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
ICANN

DNS

PKI

Authentication

Centralized User Data
Decentralized DNS + PKI
Background
## How Blockchains Work

<table>
<thead>
<tr>
<th>Name</th>
<th>Coins</th>
</tr>
</thead>
<tbody>
<tr>
<td>Muneeb Ali</td>
<td>8 coins</td>
</tr>
<tr>
<td>Brian Kernighan</td>
<td>10 coins</td>
</tr>
<tr>
<td>Paul Krugman</td>
<td>2 coins</td>
</tr>
<tr>
<td>Muneeb -&gt; Krugman</td>
<td>2 coins</td>
</tr>
<tr>
<td>Bill Gates</td>
<td>0 coins</td>
</tr>
<tr>
<td>Muneeb -&gt; Bill</td>
<td>2 coins</td>
</tr>
</tbody>
</table>
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
Verifying that +timblee is my blockchain ID. onename.com/timblee

4:50 PM - 8 Jun 2016
2015-02-28 220006 f4fa7479fc... OP_NAME_UPDATE  

2015-02-27 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 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
Network latency:

(a) CCDF of network latency (03/14 – 04/15)
(b) Network latency per new block (03/14 – 04/15)

50th percentile: 7 minutes
90th percentile: 22 minutes
99th percentile: 46 minutes
99.9th percentile: 78 minutes
Design of Blockstack
“Security Box”

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

- bitcoin node (bitcoind)
- blockstack server
- bitcoind peer connection
- rpc connection to bitcoind
Transactions are parsed as updates to the name DB.
Example Zone File:

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

1. $h$, $\text{CH}(h)$ is trusted

2. $\text{CH}(h-8)$ is now trusted, because $\text{CH}(h)$ was trusted

3. Block $h-11$’s name operations can be verified now
Performance
Largest non-financial production system on Bitcoin

- Bytes written

- Blockstack

- Graph showing growth from Jan 2015 to Jan 2016
- Mostly network bound (~5% overhead in filesize)
- 2 secs CPU for 100MB file
Future Work
Scalability: Multiple Blockchains

Global Naming (TLDs)

Blockchain Driver

Bitcoin

Blockchain Driver

Ethereum

Blockchain Driver

Hyperledger
## Namespaces:

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

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

$ sudo pip install blockstack
$ blockstack lookup fredwilson.id

You should get a response like this:

```json
{
    "data_record": {
        "name": "Fred Wilson",
        "bio": "I am a VC",
        "website": "http://avc.com"
    }
}
```
plus open-source contributors and 900+ community members
We’re hiring! Come to our BoF tonight!

Thank You!

Comments? Tweet them @muneeb, @judecnelson

Web: http://blockstack.org

Code: github.com/blockstack