Darryl Morris Follow
Independent Ethereum Developer
Mar 31 · 10 min read

Self-Sovereign Identity Systems, Blockchain Alternatives to Aadhaar

This is the companion article to recent talks given at the World Blockchain Conclave in Mumbai and Bangalore, March 2018. Thank you to 1.21GWS for hosting these events and trusting me with the platform.

https://www.youtube.com/watch?v=_OeLVx-C_Us

Indra and Vironchana Seek the 'Self'

In the Hindu sacred text call the *Chandogya Upanishad* [1], is a story where *Indra*, the king of the gods and *Virochana*, the king of the demons seek knowledge of the true self at the ashram of *Prajapati*, the lord of all beings…

Prajapati asks, *"Desiring what have you come to live here?"*

Indra and Virochana reply, *"We seek that self which is free from evil, free from old age, free from death, free from grief, free from hunger and thirst. He who has found out, he who understands that self, he obtains all worlds and all desires."*

Parajapati says, *"That person which is seen in the eye, that is the self. That is the immortal, the fearless. Look at yourself in this pan of water. What do you see?"*

"We see ourselves as we are in every detail, our clothes, our hair, even to the lines in our eyes and even the whirls on our fingers."

Prajapati replies, *"Thank you for your enrolment. Here is your Aadhaar number. It is free from evil, free from old age, free from death free from grief, free from hunger and thirst. Understanding this self you will obtain all worlds and desires."*

Indian Government Defying Indian Culture

For those unfamiliar with Indian culture, its ancient scriptures or its ongoing attempts to enforce and defend an architecturally weak, massive biometric identity system called *Aadhaar,* a lot maybe missed in the above joke. I do apologise, but can report that the intended audience responded with applause at the irony it points out.

India's entire cultural history, descending from at least the last ice age 10,000 to 15,000 years ago is premised on the search of the true *self* and subsequent liberation through identification with that *self*. In that search, the most certain of teachings is that this true self is *not* the physical body which changes, is subject to sickness and injury and ceases to exist.

With the likes of powerful computer vision algorithms and other biometric sensor technology, the penetration of state, private and personal surveillance technology has exploded globally with often outright contempt of privacy.

There are largely two paths that are being pursued by agencies to access as much private and surveillance data as possible. These are the draconian 'state surveillance' policies such as taken by China which gather and analyse private data by dictate and the softer 'capitalist surveillance' being practices by the likes of Facebook and Google who gather data on a voluntary opportunistic basis by offering valuable knowledge content and social media products.

India has for the past few years been increasingly forcing its central *Aadhaar* 'single point of truth' identity system into civil and commercial services far beyond its publicised intent of increasing the efficiency in dispensing of welfare services. This it has done in response to the UN's Sustainable Development Goals of a legal identity for everyone and has elected to use biometric technology to support that purpose. However, the predicted embodiment of its weaknesses and demonstrated flaws have manifested into arbitrary exclusion and death by starvation of many of those it was built to help on the one hand and '360 degree' surveillance profiling on the other .

The fact that single sources of truth become single points of failure in the first instance and power choke points in the second is the root of deepest concern with *Aadhaar* and all *Aadhaar* like centralised authoritative biometric identity systems. Instead of increasing the inclusion rates of a population, it strictly demarcates the haves and have-nots along the arbitrary line of whether a biometric authentication succeeds or fails.

It is for these reasons that *Aadhaar* is being challenged before the Indian Supreme Court by petitioner advocates, Shyam Divan, Kapil Sibal and Gopal Subramaniam. The arguments in brief are:

- The body is being leashed to a massive centralised 'man-in-the-middle' state surveillance and control system and considered your only acceptable identity.
- Leashes which can probabilistically or purposely fail to deliver services.

- *Aadhaar* authentication is a single point of failure and potential choke point
- It invalidates all other valid identity documents by non-acceptance.
- Sold as 'optional' but practically impossible to live without.
- The government seeks a cradle to grave branding on whole population.
- Biometric enrolment and authentication failure leads to exclusion and expulsion.
- The UADAI/Aadhaar/SRDH architecture is an unsecure surveillance network and national security risk
- Constitution does not permit a surveillance state.
- The Aadhaar enables new categories of 'Aadhaar enabled' fraud which are hard to prove and defend against
- Fundamental freedoms such as privacy cannot be sold.
- Individuals must part with their biometrics and alternative identification in violation of freedom of privacy and right to identify by alternative means.
- Individuals have no right to complain against a violation.
- The state dominates and makes transparent the individual rather than the State being transparent and subservient to the individual.
- Designed so public and private corporations can access a 360 profile of you

The Two Greatest Sins

From these arguments we can deduce two great sins that are and will be committed to by any and all centralised authoritarian biometric identity systems which render them morally illegitimate;

1. They make presumptions upon the state of people's bodies over which it has no right to do.
2. They enforce those presumptions to privilege those where the presumption is correct and exclude those where it is not

The temptation to use these systems is strong in that the body is 'almost' robust enough against change for it to work *most* of the time for *most* people. But it denies the fact that the body changes not only by ageing but more rapidly through injury and disfigurement (such as burning and acid attacks which are a common in India).

Why Is Identity A Problem?

Identity is only a problem for other people, other institutions. It is never such a problem for people of sound self-aware minds. For the likes of a government, the requirements of holding an identity are artificial in the sense that in the absence of the government, the identity is meaningless. It is something that is imposed upon an individual to distinguish between individuals. The natural presumption is that an individual is a 'body' and so some biometric data would seem a suitable identifier of individuals.

But the very presumption that an identity has an associated physical body is ever being challenged in the modern world of commerce and technology. It has long been anti-intuitive nonsense that a 'corporation' can have legal status as a 'person' when no two things could be more dissimilar.

Any trust that an identity must be a person is further blown away by the internet ecology where a perceived identity may be a person or maybe a toaster.

We Think We Only Have One

A fundamental rethink of identity must be undertaken if civilisation is to continue in any self determined and free thinking way. In order to progress, we must **give up the notion that *identity* is a singlton** and replace it with the more loose notion that identities are *relational* and *pluralistic*. We also must identify just what it is we are seeking to protect and keep private and what privacy actually implies.

Personal/Existential Identity

- Your *self view* arrived at by simple self awareness
- Nobody else's business, it is *private within the mind, emotions and body*
- **It is what must be protected against all harassment and violence**
- Day to day awareness of different aspects of self change
- Not a singleton identity

Self Declared Identity

- Who you say you are.
- May be different on different days
- Is different to different people
- Taken by others on trust
- Not a singleton identity

Social Identity

- Who others say you are.
- The collective impressions you receive from and have upon society
- But you are a different person to different people with different relationships.
- Not a singleton identity

Imposed Identity

- Imposed upon you by an authority
- Different authorities impose identities based on some presented fact or proof of some other identity
- Not a singular identity

Identity IS NOT SINGULAR so stop pretending it is

Lets instead treat identities as pluralistic *relationships*, outside of which no one else has any business.

There is really no need for your electricity supplier to know who your kindergarten teacher was, yet with centralised identity databases and profiling, that's exactly the kind of information that may be offered to them by some third party analytics company.

What we seek with *Self-Sovereign* identity systems is an anonymising layer of distinct, purpose specific identity relationships with different counter-parties. For this we can explore and develop the following notions of identity relationships;

Transactional Identities

- A growing record of transactions of an entity or agent with another entity.
- Economic footprints which could be used as evidence for an attested identity.
- Many identities can be run in parallel by a single agent

Reputational Identity

- A more formalised social identity
- Identities built upon a history of third-party ratings of interactions

- Can act as abstracts of Transactional Identities

Attested Identity

- Identity by 'accepted' attestation of facts by third-parties such as an attendance record or certificate.
- An aggregated identity from proofs of different identity sources
- Attested identity networks could build up 'webs of trust'.
- Can involve preferential attachment to trusted webs for efficient trust routing

Identity on Blockchain

Blockchains typically have only a single type of identity primitive, a public key address which can be proved by an owner of the associated private key by signing data. *Ethereum* additionally allows residence of deterministic *Smart Contracts* at public addresses.

Typically no assumptions can be made of the agent signing data. It may be a human, an organisation, a device or a some other bot. Further, there is practically no limit to number of private keys a single agent may control.

This anonymity and plurality of possible identities makes blockchain perfect for next generation identity systems which can maintain privacy and prevent cross contamination of personal and private information between different counter parties.

What About Sybil?

The cry of identity systems like *Aadhaar* is that they seek to 'deduplicate' identities and their associated personal data. That is, the same data may be held under different identities, or that multiple identities of a single person may have different data. The goal is to reduce the data to a single trusted mapping of identity to data.

In blockchain, no such single identity/data trust model can be established and nor should such attempts be made. However to a provider of some benefit, such as a government, this is a most undesirable property as any one person may apply for unlimited benefits using an unlimited number of anonymous identities.

The 'blockchain' way is to manage such problems is through the economics of capital, collateral and penalties. For a blockchain identity to derive from some institutional benefit, that benefit must be engineered in some way to first accept collateral from the identity which it can return, enhance or harm depending upon the subsequent behaviour of the identity or some other proof of cheating.

For a blockchain identity, this collateral might be provided from what I call *Civil Capital.*

Civil Capital

Civil Capital I define as, *the weight of trust an identity gains over its history of civil activities.*

This weight may be multi-factorial, drawing from reputation systems, transaction counts and quality and attestations. It is something that accumulates over time and so gains in value. It should be offerable in part for staking or collateral in order to receive some offered benefit, loan or more novel applications such as games, duals or betting if such is appropriate.

Self-Sovereign Identities [3]

We can now start to see the shape of this new paradigm and point out its salient features;

- Privacy through self created ‘de-individualised’ identities
- Individuals, collectives and digital agents can protect themselves by control over their personal and private information using pluralistic decentralised identities.
- These identities become single sources of truth to user owned and updated personal data.
- They can be pluralistic for different purposes, e.g. one to manage your financial or social relationships, one to manage your healthcare relationships and data, one for academic or employment records and so on.
- Identity through ownership of private keys.
- Key selection left up to owner, could be biometric, could be brainwallet or seeded, etc.
- They are portable and borderless. A tourist, businessperson or refugee could still identify themselves no matter where they end up.
- They can act as locally authenticated ‘single sign-on’ to blockchain and off-chain services.
- Can permission owned encrypted data and control data sharing relationships.
- Personal data is locally accessible and locally authenticated from distributed encrypted storage layers such as IPFS and Ethereum’s SWARM protocols.
- And of course can send and receive money and manage finances and assets without the need of intermediaries.

This enormous paradigm shift in the notion of identity from singular and transparent to plural and anonymous, brings with it fundamental challenges and disruption to all institutions that have historically relied upon a singlton identity model. However the opportunities that self-soverign identity brings opens the way for an equally powerful and liberating revolution of governance in general which shall be explored in my following article on Delegative Democracies and Decentralised Governance.

Self-Sovereign Projects

A number of self-sovereign projects are in current development (for the reader to investigate) the foremost being;

- uPort.me [4]
- ERC725 together with ERC735 [5,6]

Indra and Vironchana Leave the Ashram

As Indra and Virochana go, Prajapati thinks, “Without perceiving, they go away not knowing the self. Who ever follows such a doctrine will surely perish.”

Virochana declares that Aadhaar is the immortal self which must be served to enjoy life and grow. He grows rich and powerful until Bali, his son, hacks UADAI and deletes Virochana’s Aadhaar profile. Aadhaar no longer authenticates for him and he perishes.

But Before reaching the gods, Indra realises that when the eyes grow cloudy and the fingerprints worn, this Aadhaar will lead one to perish. He comes back to Prajapati and asks, “Can you teach me about blockchain self-sovereignty instead?”

(And returned a third time to learn the true self also, the Atma!)

References

1. **Chandogya Upanishad** *Ch6, section 7*
2. **sflc.in** *Updates on Aadhaar Final Hearing*

3. **www.lifewithalacrity.com** *The Path To Self-Sovererereign-Identity, Christopher Allen*

4. **uPort.me** *Open Identity System for the Decentralized Web, Consensys*

5. **ERC725** *A Self-Sovereign Identity Standard For Ethereum, Fabian Vogelsteller*

6. **ERC735** *Claim Holder, Fabian Vogelsteller*