# CURSO BLOCKCHAIN

## INSTRUCTORES BLOCKCHAIN AT BERKELEY

## University of California at Berkeley

BLOCKCHAIN AT BERKELEY

PONENTES LÍDERES MUNDIALES

Nadir Akhtar • Aparna Krishnan

**1.** BITCOIN PROTOCOL AND CONSENSUS:
A HIGH LEVEL OVERVIEW
- Consensus Buildup.
- Blockchain tech implications.

**2.** BLOCKCHAIN HISTORY:
FROM THE CYPHERPUNK MOVEMENT TO JPMORGAN CHASE
- Libertarian dreams, ideals, intentions.
- Prebitcoin-2010 The early development of Bitcoin.
- 2010-2012: The rise and fall of the early Bitcoin companies.
- 2013-2014:Bitcoin becomes. mainstream (bubble), The rise of altcoins.
- 2013-2014: The first wave of Bitcoin-oriented startups: Coinbase - successful.
- 2015: Scalability and Lightning. Networks, Ethereum + the DAO.
- 2015: The rise of interest in "blockchain" from the private companies.
- Where does the community exist?
- General statement on consensus.
- 2016: Privacy centric coins Zcash + Monero.
- 2017: Bubble in 2017- ethereum + ICOs, ETF filings , ICOs - SEC ruling.

**3.** BITCOIN MECHANICS AND OPTIMIZATIONS:
A TECHNICAL OVERVIEW
- Cryptographic Hash Functions.
- Cryptography! ECDSA!.
- Bitcoin Mechanics.

EXTRA:
- Additionally Privacy.

**4.** BITCOIN
IRL
- Wallets
- Wallet Mechanics.
- Mining Incentives.
- Real World Mining.
- Bitcoin Governance.

**5.** ETHEREUM & SMART CONTRACTS:
ENABLING A DECENTRALIZED FUTURE
IRL
- Bitcoin scripting => EVM.
- Smart contract examples (Philip's smart contract (or our own).
- Protocol features: Bitcoin vs. Ethereum.
- Differences from bitcoin- Account based.
- Smart Contracts introduction.
- Basic use cases.
- Advanced use cases
- DAOs
- Building intuition: Dapp generalizations.
- Technical limitations of blockchain technology.
- What blockchain isn't good for.
- Slide explaining when we should use a blockchain - with all the use cases.
- Vision for smart contracts.

**6.** GAME THEORY & NETWORK ATTACKS:
HOW TO DESTROY BITCOIN
- [2.3 Double spend][5.5 Forking attack].
- Network Attacks.
- Malicious Mining Profit Strategies.
- Proof that 51% attacking Bitcoin is profitable.
- A way to offset cost of pool wars.
- Lemmas 1,2,3.
- Additional ideas.
- Generalization of Vulnerabilities.
- Post block reward bitcoin.
- Overview of definitions.
- Somewhere: Merge Mining.

**7.** CRYPTOECONOMICS
- Definitions
- [8.5 Proof-of-Stake and Virtual Mining].
- Attacks on Proof of Stake and potential defenses against them.

**8.** ALTERNATIVE
CONSENSUS
- Formal definition of consensus.
- Proof-of-Work-ish Consensus Mechanisms.
- Proof of Stake.
- Voting-based Consensus Algorithms.
- Federated Consensus.

**5 AL 8 DE ABRIL 2018**

CENTRO DE CIENCIAS DE LA COMPLEJIDAD, UNAM

C D M X

info@blockchainexpertise.mx
www.blockchainexpertise.mx

BLOCKCHAIN Expertise MX

LUMIT BLOCKCHAIN TECHNOLOGIES