Decentralizing Aadhaar Authentication using a Blockchain

Mehul Agarwal

October 2018

Abstract. The Unique Identity project of India, Aadhaar, provides a unique biometric identity to 1.2 billion residents of India. Today, it has effectively replaced traditional methods of identity verification to obtain various services across the country. The efficacy and need of this change has been debated, and as with any project of such scale, there are concerns of privacy, surveillance and the overall security of the system.

A decentralized blockchain layer added to Authentication of the Aadhaar project in India can add to the security of the process reducing the threat of identity theft to a bare minimum. While onion hashing and better encryption techniques may be developed in the current centralized process of Authentication to help mask an identity, it can still be exploited by internal bad actors. By adding an immutable decentralized layer without disturbing the current architecture, this proposal aims to provide a practical and implementable mechanism to include the benefits of a blockchain to a previously centralized process. It also proposes to construct a private blockchain layer at first, slowly building a completely decentralized (public) one.

This extra layer will maintain logs for each authentication with a unique and immutable authentication hash, hence no authentication would go unaccounted and integrity of every authentication will be ensured. Blockchain as an independent and parallel layer to the current Architecture inherently ensures that even someone with access to the central servers of Aadhaar would additionally need control over the consensus (A 51% attack) to introduce an illegitimate authentication. For most practical purposes, this makes sure that even people on the inside (i.e. working at the UIDAI) cannot counterfeit an authentication. The incentivization of such a layer would involve economic assets to ensure that any public entity may take part in a Proof of Stake consensus protocol. This opens up opportunities for an implementation of a competent Indian state-backed cryptocurrency with smart contracts leading to better business integrity and minimization of disputes related to fraud and non-payment.