

Department of Mathematics

Cryptocurrency Crash Course

Dr. Artem Kotelskiy

(cyber.fund)

Title: Blockchains' Past, Present, and Future

About the course: Join us for a captivating series of lectures organized by the Department of Mathematics. Dr. Artem Kotelskiy, a Princeton-educated mathematician from cyber.fund, will delve into the fascinating world of blockchains. Discover the background and motivation behind this revolutionary technology, as well as insights into cryptocurrencies like Bitcoin and Ethereum. Sessions are scheduled for Thursday, April 25, 2024, from 9:30 to 10:30 am, 11:00 am to 12:00 pm, and 2:00 to 3:00 pm at JD 1600. Open to the public, no specific background knowledge required.

About the Speaker: The first 10 years of Artem's career were devoted to pure mathematics – he was studying knots and manifolds in places like Princeton, Indiana and Stony Brook Universities. He was interested in the blockchain space as early as 2015 – on the side he did both researching and investing in the space. Two years ago he taught a successful course on blockchains in Stony Brook (artofkot.xyz/blockchain-course), and last year Artem decided to dive into the space full-time, as a research lead in a venture fund (cyber.fund).

Thursday April 25, 2024

9:30-10:30, 11:00-12:00, 2:00-3:00

ROOM: JD 1600

Host: Ali Pakzad

Dr. Artem Kotelskiy

(cyber.fund)

Thursday April 25, 2024

Room: JD 1600

Cryptocurrency Crash Course: Blockchains' Past, Present, and Future

9:30-10:30 AM In the first lecture we present the background and motivation for blockchains. In particular, we will go through the following sequence of concepts: *need for scaled coordination → centralized systems → distorted incentives to keep rules in check, censorship, single point of failure → distributed systems, SMR problem → collusion problem → neutral, permissionless consensus → incentives & Sybil problems*

11:00-12:00 PM In the second lecture, we will see how Bitcoin has solved the fundamental problem in computer science – making consensus protocol permissionless. Namely, we will go into the basics of required cryptography (digital signatures & hash functions), as well as explain the proof-of-work Sybil resistance mechanism, and Bitcoin's incentives structure to run the network.

2:00-3:00 PM In the third lecture we will examine innovations brought by Ethereum. Namely, we will start with its core functionality called "smart contracts", which allow for programmable incentives and coordination via a distributed compute. After that we will touch upon the biggest product-market-fit of Ethereum – Decentralized Finance, a financial ecosystem built on smart contracts. We will then also cover proof-of-stake, a new much more efficient Sybil resistance mechanism, recently implemented by Ethereum. Time-permitting, we may touch the current challenges in blockchain research, related to scalability & privacy.

Host: Ali Pakzad