IN5420/IN9420 - Distributed Blockchain Technologies

List of topics and reading material - Spring 2022

You can find below the list of 14 topics to be covered in the course, along with the relevant materials. Some topics refer to the following textbook: “Bitcoin and Cryptocurrency Technologies” by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. You can download it here. Chapters 2 and 3 are left for self-study, as well as the Bitcoin paper. Optional material can be found at the end of this document.

1) **Bitcoin:** we start the course with the first Blockchain platform. This topic focuses on the data structure and how mining and proposing blocks work in Bitcoin.
    - Data structure: how the blockchain is structured and what are the advantages
        - Merkle tree 1
        - Merkle tree 2
    - PoX for Bitcoin:
        - “Bitcoin mining”: chapter 5 in the book
        - “Alternative Mining Puzzles”: chapter 8 in the book
        - Section 6 of Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies

2) **Beyond Bitcoin:** this topic should focus on the future opportunities and challenges of blockchain technologies, beyond what Bitcoin can do. How to improve the Bitcoin design to build new infrastructures that can support many different applications?
    - General perspectives: SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies
    - Scaling: On Scaling Decentralized Blockchains
    - Decentralizing applications: A Survey of Decentralizing Applications via Blockchain: The 5G and Beyond Perspective (only Sections 4 and 5)

3) **Byzantine Fault Tolerance:** this topic focuses on the “traditional” BFT consensus algorithms, and how they differ to consensus in blockchain technologies (deterministic vs probabilistic).
    - For additional background (optional for the course) you may check the Wikipedia page
    - Practical Byzantine Fault Tolerance
    - The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication

4) **Blockchain Networking:** this topic focuses on networking aspects of blockchain technologies, such as transaction and block propagation, and P2P overlay topology. What is the impact of these aspects in the security and performance of blockchain systems?
    - Survey on Blockchain Networking: Context, State-of-the-Art, Challenges (Sections 1 to 5)
    - Information propagation in the Bitcoin network
    - Topology: Perigee: Efficient Peer-to-Peer Network Design for Blockchains
    - Accelerating propagation: PiChu: Accelerating Block Broadcasting in Blockchain Networks with Pipelining and Chunking

5) **Ethereum:** this topic focuses on understanding the design of Ethereum. In particular, the differences between Ethereum and Bitcoin: data structure, consensus algorithm, smart contract support, migration to Proof-of-Stake, etc.
    - "Ethereum and Smart Contracts": chapter 10.7 in the book
    - Ethereum whitepaper
    - Trie database in Ethereum
    - Ethereum 2.0 upgrades
    - Migration towards PoS FAQ

6) **Hyperledger Fabric:** this topic focuses on understanding Hyperledger Fabric as a representative of permissioned blockchain systems, and how it differs from permissionless systems such as Ethereum.
    - Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains
    - Hyperledger Fabric documentation
    - Comparison of Ethereum, Hyperledger Fabric and Corda (ignore Corda)

7) **Alternative Consensus 1:** the focus of this topic is on alternative consensus algorithms other than what was studied before in the course. What is the impact of these alternatives in the system design (data structures, for example), and what are their advantages over more conventional algorithms (such as Proof-of-Work)?
    - Scalable and Probabilistic Leaderless BFT Consensus through Metastability (Appendix excluded)
    - Algorand: Scaling Byzantine Agreements for Cryptocurrencies

8) **Alternative Consensus 2:** the focus of this topic is on alternative consensus algorithms other than what was studied before in the course. What is the impact of these alternatives in the system design (data structures, for example), and what are their advantages over more conventional algorithms (such as Proof-of-Work)?
    - Bitcoin-NG: A Scalable Blockchain Protocol
    - Blockene: A High-throughput Blockchain over Mobile Devices
    - Deconstructing Blockchains: A Comprehensive Survey on Consensus, Membership and Structure (only Section IV specifically PoX not covered in topic 1b)

9) **IOTA:** this topic focuses on understanding IOTA as a representative of DAG-based blockchain systems. What are the advantages and challenges of building the ledger as a DAG instead of a linear chain?
    - Five parts illustrated tutorial by Alon Gal
    - The Tangle (ignore the mathematical proofs)
    - The Coordicide (only Sections 1, 2, 3 and 6.1: how the coordinator is being removed?)
    - SoK: Diving into DAG-based Blockchain Systems (only Sections 6.1, 6.3, 6.4, 6.6)
    - Other IOTA papers (optional)

10) **Zerocash:** this topic focuses on understanding the concept of zero-knowledge proofs and their applications, by taking Zerocash as a representative system.
    - zk-SNARKs
    - A Survey of Zero-Knowledge Proofs with Applications to Cryptography
    - Zerocash: Decentralized Anonymous Payments from Bitcoin (no need to read the Appendix)

11) **Scaling Blockchain:** the goal of this topic is to go deeper into more advanced scaling mechanisms (sidechains and sharding).
    - Sidechains:
        - Chapter 10.6 of the book
        - Ethereum “layer 2”
        - The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments
    - Sharding: Monoxide: Scale out Blockchains with Asynchronous Consensus Zones

12) **Smart Contracts:** this topic focuses on understanding what smart contracts are, their applications and challenges.
    - Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab
    - A Massive Analysis of Ethereum Smart Contracts Empirical Study and Code Metrics
    - Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts
    - Why Many Smart Contract Use Cases Are Simply Impossible

13) **Blockchain Storage:** the focus of this topic is on different decentralized storage protocols often used along with blockchain technologies for off-chain storage. Examples include IPFS/Filecoin, Sia, Storj, Arweave, among others. How do they work, and what are the trade-offs between on-chain and off-chain storage?
    - IPFS and Friends: A Qualitative Comparison of Next Generation Peer-to-Peer Data Networks
    - When Blockchain Meets Distributed File Systems: An Overview, Challenges, and Open Issues (Only Sections I-III)

14) **Applications:** this topic covers the usage of blockchain technologies to build real-world applications in different scenarios. How do these systems leverage blockchain technologies to support the different use cases?
    - Healthcare: MedRec: Using Blockchain for Medical Data Access and Permission Management
    - Supply chain: A Blockchain-Based Framework for Supply Chain Provenance
    - IoT: Blockchain- and IPFS-Based Data Distribution for the Internet of Things
    - Machine Learning: A Blockchain-based Decentralized Federated Learning Framework with Committee Consensus

Optional, additional material for the interested students:

- Critical analysis of whether you actually need a blockchain: Do you need a Blockchain?
- Escrow protocols for cryptocurrencies: How to buy physical goods using Bitcoin
- Town Crier: An Authenticated Data Feed for Smart Contracts
- Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing
- A Formal Foundation for Secure Remote Execution of Enclaves (good coupled with Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts)
- BigchainDB 2.0 The Blockchain Database
- Although becoming outdated, BLOCKBENCH: A Framework for Analyzing Private Blockchains is an interesting effort to evaluate and compare different blockchain systems within a single framework.

- Online Payments by Merely Broadcasting Messages proposes a decentralized payment system that does not require consensus: it is replace by another primitive called byzantine reliable broadcast, which can achieve better performance.
- Lay Down the Common Metrics: Evaluating Proof-of-Work Consensus Protocols' Security presents interesting metrics to measure the security of blockchain systems

You can also find more useful material in the following websites:

- GitHub repository
- Coindesk
- Zkcapital (available through mailing list subscription as well)