Abstract

Currently, important paper documents that have historically been kept in physical safe places are moving to an electronic medium. Bank account details, proofs of ownership, passwords and more recently crypto keys are forever lost when a person dies or is seriously injured.

There are several centralised key recovery solutions which rely on trusted third parties to manage a user's keys (AirGap, Casa, Torus). Similarly, users can currently store their secrets in cloud based centralised data storage solutions if they choose. The recent emergence of decentralised technologies (Ethereum, IPFS) has allowed systems that traditionally rely on centralised infrastructure to now be built in a decentralised, trustless way.

This project utilises the technologies that are underpinning the current decentralised web movement (web3) and applies them to the long-term storage and access of documents. The project describes the design of an encrypted data vault such that a user can safeguard their secrets and enable inheritance over the long-term using the decentralised storage networks Filecoin and IPFS. Furthermore, the project proposes a design for a novel DKMS (Decentralised Key Management System) that utilises Ethereum based NFTs (Non Fungible Tokens) to employ social key recovery.