Data DAO Hackathon

August 15 - Sept 11, 2022

Afiant

A Decentralized Identifier (DID) System Tool

Overview

The quest for a self sovereign identity solution has been in the works for the past few years with the latest in technical advances involving the creation and use of a decentralized Identifier (DID) as outlined by W3C. DID have great potential to be the future of digital identities in the future generations of the internet.

Afiant is a DID system tool that integrates various technologies to allow the creation and maintenance of DIDs and perform other DID related functionalities while utilizing IPFS and Filecoin both via FilSwan MCS.

There are primarily three core functionalities in Afiant. First, Afiant facilitates the generation of a DID and DID document via the ION protocol. The DID can then be used to generate a JSON Web Token (JWT) and be used for authorization and authentication of the data. Afiant will also provide an option to encrypt the data file before uploading the file to IPFS via FilSwan.

Second, Afiant integrates API3 with Filswan for the DID document service endpoint. This service endpoint points to the DID document data. Using API3 is significant because it can act as a first party blockchain oracle to use the data on or off chain and also allow users to have more control over their DID data.

Third, Afiant allows the embedding of a DID into a NFT that is minted by FilSwan. This allows for various use cases such as proof of NFT ownership via a DID or associating various DIDs with a NFT to show creator credits.

All of Afiant's functionalities mentioned above each have a working proof of concept written in node.js. Afiant is a prototype that encapsulates all these functionalities into a single command line tool.

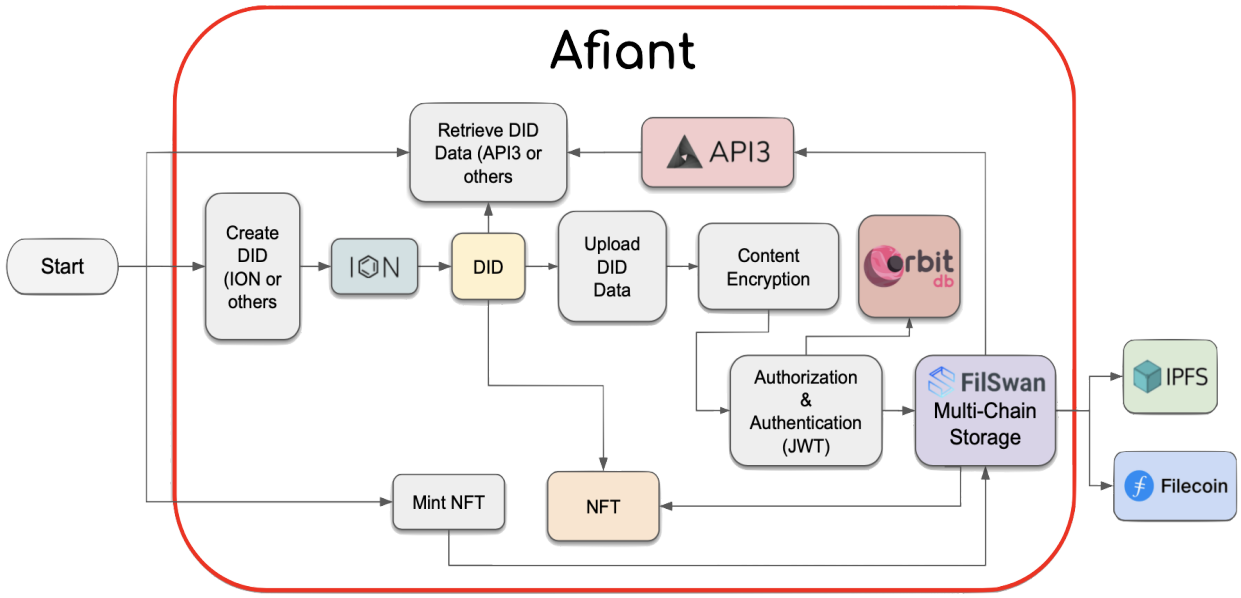
Key Functionalities

The following outlines Afiant's key features and functionalities::

1. **Decentralized Identifier (DID):** **Generate a DID** using ION. Other solutions can be used here to create DIDs.
2. **DID document service endpoint:** Create a DID document service endpoint for data retrieval using API3 as a gateway connecting from FilSwan. API3 allows the endpoint to be a **first party blockchain Oracle**.
3. **Data storage:** Uses FilSwan MCS to facilitate the storing and retrieval of data to and from IPFS and creating persistent data with Filecoin.
    a. **Encrypt/Decrypt data:** Afiant can **encrypt data files** prior to uploading to IPFS via Filswan.
    b. **Authorization/Authentication:** Afiant **generates a JSON Web Token (JWT)** signed by the DID and allows for user authentication and data authorization. The DID is stored in OrbitDb for verification.
4. **NFT with DID:** Mint a NFT using FilSwan MCS and then **embed the DID in the NFT attribute.**

System Overview

The following diagram shows the technical system overview of Afiant, which integrates various third-party technologies to facilitate DID functionalities. Afiant leverages FilSwan to access IPFS and Filecoin.



Proof of Concept

There is a proof of concept (written in node.js code) for each of the components in Afiant.. The following will describe each component with further technical details:

1. ION - generate a DID and DID Document

   Afiant currently uses ION to generate DID and DID Document, but is open to using other protocols to anchor the DID to other blockchain or non-blockchain based technologies.

2. API3 - generate a first party oracle endpoint that retrieves data from Filswan MCS

   At this time, the service endpoint retrieves the FilSwan deal details only given a dealId. Since this is only a proof of concept, this service endpoint is only a docker container. In

production, this service endpoint will be an internet (https) gateway., which will allow for a complete end-to-end integration in Afiant (from DID creation, to linking the DID to the service endpoint data, to retrieving data from API3 and FilSwan) .

3. FilSwan MCS - upload, pay to store data to IPFS, and to mint NFTs.

   FilSwan is used to upload the data file and then pay for persistent storage. Also, Afiant uses FilSwan to mint NFTs. Other direct calls to FilSwan MCS include “get file details” and “listing all files” and are used to support Afiant’s core functions.

4. JSON Web Token (JWT) - generate JWT signed by a DID and maintained in OrbitDb.

   At this time, a JWT will be generated and signed with a DID created from ION. This DID is then stored into the OrbitDB database as part of the authentication and authorization workflow.

5. Data Encryption - Encrypt and decrypt data

   Afiant provides the option to encrypt their DID data file prior to uploading it to IPFS via FilSwan. The same data file can be decrypted as needed.

6. NFT - Mint NFT with embed DID

   The DID created from ION will be embedded into the attributes of a newly minted NFT via FilSwan MCS.

Prototype

Afiant is a working prototype in the form of a command line tool that encapsulates all the above proof of concept and DID functionalities.

Afiant command line tool:

```
Usage: index [options]

Options:
  -d, --did       generate a new DID (ION)
  -u, --upload    upload to service endpoint (FilSwan)
  -e, --encrypt   encrypt or decrypt file
  -j, --jwt       generate a json web token (JWT)
  -s, --service   get files from service endpoint (API3 and FilSwan)
  -m, --mint      mint NFT with DID (FilSwan)
  -t, --maintain  Get file details or list all files (FilSwan)
  -h, --help      display help for command
```

Usage: node index.js [options]

Options:

-d, --did **generate a new DID (ION) -** Creates a DID using ION protocol

-u, --upload **upload to service endpoint (FilSwan) -** Upload file to IPFS using FilSwan. It will ask for file input. Then it provides an option to generate a JSON Web Token (JWT) and also provides an option to encrypt the file.

-e, --encrypt **encrypt or decrypt file** - Encrypt or decrypt a file, which can be used prior to uploading to IPFS via FilSwan. Encryption is also available via the upload option above.

-j, --jwt **generate a json web token (JWT)** - Generate a JWT token with a DID and store the data in OrbitDb.

-s, --service get files from service endpoint (API3 and FilSwan) - Retrieve data from Filswan and provide a DID service endpoint using API3. This endpoint becomes a first party blockchain oracle.

-m, --mint mint NFT with DID (FilSwan) - Mint a NFT with a DID embedded into the attribute.

-t, --maintain Get file details or list all files (FilSwan) - Helper functions directly from Filswan to support Afiant's core functions.

-h, --help display help for command - Afiant help into