Experiences with Scaling Blockchain-based Data Stores

Muneeb Ali, Co-Founder & CTO
Table of Contents

Brief Intro to Bitcoin and Blockchain
Decentralized Identity on the Blockchain
Experiences from a Production Network
Blockstore: Key-Value Store on BTC Blockchain
Experiences with Scaling Blockchain-based Data Stores
Onename. Decentralized identity on the bitcoin blockchain
Presentation at USENIX ATC 2015
Let's design a new currency…
Let's design a new currency...

<table>
<thead>
<tr>
<th>Muneeb Ali</th>
<th>10 coins</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brian Kernighan</td>
<td>10 coins</td>
</tr>
</tbody>
</table>
Ledger Currency

Let's design a new currency...

<table>
<thead>
<tr>
<th>Name</th>
<th>Coins</th>
</tr>
</thead>
<tbody>
<tr>
<td>Muneeb Ali</td>
<td>10</td>
</tr>
<tr>
<td>Brian Kernighan</td>
<td>10</td>
</tr>
<tr>
<td>Paul Krugman</td>
<td>0</td>
</tr>
</tbody>
</table>
Ledger Currency

Let's design a new currency...

<table>
<thead>
<tr>
<th>Name</th>
<th>Coins</th>
</tr>
</thead>
<tbody>
<tr>
<td>Muneeb Ali</td>
<td>10</td>
</tr>
<tr>
<td>Brian Kernighan</td>
<td>10</td>
</tr>
<tr>
<td>Paul Krugman</td>
<td>0</td>
</tr>
<tr>
<td>Muneeb —&gt; Krugman</td>
<td>2 coins (unconfirmed)</td>
</tr>
</tbody>
</table>
## Ledger Currency

Let's design a new currency…

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></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>
</tbody>
</table>

Muneeb —> Krugman 2 coins (confirmed)
Congratulations!

You just learned how Bitcoin works.
## Ledger Currency

<table>
<thead>
<tr>
<th>Name</th>
<th>Coins</th>
</tr>
</thead>
<tbody>
<tr>
<td>Muneeb Ali</td>
<td>8</td>
</tr>
<tr>
<td>Brian Kernighan</td>
<td>10</td>
</tr>
<tr>
<td>Paul Krugman</td>
<td>2</td>
</tr>
<tr>
<td>Muneeb → Krugman</td>
<td>2 coins (confirmed)</td>
</tr>
<tr>
<td>Bill Gates</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Coins</td>
</tr>
<tr>
<td>----------------</td>
<td>-------</td>
</tr>
<tr>
<td>Muneeb Ali</td>
<td>8</td>
</tr>
<tr>
<td>Brian Kernighan</td>
<td>10</td>
</tr>
<tr>
<td>Paul Krugman</td>
<td>2</td>
</tr>
<tr>
<td>Muneeb -&gt; Krugman</td>
<td>2 coins (confirmed)</td>
</tr>
<tr>
<td>Bill Gates</td>
<td>0</td>
</tr>
<tr>
<td>Muneeb -&gt; Bill</td>
<td>2 coins (unconfirmed)</td>
</tr>
</tbody>
</table>
We need a **distributed ledger** (blockchain)
Distributed Ledger

It’s a file!
It grows as you make more transactions
How Blockchain Works

• Private-public key pairs

```python
>>> from pybitcoin import BitcoinPrivateKey
>>> priv = BitcoinPrivateKey()
>>> priv.to_hex()
'91149ee24f1ee9a6f42c3dd64c2287781c8c57a6e8e929c80976e586d5322a3d'
```
How Blockchain Works

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

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

>>> pub.address()
'13mtgVARiB1HiRyCHnKTi6rEwyje5TYKBW'
```
How Blockchain Works

- 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 Blockchain Works

Alice’s transfer to Bob
FROM
TO

Transactions

PUBLIC
LEDGER
How Blockchain Works
How Blockchain Works

1  2  3  

Register hash(name)

…..  

3000  

Update name
Decentralized Identity: Onename
Decentralized Identity: Onename

**Name u/naval**

<table>
<thead>
<tr>
<th>Summary</th>
<th>Current value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Active</td>
</tr>
<tr>
<td>Expires after block</td>
<td>253461 (27772 blocks to go)</td>
</tr>
<tr>
<td>Last update</td>
<td>2015-02-09 23:11:58 (block 217461)</td>
</tr>
<tr>
<td>Registered since</td>
<td>2014-02-24 14:49:58 (block 164024)</td>
</tr>
</tbody>
</table>

```json
{
   "website": "https://angel.co/naval",
   "bio": "Co-founder Angellist \u2022 Founder Epinions, Vast \u2022 Author Startupboy, Venture Hacks \u2022 Investor Twitter, Uber, Yammer, Postmates",
   "github": {
      "username": "navalr",
      "proof": {
         "url": "https://gist.github.com/navalr/f31a74054f059ec0ac6a"
      }
   },
   "name": {
      "formatted": "Naval Ravikant"
   },
   "graph": {
      "url": "https://s3.amazonaws.com/ghp/naval"
   },
   "next": "i/naval-1"
}
```
Decentralized Identity: Onename

<table>
<thead>
<tr>
<th>Date</th>
<th>Id</th>
<th>OP_NAME_UPDATE</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-03-17</td>
<td>167336</td>
<td>b87f45971c5...</td>
<td>{&quot;website&quot;: &quot;<a href="https://angel.co/napal">https://angel.co/napal</a>&quot;, &quot;bio&quot;: &quot;Co-founder Angellist \u2022 Founder Opinions, Vast \u2022 Author Startupbox, Venture Hacks \u2022 Investor Twitter, Uber, Yammer, Postmates&quot;, &quot;name&quot;: &quot;Naval Ravikant&quot;, &quot;twitter&quot;: &quot;:@nalal&quot;, &quot;cover&quot;: &quot;<a href="https://pbs.twimg.com/profile_banners/745273/1355705777/web_retina">https://pbs.twimg.com/profile_banners/745273/1355705777/web_retina</a>&quot;, &quot;bitcoin&quot;: &quot;1H5KP4ro7Crx1w5FrenchL1n3ANnJn15hN&quot;, &quot;next&quot;: &quot;i/napal-1&quot;}</td>
</tr>
<tr>
<td>2014-02-24</td>
<td>164024</td>
<td>c117d03e48...</td>
<td>{&quot;status&quot;: &quot;reserved&quot;, &quot;message&quot;: &quot;This OnName username is reserved for Naval Ravikant. If this is you, please email <a href="mailto:reservations@onname.io">reservations@onname.io</a> to claim it for free.&quot;}</td>
</tr>
<tr>
<td>2014-02-24</td>
<td>163976</td>
<td>669989702b...</td>
<td>24b1d3a13ef250fc37184b8d0e89b714f483dfa4</td>
</tr>
</tbody>
</table>
Lessons from Namecoin

- Reliability and security of the blockchain
- Limit on size of data (520 bytes)
- Software engineering challenges
- Scalability challenges
Experiences with Scaling Blockchain-based Data Stores

Onename. Decentralized identity on the bitcoin blockchain

Presentation at USENIX ATC 2015

Blockstore

Blockstore

Virtual Blockchain

Mirror1

DHT

Mirror2

Bitcoin Blockchain

name_op, hash
name_op, hash
name_op, hash
name_op, hash
name_op, hash
name_op, hash
Experiences with Scaling Blockchain-based Data Stores

Onename. Decentralized identity on the bitcoin blockchain

Presentation at USENIX ATC 2015
Blockstore

- Opensource (python), simpler (no blockchain functionality)
- Can support multiple data stores (mirrors)
- Separates control plane from data plane
- Enables to experiment with namespaces / spamming / pricing
Experiences with Scaling Blockchain-based Data Stores

Onename. Decentralized identity on the bitcoin blockchain

Presentation at USENIX ATC 2015
Experiences with Scaling Blockchain-based Data Stores

Onename. Decentralized identity on the bitcoin blockchain

Presentation at USENIX ATC 2015

Question?

Thank You!
muneeb@onename.com
@muneeb

More information:

Community: blockstack.org
Code: github.com/blockstack