RAPPORT DE PROJET

Projet : Blockchain appliquée à un processus électoral

Projet réalisé par Sonia Hammouche

Sommaire

Introduction

Une élection est la procédure par laquelle des électeurs, accordent leur suffrage a un candidat qu'ils jugent apte à les représenter dans des assemblées administratives de ressort de compétence variable.

“À l'égard des élections du prince et des magistrats [dans une république], il y a deux voies pour y procéder, savoir le choix et le sort", Rousseau, Contr. IV, 3.

Quels sont les différents modes de scrutin ?

- Le scrutin majoritaire
- Sc scrutin mixte
- Scrutin mixte

Partie 1 : Développement d'outils cryptographiques

La cryptologie, science du secret englobe la cryptographie, le codage secret d'un message.

Cryptographie à clé publique : le principe de la cryptographie a clé publique est basé sur l'existence d'une fonction dite à sens unique, pour transformer un message en message codé.

Le système RSA

On prend p est un diviseur du nombre entier n s'il existe un nombre entier q tel que n = p * q, deux nombres entiers p et q sont dit premier entre eux si pgcd (p, q) =1, le théorème de Bezout : il existe deux nombres entiers relatifs (l'un positif, l'autre négatif) m et n tels que $m \times p + n \times q = 1$. Forts de ces résultats, énonçons la propriété fondamentale du fonctionnement du RSA.

Protocole RSA pour le codage

On calcule deux nombres premiers p et q, choisit e un nombre premier avec $(p - 1)(q - 1)$ et d tel qu'il est défini dans le théorème, c'est-à-dire tel qu'il existe un nombre entier relatif m tel que : $e \times d + m \times (p - 1)(q - 1) = 1$

On utilise, random_prime_number, puis pour générer les nombre n, s, u on utilise la fonction generate_kay_values;

Pour ce faire, elle peut utiliser un algorithme de calcul très connu depuis l'Antiquité (vers 300 ans avant Jésus-Christ) appelé algorithme d'Euclide. Elle calcule également $n = p \times q$.

On garde une partie des nombres en secret et les autres on les conserve secrètement, quand on veut transférer une information secrète en suivant le

protocole en question, transforme son information en un nombre entier A, inferieur à n, la personne qui reçoit l'information élève A la puissance e, et prend le reste de la division du nombre qu'il a obtenu A^e Par le n.

La clé publique est constituée par le nombre n et e, si on veut coder un message, on le transforme en fermant la serrure publique, fermer la serrure publique consiste transforme le message en plusieurs nombres tous entiers et inferieurs à n, la seule façon de retourner au message initial est de posséder la clé privée.

Démonstration :

Comme e est supposé premier avec $(p-1)(q-1)$, on sait d'après le théorème de Bezout qu'il existe un entier d tel que $e \times d = 1 + m \times (p-1)(q-1)$. Soit $à$ un nombre premier avec $p \times q$. On a

$a^{ed} = a^{1 + m \times (p-1)(q-1)}$

$= a \times (a^{\phi(p \times q)})^m$

$\equiv a \times 1^m \ [p \times q]$

$\equiv a$

En utilisant le petit théorème de Fermat généralisé.

Partie 2 : Création d'un système de déclarations sécurisés par chiffrement asymétrique.

On définit une structure qui va représenter une clé, soit publique, soit privée sachant que la clé publique est définie : pKey = (s,n) et la cle privée : sKey = (u,n)

Dans le cadre de cette partie, j'ai recode les deux fonctions déjà présentent dans la bibliothèque stdlib, a fin de gerer le cas des segfault

J'aime les maths, les chats

Une merveilleuse opportunité pour perfectionner mes compétences et travailler en équipe pour la réalisation de nouveaux projet innovants.

Partie 2 : Création d'un système de déclarations sécurisés par chiffrement asymétrique.

La cryptographie asymétrique est un procédé qui intègre deux clés de chiffrement, une clé publique et une clé privée. Par convention, la clé de chiffrement du message est appelée clé publique (et peut-être communiquée sans restriction aucune), et la clé de déchiffrement du message est appelée clé privée. Cette dernière ne doit être communiquée sous aucun prétexte. Avec une clé publique, l'expéditeur code dans un algorithme de chiffrement un message ou une énigme qui ne pourra être, au final, décodé ou résolu que par le destinataire détenteur d'une clé privée, donnée en entrée d'un algorithme de déchiffrement. Dans l'écosystème bitcoin, la cryptographie est utilisée pour protéger les fonds d'un détenteur de cette cryptomonnaie, pour encrypter le porte-monnaie, mais aussi pour préserver l'intégrité de la blockchain Bitcoin.

Partie 3 : Manipulation d'une base centralisée de déclarations.

On considère a considéré un système de vote centralisé ou on toutes les déclarations de vote (un fichier.txt) dans ce fichier on collecte toutes les expressions de voix par tout ce qui ont droit et qui ont fait un vote conforme au modèle de référence, ce fichier nous permet aussi à partie des votes de déclarer le vainqueur qui sont stocké en liste après le vote.

Partie 4 : Implémentation d'un mécanisme de consensus.

Les blockchains publiques ont un véritable avantage concurrentiel sur les serveurs centralisés et les chaînes de consortium en signalant de manière crédible la neutralité. À l'heure actuelle, il semble que de tels avantages ne valent peut-être pas les coûts des chaînes publiques, mais ce ne sont que les chaînes publiques d'aujourd'hui.

Les blockchains du futur avec preuve de participation et de partage seront des milliers de fois plus efficaces, et donc les sacrifices d'efficacité de mettre des choses sur une chaîne deviendront de plus en plus acceptables.

Les chaînes de blocs ne visent PAS à réduire les coûts de calcul (du moins par rapport aux serveurs centralisés). Les chaînes de blocs consistent à engager un sacrifice sous la forme de coûts de calcul augmente pour obtenir une * diminution * des * coûts sociaux *.

Partie 5 : Manipulation d'une base décentralisée de déclarations.

Les serveurs centralisés peuvent décider de modifier les règles plus tard, ils peuvent être piratés ou simplement fermés si l'entreprise disparaît. Le reçu blockchain Merkle, en revanche, est éternel.