

Implementación de una blockchain resistente a ataques criptográficos cuánticos

Trabajo Fin de Grado

Autor

María Victoria Granados Pozo

Directores

Gabriel Maciá Fernández

Francisco Javier Lobillo Borrero

Doble grado de Ingeniería Informática y Matemáticas
Universidad de Granada

26 de Noviembre de 2020



**UNIVERSIDAD
DE GRANADA**

Introducción



@mvictoria1997/TFG
@mvictoria1997/core

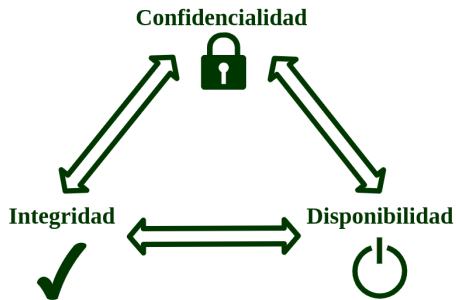


Figure: Pilares de la seguridad informática

Objetivos

Implementación del algoritmo UOV

Funciones propias del algoritmo y aritmética del cuerpo finito de 2^7 elementos.

Integración del algoritmo UOV

Modificación del algoritmo de firma de la blockchain de ARK por el algoritmo UOV.

Tecnologías utilizadas

OpenProj

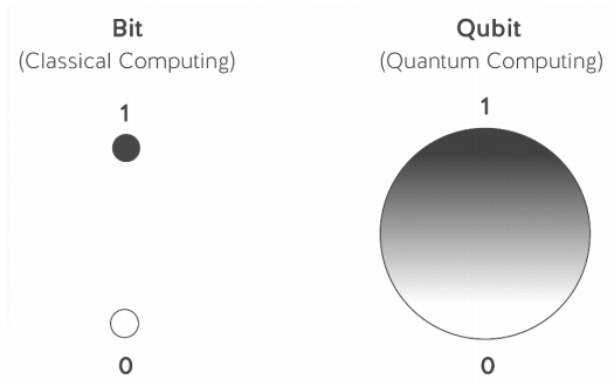
L^AT_EX



Contenidos teóricos

Computación cuántica

Estados de un bit y un cúbit



Propiedades computación cuántica

- Superposición cuántica.
- Entrelazamiento cuántico.
- Teletransporte cuántico.



Comparativa computación cuántica y clásica

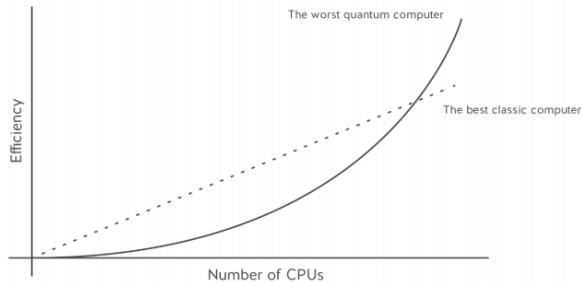


Figure: Comparativa de cómputo de de un ordenador cuántico y clásico

Blockchain

Descripción

Una cadena de bloques es un sistema de almacenamiento de información dividido en bloques de datos enlazados mediante el *hash*.

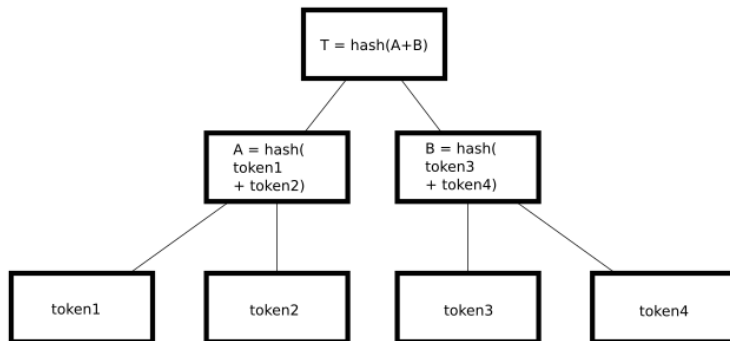


Figure: Estructura árbol de Merkle

Aplicaciones

- ◇ Área financiera o criptomonedas.
- ◇ Centros de salud.
- ◇ Firma de documentos.
- ◇ Cadenas de suministro.



Algoritmo UOV (*Unbalance Oil and Vinegar*)

Ventajas del algoritmo UOV

- ▲ Problema NP-duro.
- ▲ No se conoce un algoritmo eficiente para la resolución de sistemas multivariados en un ordenador cuántico.
- ▲ Simplicidad de las operaciones.
- ▲ Requiere bajos recursos *hardware*.

$$\mathcal{P} : \mathbb{F}_{2^r}^n \rightarrow \mathbb{F}_{2^r}^m$$

$$\mathcal{P} = \mathcal{F} \circ \mathcal{T}, \text{ donde } \mathcal{T} : \mathbb{F}_{2^r}^n \rightarrow \mathbb{F}_{2^r}^n \text{ y } \mathcal{F} : \mathbb{F}_{2^r}^n \rightarrow \mathbb{F}_{2^r}^m$$

$$f_k(x) = \sum_{i=1}^v \sum_{j=i}^n \alpha_{i,j,k} x_i x_j + \sum_{i=1}^n \beta_{i,k} x_i \quad (1)$$

donde $\alpha_{i,j,k}$ y $\beta_{i,k}$ se toman aleatoriamente en \mathbb{F}_2 siendo $(\alpha_{i,j,k})_{\substack{1 \leq i \leq v \\ 1 \leq j \leq n}}$ un vector de matrices triangulares superiores.

Planificación y presupuesto

Diagrama de Gantt

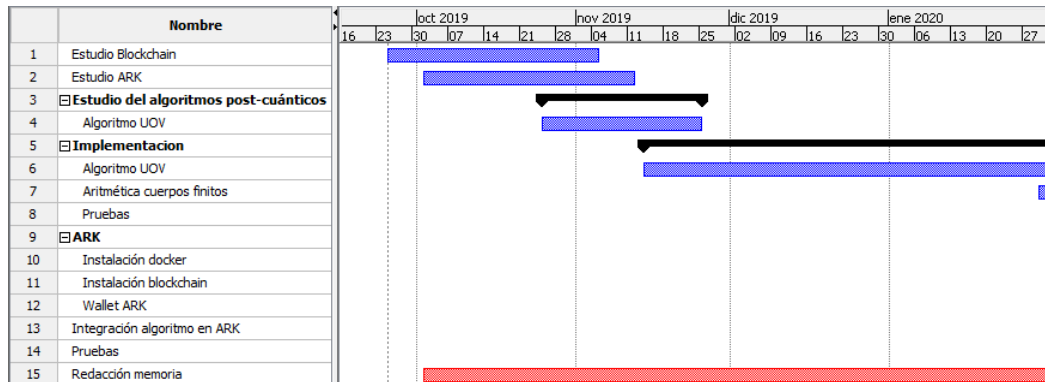


Diagrama de Gantt

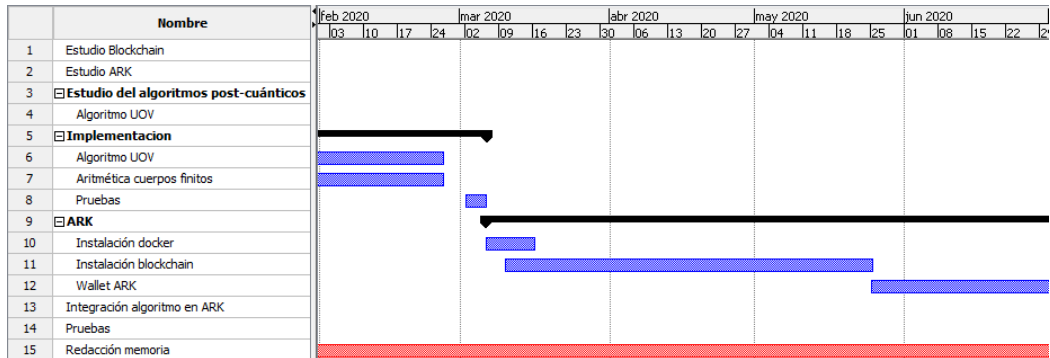
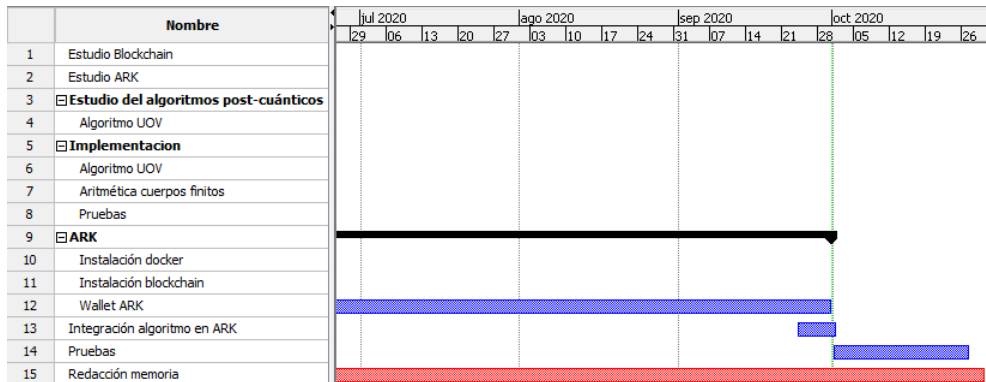


Diagrama de Gantt



Presupuesto desglosado

Tipo de costes	Cantidad
Recursos humanos tutores	4.830€
Recursos humanos alumna	10.720€
Indirectos	1.578,24€
Directos	210,40€
Viajes	22€
Gastos imprevistos	868,03€
TOTAL (€)	18.228,67€

Table: Presupuesto total desglosado

Diseño

Bloques del diseño

Deployer

Da la posibilidad de crear una cadena de bloques personalizada.

Core

Gestiona la creación de bloques y almacenamiento de transacciones (parte modificada).

Base de datos

Almacenar y servir datos de las transacciones y bloques.

ARK Desktop Wallet

Interfaz para la realización de transacciones.

Explorer ARK

Interfaz para la visualización de los bloques y transacciones.

Posibles configuraciones de los bloques

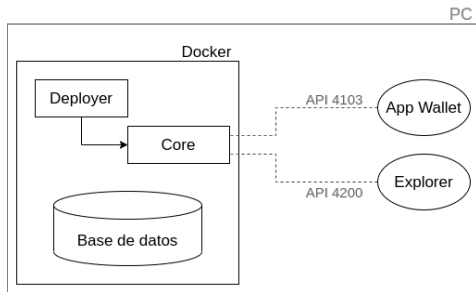


Figure: Diagrama de bloques prototipo

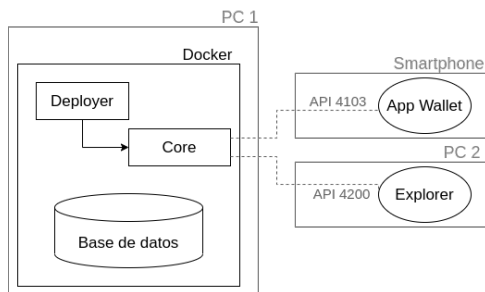


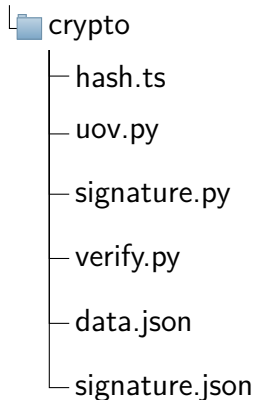
Figure: Diagrama de bloques ejemplo

Implementación

Estructura directorio

core-bridgechain/packages/crypto/src/crypto

core-bridgechain/packages/crypto/src



Demostración práctica

Conclusiones e investigaciones futuras

Conclusiones

- ✓ Implementación algoritmo UOV y aritmética del cuerpo finito de 128 elementos.
- ✓ Comparación de los tiempos de ejecución en python y SageMath.
- ✓ Integración del algoritmo en la *blockchain* ARK.
- ✓ Ejecución de la *blockchain* ARK modificada.
- ✓ Ver los bloques firmados en el *explorer* de ARK.

- Trabajar con la base de datos.
- Integrar la *blockchain* ARK modificada en otra cadena de bloques.

¡Gracias por su atención!