Master en Ingénierie des Systèmes d'Information en Entreprise

AUTHENTIFICATION DE DOCUMENTS ADMINISTRATIFS À L'AIDE DE LA BLOCKCHAIN

Encadré par :

Dr. Yaya TRAORE

Maître de conférences en Informatique

Présenté par :

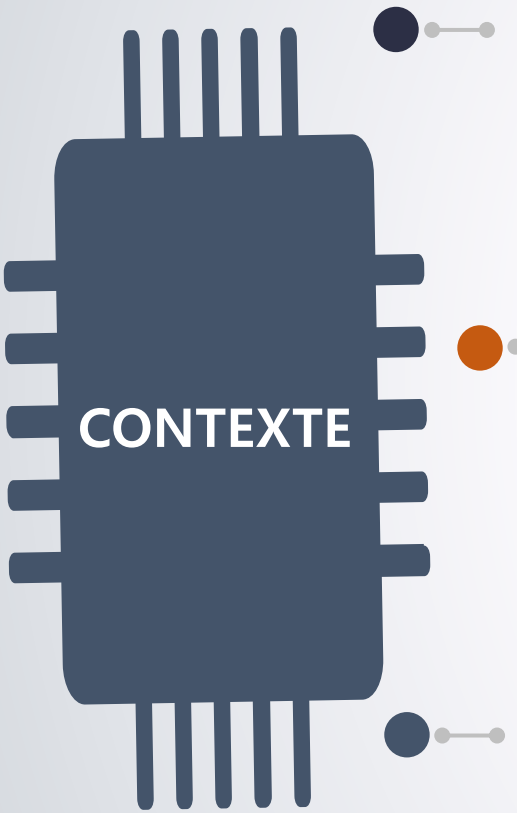
M. HIEN Zilèdem Pierre Canisius

Année universitaire : 2023-2024

PLAN

1. Introduction
2. État de l’art
3. Méthodologie
4. Implémentation
5. Démonstration
6. Conclusion

INTRODUCTION



Les documents administratifs ont toujours joué un rôle central non seulement dans le fonctionnement de l'Administration mais aussi dans la relation entre l'Administration et ses usagers/clients.

Cependant, le phénomène de documents administratifs numériques falsifiés ou d'origine douteuse est grandissant.

Conséquences :

- Crise de confiance entre usager/client et Administration;
- Perte de temps énorme aux structures qui restent en veille;
- Des ressources financières et humaines utilisées pour des opérations d'authentification.

Quel outil pour prévenir et/ou détecter les tentatives de falsification de documents administratifs ?

La technologie blockchain peut-elle garantir l'authenticité des documents administratifs de façon plus sécurisée, transparente et efficace ?

- Proposer une approche d'authentification de documents administratifs à l'aide de la blockchain.
- Mettre en place une DApp basée sur l'approche et qui offre la possibilité de vérifier l'authenticité de documents administratifs.

ÉTAT DE L'ART

CONCEPTS DE BASE : Document administratif

Sont considérés comme documents administratifs : « les documents produits ou reçus, dans le cadre de la mission de service public, par l'État, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission ».

Loi N°051-2015/CNT portant droit d'acces a l'information publique et aux documents administratifs, article 4, p.4

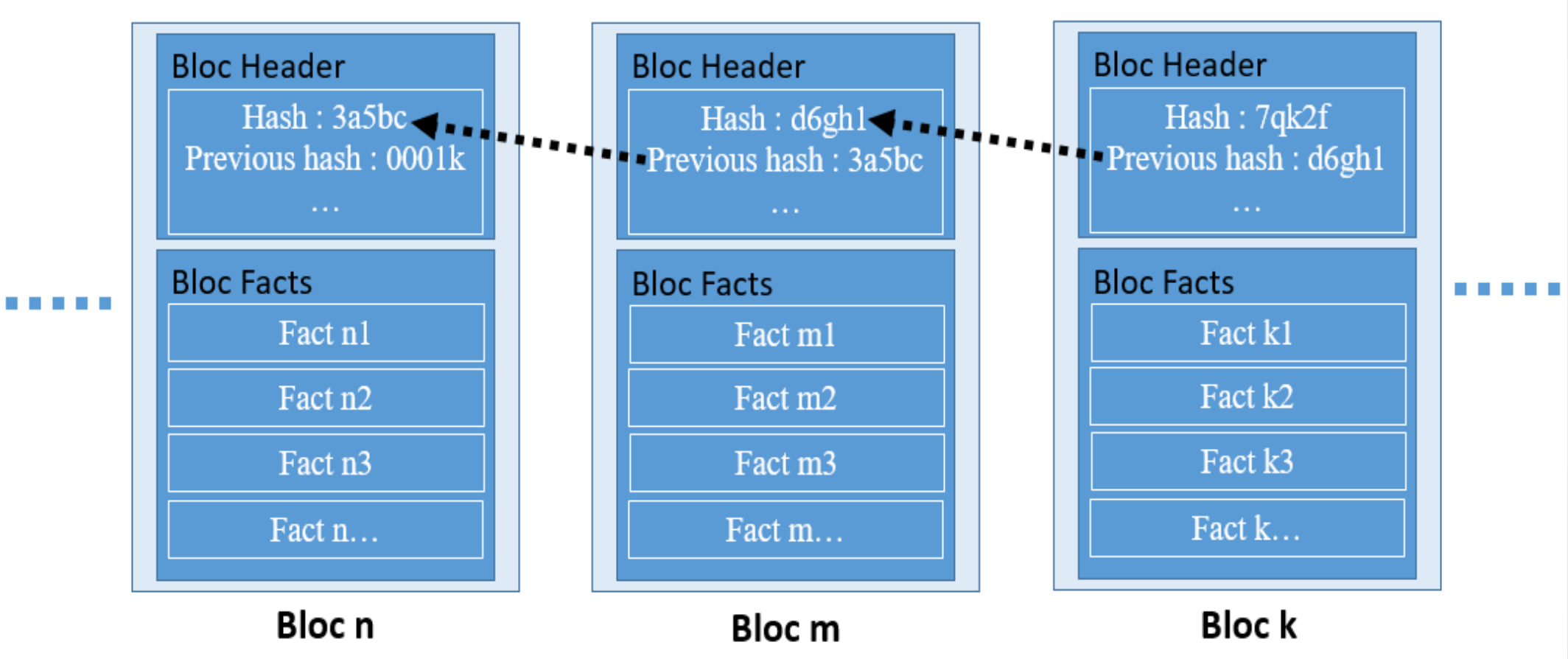
CONCEPTS DE BASE : Authentification de document

L'authentification d'un document est un processus par lequel un système informatique ou un humain prouve ou certifie qu'un document est authentique. Et un document est dit authentique s'il s'agit de l'original, ou d'une copie conforme à/de l'original après vérification et validation par un sujet habilité ou compétent.

CONCEPTS DE BASE : Blockchain

- Selon le Mathématicien *Jean-Paul Delahaye*, c'est : « un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible ».
- Ou encore une technologie numérique de stockage chronologique et de transmission d'informations sous forme de blocs reliés les uns aux autres de manière sécurisée et sans autorité centrale.

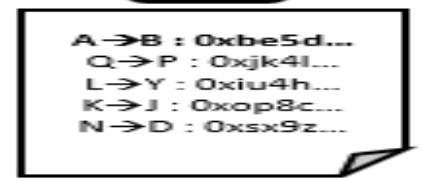
CONCEPTS DE BASE : Blockchain



1

(1) A initie une transaction vers B. Les données de la transaction peuvent être de l'argent, un contrat, un fichier, ...

2

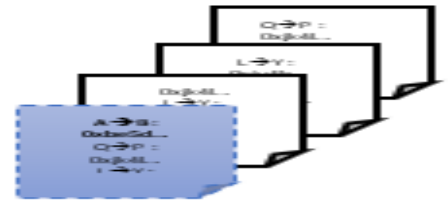


(2) La transaction est **inscrite dans un bloc** qui pourrait déjà contenir plusieurs autres opérations.

3

(3) Les transactions du bloc sont **soumises à un réseau** blockchain. Elles sont **vérifiées** et acceptées par les membres du réseau via un mécanisme de consensus. Ceux-ci (en ayant accès à la chaîne de blocs précédents) entrent donc en compétition pour valider le bloc.

4



(4) Si le bloc contenant les transactions est **validé**, il est **daté et ajouté** à la chaîne de blocs précédents.

5

(5) La transaction est confirmée entre A et B. B peut donc recevoir la transaction.

6

(6) L'historique des transactions est conservé dans un registre crypté auquel tous les membres du réseau ont accès. Ces membres s'assurent de l'impossibilité d'une corruption de la blockchain par quelqu'un qui souhaiterait ajouter ou retirer des transactions au registre.

Etape 1

Etape 2

Etape 3

MÉTHODES D'AUTHENTIFICATION ET TRAVAUX EXISTANTS

Ref.	Méthodes ou techniques	Technologies/ Protocoles	Avantages	Limites
[24]	**Technique de signature numérique**	PKI + Algorithmes (RSA, ECDSA, …) + PAdES + CAdES + OpenSSL + autres	• adaptée pour doc électroniques jurid et admin • prouve l'identité de l'auteur et l'intégrité du doc	• nécessité d'avoir une PKI et un cadre règlementaire
[36]	**Technique de hachage ou empreinte numérique**	Algorithmes de hachage (SHA-2, SHA-3) +OpenSSL + autres	• prouve l'intégrité du doc	• ne prouve pas l'identité de l'auteur • utilisé en complément avec une signature numérique
[8]	**Technique d'horodatage électronique**	RFC 3161 + Autorité de certification + Adobe Timestamp Server + Blockchain + autres	• adapté pour doc électroniques jurid et admin • prouve qu'un doc existait à une date donnée et qu'il n'a pas été frauduleusement modifié ou antidaté	• utilisé en combinaison avec une signature numérique et une empreinte numérique du doc

MÉTHODES D'AUTHENTIFICATION ET TRAVAUX EXISTANTS

Ref.	Méthodes ou techniques	Technologies/ Protocoles	Avantages	Limites
[35] [31]	**Technique des RFID et codes QR**	QR Code + BD + puce RFID/NFC + autres	• adaptés pour doc papier nécessitant une vérification rapide	• mise en œuvre relativement complexe et coûteuse (RFID) avec de potentielles failles de sécurité (QR Code) • non adapté pour doc électroniques
[4] [21]	**Technique Blockchain**	Ethereum + Smart contracts + P2P + autres	• adaptée pour doc électroniques de plusieurs types • prouve l'horodatage et l'immuabilité (donc l'existence du document) • prouve l'intégrité de doc • vérification possible par le public et sans autorité centrale	• implique plusieurs technologies émergentes • complexe à mettre en œuvre

POSITIONNEMENT

Au regard des travaux réalisés dans le domaine, nous avons adopté la technique de Blockchain Ethereum en combinant l'utilisation d'un contrat intelligent, de la signature numérique en s'appuyant sur la technique à clés asymétriques ECDSA avec une courbe elliptique secp256r1, de l'horodatage électronique, et de la technique de hachage basé sur l'algorithme SHA-256.

Pour nos expérimentations, nous choisissons les communiqués officiels comme type de documents administratifs.

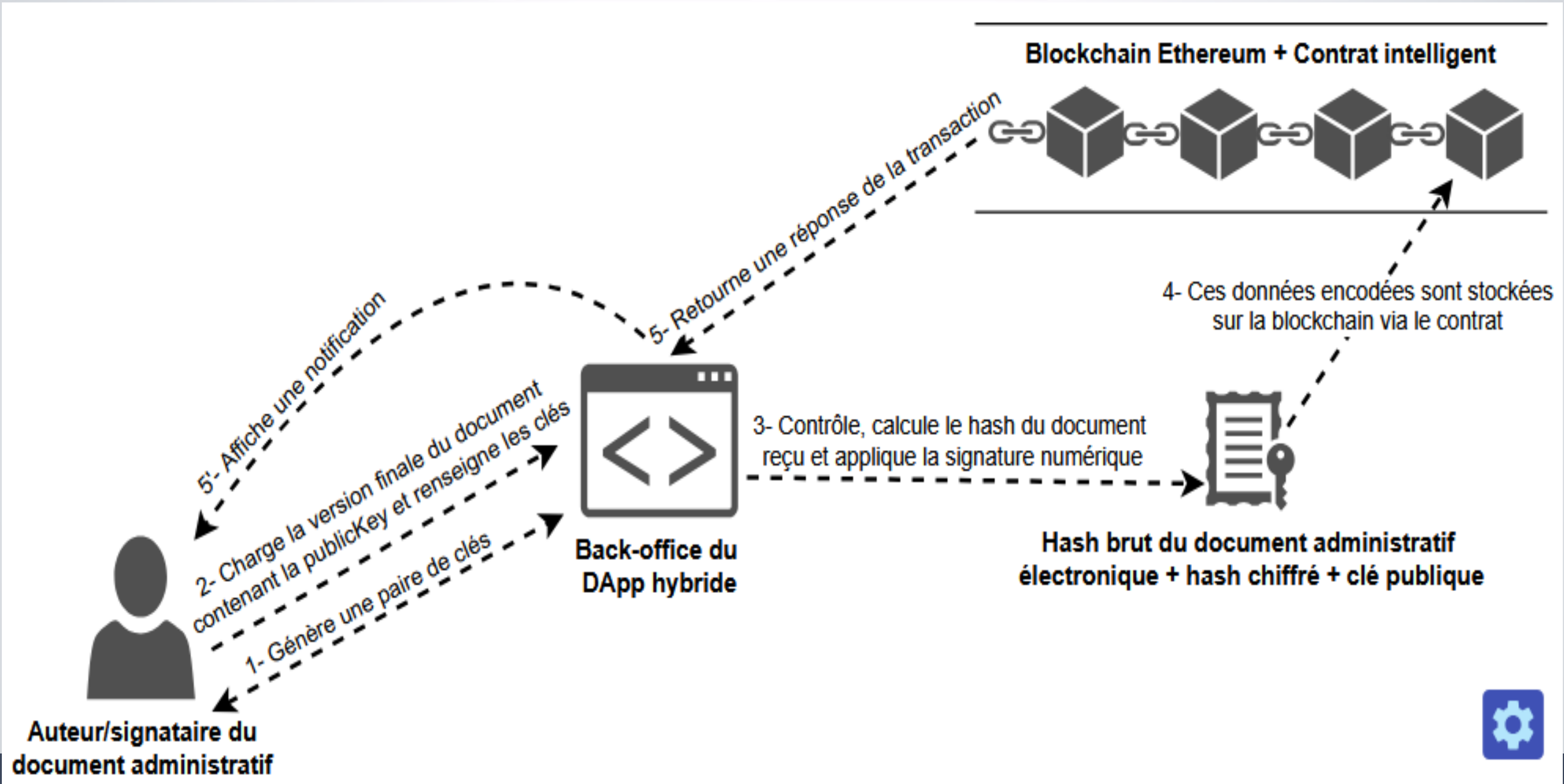
MÉTHODOLOGIE

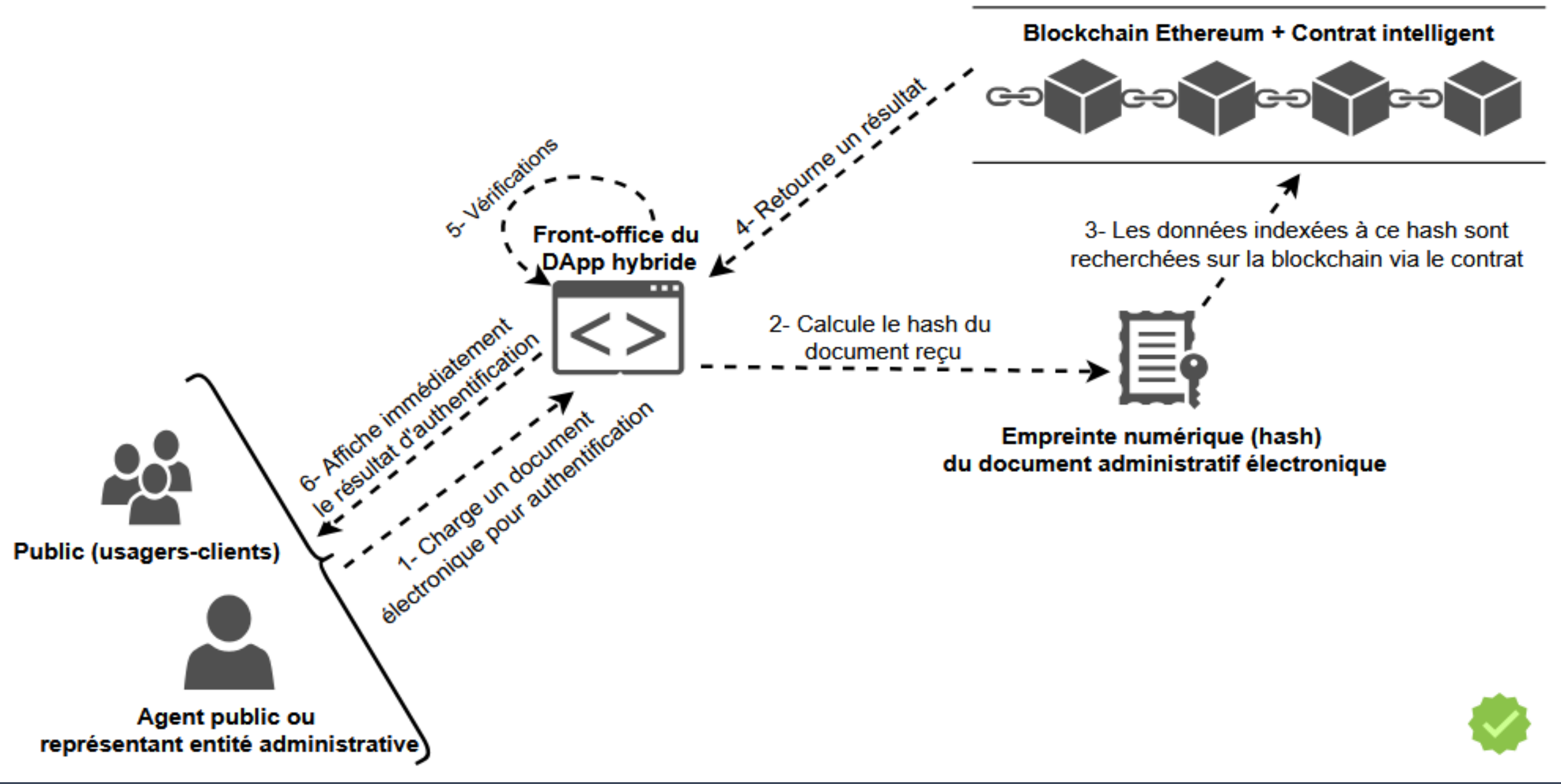
Système d'authentification de documents administratifs basé sur la blockchain Ethereum

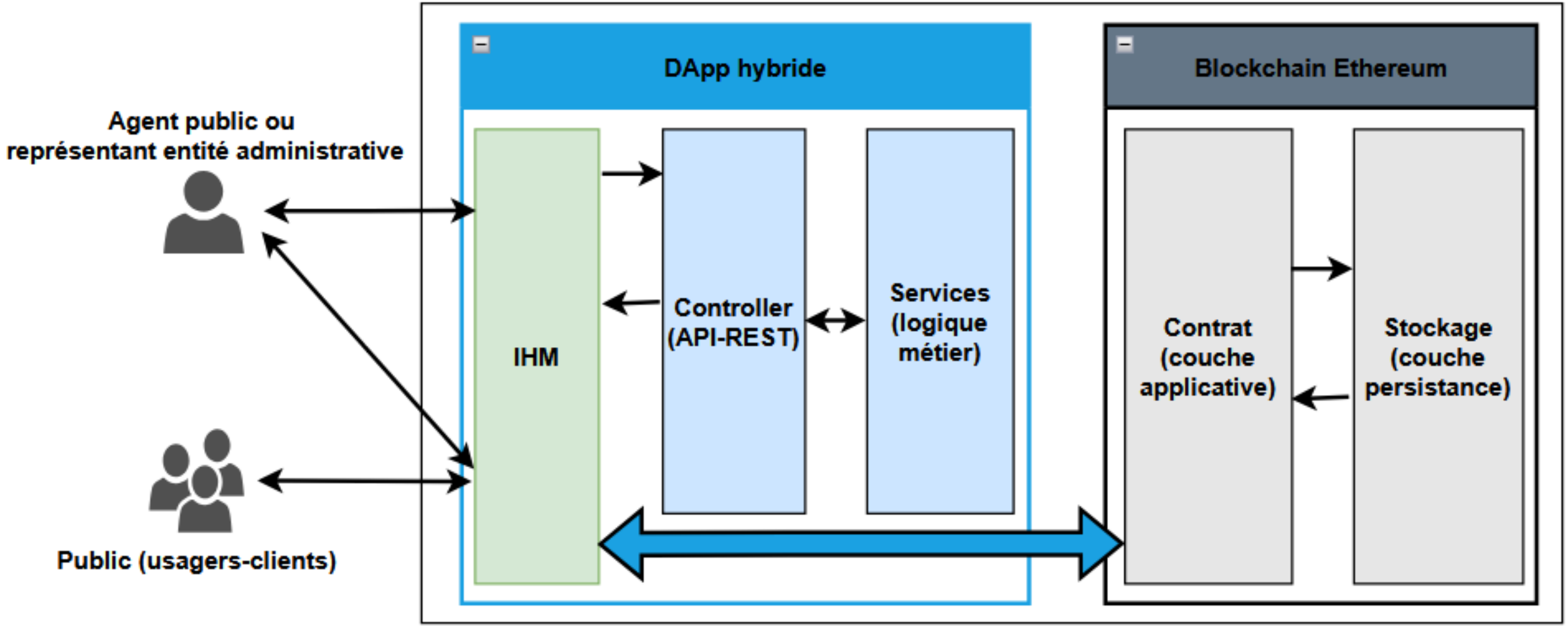
PHASE 1
Action : Enregistrement de documents administratifs dans la blockchain
Acteurs : Représentant d'entité administrative

PHASE 2
Action : Vérification/authentification de documents administratifs via la blockchain
Acteurs : Public (usager-client) et/ou Entité administrative

NB : La PHASE 1 nécéssite d'avoir une paire de clés cryptographiques


Blockchain Ethereum + Contrat intelligent
5- Retourne une réponse de la transaction
4- Ces données encodées sont stockées sur la blockchain via le contrat
5'- Affiche une notification
2- Charge la version finale du document contenant la publicKey et renseigne les clés
1- Génère une paire de clés
3- Contrôle, calcule le hash du document reçu et applique la signature numérique
Back-office du DApp hybride
Hash brut du document administratif électronique + hash chiffré + clé publique
Auteur/signataire du document administratif


Blockchain Ethereum + Contrat intelligent
4- Retourne un résultat
5- Vérifications
Front-office du
DApp hybride
3- Les données indexées à ce hash sont
recherchées sur la blockchain via le contrat
2- Calcule le hash du
document reçu
6- Affiche immédiatement
le résultat d'authentification
1- Charge un document
électronique pour authentification
Empreinte numérique (hash)
du document administratif électronique
Public (usagers-clients)
Agent public ou
représentant entité administrative



Architecture simplifiée en couches de notre approche

IMPLÉMENTATION

OUTILS ET TECHNOLOGIES UTILISÉS (1/2)

LES LANGAGES

LES FRAMEWORKS

OUTILS ET TECHNOLOGIES UTILISÉS (2/2)

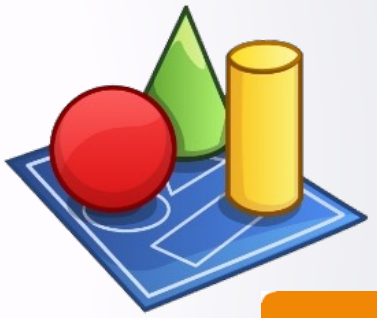
LES PROTOCOLES /TECHNOLOGIES

HTTP, API REST, API JSON

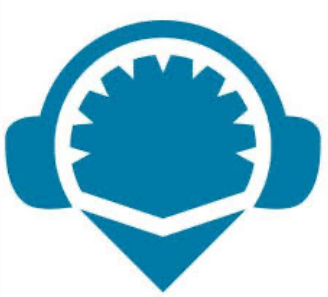
RPC, WEB3, ETHERS.JS, ABI,

SHA-256, BOUNCYCASTLE

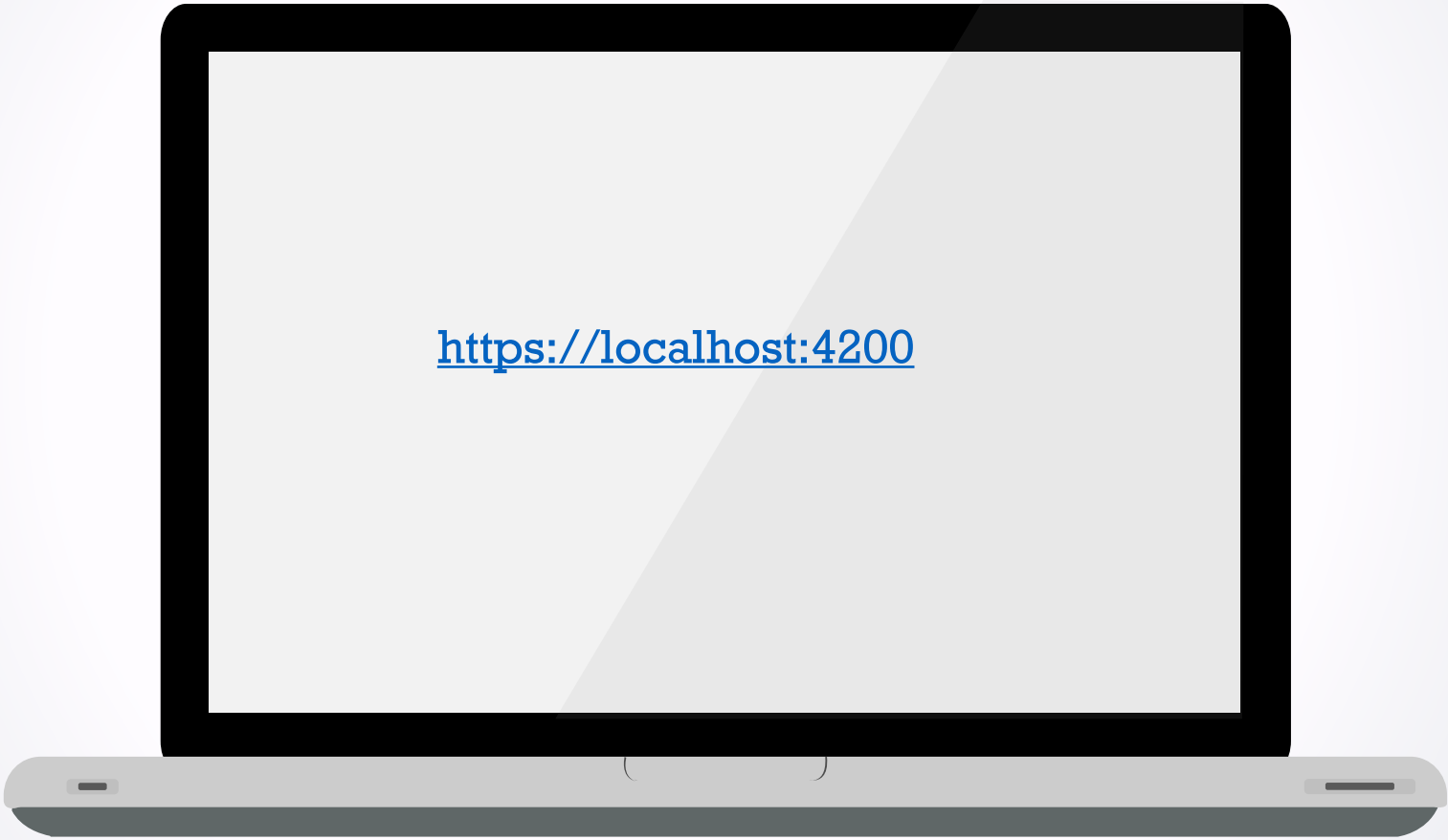
LES MODELISATIONS



LES IDE



DÉMONSTRATION


https://localhost:4200

CONCLUSION

Un travail vraiment passionnant d'explorer l'utilisation de la technologie Blockchain pour améliorer les services publics gouvernementaux, surtout dans les processus d'authentification de documents.

L'intégration d'Ethereum dans notre DApp ADOBLOCK constitue une solution viable et fiable pour garantir plus de sécurité et d'intégrité des documents administratifs, notamment les communiqués officiels. Ce qui permet de diminuer considérablement les cas de falsifications/fraudes documentaires et de renforcer la confiance entre l'Administration et ses usagers/clients.

- Implémenter le module de gestion des utilisateurs du back-office de la DApp de sorte à ce que chaque compte d'accès à la DApp soit systématiquement associé à un EOA.

- Effectuer la mise en échelle de la DApp sur un réseau public blockchain de tests plus réaliste tel que Testnets (Goerli, Sepolia, ou autre) avant d'envisager sa mise production sur le réseau public Ethereum Mainnet (coûteux en frais de gaz, mais sécurisé).

Merci pour votre attention.