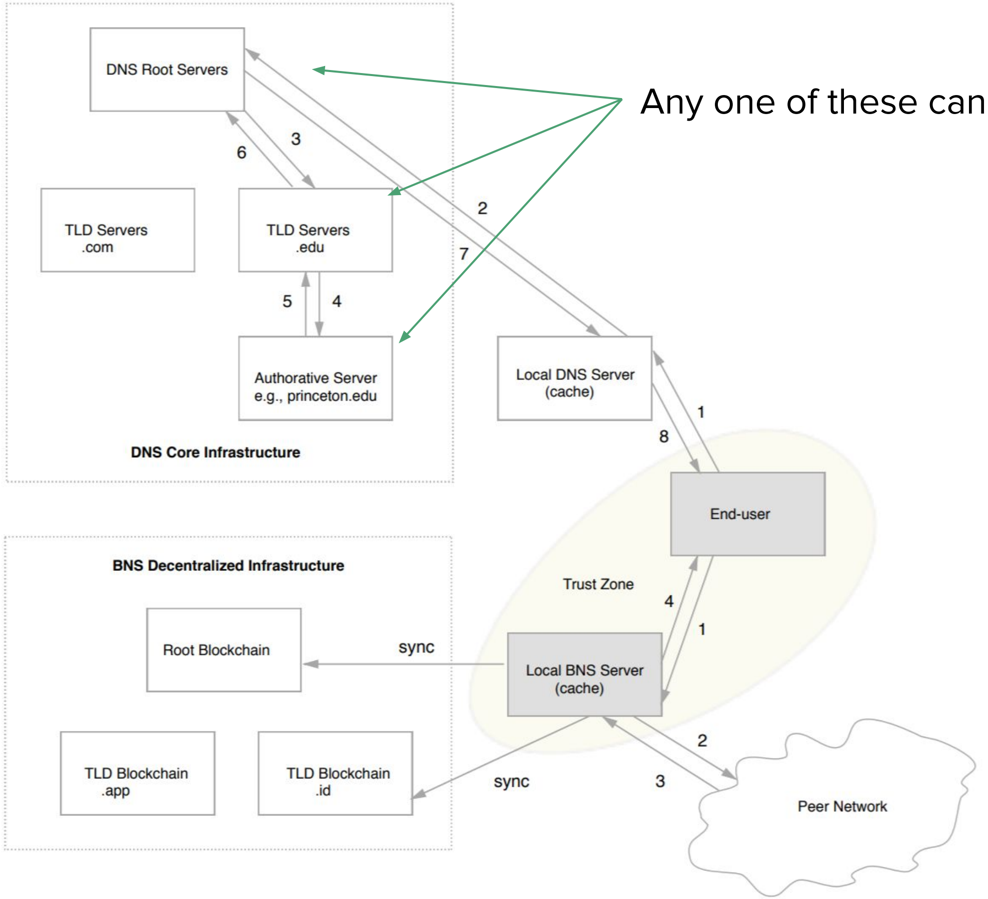
BlockStack

Revolutionary Technology or Flashy Gimmick?

Hyun Choi (hchoi26)

Background

- Traditional DNS is highly centralized and is vulnerable to attacks
- Blockstack aims to decentralize the Internet with the following goals:
    - Decentralized naming & discovery
    - Decentralized storage
    - Comparable performance
- Traditional webapps ➜ no way to verify if your data is secured, or deleted when you request it to be deleted
- Decentralization allows for users to take control of their own data
- Requires a way to verify (without trusting any one entity) the legitimacy and integrity of the data provided



Any one of these can be compromised

Figure 2: *A recursive DNS query (top) and an iterative BNS query.*

Short Intro to Blockchain

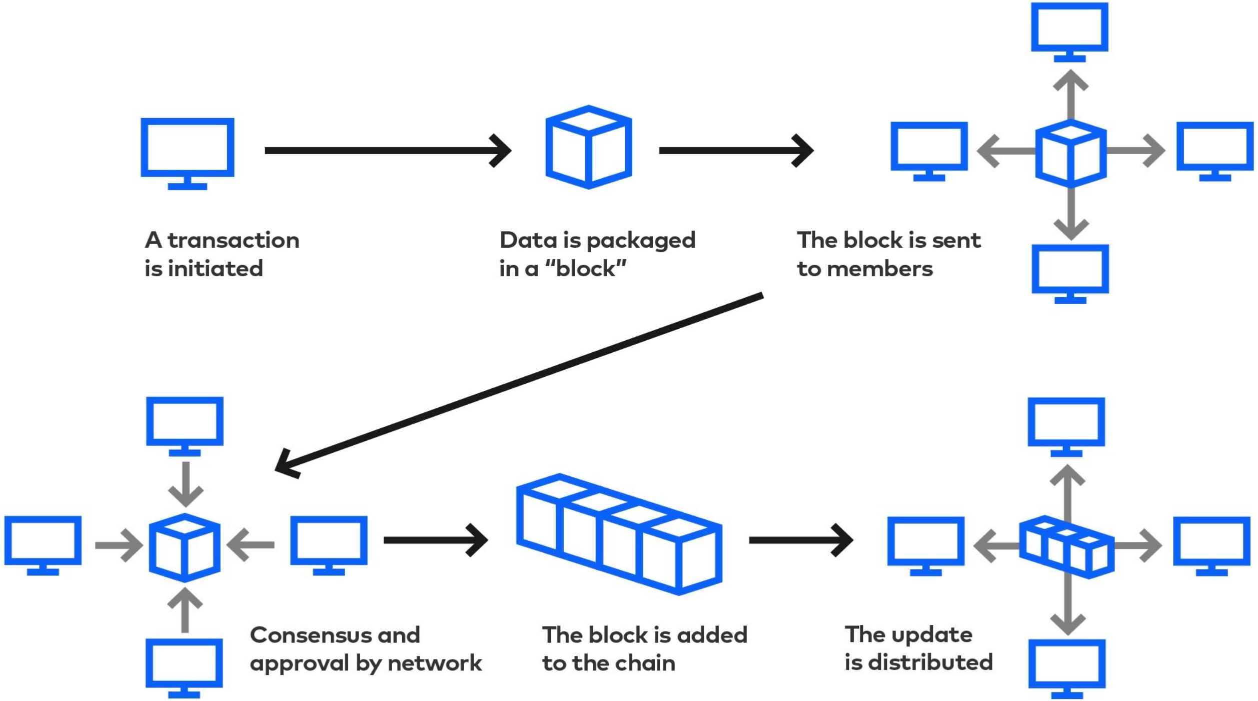
The Bitcoin Blockchain

- A blockchain is essentially a distributed, decentralized linked list of records
- Each record (block) can contain main transactions, in the case of Bitcoin
- Each node participating in the blockchain has a complete archive of every single block in the blockchain

The Bitcoin Blockchain

- Adding blocks to the Bitcoin blockchain requires “proof-of-work”
  - Essentially, a “miner” computer must solve a computationally intensive math problem that is based on the current chain of blocks
  - If they solve it before anyone else, they get to add a block to the blockchain, receive a reward (currently 6.25 BTC = US$66,931.88), and everyone starts all over again to “mine” a block
- Each transaction must be accompanied by a “transaction fee” to the miners to incentivize including your transaction in the block they are mining
- This structure allows users to trust that the blockchain has not been tampered with, without having to trust any one person.

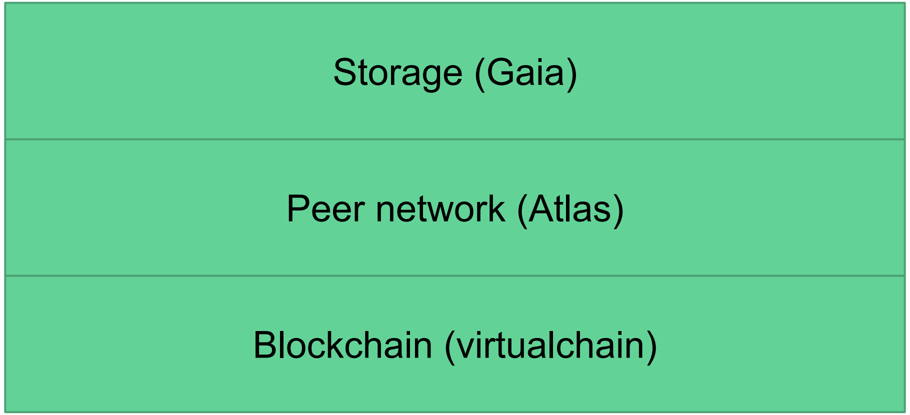
Blockchain questions?



Source: slalom.com

Structure of Blockstack

The Layers of Blockstack

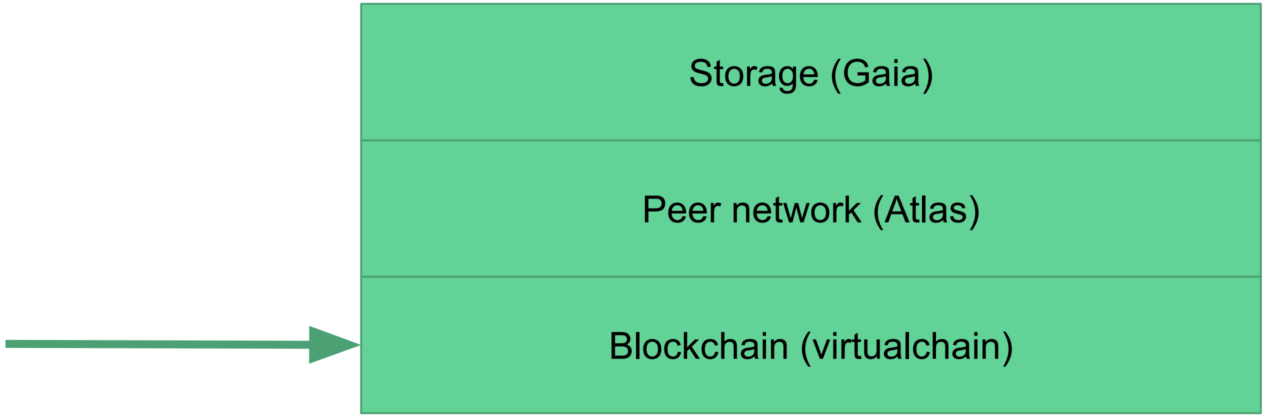


Storage (Gaia)

Peer network (Atlas)

Blockchain (virtualchain)

The Layers of Blockstack



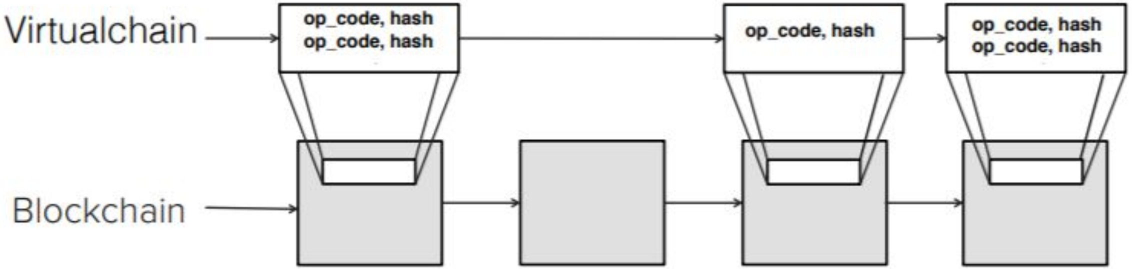
Storage (Gaia)

Peer network (Atlas)

Blockchain (virtualchain)

Virtualchains

- Blockchains offer a “totally-ordered, tamper-resistant log of state transitions”
- A traditional blockchain does not have enough bandwidth to handle the storage requirements of most applications
- Solution ➔ separate the data storage from the blockchain, and store the hashes of data instead



But what if the blockchain itself is compromised?

But what if the blockchain itself is compromised?

- Cross-chain migration!
- Blockstack actually migrated from Namecoin to Bitcoin because Namecoin was less secure due to its smaller size
- Underlying blockchain with higher computational power backing it is required

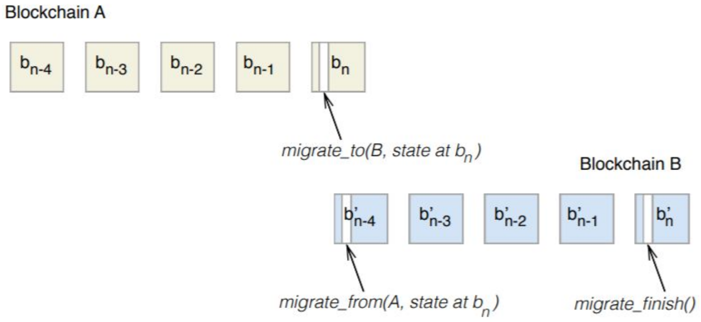
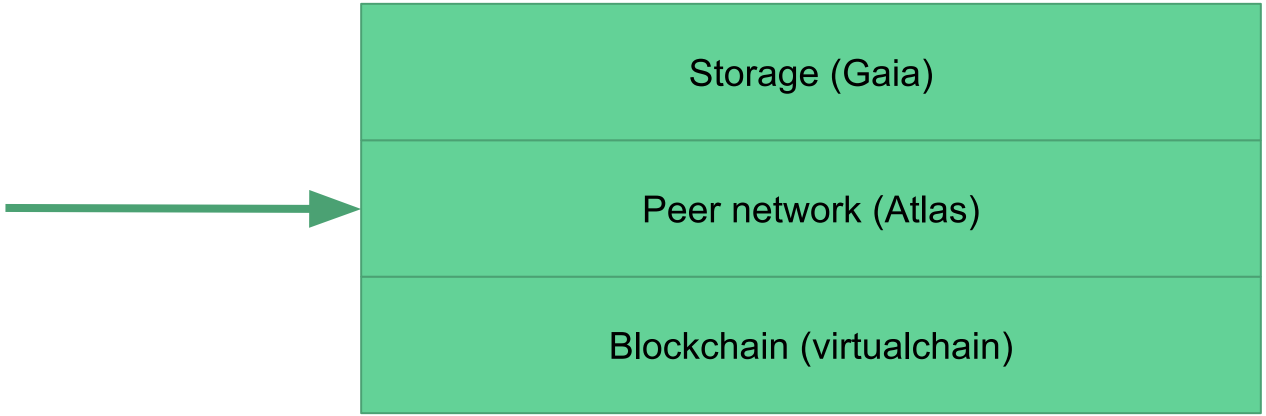


Figure 6: A framework for migrating from blockchain A to blockchain B.

The Layers of Blockstack



Storage (Gaia)

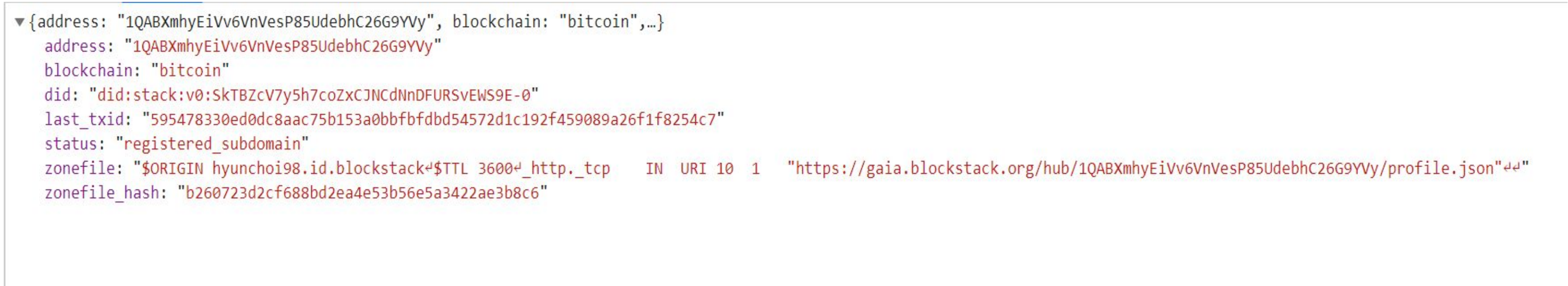
Peer network (Atlas)

Blockchain (virtualchain)

Atlas Network

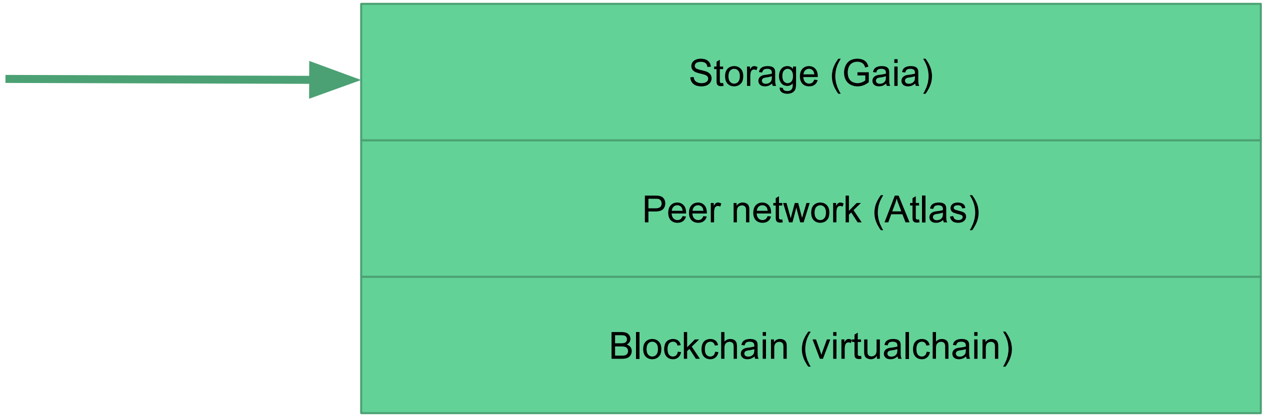
- Peer network whose nodes maintain a “100% state replica”
- Would only take 100GB to store zone files for all 250 million ICANN domains
- When a new node enters the network, it pulls the hashes of values from the blockchain, and then asks other randomly-chosen nodes for the actual zone files

Zone Files



```
▼{address: "1QABXmhyEiVv6VnVesP85UdebhC26G9YVy", blockchain: "bitcoin",…}
   address: "1QABXmhyEiVv6VnVesP85UdebhC26G9YVy"
   blockchain: "bitcoin"
   did: "did:stack:v0:SkTBZcV7y5h7coZxCJNCdNnDFURSvEWS9E-0"
   last_txid: "595478330ed0dc8aac75b153a0bbfbfdbd54572d1c192f459089a26f1f8254c7"
   status: "registered_subdomain"
   zonefile: "$ORIGIN hyunchoi98.id.blockstack↵$TTL 3600↵_http._tcp    IN  URI 10  1   "https://gaia.blockstack.org/hub/1QABXmhyEiVv6VnVesP85UdebhC26G9YVy/profile.json"↵↵"
   zonefile_hash: "b260723d2cf688bd2ea4e53b56e5a3422ae3b8c6"
```

The Layers of Blockstack



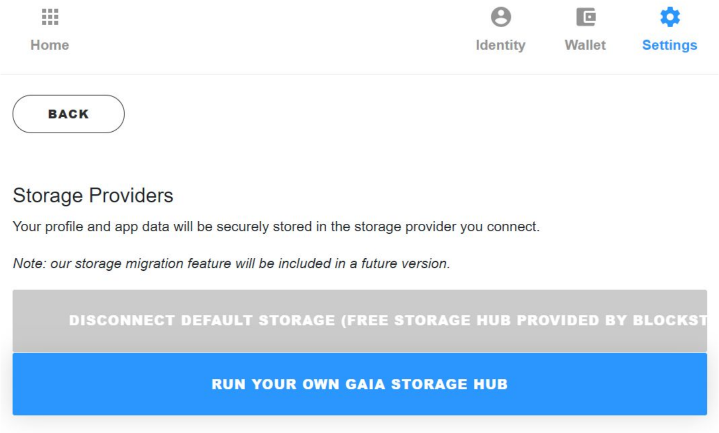
Storage (Gaia)

Peer network (Atlas)

Blockchain (virtualchain)

Gaia Storage

- Decentralized storage by giving users control over where their data is stored
- Can choose to use cloud providers like GDrive or AWS
- Can choose to self-host data! (more complex than I thought)
- By default, data is stored on free storage provided by Blockstack


Home
Identity
Wallet
Settings
BACK

Storage Providers

Your profile and app data will be securely stored in the storage provider you connect.

Note: our storage migration feature will be included in a future version.

DISCONNECT DEFAULT STORAGE (FREE STORAGE HUB PROVIDED BY BLOCKST
RUN YOUR OWN GAIA STORAGE HUB

Why this structure?

- Separates out Security, Indexing, and Storage to places that each have a competitive advantage over those functions

- Security: The blockchain gives users a way to independently verify the integrity of data
- Indexing: The peer network gives Blockstack a decentralized way to store info about where data is located, without having to actually store data (expensive)
- Storage: Using the Gaia network gives:
    - Abstracts away the problem of immense data storage to those that are good at it (AWS, Google)
    - Full control over your own data (especially if own server) -- can delete and modify at will

No need to trust Gaia or Atlas!

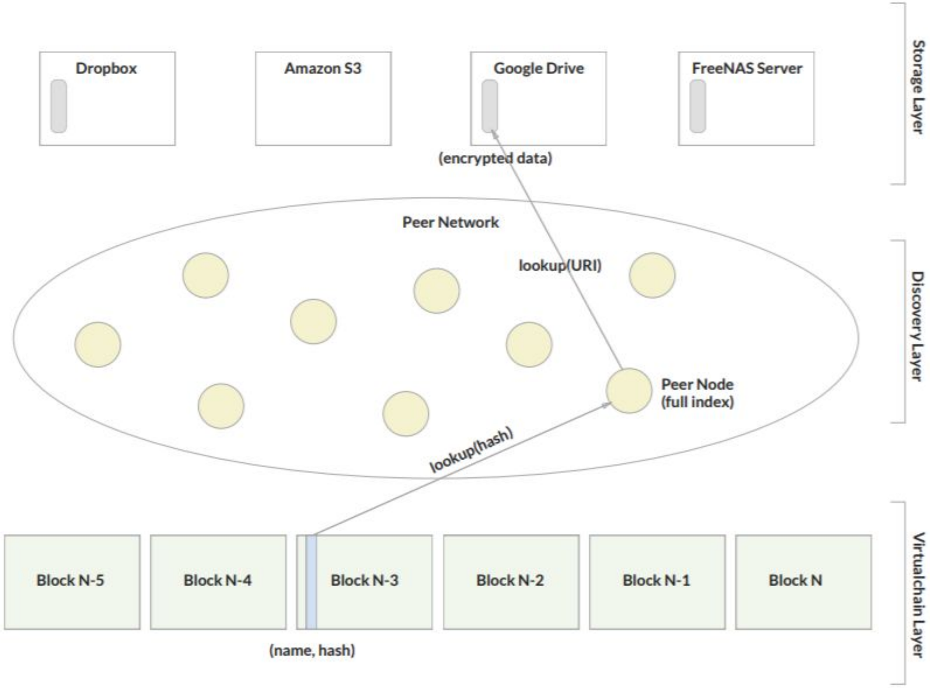


Figure 7: Overview of Gaia and steps for looking up data.

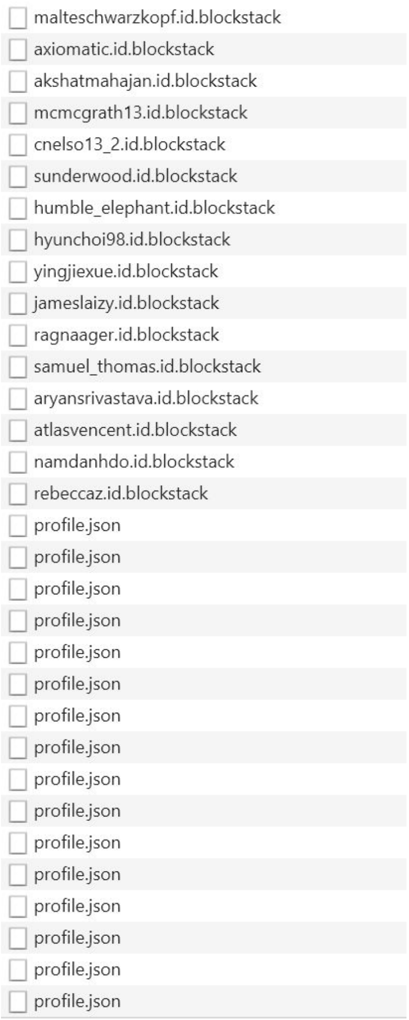
How does this improve privacy?

How does this work in practice?

Blockslack

- When you refresh Blockslack and click on our class' chatroom, the site loads each of our usernames and finds everyone's zonefiles

- Then it uses those zonefiles to find everyone's profile.json file stored in the Gaia network



□ malteschwarzkopf.id.blockstack
□ axiomatic.id.blockstack
□ akshatmahajan.id.blockstack
□ mcmcgrath13.id.blockstack
□ cnelso13_2.id.blockstack
□ sunderwood.id.blockstack
□ humble_elephant.id.blockstack
□ hyunchoi98.id.blockstack
□ yingjiexue.id.blockstack
□ jameslaizy.id.blockstack
□ ragnaager.id.blockstack
□ samuel_thomas.id.blockstack
□ aryansrivastava.id.blockstack
□ atlasvencent.id.blockstack
□ namdanhdo.id.blockstack
□ rebeccaz.id.blockstack
□ profile.json
□ profile.json
□ profile.json
□ profile.json
□ profile.json
□ profile.json
□ profile.json
□ profile.json
□ profile.json
□ profile.json
□ profile.json
□ profile.json
□ profile.json
□ profile.json
□ profile.json
□ profile.json

My Personal Experience with Blockslack

- Latency between when I press “Enter”, how the requests are handled, and when the sent message actually shows up on my browser
- Sometimes messages just don’t show up -- unsure if this is an issue with my Chrome or a Gaia issue

- Did anyone else have any issues using Blockslack?

Possible issues with Blockstack architecture?

- Can require constant reading and writing to a third-party storage provider ➔ latency issues
- What if third-party storage goes down?
- Is it actually a good idea to trust individual users with their own data?

Any others?

Is a decentralized Internet the future?