Intelligible

Intelligible Identity and Certificate

BitNomos

Mirko Zichichi

Academic Supervisors:
Stefano Ferretti
Víctor Rodríguez-Doncel
Mentor:
Massimo Durante

Company Tutor:
Luca Cervone

Introduction: the problems

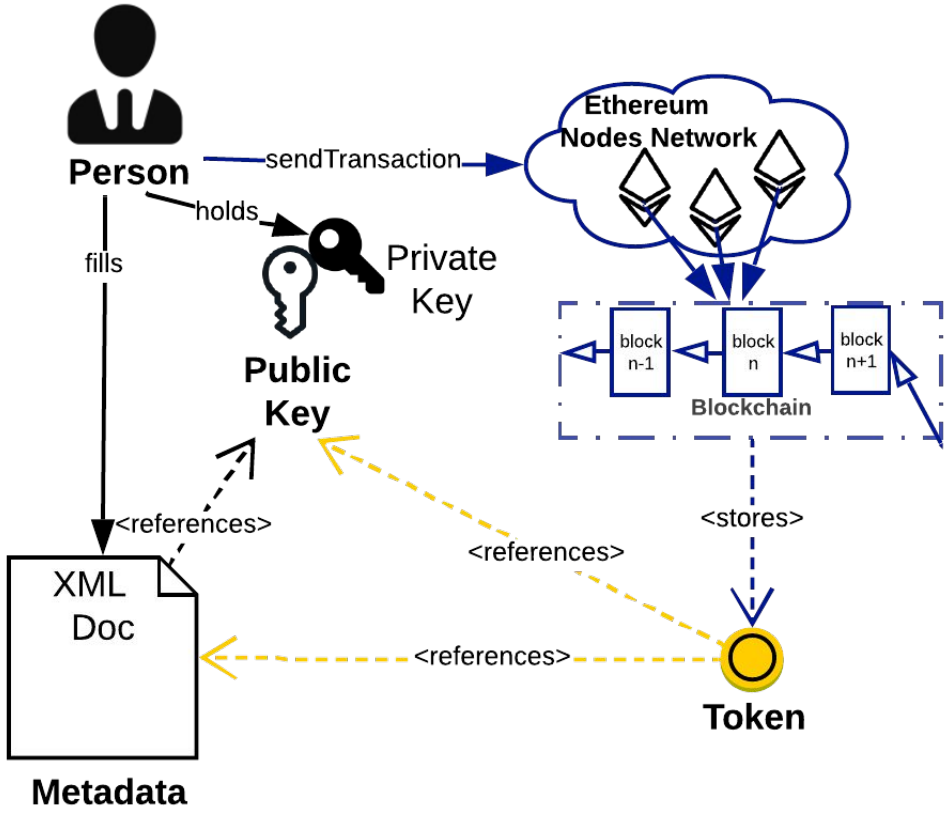
- Certificate verification paradigm based on centrality and hierarchy ->
  - decentralization in the verification of the authenticity of the claims of a digital certificate or online identity
  - resistant to counterfeiting and unauthorised duplication

- Digital certificates and licenses are usually not standalone documents ->
  - intelligible -> the individual is provided with the means to be made fully aware of their content
  - machine readable -> processing environment is provided with an operational and legal context
  - support verifiability and tracing back to what has caused a possible legal dispute

Intelligible Identity

Consists in a combination of:

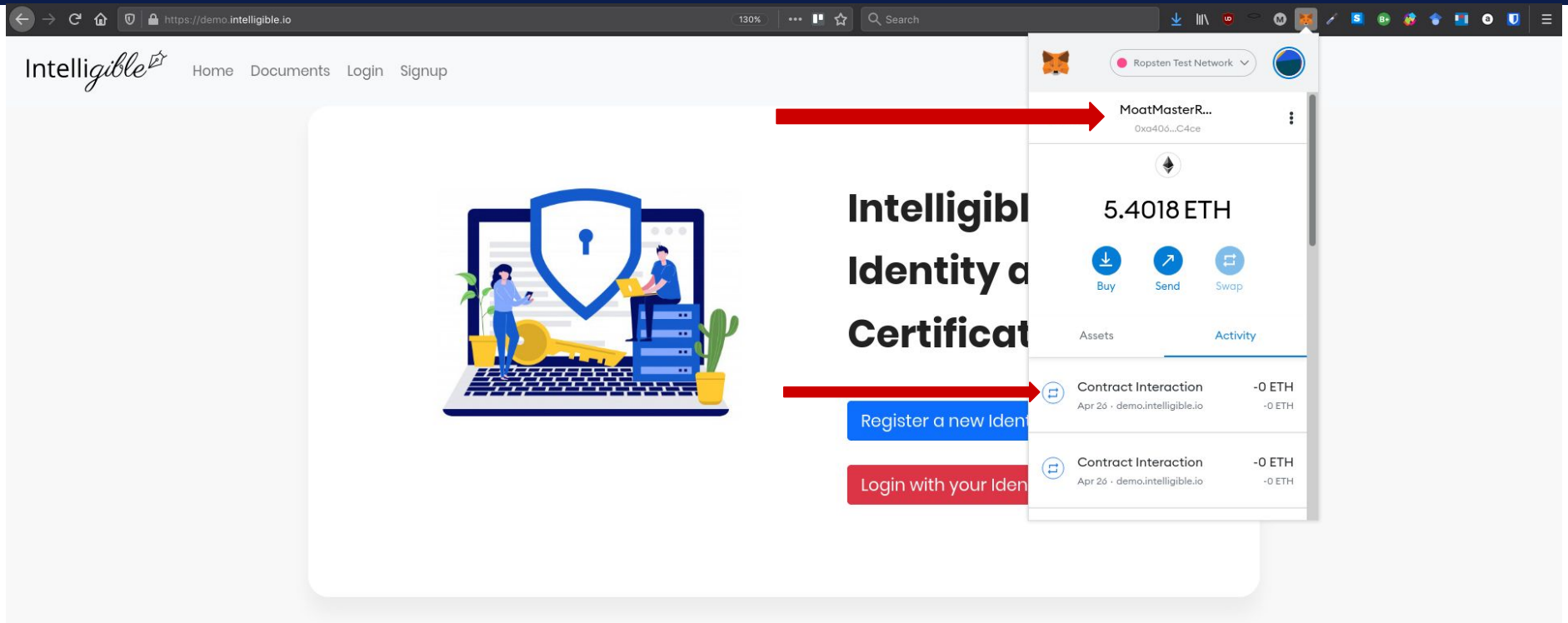
- A keypair -> (Public Key, Private Key)
- A token stored on the Ethereum blockchain
- An XML document stored off-chain for metadata



Intelligible Identity - Keypair

- The keypair consists in the basis for the identity authentication
- The public key is used to publicly authenticate the identity and it is stored publicly in the blockchain
- The private key is used to digitally sign documents and it is stored in the local device in a software wallet
- The implementation consists in the Ethereum Elliptic Curve Digital Signature Algorithm (ECDSA) for the keys generation and Metamask for the software wallet
- In the Ethereum blockchain the public key become an address

Intelligible Identity - Keypair



Intelligible Identity - Token

- A smart contract named “IntelligibleIdentity” is issued in the Ethereum blockchain and can be considered as a registry for issuing new Identities
- Such registry contains a list of Non Fungible Tokens, that represents the identity as an asset
- Each token is unique as it contains an immutable reference to an off-chain document containing the identity metadata
- The implementation consists in an ERC721 Token that contain an IPFS CID, i.e. the hash digest of the document

Intelligible Identity - XML document

- Is the document that contains the metadata of the Identity
- It includes all the references to actors, softwares and other documents involved in the creation and issuing of the Intelligible Identity
- Is digitally signed by the issuer (and the software)

idIssuer	*name*: Miles_Davis2021-03-04T15:56:50.229Z; *href*:/akn/eu/doc/intelligibleIdentity/person/Miles_Davis2021-03-04T15:56:50.229Z/;
issuerRole	*name*: Issuer; *href*: /akn/ontology/roles/intelligibleIdentity/issuer;
idReceiver	*name*: Miles_Davis2021-03-04T15:56:50.229Z; *href*: /akn/eu/doc/intelligibleIdentity/person/Miles_Davis2021-03-04T15:56:50.229Z/;
receiverRole	*name*: Receiver; *href*: /akn/ontology/roles/intelligibleIdentity/receiver;
issuerSoftware	*name*: IntelligibleSuite@0.1.0; *href*: /akn/eu/doc/object/software/IntelligibleSuite/ver@0.1.0.akn

Identity	*name*: Miles Davis; *email*: miles.davis@email.com;
Ethereum	*accountAddress:* 0x6A1303a53c75c9256c1dF7D88ADc7adCC788ffca; *registrySmartContract:* 0x7d4dD48cC245396C2Ad915E638fF9140E74B6840; *tokenId:* 307;

idIssuer signature	*0x57addbf9c2c80a820633edf57498f2880fcd48297d7a5de0cb7b74dd18c4db56302cd756e67213b98ae6dad57c40a1a90137bffc3091d357267f4e52de7e90aa1c*
issuerSoftware signature	*0x7986ae517cbe39eaadb7b9e7f258fa3f1c555c677e7ee3a2f868743b6d2092fb4277c044d8a610c68409ec25500e5c2d704746f558696b15bc92350bdec0d61f1c*

Intelligible Identity - Advantages

- Unique but yet decentralized registry for associate a public key to an identity
  - The registry allows to publicly identify and verify the public keys associated to the issuer and the receiver of the Intelligible Identity
  - The registry cannot be easily altered thanks to the immutability property of Ethereum smart contracts

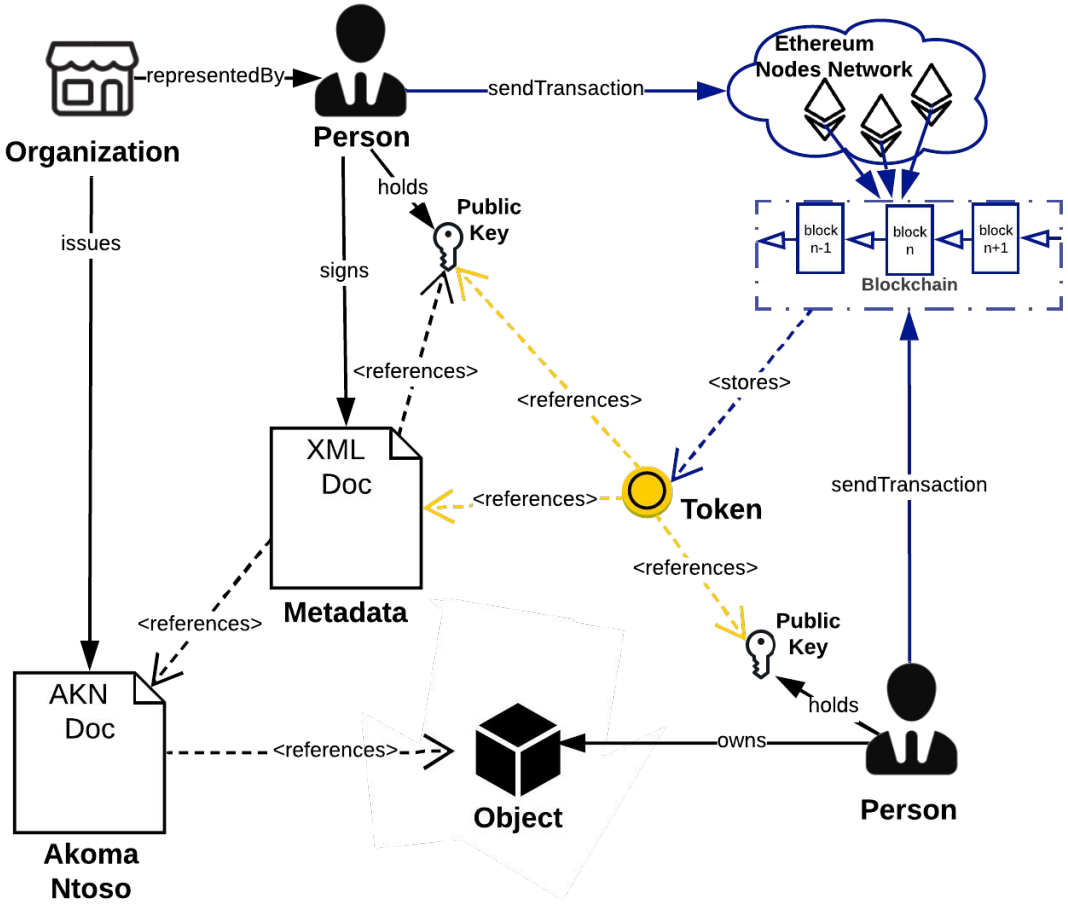
- Built-in linkability thanks to the use of standard and ontologies
  - The XML document can be used to represent W3C Decentralized Identifiers (DIDs) and other authentication standards
  - The metadata document enables the verification of one's identity in any other document where his digital signature has been placed
  - Although it is stored off-chain, it cannot be altered because its hash digest is stored within the token

- Great interoperability thanks to the use of Ethereum and ERC721 Non Fungible Token
  - Ethereum is currently the most used technology for building decentralized application and many websites already supports the ERC721 interface
  - This means that the Intelligible Identity can be implemented in several already functioning services with low effort

Intelligible Certificate

Consists in a combination of:

- A set of Intelligible Identities
- A token stored on the Ethereum blockchain
- An XML document stored off-chain for metadata



Intelligible Certificate - Identities

- An Intelligible Certificate is linked to two or more identities represented by Intelligible Identities, i.e. the ones who digitally sign
- An Intelligible Certificate might issued by an organization represented by a person with an Intelligible Identity
- The certificate receiver is another Intelligible Identity and an object he owns may constitute the purpose of the certificate
- The signatories receive the uncomplete certificate in a process that is traced in the blockchain

Intelligible Certificate - Token

- A smart contract named “IntelligibleCertificate” is issued in the Ethereum blockchain and can be considered as a registry as well, such as in the case of Identities
- For certificates, however, the writing to registry might be limited to the issuer organization and its members
- Therefore, there can be a registry (i.e. a smart contract) for each organization
- Also in his case Non Fungible Tokens represents the certificates as assets and contains an immutable reference to the off-chain XML document
- The implementation consists in an ERC721 Token that contain an IPFS CID, i.e. the hash digest of the document

Intelligible Certificate - XML document

- It includes all the references to actors, softwares and other documents involved in the creation
- Contains all the information related to the certificate and the certified entity (e.g. object)
- It can link to one or several Akoma Ntoso documents
- Is digitally signed by the issuer and the receiver (and the software)

certIssuer	*name*: IntelligibleCompany; *href*: /akn/eu/doc/intelligibleIdentity/organization/IntelligibleCompany;
certIssuer Representative	*name*: Miles_Davis2021-03-04T15:56:50.229Z; *href*: /akn/eu/doc/intelligibleIdentity/person/Miles_Davis2021-03-04T15:56:50.229Z/;
certReceiver	*name:* MarcelPoint2021-03-04T16:00:56.484Z; *href:* /akn/eu/doc/intelligibleIdentity/person/MarcelPoint2021-03-04T16:00:56.484Z/;
certEntity	*name*: CertifiedEntity; *href*: /ipfs/QmcyQoP9W9kLq9Eg3XVDoG3Y89E7DCXmVPYfEaNSJjtpRX;

Certified Entity Information	*certificateType:* GDPRCompliance; *certifiedEntityType:* software; *certificateObject:* mochav8.3.0;
Ethereum	*registrySmartContract:* 0xAD04614C3A27f5eAe8E8252e3D3c4b4A8bD2eb82; *tokenId:* 155;

certIssuer Representative signature	*0x36b194ca916e5449e39dbf6c464a30ffb277554c742ece81c0d1ab35a86e1044100c1746c6b2046118871d83535d7d0b209eff912af311ff1c586e53c88d6e8c1b*
certReceiver signature	*0xfe568c3eb256b12d4f85792da4098bd89f87f0010ca063bab103ee11ec4946f648fdf76ad5de08aeeaf67a8933dfedf38f2c1eed2f86c5ade881452ba554a67e1b*

Intelligible Certificate - Advantages

- Interoperability at smart contract level
  - Each Organization can have its own registry able to “talk” with other registries directly on the blockchain
  - A hierarchy of registries can be created but certificates will always be represented by Non Fungible Tokens

- Public verifiability of Certificates without accessing to the content
  - Each certificate is represented through the XML document whose hash digest is stored on the blockchain. This means that any alteration can be verified if one has access to the document, but the contents cannot be read by anyone without access.
  - The token representation can easily be used to track the lifecycle of the certificate.

- The link to an Akoma Ntoso document allows continuity of usage when referring to other legal and plain documents already marked-up that relate to the certificate lifecycle.

- The combination with Intelligible Identities allows an easy signature verification

Intelligible Certificate Use Case