Special Topics Course

Title: Foundations of Blockchains
Instructor: Anastasios Sidiropoulos

Method of instruction: The instruction will be based on the following main components:

- During the first half of the course, the instructor will present various fundamental methods and ideas used in the design of blockchains, cryptocurrencies, and related objects. Any necessary prerequisites will also be discussed during this time.
- During the second half of the course, the students will read and present research papers.
- The students will work on a project of their interest that incorporates ideas discussed in the class. The students will have the option to either conduct original research or experimentally evaluate prior work. The project will be performed in teams of 1–3 students. The students will be encouraged to start thinking about possible research topics early in the semester. The instructor will hold frequent meetings with each team to guide their progress.

Narrative description: A blockchain is a tamperproof sequence of data that can be read and augmented by everyone. The first widely used implementation of such a structure, proposed by Satoshi Nakamoto, is the Bitcoin protocol. Blockchains have found numerous applications, such as cryptocurrencies and smart contracts, and hold the potential to revolutionize the way a democratic society operates.

From the scientific point of view, blockchains present several new exciting opportunities, as well as technical challenges. The intellectual underpinnings of the design of such public ledgers lie in the intersection of cryptography, distributed computing, algorithms, game theory, and economics. This unique combination of diverse scientific disciplines necessitates the development of new theoretical foundations for this emerging area. Consequently, a new intellectual framework has started emerging for reasoning about public ledgers, their powers and limitations.

Goal: In this course, the students will be exposed to the theoretical foundations underpinning the design and operation of blockchains. Emphasis will be given on understanding how the properties of blockchains lead to several other important primitives, such as cryptocurrencies, smart contracts, digital assets, and so on. Furthermore, the students will learn about important technical advances, such as scaling, transaction routing, energy consumption, and so on.

Student deliverables: The students will have to read all the papers, and they will be expected to actively participate in all the lectures. Furthermore, each student will present at least one research paper to the class. For the final project, the students will have to submit a proposal of their selected topic within the first half of the course, a final report at the end of the class, and they will be asked to give a brief presentation on their findings.

Class meetings: There will be two 75' meetings per week.

Prerequisites: The course will be accessible to students with a wide range of backgrounds, including both theoretical and applied areas of computer science. Some familiarity with discrete math (equivalent to CS 201), algorithms (equivalent to CS 401) and computability theory (equivalent to CS 301) will be assumed. All necessary cryptographic primitives (elements of public key cryptography, zero knowledge proofs, elliptic curve cryptography, and so on) will be introduced during the course.

Exams: There will be no exams.

Readings: Selected books and research papers from the following tentative list of topics:

Byzantine Agreement: What is the Byzantine generals problem? How does Nakamoto consensus solve the token distribution problem?

Game-theoretic aspects of blockchains: Is the Bitcoin protocol incentive-compatible? How can we mathematically analyze chain forks?

The Bitcoin protocol and its extensions: What is the Bitcoin Backbone protocol? Can we verify parts of a blockchain without reading the whole list of blocks? What are Non-interactive Proofs of Proof of Work?

Network-theoretic aspects of blockchains: What is a peer-to-peer network? What is an eclipse attack? How does this affect the security of cryptocurrencies?

Energy consumption: The Nakamoto consensus is based on a "proof of work" algorithm, which uses an enormous amount of energy. Several other "proof of stake" protocols have been proposed that try to mitigate this issue (Algorand, Fruitchains, Ouroboros, etc). How do these protocols work?

Scalability: The Bitcoin protocol can support only a limited number of transactions per second. Recent theoretical work suggests that this is an inherent limitation of blockchains. In order to bypass this obstacle, various other, so-called "second-layer" algorithms and protocols have been proposed. Some of these proposed solutions include the lightning network, plasma, rollups, side-chains, and so on. How do these work?

Turing-completeness: The Bitcoin protocol supports only a limited number of types of transactions, specified as the Bitcoin script language. This language is powerful enough to program various interesting primitives, such as inter-blockchain transactions, the lightning network, and so on. However, this language is not Turing-complete. Many other blockchains have been created (e.g., Ethereum, Cardano, and so on) that provide a Turing-complete set of transactions, and can be used to implement arbitrary mechanisms, such as voting, governance, public registries, and so on.

Economic aspects of blockchains: The construction of blockchains with Turing-complete languages has lead to the implementation of a plethora of financial primitives that operate without a central authority. These include: decentralized autonomous organizations (DAOs), algorithmic stable coins, automated marked makers, trustless loans, and so on.

Beyond blockchains: Motivated by the success of applications that run on a single blockchain, researchers have proposed various mechanisms for transferring value and state across different blockchains. These include, Polkadot, Chainlink, and so on. How do these systems work? What are the underlying theoretical guarantees of such systems?

Sample of relevant papers:

- Xi Chen, Christos Papadimitriou, Tim Roughgarden, *An Axiomatic Approach to Block Rewards.*
- J Garay, A Kiayias, N Leonardos, *The bitcoin backbone protocol: Analysis and applications.*
- A Kiayias, A Russell, B David, R Oliynykov, *Ouroboros: A provably secure proof-of-stake blockchain protocol.*
- A Kiayias, A Miller, D Zindros, *Non-interactive proofs of proof-of-work.*
- J Chen, S Micali, *Algorand.*
- Y. Gilad, R. Hemo, S. Micali, G. Vlachos, N. Zeldovich, *Algorand: Scaling Byzantine Agreements for Cryptocurrencies.*
- I Eyal and E G Sirer. *Majority is not Enough: Bitcoin Mining is Vulnerable.*
- S Tochner, A Zohar. *How to Pick Your Friends - A Game Theoretic Approach to P2P Overlay Construction.*
- Lewis Gudgeon, Sam Maximilian Werner, Daniel Perez, William J. Knottenbelt. *DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency.*