

Defi Infrastructure

Week 1

1.

Question 1

Both early barter trading and modern day DeFi are peer-to-peer systems of market exchange.

1 / 1 point



True



False

Correct

Barter markets were very inefficient because you had to exactly match participants. Money arose to solve the inefficiency of barter. As we will see, the tokenization of goods and services will likely lead to a resurgence of barter.

2.

Question 2

Which of the following is **NOT** a primary or secondary role of money?

1 / 1 point



Store of value



Method to earn interest



Medium of exchange



Unit of account



Transfer of value

Correct

Good Job!

3.
Question 3

Iraqi Swiss Dinars were an example of a currency that had intangible value.

1 / 1 point

☒

True

☐

False

Correct

Saddam dinars were backed by the Iraqi central bank. Iraqi Swiss Dinars had no official backing but had intangible value; people simply accepted it as 'money' and continued to use it.

4.
Question 4

Which of the following are TRUE about centralized finance as per the lecture, "Brief overview of CeFi problems"?

1 / 1 point

☒

Fund transfer are not instantaneous

☐

Costs of transacting are low

☐

Every person without exception has access to banks

☐

Perfect interoperability of commercial banking institutions

Correct

Nice work!

5.

Question 5

Why do small entrepreneurs have to fund their businesses with credit cards?

1 / 1 point



Size of these entrepreneurs' businesses is too small to interest institutional channels of finance.



They are afraid that the banks may fail.



Although credit card borrowing is costly, the return on business is always higher than that; thus, profits are mostly assured.



They want to use their credit card so they can build credit history by increasing the volume of their credit card transactions

Correct

Excellent! It is much more profitable for a bank to deal with one large client than a number of small clients. Hence, small businesses often are forced to use credit cards to finance their business investments.

6.

Question 6

Which of these early DeFi ideas made trading stocks cheaper?

1 / 1 point



3-day settlement



Demat accounts



Brokers



Dark pools

Correct

Great! Dark pools broke the exchange monopoly where trading of any stock had to take place on a single exchange. In Dark Pools, executing brokers could trade in a peer to peer way. However, this is not purely DeFi because of the role of executing brokers. That is, when you trade with an App like Robinhood, your order is given to an executing broker. In DeFi, there would be a decentralized app that allowed you to directly transact with your peer rather than using Robinhood plus the executing broker.

7.

Question 7

Which are the problems the plague centralized finance? Hint: You can choose more than one.

1 / 1 point



Limited access

Correct

These are all problems in traditional centralized finance. This will be discussed later in the course.



Centralized control

Correct

These are all problems in traditional centralized finance. This will be discussed later in the course.



Inefficiency

Correct

These are all problems in traditional centralized finance. This will be discussed later in the course.



Opacity

Correct

These are all problems in traditional centralized finance. This will be discussed later in the course.



Lack of interoperability

Correct

These are all problems in traditional centralized finance. This will be discussed later in the course.

8.

Question 8

Most current Fintech initiatives use legacy banking infrastructure?

1 / 1 point



True



False

Correct

Indeed, most Fintech uses the legacy financial infrastructure. For example, Robinhood uses the same traditional brokers and same traditional banks. Apple Pay is just replacing a credit card swipe, there is still a 3% charge.

9.

Question 9

Which ideas did Satoshi Nakamoto combine to introduce Bitcoin?

1 / 1 point



Proof of stake



Blockchain

Correct

Great Choice! The two ideas Nakamoto combined were Haber and Stornetta's (1991) idea of blockchain providing an immutable record and Back's (2002) idea of hash cash which was an early form of proof of work. The proof of work ensured that the ledger could not be edited unless extreme computing power was available.



Mining pools



Proof of work

Correct

Nice Job! The two ideas Nakamoto combined were Haber and Stornetta's (1991) idea of blockchain providing an immutable record and Back's (2002) idea of hash cash which was an early form of proof of work. The proof of work ensured that the ledger could not be edited unless extreme computing power was available.

10.

Question 10

Which of the following statements are **FALSE** with respect to the bitcoin blockchain?

1 / 1 point



Mistakes can be edited and fixed

Correct

The Proof of Work makes it computationally too expensive to censor (change) the bitcoin blockchain history so it is censorship resistant. It is also very easy to move bitcoin (or any crypto) because there is no physical transfer, you just update the ledger and everyone has a copy of the ledger. However, you cannot edit (or censor) history. Further, bitcoin's blockchain is not equipped to run smart contracts. It is purely a transactional platform. Ethereum is an example of a blockchain that can run smart contracts.



Censorship resistant



Computational platform for smart contracts

Correct

The Proof of Work makes it computationally too expensive to censor (change) the bitcoin blockchain history so it is censorship resistant. It is also very easy to move bitcoin (or any crypto) because there is no physical transfer, you just update the ledger and everyone has a copy of the ledger. However, you cannot edit (or censor) history. Further, bitcoin's blockchain is not equipped to run smart contracts. It is purely a transactional platform. Ethereum is an example of a blockchain that can run smart contracts.



Allows for portability of Bitcoin

Week 2

1.

Question 1

Blockchain was invented by Satoshi Nakamoto in the famous 2008 paper.

1 / 1 point

☐

True

☐

False

Correct

Correct! it was invented by Haber and Stornetta in 1991. Nakamoto's use of blockchain was the application that made blockchain famous.

2.

Question 2

No matter how many times an (identical) data set is hashed, the output will always be the same.

1 / 1 point

☐

True

☐

False

Correct

Great! A hash is a one-way function. When you pass the data (input) through the function, there is a unique output (the hash). The same input provides the same output. It is not random. However, if the data/input are altered in any way, the hash changes.

3.

Question 3

Blockchains are called blockchains because the ledger is broken into smaller datasets or blocks. The last line of the block contains a cryptographic hash that is repeated as the first line of the next block thus serving as the "chain".

1 / 1 point

☐

True



False

Correct

Yes! This is exactly how the main blockchains like Bitcoin and Ethereum operate. Any alteration of a block causes the hash in the last line to change thus breaking the chain because it does not match the first line of the next block. The network sees this and replaces the corrupt block with one where the chain is not broken.

4.

Question 4

Go to <https://emn178.github.io/online-tools/sha256.html> and enter the word DeFi (be careful of capitalization and no spaces). Which is the correct SHA-256 output (first six characters):

1 / 1 point



da9fa3



0000sn



340a4d



3871f9

Correct

Excellent!

5.

Question 5

Miners gather transactions, verify that the transactions are valid, hash the transactions (which happens very quickly) and post a new block.

1 / 1 point



True



False

Correct

Great! It is more complex. The miners gather transactions and pick the ones with the largest fees. They verify the transactions (making sure you are not spending more than you have.) They then add a random piece of data called a nonce. Then they hash. They are looking for a unique hash with many leading zeros. If they don't get the rare hash, they alter the nonce and try again. The miner that wins proposes the block of transactions and the nonce. Anyone in the network can hash the

transactions+nonce and get the rare hash (it is easy to verify). This is proof of work and it is computationally very difficult for the Bitcoin and Ethereum blockchains.

6.

Question 6

It is possible today, albeit very computationally challenging, to derive the private key associated with a public key.

1 / 1 point

☐

True

☐

False

Correct

Great Job!

7.

Question 7

The gas required to operate on the Ethereum blockchain is paid in another cryptocurrency acceptable on the Ethereum blockchain.

1 / 1 point

☐

True

☐

False

Correct

Nice work!

8.

Question 8

Miners on the Ethereum blockchain can choose any transactions to add to their block. Thus, inevitably, they end up choosing those transactions that bid the highest fees.

1 / 1 point

☐

True

☐

False

Correct

Great! There is a base fee that depends on the computational needs and the congestion of the network that is burned. There is also a tip or priority fee and this is what the miner gets. Higher tips mean it is more likely the miner will quickly add the transaction to a candidate block.

9.

Question 9

Oracles enable external information to be used in computations on the Ethereum blockchain.

1 / 1 point

☐

True

☐

False

Correct

Nice Work! Blockchains are self contained. For example, there is no way to get, say, the price of gold from the Ethereum blockchain. Hence, we need a mechanism that works algorithmically to go outside of the blockchain to a particular URL to collect that information. When you engage with a smart contract, you can see the source of the information and you need to trust that information source.

10.

Question 10

There are three types of stablecoins: fiat or other asset collateralized, cryptocollateralized, and non-collateralized.

1 / 1 point

☐

True

☐

False

Correct

Excellent! USDC is a good example of a fiat collateralized stablecoin. DAI is an example of a crypto collateralized stablecoin which we will explore in detail in the third course. The non-collateralized are challenging in that they rely on dynamic money supply and other mechanisms.

11.

Question 11

DAOs or decentralized autonomous organizations have a board of directors, a CEO that has control over major decisions, and company headquarters.

1 / 1 point

☐

True



False

Correct

Good Job! DAO's are algorithms that enable peer to peer interaction via decentralized applications. DAOs often have a decentralized governance mechanism in the form of a governance token whereby token holders vote on important parameters

Week 3

1.

Question 1

There is little difference between a dApp and an Apps like Robinhood, Venmo, Zelle, WeChat Pay, Alipay, etc.

1 / 1 point



True



False

Correct

Nice work! dApps allow peers to interact with each other via a smart contract. The Apps that are listed are all run by centralized institutions. You interact with the centralized institution and they collect your data. These dApps are available to anyone - there is no screening. There is near zero organizational overhead. This is fundamentally different than decentralized applications.

2.

Question 2

Keepers and Oracles are essentially the same, except that keepers do for DeFi platforms what Oracles do for blockchains.

1 / 1 point



True



False

Correct

Great! Keepers are associated with externally owned accounts and they maintain key features of a blockchain protocol and get rewarded for it. As we will see in the third course, they will search for undercollateralized loans and close out positions for a fee. Oracles bring external information into a blockchain and are completely different.

3.

Question 3

While vampirism is a risk to DeFi platforms due to their open-source nature (i.e., code can be copied and repurposed), there is a benefit of using existing code and improving on it.

1 / 1 point



True



False

Correct

Excellent! Smart contracts are open source. It is easy to grab the code and make improvements. Vampirism usually refers to a situation where the code is exactly replicated with a small change - usually a higher reward for using the platform. The existing platform may need to raise rewards to remain competitive.

4.

Question 4

Yield farming refers to a situation where a user deposits crypto funds (potentially in various different DeFi platforms) and seeks the highest possible rewards or savings rates.

1 / 1 point



True



False

Correct

Yes! The user could be paid the equivalent of a savings rate. The user might also get another token, such as a governance token, as a reward. The governance token reward means that the user

becomes an integral part of the platform (it is analogous to getting a reward in J.P. Morgan stock as well interest on a deposit at J.P. Morgan's bank). As we will see in the next course, the user make also get an equity token (representing a share of the liquidity pool), that could be redeployed to earn further rewards.

5.

Question 5

Initial DeFi Offering, or IDOs, are a long, expensive process, that includes filing with securities regulators such as the SEC in the US.

1 / 1 point



True



False

Correct

Awesome! If the token is not a security, it is easy and quick to do an IDO. You add your token and some other such as ETH to the pool. If you add 100,000 USDC and 1 million of your token, then your token has a price of 0.1 USDC (or 10 cents). With this method, a new protocol can establish a value for their token quickly. Of course, there is no guarantee that the token price will go up.

6.

Question 6

DeFi refers to a fast-growing and highly opaque corner of the cryptocurrency market.

1 / 1 point



True



False

Correct

Super! This is an exact quote from a letter from U.S. Senator Elizabeth Warren to the Secretary of the U.S. Treasury, Janet Yellen on July 26, 2021. In contrast to this statement, DeFi is completely transparent. Smart contracts can be read by anyone. It is also possible for anyone to figure out the balances associated with various addresses. Centralized finance is highly opaque. We don't know the health of banks, brokers, and insurance companies. We rely on regulators to watch them.

7.

Question 7

A DeFi protocol is truly decentralized only if special privileges are given to the administrator.

1 / 1 point



True



False

Correct

Great Job! Often a new protocol is launched whereby the developers have a large amount of control. At this stage, it is not decentralized because the developers control the application. This is often convenient because there could be fine tuning that has to happen quickly. To become decentralized, the governance needs to be distributed to a larger population. Often a governance token is launched and distributed to the users of the platform. In the third course we talk about this. Also, if the protocol is too centralized, it is possible that someone forks the protocol and makes it decentralized. This is another mechanism to ensure decentralization.

8.

Question 8

DeFi Legos is a concept that implies that each DeFi protocol is rigid and is incapable of interacting with other DeFi protocols.

1 / 1 point



True



False

Correct

Good! Interoperability is one of the key benefits of DeFi. We say DeFi Legos because the pieces fit together and when connected make something greater than the sum of the pieces.

9.

Question 9

Tokenizing physical assets is much more straightforward than tokenizing virtual assets.

1 / 1 point



True



False

Correct

Excellent! It is much more complicated to tokenize physical assets. For example, USDT and USDC need to hold collateral that needs a constant audit. Indeed, and surprisingly, much of this collateral is not in dollars but in risky commercial paper and other products. The collateral is not immediately transparent to users. The same goes for gold tokens where you need to warehouse the gold, set up security, pay for audits. For virtual collateral, anyone can see the collateralization ratios. That is, it is like there are instantaneous audits. There are no warehousing costs.

10.

Question 10

One disadvantage of an Initial DeFi Offering is that an artificial floor on the cryptocurrency price is established that potentially could inhibit price discovery.

1 / 1 point



True



False

Correct

Great! It is possible that the fair value of the token is less than the floor price. Some market participants might be misled by this, i.e., thinking that the token is worth more than the fair value

Week 4

1.

Question 1

All cryptocurrencies are anonymous and the technology makes it easier for criminals to operate.

1 / 1 point



True



False

Correct

Good! The main cryptos are only pseudonymous. That is, you can set up an address to receive illicit funds. Everybody sees the transaction. Every time you move the funds, everyone sees that too. If an address is identified as a person's particular address, then justice is swift (given blockchain is an immutable record, you cannot say the transaction has been forged). That said, there are some cryptos that are truly anonymous.

2.

Question 2

The Bitcoin and Ethereum blockchains are routinely hacked so these cryptos are not safe to use.

1 / 1 point



True



False

Correct

Well done! Exchanges are sometimes hacked but this has nothing to do with blockchain. There was a high profile story about U.S. government recovering funds that were extorted from the Colonial Pipeline. Again, this had nothing to do with blockchain hack. The criminals' computer was broken into and they unwisely kept their private keys on the computer. Smart contracts are sometimes exploited. These are algorithms that are deployed to the Ethereum blockchain. Again, this is independent of the Ethereum blockchain and simply reflects a smart contract that is not secure.

3.

Question 3

Central banks' Central Bank Digital Currencies or CBDC have nothing to do with DeFi.

1 / 1 point



True



False

Correct

Nice work! Think of CBDC as centralized digital currencies. They may use a ledger that has some resemblance to a blockchain. However, they are centralized. That is the central bank controls the money supply. The central bank can add or subtract supply. The central bank can censure or block. Further, the ledger might not be transparent. This does not really resemble a blockchain construct and has little to do with DeFi.

4.

Question 4

All cryptocurrencies have no fundamental value.

1 / 1 point



True



False

Correct

Kudos! First, there are many types of cryptos. For example, those that are back by an asset like gold or USD, have fundamental value. Second, even for those cryptos that have no backing, like bitcoin or ethereum, you need to take into account intangible value. For example, Ethereum opens up the possibility of a new way of doing borrowing and lending, exchange, etc., which gives it value.

5.

Question 5

Quantum computing poses very little threat to the main cryptocurrencies.

1 / 1 point



True



False

Correct

Good! For those using Proof of Work hashing, quantum is likely irrelevant because quantum computing is not helpful in finding collisions (two inputs producing the same output or hash). Quantum computing might allow a computer to derive a private key from a public key. However, before that happens, a new quantum proof signature algorithm will be deployed. These algorithms already exist today.

6.

Question 6

Today the cost of transacting on the main networks like Bitcoin and Ethereum is trivial, opening up a new way to handle day to day transactions, like buying a coffee at Starbucks.

1 / 1 point



True



False

Correct

Super! The cost of transacting on the Bitcoin blockchain is very high making it only useful for large value transactions. The cost of transacting on the Ethereum blockchain is lower but still not low enough for smaller transactions. Ethereum is taking steps to greatly increase its capacity which will reduce transaction costs. We study these changes in the fourth course.

7.

Question 7

DeFi is so hard to understand that it will likely go nowhere.

1 / 1 point



True



False

Correct

Yes! Just because something is complex does not mean it will go nowhere. Few understand how the Internet or email works - yet we use it every day. The DeFi technology is early and will only be widely adopted when the user interface becomes so simple that anybody can use it without understanding all the details. However, at this stage there are some barriers to entering. Taking this course empowers you to be a leader in this space.

8.

Question 8

Given the rise of cryptocurrencies like bitcoin and ethereum, the price volatility has substantially decreased due to widespread use.

1 / 1 point



True



False

Correct

Great! Volatility has not substantially changed. The main cryptos are about five times more volatile than the stock market or gold. I believe there are two main driving forces. First, the markets are still relatively illiquid, meaning a big buy order or sell order could substantially move the price leading to volatility. Second, and more importantly, it is really hard to value cryptos. For stocks, we can forecast earnings. While analysts might disagree on a stock's value, there is a range of valuation. For bitcoin and ethereum, the range is massive because some believe they are worth zero and others a million dollars.

9.

Question 9

The DeFi space is just too small compared to banks and, as such, is doomed to be a failure.

1 / 1 point



True



False

Correct

Great! The first part is true. DeFi is very small. Less than 1% of the size of CeFi. However, just because you are small today does not doom you to failure. All new technologies start out small. The key is the growth rate. DeFi has grown from non-existent just a few years ago to a substantial size, albeit still small compared to CeFi. The key to the future is whether the growth rate continues.

10.

Question 10

Mining that underlies Proof of Work crypto protocols like Bitcoin and (currently) Ethereum is environmentally damaging.

1 / 1 point



True



False

Correct

Nicely done! Bitcoin uses the equivalent energy as Argentina. Ethereum is also energy intensive but they will switch to a less energy intensive mechanism -- we discuss in the fourth course. The Proof of Work mining is both a strength and a weakness. It is a strength because of the unprecedented security. It is infeasible to hack either chain. However, this comes at a cost. In the fourth course, we go into considerable detail in a section called Environmental Risk.