Blockchain appliquée à un processus électoral

Thème du projet

- L’objectif de ce projet est de proposer une piste de réflexion sur les protocoles et sur les structures de données à mettre en place pour permettre d’implémenter efficacement le processus de désignation du vainqueur de l’élection, tout en garantissant l’intégrité, la sécurité et la transparence de l’élection.

Plan du projet

- Partie 1 : Génération de nombre premier et chiffrement/déchiffrement à l'aide de clé publique/secrète (RSA).
- Partie 2 : Utilisation des fonctions de la partie 1 afin de sécuriser (chiffrement) et ensuite stocker des déclarations de vote signées.
- Partie 3 : Stockage et manipulation (simulation processus de vote) des données relative au votants, candidats et déclarations signées.
- Partie 4/5 : Introduction au fonctionnement de la Blockchain (chaîne de blocs) par la manipulation des blocs (production et vérification), à la décentralisation (consensus PoW) et enfin constitution de l'arbre représentant la Blockchain

Structures du code

- Division du code en 4 composantes :
- « struct » : comprenant les déclarations des différentes structures utilisés
- « chiffrement » : comprenant les fonctions permettant le chiffrage et déchiffrage des données (chiffrement via RSA ou encore SHA_256)
- « readwrite » : comprenant les fonctions qui interagissent avec des fichiers
- « compute » : comprenant les fonctions de calcul

Structures utilisées

- 9 structures ont été utilisées pour ce projet, parmi liste chaînée, table de hachage et arbre:

- Key : conserve un couple (u/s, n) représentant la clé publique ou secrète
- Signature : conserve le vote chiffré à l'aide de la clé privée du votant dans un tableau de long
- Protected : conserve la clé publique du votant, son vote ainsi que la signature du vote
- CellKey : liste chaînée de Key
- CellProtected : liste chaînée de Protected
- Hashcell : conserve une clé ainsi qu'une valeur qui pour être utiliser pour en autre de comptabiliser le nombre de voix
- Hashtable : Table de hachage stockant les structures Hashcell
- Block : conserve la clé de l'émetteur d bloc, une liste de votes CellProtected, le hash (identifiant du bloc), le hash du bloc émis précédemment et enfin une preuve de travail (nonce)
- Celltree : Arbre représentant la Blockchain, conserve un bloc et des nœuds père, frères et fils

Présentation des fonctions jugées importantes

- Compute_winner : manipulation d’une table de hachage
- read_tree() : constitution de l’arbre représentant la Blockchain

Project tour : Blockchain appliquée à un processus éléctoral