CSE446: Blockchain & Cryptocurrencies

Lecture – 1: The beginning

Inspiring Excellence

Course Instructors

Dr. Md Sadek Ferdous

Associate Professor, CSE, BRAC University

E-mail: sadek.ferdous@bracu.ac.bd

Lab teachers

Mr. Partha Bhoumik

Mr. Monirul Haque

Research Assistant (RA)

Mr. Md. Yeasin Ali

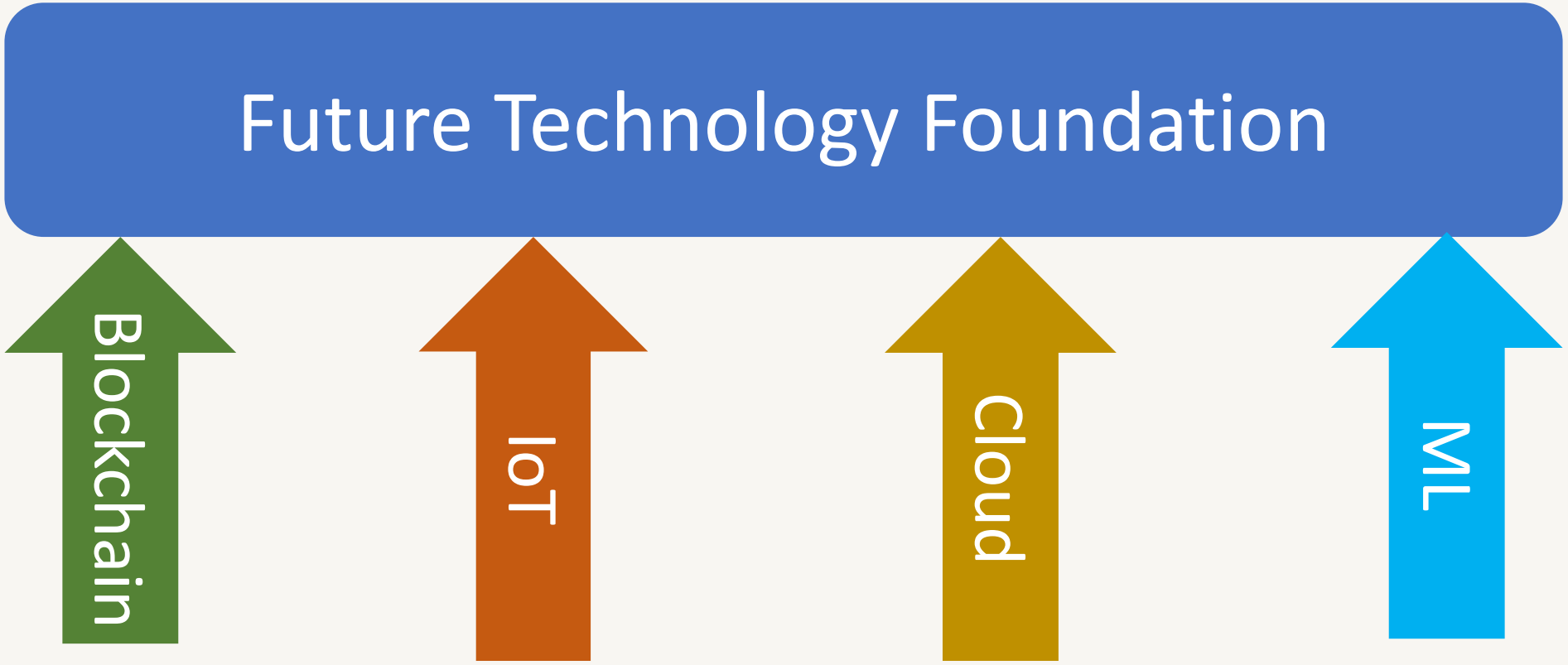
Intro

- Say your name, and short background
- Any story about how you chose this class or interest in blockchain/cryptocurrency?
- Any other personal goals for the class

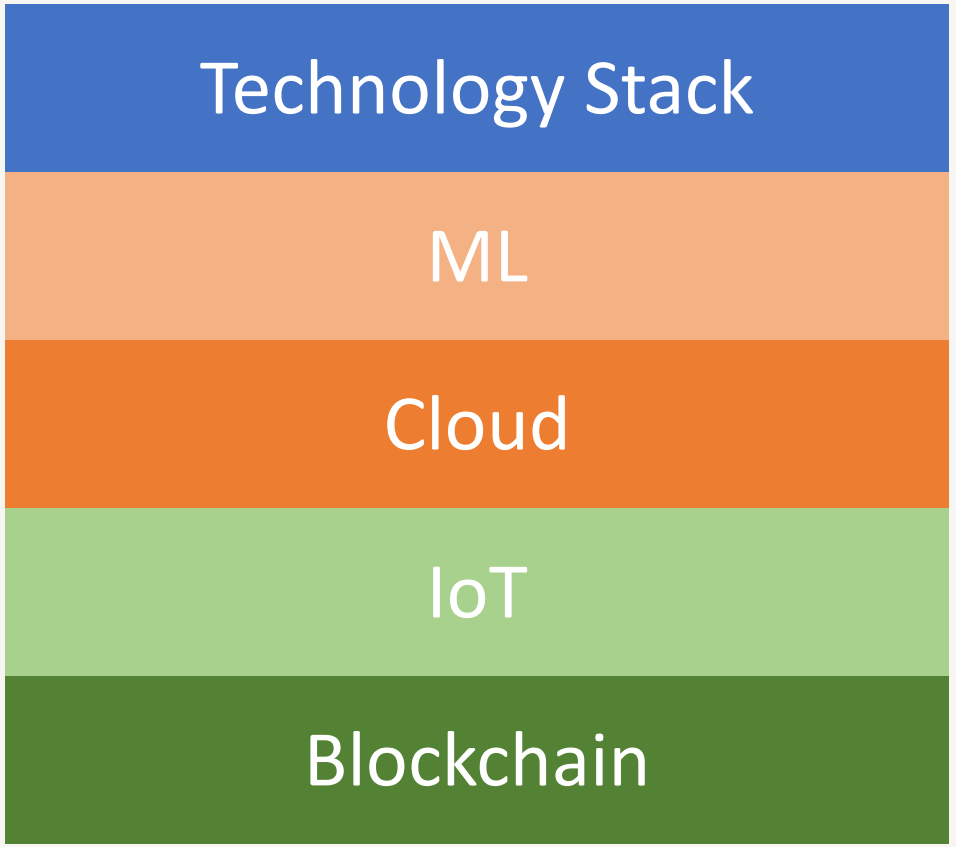
Agenda

- Technology outlook
- Course motivation
- Course information
    - Objectives, Outcome, Syllabus, Schedule, Marks distribution, textbooks
- Motivations behind blockchain
- Bitcoin background

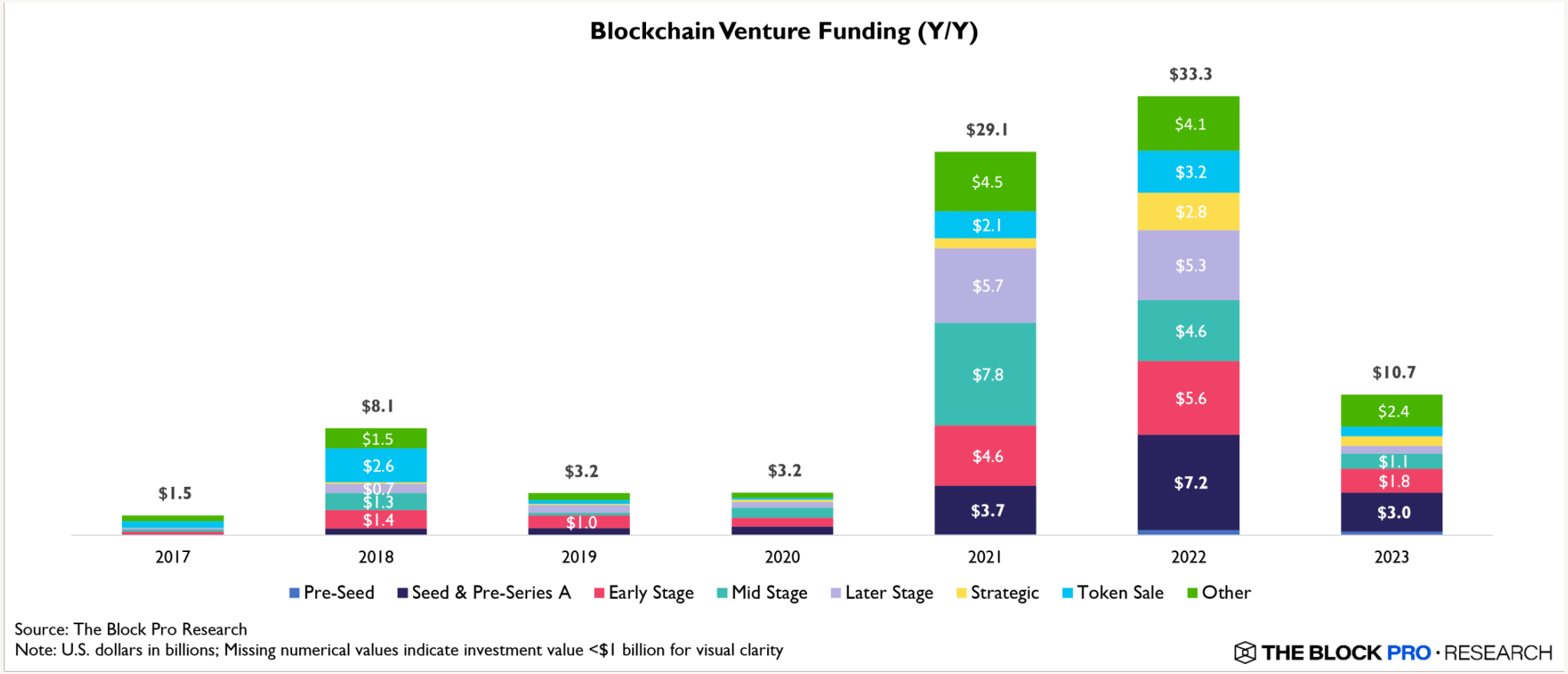
Technology outlook



Technology outlook



Blockchain: In Data



https://www.linkedin.com/pulse/look-2023s-blockchain-investment-landscape-projections-fvrif/

Blockchain: In Data

https://www.coingecko.com/en/coins/bitcoin

Blockchain: In Data

Top jobs of the future

Many popular jobs with the highest-paying skills we see today, such as AI engineers, were nonexistent a few years ago. In addition to many of the positions we've already covered, the future looks bright for jobs in cloud computing, blockchain, AI, and robotics, to name a few. These categories require specific knowledge bases and skillsets and are good candidates for technology specialists interested in upskilling to help ensure greater job security and demand.

Cloud computing

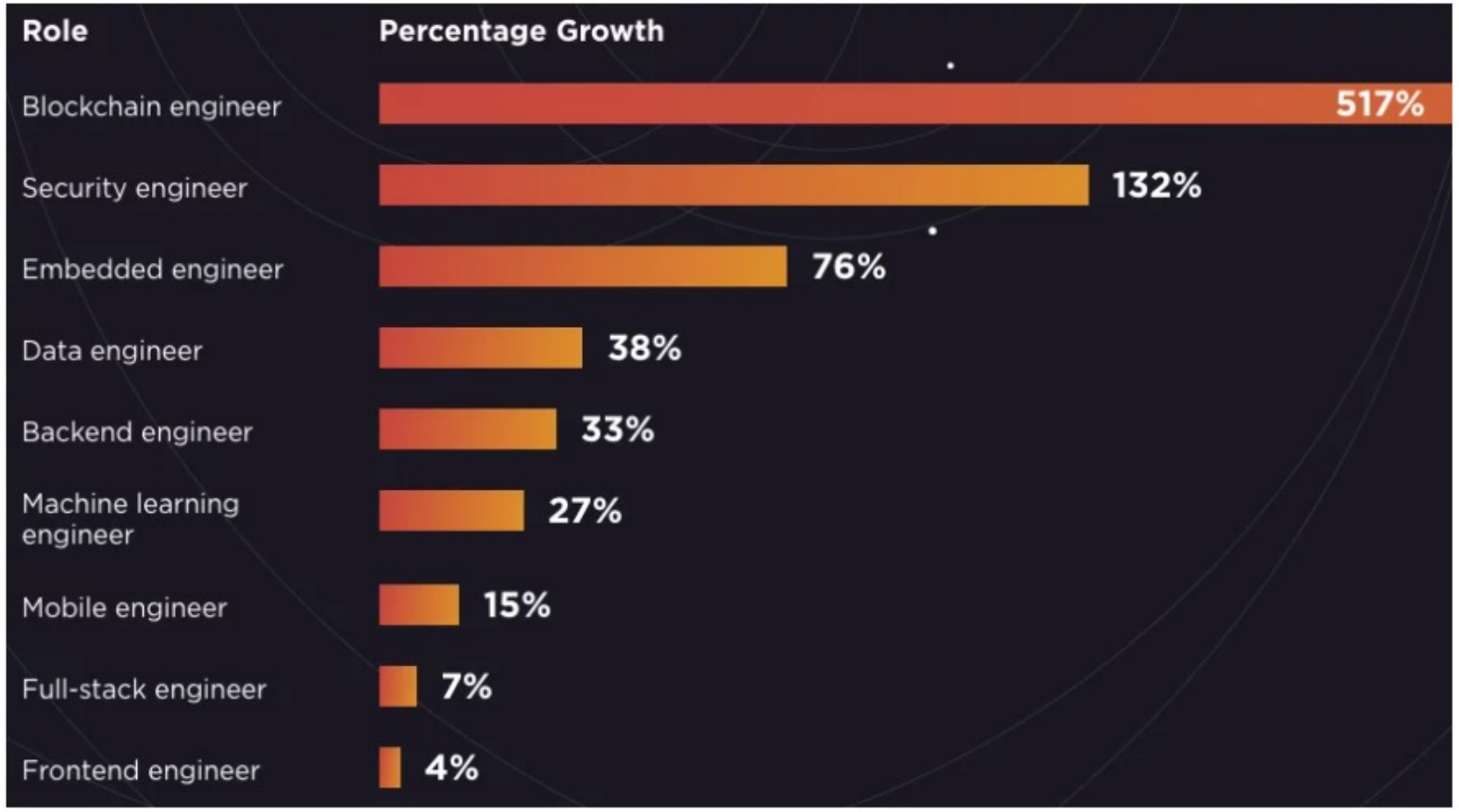
Businesses are shifting from a corporate data center-centric model to cloud-based XaaS (anything as a service) platforms. Reasons include the ability to be more agile and adaptive, better support a remote workforce, and shift from CapEx to OpEx financial model, which helps preserve cash. Simultaneously, individuals use the cloud to store and manage their data versus on a personal network or computer. Sought-after cloud computing skills include programming, ML, AI, IT and cybersecurity expertise, development operations, and serverless architecture knowledge. The average rate for cloud computing platform developers ranges from $40 to $150 per hour.

Blockchain

This system, created behind Bitcoin cryptocurrency, is a virtual ledger capable of recording and verifying a high digital transaction recording volume. It's practically if not totally impossible to change, hack, or cheat the system, making Bitcoins impervious to being hacked, double spent, or faked. Companies in various business sectors are rushing to use blockchain in innovative ways, creating a greater demand for blockchain developers. Skills for blockchain specialists include in-depth knowledge of blockchain architecture, web development, public architecture, and expertise in programming languages such as Python, Java, and C++. The average rate for blockchain developers ranges from $50 to $125 per hour.

https://www.upwork.com/resources/in-demand-jobs-and-skills

Blockchain: In Data



Source: DAppUniversity

https://www.blockchain-council.org/blockchain/what-is-the-salary-for-a-blockchain-developer-in-the-usa/

Blockchain

- Blockchain is one of the coolest technologies
- It is exciting and challenging at the same time
    - It will challenge your academic acumen and test your tech skills
- Hopefully, you all will have lots of fun!

CSE446: objectives

- To understand the motivation behind blockchain technologies
- To acquire a deep knowledge about different constructs of Bitcoin, Ethereum and Hyperledger Fabric
- To be able to develop a clear understanding about the strengths and weaknesses of the current blockchain systems
- To have a clear understanding of the applicability of blockchain for a particular application scenario
- To have extensive hands on experiences, including Ethereum and Fabric

CSE446: outcome

- To learn the motivations and the overall philosophy of blockchain systems
- To able to explain the underlying principles and techniques associated with a few blockchain systems
- To develop a clear technical understanding of Bitcoin, Ethereum and Hyperledger Fabric
- To develop practical know-how involving different blockchain systems
- To be able to utilise different blockchain platforms to solve outstanding issues or to improve existing application domains

CSE446: syllabus

- Basic cryptography review (Symmetric Encryption, Asymmetric encryption, Hash function, Digital Signature, Merkle Tree, etc.)
- Introductory concept on distributed systems (Byzantine Generals Problem, Fault Tolerance, Distributed Consensus, etc.)
- History of money and digital currency
- Blockchain fundamentals
- Bitcoin and its technical aspects (address, wallets, nodes, transactions, blocks, blockchain, mining, Bitcoin consensus algorithms)
- Different Blockchain consensus algorithms (Proof of Work, Proof of Stake, Delegated Proof of State, Byzantine Fault Tolerance algorithm and others)

CSE446: syllabus

- Ethereum and its technical aspects (Ethereum model, Ethereum Virtual Machine, block structure, blockchain, consensus, Solidity)
- Hyperledger Fabric and its technical aspects (Network, Identity, Membership Service Provider, Peers, Policies, Ledger, Ordering service, chaincode)
- Blockchain properties, strengths and weaknesses
- Security and privacy issues in Blockchain
- Blockchain Governance
- Blockchain applications
- Advanced concepts (Layer 2 solutions, Scaling, cross-chain transactions and others)

CSE446: tentative schedule

Weeks	Topics
Week – 1	Introductory topics, Basic cryptography review
Week – 2	Introductory concept on distributed systems, history of money, history of digital currency, Blockchain fundamentals
Week – 3	Bitcoin – 1
Week – 4	Bitcoin – 2
Week – 5	Blockchain consensus algorithms, Ethereum – 1
Week – 6	Ethereum – 2
Week – 7	Fabric
Week – 8	Blockchain properties, strengths and weaknesses
Week – 9	Security and privacy issues in Blockchain
Week – 10	Blockchain Governance, Blockchain applications
Week – 11	Advanced concepts, course review

CSE446: tentative lab topics

Weeks	Topics
Week – 1	**First week off**
Week – 2	Wallet & Transaction with Metamask
Week – 3	Blockchain with JavaScript
Week – 4	Ubuntu basics
Week – 5	Blocksim (Blockchain Simulator)
Week – 6	Geth
Week – 7	Solidity
Week – 8	Ethereum DApp Development
Week – 9	Hyperledger Fabric - 1
Week – 10	Hyperledger Fabric - 2
Week – 11	Fabric Project Submission

CSE446: marks distribution

- Theory – 75
  - Class attendance: 5
  - Quizzes: 15
  - One midterm: 25
  - Final exam: 30
- Lab – 25

CSE446: textbooks

- Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction
  - By Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. Princeton University Press, 2016
- Mastering Bitcoin
  - By Andreas Antonopoulos. O'Reilly Publishing

(Bitcoin) blockchain motivation

https://i.imgflip.com/6t9jr0.jpg

(Bitcoin) blockchain motivation

- The seed was in the great financial crisis of 2007-2008
- Low interest rates and dubious lending regulations meaning a housing bubble was created in the USA
- People even with bad credit ratings and unstable income flow started to get loans for their houses, called subprime mortgages
- At some point, they could not afford to pay their loans and started to default
- This resulted in more houses on the market, surpassing the demand
- And the housing bubble was burst, the house prices started to fall down

(Bitcoin) blockchain motivation

- The homeowners suddenly found that their debts were more than their house prices and they stopped paying back their loans, resulting in more defaults
- Now, the FIs (Financial Institutions) had trillions of dollars of near worthless investment in subprime mortgages
- In 2007, subprime lenders started to collapse, filing for bankruptcy
- The impact was felt across the globe, particularly in the USA and Europe
- Northern Rock (a British bank) faced acute liquidity issues and requested for bailout

(Bitcoin) blockchain motivation

- In 2008 Bear Stearns, one of the biggest investment banks during that time, collapsed and ultimately sold to JPMorgan at an incredible low price
- The ultimate shock came when Lehman Brothers collapsed in September 2008 with a debt of $613 Billion, the largest in the US history
- This kickstarted the downward spiral recession in many developed countries

15 September 2008

https://www.independent.co.uk/news/business/analysis-and-features/financial-crisis-2008-why-lehman-brothers-what-happened-10-years-anniversary-a8531581.html

(Bitcoin) blockchain motivation

- Interested to know more about this: https://www.youtube.com/watch?v=GPOv72Awo68

https://pisces.bbystatic.com/image2/BestBuy_US/images/products/4921/4921700_so.jpg

(Bitcoin) blockchain motivation

The principal motivation behind Bitcoin was to dissolve trust in a centralised authority controlling the monetary system of any country!

(Bitcoin) blockchain motivation

The solution: distributed trust, or
even better, required to trust minimal entities

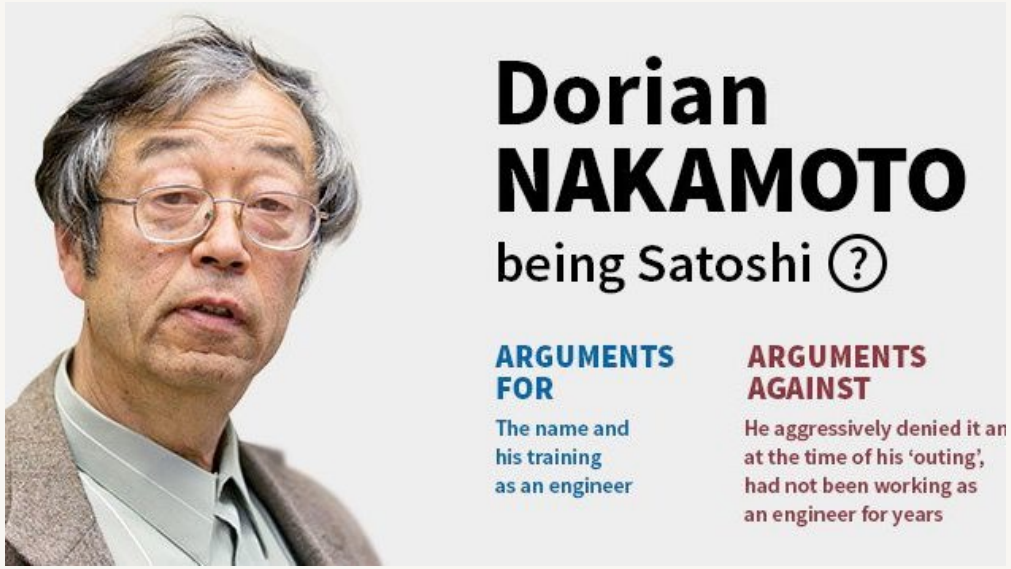
Bitcoin background

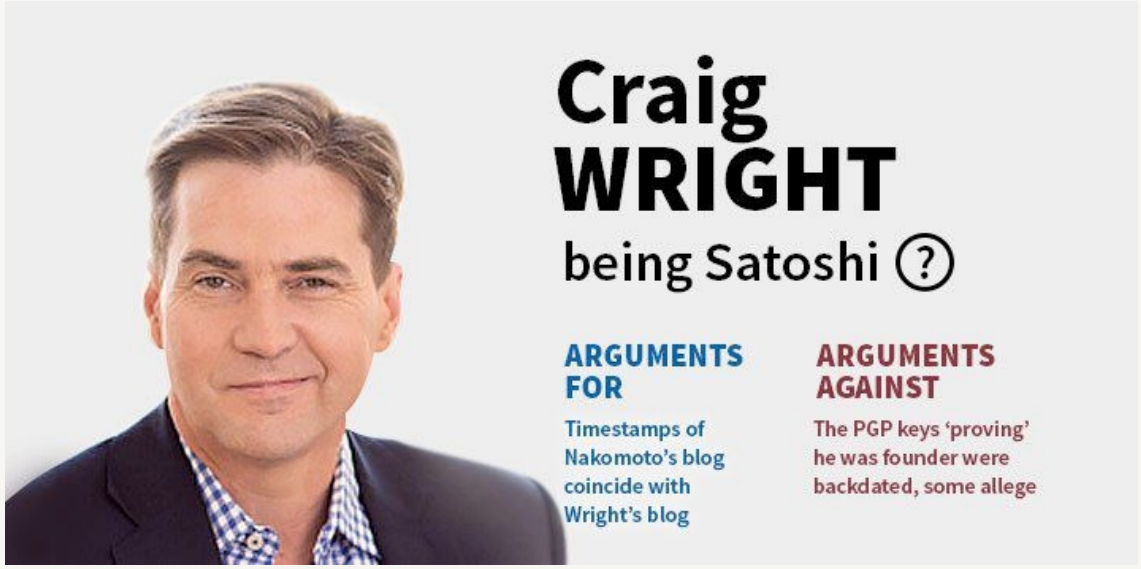
- From: Satoshi Nakamoto <satoshi <at> vistomail.com> Subject: Bitcoin P2P e-cash paper
  Newsgroups: gmane.comp.encryption.general
  Date: Friday 31st October 2008 18:10:00 UTC
- “I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.”

“Bitcoin: A Peer-to-Peer Electronic Cash System”

Bitcoin background

Who is Real Satoshi? Please stand up……





Bitcoin background

Chancellor Alistair Darling on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

03 January 2009

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", *The Times* has learnt.

18 Aug. 2008

bitcoin.org registered

31 Oct. 2008

Bitcoin paper released

9 Jan. 2009

Bitcoin code open-sourced

3 Jan. 2009

Bitcoin network went live, first block mined with the message:

"The Times 03/Jan/2009 Chancellor on bring of second bailout for banks"

23 April. 2011

Satoshi disappears from the Internet stating he moved to other things!

https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h

Bitcoin background

- The recipient of the first bitcoin transaction was programmer Hal Finney 12 January 2009
- The value of the first bitcoin transactions were negotiated by individuals on the bitcoin forum

https://thebarterbubble.com/wp-content/uploads/2019/02/The-Barter.jpg

Bitcoin background

Pizza for bitcoins? May 18, 2010, 12:35:20 AM

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested, please let me know and we can work out a deal.
Thanks,
Laszlo

https://bitcointalk.org/index.php?topic=137.msg1141

Bitcoin background

Pizza for bitcoins? May 21, 2010, 07:06:58 PM

"So nobody wants to buy me pizza? Is the bitcoin amount I'm offering too low?"

Pizza for bitcoins? May 22, 2010, 07:17:26 PM

"I just want to report that I successfully traded 10,000 bitcoins for pizza. Pictures: http://heliacal.net/~solar/bitcoin/pizza/

Thanks jercos!"

https://bitcointalk.org/index.php?topic=137.msg1141

Bitcoin background

- May 22, 2010 - $41
  - $20.50 per pizza
- January 21, 2024 - $416 million
  - 28979,048,500 BDT ~= 4553 Crore BDT!
- Bitcoin Pizza day every year: May 22

Laszlo Hanyecz

https://miro.medium.com/max/382/0*puqFpqT3Y69O0gDp

Bitcoin background

Question?

Discord Class URL: https://discord.gg/TqtzC7dkzG

i) Mention your student ID in the #verify channel.
ii) Change your server profile name to id_FullName (e.g.,20XXXXXX_Bob).