Cryptocurrency DA

Course code	:	BKT4006 –
Course Tittle	:	Cryptocurrency Technologies
Name	:	Rishabh Kumar Rai
Registration Number	:	20BKT0076

Q1) . How do bitcoin and it's blockchain actually work

The Bitcoin Blockchain

The Bitcoin blockchain is a database of transactions secured by encryption and validated by peers. Here's how it works. The blockchain is not stored in one place; it is distributed across multiple computers and systems within the network. These systems are called nodes. Every node has a copy of the blockchain, and every copy is updated whenever there is a validated change to the blockchain.

The blockchain consists of blocks, which store data about transactions, previous blocks, addresses, and the code that executes the transactions and runs the blockchain. So, to understand the blockchain, it's important first to understand blocks.

Blocks

When a block on the blockchain is opened, the blockchain creates the block hash, a 256-bit number that encodes the following information:

- The block version: the Bitcoin client version
- The previous block's hash: the hash of the block before the current one
- The coinbase transaction: the first transaction in the block, issuing the bitcoin reward
- The block height number: how far away numerically the block is from the first block
- Merkelroot: A 256-bit number that stores the information about all previous blocks
- Timestamp: the time and date the block was opened
- The target in bits: the network target
- The nonce: a randomly-generated 32-bit number

Queued transactions are entered into the block, the block is closed, and the blockchain creates the hash. Each block contains information from the previous blocks, so the blockchain cannot be altered because each block is "chained" to the one before it. Blocks are validated and opened by a process called mining.

Bitcoin Mining

Mining is the process of validating transactions and creating a new block on the blockchain. Mining is conducted by software applications that run on computers or machines designed specifically for mining called Application Specific Integrated Circuits.

The hash is the focus of the mining programs and machines. They are working to generate a number that matches the block hash. The programs randomly generate a hash and try to match the block hash, using the nonce as the variable number,

increasing it every time a guess is made. The number of hashes a miner can produce per second is its hash rate.

Mining programs across the network generate hashes. The miners compete to see which one will solve the hash first—the one that does receives the bitcoin reward, a new block is created, and the process repeats for the next group of transactions.

Bitcoin's protocol will require a longer string of zeroes depending on the number of miners, adjusting the difficulty to hit a rate of one new block every 10 minutes. The difficulty—or the average number of tries it takes to verify the hash—has been increasing since Bitcoin was introduced, reaching tens of trillions of average attempts to solve the hash.1 As this suggests, it has become significantly more difficult to mine Bitcoin since the cryptocurrency launched.

Mining is intensive, requiring big, expensive rigs and a lot of electricity to power them. And it's competitive. There's no telling what nonce will work, so the goal is to plow through them as quickly as possible with as many machines working on the hash as possible to get the reward. This is why mining farms and mining pools were created.

Halving

Halving is an important concept in Bitcoin mining. At first, the mining reward was 50 BTC for solving the hash. About every four years, or 210,000 blocks, the reward is cut in half. So, rewards were cut to 25 in 2012, 12.5 in 2016, and 6.25 in 2020. The next halving is expected to occur in 2024 when the reward will reduce to 3.125, followed by a reduction to 1.5625 around 2028.

The last bitcoin is expected to be mined somewhere around 2140. All 21 million bitcoins will have been mined at that time, and miners will depend solely on fees to maintain the network.

Keys and Wallets

A common question from those new to Bitcoin is, "I've purchased a bitcoin, now where is it?" The easiest way to understand this is to think about the Bitcoin blockchain as a community bank that stores everyone's funds. You view your balance using a wallet, which is like your bank's mobile application. If you're like many people today, you don't use cash very often and never see the money in your checking account. Instead, you use credit and debit cards, which act as tools to access and use your money. You access your bitcoin using a wallet and keys.

Keys

A bitcoin at its core is data with ownership assigned. Data ownership is transferred when transactions are made, much like using your debit card to transfer money to an

online retailer. You use your wallet, the mobile application, to send or receive bitcoin.

When bitcoin is assigned to an owner via a transaction on the blockchain, that owner receives a number, their private key. Your wallet has a public address—called your public key—that is used when someone sends you a bitcoin, similar to the way they enter your email address in an email.

You can think of the public and private keys like a username (public key) and password (private key) used to access your funds.

Wallets

A wallet is a software application used to view your balance and send or receive bitcoin. The wallet interfaces with the blockchain network and locates your bitcoin for you. The blockchain is a ledger with portions of bitcoin stored on it. Because bitcoin is data inputs and outputs, they are scattered all over the blockchain in pieces because they have been used in previous transactions. Your wallet application finds them all, totals the amount, and displays it.

There are two types of wallets, custodial and noncustodial. A custodial wallet is one where a trusted entity, like an exchange, holds your keys for you. For example, when you sign up for a Coinbase exchange account, you can elect to have them store your keys for you as custodians.

Noncustodial wallets are wallets where the user takes responsibility for securing the keys, such as in your wallet application on your mobile phone. Storing keys in an application connected to the internet is referred to as hot storage. However, hot storage is the vulnerability most often exploited.

You should always use a reputable wallet provider, like from a registered cryptocurrency exchange. Read reviews and research wallets to ensure you're choosing one that is reliable.

To remedy this, the cryptocurrency community has developed methods for storing your keys offline. Most commonly, you'll hear about hot storage, cold storage, and deep cold storage. Hot storage is any wallet that stores your keys and has an active connection to the internet—this is the most vulnerable method. An example of a hot wallet is the wallet application on your mobile device.

Cold storage is any method that is not connected to the internet. This could be a removable USB drive or a piece of paper with your keys written on it (this is called a paper wallet). Deep cold storage is any cold storage method that is secured somewhere that requires additional steps to access the keys beyond removing the

USB drive from your desk drawer and plugging it in. Examples might be a personal safe or storage deposit box—anything that takes extra effort to retrieve your keys.

Bitcoin Transactions

A bitcoin transaction happens when you send or receive a bitcoin. To send a coin, you enter the receiver's address in your wallet application, enter your private key, and agree to the transaction fee. Then, press whichever button corresponds to 'send.' The receiver must wait for the transaction to be verified by the mining network, which can take up to 30 minutes because transactions wait in a mining queue called the mempool.2

(Minutes, 7-day average)
The mempool is where transactions waiting to be verified go. The network, on average, confirms a block of transactions about every ten minutes, but not all new transactions go into the new block that is created. This is because blocks only hold a certain amount of information, and each transaction comes with a mining fee.

Transactions must meet the minimum transaction fee threshold to be processed, and the transactions with the highest fees are processed first. This is why you may hear about the problem of rising fees—Bitcoin is so popular that demand for transactions has increased, allowing (or requiring) miners to charge higher fees.

Transaction fees were established to create an incentive for people to become network nodes and miners. Bitcoin mining is also expensive, so fees help to offset the cost of equipment and electricity used.
Once the fee is met, the transaction is transferred to a block, where it is processed. Once transaction information within the block is validated by miners, the block is closed, and all receivers collect their bitcoin. Both wallets display their appropriate balances, and the next transactions are processed.

Bitcoin Security

There are many parts that make up the Bitcoin blockchain and network, but it is not necessary to understand it all to use this new currency technology. You only need to know that you use a wallet to send, receive, and store your bitcoin keys; you also should use a cold storage method for security because non-custodial wallets can be hacked.

Custodial wallets can also be hacked, but many who offer this service take measures to reduce the chances that hackers can get into the storage systems. Most are turning to enterprise-level cold storage techniques businesses use to store essential data for extended timeframes.

For good reason, many people are concerned about Bitcoin's level of security, especially since it involves exchanging money for encrypted data ownership. However, it's important to note that the Bitcoin blockchain has never been hacked

because of the community consensus mechanisms used. Wallets are the weak spot, so if you're looking to get involved in Bitcoin, it's essential to understand how to utilize cold storage methods and keep your keys out of your hot wallet.

Q2) How secure and anonymous are Bitcoins?

Security:

It’s protected by the 256-bit SHA hash functions, the same level of security that banks, the military, and virtual private networks (VPNs) use to encrypt their systems. But unlike encryption, which can be decrypted, SHA hash functions provide a unique fingerprint for each transaction that cannot be reconstructed.
In other words, cryptography in blockchains is used to sign the data with a **unique, unbreakable identifier** that other network participants can verify using the same cryptographic algorithm.
The blockchain also builds security by consensus. For it to be hacked, someone would need to take over 51% of Bitcoin mining capabilities, which would be incredibly unlikely. However, your cryptocurrency wallet isn’t necessarily secure — and that’s where you’d store your bitcoin.
The cryptographic system makes transactions irreversible — in other words, a block once created on the chain cannot be modified. However, you can add information to it. This restricts people from being able to reverse any transaction that has already taken place.

The Bitcoin blockchain is public. While the words transparency and public do not sound safe, in the case of Bitcoin it is. Despite the anonymity of the user, all transactions on the network are accessible to the public, making it difficult to hack or cheat the system.

It is decentralised. The Bitcoin network is distributed and has thousands of nodes all over the world that keep track of all transactions happening on the system. This ensures that in case something goes wrong on one server, there are others to pick up the slack. Hacking into any one server is pointless.

This is not to say that it is foolproof or impossible to hack — but it certainly isn't easy either. With Bitcoin and other cryptocurrencies, you're more likely to suffer losses

from bad investing, or be tricked into giving up your coins, than to have them hacked away from you.

Anonymous

cryptocurrency is entirely anonymous. On the other, it is completely transparent and trackable.

It is anonymous in the sense that you can hold a crypto address without revealing anything about your identity in that address. One person could hold multiple addresses, and in theory, there would be nothing to link those addresses together, or to indicate that the person owned them.

Sending and receiving virtual currency is like writing under a pseudonym. If an author’s pseudonym is ever linked to their identity, everything they ever wrote under that pseudonym will be linked to them.

In the original Bitcoin whitepaper, it was actually recommended that users use a new address for each transaction, to avoid them being linked to a common owner.

Q3) Can Cryptocurrency be regulated?

Regulating bitcoin is possible. In fact, the fiat onramps and tight KYC and AML regulations have already begun to regulate it. Although other nations have outright outlawed cryptocurrencies, it would take a serious breach of the Constitution's moral principles for bitcoin ownership rights to be violated in the US.

The problem with regulating Bitcoin and other currencies is that they’re conducted over a P2P network. While governments have been successful in regulating venues, such as the Pirate Bay and Silk Road, there are so many cryptocurrencies. The main difference with cryptocurrencies is that transactions can be conducted over exchanges or through direct transactions using your cryptocurrency wallet.

Yet, this doesn’t mean the government is completely helpless against cryptocurrency regulations, or are they?

Ways the Government Can 'Crack Down' on Cryptos

The number one way that the government could regulate cryptocurrencies is by taxing any fiat money you use to cash out a virtual token. The main caveat with this is that this would have to apply to specific tokens and a cryptocurrency owner could simply turn to another coin to cash out. Beyond this, many early adopters and hardliners prefer cryptocurrencies as medium of exchange for basic goods and services over traditional fiat currencies.

Right now, cryptocurrencies fall under the jurisdiction of the SEC for investment, the CTFC for any crimes involving interstate commerce, and the IRS, making it subject to either income or a capital gains tax.

The SEC recently approved one Bitcoin futures ETF over the CBOE and one over the CME. No other futures ETFs have been issued at this time, although many applications have been submitted.

The most regulatory kraut the SEC currently holds in the crypto space is over ICOs. It recently halted an ICO after it was found to be conducting fraudulent transactions.

On the same note, the CTFC recently subpoenaed major crypto exchanges Bitfinex and Tether because Tether couldn't verify over $2.3 billion in reserves. This caused Bitcoin prices to momentarily fall by 10%.

Much of the proposed regulations being mulled around the world comes on the fears of a dangerous speculative bubble that many fear could harm the nation if cryptocurrency commodities tumble.