5ème COLLOQUES FRONTIERES NUMERIQUES 2023
7,8 et 9 Juin
Hammamet - TUNISIE

Vers une nouvelle procédure d'authentification basée sur la technologie Blockchain 2.0 pour les réseaux cellulaires

Présenté par : Meriem BOUKESSESSA
Co-auteurs : Adda ALI PACHA, Abdelkader GHAZLI
Laboratoire de Codage et de Sécurité de l'Information LACOSI

08/06/2023

Introduction

Au fur et à mesure que les réseaux mobiles deviennent de plus en plus omniprésents, de part l'arrivée des nouvelles tendances technologiques, la sécurité des communications est une préoccupation majeure.

Les réseaux mobiles et leur sécurité

Aucune mesure de sécurité

Authentification unilatérale de l'utilisateur et chiffrement dans la partie radio

Authentification Bilatérale du réseau et de l'utilisateur et intégrité des données

Authentification bilatérale avec introduction d'une clé de base Kasme

Authentification bilatérale avec décision finale du réseau principale et Identité caché durant l'enregistrement

Blockchain, qu’est ce que c’est ?

La Blockchain est une technologie décentralisée, transparente et sécurisée qui stocke les informations sous forme de blocs connectés chronologiquement. Elle garantit l'intégrité des données et facilite la confiance entre les participants sans nécessiter d'autorité centrale.

Analyse du projet

Blockchain 1.0

Gestion de crypto monnaies

Blockchain 2.0

Cryptomonnaies + Applications décentralisées

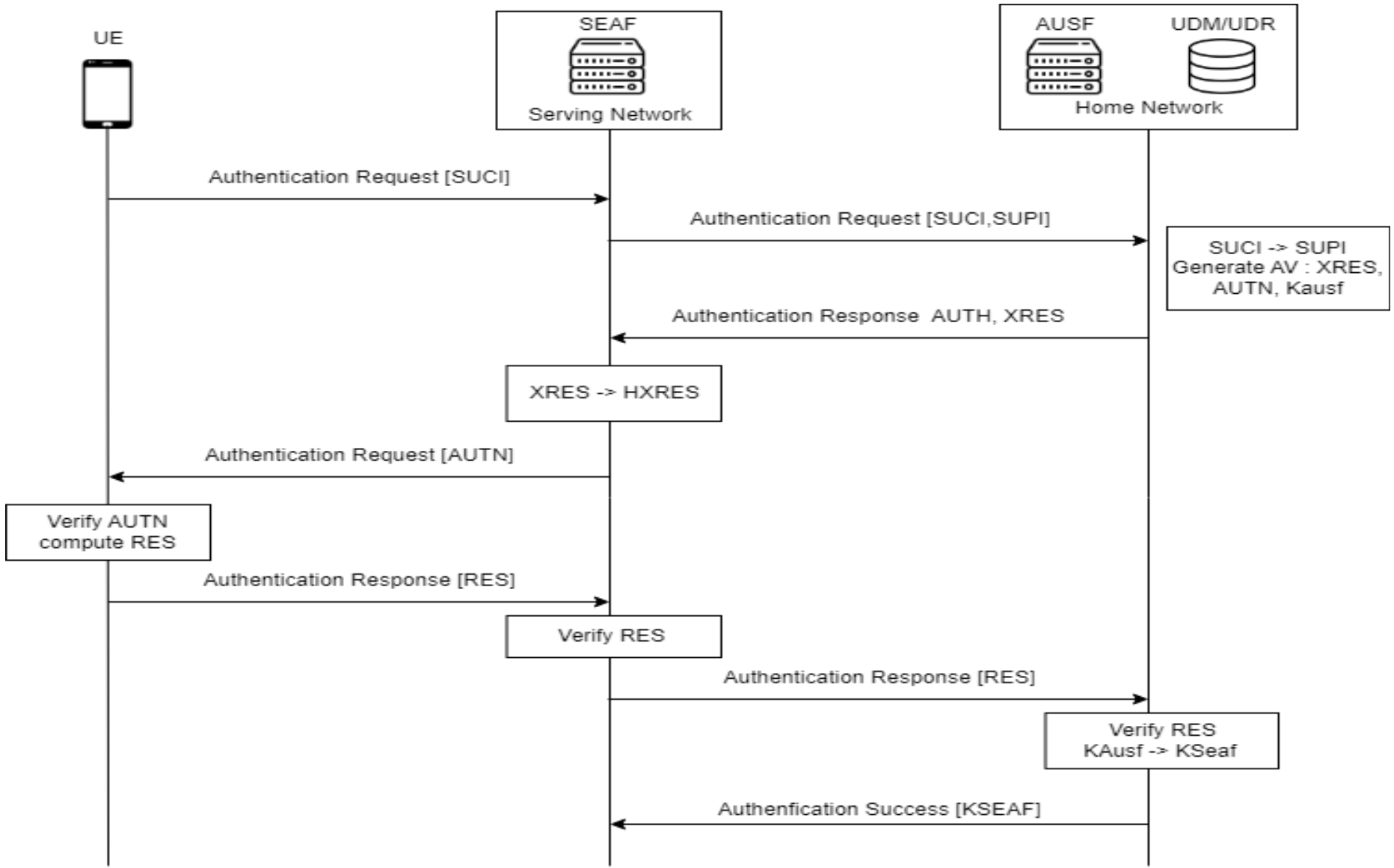
Blockchain 3.0

HYPERLEDGER FABRIC

Dapps avec infrastructure plus robuste

Situation du problème

La procédure d'authentification dans la 5G :



Situation du problème

POSITIF	NÉGATIF
› Introduction de l'identité SUPI	› Architecture centralisée
› Prise de décision finale de l'authentification par le réseau	› Complexité accrue des réseaux 5G
› EAP-AKA : protocole d'authentification étendu avec le protocole d'authentification et de clé	› Création de nouvelles surfaces d'attaques potentielles.
	› Augmentation du nombre d'éléments connectés.

Blockchain comme solution

Blockchain comme une base de données distribuée pour enregistrées les règles

Améliore la non-répudiation et l'immuabilité des règles

Les décisions d'accès sont prises par une authorité hors blockchain
point de défaillance unique

Blockchain comme une base de données et comme un point de décision

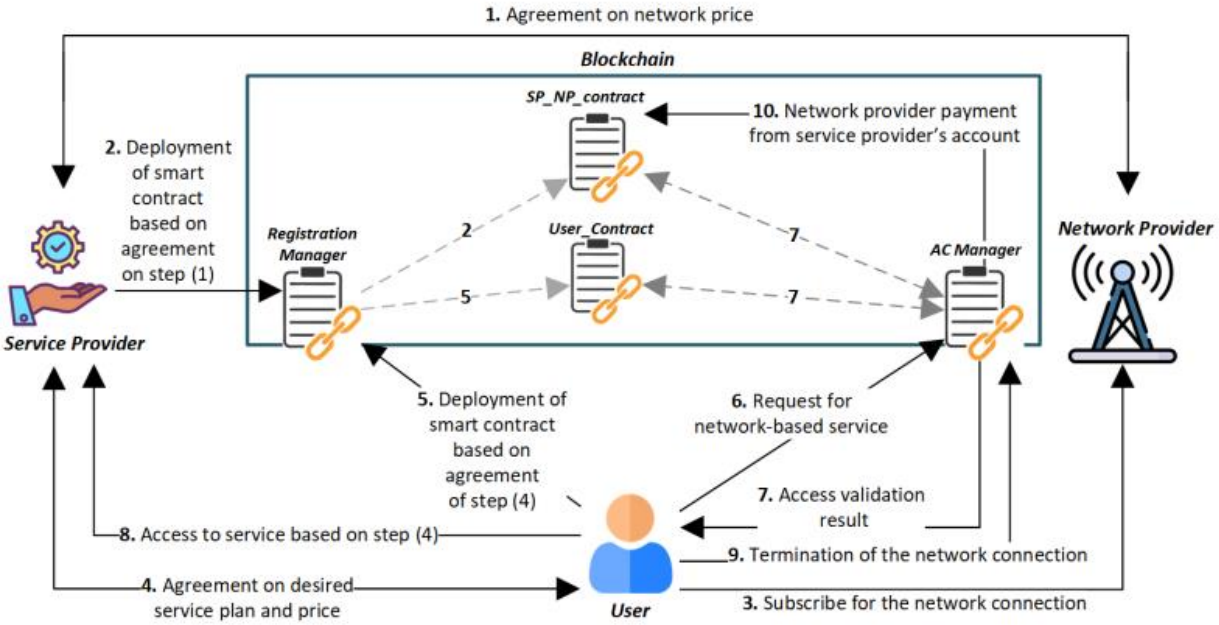
Toutes les règles sont stockées dans la blockchain et les décisions d'accès sont utilisée en utilisant des contrats intelligents

Haute complexité
Efficacité temporelle très faible

Haute évolutivité
Tolérance aux pannes, disponibilité et non répudiation

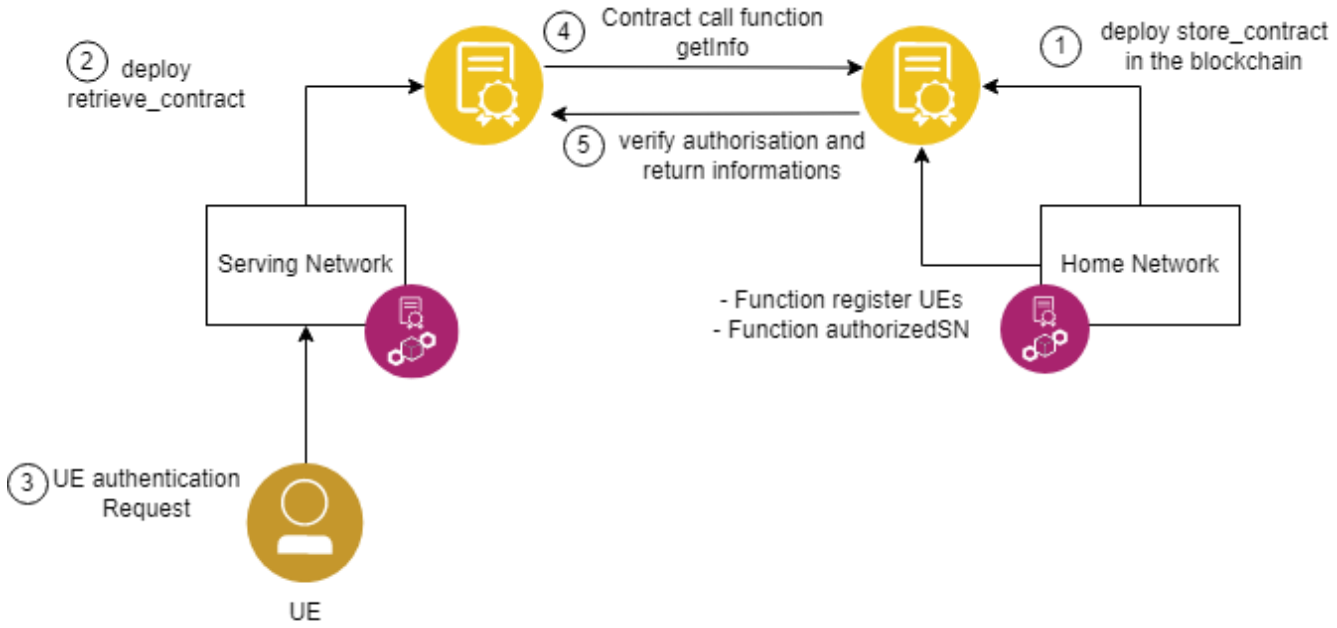
Exemple

"A Novel Access Control Method Via Smart Contracts for Internet-Based Service Provisioning" F. Ghaffari, E. Bertin, N. Crespi, S. Behrad and J. Hatin, "A Novel Access Control Method Via Smart Contracts for Internet-Based Service Provisioning," in *IEEE Access*



Fonctionnalité	Proposition
Access control automation	Yes
Purpose of blockchain usage	Blockchain for both database and access control process
Scalabitity	High
Access decision making	Distributed
Remove single point of failure	Yes
Fault tolerance	Yes
Access Control Model	ABAC

L'approche



Algorithm1 UEs Information registration

function resigterUEs (_SUCI, _SUPI, _AVs)

1. Require HNAddress == msg.sender
2. UEINFO.SUCI ← _SUCI
3. UEINFO.SUPI ← _SUPI
4. UEINFRO.AV ← _AVs
5. UEs ← UEINFO

Algorithm 2 Authorized_SN registration

function authorizedSN (SN_Address)

1. Require HNAddress == msg.sender
2. **push** SN_Address in authorized_SN

Algorithm 3 UE infromation retrievial

function getInfo (_SNAddress, SUCI)

1. Require _SNAddress == msg.sender
2. Generate a random number N
3. **return** store_contract.info_access (SUCI, _SNAddress, N)

Algorithm 4 UE information access

function info_access (N, _SNAddress, SUCI)

```
1.  for i =0 ; i < newnonces.length ; i++ do
2.    if N ≠ newnonces[i]
3.      newnonces.push(N)
4.      for j=0 ;  j < authorized_SN.length ; j++ do
5.        If _SNAddress == authorized_SN [ j ]
6.          for k = 0 ; k < UEs.length ; k++ do
7.                    If keccak256(abi.encodePacked(UEs[ k ].SUCI)) ==
      keccak256(abi.encodePacked(SUCI)
8.                return UEs[ k ]
9.              end if
10.         …
11.   end for
```

Functions	Transaction Cost	Execution cost
registerUEs	684578 gas	658806 gas
AuthorizedSN	68455 gas	47023 gas
getInfo	91863 gas	69639 gas

L’approche

Par son existence sur un réseau blockchain, où toutes les transactions sont enregistrées, notre protocole possède les propriétés d'immutabilité et de transparence de toutes les données enregistrées. Nous avons mis en place un mécanisme de protection des données dans le contrat intelligent : le HN et les SN se voient attribuer une adresse unique sur la blockchain, et chaque SN ne peut pas effectuer une demande d'information sans être autorisé et surveillé, le HN ne considère aucune entité comme étant de confiance, il vérifie la présence de l'identité du SN dans sa liste de cellules autorisées qui est mise à jour fréquemment, et seul le HN est autorisé à ajouter et à supprimer des autorisations.

Pour conclure

Notre proposition d'authentification et d'accord de clé basé sur la blockchain dans un réseau 5G, vise à améliorer les caractéristiques de sécurité grâce à l'utilisation d'un modèle de zéro confiance Le HN, avant d'accorder l'accès à un SN, doit vérifier l'éligibilité préalablement enregistrée dans la blockchain. L'execution de notre contrat intelligent est estimé au moyen de gaz mesuré en Wei (petite unité dans Ethereum) et le plus les fonctions sont complexes et le contrat est chargé, plus l'execution est couteuse. Pour la notre, le gaz calculé est acceptable, selon les résultats de simulation.

Nos travaux futurs se concentreront davantage sur les améliorations de notre système. qui sera émulé sur avec l'uttilsation d'un SDR dans le but de reproduire fidèlement le comportement d'un réseau réel.

Merci

24Slides