



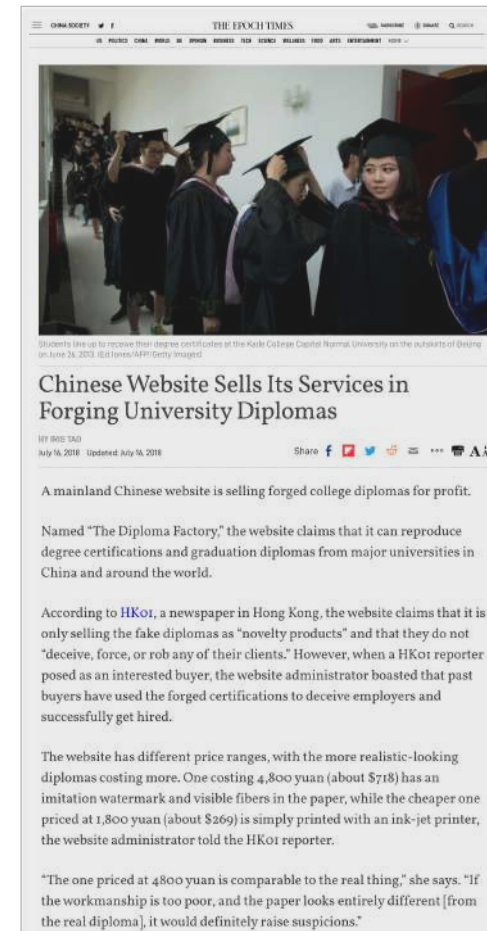
# Ordre du jour

- Vérification des diplômes
- La Blockchain
- Les Smart Contracts
- Solution durable
- La solution en détail
- Les alternatives

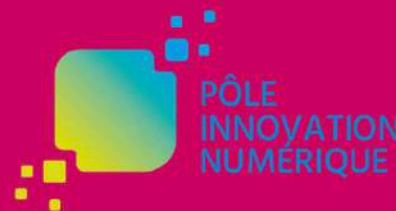
# C'est facile de créer des faux diplômes



Les diplômes scannés peuvent être modifiés



Accélérateur de Sciences  
et services numériques



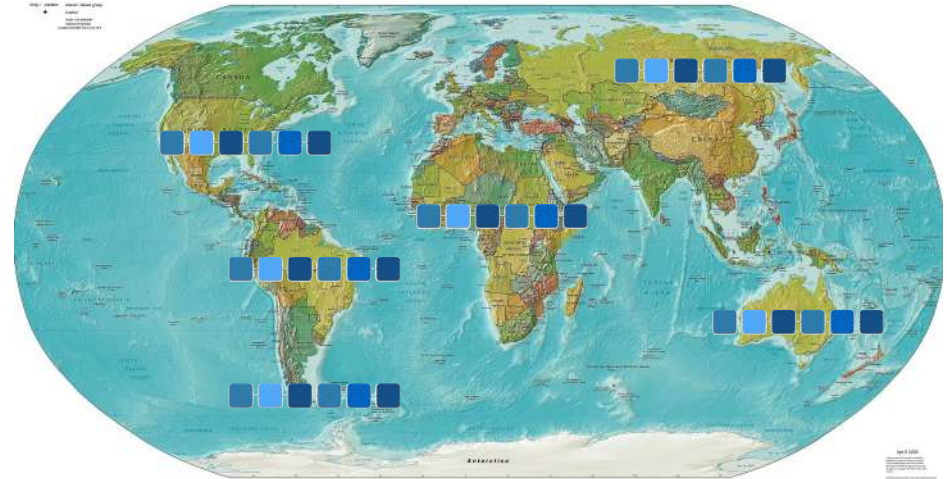
UNIVERSITÉ  
DE GENÈVE

# Comment vérifier ?

- Travail manuel
- Faire confiance à un numéro de téléphone, un email ?
- Preuve de la vérification ?
- Que faire quand l'université n'est pas/plus disponible ?
- Protection des données

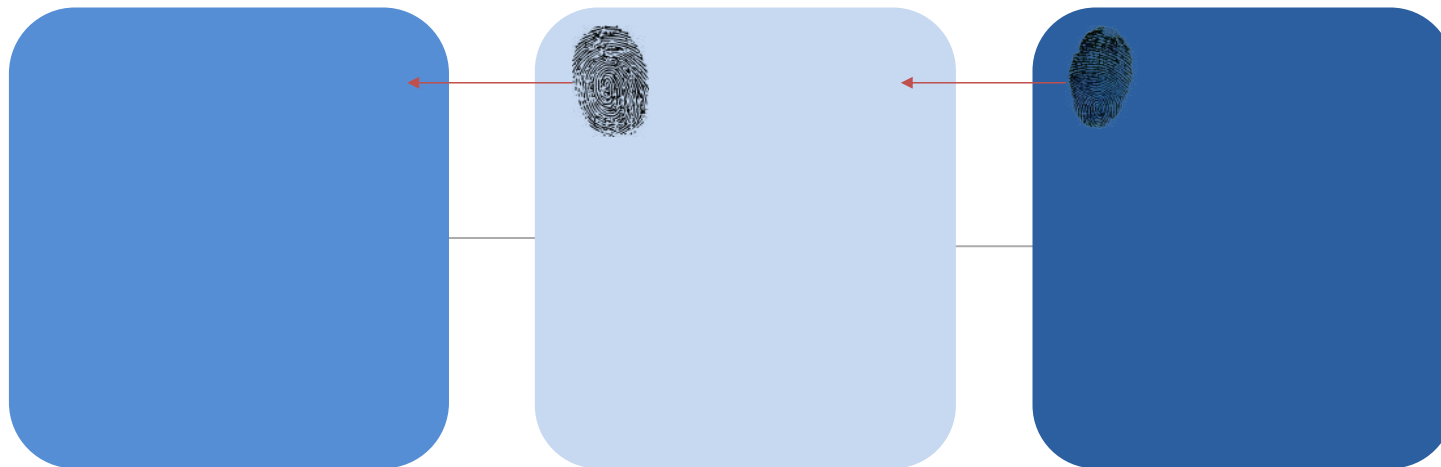
# Blockchain

- Stockage des données
- Immuable et permanente
- Distribué dans le monde
- Décentralisé
- Sécurisé par des algorithmes



# La blockchain est chaînée par les valeurs hashes

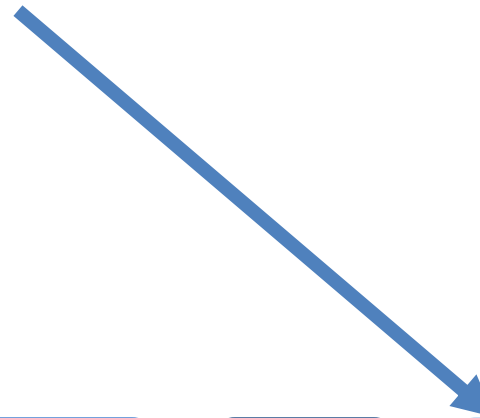
- Pour modifier un bloc, il faut aussi modifier tous les blocs après
- La création des blocs nécessite beaucoup de puissance de calcul (proof of work), beaucoup de coins (proof of stake) ou des permissions (proof of authority)



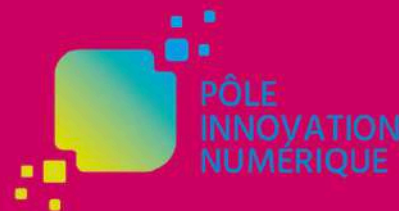
# Comptes Blockchain

- Les comptes Blockchain consiste d'un pair des clés publique et privée.
- Toutes les transactions d'un compte sont signées par une signature électronique.
- Les nœuds d'une blockchain vérifient la signature des transactions.

# Vérification d'un document par une blockchain



Accélérateur de Sciences  
et services numériques



UNIVERSITÉ  
DE GENÈVE



# Questions ouvertes

- Comment vérifier cet hash ?
- Comment révoquer un diplôme ?
- Est-ce que c'est l'université qui à mis le hash ?

# Les smart contracts

Deux significations distinctes :

Petits logiciels pour une blockchain programmable

- transparent
- immuable
- protégé contre des manipulations

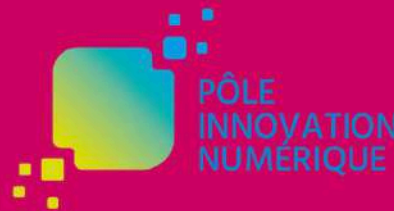


Un contrat juridique

- défini en code et pas en jargon juridique
- exécuté automatiquement
- conclut par transaction électronique



Accélérateur de Sciences  
et services numériques



UNIVERSITÉ  
DE GENÈVE

```

function setAdmin(address _admin) onlySuper() external{
    admin=_admin;
}

function setUser(address _user) onlySuper() external {
    user=_user;
}

function addDiploma(uint256 _hash1,uint256 _hash2, Status _status) onlyUser() external
{
    if(!(_hash1==0)){emit ErrorMessage('hash1 already exists'); return;}
    if(!(_hash2==0 || hashes[_hash2]==0)){emit ErrorMessage('hash2 already exists'); return;}
    if(!(_hash1!=_hash2)){emit ErrorMessage('hash1 and hash2 need to be different. If only one hash leave hash2=0'); return;}
    Diploma memory diploma = Diploma({hash1: _hash1, hash2: _hash2,numberEntries: 0});
    uint24 diplomaNr=uint24(diplomas.push(diploma));
    diplomas[diplomaNr-1].entries[0]=Entry(now,msg.sender,_status);
    diplomas[diplomaNr-1].numberEntries=1;
    hashes[_hash1]=diplomaNr;
    hashes[_hash2]=diplomaNr;
}

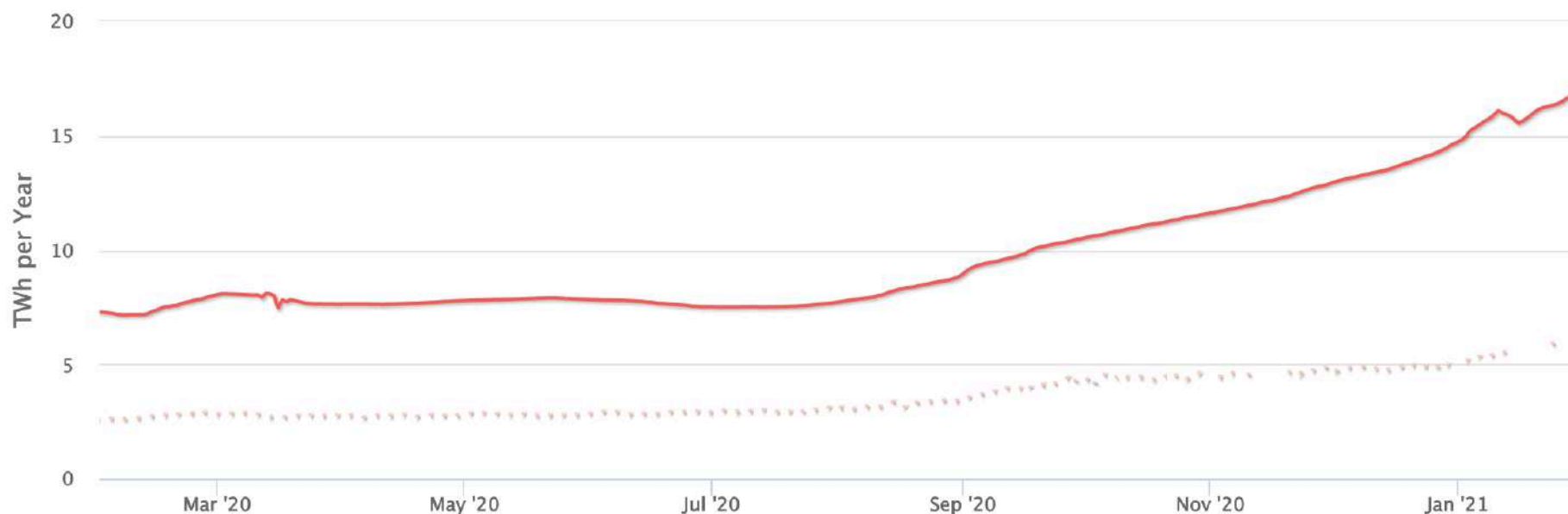
function changeDiploma(uint256 _hash, Status _status) onlyAdmin() external
{
    if(!(_hash!=0)){emit ErrorMessage('hash does not exist'); return;}
    uint24 diplomaNr=hashes[_hash];
    diplomas[diplomaNr-1].entries[diplomas[diplomaNr-1].numberEntries]=Entry(now,msg.sender,_status);
    diplomas[diplomaNr-1].numberEntries++;
}

function requestDiploma(uint256 _hash) external view returns (Status, string memory, string memory, uint, uint, uint, uint)
{
    if(hashes[_hash]==0) return(Status.Fail,statusString[uint24(Status.Fail)], 'No diploma registered with the hash given.',0,0,0,0);
    uint24 diplomaNr=hashes[_hash];
    Status status=diplomas[diplomaNr-1].entries[diplomas[diplomaNr-1].numberEntries-1].status;
    return (status, statusString[uint24(status)], string(abi.encodePacked('Diploma found with status ', statusString[uint24(status)])));
}

```

# Une solution durable ?

Ethereum Energy Consumption Index Chart



Source : <https://digiconomist.net/ethereum-energy-consumption/>

17 TWh for 500 mio transactions  $\hat{=}$  34 kWh par transaction

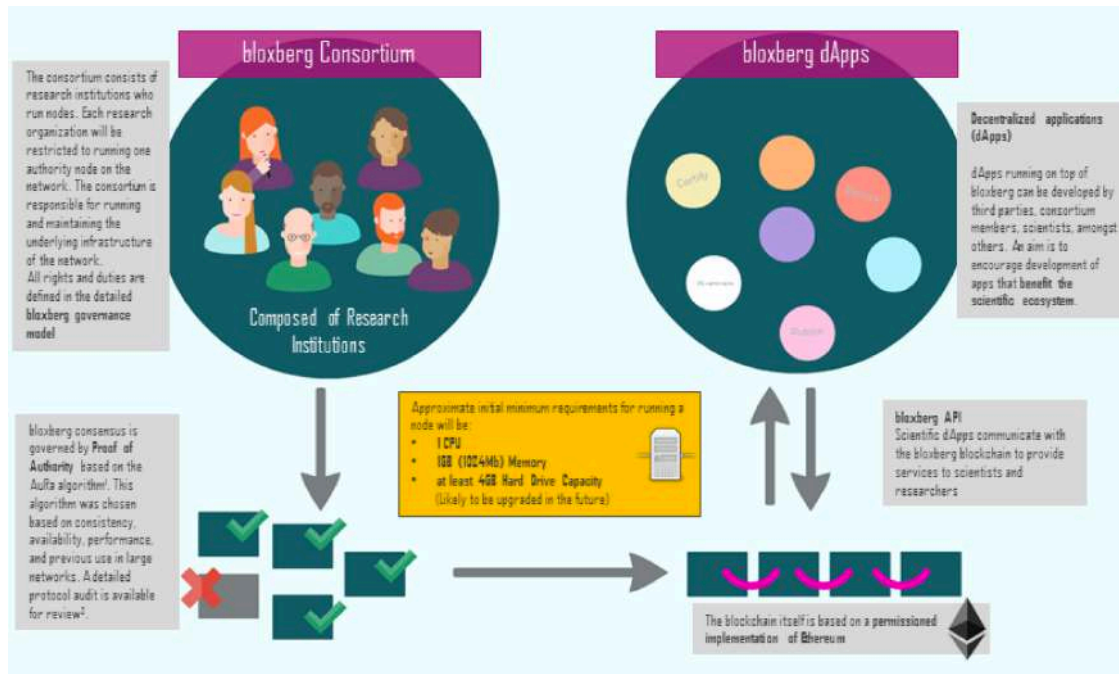
Accélérateur de Sciences  
et services numériques




UNIVERSITÉ  
DE GENÈVE

# bloXberg

## The Trusted Research Infrastructure



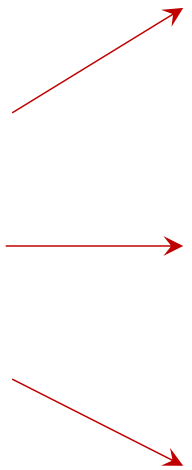
Organization	Country	Contact
 Max Planck Society	Germany	Sandra Vengadasalam
 UNIVERSITY of NICOSIA	Cyprus	Soulla Louca
 UCL	UK	Tomaso Aste
 IT University of Copenhagen	Denmark	Roman Beck
 UNIKASSEL VERSITÄT	Germany	Walter Blocher
 Georgia Tech	USA	Vijay K. Madiseti
 Tepper SCHOOL OF BUSINESS	USA	Sevin Yeltekin
 University of Johannesburg	South Africa	Maria Frahm-Arp
 UNIVERSITY OF SARAJEVO School of Economics and Business	Bosnia and Herzegovina	Zlatko Lagumdžija
 ETH Zürich	Switzerland	Sven Koessling
 UNIVERZITET U BEOGRADU	Serbia	Aleksandar Markovic

Accélérateur de Sciences et services numériques



UNIVERSITÉ DE GENÈVE

# Est-ce que c'est nécessaire d'utiliser une blockchain ?



Validation par un serveur de l'université dépend d'un serveur de l'université ou d'un tiers.



Révocation d'un diplôme n'est pas possible.

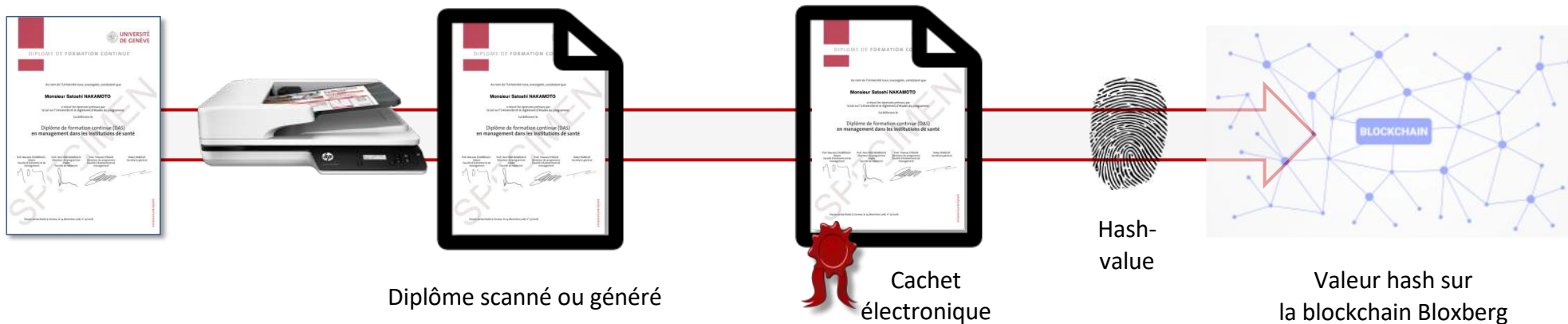


Est-ce que Bloxberg va encore exister en 50 ans ?

## Les besoins

- Sécurité
- Pérennité
- Autonomie
- Ergonomie
- Automatisable
- Légalité
- Protection des données
- Révocabilité
- Intégrable
- Durable

# Combination of 3 Verification Techniques



Vérification par un serveur de l'Université de Genève



Vérification du cachet électronique



Vérification directe contre la Blockchain

Accélérateur de Sciences et services numériques



UNIVERSITÉ DE GENÈVE

# UNIGE ECERT

Le POC offre 6 chemins  
de vérifications

## ONLINE VERIFICATION OF DIPLOMAS UNIVERSITY OF GENEVA

Forged diplomas are a sad reality. When presented with a PDF-copy of diploma, it is often not possible to tell whether the diploma is real.

In a pilot project the University of Geneva offers five ways to verify a diploma:

- Verify the diploma online through the id of the diploma (can be deactivated for privacy reasons)
- Verify the diploma online through the data on the diploma
- Verify the original pdf file of the diploma online

### Verify diploma online

- Verify the electronic seal off-line in Acrobat Reader

[See here how the verification in Acrobat Reader works](#)

- Verify the diploma directly against the Blockchain Ethereum

[See here how you can directly verify a diploma against the Blockchain Ethereum](#)

Accélérateur de Sciences  
et services numériques



UNIVERSITÉ  
DE GENÈVE



## UNIGE ECERT

## VALIDATE DIPLOMA

This page allows you to check validity of diploma using it's fields or using official diploma file (PDF/A).

Verify by ID    Verify by Data    Verify Original PDF

**Student informations**

Student name(s)

Student first name(s)

Student birthdate

**Diploma informations**

Diploma type (CAS, MAS, MBA)

Diploma name

Diploma note

Diploma issue date

Diploma number

Diploma identifier

Institution

Faculty

Un app Web qui offre 3 possibilités de vérification :

- Par l'ID
- Par l'ID+des données
- Par le fichier original



Specimen Diploma for Testing (TEST)

Un diplôme  
vérifié

Online verification of diploma for

**NAKAMOTO SATOSHI**

**1989-01-09**

Centre Universitaire d'Informatique

Diploma number  
25/2018

Diploma identifier  
NDBiMjQoMTeyNjQx

Diploma issue date  
2018-12-14

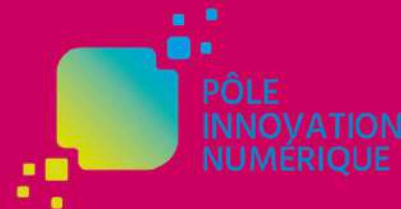
**SPECIMEN DIPLOMA FOR TESTING (TEST)**  
**CAS Blockchain & DLT**

with Distinction

Verified 2019-01-18 at 23:14

This entry has been verified (2019-01-18 at 23:14) with our internal database and the blockchain smart contract.  
(0xEg5DgEfs9a4AB1d2d39062d4cE276F88b005016f)

Accélérateur de Sciences  
et services numériques



UNIVERSITÉ  
DE GENÈVE

# Architecture de vérification

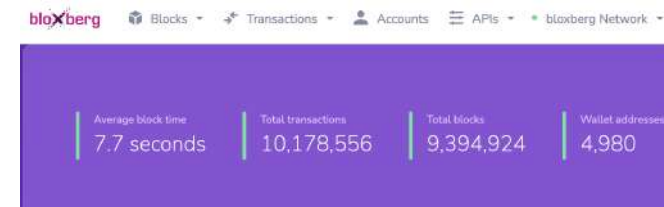
- utiliser l'APP de l'université →



- utiliser l'API de l'université →



- utiliser un nœud existant →



- propre nœud Bloxberg



# Protection des données

- Est-ce que le hash sur Bloxberg est considéré comme donnée à caractère personnel ?
- Est-ce que la visibilité des révocations est justifiée ?

# Alternatives

- Services externes, commerciales
  - pérennité ?
  - accès indépendant ?
- Blockchains publiques
- EBSI / ESSIF

# EBSI / ESSIF

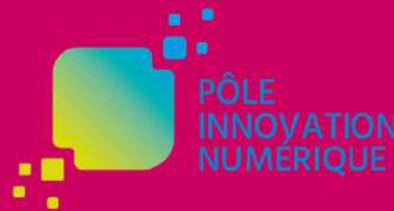


European Blockchain Services Infrastructure (EBSI)

European Self-Sovereign Identity Framework (ESSIF)

- Visibilité d'une révocation
- Pas besoin de séparer le nom et le diplôme
- Nécessite un wallet – convivialité (usability)

Accélérateur de Sciences  
et services numériques



UNIVERSITÉ  
DE GENÈVE

