

**BIU**Center for Research in Applied
Cryptography and Cyber Security
Bar-Ilan UniversityFeb
20-23
2023

THE
13TH
BIU WINTER SCHOOL
ON CRYPTOGRAPHY



Blockchain Technologies

School organizers: Ittai Abraham, Gilad Asharov, Mor Weiss and Eylon Yogev

Monday | February 20, 2023

Part 1 – Introduction

08:15-08:45	Registration
08:50-09:00	Opening remarks
09:00-10:00	Dan Boneh: What are Blockchains and What Are They For?
10:00-10:15	Coffee break
10:15-11:15	Valeria Nikolaenko: An Overview of PoW and PoS Consensus
11:15-11:30	Coffee break
11:30-12:30	Dan Boneh: An Overview of the Ethereum Execution Layer
12:30-14:00	Lunch
14:00-15:00	Arthur Gervais: CeFi Versus DeFi
15:00-15:15	Coffee break
15:15-16:15	Valeria Nikolaenko: Hard Problems in Blockchains
16:15-16:30	Coffee break
16:30-17:30	Arthur Gervais: The Risk of Censorship and De-anonymization

Wednesday | February 22, 2023

Part 2 – Proofs: Privacy, Scaling and Bridges (continue)

09:00-10:00	Mary Maller: How Custom Gates Are Used During Arithmetization
10:00-10:15	Coffee break
10:15-11:15	Mary Maller: A Close Look at a Lookup Argument
11:15-11:30	Coffee break
Part 3 - Consensus and Data Availability	
11:30-12:30	Rafael Pass: Permissionless Consensus I
12:30-14:00	Lunch
14:00-15:00	Rafael Pass: Permissionless Consensus II
15:00-15:15	Coffee break
15:15-16:15	Valeria Nikolaenko: Data Availability Sampling, Data Dispersal and Reconstruction
16:15-16:30	Coffee break
16:30-17:30	Alexander Spiegelman: DAG Meets BFT & Theory Meets Practice

Tuesday | February 21, 2023

Part 2 – Proofs: Privacy, Scaling and Bridges

09:00-10:00	Dan Boneh: What Are Snarks and What Are They Good For?
10:00-10:15	Coffee break
10:15-11:15	Eli Ben Sasson: A Cambrian Explosion of Cryptographic Proofs
11:15-11:30	Coffee break
11:30-12:30	Eli Ben Sasson: Arithmetization - What's Algebra Got to Do With It? + From Fri to Polynomial Commitment Schemes
12:30-14:00	Lunch
14:00-15:00	Dan Boneh: Proving Properties of Committed Polynomials, and the Derived Snarks
15:00	Excursion

Thursday | February 23, 2023

Part 4 – DeFi and MEV

09:00-10:00	Arthur Gervais: Decentralized Exchanges, Sandwich, Arbitrage
10:00-10:15	Coffee break
10:15-11:15	Arthur Gervais: Lending, Liquidations, Stablecoins
11:15-11:30	Coffee break
11:30-12:30	Valeria Nikolaenko and Dan Boneh: MEV and Fair Ordering
12:30-14:00	Lunch
14:00-15:00	Arthur Gervais: DeFi Attacks
15:00-15:15	Coffee break

Part 5 – Crypto Wallets

15:15-16:15	Yehuda Lindell: Building Blockchain Wallets - Challenges and Solutions
16:15-16:30	Coffee break
16:30-17:30	Yehuda Lindell: Building Blockchain Wallets - Technical Details

This school is sponsored by

Gold



Silver

ALEPH
ZERO

STARKWARE

Technology
Innovation
Institute

Bronze

ESPRESSO
SYSTEMSethereum
foundation