BBM 443
Fundamentals of Blockchain

BBM 443 – Fundamentals of Blockchain

- Instructor : Adnan Özsoy
- Friday 13.45 – 16.30 @ D8
- adnan.ozsoy@hacettepe.edu.tr
- Office : 114

Course Objectives

“This course provides a thorough understanding of the fundamental concepts and recent advances in blockchain and cryptocurrencies. The main objective is to provide students practical and theoretical foundations to use and develop applications using the blockchain technology and can solve challenging problems in cryptocurrencies.”

Not Course Objectives

- Make you rich $$$
- Give insider information
- Create money out of thin air
- Teach you magic

Course Outline

11.Oct	Lecture 1: Introduction
18.Oct	Lecture 2: Blockchain Fundamentals
25.Oct	Lecture 3: Bitcoin Mechanics
1.Nov	Lecture 4: Ethereum and Smart Contracts
8.Nov	Lecture 5: Distributed Application Development
15.Nov	Lecture 6: Wallets, Mining, Pools
22.Nov	Lecture 7: Blockchain Security
29.Nov	Lecture 8: Scaling Blockchain
6.Dec	Lecture 9: Midterm
13.Dec	Lecture 10: Consensus Algorithms
20.Dec	Lecture 11: Real-World Applications
27.Dec	Lecture 12: Cryptocurrency Ecosystem
3.Jan	Lecture 13: Presentation
10.Jan	Lecture 14: Presentation

Resources

Text Book

- Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction Hardcover, Arvind Narayanan, Joseph Bonneau, Edward Felten,Andrew Miller,Steven Goldfeder, 2016
Free pre-publication draft @ http://bitcoinbook.cs.princeton.edu/
- Mastering Bitcoin: Programming the Open Blockchain 2nd Edition, Andreas M. Antonopoulos, 2017

Reference Material

- Blockchain Berkeley : https://blockchain.berkeley.edu/decal/sp19/fund/
- Blockchain Princeton : http://bitcoinbook.cs.princeton.edu/
- Mastering Ethereum, by Andreas M. Antonopoulos, Gavin Wood https://ethereumbook.info/, https://github.com/ethereumbook/ethereumbook/blob/develop/book.asciidoc

Grading

Project	: 20 % - 1 project - individual
Attendance	: 5 % - not mandatory
Final Exam	: 50 %
Final Report	: 25 % - Group of 4-5

Project

- Project
  - Solidity
  - Individual project

Final Report

- Need to start immediately
- Group Project
- Pick a topic where Blockchain can help
- Review Literature, compare state-of-the-art technologies
- Propose a solution, model,
- Present your work
- Bonus for implementation

Communication & Course Material

https://piazza.com/hacettepe.edu.tr/fall2019/bbm443

Basic Concepts

How all started???

Pre Bitcoin-2009:

Libertarian Dreams and Ideals

Libertarian Dreams

- With the advance of technology in the 1980s and 90s, the Cypherpunk movement came into being
- Cypherpunk Manifesto: “Privacy is necessary for an open society in the electronic age.”
- Roots in libertarianism and cryptography

Libertarianism is a political ideology advocating the non-aggression principle and laissez faire government
(transactions between private parties are free from government intervention such as regulation, privileges, tariffs and subsidies.)

Cryptography is the science of securing communication in the presence of third parties

Cypherpunks and Crypto-Anarchists

- Cypherpunks were obsessed over how technology would change the relationship between the individual and the state
- Hopeful about the new tools people had but concerned about how people could protect their personal information and maintain their privacy from government

Untraceable Electronic Cash †

(Extended Abstract)

David Chaum[1] *Amos Fiat*[2] *Moni Naor*[3]

[1] Center for Mathematics and Computer Science
Kruislaan 413, 1098 SJ Amsterdam, The Netherlands

[2] Tel-Aviv University
Tel-Aviv, Israel

[3] IBM Almaden Research Center
650 Harry Road, San Jose, CA 95120

CRYPTO 1988

DigiCash™

David Chaum

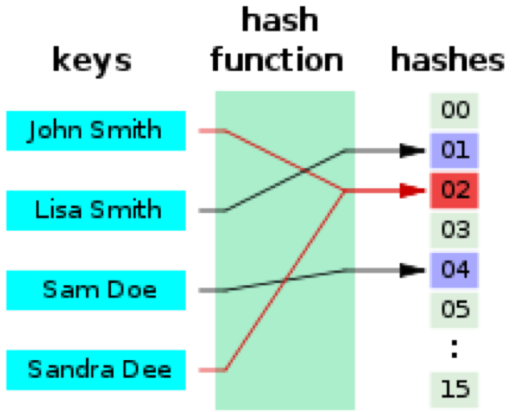
Photo: Declan McCullagh (2002)

Changing Money

- The existing financial system was viewed as one of the greatest threats to individual privacy
- DigiCash is the most famous example of the early cryptocurrencies
- The inventor of DigiCash, David Chaum, used public-key cryptography
- However, DigiCash was a central organization, meaning that Chaum's company needed to confirm every digital signature.
- Eventually, Chaum's company went bankrupt and DigiCash went down with it

Crypto-Innovation

- Cypherpunks also worked on technological innovations, including the cryptographic hash function.
- A hash function is a math equation that is easy to solve but hard to reverse-engineer.
- The early experiments of the Cypherpunks continued to hit hurdles that resulted in failure



2009-2010:
The early development of Bitcoin

WHO IS?

SATOSHI NAKAMOTO

Satoshi Nakamoto and Bitcoin

- Satoshi Nakamoto is the anonymous creator of Bitcoin who wrote a nine-page white paper that brilliantly combined all previous efforts to create a self-sustaining digital money.
- Although some, disheartened by history, were bearish on the currency, a few of the early pioneers supported the project as the solution to their past problems

Genesis Block

- Genesis block mined Jan 3, 2009
- The coinbase of the genesis block references a story in the Times of London newspaper involving the Chancellor bailing out banks
- First bitcoin transaction on Jan 12, 2009 with Hal Finney

Block 0

Short link: http://blockexplorer.com/b/0

Hash: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Next block: 00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048

Time: 2009-01-03 18:15:05

Difficulty: 1 ("Bits": 1d00ffff)

Transactions: 1

Total BTC: 50

Size: 285 bytes

Merkle root: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Nonce: 2083236893

Raw block

Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
4a5e1e4baa...	0	0.204	Generation: 50 + 0 total fees	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa: 50

Waited 6 days to create the second block, A'raf 54, Exodus 31:17

The Six Million Dollar Pizza

- On May 21, 2010, Laszlo Hanyecz purchased $25 worth of pizza for 10,000 BTC
- This was the world's first ever Bitcoin transaction for a tangible asset
- 10,000 BTC is now equivalent to $64,830,000

Mt. Gox

- In 2010 Mt. Gox was established and consolidated itself as the biggest bitcoin exchange during the beginning stages of bitcoin.
- On 6/19/11, Mt. Gox suffered a significant breach of security that resulted in fraudulent trading and required the site to be shut down for seven days.
- In 2014, Mt. Gox lost 744,408 bitcoins in a theft that went unnoticed for years
- Eventually, Mt. Gox declared bankruptcy

Silk Road

anonymous market

messages 0 | orders 0 | account B0

Search Go

Shop by Category

- Drugs *4,086*
  - Cannabis *983*
  - Dissociatives *77*
  - Ecstasy *318*
  - Opioids *350*
  - Other *157*
  - Precursors *18*
  - Prescription *901*
  - Psychedelics *587*
  - Stimulants *405*
- Apparel *82*
- Art *5*
- Books *778*
- Collectibles *15*
- Computer equipment *42*
- Custom Orders *27*
- Digital goods *369*
- Drug paraphernalia *152*
- Electronics *36*
- Erotica *296*
- Fireworks *5*
- Food *4*

100 x Anadrol 50MG Oxymetholone (sealed)

฿12.41

1 gram MDMA

฿5.89

1/2g Cocaine

฿5.44

10 Pieces White Heart 130-150mg MDMA Content

฿4.49

Red and White Filter (10 packs x 20 cigarettes)

฿1.90

VEGA 100mg Sildenafil citrate 4 tablets

฿1.50

10 gram Santa Maria

฿11.58

1/4 oz G13

฿8.13

Silk Road

- On February 2011, Silk Road opened for business: Silk Road, a Bitcoin marketplace, launched an illicit marketplace for drug deals, called the eBay for drugs.
- On October 2013, the FBI shut down Silk Road, seizing 3.6M dollars worth of bitcoin
- Ross Ulbricht, the founder of Silk Road, is currently serving a life sentence without possibility of parole

Bitcoin Bubble and Burst

Cryptocurrency / Blockchain

What is Blockchain

Definition:

A blockchain, originally block chain, is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is resistant to modification of the data.

What is Blockchain

Definition: A blockchain is

-a growing list of records,

-distributed ledger,

-time-stamped,

-cryptographically secured,

-immutable

-consensus-validated,

A new way of storing information
Not an improvement
Not an update

Sample Applications

Insurance - Coverage Proof – Nationwide insurance

Health - MedRec – Patient information share permission

Land Registry

Voting

Donation – BitGive

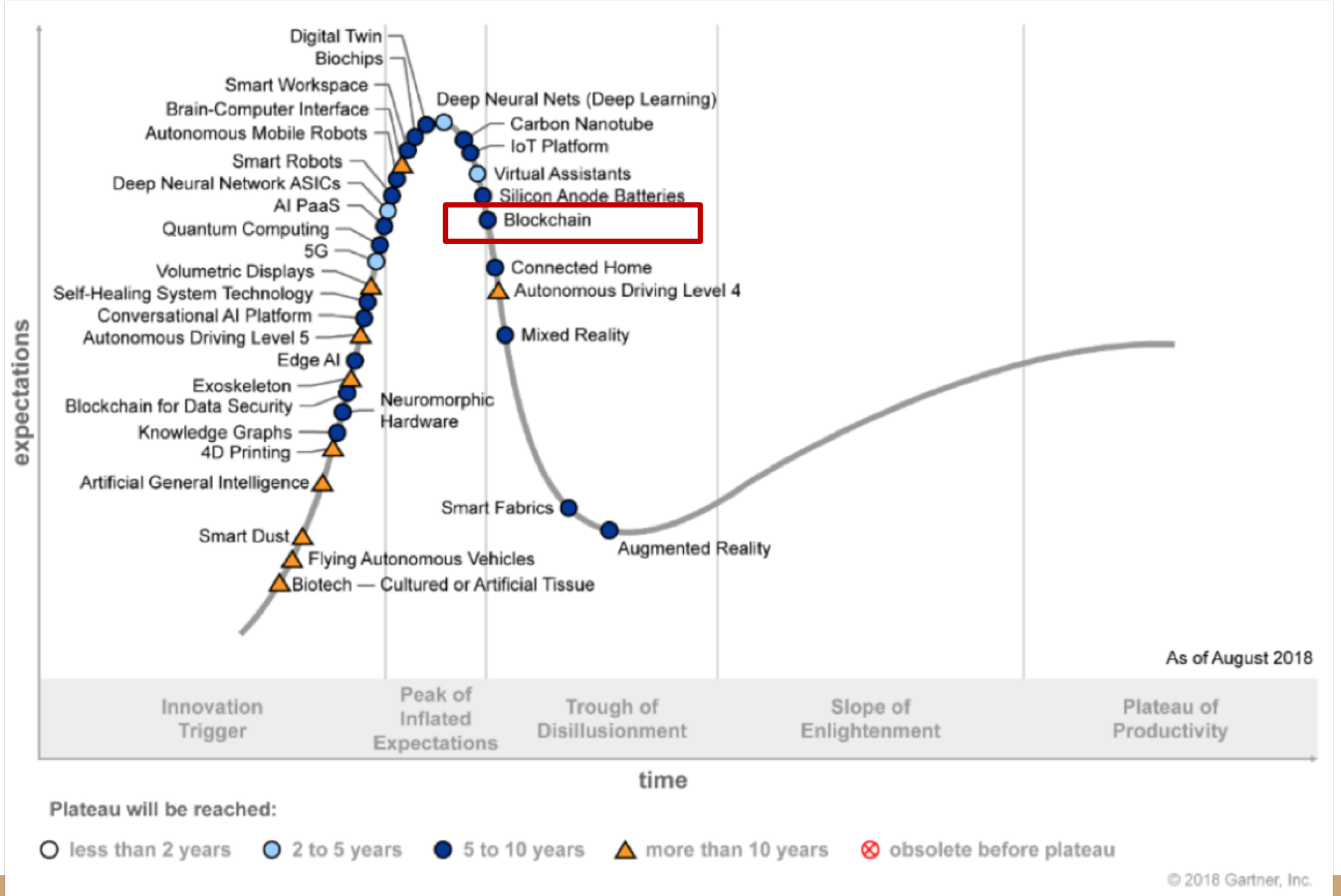
Finance – Bitcoin, Ripple

Supply Chain – IBM Blockchain

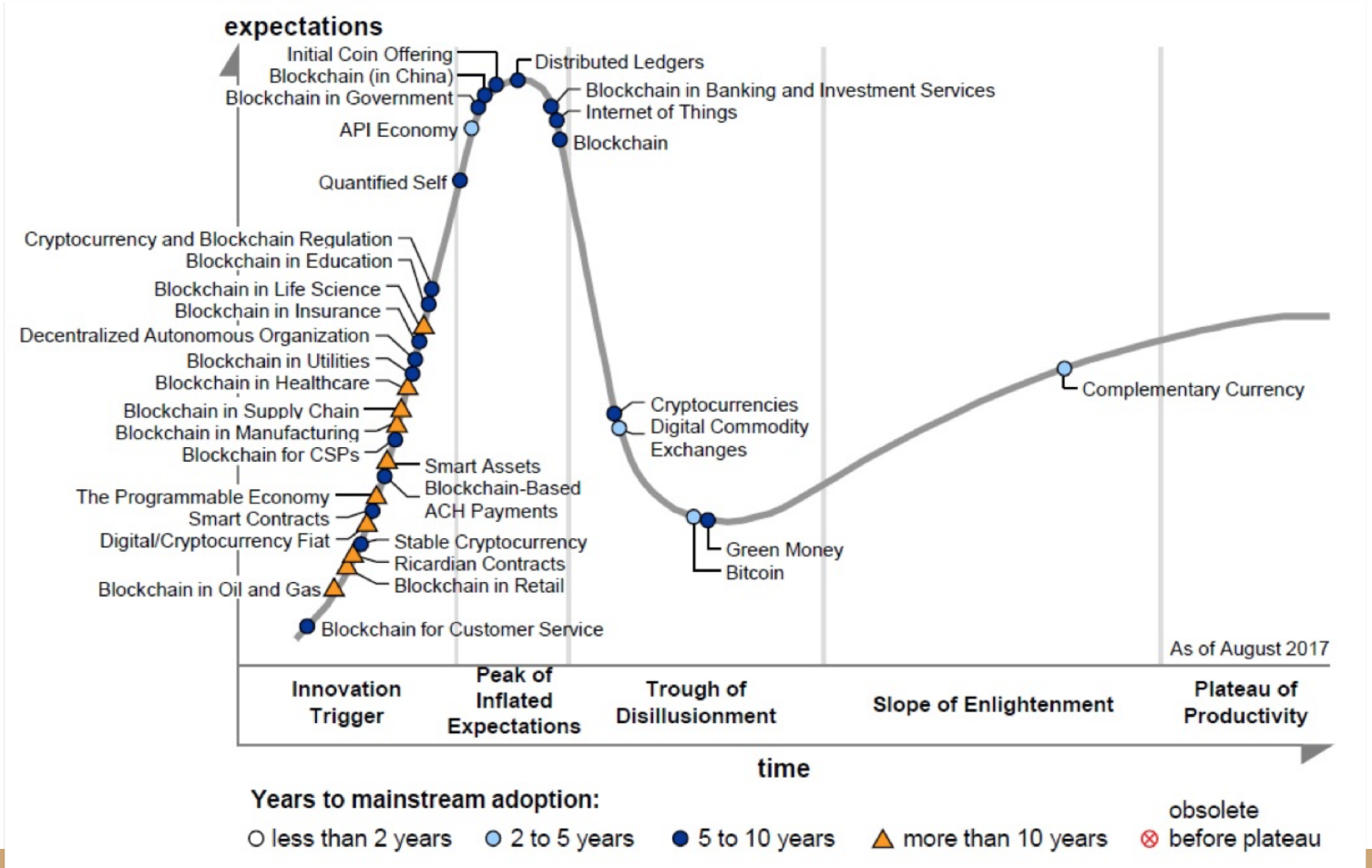
Social Media – Matchpool

Ticket Sale – Guts

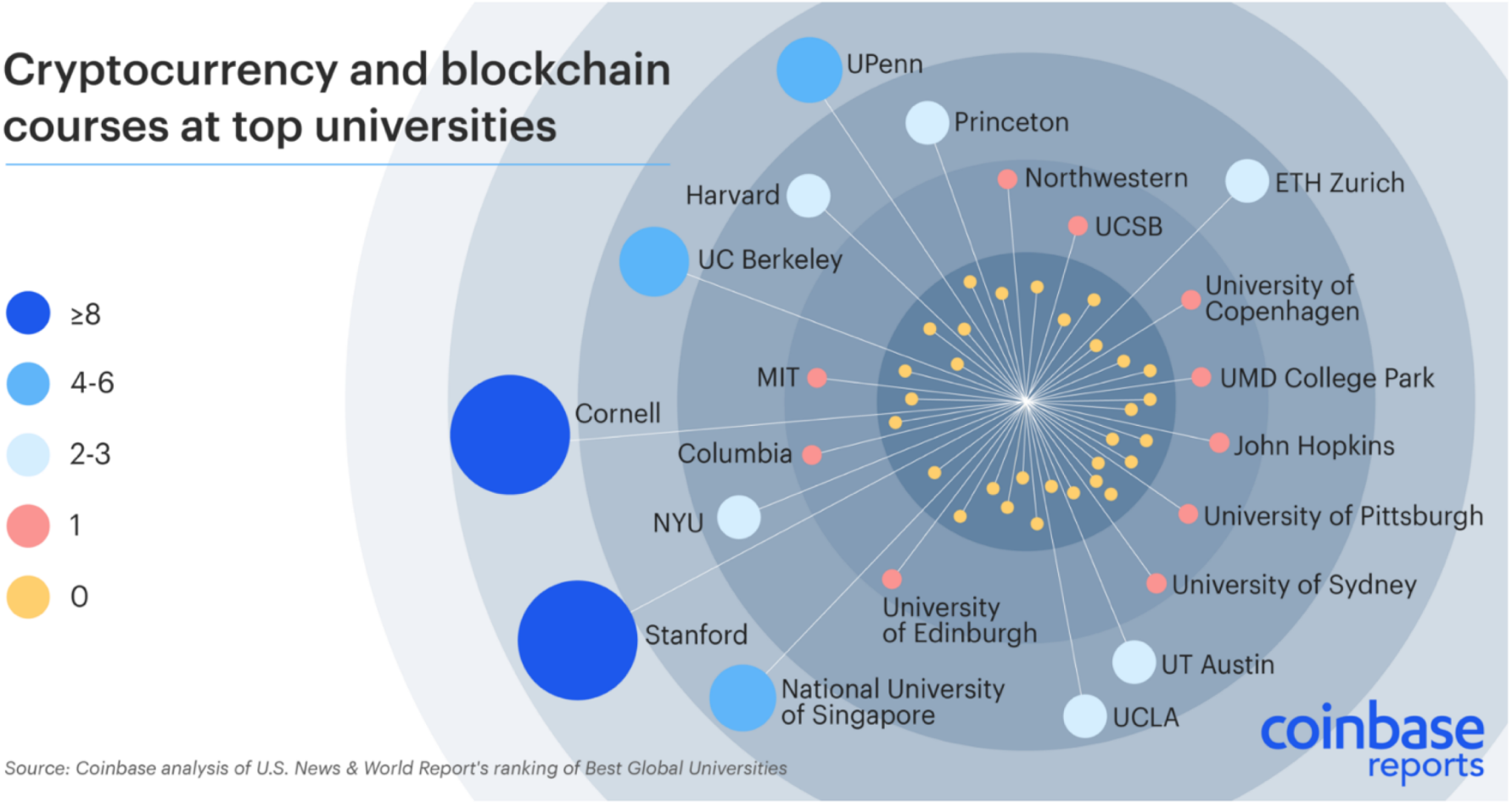
Gartner Hype Cycle for Emerging Technologies, 2018



Gartner Hype Cycle for Blockchain Technologies, 2017



Cryptocurrency and blockchain courses at top universities



Source: Coinbase analysis of U.S. News & World Report's ranking of Best Global Universities

Next class - High Level Overview

To Do:

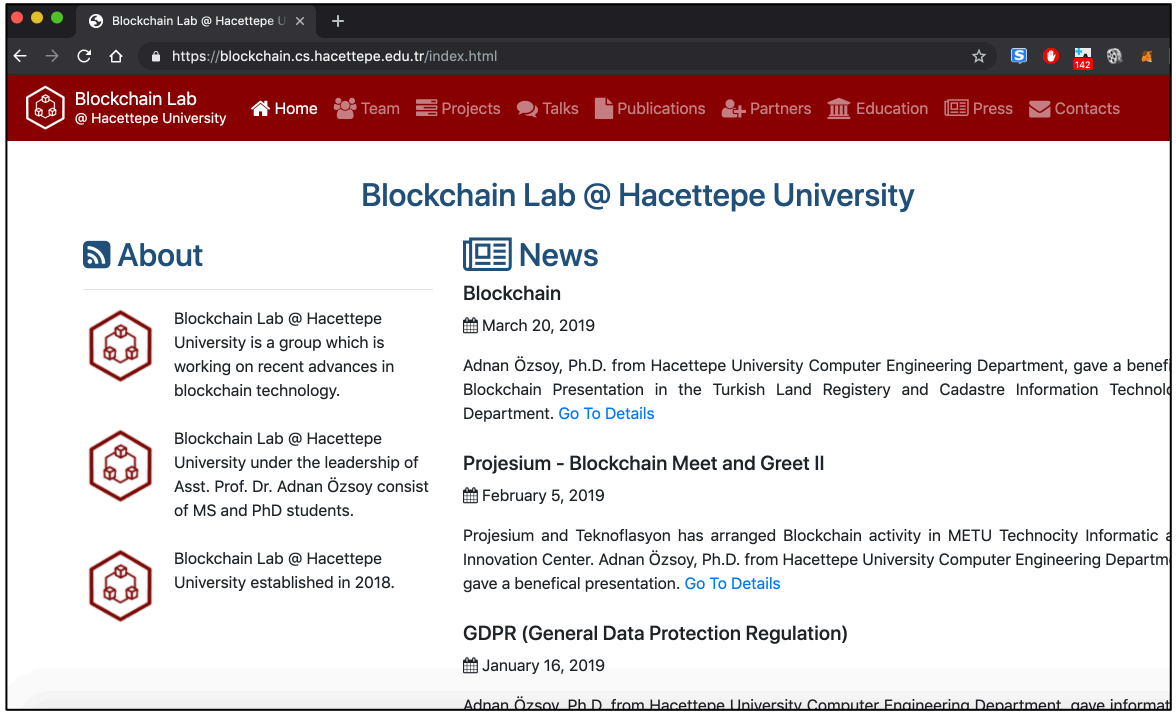
1. Join Piazza

Suggested Readings:

1. How Bitcoin Works in 5 minutes
    - General - https://www.youtube.com/watch?v=t5JGQXCTe3c
    - Technical - https://www.youtube.com/watch?v=l9jOJk30eQs
2. Bitcoin Developer Guide - Up to but not including "P2PKH Script Validation"
    - https://bitcoin.org/en/developer-guide#block-chain-overview

Blockchain Lab @ Hacettepe University

http://blockchain.cs.hacettepe.edu.tr



References

Slides mainly adopted from

- Blockchain @ Berkeley : https://blockchain.berkeley.edu/
- Blockchain @ Princeton : http://bitcoinbook.cs.princeton.edu/