Lecture 29

Blocks and blockchain

ECE 422: Reliable and Secure Systems Design

UNIVERSITY OF ALBERTA

Instructor: An Ran Chen
Term: 2024 Winter

Schedule for today

- Blockchain technology
  - Why Bitcoin has value?
  - A form of distributed ledger technology
  - Blocks and blockchain
- Why maintain and create new blocks?
  - Block rewards (i.e., mining rewards)
  - Bitcoin Halving
- Who maintain and create new blocks?
  - Proof of Work (PoW)
  - Brief introduction into mining principles
- Next class: Mining principles

Bitcoin

Bitcoin is a cryptocurrency, a virtual currency designed to act as money

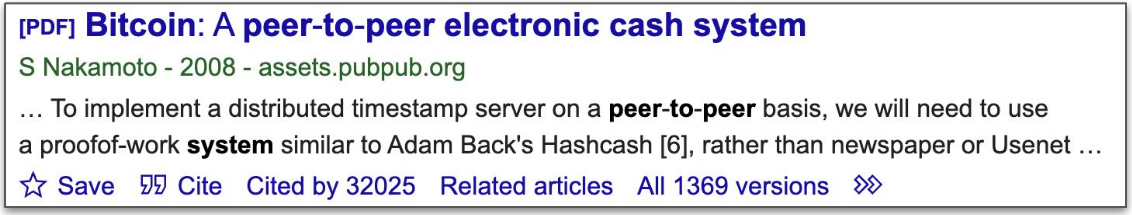
- Introduced by an anonymous developer or group of developers using the name “Satoshi Nakamoto”

Bitcoin outlines the concept of a decentralized distributed ledger system

- Electronic cash system
- No trusted third-party (e.g., central banks)
- Peer-to-peer network

History of Bitcoin

- On Oct. 31, 2008, “Satoshi Nakamoto” wrote an email to a cypherpunk mailing list discussing about an electronic cash system
- The concept of Bitcoin was shared through a paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System”, later known as the Bitcoin white paper
- On Jan. 3, 2009, the first bitcoin was mined
- On Jan. 12, 2009, the world’s first Bitcoin transaction took place
  - Transaction of 10 Bitcoin (BTC) to a regular poster on the cypherpunk mailing list



[PDF] **Bitcoin**: A **peer-to-peer electronic cash system**

S Nakamoto - 2008 - assets.pubpub.org

… To implement a distributed timestamp server on a **peer-to-peer** basis, we will need to use a proofof-work **system** similar to Adam Back's Hashcash [6], rather than newspaper or Usenet …

Iconic Bitcoin Pizza Day

- On May 22, 2010, programmer Laszlo Hanyecz offered 10,000 Bitcoin for two large pizzas at the BitcoinTalk online forum
- Jeremy Sturdivant took up Hanyecz's offer and delivered the meal in exchange for the Bitcoin
- This marked the first real-world transaction for the currency

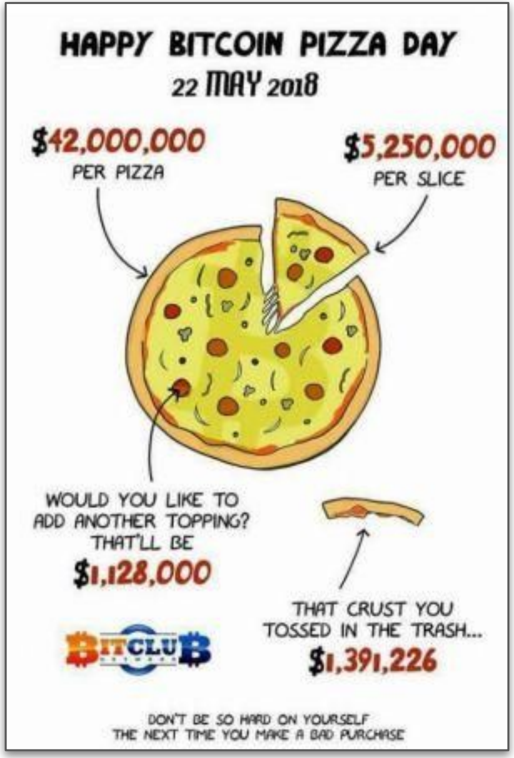

HAPPY BITCOIN PIZZA DAY
22 MAY 2018
$42,000,000
PER PIZZA
$5,250,000
PER SLICE
WOULD YOU LIKE TO ADD ANOTHER TOPPING? THAT'LL BE
$1,128,000
THAT CRUST YOU TOSSED IN THE TRASH...
$1,391,226
BITCLUB
DON'T BE SO HARD ON YOURSELF THE NEXT TIME YOU MAKE A BAD PURCHASE

Image from cryptonews

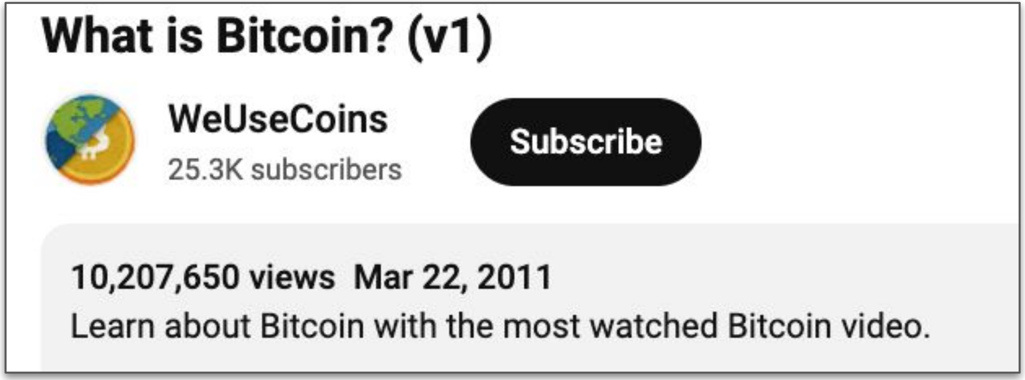
The Big Bang Theory Season 11 Episode 9
The Bitcoin Entanglement

Locked USB Drive

Stefan Thomas, a German-born programmer living in San Francisco, has two guesses left (already tried eight incorrect guesses) to figure out a password that is worth, as of this week, about $657 millions.

Thomas said that his 7,002 bitcoins were left over from a payment he received for making a video titled “What is Bitcoin?” that published on YouTube in early 2011, when a bitcoin was worth less than a dollar.

- WIRED updates in 2023
- BCC on James Howells
  - 7,500 BTC in the landfill



What is Bitcoin? (v1)

WeUseCoins

25.3K subscribers

10,207,650 views Mar 22, 2011

Learn about Bitcoin with the most watched Bitcoin video.

Schedule for today

- Blockchain technology
  - Why Bitcoin has value?
  - A form of distributed ledger technology
  - Blocks and blockchain
- Why maintain and create new blocks?
  - Block rewards (i.e., mining rewards)
  - Bitcoin Halving
- Who maintain and create new blocks?
  - Proof of Work (PoW)
  - Brief introduction into mining principles
- Next class: Mining principles

Why Bitcoin has value?

- Decentralized = Peer-to-peer network
  - Transactions between private users are not regulated
  - Central banks offer credibility (regulated by the government)
  - Idea: Save effort and money from the third-party authority
- Flat transaction fee = Congestion of the network and size of the transaction
  - Fee for larger transactions ($1,000,000) = Fee for smaller transactions ($100)
  - Central banks with percentage rate (Why fixed costs matter for Bitcoin by Bank of Canada)
  - Idea: Depending on how many people are making transactions
- Scarcity = Limited to a total of 21 million Bitcoin
  - Over 19.5 million Bitcoins currently in circulation, leaving 1.5 million yet to be mined
  - Central banks regulate the money supply based inflation and economic growth = unlimited

Why Bitcoin has value?

- Decentralized → Blockchain technology
  - Transactions between private users are not regulated
  - Central banks offer credibility (regulated by the government)
  - Idea: Save effort and money from the third-party authority
- Flat transaction fee → Block rewards
  - Fee for larger transactions ($1,000,000) = Fee for smaller transactions ($100)
  - Central banks with percentage rate (Why fixed costs matter for Bitcoin by Bank of Canada)
- Scarcity → Bitcoin halving
  - Over 19.5 million Bitcoins currently in circulation, leaving 1.5 million yet to be mined
  - Central banks regulate the money supply based inflation and economic growth = unlimited

Message from Government of Canada

“Crypto assets are very risky.

Unlike the Canadian dollar, crypto assets are not legal tender in Canada. A government or central bank doesn’t issue or oversee them.

Crypto assets are also quickly evolving, unstable and complex. You should learn more about crypto assets and their risks before investing or using them. You may also want to consult a financial advisor.”

- Risks of using crypto assets from Government of Canada
- Avoid crypto investment fraud from Competition Bureau Canada
- Warnings about crypto assets from Canadian Securities Administrators

Schedule for today

- Blockchain technology
  - Why Bitcoin has value?
  - A form of distributed ledger technology
  - Blocks and blockchain
- Why maintain and create new blocks?
  - Block rewards (i.e., mining rewards)
  - Bitcoin Halving
- Who maintain and create new blocks?
  - Proof of Work (PoW)
  - Brief introduction into mining principles
- Next class: Mining principles

Distributed ledger technology

Distributed ledger technology (DLT) is a system for recording digital transactions without the need for a centralized authority.

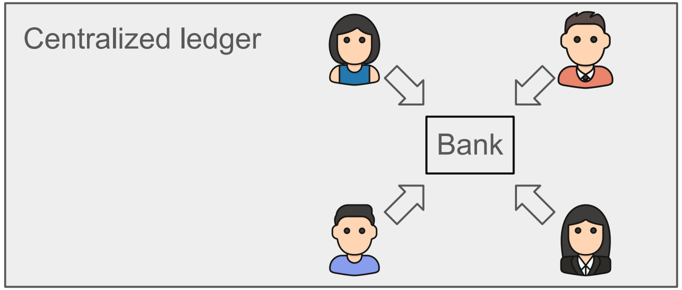
- Database spread across several nodes or computing devices
- Each node replicates and saves an identical copy of a public ledger
- Each participant node of the network updates itself independently

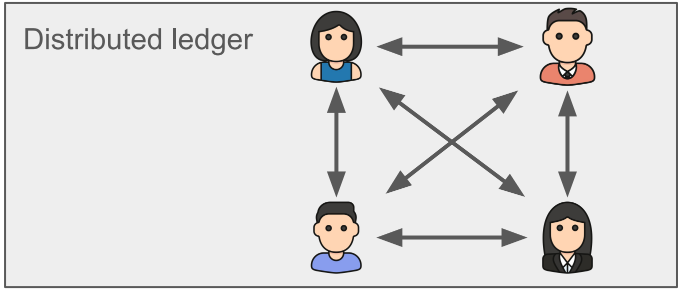
Distributed ledger technology

Distributed ledger technology (DLT) is a system for recording digital transactions without the need for a centralized authority.

- Database spread across several nodes or computing devices
- Each node replicates and saves an identical copy of the ledger
- Each participant node of the network updates itself independently

The distributed ledger technologies focuses on reducing the cost of trust.





Blockchain technology

Blockchain technology is a way to implement a distributed ledger system which employs a chain of blocks (i.e., blockchain) to store transactions.

- Blockchain stores transactions in blocks that are linked together in a chain
- As the chain provides a chronological consistency, ledgers are immutable

As a form of peer-to-peer network:

- Node requests a transaction
- Transaction is validated and recorded by other nodes in the network
- When the record reaches ~4,000 transactions, they forms a block
- Block is added to the existing chain of blocks, also known as a blockchain

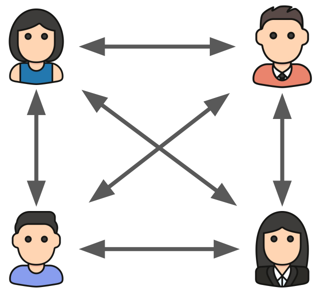
Peer-to-peer network

Assume the network is between Alice, Bob, Carol and Dave

- Alice pays 10 BTC to Bob
- Bob pays 2 BTC to Charlie
- Charlie pays 1 BTC to Dave …

Once the list reach ~4,000 transactions

- List of transactions is packaged into a block
- The block is connected to the chain of all prior transactions (i.e., blockchain)



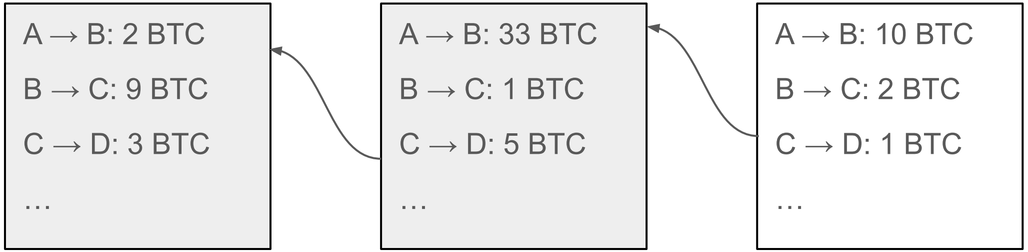
List of transactions

A → B: 10 BTC

B → C: 2 BTC

C → D: 1 BTC

…



A → B: 2 BTC
B → C: 9 BTC
C → D: 3 BTC
…

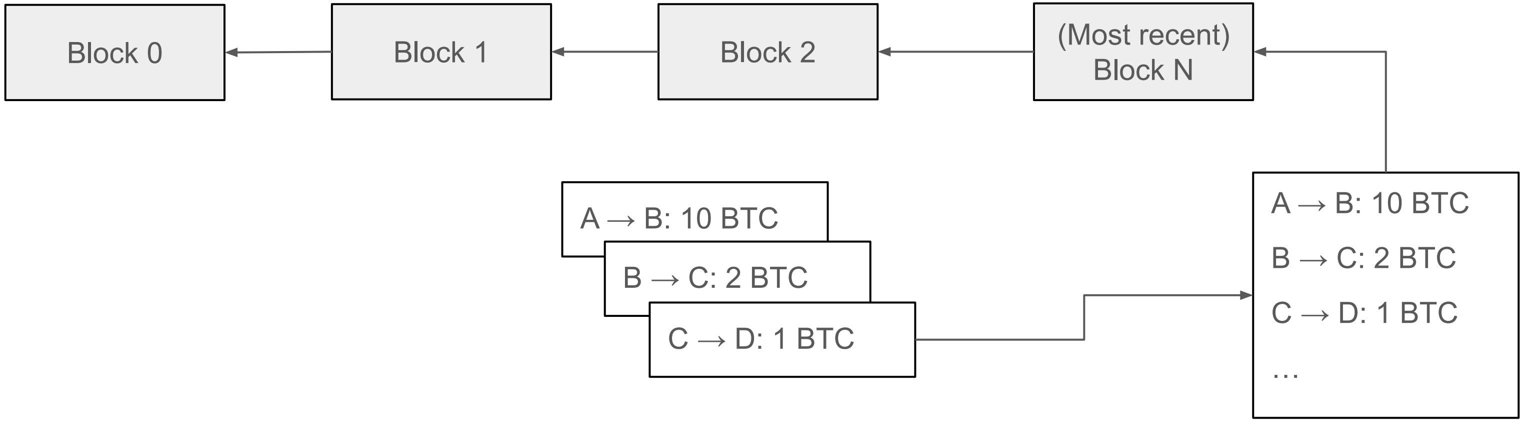
A → B: 33 BTC
B → C: 1 BTC
C → D: 5 BTC
…

A → B: 10 BTC
B → C: 2 BTC
C → D: 1 BTC
…

A basic protocol

Design: Decentralized network without a centralized authority

- Everyone keeps a copy of the blockchain on their own public ledger
- Every time new transactions are packaged into blocks, the public ledge is updated



Challenges in a distributed ledger system

There are two main challenges in the basic protocol:

- Why maintain and create new blocks?
  - Fact: Everyone uses the system to make transitions
  - What is the incentive of recording transactions for other people?
    - E.g., roommate agreement, Alice and Bob only make transactions with each other
    - Why should they help create the sticky note (with other roommates’ transactions)?
- Who maintain and create new blocks?
  - Fact: Network delays exist, everyone has a ledger with different transactions order
  - Whose ledger do we rely on?
    - E.g., roommate agreement, every roommate has their own ledger
    - Whose notebook do we use to update the sticky note?

Schedule for today

- Blockchain technology
  - Why Bitcoin has value?
  - A form of distributed ledger technology
  - Blocks and blockchain
- Why maintain and create new blocks?
  - Block rewards (i.e., mining rewards)
  - Bitcoin Halving
- Who maintain and create new blocks?
  - Proof of Work (PoW)
  - Brief introduction into mining principles
- Next class: Mining principles

Why maintain and create new blocks?

Creating rewards for block creators (i.e., Bitcoin miners):

- Reward 1: Transaction fee
  - Each Bitcoin transaction includes a fixed transaction fee for the block creators
  - From senders to block creators
  - Same transaction fee that central banks charge
- Reward 2: Block reward (i.e., mining reward)
  - Each creation of new blocks is rewarded with a block reward
  - From the system to block creators
  - Only one block creator per block

Block rewards

The design of block rewards is called Bitcoin halving

- Initial block reward: 50 BTC (in 2009)
- Bitcoin halving: Block rewards decrease by half every four years
- Next Bitcoin halving: April 2024
  - Block reward falls from 6.25 to 3.125 BTC

Block rewards is the only way for new bitcoins to enter circulation, produced by block creators, or commonly known as Bitcoin “miners”

Bitcoin halving

The design of block rewards is called Bitcoin halving

- Initial block reward: 50 BTC (in 2009)
- Block rewards decrease by half every four years
  - Block time: 10 minutes between every new block (more on this later …)

Calculating the total number of BTC:

- Number of blocks over 4 years = 6 blocks per hour x 24 hours per day x 365 days per year x 4 years = 210,240
- 2009 to 2012 = 50 BTC per block
- 2013 to 2016 = 25 BTC per block
- 2017 to 2020 = 12.5 BTC per block …
- Total number of BTC = 210,240 (50 + 25 + 12.5 + 6.25 + …) ≅ 21,000,000 BTC

This ensures the scarcity of Bitcoin

Challenges in a distributed ledger system

There are two main challenges in the basic protocol:

- Why maintain and create new blocks?
  - Answer: Rewards available ($$$) for the block creators
  - Note that the rewards reduce by half every four years

Why Bitcoin has value?

- Decentralized → Blockchain technology
  - Transactions between private users are not regulated
  - Central banks offer credibility (regulated by the government)
- Flat transaction fee → Block rewards
  - Fee for larger transactions ($1,000,000) = Fee for smaller transactions ($100)
  - Central banks with percentage rate (Why fixed costs matter for Bitcoin by Bank of Canada)
- Scarcity → Bitcoin halving
  - Over 19.5 million Bitcoins currently in circulation, leaving 1.5 million yet to be mined
  - Central banks regulate the money supply based inflation and economic growth = unlimited

Challenges in a distributed ledger system

There are two main challenges in the basic protocol:

- Why maintain and create new blocks?
  - Answer: Rewards available ($$$) for the block creators
  - Note that the rewards reduce by half every four years
- Who maintain and create new blocks?
  - Fact: Network delays exist, everyone has a ledger with different transactions order
  - Whose ledger do we rely on?
  - In addition, everyone wants to be the block creators
  - Who gets to create new blocks?

Schedule for today

- Blockchain technology
  - Why Bitcoin has value?
  - A form of distributed ledger technology
  - Blocks and blockchain
- Why maintain and create new blocks?
  - Block rewards (i.e., mining rewards)
  - Bitcoin Halving
- Who maintain and create new blocks?
  - Proof of Work (PoW)
  - Brief introduction into mining principles
- Next class: Mining principles

Who maintain and create new blocks?

Proof of Work (PoW) is a consensus algorithm which is used to verify transactions and create new blocks.

- In PoW, participants (miners) compete to solve complex mathematical puzzles
  - Puzzles are difficult to solve but easy to verify the solution
- First one to find a valid solution gets the rights to create new blocks (and its block creation rewards)

This process of “mining” for the solution is referred to as Bitcoin mining.

Review on hash functions

Proof-of-Work uses hash functions to associate the amount of work done with a block of transactions.

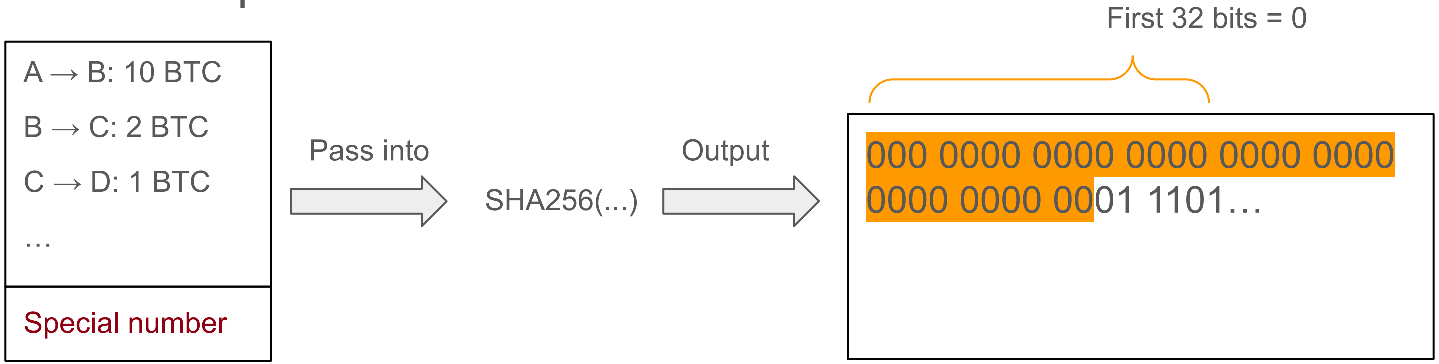
To recall on hash functions:

- Hash functions are irreversible
    - Analogy to jigsaw puzzles: cutting the paper into one million pieces of jigsaw puzzle and shuffling it
- Easy to apply the hash function, hard to find the original data
    - Analogy to birthday problem: hard to guess the person based on a birthday
- SHA256 produces a hash of 64 hexadecimal characters / 256 bits
    - SHA256(?) = 110 1000 1110 0110 0101 0110 …
    - Brute force is the only solution

Mining principle

Proof-of-Work is about finding a special number:

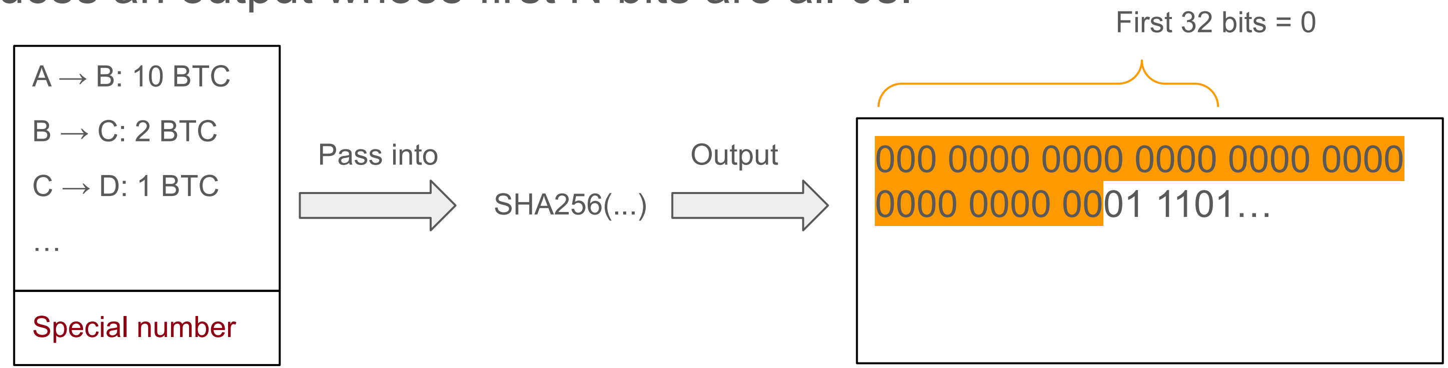
- Combined with the other information from the block and applied SHA256 produces an output whose first N bits are all 0s.



Mining principle

Proof-of-Work is about finding a special number:

- Combined with the other information from the block and applied SHA256 produces an output whose first N bits are all 0s.



First 32 bits = 0

A → B: 10 BTC

B → C: 2 BTC

C → D: 1 BTC

…

Special number

Pass into

SHA256(...)

Output

000 0000 0000 0000 0000 0000 0000 0000 0001 1101…

However, this is very difficult!

- 32 fixed bits, each bit presents the possibility between 0 and 1.
- Probability: 2^{32} = (4 billions) → Random guess = 1 out of 4 billions

Announcements

- No class on Friday
- Reminder to contribute to projects
  - Peer evaluation will be available
  - Team participation required for the demo