Bitcoin and Cryptocurrency Technologies
Lecture 0: Class Structure Overview

Yuri Zhykin

Feb 17, 2025

Contacts

- @rodentrabies on Telegram
- https://github.com/rodentrabies

Course structure 1/2

- History and economics of Bitcoin
  - Economic concepts and properties of money
  - Computer cryptography and cypherpunk movement
  - Bitcoin invention and innovation
- Crypto means Cryptography
  - Cryptography basics
  - Hash functions
  - Public key cryptography
  - Elliptic curves
  - Cryptographic signatures
- Bitcoin chain data model
  - Transactions
  - Inputs and outputs
  - Blocks
  - Chain of blocks and Proof of Work

...

Course structure 2/2

...

- Deep dive into Bitcoin transactions
  - Transaction scripts
  - Transaction validation
  - Bitcoin wallets
- Bitcoin network
  - Peer-to-peer network architecture
  - Mempool and mining
  - Network parameters and dynamics
- Second layer protocols
  - Scalability problem
  - Payment channel networks
  - Non-fungible tokens
- Other cryptocurrency systems
  - Ethereum: maximum flexibility
  - Monero: maximum privacy

Assignments

- 2 lab tasks (first year)
  - Build and setup of a Bitcoin node software
  - Interaction with Bitcoin network from command line
- 1 lab task (second year)
  - Write a set of functions for parsing Bitcoin chain data
- Final test
  - 20/100 random single/multiple choice questions