DeFi Primitives

Week 1

1.

Question 1

DeFi transactions are atomic meaning that if there is a problem at any step in the transactions the initial money or data transferred is locked forever in the contract.

1 / 1 point

True

False

Correct

Great! Atomicity means that if there is any problem with any step in the transaction, we automatically revert to the initial state. Hence, nothing is “lost” (other than a gas fee).

2.

Question 2

Ethereum has externally owned accounts and contract accounts whereas bitcoin only has contract accounts.

1 / 1 point

True

False

Correct

Excellent! EOA are used for transfers, i.e., transferring one ETH or BTC to another user. Ethereum, in contrast to Bitcoin, allows for smart contracts. Hence, it is possible to have a contract account. That is, an EOA can interact with either other AOA or CAs. There are no smart contracts in bitcoin and no contract accounts.

3.

Question 3

Higher gas fees occur when there is not much demand. The miners thus have lower revenue and need to raise gas prices to break even.

1 / 1 point

True

False

Correct
Yes! When there is considerable congestion in the network, users will pay a premium (priority fee) to get their transaction approved quickly and gas fees also increase. As Ethereum moves to ETH 2.0, there will be far less congestion in the network meaning that the cost of doing transactions will drop.

4.

Question 4
Pending transactions are hidden in the mempool. We publicly see the transactions once they are approved by miners and show up in the Ethereum blockchain.

1 / 1 point

True

False

Correct
Great Job! Anyone, including the miners, can see the pending transactions in the mempool. This is true for Ethereum and Bitcoin.

5.

Question 5
Miner Extractable Value refers to the priority fees or tips that miners get for doing certain transactions before others.

1 / 1 point

True

False

Correct
Correct! MEV is when miners strategically exclude or reorder transactions so they can profit. Remember that all pending transactions are public information. This means that a miner can legally front-run (see a transaction that is pending, e.g., a large buy order and jump ahead of it to profit from price movements). Of course, the miner might not win the block. However, many miners may be trying the same idea. MEV is largely a problem with Proof of Work consensus systems. ETH 2.0 will use an alternative consensus mechanism, Proof of Stake.

6.

Question 6
Equity tokens are ERC-20 tokens exclusively backed by stocks trading on world stock exchanges like NYSE, NASDAQ, etc.

1 / 1 point

True

False

Correct
It is much more general. An equity token might represent a user's share of a liquidity pool. Suppose you contribute some ETH into a liquidity pool. To keep track of your share of ownership in the pool, an equity token is issued (minted). When you redeem the original investment, the token is destroyed (burned).

7.

Question 7
Which of the following are use cases for utility tokens:

*More than one answer can be chosen.

1 / 1 point

Collateral

Correct
Utility tokens are tokens that are required to utilize the functionality of the smart contract system. They can represent collateral (SNX studied later), stake (LINK), stablecoins (DAI), and used to pay fees (DAI). We discuss these later.

Reputation or stake

Correct
Utility tokens are tokens that are required to utilize the functionality of the smart contract system. They can represent collateral (SNX studied later), stake (LINK), stablecoins (DAI), and used to pay fees (DAI). We discuss these later.

Stablecoins

Correct
Utility tokens are tokens that are required to utilize the functionality of the smart contract system. They can represent collateral (SNX studied later), stake (LINK), stablecoins (DAI), and used to pay fees (DAI). We discuss these later.

Pay application-specific fees.

Correct

Utility tokens are tokens that are required to utilize the functionality of the smart contract system. They can represent collateral (SNX studied later), stake (LINK), stablecoins (DAI), and used to pay fees (DAI). We discuss these later.

8.

Question 8

Governance tokens represent the holder's share of the asset ownership, very similar to TradFi stocks which represent share of company and voting rights.

1 / 1 point

True

False

Correct

Good! Equity tokens represent the share of ownership. The governance tokens apply to voting rights. Governance is used to vote on changes in the system such as adjusting parameters, adding new components or altering functionality.

9.

Question 9

ERC-721 or non-fungible tokens (NFTs) represent the unique ownership of a unique asset.

1 / 1 point

True

False

Correct

NFTs are sometimes called deeds because a deed is proof of ownership of a unique asset. NFT are popular in art, gaming, video, music and have many applications.

10.

Question 10

An ERC-721 token can be fractionalized within the ERC-721 standard so that, for example, many could share ownership of a valuable piece of art.

1 / 1 point

True

False

Correct
ERC-721 cannot be fractionalized within ERC-721 (that's why I repeated ERC-721 twice here). However, it is straightforward to vault an ERC-721 and then issue ERC-20 equity tokens based on the ERC-721 asset. The key here is that you need to use ERC-20 fungible tokens to do this. The ERC-721 cannot be split.

Week 2

1.
Question 1

There is no risk in escrowing funds in a smart contract because you can always get the funds back (atomicity property).

1 / 1 point

True

False

Correct

There are plenty of risks. If the smart contract is not written properly it is possible that the custodied funds could be lost forever.

2.
Question 2

Burning a token is accomplished by altering the private key (e.g., interchanging some of the bits).

1 / 1 point

True

False

Correct

Yes! There are two ways to burn an ERC token. First, burning is accomplished by sending the token to an unowned address. This is a public address that is not derived from a private key. Second, burning can be accomplished by sending the token to a contract that is specifically designed so that the token can never be re-spent. The second method is preferred. In EIP-1559, the gas fees are burned. In this case, ETH is burned. This is accomplished by taking the transaction fee and not updating anyone's (the miner's) account balance.

3.
Question 3

Minting (or inflating) an ERC-20 is done (for example) to represent new ownership in an asset pool or to reward user behavior.

1 / 1 point

- (•) True
- ( ) False

Correct

Good! When a user adds to a liquidity pool, it is common to mint an equity token that represents that user's share in the pool. That equity token is valuable and is often traded on its own. Minting is also used to reward users for using a protocol. Minting is also used in algorithmic stablecoins to increase supply thereby driving down prices towards the desired peg.

4.
Question 4

Linear bonding curves with positive slopes make it more expensive for the first users to buy a token.

1 / 1 point

- ( ) True
- (•) False

Correct

Excellent! The first users get the best deal in most bonding curves. In the example, I used TKN= mS where m (slope) =1. The first TKN would cost 1 ETH. The second would cost 2 ETH.

5.
Question 5

The two main types of incentives are: staked incentives and direct incentives.

1 / 1 point

True

False

Correct

Good! Staked incentives apply to the balance of tokens custodied in a smart contract. Direct incentives apply to users with the system who do not have a custodied balance.

6.
Question 6

An example of a slashing situation is when a user's staked balance is reduced because of an undercollateralization event.

1 / 1 point

True

False

Correct

Awesome! If a liquidation is triggered because of undercollateralization, there is a slashing of the collateral that is used to pay the keeper that closed out the position. In this case, the slashing is done because a condition is violated. The user knows this could happen. The slashed proceeds are used to reward the keeper.

7.
Question 7

Keepers are triggered algorithmically and are part of the smart contract mechanism.

1 / 1 point

True

False

Correct

Great! Keepers are externally owned addresses. They are not part of the algorithm of the smart contract. They watch for events like undercollateralization and close out positions that violate the term of the contract. They are rewarded.

Week 3

1.
Question 1

Exchanges like Coinbase and Binance are exemplars of decentralized finance.

1 / 1 point

True

False

Correct

Super! Coinbase and Binance are examples of centralized exchanges that often provide trading for DeFi products. They are companies and Coinbase is even listed on the NASDAQ exchange. Sometimes they are called CeDeFi., Later we will talk about truly decentralized swapping known as DEX.

2.
Question 2

The following are signs that a centralized exchange may be faking volume (choose all that are correct):

1 / 1 point

Rapidly offsetting trades

Correct

There is a lot of fake volume and it is likely that over 90% of the world exchange volume is fake. Remarkably (at the time of drafting these questions), there are 18,998 exchanges for trading crypto.

It is easy to create fake volume because you can easily move money from your left pocket to your right. The centralized exchanges that are trustworthy are largely the ones that are regulated. I will argue that these centralized exchanges will be replaced eventually by DEX.

☑

Wide spreads

Correct

There is a lot of fake volume and it is likely that over 90% of the world exchange volume is fake. Remarkably (at the time of drafting these questions), there are 18,998 exchanges for trading crypto. It is easy to create fake volume because you can easily move money from your left pocket to your right. The centralized exchanges that are trustworthy are largely the ones that are regulated. I will argue that these centralized exchanges will be replaced eventually by DEX.

☑

Long gaps with no trading

Correct

There is a lot of fake volume and it is likely that over 90% of the world exchange volume is fake. Remarkably (at the time of drafting these questions), there are 18,998 exchanges for trading crypto. It is easy to create fake volume because you can easily move money from your left pocket to your right. The centralized exchanges that are trustworthy are largely the ones that are regulated. I will argue that these centralized exchanges will be replaced eventually by DEX.

☑

Constant volume no matter what time of the day or day of the week

Correct

There is a lot of fake volume and it is likely that over 90% of the world exchange volume is fake. Remarkably (at the time of drafting these questions), there are 18,998 exchanges for trading crypto. It is easy to create fake volume because you can easily move money from your left pocket to your right. The centralized exchanges that are trustworthy are largely the ones that are regulated. I will argue that these centralized exchanges will be replaced eventually by DEX.

☑

No clustering of volume around round numbers

Correct

There is a lot of fake volume and it is likely that over 90% of the world exchange volume is fake. Remarkably (at the time of drafting these questions), there are 18,998 exchanges for trading crypto. It is easy to create fake volume because you can easily move money from your left pocket to your right. The centralized exchanges that are trustworthy are largely the ones that are regulated. I will argue that these centralized exchanges will be replaced eventually by DEX.

Exchange has applied to be fully regulated by a U.S. regulatory body.

3.
Question 3

There are two types of decentralized exchange: order book matching and automated market makers.

1 / 1 point

True

False

Correct

Order book matching is costly to do on chain. However, as we will see, there are some workarounds including a Layer 2 (multisignature wallet that is secure off chain) that we will study in the third course. AMMs are popular because they are always available for trading and the liquidity is transparent.

4.
Question 4

The invariant is the product of the value of one token and the value of the other token in the AMM.

1 / 1 point

True

False

Correct

The invariant = x*y where x is the number of token 1 and y is the number of token 2 (note the number, not the value). When the Uniswap v2 is set up, the total value of all of the x and all of the y tokens are identical. So if token 1 is worth 1 cent and token 2 is worth $1 and we put an equal amount of value (say $100 of each), the invariance would be 10,000x100=1,000,000.

5.
Question 5

A liquidity provider does not incur impermanent loss if the exchange rate between two tokens remains constant or varies but returns to the same rate as when the liquidity was added.

1 / 1 point

True

False

Correct

Yes! Both of these conditions are rare, hence the liquidity provider will almost always incur impermanent loss (which is the opportunity cost of the value of the token if you have just held them vs. what happens in the AMM). Of course, the liquidity providers are getting rewards for providing liquidity in the first place. It is likely these rewards are much greater than the impermanent loss.

6.
Question 6

Given there is no external collection mechanism, no credit scores, and no identification of borrowers, loans in DeFi need to be collateralized - indeed, overcollateralized.

1 / 1 point

True

False

Correct

Excellent! The overcollateralization prevents any counterparty from defaulting. Think of mortgages. The bank holds your house as collateral. If you stop paying, the bank has recourse over your house. The same intuition applies in DeFi except that the collateral is crypto.

7.
Question 7

Crypto-collateralized stablecoins are analogous to collateralized loans.

1 / 1 point

True

False

Correct

Good! The value of the stablecoin is kept near the peg because users can see the value of the collateral. Indeed, all currency whether crypto or non-crypto is like a loan or an IOU. Fiat currencies are not collateralized today. Before August 15, 1971, the USD was collateralized with gold.

8.
Question 8

The interest rate on flash loans is high because they have both duration risk and counterparty credit risk.

1 / 1 point

True

False

Correct

Flash loans are executed with zero duration (within a single transaction the loan is taken out and repaid). There is no counterparty risk because the transaction is atomic - any problem with the transaction and we revert to the original state before the loan was taken out. Also, there is no “interest rate”. Some protocols charge a fee but others do not.

9.
Question 9

Given that flash loans have zero duration and have no counterparty credit risk, these loans are “risk free”.

1 / 1 point

True

False

Correct

There are always risks. One of the major risks is smart contract risk which we discuss in the fourth course in great detail.

Week 4

1.
Question 1

You need to transfer fiat currency to buy ethereum on the Ropsten Test Network.

1 / 1 point

True

False

Correct

Great! The testnet is an area where new ideas are tried. Developers deploy their first versions of their smart contracts to the testnet and then try to find weaknesses. Test ETH is free. All ERC-20 tokens on the testnet are free. It is a testing ground. Nevertheless, your address works on both the testnet and the mainnet. You have a dropdown to choose.

2.
Question 2

Send 0.1 testETH to my address: **0xff65F352156D2c69F9AbbF1AEF18E6d85314Ecce**

Once you have completed this, answer “true” (honor system because the functionality of Coursera does not interact with DeFi yet). Also, you can send me real ETH too off the mainnet!

1 / 1 point

True

False

Correct

Thank you!

3.
Question 3

Hashing some data is the same thing as encrypting the data.

1 / 1 point

True

False

Correct

Super! Cryptographic hashing is a one-way function. However, in encrypting, the function goes two ways. That is, if you encrypt a document, there is a key to decrypt and recover the original document. Once you hash a document, there is no way (other than brute force) to recover the original document. Also, some of the original data is lost in hashing. For example, you could hash a 50gb file and the size of the hash is only 64 hexadecimal characters (or 256 bits). It does not make sense that you can recreate the 50gb file with so little information.

4.
Question 4

Hashing the same data with a SHA-256 and a Keccak-256 delivers the identical hash (though Keccak has more steps).

1 / 1 point

True

False

Correct

They are completely different algorithms and will deliver different outputs. Go to: https://emn178.github.io/online-tools/sha256.html and try for yourself

5.
Question 5

Asymmetric key cryptography is when there is a single key to encrypt and decrypt.

1 / 1 point

True

False

Correct

Great! Symmetric key cryptography has a single key that is used to encrypt and decrypt (for example, if you encrypt a PDF, you do this with a single key which is in the form of a password). Asymmetric key cryptography is extensively used in blockchain technology. Here there is a public key that anyone can see but a private key that is secret. For example, anyone can encrypt a file with your public key and send it to you. Only you can decrypt the file with your private key. The asymmetric keys are used in digital signatures that are crucial for Ethereum and Bitcoin transactions.

6.
Question 6

A private key is just a random number.

1 / 1 point

True

False

Correct

Yes! It is a long random number, in Ethereum and Bitcoin, 512 bits or 128 hexadecimal characters. The public key is derived from the private key using elliptic curve operations. It is easy to go from the private key to the public key. However, given the state of computing today, it is infeasible to derive the private key from the public key.

7.
Question 7

An Ethereum address is just your public key.

1 / 1 point

True

False

Correct

Well done! It is derived from the public key. Step one is to do a Keccak-256 hash of the public key (removing the 04 from the beginning of the key). Step two is to select the last 40 hexadecimal characters. Step three is to prepend “0x"

8.
Question 8

Digital signatures, in contrast to regular signatures, change every time you sign - even if the message (or data) is identical.

1 / 1 point

True

False

Correct

The signature consists of the message (data, which might be a transaction), your private key, and a nonce (random piece of information). The nonce changes every time so each signature is unique. Anyone can verify that you signed knowing the message and your public key (along with some shared parameters of the ECDSA).

9.
Question 9

Consensus is the process by which nodes agree on the same ledger.

1 / 1 point

True

False

Correct

Good! Vitalik Buterin’s (founder of Ethereum) succinct definition of consensus is “Consensus is the process by which all nodes agree on the same ledger.” Notice I dropped the “all”. Remember, the

ledger or blockchain, is a shared database amongst all the nodes in the network. There needs to be agreement on a single ledger. However, consensus is complicated. It is not clear that all need to agree. But if there is disagreement that could be a forking situation.

10.
Question 10

Consensus is when 51% (rounded, anything above 50%) agree.

1 / 1 point

True

False

Correct

While this might be true for Ethereum and Bitcoin, consensus could be defined in many ways. Consensus could be supermajority (e.g., 66%). Consensus might be unanimity (100%). Indeed, it is possible to have differential weighting of votes. So consensus does not necessarily mean majority.

11.
Question 11

Proof of Stake, like Proof of Work, is very energy intensive.

1 / 1 point

True

False

Correct

Good! In Proof of Work, many miners are trying at the same time to solve the same problem. The work is redundant and very energy intensive. In Proof of Stake, a single miner is chosen probabilistically based on their stake, to add a block. That is, if you have 10% of the total staked value, then there is a 10% chance (over a longer period) that you will be chosen. Given there is no redundancy, this technology is much more energy friendly.

12.
Question 12

A drawback of Proof of Stake is that it could lead to centralization.

1 / 1 point

True

False

Correct

Yes! This argument is that the rich get richer.

13.
Question 13

Ethereum’s throughput is about 15 transactions per second which means that DeFi can never compete with TradFi like Visa.

1 / 1 point

True

False

Correct

It is true that Ethereum only does a small fraction of what Visa does, but that is today. There are plenty of initiatives, including the move to Proof of Stake, that will change this.

14.
Question 14

Which of the following is NOT a current consensus mechanism in DeFi:

1 / 1 point

Government edict

Proof of Delegated Stake

Proof of Activity

Delegated Byzantine Fault Tolerance

Correct

Nice Job! There are many consensus mechanisms in the world of blockchain technology and this is an active area of research. However, centralized government edict is not one of them.

15.
Question 15

In Ethereum, account balances are updated in transactions whereas in Bitcoin a user accumulates unspent transaction outputs.

1 / 1 point

True

False

Correct

Super! Bitcoin’s system is different from Ethereum’s. In Bitcoin, a user will have unspent transaction outputs representing various amounts of bitcoin. These can be combined to pay for something and anything left over (the change) is sent back to the user in the form of a new unspent transaction output. Ethereum’s system is much more straightforward in that the balances of an address are updated after transactions.