Authentification des comptes dans la blockchain pour la détection des attaques

Christian Adja

Sabir MOHAMED
LRE Sécu-Système

Blockchain

La blockchain est un registre qui a la particularité d’être partagée simultanément avec tous ses utilisateurs, tous également détenteurs de ce registre, et qui ont également tous la capacité d’y inscrire des données.

Il s’agit d’une technologie principalement utilisée pour l'échange et la transaction de données, mais pas que.

Il peut être mise en place dans un cadre publique ou privée

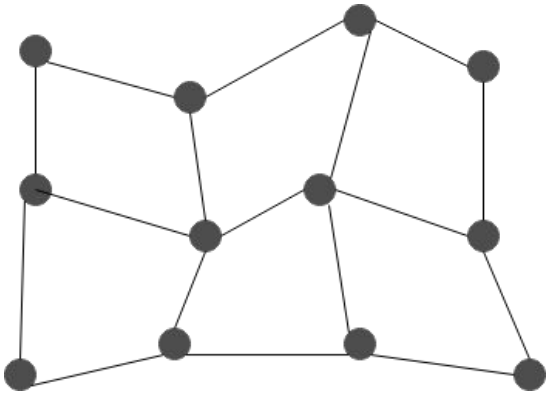
Il repose sur plusieurs technologies.

LRE
LABORATOIRE DE RECHERCHE DE L'EPITA

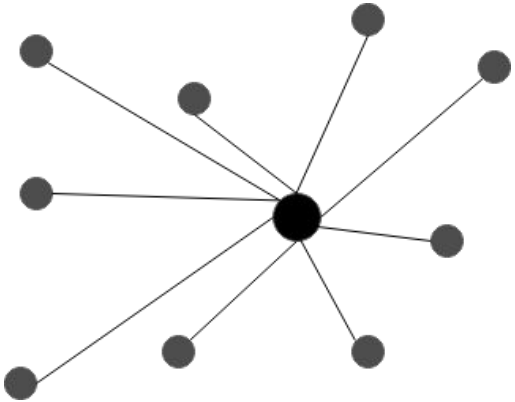
Technologies utilisées dans la blockchain

Distributed Ledger

- Enregistrement des détails des transactions dans plusieurs emplacements.
- Système de stockage distribué



Distribué



Centralisé

Technologies utilisées dans la blockchain

Distributed Ledger

- Enregistrement des détails des transactions dans plusieurs emplacements.
- Système de stockage distribué

Cryptographie

Pour garantir l'authenticité des données et la non-répudiation la blockchain utilise le **hachage** et la **signature** (cryptographie asymétrique)

Consensus

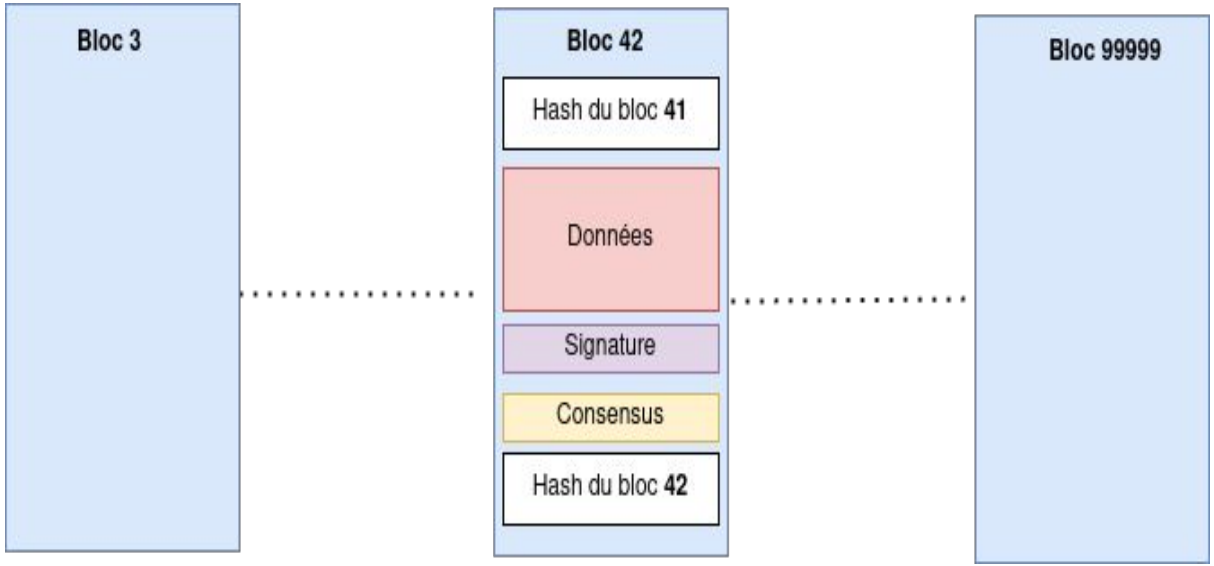
Processus qui permet aux acteurs de se mettre d'accord pour valider une entrée dans le registre

(Ex : Proof of work)

LRE
LABORATOIRE DE RECHERCHE DE L'EPITA

Comment ça fonctionne ?

- Les transactions effectuées sont regroupées par bloc
- Les blocs sont validés par les noeuds du réseau et sont rajoutés à la chaîne
- Une fois validé, la transaction est alors visible par tous les utilisateurs



Blockchain Ethereum

- Elle permet de faire des transactions avec la cryptomonnaie “ether”
- Elle permet de créer des contrats intelligents (**smart contracts**)
- Elle permet de développer des applications décentralisées

LRE
LABORATOIRE DE RECHERCHE DE L'EPITA

Qu’est ce qu’un smart contract ?

<u>Les différents types de comptes</u>

- Compte externe (**EOA**) : Comptes des utilisateurs finaux avec une adresse unique qui est le hash de la clé publique. Il peut envoyer et recevoir des transactions.
- **Smart contract** : Un programme informatique auto-exécutable qui tourne dans une **EVM** (Ethereum virtual machine). Il a une adresse unique qui est utilisée pour faire des transactions et exécuter des fonctions.

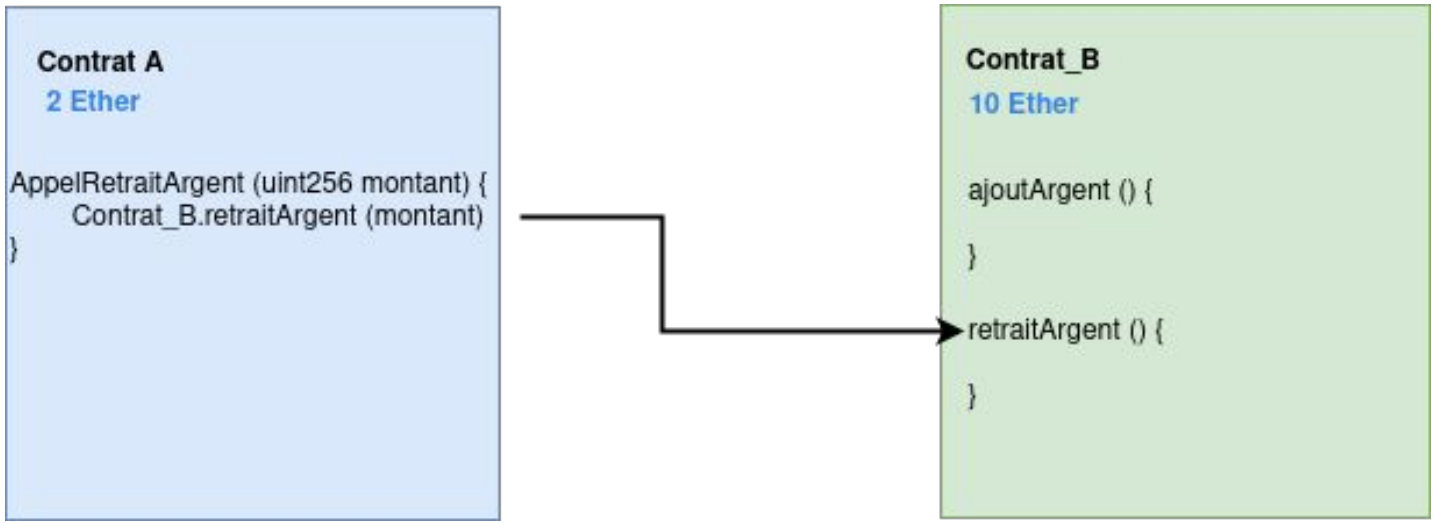
LRE
LABORATOIRE DE RECHERCHE DE L'EPITA

Comment fonctionnent les smart contracts?

- Le contrat peut être rédigé en Solidity ou en Vyper par toute personne faisant partie de la blockchain ethereum
- Une fois écrit il doit être compilé
- Il est ensuite déployé dans l'EVM
- Il faut avoir suffisamment d'éther pour le déployer
- Le contrat déployé est immuable
- Les contrats intelligents peuvent communiquer entre eux

LRE
LABORATOIRE DE RECHERCHE DE L'EPITA

Communication entre smart contracts



Pourquoi on s'intéresse aux contrats intelligents ?

- Ils sont sujets à beaucoup d'attaques [1]
- Les attaques sont toujours du même acabit : **un contrat intelligent qui attaque un autre contrat intelligent**
- L'authentification de l'utilisateur à l'origine d'un contrat intelligent est un réel défi

[1] Ethereum smart contract security research: survey and future research opportunities

LRE
LABORATOIRE DE RECHERCHE DE L'EPITA

Problématique

- Proposer un moyen **fiable** pour authentifier l'utilisateur qui a déployé le smart contract
- Une méthode qui conserve l'anonymat de cet utilisateur
- Une méthode avec un moindre coût

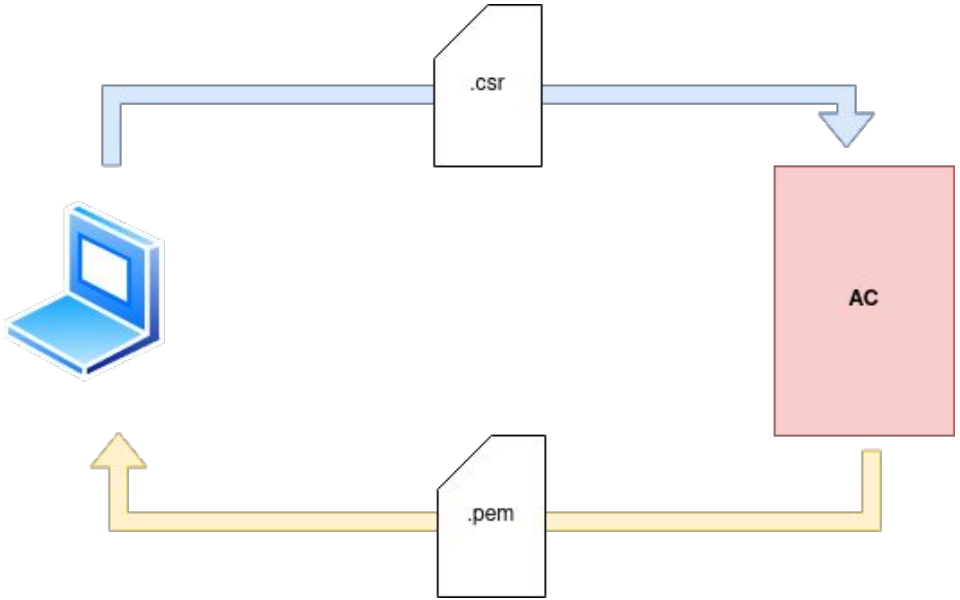
LRE
LABORATOIRE DE RECHERCHE DE L'EPITA

Solution

Implémentation d’une méthode d'échange et de transaction utilisant les **certificats électroniques**.

LRE
LABORATOIRE DE RECHERCHE DE L'EPITA

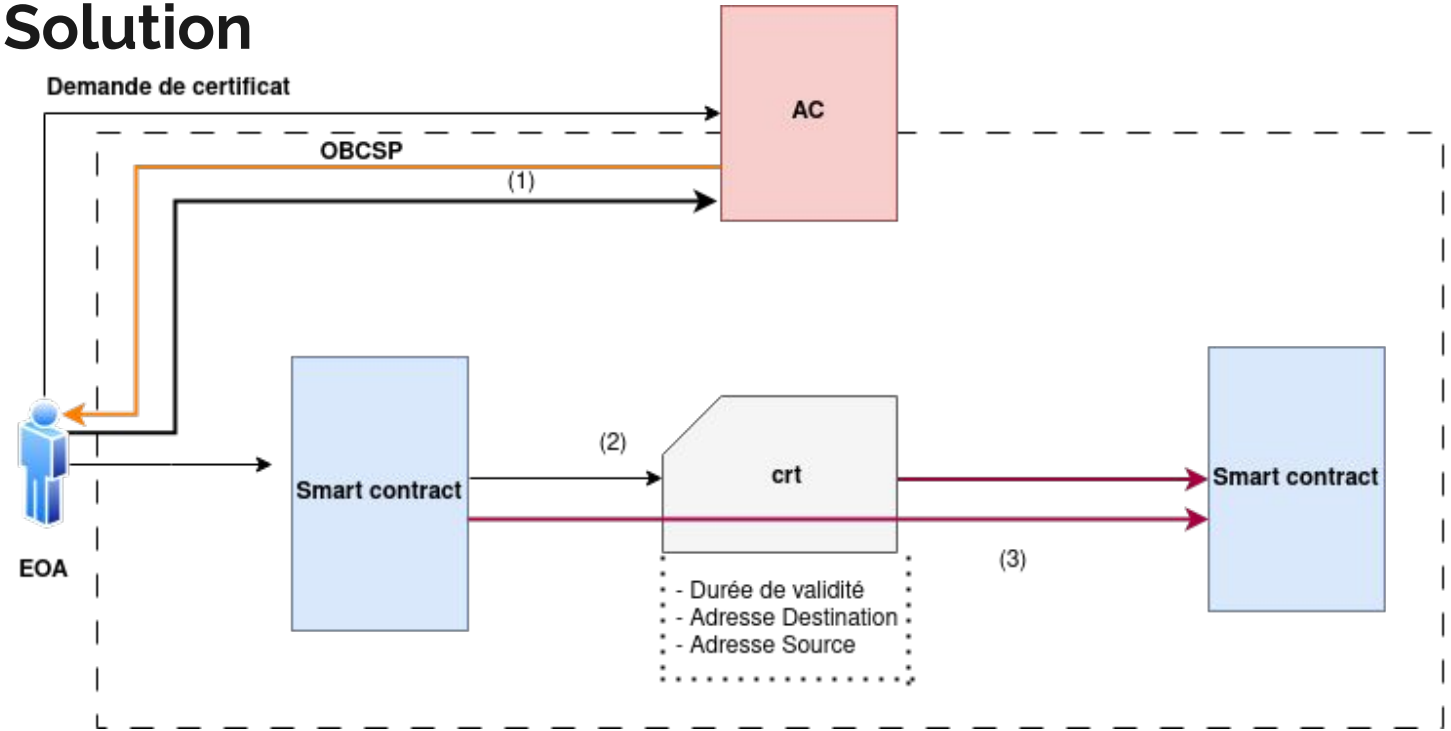
Certificat Électronique



- Une durée de validité bien définie
- Peut être révoqué par l'AC

OBCSP : Online Blockchain Certificate Status Protocol

Solution



Inconvénients de cette solution

- Sollicitation fréquente de l'autorité de certification
- Ajout de nouvelles extensions
- Traçabilité de l'utilisateur à l'origine du contrat

LRE
LABORATOIRE DE RECHERCHE DE L'EPITA

Avantages

- Authentification des utilisateurs
- Éviter les attaques

Références

https://ethereum.org/fr/developers/docs/accounts/

https://ethereum.org/fr/developers/docs/evm/

https://ethereum.org/fr/developers/docs/smart-contracts/

https://ethereum.org/fr/developers/docs/smart-contracts/compiling/

https://ethereum.org/fr/developers/docs/accounts/

https://eips.ethereum.org/EIPS/eip-1271

https://solidity-fr.readthedocs.io/fr/latest/structure-of-a-contract.html

https://www.mdpi.com/2624-800X/2/2/19

https://www.sciencedirect.com/science/article/pii/S2096720922000070

https://www.edx.org/course/blockchain-understanding-its-uses-and-implications

https://www.sciencedirect.com/science/article/pii/S1877050920323589

https://dasp.co/index.html

https://ieeexplore.ieee.org/abstract/document/8662573

https://openknowledge.worldbank.org/entities/publication/563eb421-4449-5319-953b-2ace8da058c0

https://dl.acm.org/doi/abs/10.1145/3560832.3563442

https://ieeexplore.ieee.org/abstract/document/9667515

https://eips.ethereum.org/EIPS/eip-4361

LRE
LABORATOIRE DE RECHERCHE DE L'EPITA