21 LECTURES

Bitcoin Masterclass

Intro

15.02.2024

`whoami`

Background: Computer science, Neuroscience

Attended the inaugural 2018 course

Working in the space since mid-2019

Now: 21 Analytics, co-founded in 2020, 21 Lectures, co-founded in 2023

Open-source: github.com/dspicher

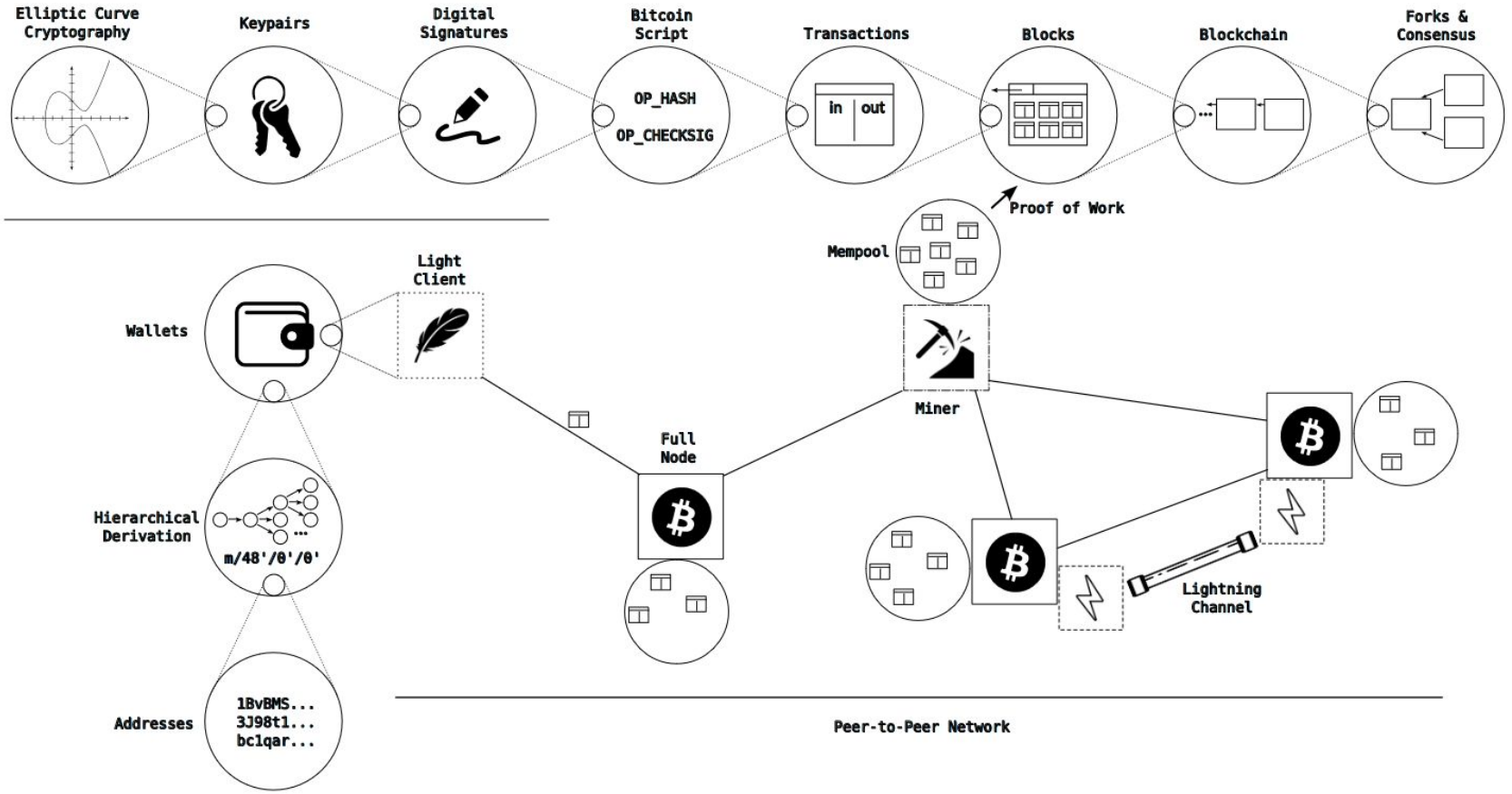
James Chiang

- https://teachbitcoin.io/
- Lots of slides
- The “bx” exercises set

Buy him a beer!

Course Goals

- Get a detailed understanding of how Bitcoin works on a technical level
  - Ready for 21 Lectures Masterclass
- Increase the scope for self-learning
- Meet like-minded people, discuss, network



Technical Concepts in Bitcoin

21 Lectures

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

Day 1 morning

- Elliptic curves
- Digital signatures
- Setup Works

Day 1 afternoon

Transactions:

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

Day 2 morning

- HD Wallets
- Blocks, mining
- Confirmation model
- Exercise: HD Wallets

Day 2 afternoon

- Forks & Reorgs
- Taproot
- SPV clients
- RSMCs / HTLCs
- Miniscript
- Exercises Contd.

Missing:

- P2P

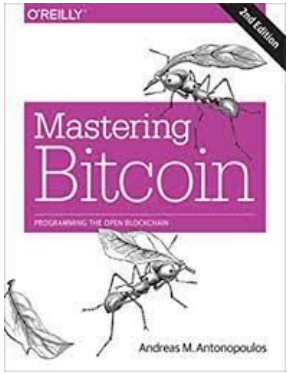
Exercises: 1-1.5 hrs

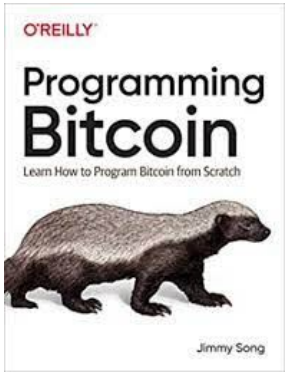
A day in the life of a Masterclass student

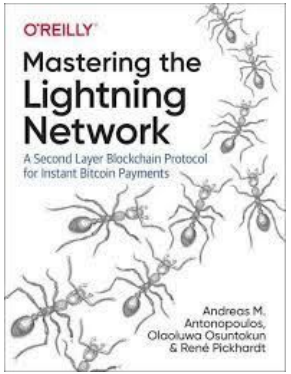
- Start 09:00
- ☕
- Lunch (included 🎉) 12:00
- Start Afternoon 13:15
- ☕
- End 17:00

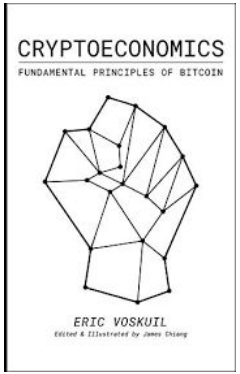
Resources


grokking
Bitcoin

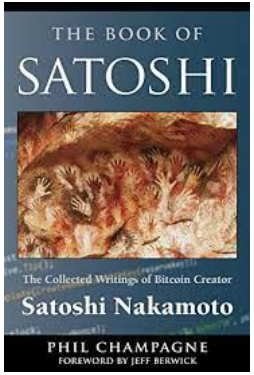

O'REILLY
2nd Edition
Mastering
Bitcoin
PROGRAMMING THE OPEN BLOCKCHAIN
Andreas M. Antonopoulos

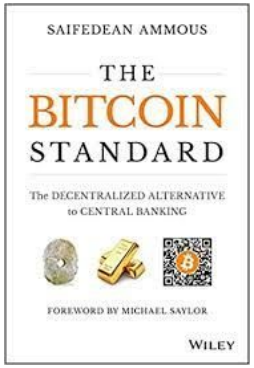

O'REILLY
Programming
Bitcoin
Learn How to Program Bitcoin from Scratch
Jimmy Song

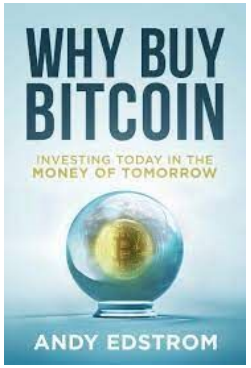

O'REILLY
Mastering the
Lightning
Network
A Second Layer Blockchain Protocol
for Instant Bitcoin Payments
Andreas M.
Antonopoulos,
Olaoluwa Osuntokun
& René Pickhardt

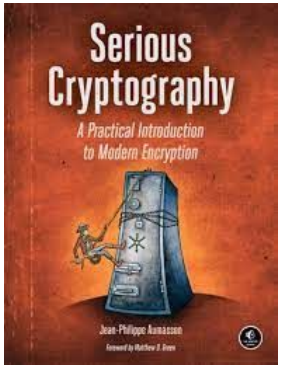

CRYPTOECONOMICS
FUNDAMENTAL PRINCIPLES OF BITCOIN
ERIC VOSKUIL


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

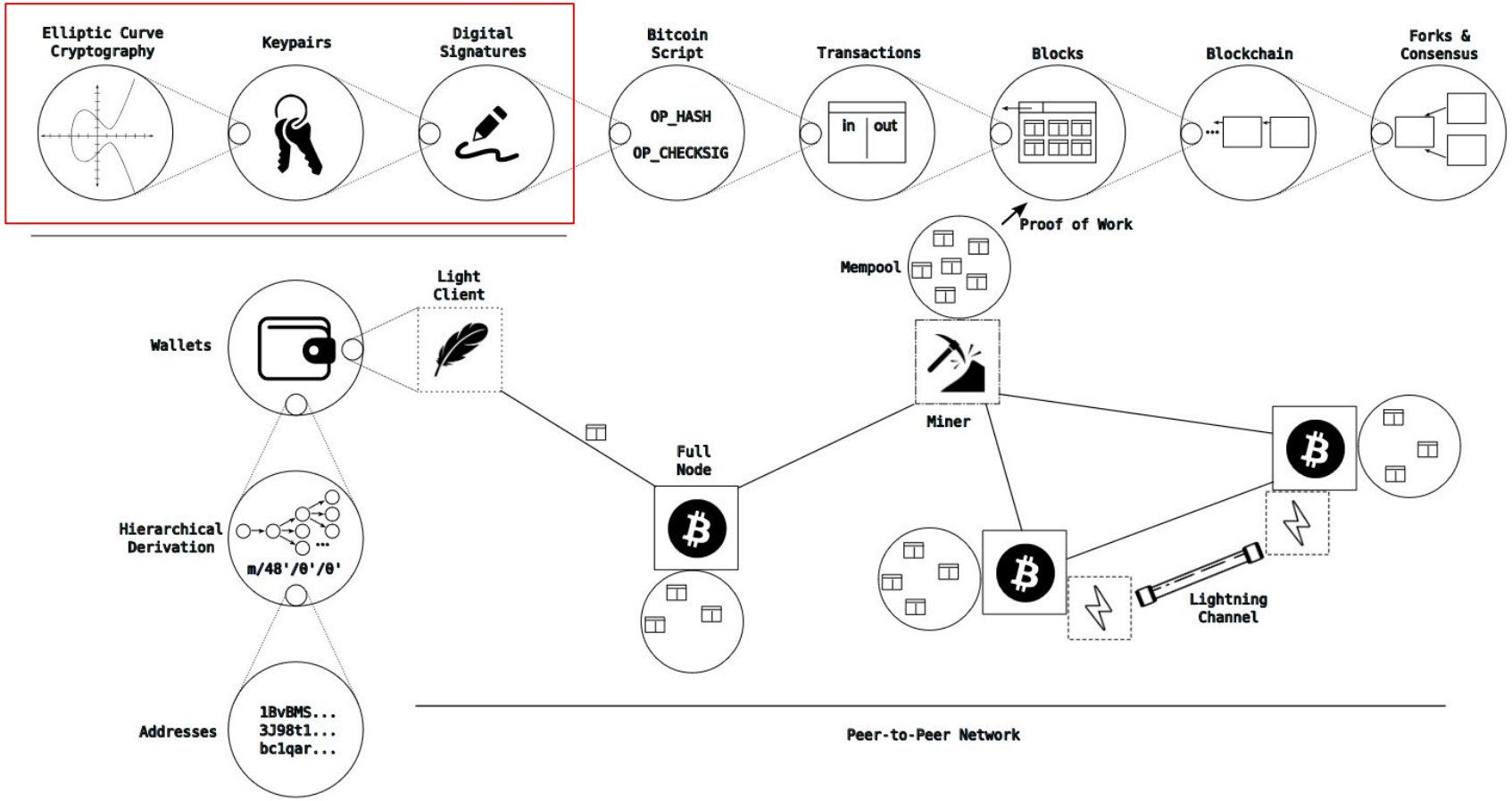
- exercises/2024_exercises
  - Spend P2PKH output prepared for you
  - Parent private key exposure for non-hardened BIP32 derivation

There is a full set of much more comprehensive exercises:

- With “bx”, the libbitcoin explorer command line tool
  - More from the user’s perspective
- Explore!

Finally …

this course is for you!



Technical Concepts in Bitcoin

21 Lectures