Examinable material for IN5420/IN9420, Spring 2023

The introduction to the course and several of the topics refer to the following textbook:
"**Bitcoin and Cryptocurrency Technologies"**
by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder

I. DATA STRUCTURE (Merkle-tree)
https://blockonomi.com/merkle-tree/
https://brilliant.org/wiki/merkle-tree

MINING IN BITCOIN
a. Chapter 5 in the book
b. Alternative mining: Chapter 8 in the book, Section 6 in Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies

II. BITCOIN IN RESEARCH
a. **SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies**
by *Joseph Bonneau ; Andrew Miller ; Jeremy Clark ; Arvind Narayanan ; Joshua A. Kroll ; Edward W. Felten*
http://ieeexplore.ieee.org/abstract/document/7163021/
b. **On Scaling Decentralized Blockchains**
By *Kyle Croman and Christian Decker and Ittay Eyal and Adem Efe Gencer and Ari Juels and Ahmed E. Kosba and Andrew Miller and Prateek Saxena and Elaine Shi and Emin Gun Sirer and Dawn Xiaodong Song and Roger Wattenhofer*
http://www.comp.nus.edu.sg/~prateeks/papers/Bitcoin-scaling.pdf
c. **Majority is not Enough: Bitcoin Mining is Vulnerable**
The algorithm of selfish mining

III. BFT
a. https://en.wikipedia.org/wiki/Byzantine_fault_tolerance
b. **The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication**
by Marco Vukolich
https://link.springer.com/chapter/10.1007/978-3-319-39028-4_9

IV. Blockchain networking
a. **Survey on Blockchain Networking: Context, State-of-the-Art, Challenges**
(Sections 1 to 5)
b. **"Information propagation in the Bitcoin network"**
c. **"Understanding blockchain: definitions, architecture, design, and system comparison"**, Section IV.C

V. ETHEREUM
a. Chapter 10.7 in the book
b. **"Understanding blockchain: definitions, architecture, design, and system comparison",** Sections III.B and IV.D.2, as well as Ethereum-related text in Section IV.B

VI. HYPERLEDGER

a. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains
b. **"Understanding blockchain: definitions, architecture, design, and system comparison"**
Sections III.C and IV.D.3, as well as Fabric-related text in Section IV.B

VII. ALTERNATIVE CONSENSUS

a. (PhD students only)
Algorand: Scaling Byzantine Agreements for Cryptocurrencies
https://dl.acm.org/citation.cfm?id=3132757
b. **Bitcoin-NG: A Scalable Blockchain Protocol**
by Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, and Robbert van Renesse
https://www.usenix.org/node/194907
https://www.usenix.org/system/files/conference/nsdi16/nsdi16-paper-eyal.pdf

VIII. IOTA

a. **"Understanding blockchain: definitions, architecture, design, and system comparison"**, Sections III.D and IV.D.4, as well as IOTA-related text in Section IV.B
b. **"SoK: Diving into DAG-based Blockchain Systems"** (only Section 5)

IX. Zerocash

What are zero knowledge proofs and how they are relevant to blockchain

X. SCALING BLOCKCHAIN

a. Sidechains (Chapter 10.6 in the book)
b. **Building blocks of sharding blockchain systems: Concepts, approaches, and open problems** (only Sections 3.1, 6.1, 7.1, 8.1, 9.1)

XI. SMART CONTRACTS

a. **Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab**
https://eprint.iacr.org/2015/460.pdf
b. **Why Many Smart Contract Use Cases Are Simply Impossible**
c. Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts
https://arxiv.org/pdf/1804.05141.pdf

XII. ADVANCED BLOCKCHAIN STORAGE

a. **IPFS and Friends: A Qualitative Comparison of Next Generation Peer-to-Peer Data Networks**
b. When Blockchain Meets Distributed File Systems: An Overview,Challenges, and Open Issues (Only Sections I-III)

XIII. APPLICATIONS

a. **Healthcare: A Survey on Blockchain for Healthcare: Challenges, Benefits, and Future Directions**
b. A Blockchain-Based Framework for Supply Chain Provenance