DeFi Risks & Opportunities

Week 1

1.

Question 1

Hacking a smart contract is difficult because you first have to gain access to the contract (break the encryption) and then find a way to exploit the contract.

1 / 1 point

True

False

Correct

The smart contracts are open for anyone to see. In traditional hacking of a centralized company, the hacker first must gain access to the site which is different. Then the hacker needs to figure out what to do. The “new attack vector” with smart contracts is that everything is open. So the hacker can focus immediately on some exploit of the contract.

2.

Question 2

An example of a smart contract logic error is rounding. If the payout is rounded, then it is possible there are insufficient funds in the contract and the transaction will fail, locking the funds forever.

1 / 1 point

True

False

Correct

Suppose the contract has 3.9999999999990 ETH and the payout is rounded to 4 ETH. The transaction will fail because the contract does not have 4 ETH. It is possible the funds are locked forever. This is a basic logic error.

3.

Question 3

An example of an economic exploit is the exchange between two tokens when the price is linked via an oracle to an illiquid exchange. The exploiter can attack the oracle exchange and manipulate the price.

1 / 1 point

True

False

Correct
Suppose the attacker sells token A heavily on the illiquid exchange driving the price down. The attacker then buys (cheap) token A from the smart contract and then dumps them on another exchange.

4.
Question 4
The DAO attack was caused by the re-entrancy bug whereby you could continually withdraw from the contract before the balance was updated.

1 / 1 point

True

False

Correct
Essentially, this is a misordering of two lines in the code. This is why it is very important to have a careful audit of the code before posting. There are companies that specialize in code audits.

5.
Question 5
The DAO was attacked by two hacking groups draining all of the funds leading to the DAO investors losing everything.

1 / 1 point

True

False

Correct
It is true that two hacking groups attacked. However, the second group, the Robin Hood group, drained 70% and was “white hat” in that they promised to give back their funds to the original investors. Also, at the time of the hack, no one lost anything because there was a mandatory hold on funds specified in the contract. Finally, in the end Ethereum forked to undo the hack. The hack still exists given the original chain is preserved in Ethereum Classic.

6.
Question 6

After this DAO episode, the SEC declared that DAO tokens were NOT securities giving the green light to many other DeFi projects like the DAO.

1 / 1 point

True

False

Correct
The SEC ruled that the DAO was an investment contract. Those putting in funds expected a reasonable rate of return. 2016 was the first time that the SEC had made any ruling in this space.

7.

Question 7
The fork that Ethereum created to undo the DAO hack was a “soft” fork.

1 / 1 point

True

False

Correct
A soft fork is for minor changes and upgrades are compatible with previous versions. Indeed, some nodes can run the old version and some the new and everything works fine. The fork that occurred in 2016 was a hard fork which is not backward compatible. In addition, it was a contentious fork (compared for example to the recent London fork for Ethereum). There was considerable disagreement as to whether the history should be changed. Many abandoned ETH and invested in ETC.

8.

Question 8
It is a red flag that a new protocol reuses a smart contract and does not even bother to delete the comments in the code that are relevant only for the original creator.

1 / 1 point

True

False

Correct

This is a red flag because it shows that the developers did little or nothing with the original code and might not even understand it. We talked about the Lendf.me exploit where the word “Compound” (where they copied the code from) appeared four times in the dForce contract.

9.

Question 9

Exploits like the Yearn.finance episode involved 161 transfers and a $200 million initial capital implying that only the wealthy are able to make a lot of money in exploiting vulnerable smart contracts.

0 / 1 point

- (•) True
- ( ) False

Incorrect

The exploit started with a $200 million Flash Loan where 116,920 ETH were borrowed from dYdX. The flash loan is uncollateralized. Hence, it is possible that the exploiter had no capital - perhaps not even a traditional bank account. The exploit emphasizes that DeFi levels the playing field. All peers are equal.

10.

Question 10

A “rug pull” is when a large amount of a token goes into a smart contract and then the developers freeze (or brick) the funds.

1 / 1 point

- ( ) True
- (•) False

Correct

Rug pull goes like this: 1) new token is launched on a DEX via an IDO; 2) very high reward is paid for offering liquidity; 3) investors are attracted and offer liquidity driving the price of the token up; 4) once the pool is large enough, the original developers sell everything on the DEX causing the price to eventually drop near zero. The original developers get all of the premium price that investors paid for the token as it was being promoted.

Week 2

1.

Question 1

All smart contracts are subject to governance risk.

1 / 1 point

True

False

Correct

No, some are just algorithms that cannot be changed such as Uniswap v2. Other protocols like MakerDAO rely upon the governance to fine tune parameters such as collateralization ratios and rewards. The protocols with governance are subject to governance risk which involves a consensus of the governance making changes that are not in the best interest of the users of the protocol.

2.

Question 2

It is always optimal to immediately launch decentralized governance when initiating a new protocol.

1 / 1 point

True

False

Correct

Often the developers retain control initially because they realize that some fine tuning of the code is necessary and it might be urgent to do it. If they have to wait for a governance vote, that could put the protocol at risk. However, the high quality protocols will have a roadmap to decentralized governance.

3.

Question 3

In the $TSD governance attack, the developers took advantage of their majority stake and printed too many $TSDs.

1 / 1 point

True

False

Correct
The developers had only 9%. The exploiter built up more than 9% and introduced a proposal to mint for themselves11.5 quintillion $TSD. The exploiter then sold 11.8 billion $TSD on Pancakeswap. You might wonder why only 11.8b? Here, think of the way a CPAMM works. At some point, the value of the $TSD gets very close to zero. That point was 11.8 billion. Also, if you have a sharp eye, the fourth Tweet from TSD incorrectly says the hacker minted 11.8 billion $TSD. It was actually 11.5 quintillion.

4.

Question 4
A DNS attack (where a website domain is taken over) is a risk that is specific to DeFi.

1 / 1 point

True

False

Correct
This risk applies to any company that has a website.

5.

Question 5
If you get an email from MetaMask saying that there is a problem with your wallet and they will fix it, then you should send them your seed phrases.

1 / 1 point

True

False

Correct
No legitimate company will ask for your private key or seed phrases. You should never give them out. In addition, these should be kept off the Internet on a USB drive or even a hard copy.

6.

Question 6
An oracle attack is only feasible if the cost of corruption is greater than the profit from corruption.

1 / 1 point

True

False

Correct
Oracles are a way to get off-chain information on-chain. It might be crypto price or a sports score. This needs to be done in a secure way. If the exploiter determines that the cost of corruption is LESS than the profit from corruption, this invites an oracle attack.

7.

Question 7
Two common oracle risks are: a) front running and b) downtime.

1 / 1 point

True

False

Correct
A popular exploit is to attack an illiquid liquidity pool that is linked to an oracle and then trade elsewhere. If the oracle is offline, then transactions sent to a smart contract with oracle calls will fail.

8.

Question 8
DEXs, such as CFAMM, attract liquidity but are subject to both smart contract risk and impermanent loss.

1 / 1 point

True

False

Correct
We have already discussed smart contract risk and the possibility of a logic error. We have also discussed impermanent loss which is the opportunity cost of the scenarios (what you would have made if you did not put your tokens in the liquidity pool). The impermanent loss occurs anytime there is a deviation from the original relative value of the tokens. Of course, the liquidity provider is making a fee when users engage the CFMM, however, it is possible that cost is greater than the benefit.

9.

Question 9
On-chain order books are always preferred to off-chain order books.

0 / 1 point

True

False

Incorrect
The problem with on-chain order books is that it is currently very costly to put potential transactions (bids and offers) on-chain because of gas fees. Some prefer off-chain, Layer 2, solutions like dYdX.

10.
Question 10
A private key is mathematically derived from the public key.

1 / 1 point

True

False

Correct
The private key is a long random number. The public key, in Ethereum, is derived from the private key using elliptic curve mathematics. Custody is about securing your private key.

11.
Question 11
The three types of custody are: a) self-custody; b) partial custody; and c) third-party custody.

1 / 1 point

True

False

Correct
Self custody would be you keeping your private keys/seed phrase off-line in an USB or even hard copy. Partial custody is where you share information and the shared information can reconstitute the key. Delegated custody would be a third party, like Coinbase, holding your keys.

12.
Question 12
MakerDAO (behind the DAI stablecoin) is not subject to governance risk because it is a centralized organization.

1 / 1 point

True

False

Correct
"DAO" is "decentralized autonomous organization". MakerDAO is decentralized and their decentralized governance token is MKR. Hence, the same governance risks apply to MakerDAO as to other centralized protocols.

13.

Question 13
The New York Times story regarding the lost $220 million of bitcoin is an example of why you should not delegate custody to a third party.

1 / 1 point

True

False

Correct
The story was about someone who self-custodied. As mentioned, you can keep your keys on a USB drive or hard copy. However, there are other possibilities including a hardware wallet. This wallet is not connected to the Internet. It holds your keys and you need a password to get into the wallet. The particular wallet in question will self-destruct after 10 failed password attempts.

14.

Question 14
A custodian such as an exchange will keep their "hot" wallet on a USB key or a hardware wallet.

1 / 1 point

True

False

Correct
Cold storage refers to keeping the private keys offline on a USB or hardware wallet. Hot wallets are vulnerable to hacks. Exchanges need to keep a certain number of keys quickly available for trading.

15.

Question 15
A user adopting a shared approach to custody is at great risk if the provider, such as BitGo, is hacked.

0 / 1 point

True

False

Incorrect
Think of sharing as needing two of three pieces to reconstitute a key. BitGo has one third. If they were hacked, the information is useless to the hackers because one-third of the key cannot reconstitute the entire key.

Week 3

1.
Question 1
The blockchain trilemma involves the trade off of: a) type of hashing algorithm; b) blocksize; and c) how frequently blocks are added.

1 / 1 point

True

False

Correct
The trilemma involves the trade offs of: a) decentralization; b) scalability; and c) security. For example, the more decentralized the slower the transactions per second.

2.
Question 2
Currently, the Ethereum blockchain is almost competitive with the centralized Visa network in terms of transactions per second.

1 / 1 point

True

False

Correct
Ethereum does about 15 TPS whereas Visa can do 65,000 TPS.

3.
Question 3

One drawback of Proof of Stake is that the rich get richer and the system can become more centralized.

1 / 1 point

True

False

Correct
One solution is to use delegated proof of stake. Here even small holders can pool together and delegate their stake to a super miner. They would participate in the rewards similar to the mechanics of today's mining pools.

4.

Question 4
An example of vertical scaling is when there is one centralized machine doing all of the transaction processing.

1 / 1 point

True

False

Correct
Chains like Solana and Algorand pursue and approach. PoW blockchains are much less efficient in terms of transaction processing. Solana can do about 50,000 TPS. However, there is a trade off. This architecture is more centralized and vulnerable to a single point of failure.

5.

Question 5
Horizontal scaling (or sharding) divides the work into multiple pieces (shards) and achieves efficiency through parallelization.

1 / 1 point

True

False

Correct
Ethereum 2.0 takes this approach with planning for 64 shards. There is a masterchain (called Beacon) that facilitates the cross-shard information flow.

6.

Question 6

The problem with Layer 2 technology is that gas fees are so high that transacting in Layer 2 is too expensive.

1 / 1 point

True

False

Correct

Layer 2 involves two on-chain transactions: the seeding of liquidity for a channel and the withdrawal of liquidity on that channel. After seeding the channel, an unlimited number of transactions can take place (with no gas fees) within the context of the multisignature wallet/channel. While this channel is off chain, it is secure. It allows for the possibility of every day transactions at minimal transactions costs

7.

Question 7

One problem with the multisignature wallet/channel is that once you supply liquidity, you need to trust that the other party will sign to allow you to repatriate your liquidity.

1 / 1 point

True

False

Correct

You can repatriate your funds at any time and you do not need the agreement of the other party. You cannot repatriate the other party's funds.

8.

Question 8

One flaw with the Layer 2 system is that each user needs to be connected to every other user creating the possibility that the user needs to manage hundreds if not thousands of payment channels.

0 / 1 point

True

False

Incorrect
There is a network effect. You just need to have a single connection to the network The system will then determine the most efficient throughput.

9.

Question 9
Optimistic Rollups provide little or no advantage because expensive gas fees need to be paid twice: once for the original transaction and second for the rolled up transactions.

1 / 1 point

True

False

Correct
Transactions are aggregated off-chain where there are no transaction fees. A hash of the transactions is then deployed to the Ethereum blockchain where gas fee is paid. However, if there are 1,000 transactions, there is only a single gas fee that is split 1,000 ways - greatly reducing costs and increasing throughput.

10.

Question 10
The Optimistic Rollups are flawed because you need to trust the aggregator.

0 / 1 point

True

False

Incorrect
The aggregator needs to escrow. If the aggregator misbehaves, the escrow will be used. This is the way that the system reduces the risk of a bad actor. So rollups without escrow are flawed but optimistic rollups include escrow.

Week 4

1.

Question 1
Major centralized exchanges like Coinbase are forced to comply with KYC and AML regulations whereas DEX has been granted an exemption.

1 / 1 point

True

False

Correct
It is just a matter of time before DEX will be subject to these regulations. However, the implementation is problematic because the DEX could just be an algorithm. How do you enforce anything? In addition, you can't shut the algorithm down. That said, regulation of DeFi is coming.

2.

Question 2
Some centralized exchanges employ geoblocks so that US persons are not allowed to trade obvious securities like tokenized stocks.

1 / 1 point

True

False

Correct
This is common for both decentralized exchanges (dYdX) and centralized exchanges (FTX). Certain tokens are clearly securities and as such need to adhere to the U.S. Securities Act.

3.

Question 3
DeFi governance tokens are immune to regulatory risk.

1 / 1 point

True

False

Correct
DeFi governance tokens are prime targets for regulators. During the lecture, we talked about Compound's approach where they airdropped their COMP token to try to get around "issuing" a security.

4.

Question 4
There are at least two types of digital asset "securities": a) tokens that represent traditional securities like stocks and bonds; and b) investment contracts.

1 / 1 point

True

False

Correct
The key gray area is the “investment contract”. It is obvious that a tokenized stock, like tokenized Tesla, is a security. The SEC has already decided that certain tokens are securities. However, there is not much guidance yet on DeFi.

5.

Question 5
There are four components to the famous Howey test for an investment contract: 1) investing money; 2) in a common enterprise; 3) with an expectation of profits; and 4) solely based on the efforts of the promoter or third party (i.e., based primarily on the managerial or entrepreneurial efforts of others).

1 / 1 point

True

False

Correct
The mission of the US SEC “... is to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation. The SEC strives to promote a market environment that is worthy of the public's trust”. If you are offering an investment contract, then you need to register with the SEC (which is a costly process) or apply for exemption. The SEC looks at manner of sale, promotional material and utility versus speculation.

6.

Question 6
If the token is designated a security by the SEC, if unregistered you cannot offer it to ANY US persons.

1 / 1 point

True

False

Correct
Regulation D allows for private placement to US persons. These need to be accredited investors. It is also possible via Regulation S to offer outside the US to non-US persons.

7.

Question 7

If regulations are too harsh, innovation is driven off shore.

1 / 1 point

- (•) True
- ( ) False

Correct

We talked about a balancing act. If regulation is too lenient, then people will be taken advantage of. If too harsh, you will squash innovation or drive innovators offshore. High quality regulators need to find the middle ground.

8.

Question 8

All current CBDC proposals involve using DeFi protocols whether on Ethereum or other decentralized chains that allow for smart contracting.

1 / 1 point

- ( ) True
- (•) False

Correct

There is very little “decentralized” in CBDC. The money supply is controlled by a central bank. The ledger technology is not permissionless.

9.

Question 9

In ALL CBDC proposals, the current commercial banks are disintermediated.

1 / 1 point

- ( ) True
- (•) False

Correct

In the direct CBDC model, everyone, whether bank or customers, deal directly with the CB. Think of having your checking account with the CB. You can argue that this leads to some disintermediation. There is a hybrid approach where customers deal with commercial banks and then the commercial banks deal with the CB.

10.

Question 10

The main advantage of the CBDC model is that it implements an algorithmic money supply rule meaning the end of inflation.

1 / 1 point

True

False

Correct

CBDC means that CBs have even more control over money supply. They can increase or decrease supply at will. They can enforce negative interest rates at their discretion. Currently, if rates are negative enough, no one will deposit money because it makes more sense to hold cash (which has a zero nominal interest rate) - the so-called “zero lower bound”.

11.

Question 11

CBDCs allow for the efficient collection of taxes.

1 / 1 point

True

False

Correct

Currently, people get around VATs or sales taxes by paying in cash currency. If cash does not exist and the government can see all transactions, then the tax is efficiently collected. This also applies to border adjustment taxes (which don’t make much sense without an efficient VAT.

12.

Question 12

DeFi is doomed because the Proof of Work mining is environmentally reckless.

1 / 1 point

True

False

Correct

Proof of Work plays a very important role. It is both a strength (security and trustlessness) and a weakness (carbon footprint). However, Ethereum is changing to Proof of Stake which is much more

environmentally friendly. Indeed, there are competitor DeFi blockchains that already implement Proof of Stake.

13.

Question 13

Both Bitcoin and Ethereum will migrate to Proof of Stake.

1 / 1 point

True

False

Correct

Ethereum will migrate. That has been in the works for a while. Bitcoin is extremely unlikely to change. Bitcoin's governance is very rigid and the miners have a lot of control. Miners don't usually hold a lot of bitcoin. Proof of Stake would effectively put them out of business.

14.

Question 14

The correct way to calculate the carbon cost of a bitcoin is to figure out how much power the bitcoin network uses in 10 minutes as well as the mix of different energy types, then divide by 6.25 bitcoin (new bitcoin produced in 10 minutes) and multiply the result by the cost of carbon (from carbon offset market).

1 / 1 point

True

False

Correct

This tells you the marginal cost of a new bitcoin. But bitcoins are fungible. The carbon cost of the first 10 million bitcoin were probably about 10 cents. There are 18 million bitcoin out there. Hence, you need to also consider the average cost. Further, even the new bitcoin gets traded. Hence, any carbon cost needs to be shared by all the holders. It is complicated.

15.

Question 15

DeFi doesn't really care about bitcoin and its environmental problems because DeFi will be based on Proof of Stake which is more carbon efficient.

1 / 1 point

True

False

Correct
Bitcoin is important to DeFi. Bitcoin is the largest capitalization cryptocurrency and wrapped versions of bitcoin are important for DeFi protocols.