Blockchain and Cryptocurrencies

Introduction

Prof. Dr. Peter Thiemann

Albert-Ludwigs-Universität Freiburg, Germany

SS 2020

Coordinates

- **Course hours:** Mo 16:00/Th 14:00, Online
- **Staff:** Prof. Dr. Peter Thiemann

  Building 079, Raum 00-015
  Phone: 0761 203 -8051/-8247
  E-mail: thiemann@cs.uni-freiburg.de
  Web: http://www.informatik.uni-freiburg.de/~thiemann

- **Staff:** Dr. Thi Thu Ha Doan

  Building 079, Raum 00-013
  Phone: 0761 203 -8053
  E-mail: doanha@cs.uni-freiburg.de
  Web: http://www.informatik.uni-freiburg.de/~doanha

- **Homepage:**
  Ilias link
  https://proglang.informatik.uni-freiburg.de/teaching/blockchain/2020/

Administrivia

- ~90 minutes lecture/week
  - stream available via Ilias on Mondays after 16:10
  - specific time of live streaming will be announced
  - questions will be answered offline
- ~90 minutes exercise/week (usually on Thurdays, live via Zoom)
- Exercise questions available on Mondays after the lecture
  - posed as a test in Ilias
  - discussed in next available exercise session
  - no need to hand in exercises during the semester
  - final exam will be a scheduled test on Ilias

What's behind the course title?

Terminology

Ledger

- record of transaction history
- traditionally centralized
- unforgeable

Blockchain

- Decentralized implementation of a ledger
- Replicated across many peers
- Safeguard against noncompliant peers
- Consensus

Terminology II

Cryptocurrency

- digital money, represents value by a digital token
- implemented with cryptographic means
- successful implementations rely on blockchain

Remark

Monetary aspects mostly illustrated with Bitcoin

Terminology III

Nonmonetary Uses: DApps

- DApps = Decentralized Apps
- Smart contracts: storing and executing programs on the blockchain
- Many use cases: certificates, crypto assets, smart property, voting, IoT management, social networking, ...

Remark

- Ethereum: 1st generation blockchain with smart contracts
- Tezos: state-of-the-art

Contents

References

Much of the course relies on two books

- Bitcoin and Cryptocurrency Technologies (Princeton University Press)
  Videos available for many chapters from the book's webpage
- Bitcoin, Blockchain, and Crypto Assets (in German)

But we add further background material, e.g., from cryptography and original literature, to make the course self-contained.

Thanks!