Blockstack, a New Internet for Decentralized Apps

Muneeb Ali
The New Internet
Problems with the traditional internet
End-to-end design principle for the Internet.

*1981 Saltzer, Reed, and Clark paper*
End-to-end Design
Problem: Trusting DNS
In 2010, an ISP in Chile started using DNS info from Chinese (Netnod) servers.
Problem: Trusting PKI
Problem: Trusting PKI
End-to-end design principle for the Internet.
Trust-to-trust

End-to-end design principle for the Internet.

*2002-2011 Clark and Blumenthal
Trust-to-Trust Design
Problem #1: DNS & PKI are not in user trust zones
Problem: Trusting cloud services
Problems with the traditional internet

Problem #1: DNS & PKI are not in user trust zones
Problem #2: User data and apps are not in user trust zones

#1: Decentralized DNS & PKI
#2: Decentralized storage & discovery
Background on Blockchains
— It’s a file!
— Append-only global log
— Every node on the network has a consistent copy
— Private-public key pairs
— Bitcoin address deterministic from public key
— Example:

**Priv:** 4c542a0725fa39ce6a120b76a5c9f2c7627ba8b92b61e43f3e9da581ebe27636

**Pub:** 040a62c54339708998fec301ef0cf8c16a01066227b4a2f686a53bfa49473ab25abdaa48da0f36b8474d5a2aceb6b7cc39c405e98040536729694168cacf25ab92

**Bitcoin address:** 1CnrAAXA743VnVbW5LZtFrZiaZpXHUYKzg

**How Blockchains Work**
Bitcoin’s P2P Network
How Blockchains Work

Prev. block-hash → Meta-data → Transactions → SHA256

Block n → Nonce (solution) → Resulting hash → Block n+1 → Nonce

Block n+1 (in-progress) → Resulting hash → Block n+2

Nonce: 000000000000000000ec9897b4a82c526d8b7f93a0fa8f02fcc1dc5e90ae6c77
Limitations of Blockchains

1. Limited data storage & bandwidth
2. Hard to introduce new features
3. Slow writes
4. The endless ledger problem
Blockchain DNS + PKI
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:

Register hash(name)  
Update name
— Namecoin, 2011
— Blockchain Name System (BNS), 2014
— Ethereum Name Service (ENS), 2017
werner.id

Owner 1KRca8gGiCITNGR65iXMPQ6d5fssDdN3ZF

Werner Vogels
CTO @ Amazon
Seattle, WA

Summary
### Summary

<table>
<thead>
<tr>
<th></th>
<th>Value Hash</th>
<th>First Registered</th>
<th>Preordered</th>
<th>Importer</th>
<th>Import Txn</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Hash</td>
<td>3dafd5f42798df3045cd2eb70a71cccf8...</td>
<td></td>
<td>374132</td>
<td>16frc3qZU7D1pWkyL6ZYwPX5UVnWc82V</td>
<td>76a9143e2b5fdd12db7580fb4d3434b31d4fe9124bd9f088ac</td>
</tr>
<tr>
<td>Expires</td>
<td>489247</td>
<td></td>
<td>374132</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Renewed</td>
<td>374132</td>
<td></td>
<td>374132</td>
<td>16frc3qZU7D1pWkyL6ZYwPX5UVnWc82V</td>
<td>76a9143e2b5fdd12db7580fb4d3434b31d4fe9124bd9f088ac</td>
</tr>
<tr>
<td>Revoked</td>
<td>false</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Zone File

```json
{"avatar":{"url":"https://s3.amazonaws.com/kd4/werner"},"bio":"CTO @ Amazon","bitcoin":{},"cover":{"url":"https://s3.amazonaws.com/dx3/werner"},"fac..."}
```
| BLOCK #407089 | NAME_UPDATE |
| BLOCK #407080 | NAME_REGISTRATION |
| BLOCK #407074 | NAME_PREORDER |
Lessons from a production deployment
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)
Namecoin Experience

— Discovered and reported the Namecoin 51% attack vector.
— First analysis of Namecoin's network reliability (production data).
— First report on selfish mining.

See USENIX ATC’16 paper for details
Blockstack Architecture
“Security Box”

Follow David Clark’s trust-to-trust principle
Blockstack

Layered Architecture
Blockstack

Layered Architecture

name DB (local)

Zone file hash | Zone file
---|---

URI's in zone files point to stored data

Discovery Layer

Domain name | Public key | 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
Example Zone File:

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

Can ask for consensus hash from friends
Virtualchains
Virtualchains

Virtualchain

Blockchain

op_code, hash

b_{n-3}

b_{n-2}

b_{n-1}

b_n

op_code, hash

op_code, hash

op_code, hash

op_code, hash
Virtualchains: Migration

Blockchain A

Blockchain B
Blockchain Name System (BNS)
DNS vs. BNS

DNS Core Infrastructure

- DNS Root Servers
- TLD Servers .com
- TLD Servers .edu
- Authorative Server

Local DNS Server (cache)

End-user

Numbers (1-8) indicate the sequence of steps in the DNS query process.
DNS vs. BNS

DNS Core Infrastructure

- DNS Root Servers
- TLD Servers (.com)
- TLD Servers (.edu)
- Authoritative Server

DNS vs. BNS

BNS Decentralized Infrastructure

- Root Blockchain
- TLD Blockchain (.id)
- TLD Blockchain (.app)

Local DNS Server (cache)

- 1: End-user
- 2: Peer Network
- 3: Local BNS Server (cache)
- 4: Peer Network

Sync

Trust Zone
Scalability: Multiple-blockchains

- Global Naming (TLDs)
- Blockchain Driver
  - Bitcoin
  - Ethereum
  - Hyperledger
Scalability: Subdomains

— Cryptographic commit of subdomains
— Use muneeb@microsoft.site instead of muneeb.id
Peer Networks & Storage
Peer Network: Atlas

— Unstructured
— Full replication
— Targets a subset of the problem space
Decentralized Storage

- Dropbox
- Amazon S3
- Google Drive
- FreeNAS Server

Peer Network

- lookup(hash)
- lookup(URI)

Peer Node (full index)

Block N-5
Block N-4
Block N-3
Block N-2
Block N-1
Block N

(name, hash)

Storage Layer

Discovery Layer

Virtualchain Layer

(encrypted data)
Solutions for Blockchain Limitations

0) Security issues —> Need most secure blockchain (migrate)
1) Storage limitations (blockchain bloat) —> Unlimited data
2) Introducing new features (hard fork) —> Virtualchain
3) Slow writes —> Get operations off blockchain path
4) Endless ledger problem —> Fast bootstrapping
Applications and Current Impact
Blockstack Todo

Sign In With Blockstack
$ 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"
    }
}
```
Storage Performance

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

- 2 secs CPU for 100MB file

- Can give comparable performance to cloud storage
Organizations building on Blockstack range from startups to academic institutions to large enterprises.

- OpenBazaar
- Microsoft
- OpenCloud

Rushwallet

Tor (pipeline)
Decentralized Apps & App Fund

— $25 million fund to build decentralized apps

Casa  Ongaku Ryoho  OpenBazaar
Afia  Guild
There are developer meetups around the world

7,153 members
24 Meetups
plus open-source contributors and 7000+ community members
Blockstack Token
Thank you

More Info:
Website: blockstack.org
Code: github.com/blockstack

Twitter: @muneeb