Verifiable Credentials と譲渡不可NFTを組み合わせたデジタル賞状の発行について

デジタル庁

概要

good digital award の賞状を、デジタルでも発行する

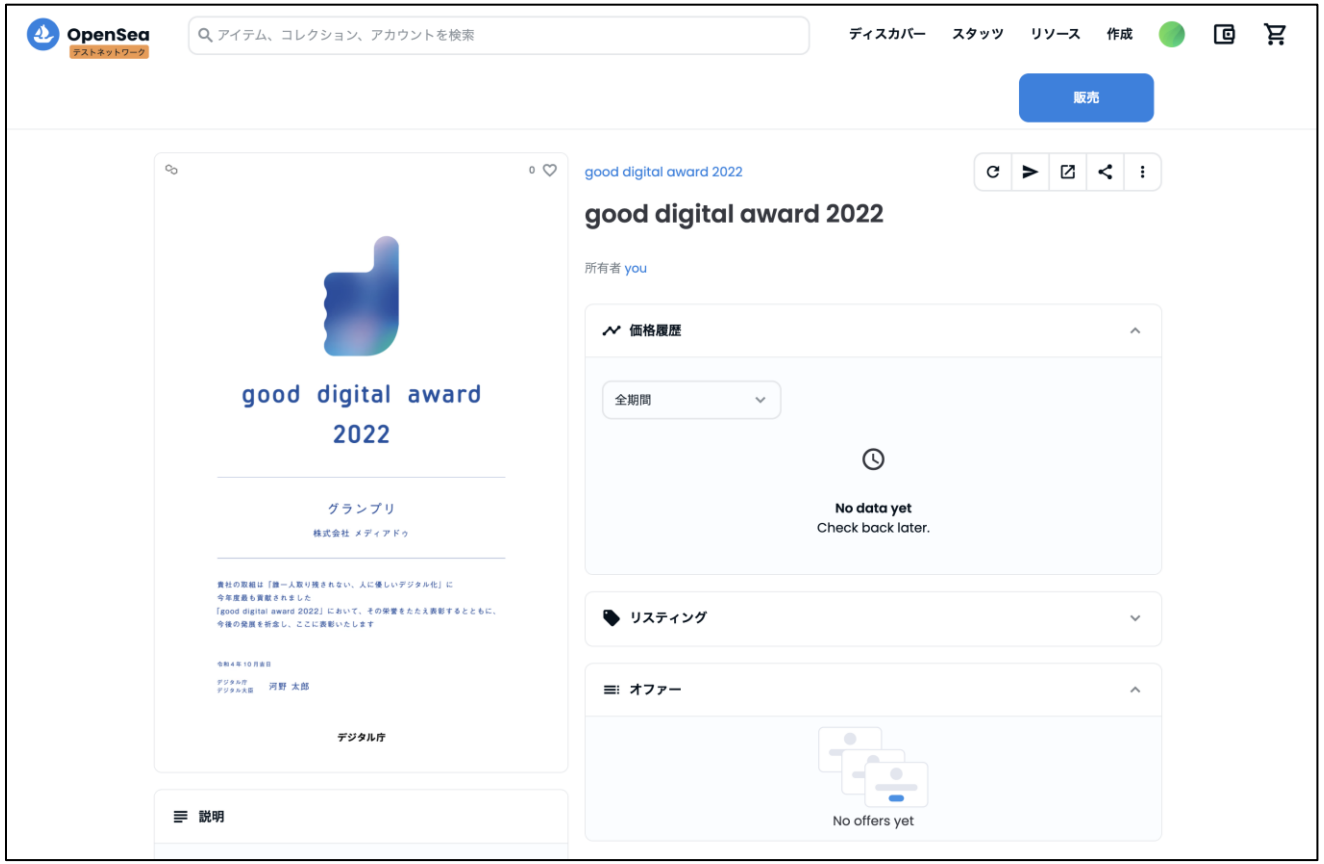
以下の要件を満たす形でシステムを実装した

- デジタル庁が発行した賞状であることを証明できる
- NFTとしても発行することで、受賞者のウォレットでも賞状が確認できる
- できるだけ分散型の技術を利用する
- 世界標準の仕組みに合わせる
- オープンな技術を採用する

ユーザー体験

本システムにより、受賞者が可能となること

デジタルの日特設サイト上で、W3C標準型式で認証済みの賞状画像を表示できる
（このページは、一般の閲覧者からも表示可能）



デジタル庁から送付するウォレットでログインすることで、Opensea 等のNFTマーケット上でデジタル賞状を表示できる
（販売したり譲渡することはできない）

Verifiable Credential (VC)を発行

Verifiable Credentials ＝「内容の検証がオンラインで可能な自己主権型のデジタル証明書」

W3Cが提唱する、自己主権型で検証が可能な資格証明書

【発行者】(Issuer) が【保持者】(Holder) に対して発行した証明書を第三者である【検証者】が検証することができるしくみ

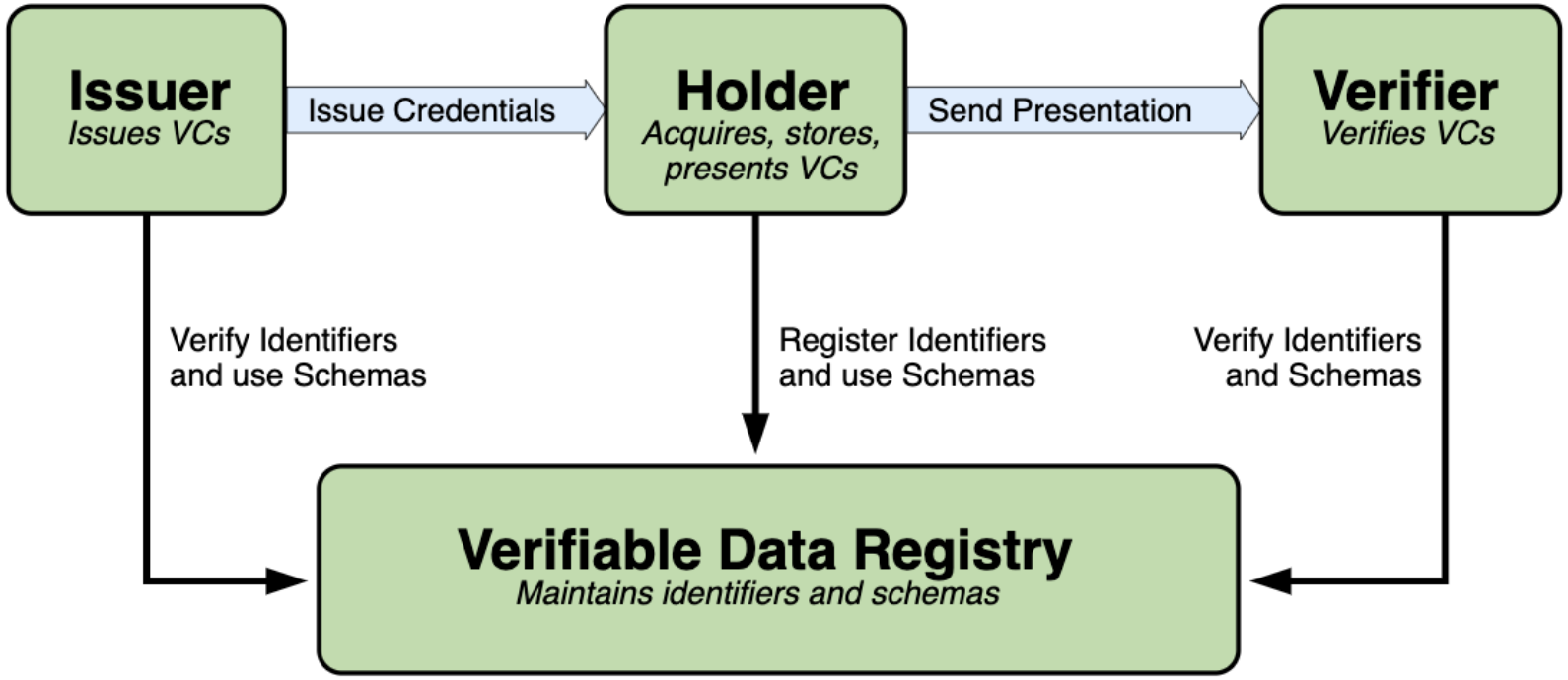


Figure 1 The roles and information flows forming the basis for this specification.

出典：Verifiable Credentials Data Model v1.1(W3C)

Blockcerts について

Verifiable Credential の中心的技術として、Blockcerts を活用した。

MIT Media Labと Learning Machine社が共同開発した
ブロックチェーン証明書の標準規格

W3C 標準の VC 規格に準拠している

今回発行したVCは、Blockcerts.org などでも確認できる

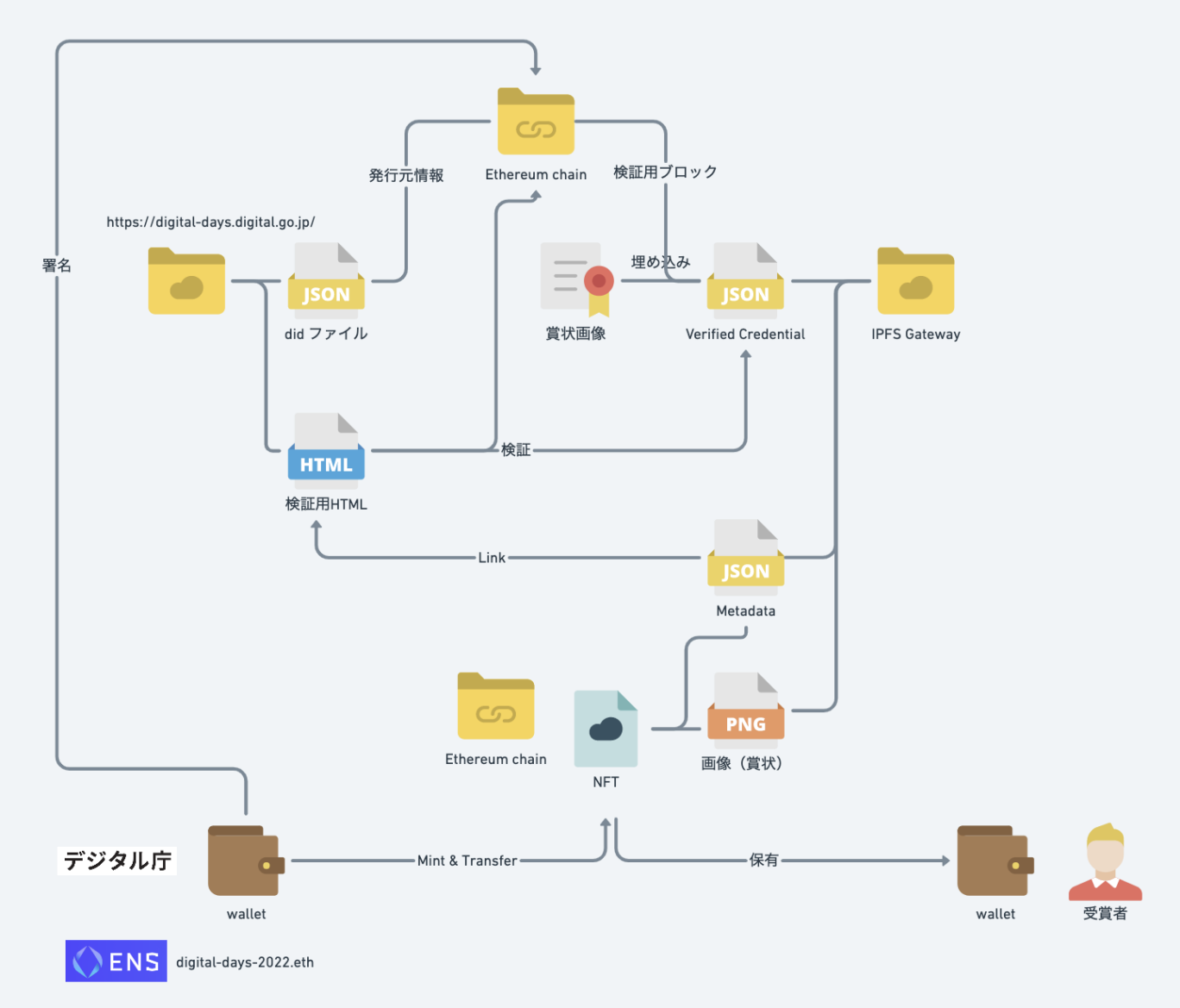
選定理由

- 今回のユースケースにマッチしている
- オープンソースである
- 世界的に利用されている
- 国内先行事例がいくつかある
- 千葉工業大学の仕組みがオープンソース化されている
  - https://github.com/pitpa/nft-vc

千葉工業大学の学修証明書
でも、Blockcerts を利用

技術的バックグラウンド

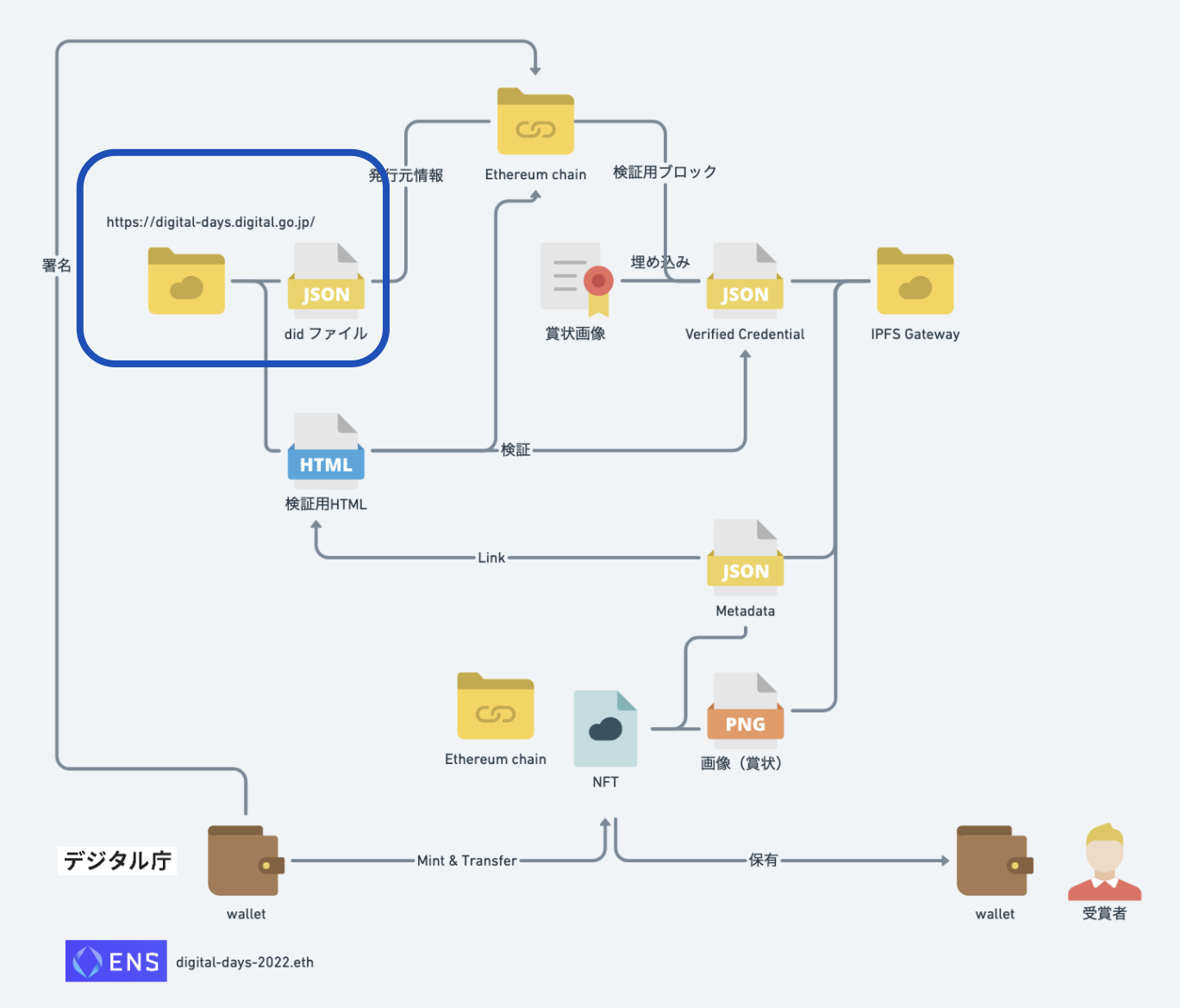
DID、Verifiable Credentials、譲渡不可NFTの組み合わせ



技術的バックグラウンド

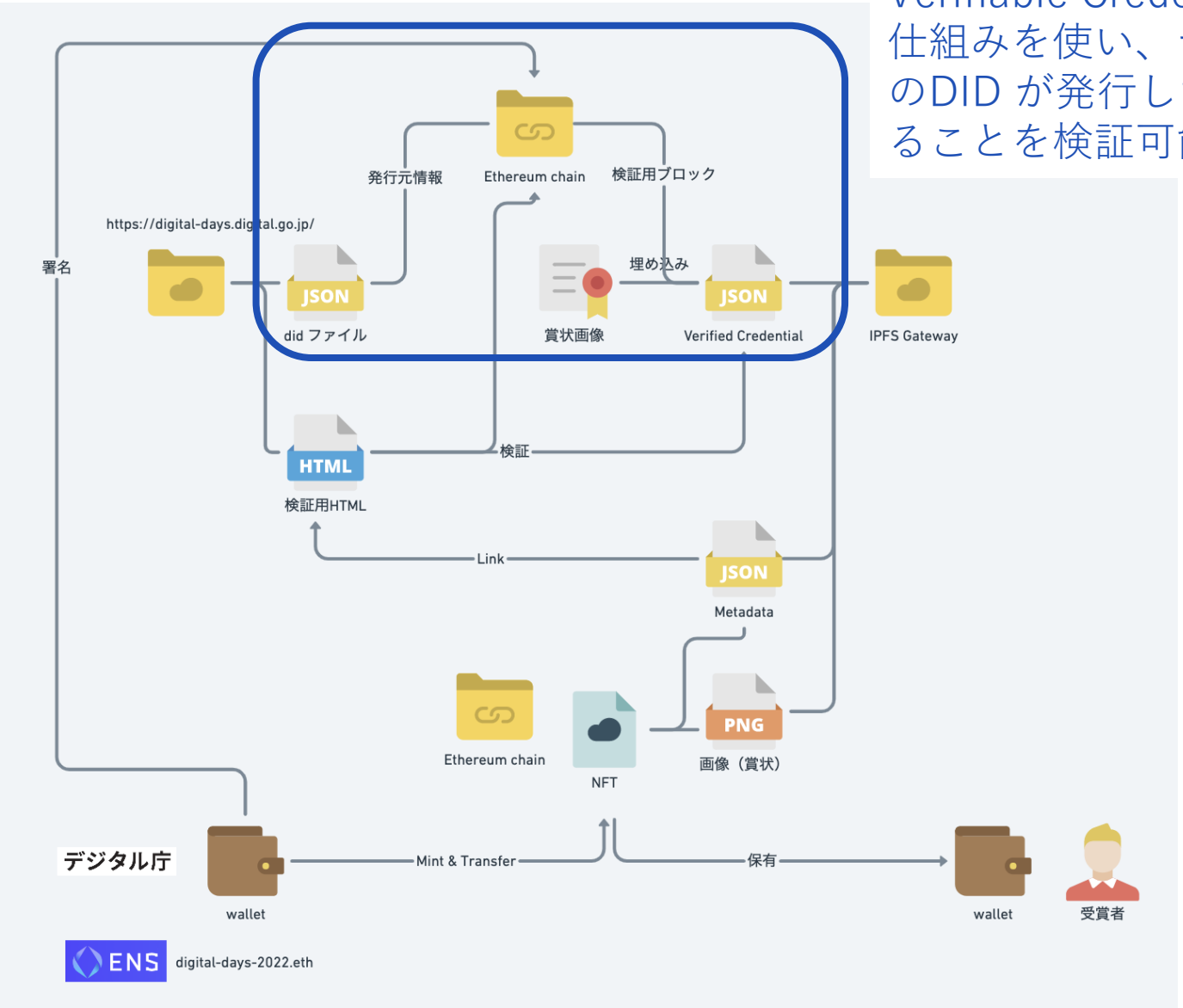
DID、Verifiable Credentials、譲渡不可NFTの組み合わせ

did:web を使い、
デジタル庁ドメインが
発行した賞状であるこ
とを示す



技術的バックグラウンド

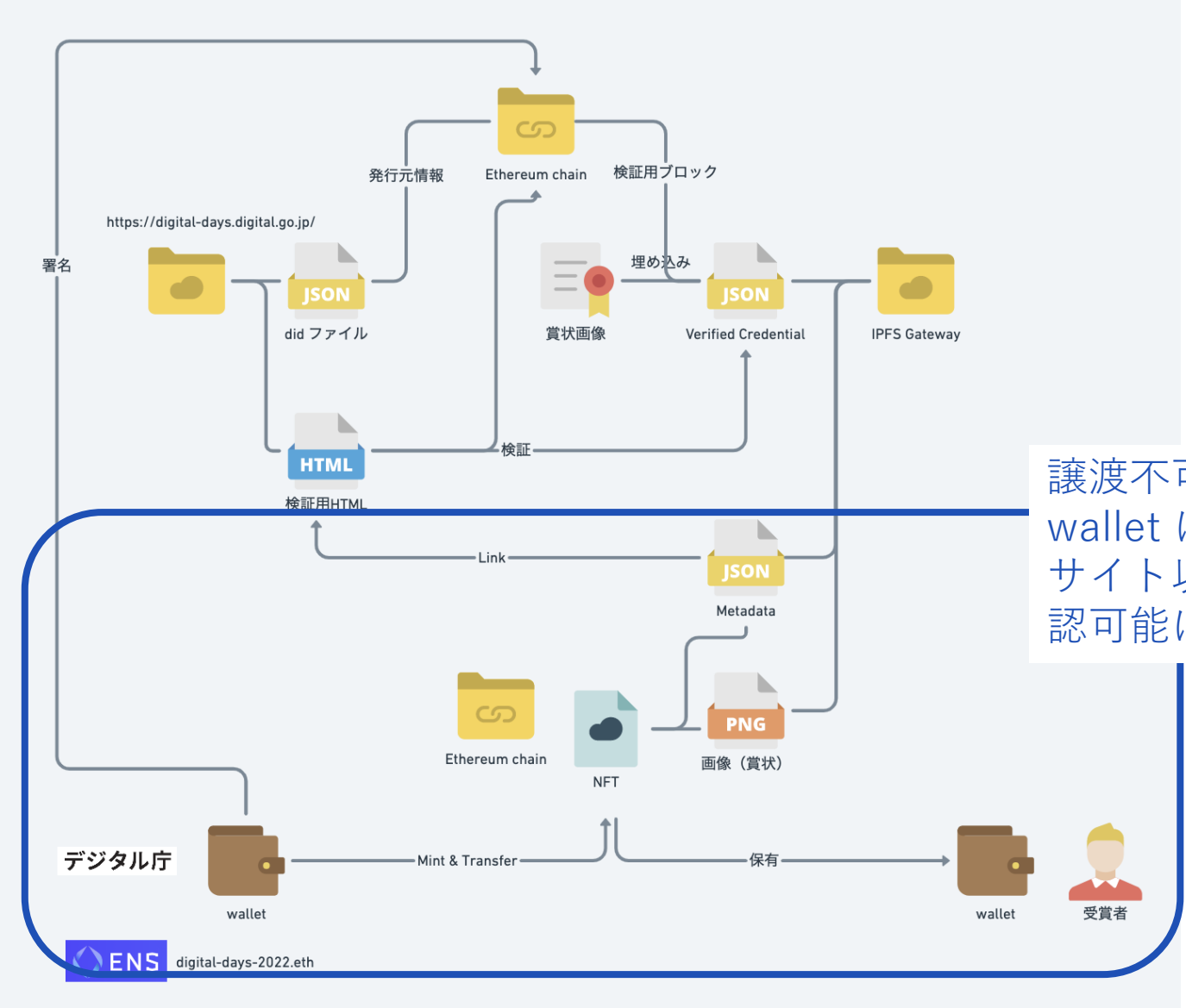
DID、Verifiable Credentials、譲渡不可NFTの組み合わせ



Verifiable Credentials の仕組みを使い、デジタル庁のDID が発行した賞状であることを検証可能にする

技術的バックグラウンド

DID、Verifiable Credentials、譲渡不可NFTの組み合わせ



譲渡不可NFTを、受賞者のwallet に送信。デジタル庁サイト以外からも賞状を確認可能にする

まとめ

good digital award の賞状を、デジタルでも発行する

以下の要件を満たす形でシステムを実装した

- デジタル庁が発行した賞状であることを証明できる
  → Blockcerts + DID の仕組みで実装
- NFTとしても発行することで、受賞者のウォレットでも賞状が確認できる
  → 譲渡不可NFTを発行し、受賞者にウォレットごと配布する
- できるだけ分散型の技術を利用する
  → DIDだけでなく、NFTやVCもIPFS上に配置
- 世界標準の仕組みに合わせる
  → W3C推奨の自己主権型の証明書（Blockcerts）を採用した
- オープンな技術を採用する
  → オープンソースの仕組みを採用した。
  デジタル庁の GitHub でもソースコードを公開予定

課題や対応

- 受賞者のウォレット配布について
  - ウォレットを持っている人は少ないことを想定し、デジタル庁でアカウントを作成、NFTを転送した上で秘密鍵と共に受賞者に送付。Metamask 等 にインポートしていただく方法で対応
- Wallet 紛失等への対応
  - （どこまで対応するかはあるが）VC には Revoke の仕組みがあるため、再発行は可能
- did ファイルを digital-days.digital.go.jp に置いているため、このサイトがなくなると検証ができなくなる
  - did:web メソッドを使うことの制約。発行エンティティのトラストをどこで確保するかは課題
- IPFS Gateway の永続性
  - NFTやVCの置き場に商用のIPFS Gateway を使っているが、課金をやめるとファイルが無くなる可能性がある
  - IPFS node を自前で運用する対策が考えられる。
  - VCもオンチェーンに乗せる選択肢もあるが、オンチェーンに書き込むと消せなくなるため、配慮が必要