DIDs and NFTs

How Do They Work Together?

JOE ANDRIEU

LEGENDARY REQUIREMENTS

DID CONFERENCE KOREA 2022

DIDs & NFTs

- Context
- DIDs as identifiers
- DIDs, VCs, and NFTs
- Interchain Identifiers
- Requirements Review

Joe Andrieu

- Legendary Requirements
  - Requirements engineering for decentralized identity systems and applications
- World Wide Web Consortium Invited Expert
  - VC Use Cases (Editor) https://w3.org/TR/vc-use-cases
  - DID Use Cases (Creator and Editor) https://w3.org/TR/did-use-cases
  - DID Method Rubric (Creator and Editor) https://w3.org/TR/did-rubric
  - VC-API Use Cases (Co-editor) in process
- Board Member, Treasurer, Producer, Facilitator, Rebooting the Web of Trust
  - 50+ papers published on decentralized identity

Current Work on NFTs

- Requirements Lead for the Earth Program
- Funded by Interchain Foundation, led by ixo
- Applying DIDs to NFTs for Cosmos
    - ixo's Impact Tokens map verifiable earth state to chain state
    - Uses Verifiable Credentials to automate policy-driven NFTs

DIDs as *Identifiers*

- Identifiers are used to refer to specific things
- Same identifier means you're talking about the same thing
  - VCs with the same subject ID
    - Statements about the same entity
- Errors are inevitable
  - Assignment & Interpretation

VCs and DIDs

DIDs Enable Identity Assurance For VCs

VC Identity Assurance Step 1

1. Onboard user at Issuer
2. Create authentication mechanism at Issuer App
3. Perform initial identity assurance (KYC)

VC Identity Assurance Step 2

1. Authenticate into Issuer's app
2. Use DID Auth to prove control of DID
3. Issue VC with that proven DID as Subject

Bonus points

- Record DID Auth proof as "evidence"

VC Identity Assurance Step 3

1. Holder signs Verifiable Presentation with Subject DID
   - Sends VP to Verifier
2. Verifier verifies
   - VP Signature
   - VC Signature
   - DID Auth Proof

Result: Cryptographic assurance that the presenter is the same party who received the VC

Errors

Issuance

- Bookkeeping errors
- Social engineering
- Technical hack

Verification

- Misinterpretation of claims
- Trusting the wrong Issuer

Why not use VCs for everything?

- With VCs
  - anyone can say anything about anyone
- Why not use VCs for
  - Authorization
  - Delegation
  - NFTs

VCs are Chomsky Complete

- VCs are statements
- Anything that can be done using language can be done with a VC
  - Chomsky meets Turing, bounded by Goëdel
- Doesn’t mean you should
- Semantic ambiguity and drift
- Different guarantees from different approaches

VCs and NFTs

Different guarantees for different uses

VCs

- Verifiable assertion by deterministic author
- Not guaranteed to be unique
- Not expected to be transferrable
  - Statements aren't transferable
    - Joe said "The sky is blue"
  - Underlying privileges and accolades are not transferable
    - Degree
    - Driver's License
    - Vaccination Record
- VCs are verifiable statements by a knowable author

NFTs

- Rivalrous Digital Goods
  - Unique
  - Provable Ownership
  - Secure transferability
    - Preventing double spend is core to NFTs
- Transferring the bits does NOT transfer ownership.

VCs & NFTs

- Both use cryptography for independent verification.
- VCs verify
  - Authenticity
  - Timeliness
- NFTs ensure
  - Uniqueness
  - Transferability
- VCs are great, but for different uses than NFTs
  - DIDs play similar, but distinct roles

Interchain Identifiers (IIDs)

- Family of DID methods
  - Created for referring to on-chain assets
- 100% DID compatible
  - IIDs are DIDs
- Two new properties
  - Linked Resources
  - Accorded Rights
- Chain agnostic
  - Make an IID for any blockchain (just like DIDs)

Linked Resources

- Privacy-enabling, verifiable resources
- Fixes HttpRange14
- Downloadable (IID Resources)
  - did:example:abc/image.png
- Referenceable (IID References)
  - did:example:abc#image.png
- Useful for identifying, providing, and verifying
  - Evidence
  - Associated Assets

Accorded Rights

- Specifies rights or privileges accorded to asset owner or their agent
- Removes ambiguity about intellectual property licensed to NFT owner
- Enables derivative and bundled rights

Next: Requirements that defined IIDs

- 12 affirmative requirments
- 1 negative requirement
- Captured at https://github.com/interNFT/nft-rfc/blob/main/nft-rfc-006.md

Requirement 1

Identify on-chain tokens

- Must be able to identify specific on-chain tokens
  - Which chain (BTC, Ethereum, Cosmos)
  - Which network (mainnet, testnet, etc.)
  - Which fork (BTC v BCH, Eth v eth Classic)
- Enable unambiguous interpretation of which asset is referenced.

Requirement 1

Identify on-chain tokens

Solution: By convention, all IIDs only refer to on-chain assets

- IID Methods define CRUD for any verifiable data registry
  - Any chain, Any smart contract, Any module
- Definable for any type of on-chain asset
  - UTXOs, Accounts, Smart Contracts, NFTs

Requirement 2
Identify off-chain resources

NFTs need to unambiguously refer to digital and real-world resources.

- Theatre ticket for to a specific performance
- Property title for a plot of land with linked assertions about easements, liens, and permits.
- Digital collectible and its visualization, perhaps specified by a content-specified hash, retrievable from IPFS

Requirement 2

Identify off-chain resources

Solution : Linked Resources

- IID References for NFT-specific identifiers
  - “within” the namespace of the IID
- IID Resources link to digitally verifiable assets like permits, certifications, etc.

Requirement 3

Work with any chain

IIDs must be able to reference any on-chain asset, for any chain.

- Allows cross-chain operations, one chain working with assets on another
- Allows off-chain operations to interoperate with any supported chain

Requirement 3

Work with any chain

- Solution: Custom IID methods for any chain
  - Uses DID method pattern
  - Any chain could have its own method(s)
  - Specific details for each chain are defined in distinct DID methods
  - All IID conformant DID methods are IID methods

Requirement 4

Enable verifiable assertions

Identifiers for both on-chain and off-chain assets must be suitable for verifiable assertions

- Identifiers should work the same way, regardless of context: offline, online, or hybrid.
- Must be usable for Verifiable Credentials

Requirement 4
Enable verifiable assertions

Solution: As DIDs, IIDs are natively supported for Verifiable Credentials

- IIDs and IID references *are* DIDs and DID URLs
- Universally self-describing, they can be used in nearly any system of assertions.

Requirement 5

Both private and public assertions

Must be able to support

- publicly revealed assertions available to anyone
- privately verifiable assertions available only to authorized parties

Requirement 5

Both private and public assertions

Solution: VCs, linked and unlisted

- Verifiable Credentials as Linked Resources
  - Verifiably publish public VCs
  - Verifiably prove unpublished VCs are associated
- Unlisted VCs can be privately created and communicated for maximum privacy.
  - Signed by NFT for verifiable, private linkage

Requirement 6

Verifiability of completeness

Prior to purchase, buyers must be able to verify all information pertinent to the use of the asset.

- Art NFT may need
  - Visual asset, authorship, certificate of authenticity
- Property Titles may need disclosures of
  - liens, warranties, easements
- Actual data may be unsuitable to put on-chain
  - GDPR & similar privacy regulations

Requirement 6

Verifiability of completeness

Solution: Linked Resources

- Linked Resources allow
  - Inline and off-chain publication
  - Verifiability regardless of publication
- All disclosures, terms, and resources can be linked from the DID Document

Requirement 7

Off-chain creation of identifiers

- When supported by a given chain, it must be possible to create identifiers off-line.
- Enables signing linked resources, e.g., VCs, by the NFT prior to minting
- Allows minting from signed transction

Requirement 7

Off-chain creation of identifiers

Solution: Create cryptographic IID first, submit signed TX to create on-chain asset

- Minting accepts any compatible, unique IID
- Resolution first checks the chain
  - If found, use chain-provided DID document
  - If not, use deterministic minimal DID document

Requirement 8

Use with self-sovereign identity (SSI)

IIDs must work with emerging self-sovereign identity approaches

- Compatible with DID and VC wallets
- Individuals manage their own identifiers and cryptographic secrets

Requirement 8

Use with self-sovereign identity (SSI)

Solution: IIDs are DIDs

- DIDs were created hand-in-hand with SSI
- DIDs are widely used for SSI
- DID technologies work with IIDs
  - Syntax, Resolution, Data Formats
  - May need updates to support new properties

Requirement 9

Use with confidential storage

IIDs must be able to work with emerging approaches to confidential storage

- Secure Data Storage
- Encrypted Data Vaults
- Confidential Storage

Requires

- Cryptographic authorization
- Encryption & decryption

Requirement 9
Use with confidential storage

Solution: IIDs are DIDs

- Confidential Storage developed with DIDs in mind.
- DID technologies work with IIDs
  - Syntax, Resolution, Data Formats
  - May need updates to support new properties

Requirements 10

Recognizability

IIDs must be recognizable as such

- IIDs (and DIDs) have unique properties compared to other bit strings.
- When used in different contexts, it must be clear that the identifier is an IID.

Requirements 10

Recognizability

Solution: IIDs are DIDs, which are URIs

- Uniform Resource Identifiers (URIs) are self-describing, using the scheme part to specify the type of identifier (a DID).
  - http: for WWW links
  - mailto: for email links
  - did: for DIDs
- Like DIDs, the method part of the IID specifies the type of IID.
- Each IID method specification states how the method supports IID conventions.

Requirement 11

Multiple metadata representations

IIDs will be used in a wide variety of contexts, with commensurate variety in serializations.

- Must be able to specify metadata in a variety of formats without losing rigor.
- Including representations of associated rights and attributes.

Requirement 11

Multiple metadata representations

Solution: Linked Resources separate the metadata from the on-chain asset control mechanism.

- Reference to off-chain resources supports any format for metadata
  - PDF
  - PNG
  - RDF-XML
- Content-based hashes can verify any digital object, in any format.

Requirement 12

Leverage tooling and infrastructure

IIDs should leverage widespread and mature tools rather than requiring bespoke or relatively untested innovative approaches.

- Immature tools are
  - Risky
  - Often lack interoperability
  - Often have limited support for different platforms
  - Dangerous for high-value transactions

Requirement 12
Leverage tooling and infrastructure

Solution: IIDs are DIDs are URIs

- Emerging DID tooling either already works with IIDs or requires minimal adjustments
- As URIs, both DIDs and IIDs leverage tools and infrastructure of the World Wide Web and the Semantic Web

Anti-Requirement 1

Human readability

IIDs are not intended for human readability.

- Decentralization and Security are more important than a human-friendly name
- NFTs and on-chain assets need identifiers that work for on-chain interactions and chain-dependent applications
- Attempting to also make them human-friendly is believed impossible (Zooko’s Triangle)

Anti-Requirement 1

Human readability

Solution: Like DIDs, IIDs choose cryptographic functionality over human readability

- Identifiers are expected to use cryptographic creation and verification
- Registries, directories, and other human-friendly mechanisms can be added on top of IIDs (just like DIDs).

DIDs and NFTs

That is How They Work Together

Questions?

JOE ANDRIEU

LEGENDARY REQUIREMENTS

JOE@LEGREQ.COM