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

UNIVERSIDAD DE GRANADA

November 18, 2020

Contenidos

Introducción

Motivación

Motivación

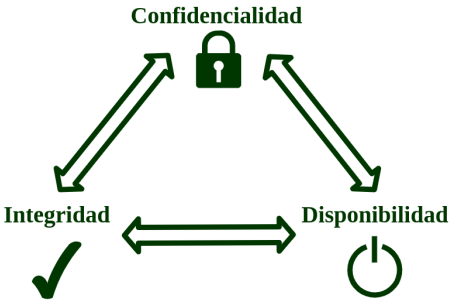


Figure: Pilares de la seguridad informática

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.

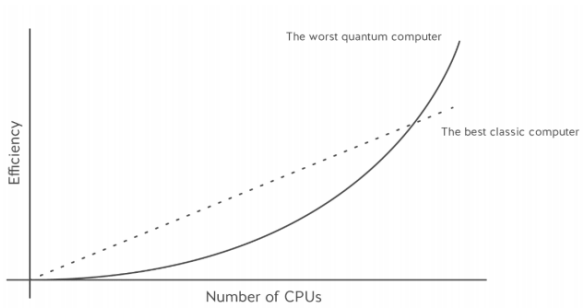
Contenidos teóricos

Computación cuántica

Propiedades computación cuántica

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

Comparativa computación cuántica y clásica



Blockchain

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*.

Esquema UOV

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

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

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

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

Planificación y presupuesto

Diagrama de Gantt

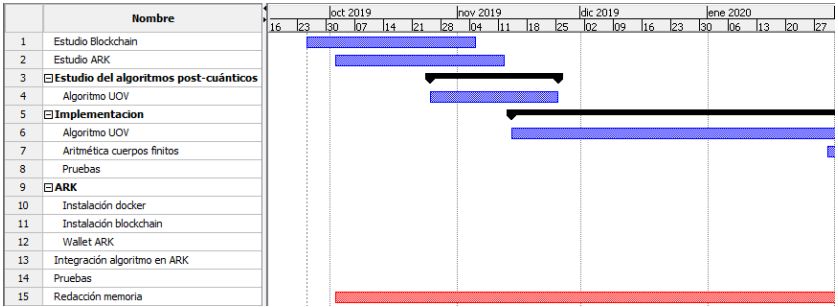


Diagrama de Gantt

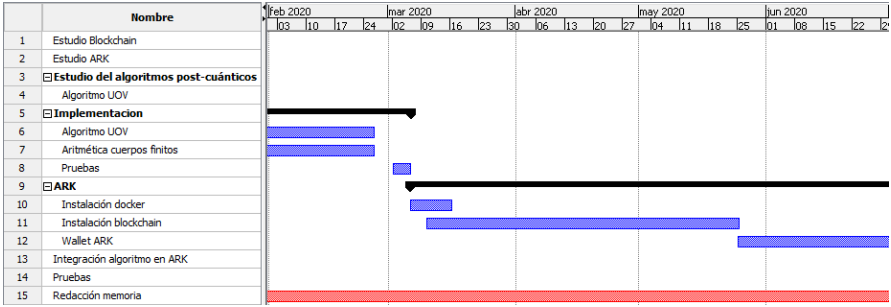
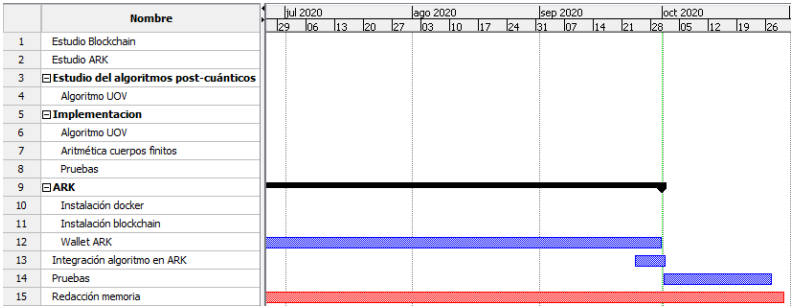


Diagrama de Gantt



Presupuesto desglosado

Tipo de costes	**Cantidad**
Recursos humanos tutores	4.830€
Recursos humanos alumna	10.720€
Indirectos	755,24€
Directos	210,40€
Viajes	22€
Gastos imprevistos	826,88€
TOTAL (€)	17.364,52€

Diseño

Diagrama de bloques del prototipo

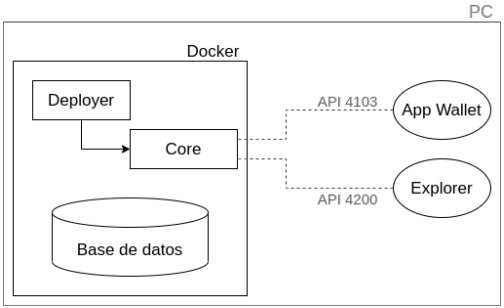


Figure: Diagrama de bloques prototipo

Demostración práctica

Conclusiones e investigaciones futuras

Conclusiones

Trabajos futuros

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

¡Gracias por su atención!