

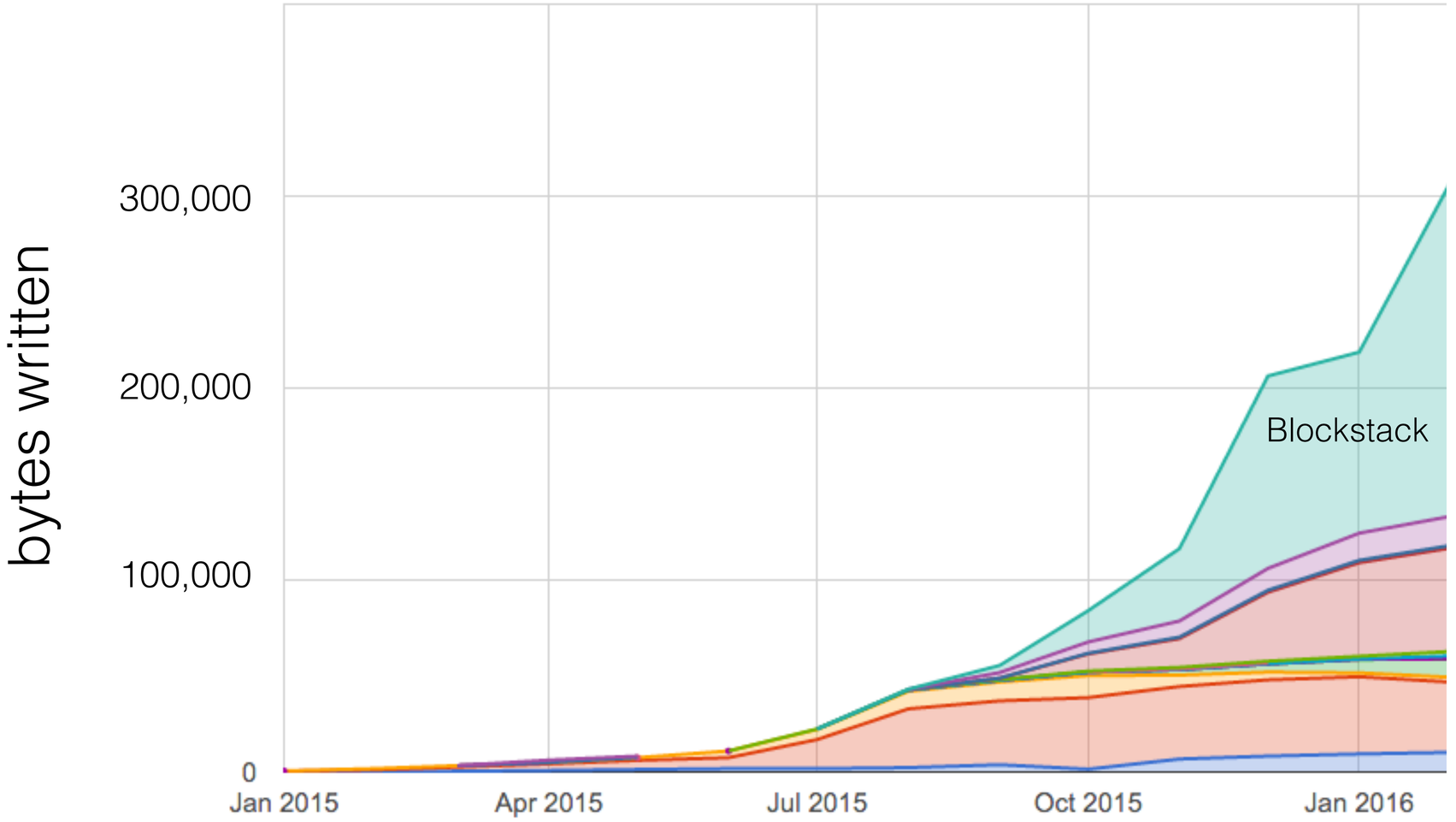
Can ask for consensus hash from friends

Light Nodes:


block with name to verify
(1)
?
h
h_o
CH(h) is trusted
(2)
?
CH(h-8) is now trusted,
because CH(h) was trusted
(3)
?
Block h-11's name operations can be verified now
(4)
?

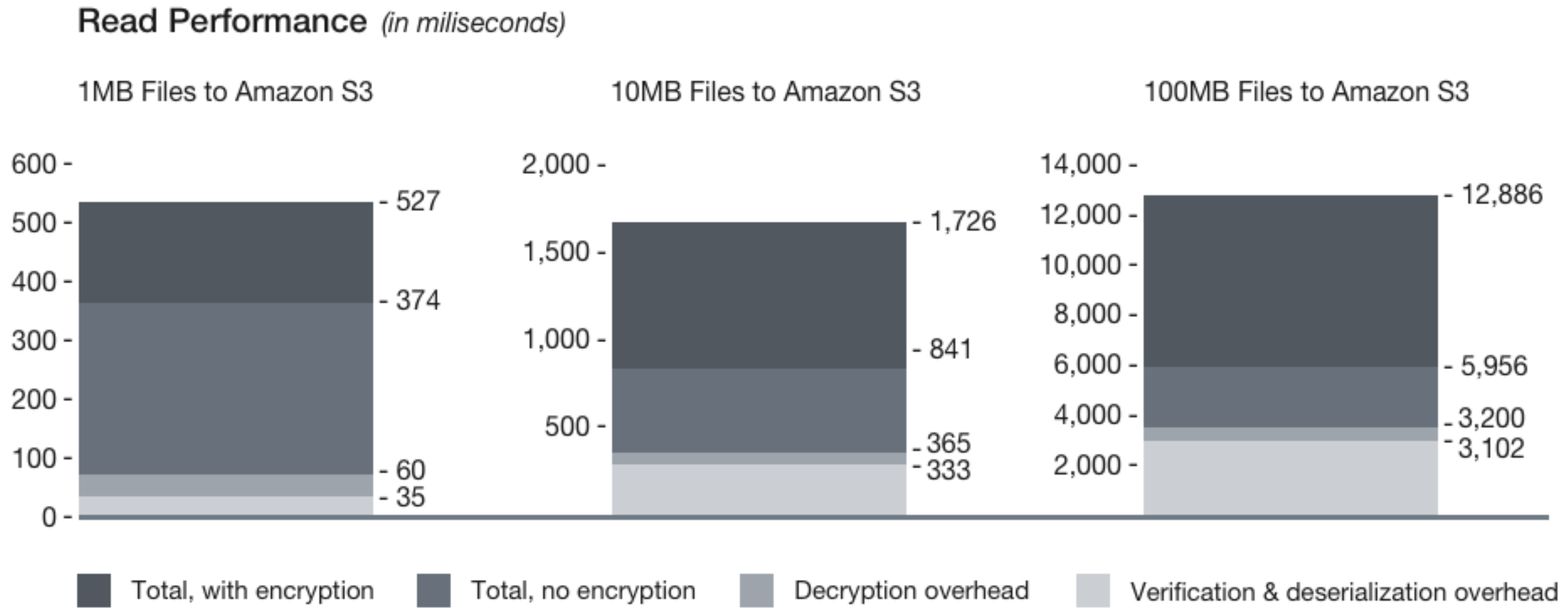
Performance

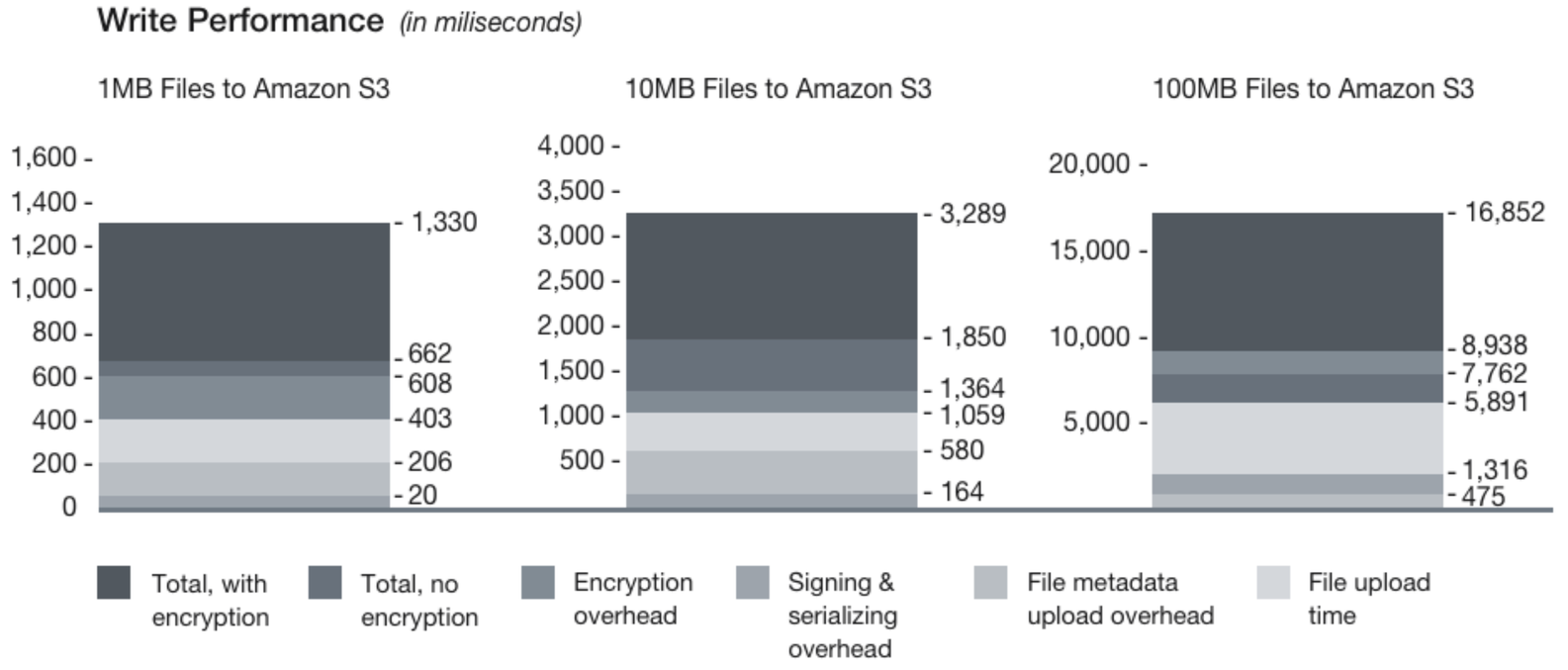
— Largest non-financial production system on Bitcoin



- Mostly network bound (~5% overhead in filesize)

- 2 secs CPU for 100MB file

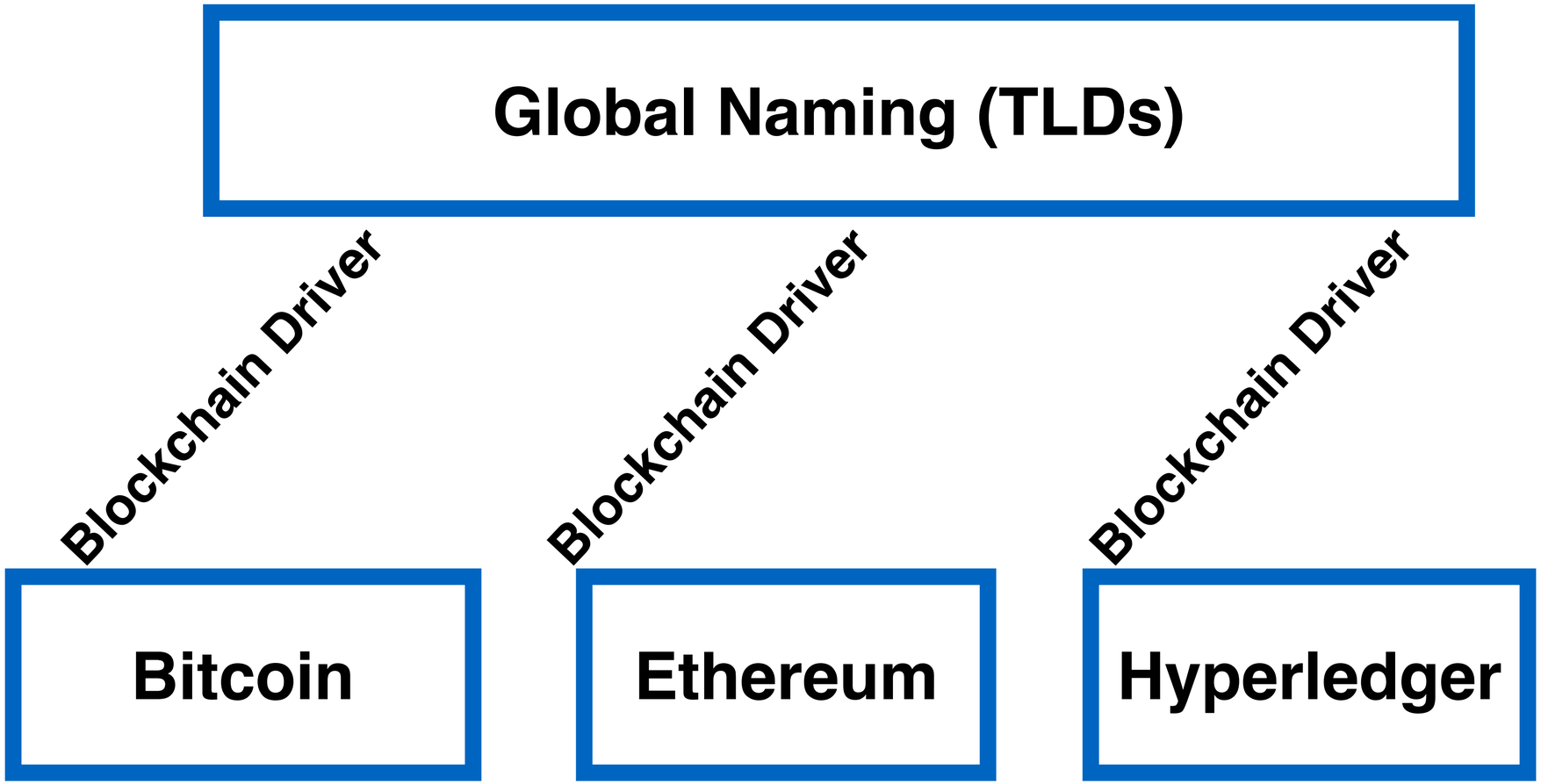




Future Work

blockstack

Scalability: Multiple Blockchains



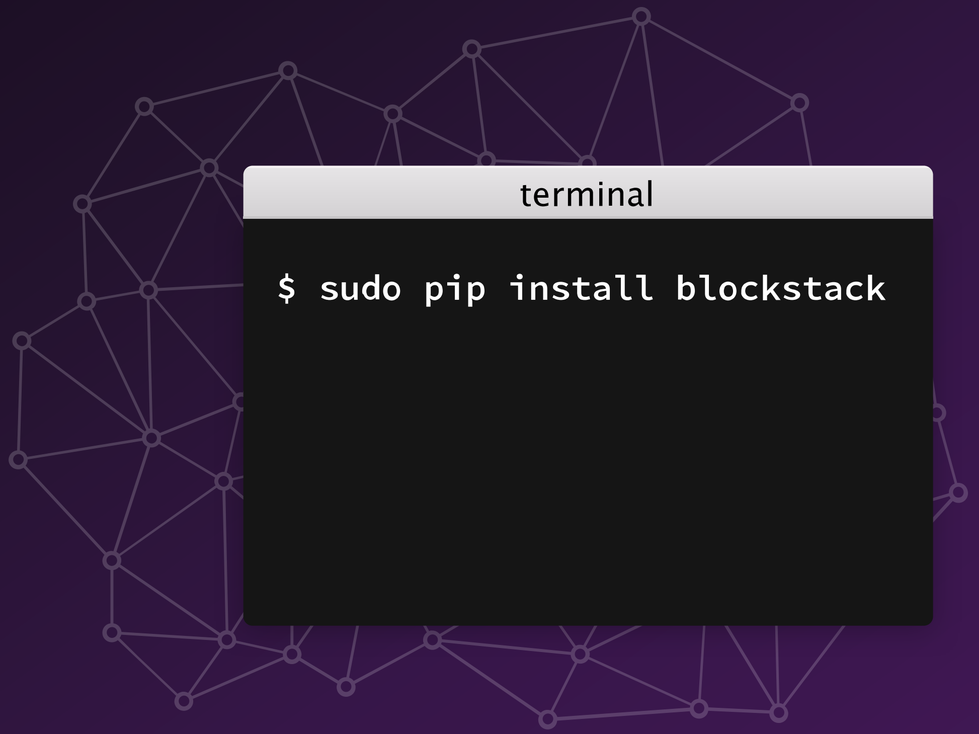
Namespaces:

#	Tentative TLD	Purpose
1	`.site`	Directing users to websites with browsers like ZeroNet, Brave and Metamask
2	`.media`	Hosted media files on systems like Mine, Ascribe, Monegraph, Verisart and Alexandria
3	`.device`	Devices on the internet of things with companies like Filament and Philips
4	`.file`	Notarized files on services like Stampery and Tierion
5	`.store`	E-commerce stores on decentralized commerce platforms like OpenBazaar and BitMarkets

blockstack

Blockstack CLI

Blockstack gives you fast, secure, and easy-to-use DNS, PKI, identity management, and custom namespaces on the blockchain



```
$ 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"
        ...
    }
}
```

+judecn

Jude Nelson

+guylepage3

Guy Lepage

+muneeb

Muneeb Ali

+ryan

Ryan Shea

Advisors

+mfreed

Mike Freedman

+jp

JP Singh

plus open-source contributors and 900+ community members

OpenBazaar

bitseed

IPFS

CONSENSYS

Microsoft

We’re hiring! Come to our BoF tonight!

Thank You!

Comments? Tweet them @muneeb, @judecnelson

Web: http://blockstack.org

Code: github.com/blockstack