Learning module 2: Encryption Techniques

Description

Blockchain technologies rely on wide variety of cryptographic primitives and techniques to ensure their functioning. Successive blocks in an ever-growing blockchain are linked together by means of cryptographic hash functions. Accounts on a blockchain are identified by cryptographic public keys and the corresponding private keys are used to authorize transactions. Encryption techniques are a core concept for the understanding of DLTs in general, and blockchains in particular.

Learning Module 2 introduces and describes in depth cryptography concepts that are central to blockchain technology. The basics principles of cryptography and cryptanalysis are presented in an initial overview. The concept of hash function is introduced, and examples of hash functions and their applications are given. Symmetric and asymmetric cryptography techniques are discussed in detail, with examples and a dedicated lab session. The concept of Zero-Knowledge Proofs is introduced and applications of cryptography in the blockchain space are discussed.

Dependencies

This module has no prerequisite.

Learning Objectives

- To introduce the key characteristics of cryptography and its possible uses in Blockchain.
- To comparatively present different cryptosystems and their evolution.
- To describe the concept of hash function and comparatively present a set of Hash Functions used in blockchain-based systems.
- To explain the fundamental concepts of symmetric and asymmetric cryptography systems.
- To present privacy-preserving cryptographic techniques and Zero-Knowledge Proofs.
- To illustrate how cryptographic techniques are applied in blockchain-based systems.
- To present relevant use cases built around Blockchain Cryptography.

Learning Outcomes

- **Understand** the key concepts in cryptography.
- **Examine** which cryptosystem is most adequate depending on the intended use case.
- **Identify** and **analyze** the different hash functions.
- **Identify** and **analyze** applications of symmetric and asymmetric cryptography.
- **Discuss** and **analyze** privacy-preserving cryptographic methods and Zero-Knowledge Proofs.
- **Identify** and **assess** applications of cryptographic methods in blockchain-based systems.
- **Examine** how encryption techniques are being utilized in relevant blockchain use cases.

The information and views set out in this publication are those of the authors and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

Syllabus

1. Introduction to Cryptography
    1.1. What is cryptography?
    1.2. Classification of cryptosystems
    1.3. Basic principles
    1.4. Main classical cryptosystems and evolution
    1.5. Perfect encryption conditions
    1.6. Cryptanalysis
2. Hash Functions
    2.1. What is a Hash function?
    2.2. Types of Hash functions: MD5, SHA-x
    2.3. Lab: experimenting with hash functions
3. Symmetric cryptography
    3.1. Definition
    3.2. Vernam, Flow and Block encryption
4. Asymmetric cryptography
    4.1. Definition
    4.2. Key exchange algorithms (Diffie-Hellman)
    4.3. RSA
5. Lab: experimenting with symmetric and asymmetric encryption
6. Zero-knowledge proofs
7. Applications of Blockchain Cryptography
    7.1. Application in QR exchanges
    7.2. Managing Bitcoin and Ethereum addresses
    7.3. Practice of block theory
8. Use-cases: Finance Sector, Health, Legal Services, Defense, Public Administration, Industrial Digitalization, Social Projects, Tackling poverty, Individual identity management