onename

Experiences with Scaling Blockchain-based Data Stores

Muneeb Ali, *Co-Founder & CTO*

Table of Contents

Bitcoin

Ledger Currency

Let’s design a new currency…

Ledger Currency

Let’s design a new currency…

Muneeb Ali	10 coins
Brian Kernighan	10 coins

Ledger Currency

Let’s design a new currency…

Muneeb Ali	10 coins
Brian Kernighan	10 coins
Paul Krugman	0 coins

Ledger Currency

Let’s design a new currency…

Muneeb Ali	10 coins
Brian Kernighan	10 coins
Paul Krugman	0 coins
Muneeb —> Krugman 2 coins (unconfirmed)	

Ledger Currency

Let’s design a new currency…

Muneeb Ali	8 coins
Brian Kernighan	10 coins
Paul Krugman	2 coins
Muneeb —> Krugman 2 coins (confirmed)	

Congratulations!

You just learned how Bitcoin works.

Ledger Currency

Muneeb Ali	8 coins
Brian Kernighan	10 coins
Paul Krugman	2 coins
Muneeb —> Krugman 2 coins (confirmed)	
Bill Gates	0 coins

Ledger Currency

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)	

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

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

How Blockchain Works

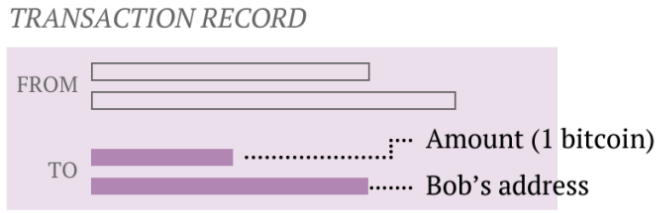
- Private-public key pairs
- Bitcoin address = deterministic from pubkey

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

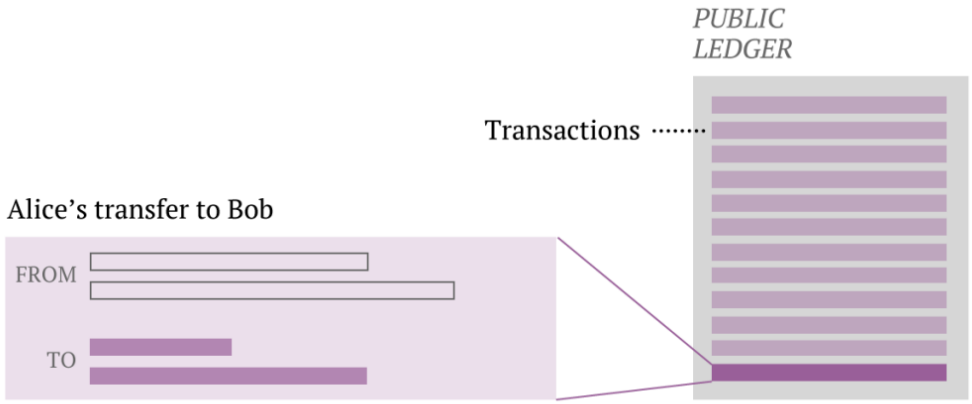
```
>>> pub.address()
'13mtgVARiB1HiRyCHnKTi6rEwyje5TYKBW'
```

How Blockchain Works

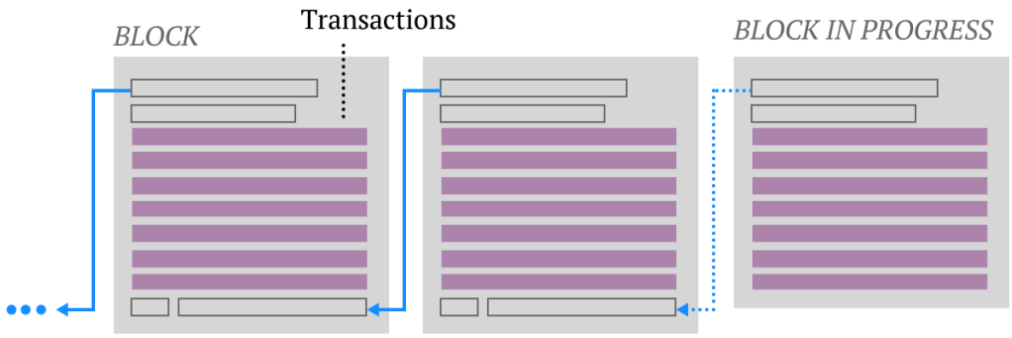
- No such thing as a “bitcoin”. Only inputs and outputs
- 21 million total bitcoins (fixed)
- 50 BTC minted each block, halved to 25 BTC



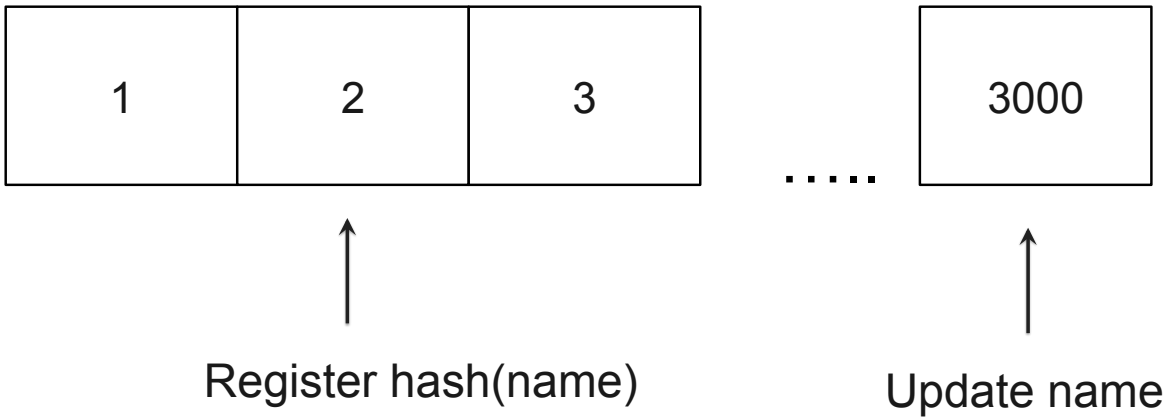
How Blockchain Works



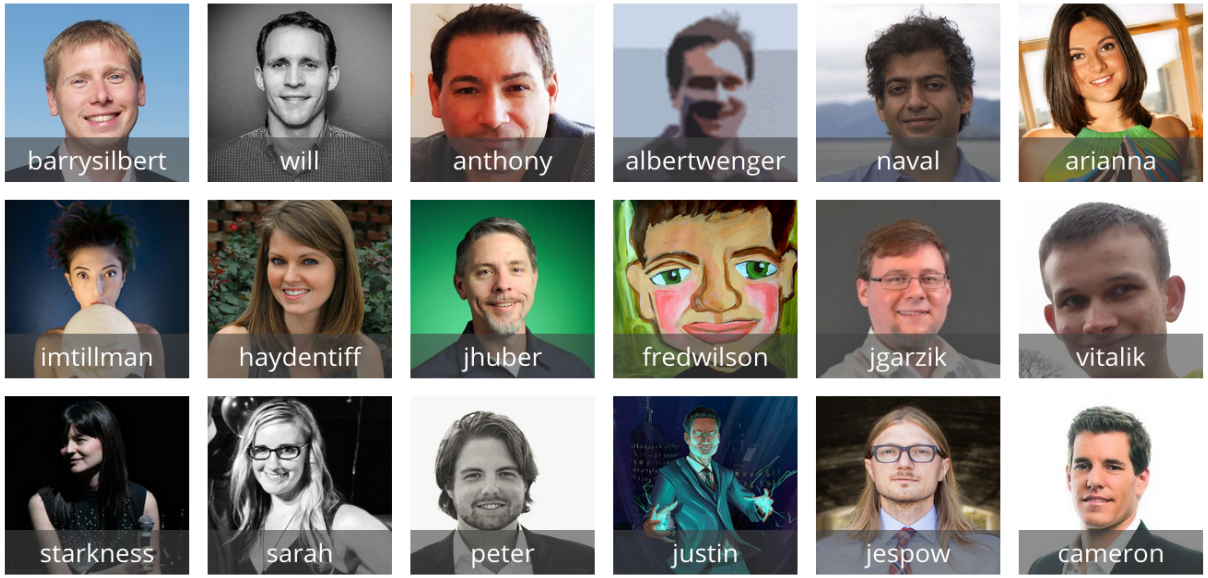
How Blockchain Works



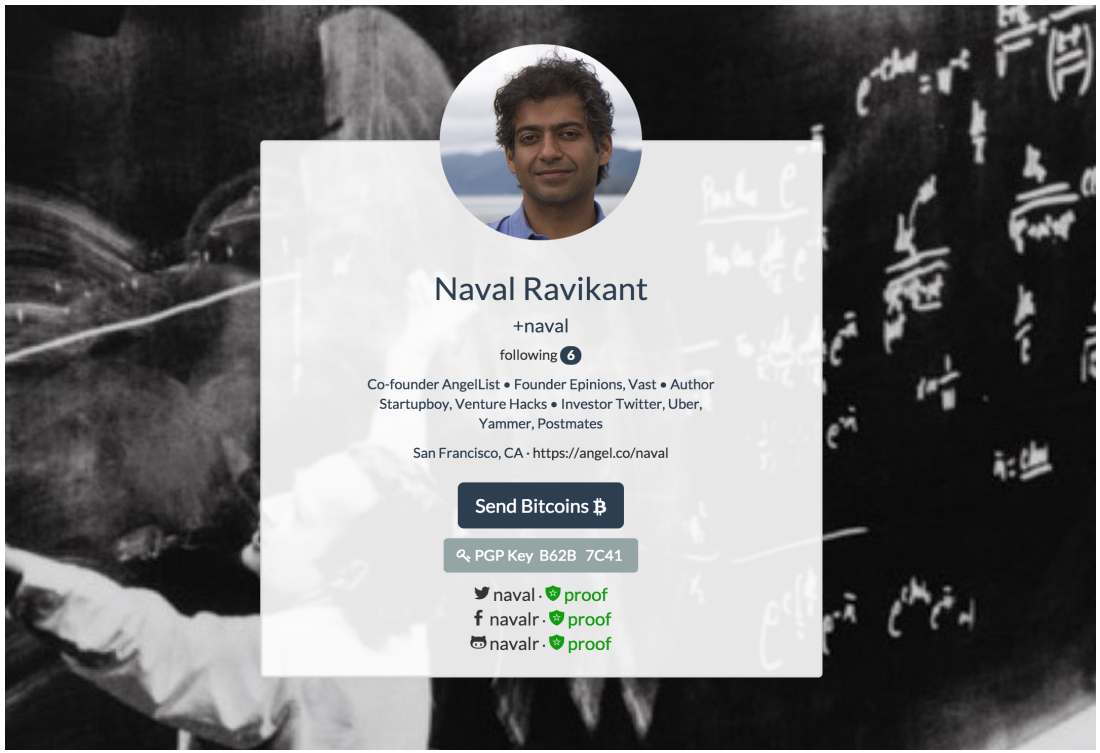
How Blockchain Works



Decentralized Identity: Onename



Decentralized Identity: Onename



Decentralized Identity: Onename

Name u/naval

Summary

Status	Active
Expires after block	253461 (27772 blocks to go)
Last update	2015-02-09 23:11:58 (block 217461)
Registered since	2014-02-24 14:49:58 (block 164024)

Current value


```
{
    "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/f31a74054f85
9ec0ac6a"
        }
    },
    "name": {
        "formatted": "Naval Ravikant"
    },
    "graph": {
        "url": "https://s3.amazonaws.com/grph/naval"
    },
    "next": "i/naval-1"
}
```

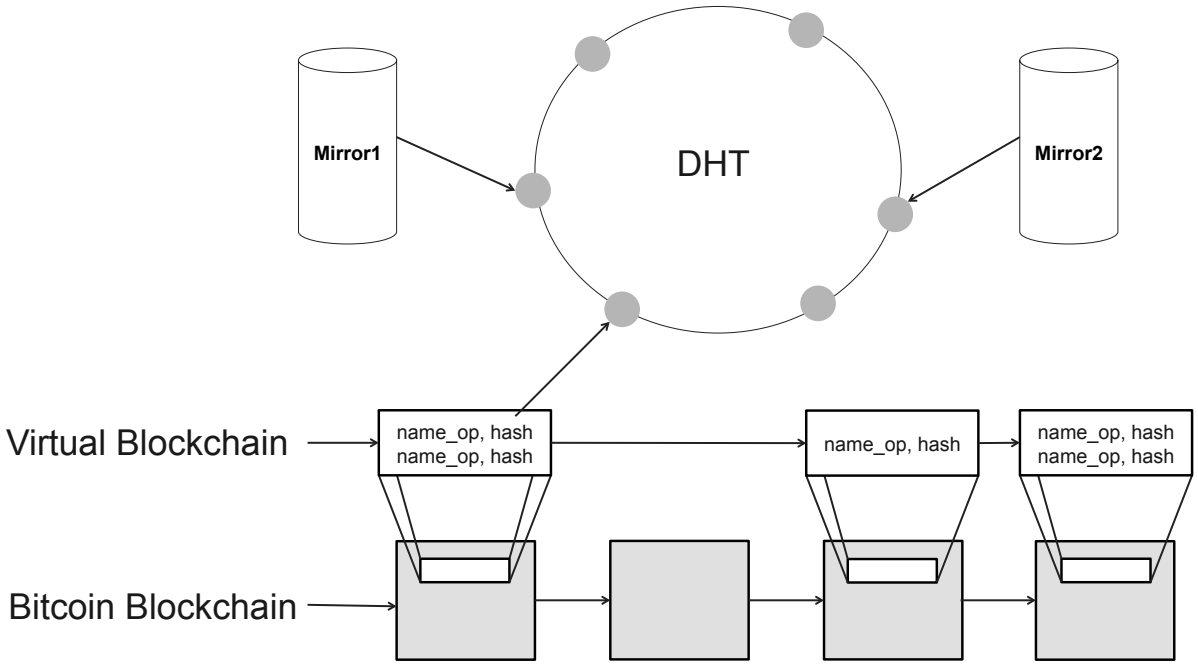
Decentralized Identity: Onename

2014-03-17 18:42:29	167336	b87f45971c...	OP_NAME_UPDATE	{"website": "https://angel.co/naval", "bio": "Co-founder AngelList \u2022 Founder Epinions, Vast \u2022 Author Startupboy, Venture Hacks \u2022 Investor Twitter, Uber, Yammer, Postmates", "name": {"formatted": "Naval Ravikant"}, "twitter": {"username": "naval"}, "cover": {"url": "https://pbs.twimg.com/profile_banners/745273/1355705777/web_retina"}, "bitcoin": {"address": "1HSKP4ro7Crx1wf5GYpyrL1n3ANnJn15hN"}, "next": "i/naval-1"}
2014-02-24 14:49:58	164024	c117d03e48...	OP_NAME_FIRSTUPDATE	{"status": "reserved", "message": "This OneName username is reserved for Naval Ravikant. If this is you, please email reservations@onename.io to claim it for free."}
2014-02-24 08:07:54	163976	669989702b...	OP_NAME_NEW	24b1d3a13ef250fc37184b8d0e89b714f483dfa4

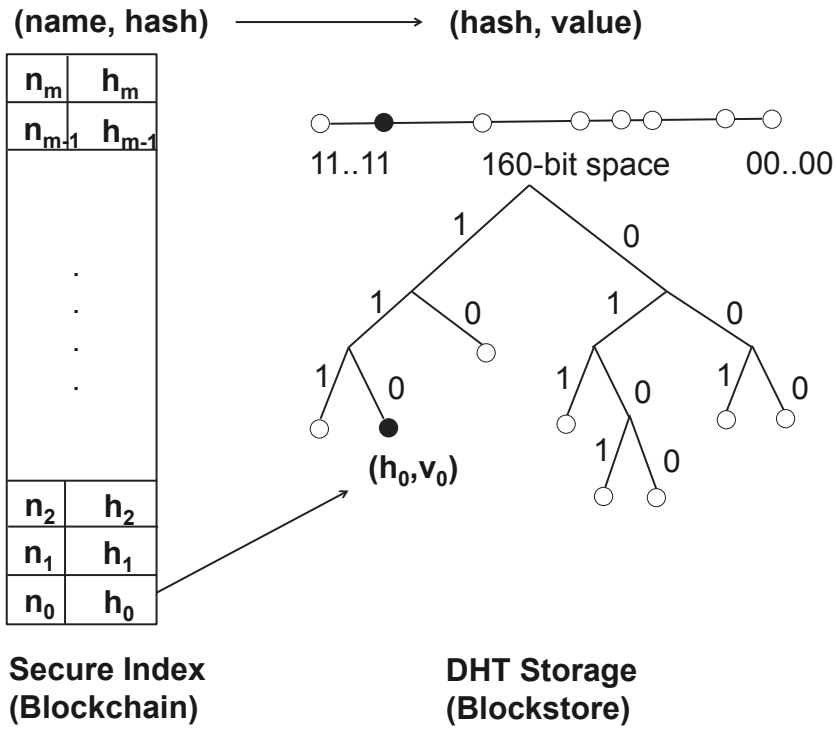
Lessons from Namecoin

- Reliability and security of the blockchain
- Limit on size of data (520 bytes)
- Software engineering challenges
- Scalability challenges

Blockstore


Mirror1
DHT
Mirror2
Virtual Blockchain
name_op, hash
name_op, hash
name_op, hash
name_op, hash
name_op, hash
Bitcoin Blockchain

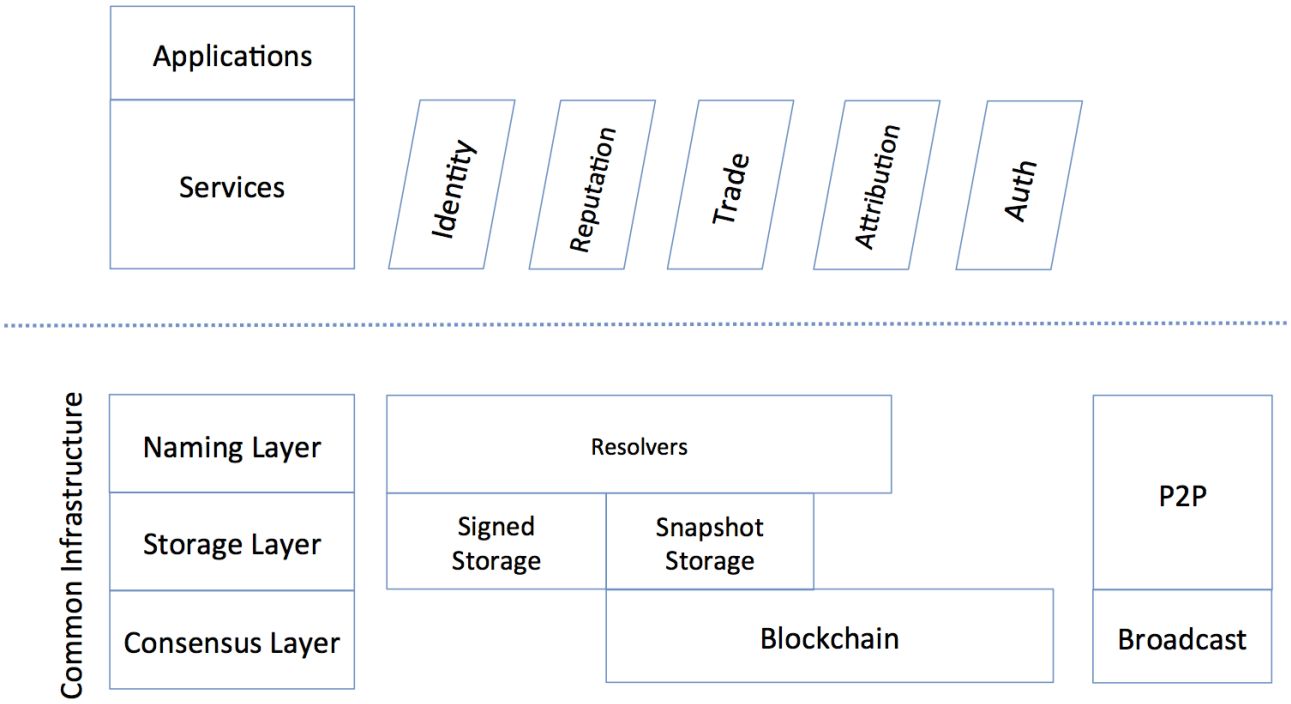
Blockstore


(name, hash)
(hash, value)
n_m h_m
n_{m-1} h_{m-1}
n_2 h_2
n_1 h_1
n_0 h_0
11..11
160-bit space
00..00
(h_0,v_0)
Secure Index
(Blockchain)
DHT Storage
(Blockstore)

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

Blockstack: Common Infrastructure for Blockchain Apps



Question?

Thank You!

muneeb@onename.com

@muneeb

More information:

Community: blockstack.org

Code: github.com/blockstack