Abstract

Proof of Identity has always been an important security consideration for organisations and individuals alike. As an alternative to passwords or other forms of authentication, ‘Decentralized Identifiers’ (or DIDs) proposed by the W3C, offer a publicly verifiable and entirely user-controlled digital identity mechanism.

Using the blockchain as a distributed ledger, DIDs can be verified by any interested party while being securely owned by a single controller. Because DIDs are fully controlled by their controller and can be verified to others without revealing any personal information, they are an attractive alternative to traditional, centralised identity management.

As an exploration into a potential extension to the DID specification, I would like to investigate how they can be used to implement an alternative fully decentralised website login mechanism that can incorporate with verifiable credentials to allow for private, ethical and user-centric authentication.