KILT: Credentials for web3

Decentralized Identifiers (DIDs): a practical primer

@KILTProtocol @maudnals

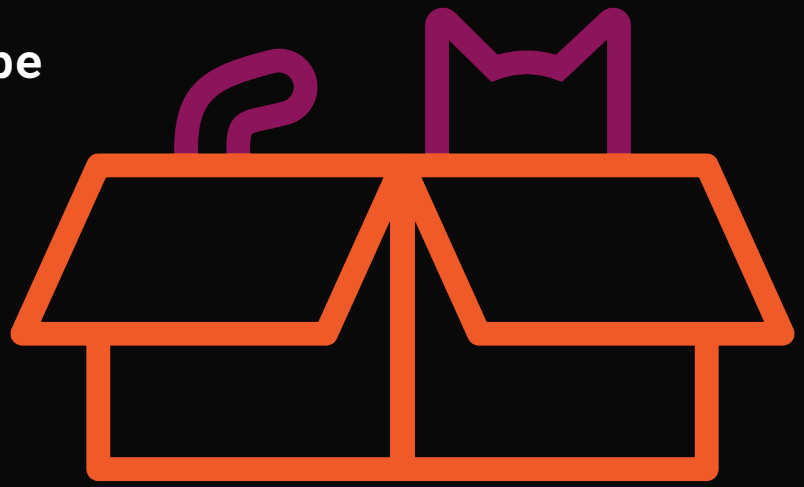
Agenda

1. KILT
2. DIDs
3. DIDs in our system
4. DIDs in practice: Universal Resolver driver implementation

But first

- KILT Protocol, Ingo Rübe
  @KILTProtocol
  kilt.io

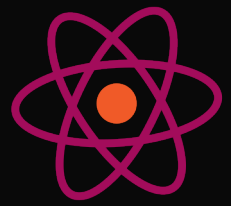
- Maud @maudnals



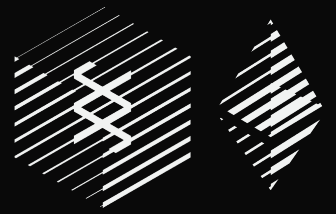
- ... You x DIDs?

Permissionless trust infrastructure

Credentials for the web3



Regulation-friendly virtual structures

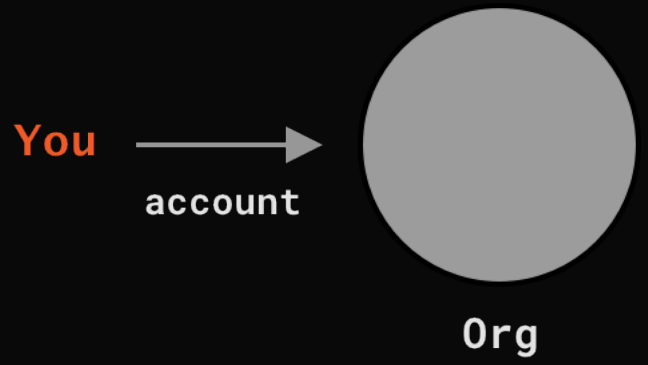


Parity Substrate-based

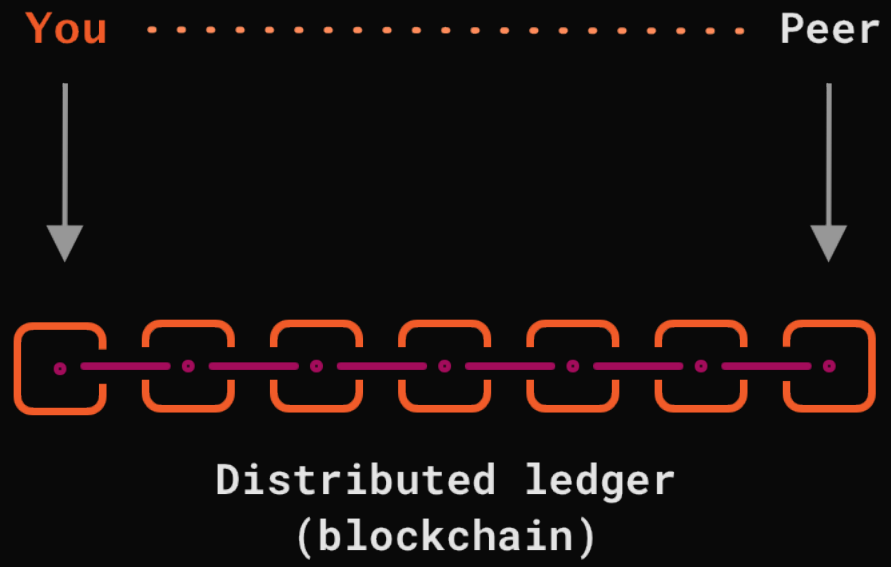
DIDs?

KILT

Now



With DIDs



Source: SSI Meetup

DIDs?

KILT

A DID is a new type of **globally unique identifier**, that does not require a centralized registration authority; control of the identifier can be proved cryptographically.

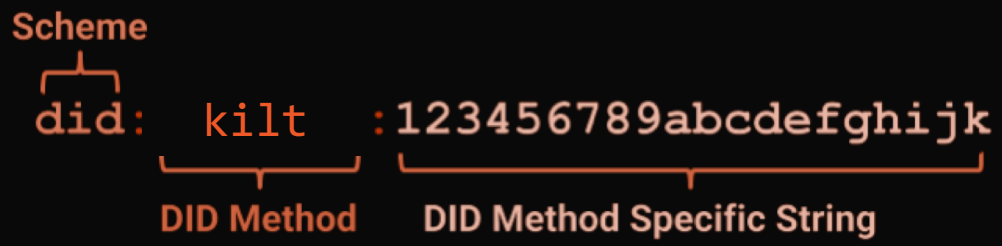
https://w3c-ccg.github.io/did-spec/

4 core properties of DIDs

1. Persistent
2. Resolvable
3. Cryptographically verifiable
4. Decentralized

NOT: human-readable

DID + DID Document



did:ethr:
did:btcr:
did:sov:
did:uport:
...

```
{
  "@context": "https://www.w3.org/2019/did/v1",
  "id": "did:kilt:123456789abcdefghi",
  "authentication": [
    {
      "id": "did:kilt:123456789abcdefghi#keys-1",
      "type": "RsaVerificationKey2018",
      "controller": "did:kilt:123456789abcdefghi",
      "publicKeyPem": "-----BEGIN PUBLIC
      KEY...END PUBLIC KEY-----\r\n"
    }
  ],
  "service": [
    {
      "id": "did:kilt:123456789abcdefghi#vcs",
      "type": "VerifiableCredentialService",
      "serviceEndpoint": "https://kilt.com/vc/"
    }
  ]
}
```

CRUD

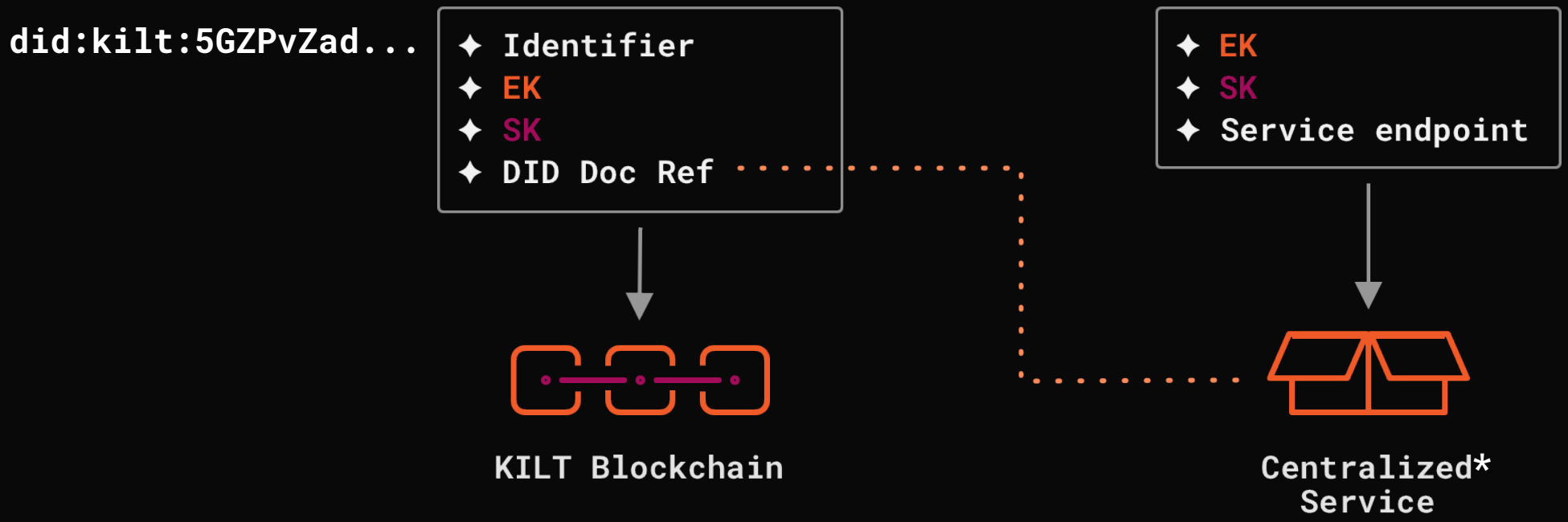
- Create
- Resolve
- Update
- De-activate

= f(DID method)

= `kilt` in our case

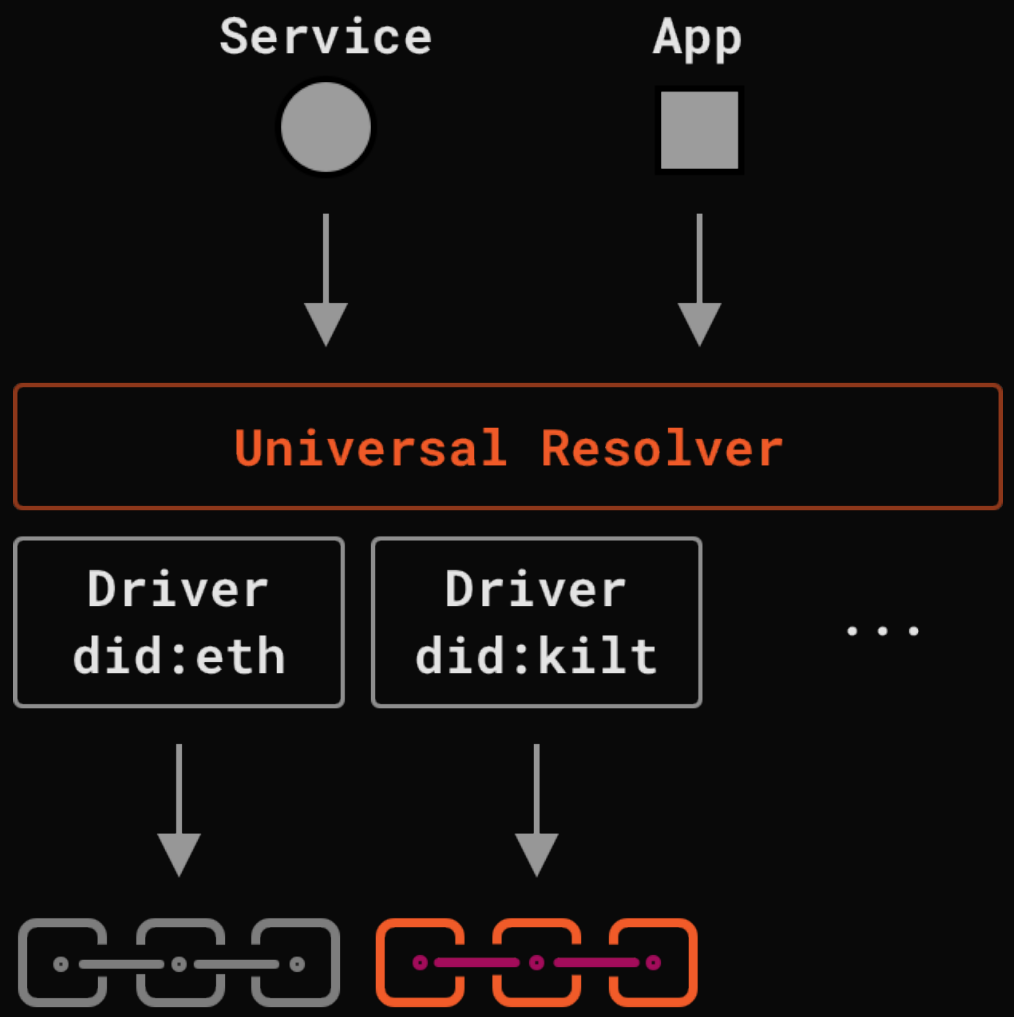
DIDs in KILT


ek, EK
Encryption keypair
sk, SK
Signing keypair


did:kilt:5GZPvZad...
Identifier
EK
SK
DID Doc Ref
EK
SK
Service endpoint
KILT Blockchain
Centralized* Service

Universal Resolver by DIF

KILT

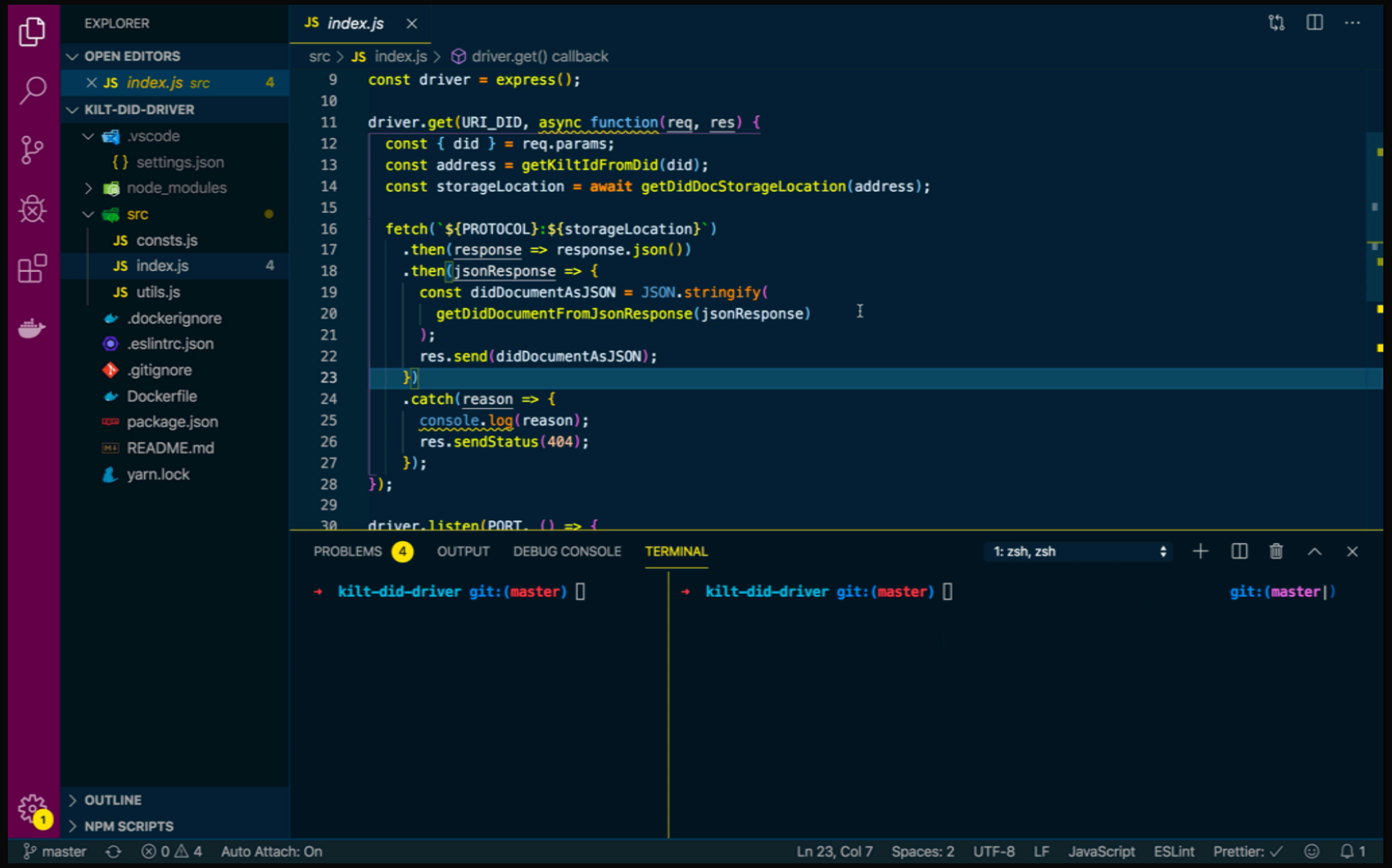


👉 uniresolver.io

Driver guidelines

- Resolve functionality only: `resolve(did) -> diddoc`
- Open-source
- Container on dockerhub
- Documented methods

KILT‘s dockerized driver



Food for thought

- DID fragments
- Remote or not
- Universal Registrar

did:kilt:123456#oidc

Thank you

@KILTProtocol
@maudnals
kilt.io

Check out TCAs 🔥
Slides coming soon

Sources

DID Resolution Webinar // DIF at SSI Meetup

DID Methods Registry

Universal Resolver: introduction