RESUMEN

Este documento describe el proceso de desarrollo, implementación y evaluación de un prototipo de cartera Bitcoin basada en hardware. Con este fin, se realiza una descripción general de la red Bitcoin para luego adentrarse en el proceso de generación de carteras Bitcoin y los algoritmos criptográficos que gobiernan este proceso. Así también, se describe la operación de las transacciones del tipo "pago a hash de llave pública" P2PKH con el fin de que el lector conozca cómo la red Bitcoin interactúa con las carteras Bitcoin mediante transacciones. Una vez desarrollado el marco teórico, se realiza el diseño de hardware y software de la cartera en base a objetivos y parámetros de diseño. Luego, se adquieren e integran los componentes de hardware, prestando especial atención a sus interfaces de comunicación y alimentación. En cuanto al software, se desarrolla una aplicación para la cartera que incorpora una interfaz gráfica de usuario adecuadamente integrada con los componentes de hardware. Una vez que todos que los dispositivos se han integrado y que el software ha sido instalado, se procede a evaluar la cartera en dos partes: la primera, un análisis estadístico de la calidad de las secuencias producidas por el generador de números aleatorios en base al NIST SP 800-22; y la segunda, un análisis cualitativo de la funcionalidad de la cartera Bitcoin tanto a nivel de procesos como de operatividad. Finalmente se plantean las conclusiones de este trabajo, las recomendaciones y las futuras líneas de investigación y de desarrollo del proyecto.

PALABRAS CLAVE:

- **BITCOIN**
- **CARTERA BITCOIN**
- **CARTERA DE HARDWARE**
- **EVALUACIÓN DE ALEATORIEDAD**

ABSTRACT

This document describes the process of development, implementation and evaluation of a Bitcoin wallet prototype based on hardware. To this end, a general description of the Bitcoin network is made before reviewing in detail the Bitcoin wallet generation process and the cryptographic algorithms that governs it. It also describes the operation of P2PKH "Pay-To-Public-Key-Hash" transactions in order to let the reader know how the Bitcoin network interacts with Bitcoin wallets. Once the theoretical framework has been developed, the hardware and software design of the wallet is carried out based on objectives and design parameters. Then, hardware components are acquired and integrated, paying special attention to their communication and power interfaces. After that, a software application is developed in order to give functionality to the wallet prototype and incorporate a graphical user interface. Once all the devices have been integrated and the software has been installed, the evaluation of the wallet is made in two parts: first, a statistical analysis based on the NIST SP 800-22 test suite in order to evaluate the quality of the sequences produced by the random number generator; and second, a qualitative analysis of the functionality of the Bitcoin wallet, both at the process and operational levels. Finally, the conclusions, recommendations and future lines of research and development of this work are presented.

KEYWORDS:

- **BITCOIN**
- **BITCOIN WALLET**
- **HARDWARE WALLET**
- **RANDOMNESS EVALUATION**