1. What is cryptocurrency?

Cryptocurrency is a decentralized virtual currency built upon the infrastructure of cryptography, economics, and computer science. It is virtual currency that allows users to wireless exchange funds and facilitate transactions within a network of users without the need for a central financial authority.

1. Who created the first cryptocurrency?

Satoshi Nakamoto

1. What is Blockchain?

A method of storing data amongst multiple parties that ensures data integrity and authenticity. Data is collected into blocks where each block enforces the integrity of the previous block by having every block link with each other, forming a chain. This chain of blocks contains the full ledger of data and is secured by hashing and a consensus algorithm.

1. What are the four components of Bitcoin?

Identity Management

Transactions

Distributed Ledger

Trustless Consensus

1. Describe the process of Proof of Work - list all the steps and describe how each bitcoin is mined.

Transaction data is grouped up into blocks. These blocks store a list of transactions within the 10-minute time frame on average. This time frame is determined by the difficulty set for each block.

The block is distributed to a group of miners who will validate the transactions through mining. They will mine each block by brute force guessing a solution to the hash puzzle of the block. This process of guessing a nonce, hashing it, and checking for a match goes on until a valid hash matches the signature, proving that the block is legitimate. Once this block’s hash signature has been found, this block will be sent to the other miners working on the node. The other miners can easily confirm if the mining puzzle is valid which also proves if the transactions within that block are valid.

The majority will reach consensus to determine if that that particular block is a valid and add it to the blockchain. The miner who successfully mined the block will be allowed to mint a new set of bitcoins as the block reward and take the transaction fees from that block. The new block will include the hash of the previous block to link it with the blockchain, completing the mining process by adding a new block to the chain.

1. How long does it take to mine one bitcoin?

10 minutes on average. Mining difficulty is adjusted in order to accommodate this 10-minute average. However, issues such as network latency might affect the time to mine as well.

1. List 3 use cases of Blockchain in Financial Systems?

Trustless Consensus-As long as the majority agrees that a transaction is valid, then it will be considered valid.

Distributed Ledger-Blockchain allows all transactions to be made available to the public and immutable. This is because all transactions are linked together and stored by miners processing these transactions

Identity Management- Users can remain anonymous in a public blockchain by using addresses in lieu of their identities. This means that anyone can participate in a blockchain network without having to reveal anything about their revealing info in order to make a transaction.

Financial transactions-Any two parties can exchange cryptocurrencies of any kind in a trustless network. These two parties do not need to trust each other or reveal who they are to the other party. As long as a valid amount of currency is present in both wallets, anyone can trade cryptocurrencies between each other.

Payments-Used to facilitate virtual payments between two addresses. As long as both parties have a sufficient number of funds needed to transfer to each other, the payment will be satisfied.

Securities Settlement-The only requirement for payment is to have a sufficient amount of funds needed to transfer from one wallet to another. No other requirements are necessary.

1. Why is it called Blockchain?

All transactions are grouped up and recorded as a block. Each block is linked to the next one through their signatures in a hash. Every block is chronologically linked together to form a chain of blocks.

1. What are the three types of Blockchain?

Public-Any node can participate in the network and contribute to the ledger. It features complete decentralization and anonymity to its participants.

Private-Is a network where people can join only if they have an invitation or permission to join. After entering, they can participate in a decentralized manner. Control over the blockchain is usually held by one entity.

Consortium-Control over the blockchain is granted to a group of people. These chosen people have the power to allow others to participate in the network and have a greater degree of control over the blockchain.

1. What is the difference between Private and Public Blockchain? Describe one example.

Because private blockchains require permission to participate, private blockchains tend to be smaller, more efficient, and more centralized than a public blockchain. Private blockchains have to be centralized because there is one source of authority who determines who is allowed to participate in the network.

Private blockchains tend to be more efficient due not having to be as concerned with consensus or anonymity as a public blockchain has to be concerned with. Private blockchains usually assume that any person who joins the network has been deemed trustworthy by the central authority.

Private blockchains are smaller on the basis that not as many people can join the network due to the necessity of having to be allowed into the network compared to public blockchains where anybody can join and participate in the network.

1. What is a merkle tree and describe its role in bitcoin?

Merkle trees are a form of tree structure that contains the amalgamation of all related transactions of a subtree. Each pair of transactions are hashed together up until the final two nodes group up to form the root hash. The root hash serves as the representation of the entire subtree for the Merkle Tree.

Merkle Trees are the core component of how blockchain stores and validates data. This technology is how each block can be stored and distributed amongst a network while maintaining its immutability. Bitcoin uses Merkle Trees to store all transactional data and maintain the integrity of the blockchain.

1. What type of hardware is used by most miners?

ASIC-Specialized hardware designed specifically to compute hashes. These are the most efficient types of hardware to use for Bitcoin mining which is why most miners would opt to use ASICs.

1. Describe the 51% attack?

When one group of people has obtained atleast 51% of the world’s mining hash power for Bitcoins. They have majority control over the blockchain, and there is a major risk where the group might intentionally break the blockchain by using their hash power to create a hard fork of the blockchain. With 51% of the world’s hash power, they have majority rule to overwrite the blockchain which means they can edit the blockchain to the desires of the group’s interests.

1. What’s the difference between Hard Fork and Soft Fork? Give an example.

A soft fork features only minor changes to how blocks are managed. The changes are minor enough that there is still backwards compatibility with the previous blocks in the chain and do not require any changes from the nodes that handle the blocks. This only affects blocks made after the soft fork has been made, but not the previous blocks. Any other blocks made after the soft fork must conform to the standards of the soft fork.

Bitcoin had a soft fork that informed the network that the block size will be cut from 1 MB to 500 KB. All miners were able to use the same fork, but they had to confirm to the 500 KB standard to have their blocks validated.

A hard fork is a complete divergence from the previous block. There is no compatibility with the previous blocks nor any compatibility with any nodes that do not conform to the standards of the hard fork. All participants must change to the new standards to either participate in the hard fork or they must remain with the previous fork. There is no compatibility between the two forms nor the blocks from the hard fork and the previous chain.

One of the major mining groups used a hard fork to create Bitcoin Cash as an alternative to Bitcoins. Bitcoin Cash wanted to increase the size of their blocks to be larger than 1 MB which removed the compatibility between the two forks.

1. What are sidechains? Write about either Liquid or RSK.

Extensions alongside a blockchain which either adds extra functionality to the cryptocurrency or off-loads some of the work that the main chain performs, increasing efficiency and scalability. Sidechains work by essentially creating a second blockchain that will communicate with the main chain. While they communicate with each other, they remain independent of each other.

Liquid-A sidechain used to speed up and hide Bitcoin transactions. Liquid creates blocks in the span of one-minute which manage the transfer of cions between the main chain and Liquid’s side chain which allows the side chain to hide the exchange parties and speed up the transfer until it merges with the main chain.

RSK-Rootstock is a sidechain used to add Ethereum compatibility and features for Bitcoin. This means providing Ethereum’s virtual machine functionality attached to bitcoins. It uses merged mining to allow miners to enact the functions of smart contracts.

1. What are the main goals of Cryptography?

Data Privacy, Data Authenticity, Data integrity

Confidentiality-Only the sender and the receiver should see what they’re sending to each other. No other third parties should be able to read without authorization.

Data Integrity-Ensure the message was not tampered with during its transition from the sender to the receiver. Nobody should be able to change the message after it has been sent.

Authenticity-Both sides can verify their presence in the conversation while maintaining confidentiality. Both sides must prove that they’re the intended recipient and the intended sender before any exchange occurs.

1. What is the main difference between symmetric and asymmetric cryptography?

Symmetric cryptography uses a public key

Asymmetric Cryptography uses a public key to be distributed to other users and a secret private key for encryption and decryption.

1. Mention one symmetric or asymmetric cryptographic algorithm?

AES is a symmetric key algorithm

RSA is an asymmetric key algorithm.

1. What are digital signatures and their usage in blockchains?

Electronic signatures that use asymmetric cryptography to sign a message. This verifies that only the person with that particular private key is capable of signing that message, verifying the integrity of the message.

In Blockchain, digital signatures are used to handle the addresses. The public key is publicly displayed as a person’s address to show who has ownership of the wallet while the private key is used to access the access and manage the wallet address associated with the public key.

1. What does a block contain?

Transaction data regarding the list of cryptocurrency exchanges made between users.

The signature of the previous block to link multiple blocks together in a blockchain. Each signature is added to the next block and hashed to make each block immutable when added to the blockchain.

A nonce discovered from mining. A miner will brute force guess a nonce value and hash it to see if it yields a valid signature which matches the block’s data.

1. Write about one property of a hash function?

One-way-A hash should not be easily decrypted to find the original input.

Deterministic-One input should always yield the same output. This verifies the integrity of a message.

Collision-Resistant-Two inputs should not share the same hash output, otherwise the hash function is broken and can be reverse engineered.

Fast to compute-It needs to be fast enough so that it can be deemed practical for everyday use.

Pseudorandom-The calculation from a string to a hash should be as random as it could be to prevent someone from figuring out how to reverse engineer or force a hash collision.

1. What are smart contracts?

A pre-programmed application that auto-executes upon receiving enough gas and payment to conduct a transaction and execute itself. It essentially executes its code upon receiving the proper amount of Ethereum and records the output of its code and transaction as the proof of purchase.

1. What’s the type of Distributed Systems that Blockchain uses?

Peer-to-Peer

1. Write about one Consensus Algorithm. Describe it and also mention if it has scalability issues.

Proof of Work-The original consensus algorithm where miners must solve complex hash problems to find a nonce that fits the signature of a block. The block that has a valid solution of the longest chain is considered a valid block. This works because these hash problems require a large amount of processing power, and each block verifies the integrity of the previous block. This deters attackers because of the large number of processing power needed to launch an attack, but it leads to scalability issues because the large number of resources, processing power, and energy required to solve these hash problems. In addition, Bitcoin blockchains are too small, meaning as the network grows, more blocks have to be processed through mining. More transactions mean more mining required to process these transactions.

Proof of Stake-Minters must choose which fork of a blockchain to validate. The block is determined by the majority consensus, and votes are determined by how many tokens a minter is willing to bet. Ethereum's stake is the cost of entry. The relatively low cost of resources to become a stakeholder allows Proof of Stake to be potentially more scalable compared to its previous counterpart, but it has not been fully proven yet. It also requires manual input from its stakeholders which might be an issue for scalability in the future.

Proof of Weight-Users have a set number of tokens. These tokens determine the weight and probability of discovering the next block. Proof of Burn-A variant of Proof of Stake where stakeholders must burn their tokens to be granted access to write blocks based on the coins they burnt.

1. What is Ethereum and how does it work?

Ethereum was created as an alternative to Bitcoin with the main goal being that the currency and the nodes running the network should be programmable and autonomous. Ethereum is Turing-complete which allows participants of a network program their own method of handling transactions. The smart contracts generate an output which is recorded into the blockchain.

1. Talk about one scaling solution for Ethereum?

Ethereum is planning to transition from Proof of Work to Proof of Stake. By having minters stake and vote for the valid token, Proof of Stake eliminates the need for an excessive amount of computational power needed to validate and process a block of transactions in a blockchain. The reduction in computational power allows for more transactions to be processed at a potentially faster rate because minters do not require investing in hardware.

Minters only need to invest into their stakes to enter the market. At the same time, the security may be maintained because minters must pay a fee to be allowed to place their stakes, serving as protection against attackers.

1. Write about one difference between Ethereum and Bitcoin?

Ethereum’s layer works through an abstract virtual machine layer known as the EVM. This allows Smart Contracts to be Turing complete and more versatile for programming their functionality as this allows for opportunities such as layer 2 solutions using Sidechains.

Bitcoin is too simple to allow for specialized programming. Bitcoin can only use Ethereum’s Smart Contract capabilities by using a sidechain such as Rootstock.

1. Talk about one DeFi stack.

DeFi-The infrastructure used to design and manage currency and assets without the need for a centralized authority figure to oversee the system.

Stablecoins were a form of cryptocurrency that is tied to the price and value of physical money, allowing for virtual exchanges in a decentralized system while retaining the stability in terms of prices as compared to Bitcoins.

1. Write about one usage of Blockchains.

Shared Ledger-Allows for any number of entities collectively manage and agree upon how a shared database should modified. This collective management capabilities is what allows a network of anonymous users to share and use the same ledger of data without any disagreements on the integrity of the data.

Permissions-A private blockchain can be shared amongst a trusted number of users, providing a baseline level of trust amongst all participants

Cryptography-Encryption and addresses allows all participants to remain anonymous while participating in a blockchain network while at the same time, this allows members of a blockchain to interact with each other without the fear of being attacked due to consensus rule.]

Consensus-All transactions are checked for their integrity by majority rule. As long as the majority are trustworthy, then the blockchain will be trustworthy as well.

1. Write about one characteristic of NFTs.

Unique-NFTs all must be different form every other NFT.

Permanent-NFTs must be immutable. Once it’s stored in the blockchain, the core data contained in an NFT cannot be changed.

Programmable-NFTs are similar to file formats attached to a payload of data. This means they can be programmed as code onto the blockchain

Permissionless-Because NFTs will exist in public blockchains, they shouldn’t require a centralized authority to manage and distribute NFTs

Digital Ownership-NFT ownership is determined by whoever possesses the corresponding address for that NFT. Only that address is considered the owner of an NFT.

1. Write about one Layer one solution.

Consensus protocol changes-Changing the consensus protocol of Bitcoin away from Proof of Work. Proof of Work is extremely inefficient and unscalable, so many would change it to different forms of consensus protocols such as proof of stake. These other consensus algorithms aren’t as heavily proven to work, but these have the potential to process more transactions and exchanges without requiring as much mining power as proof of work does.

Sharding-Rather than have an entire network work on each block of data one at a time.

1. Name 3 use cases for stablecoins.

Allow for use of assets that have a stable value.

Allows two parties to do large scale transactions without requiring the oversight of a bank.

Stablecoins can serve as an intermediary form of currency between two parties that of two countries that use two different forms of physical currency. This allows two the two parties to exchange money internationally without the downtime that a direct payment would force.

1. What’s a scalability trilemma?

The issue with blockchains is that they need to balance among three priorities. Choosing to prioritize one feature may come at the risk of sacrificing one or two of the other priorities needed for an established blockchain.

Scalability-As the network grows, more transactions will take place in the network. This makes it much more difficult for cryptocurrencies like Bitcoin to process transactions due to the 10-minute time average needed to create a block. As more data is pushed onto a blockchain exponentially, it becomes increasingly more difficult for miners and stakers to look at, process, and validate every piece of data.

Decentralization-But block size cannot be changed to allow for more transactions because it creates a risk giving more power to those with better hardware resources which risks leading to more miner centralization and a higher risk of a 51% attack.

Security-It is difficult and risky to transition to another system without the risk of attackers taking advantage of a new system. There needs to be enough rewards to incentivize all parties to participate honestly while making sure the cost and resources needed to launch an attack on the network to too high for any one entity to initiate. Bitcoin’s scaling power makes it so that the cost to attack a network is equal to the cost to defend the network, meaning the majority will overpower the attackers. Scalability might run a risk of allowing an attacker’s power to grow.

1. Name two 2 layer projects and what’s the issue they are trying to solve.

Payment Channels-Creates a channel of nodes that handle and manage a majority of transactions for a set amount of time. Once the time period expires, the channel closes and the transactions recorded in this sidechain are merged with the main chain. This allows for much faster processing of transactions.

Sidechains-Another chain is established alongside the blockchain. The sidechain offloads some of the responsibilities of the main chain such as storing and processing transactions and provide additional functionalities that the main chain would normally not be able to do. Sidechains communicate with the main chain to take on some of the main chain’s workload, allowing the blockchain as a whole to work much more efficiently.

Rollups-Takes only the minimum amount of data necessary to be recorded as a transaction. The data actually added to the blockchain is used to reconstruct the block of data and check its integrity. This greatly reduces the workload on blockchain and speeds up the rate of transactions greatly.

1. What’s the difference between ZK-rollups and Optimistic-rollups?

ZK-rollups-A sidechain is created to offload transactions from off of the mainchain. The main chain will hold smart contracts which holds the transaction money. The smart contracts will process and validate the transactions of the sidechains through zero-knowledge proofs.

Optimistic rollups-Smart contracts relay between the sidechain and the main chain. Roll up contracts send transactions to the sidechain to be processed. After being processed by the sidechain, they’re taken back to the main chain and are marked as validated and executed.

The main difference between the rollups is that ZK-rollups use ECDSA to sign their transactions. Optimistic-Rollups aim to increase the transaction speed by changing the signature from ECDSA to BLS. ZK-Rollups also assumes legitimacy and checks using zero-knowledge proofs. Optimistic Rollups checks transactions for fraud.

1. Name one Layer 1 chains that is EVM compatible.

Avalanche, Polkadot, Cosmos

1. What is Leverage and Deleverage?

Because bitcoin’s value is volatile in the market, the potential earnings and rewards change for all people holding onto their bitcoins. This means that depending on the price of Bitcoins as time goes on, the potential rewards change as well.

Leverage is when people’s investments into Bitcoins increase the value on their returns. This happens when Bitcoin’s prices increases compared to the initial cost of investments, meaning that if a person traded their Bitcoins for money, they would make a return. This process is capital efficient.

Deleverage is the opposite where the price of Bitcoins drops below the initial cost of investments into Bitcoins. This means a loss in profits. In terms of Bitcoins, this usually occurs when the price of BTC crashes.

1. Write about your favorite blockchain project.

I find NFTs to be the most amusing project stemming from blockchain technology. For me, it doesn’t really seem to have much of a practical purpose outside of proof of digital ownership. There is no practical use for NFTs outside of trading for artwork online, yet there is an expanding market of people that just want to have the rights for specific files like images or videos. I like looking at NFTs because I mostly get to enjoy watching the absurd value people put into online files.

1. What is PolkaDOT?

A web3.0 project that aims to create a decentralized network by using independent blockchains as a means to relay information amongst its users. These blockchains will provide a means to communicate with each other allowing for independent ownership while maintaining cross-platform communication. This project also aims to allow users to communicate with each other and process online transactions without requiring trust by having these parties relay on independent blockchains of information as their source.

1. Your favorite token for trading?

I don’t trade. I don’t trust cryptocurrencies enough to participate in the market. The market is too volatile and unreliable in my opinion to trust at the moment, and I still don’t want to put my faith into stablecoins.