Proposed topics for IN5420/IN9420, Spring 2018

Several of the topics refer to the following textbook:
"**Bitcoin and Cryptocurrency Technologies"**
by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder
A preprint is freely available, e.g. at
https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf

I. BITCOIN OVERVIEW
   a. Chapter 2 in the book
   b. Chapter 3 in the book

II. MINING IN BITCOIN
   a. Chapter 5 in the book
   b. Alternative mining: Chapter 8 in the book

III. DATA STRUCTURE (Merkle-tree and derivatives)
   a. http://en.wikipedia.org/wiki/Merkle_tree
   b. http://en.wikipedia.org/wiki/Patricia_tree
   c. https://easythereentropy.wordpress.com/2014/06/04/understanding-the-ethereum-trie/

IV. BITCOIN IN RESEARCH
   a. **Bitcoin under the hood** by *Aviv Zohar*
      https://dl.acm.org/citation.cfm?id=2701411
   b. **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/
   c. 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

V. ETHEREUM
   a. https://github.com/ethereum/wiki/wiki/White-Paper
   b. https://en.wikipedia.org/wiki/Ethereum
   c. https://www.coindesk.com/research/understanding-ethereum-report/
   d. Chapter 10.7 in the book

VI. CORDA
   a. https://docs.corda.net/_static/corda-introductory-whitepaper.pdf
   b. https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/
   c. https://docs.corda.net/

VII. HYPERLEDGER

a. http://www.thedata.co/sites/thedata.co/files/u1/Hyperledger%20Whitepaper.pdf
b. https://hyperledger-fabric.readthedocs.io/en/release/
c. Partial high-level comparison between the three major implementations: Table 1 in https://medium.com/@philippsandner/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6
d. A benchmark that compares Hyperledger with Ethereum http://www.comp.nus.edu.sg/~ooibc/blockbench.pdf

VIII. BFT

a. https://en.wikipedia.org/wiki/Byzantine_fault_tolerance
b. Practical Byzantine Fault-Tolerance
by Barbara Liskov and Miguel Castro
http://pmg.csail.mit.edu/papers/osdi99.pdf
c. 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

IX. ALTERNATIVE CONSENSUS

a. **Algorand: Scaling Byzantine Agreements for Cryptocurrencies**
by Gilad, Yossi and Hemo, Rotem and Micali, Silvio and Vlachos, Georgios and Zeldovich, Nickolai
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

X. SCALING BLOCKCHAIN

a. Sidechains
Chapter 10.6 in the book
b. **Enabling blockchain innovations with pegged sidechains**
by Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille
https://blockstream.com/sidechains.pdf
(only the overview, no need to study the paper thoroughly)
c. https://web.archive.org/web/20151212001135/http://blog.sldx.com/three-challenges-for-scaling-bitcoin/
Overview of a number of ideas
d. braiding
https://scalingbitcoin.org/hongkong2015/presentations/DAY2/2_breaking_the_chain_1_mcelrath.pdf
e. treechains
http://www.mail-archive.com:80/bitcoin-development@lists.sourceforge.net/msg04388.html

XI. SMART CONTRACTS

a. **Formalizing and Securing Relationships on Public Networks**
   Nick Szabo
   http://ojphi.org/ojs/index.php/fm/article/view/548/469
   First introduction of the concepts
b. Section II.D in **Blockchains and Smart Contracts for the Internet of Things**
   Konstantinos Christidis and Michael Devetsikiotis
   http://ieeexplore.ieee.org/document/7467408/
c. **Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab**
   Kevin Delmolino, Mitchell Arnett, Ahmed Kosba, Andrew Miller, and Elaine Shi
   https://eprint.iacr.org/2015/460.pdf
d. **Making smart contracts smarter**
   Luu, Loi and Chu, Duc-Hiep and Olickel, Hrishi and Saxena, Prateek and Hobor, Aquinas
   https://dl.acm.org/citation.cfm?id=2978309

XII. ADVANCED BLOCKCHAIN STORAGE

a. **IPFS white paper**
   https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf
b. Selected info and responses to questions in
   https://github.com/ipfs/faq/issues/47
c. **A Secure Sharding Protocol For Open Blockchains**
   Luu, Loi and Narayanan, Viswesh and Zheng, Chaodong and Baweja, Kunal and Gilbert, Seth and Saxena, Prateek
   https://dl.acm.org/citation.cfm?id=2978389
   (skip the proofs in Section 4)

XIII. APPLICATIONS

a. **Blockchains and Smart Contracts for the Internet of Things**
   Konstantinos Christidis and Michael Devetsikiotis
   http://ieeexplore.ieee.org/document/7467408/
b. **LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy**
   Ali Dorri, Salil S. Kanhere, Raja Jurdak, Praveen Gauravaram
   https://arxiv.org/abs/1712.02969
c. **Providing Privacy, Safety, and Security in IoT-Based Transactive Energy Systems using Distributed Ledgers**
   Aron Laszka, Abhishek Dubey, Michael Walker, Douglas Schmidt
   https://arxiv.org/abs/1709.09614

Side note: Unfortunately, we will not have time to study about privacy in Bitcoin. Interested students are welcome to read Chapter 6 in the book.