BLOCKSTACK BERLIN

A SIGNATURE FUND EVENT

Subdomains: Scalable User Registration

By Jude Nelson

BLOCKSTACK

Requirements for Usernames

Globally unique

Human-friendly

Strongly owned

Inexpensive to acquire

Instantly usable

Requirements for Usernames

	Facebook	PGP	Blockstack	**Subdomains**
Globally unique	X	X	X	**X**
Human-friendly	X		X	**X**
Strongly owned		X	X	**X**
Inexpensive	X	X		**X**
Instantly usable	X	X		**X (soon!)**

Limits of On-chain Usernames

Limited Throughput

- Capped by blockchain
- Need all chain state

} Max ~72K name registrations per day

Misaligned Incentives

- Squatters lock up names, drive up name prices
- Blockchain speculators drive up transaction prices

True for all blockchain naming systems

Subdomains: Off-chain Usernames

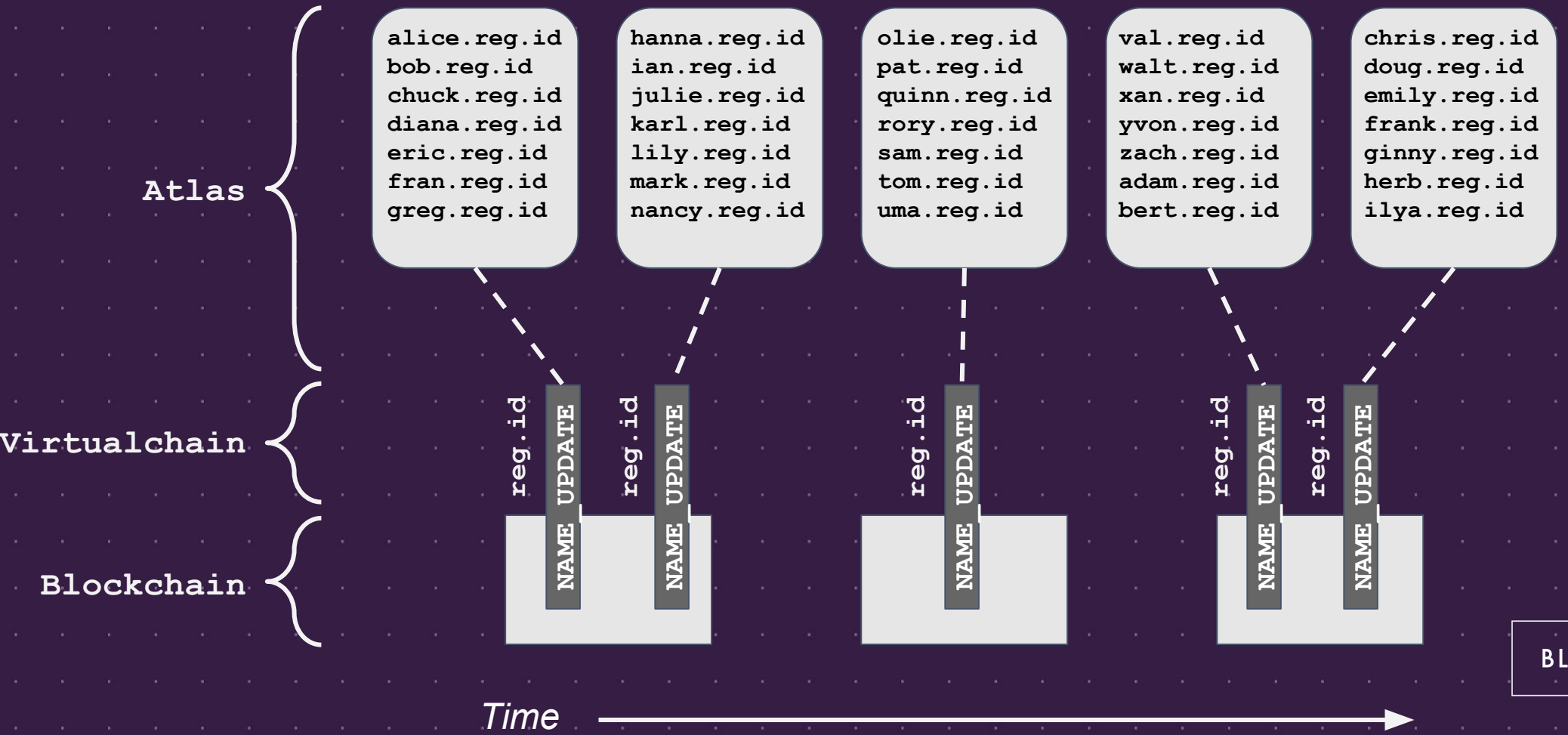
1 blockchain tx == 100's of subdomains

- Decouple *name* throughput from *chain* throughput
- Decouple *name* state replication from *chain* state replication

Fixes Incentives

- Name owners compete to register subdomains
- Dedicated storage space for name state

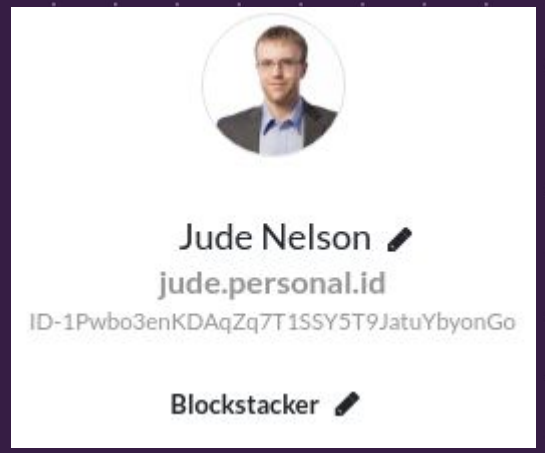
How Subdomains Work



Subdomains are embedded in Atlas zone files for `reg.id`

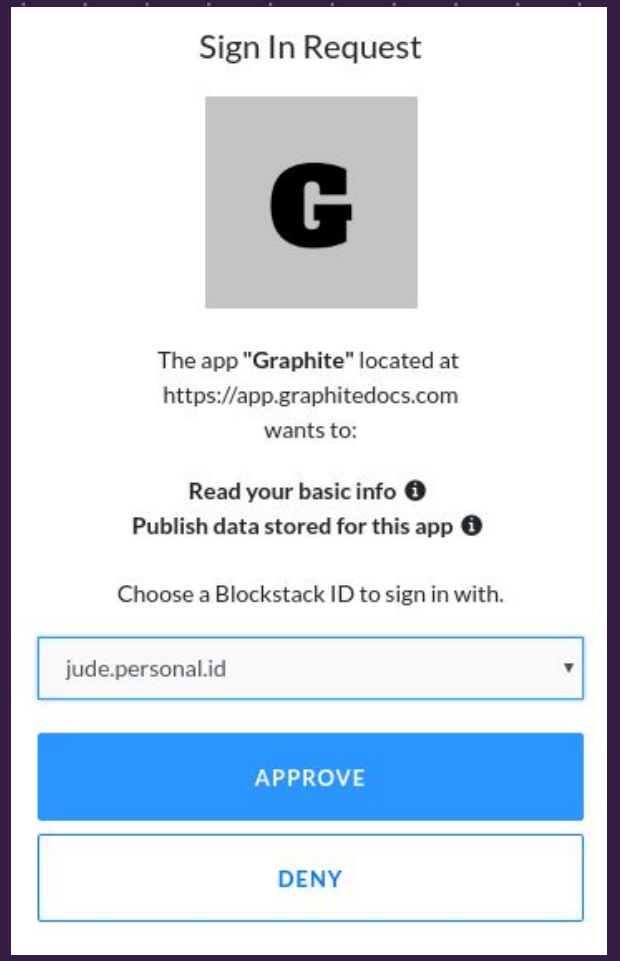
BLOCKSTACK BERLIN
A SIGNATURE FUND EVENT

Subdomains are First-class Usernames



Subdomains have profiles

You can use apps with subdomains



BLOCKSTACK BERLIN
A SIGNATURE FUND EVENT

Subdomains are First-class Usernames

```
$ curl https://core.blockstack.org/v1/names/jude.personal.id
{
  "address": "1Pwbo3enKDAqZq7T1SSY5T9JatuYbyonGo",
  "blockchain": "bitcoin",
  "last_txid": "8b383b2e27a573b9d6205af677682cddf2d736bfdb8e56dfab0eefefc0c846eb",
  "status": "registered_subdomain",
  "zonefile_hash": "16ebbb1cadb18a90deb8f1a6beb22e42ffef19d6",
  "zonefile_txt": "$ORIGIN jude.personal.id\n$TTL 3600\n_https._tcp URI 10 1
\"https://gaia.blockstack.org/hub/1Pwbo3enKDAqZq7T1SSY5T9JatuYbyonGo/profile.json\"
\n"
}
```

BLOCKSTACK BERLIN

A SIGNATURE FUND EVENT

Subdomains are First-class Usernames

```
$ curl https://core.blockstack.org/v1/users/jude.personal.id
{
  "jude.personal.id": {
    "owner_address": "1Pwbo3enKDAqZq7T1SSY5T9JatuYbyonGo",
    "profile": {
      "@context": "http://schema.org",
      "@type": "Person",
      "description": "Blockstacker",
      "image": [
        {
          "@type": "ImageObject",
          "contentUrl": "https://gaia.blockstack.org/hub/1Pwbo3enKDAqZq7T1SSY5T9JatuYbyonGo//avatar-0",
          "name": "avatar"
        }
      ],
      "name": "Jude Nelson"
    },
    "public_key": "02d4afde4d4085c94e387d5df1ce48ee58685aa38da5eb4177487788fe1fa47b94",
    "verifications": [],
    "zone_file": {
      "$origin": "jude.personal.id",
      "$ttl": 3600,
      "uri": [
        {
          "name": "_https._tcp",
          "priority": 10,
          "target": "https://gaia.blockstack.org/hub/1Pwbo3enKDAqZq7T1SSY5T9JatuYbyonGo/profile.json",
          "weight": 1
        }
      ]
    }
  }
}
```

BLOCKSTACK BERLIN

A SIGNATURE FUND EVENT

Subdomain Registrars

Any name owner can run a subdomain registrar

- Public registrars (like `personal.id`)
- App- and org-specific registrars

User signs / Name owner propagates

- All subdomain state is stored in Atlas
- User does not need to spend Bitcoin

Subdomain Transactions

Encoded as a sequence of `TXT` records

- Fully-replicated, totally-ordered tx history (in Atlas)
- Have their own zone files within their `TXT` record

Subdomain transaction types

- **`CREATE`**: no signature, sets **`owner`**
- **`UPDATE`**: signed by prev. **`owner`**, sets new **`zf[0-9]`**
- **`TRANSFER`**: signed by prev. **`owner`**, sets new **`owner`**

Subdomain Transaction Anatomy

Name, Address, Sequence number, Zone file, [Signature]

```
$ORIGIN personal.id
$TTL 3600
jude IN TXT "owner=1Pwbo3enKDAqZq7T1SSY5T9JatuYbyonGo"
"seqn=0" "parts=1" "zf0=JE9SSUdJTiBqdWRlLnBlcnNvbmFsLmlkCiRUV
EwgMzYwMApfaHR0cHMuX3RjcCBVUkkgMTAgMSAiaHR0cHM6Ly9nYWlhLmJsb2
Nrc3RhY2sub3JnL2h1Yi8xUHdibzNlbktEQXFacTdUMVNTWTVUOUphdHVZYnl
vbkdvL3Byb2ZpbGUuanNvbiIK"
```

Subdomain Caveats

Need a registrar's cooperation

- Registrar must replicate *all* zone files

`CREATE`, `TRANSFER` txs *must* be sent by same registrar

- Only `personal.id` can propagate these for `jude.personal.id`
- Prevents subdomain ownership history reorgs
  - If we did not do this, name owners could steal subdomains

Subdomains never expire

Subdomain Cost and Bandwidth

~120 subdomain transactions per `NAME_UPDATE`

- Atlas zone files are 40kb in Blockstack Core 0.18
- `NAME_UPDATE`s are ~425 bytes

8 `NAME_UPDATE`s/block (3,4%) == 138K subdomains/day

- About the same rate as Twitter sign-ups

At 20 sat/byte, €8K/BTC, a subdomain costs €0,005

WIP: Instantaneous Subdomains (#750)

Subdomain registrars resolve unconfirmed subdomains

- Users can use apps without having to wait!
- Subdomains eventually confirm and replicate with Atlas

Users get a signed ticket for their subdomain

- Creates audit history to detect bad registrar behavior

Summary

Subdomains are usernames that:

- Are globally unique, strongly owned, and human-friendly
- Are cheap and instantly usable
- Do not require the user to have Bitcoin (or any token)
- Never expire

Subdomains have first-class support in Blockstack

Further Reading

Blockstack Naming Service

- blockstack-core/docs/blockstack_naming_service.md

Atlas Peer-to-Peer Network

- blockstack-core/docs/atlas_network.md

Running a Subdomain Registrar

- blockstack-core/docs/subdomains.md