COURSE 03
Mastering Bitcoin Self-Custody
Course description

Course 03

Mastering Bitcoin Self-Custody, Security, and Strategies

Description

In an era where digital sovereignty is increasingly central, self-custody of one's bitcoins is not only a technical skill, but an act of personal responsibility. Mastering Bitcoin Self-Custody is a course designed for those who want to manage their bitcoin funds securely, knowledgeably, and independently, mastering the fundamental tools and strategies of self-custody.

Target participants

- Financial Advisors
- Asset managers
- Financial Professionals

Speaker

Dr. Marco Caldana

Materials

- Course presentation
- Summary sheets
- Access to selected Route Crypto Training resources

Contents

Elements of cryptography

- Definition and basic concepts
- Historical overview and examples
- Symmetric cryptography
- Main algorithms
- Asymmetric encryption
- Main algorithms
- Hybrid cryptographic systems
- HASH function
- The "CYPHERPUNK" movement

Course 03 - Mastering Bitcoin Self-Custody, Security, and Strategies

Cryptographic verification of downloaded software

- General considerations
- Objectives pursued
- Methods used
- What about smartphones?
- GPG in depth
- Practical examples
- Electrum software with Windows
- Sparrow software with Linux (Ubuntu) or Specter software with Mac OS

Generation of "secure" passwords

- "Classic" passwords
- Entropy: general concept and calculation
- Passphrases
- Diceware
- Additional tools
- Two-factor authentication (2FA)
- Passkey
- Password Manager

Anonymity and privacy systems

- TOR – The Onion Routing
- VPN - Virtual Private Network
- Additional elements that can be integrated into the course:
- Live OS (Tails)
- DNS – Domain Name Server
- Orbot

Bitcoin wallet

- Preliminary information
- Basic concepts
- What is a seed?
- What is a private key?
- What is a Bitcoin address?
- What is a UTXO?
- Types of wallets
- Points to consider
- Key best practices
- Wallets with special features
- Shamir's Secret Sharing (SSS)

Course 03 - Mastering Bitcoin Self-Custody, Security, and Strategies

Signing Devices

- Introduction
- Fundamental and distinctive features
- Brands and reference products

Functional design of a security framework

- Understanding threats (Threat Modeling)
- Possible/realistic scenarios and possible mitigations o External/exogenous causes o Internal/endogenous causes
- Practical implementation of a security setup

YouChainSwiss DAC
Digital Asset Classroom