Bitcoin Advanced Course

Monday & Tuesday intro

22.11.2021

A two-day whirlwind tour across Bitcoin's core concepts

Monday morning

- Elliptic curves
- Digital signatures
- DS exercise & setup

Monday afternoon

Transactions:

- Scripting, P2SH
- Timelocks, Timestamping
- SegWit
- Exercise: Spend a testnet P2PKH

Tuesday morning

- HD Wallets
- Blocks, mining
- Confirmation model
- Forks & Reorgs
- Exercise: HD Wallets

Tuesday afternoon

- SPV clients
- RSMCs / HTLCs
- Miniscript
- Exercises

Missing:

- P2P

Exercises: 1-1.5 hrs

`whoami`

Background: Computer science, neuroscience

Attended the inaugural 2018 course

Working in the space since mid-2019

Now: 21 Analytics, co-founded in 2020

Open-source: github.com/dspicher

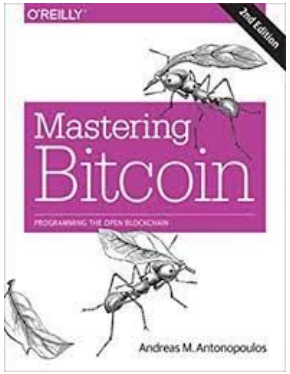
James Chiang

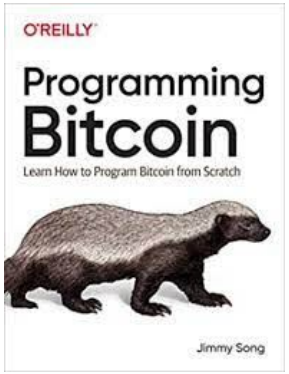
- https://teachbitcoin.io/
- All pretty slides
- The “bx” exercises set

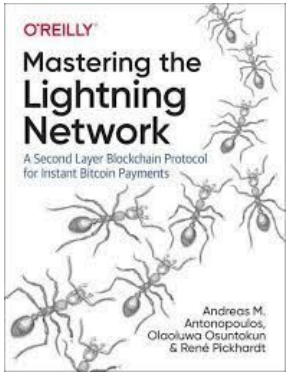
Buy him a beer!

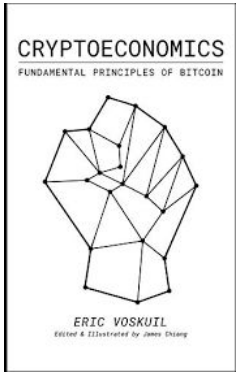
Resources


grokking
Bitcoin

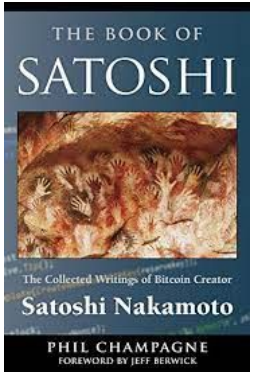

O'REILLY
2nd Edition
Mastering
Bitcoin
PROGRAMMING THE OPEN BLOCKCHAIN
Andreas M. Antonopoulos

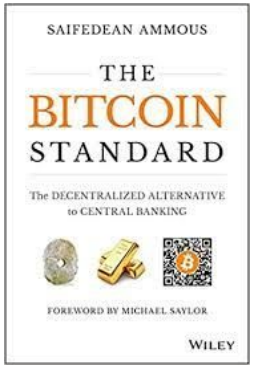

O'REILLY
Programming
Bitcoin
Learn How to Program Bitcoin from Scratch
Jimmy Song

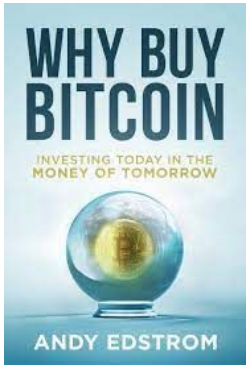

O'REILLY
Mastering the
Lightning
Network
A Second Layer Blockchain Protocol
for Instant Bitcoin Payments
Andreas M.
Antonopoulos,
Olaoluwa Osuntokun
& René Pickhardt

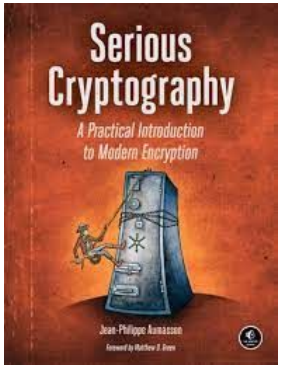

CRYPTOECONOMICS
FUNDAMENTAL PRINCIPLES OF BITCOIN
ERIC VOSKUIL


THE
BLOCKSIZE
WAR
JONATHAN
BIER
THE BATTLE
FOR CONTROL
OVER BITCOIN'S
PROTOCOL RULES


THE BOOK OF
SATOSHI
The Collected Writings of Bitcoin Creator
Satoshi Nakamoto
PHIL CHAMPAGNE
FOREWORD BY JEFF BERWICK


SAIFEDEAN AMMOUS
THE
BITCOIN
STANDARD
The DECENTRALIZED ALTERNATIVE
to CENTRAL BANKING
FOREWORD BY MICHAEL SAYLOR
WILEY


WHY BUY
BITCOIN
INVESTING TODAY IN THE
MONEY OF TOMORROW
ANDY EDSTROM


Serious
Cryptography
A Practical Introduction
to Modern Encryption
Jean-Philippe Aumasson

Other resources

- BIPs: the closest thing to a specification for Bitcoin
- Optech Newsletter
- Bitcoin from the command line
- Libbitcoin source code

Exercises

Two prepared exercises

- bx/2021_exercises
  - Spend P2PKH output prepared for you
  - Parent private key exposure for non-hardened BIP32 derivation

Two full sets:

- With “bx”, the libbitcoin explorer command line tool
  - More from the user’s perspective
- Using Python, from “Programming Bitcoin”, Jimmy Song
  - See how the sausage is made
- Explore!

Exercise setup

- Make sure container is not running
  - docker-compose down
- Get latest upstream changes
  - git pull --rebase
    - In both the root repo (where the docker-compose.yml file is)
      - All presentations
      - New Python dependency for exercise
      - Index for the Python exercises
    - And the exercises/bx repo
      - 2021_exercises
  - You might run into issues if you have changed things
- Rebuild container
  - docker-compose up --force-recreate --build
- Enjoy!