Unit 4

CHAPTER 4

Cryptocurrency - Bitcoin and Token

University Prescribed Syllabus

Introduction, Bitcoin and the Cryptocurrency, Cryptocurrency Basics Types of Cryptocurrency, Cryptocurrency Usage, Cryptowallets: Metamask, Coinbase, Binance.

4.1 INTRODUCTION TO CRYPTOCURRENCY

GQ. What is Cryptocurrency ? Explain in brief.

- Cryptocurrency is a kind of digital asset that enables safe transactions using distributed ledger, or blockchain, technology.
- Despite the widespread misunderstanding of the technology, several central banks are considering introducing their own domestic cryptocurrency.
- Since 1998, the concept of "cryptocurrencies" has been discussed.
- B-Money and Bit Gold were the first known attempts to create a digital cryptocurrency, but neither proved successful.
- Digital or virtual currencies that operate on cryptographic principles are known as cryptocurrencies.
- As implied by the name, they are not substantial or have no actual presence.

- They are essentially a collection of computer programming codes,but offers greater usefulness and security than many current currencies.
- Blockchain technology, which we have previously studied in earlier chapters, is the foundation of cryptocurrency.
- In the case of cryptocurrencies, the ledger records all transactions made and created using those currencies on the network. Each user on a certain blockchain will have a distinct account Id or address. Currency is Debited and Credited to this account.
- These accounts are constantly connected to the cryptocurrency.
- Wallets, an application, allows users to manage their accounts.
- Both the sender and the recipient need to have accounts. Anyone on the network may transact with anyone else using their wallets.
- Nodes verify the transactions, which are then recorded on the blockchain ledger. Therefore, the unchangeable and encrypted blockchain record serves as the foundation of bitcoin.
- The encryption system, peer-to-peer network, and lack of a central authority or central server to govern are other important characteristics of blockchain that are also relevant to cryptocurrencies.
- Each cryptocurrency will use a blockchain system to operate.
- Bitcoin, which uses the bitcoin blockchain, is one of the most well-known cryptocurrencies.
- Another cryptocurrency that is quickly expanding and uses the Ethereum protocol is ether.
- In compare to conventional currencies, cryptocurrencies provide participants a very high level of anonymity.
- A user's account ID will be the only part of his identification that may be seen; everything else will be encrypted.The true identify of a user will not be known to the participants.
- There are various benefits and drawbacks to cryptocurrencies.
- The current cryptocurrency market is highly competitive and fragmented. Experts identifiedmore factors that will determinate and rise the attractiveness and confidence in using cryptocurrency.

- The cryptocurrencies should be:
  (1) Cost effective to issue
  (2) Available immediately
  (3) Governed and regulated
  (4) Instantly liquid—liquidity should be instantly generated or generated
  (5) on demand
  (6) Secure and immutable—cannot be double spent
  (7) Trusted—backed by a lender of last resort (e.g. a central bank)
  (8) Free from fractional reserve banking in its crypto-form
  (9) Transparent with transaction finality (directly or remotely)
  (10) Add purpose to economic activity (commerce) and have sustainable value
  (11) Have standards to enable interoperability
  (12) Be legitimate—a competent authority to impose these standards

4.2 BENEFITS OF CRYPTOCURRENCY

GQ. State and explain the advantages of cryptocurrency.

(1) Compared to current banking systems, cryptocurrencies allow extremely quick transactions. A transaction may be validated in Bitcoin in as little as 10 minutes, while it takes Ethereum roughly 10 seconds.

(2) Transactions performed using cryptocurrencies are completely anonymous; neither the person who made the transaction nor the recipient can be determined. Only the sender's and receiver's network addresses will be used by the participants. These participants' identities won't be made public on the shared ledger.

(3) There are no payment restrictions. Transactions are not subject to any limitations. The user is able to send money at any moment, from any location to any location. No time restrictions, such as bank holidays, apply.

(4) The majority of bitcoin transactions are free. Or the fee is significantly lower than the current fees for banking transactions. Anyone may conduct transactions in bitcoin without having to pay any transaction fees. In order to expedite their transaction, the user may also choose to charge transaction fees. In other words, if someone pays a transaction fee, more miners will arrive to validate the transaction, which speeds up the process.

(5) Cryptocurrencies are among the safest payment methods on the market right now. It possesses the "unchanging" quality, which means that if a blockchain-based cryptocurrency transaction has already taken place, it cannot be undone. Therefore, the likelihood of fraudulent transactions is quite low.

(6) Most cryptocurrencies operate on a decentralised network, and their exchange rates are dynamically determined by supply and demand variables. Such autonomous cryptocurrencies cannot be stopped by by government law or other means. A government's sole option is to limit the currency's ability to be converted into regular money. They are unable to halt cryptocurrency transactions, though.

(7) Transactions using cryptocurrencies do not require the use of a user's identify. All additional information is securely scrambled and will only be used to access the wallet addresses of the sender and recipient. No personal information will be given to the recipient of a cryptocurrency when it is sent to another person or organisation. Between two accounts, just the sum of bitcoin will be transferred.

(8) Most cryptocurrencies have a set quantity of currency in their exchequer, hence there is no inflation. It is 21 million in the case of bitcoin. There won't be any fresh bitcoins after the entire item has been mined. Therefore, depreciation is not a possibility.

(9) Immediate asset availability - the cryptocurrency will be available immediately for consumersand businesses to spend, without any waiting period.

(10) Immediate access to liquidity - the cryptocurrency will be highly liquid-liquidity generatedinstantly on demand.

(11) Free up working capital - the need for banks to hold reserves will be minimized as themoney held for use as reserves will be available for other purposes thus optimizing intradayliquidity.

(12) Transaction efficiency - cryptocurrency transactions are fast and immediate-they improve efficiency by cutting out the middle man and avoiding lengthy back-office reconciliation processes.

(13) Transaction security - central bank-issued cryptocurrency transactions can be tracked protecting security. Security is also enhanced as there is no double spending.

(14) Over and above these benefits, a central bank-issued cryptocurrency can have a much larger impact on the wider economy and for all market participants because it can :

(15) Boost economic growth-a central bank issued cryptocurrency can permanently boost economic growth.

(16) Act as an enabler for mobile and digital commerce-it can replace current immediate payment models by delivering the currency into the market in a more immediate, efficient and effective manner.

(17) Ensure stability in the financial system-a cryptocurrency can help maintain financial stability and provide policy makers with more effective tools to smooth out financial booms and busts. In periods of high inflation for fiat currencies, banks can hold cryptocurrencies, thus protecting their wealth.

(18) Work as a crypto-reserve currency-commercial banks can keep a portion of their reserves in cryptocurrency rather than in fiat currency, thus complementing the fractional reservebanking system.

(19) Effectively monitor the supply of money-a central bank issued cryptocurrency can help policy makers control the amount of money in the economy, as well as the supply of the cryptocurrency. This is currently not possible as banks create money by using deposits as loans.

(20) Lower costs-crypto currencies will enable the banking system to cut the costs of banknote issuance, circulation and handling. In addition, transaction costs will be significantly reduced especially for cross border transactions.

(21)Allow for traceability-transactions in central bank issued cryptocurrencies can be tracked, and simultaneously ensure that the users information remains protected, thus protecting privacy. A central bank issued currency follows KYB and KYC procedures which will allow the central bank to identify users when there is a need to.

4.3 DRAWBACKS OF CRYPTOCURRENCY

GQ. State and explain the disadvantages of cryptocurrency.

(1) Despite the fact that demand for "cryptocurrency" is rapidly rising, several governments have not officially endorsed transactions involving "cryptocurrency." And currently, only a few select domains are allowed to use it. Additionally, the general public is still a long way from adopting "cryptocurrencies."

(2) Variable rate might be viewed as either a benefit or a drawback. Although the exchange rate of cryptocurrencies is determined by a rigorous demand-supply law, current market patterns point to an unusual increase in that rate, particularly for Bitcoin. However, it is anticipated to return to its regular speed very shortly.

(3) Governments cannot regulate cryptocurrencies, but they may ban them and make transactions involving them unlawful. It inevitably cast a shadow on such bold, unrestrained gestures.

(4) Money launderers and the black market are drawn to cryptocurrencies because of their anonymity. Misuses are repeatedly reported since the identity is kept a secret. Undoubtedly, the potential of cryptocurrencies may be utilised to create a more transparent economic system, but before making such significant advancements, security concerns and loopholes must be addressed. We may anticipate a fully authorised cryptocurrency-based economic system in the near future since a prospective technology like this cannot be completely prevented.

(5) As the majority of cryptocurrencies lack a centralised administration, it is everyone's responsibility to keep their

account secure. Nobody can assist whomever loses the wallet key in obtaining it again.

(6) Since there are often only a finite quantity of cryptocurrencies, the supply and demand essentially determines how much they are worth. Deflation is more likely to occur in cryptocurrencies than in any other type of economic system since most of them only have a set number of units.In the case of bitcoin, if someone retains the cryptocurrency for a long period, the supply will decline while the demand rises, which would result in deflation.

4.4 INTRODUCTION TO BITCOIN

GQ. What is Bitcoin? Describe how it works.

- The first blockchain implementation in the world and the first cryptocurrency is Bitcoin.
- We have covered the definition of cryptocurrency. Let's get a bit more into the subject with the most well-known cryptocurrency, Bitcoin, in this part.
- Satoshi Nakamoto created bitcoin in 2009 using the conceptual framework proposed by certain scholars in the late 1990s.
- It does have a P2P shared network, distributed ledgers, and data that is cryptographically secured, exactly like a traditional blockchain.

4.4.1 Working of Bitcoin

- Using Bitcoin is easy; we do not need any programming expertise or technological understanding.
- The first step is to register for a Bitcoin blockchain account.
- To do that, making a digital wallet is the most straightforward method.
- Numerous wallet service providers exist, including Coinbase and BitCore.
- In order to create an account, the user must supply a "Key" that is similar to a password.

- The wallet will create a legal bitcoin private key-public key pair using this key.
- The user's visible account ID is the public key, which is accessible to everyone.
- In contrast, the user maintains the private key, which serves as his account access key, to himself.
- If someone misplaces their private key, they are unable to access their accounts and money.

4.4.2 Buy Bitcoin

- Purchasing Bitcoin via a bitcoin exchange is the simplest method to get them.
- Several online bitcoin exchanges let users convert fiat money to bitcoin.
- People may convert their regular money into bitcoin and transfer it to their wallet.
- Participation in bitcoin mining is another way to obtain bitcoin.

4.4.3 Transactions

- A transaction is when you send bitcoin from one account to another. The primary method is through wallets.
- The wallet app will have a screen where we can enter the recipient's account ID and the amount we want to send.
- The transaction will be verified by the miners when we have completed it, and if it is valid, it will be added to the blockchain record.
- Transactions with Bitcoin are free of charge. Bitcoin transaction confirmation typically takes ten minutes, however it may be sped up by paying a tiny transaction fee.

4.4.4 Bitcoin Mining

- The most significant and fascinating aspect of bitcoin is its mining.
- This is the procedure used to verify and add new transactions

to the claimed "blockchain."

- Because of the need for specialized mining hardware, not all nodes participate in mining.
- The nodes involved in the mining process are referred to as "miners.".
- Any time a new bitcoin transaction occurs in the network and is broadcast to all users.
- The miners take in this transmission when verifying transactions.
- The transactions are added to a block when they have been confirmed.
- For miners, to determine a hash value for the fresh block is the main task.
- The block reward, which is a certain number of bitcoins, is given to the miner who discovers the hash value first.
- Finding the hash value is not difficult. Each node has that ability. In order to encourage competition among the nodes, a difficulty level is attached to it. The amount of difficulty indicates how challenging it is to locate the hash.
- Difficulty level shrinks the set of hash values that a block can have. Since the hash length is 256 bits, it can have any value from the enormous range of 2^256 possible values, regardless of difficulty level.
- The target is significantly reduced by adding a level of difficulty.
- The miner must locate a hash value that begins with a specific number of zeroes since the difficulty level is expressed in terms of the number of zeroes.
- The nodes keep looking for new hash values and determine if they meet the required level of difficulty.
- Because a block's contents never changes, its hash also never changes. Consequently, the only way to experiment with alternative hash values is to associate a nonce with the block's content. The nonce is an arbitrary string of 32-bit length. i.e. H(block + nonce). Because the target set is so limited, there is a lower chance of success.

- The matching hash is calculated each time the miners use brute force to change the nonce.
- Because the miners must test out several permutations of "Nonce," this is the true game, and node computing power is crucial.
- The node with specialized hardware and high processing power has a better chance of succeeding in this game and receiving the block reward.
- The block and nonce will be announced by the first person to find hash. When they get this, other miners halt their work and check to see if the received hash meets the required degree of difficulty. If so, the nodes demonstrate their approval by including it in the blockchain.

4.4.5 The value of Bitcoin

- There is a claim that Bitcoin is worthless, because it answers no real need and solves no real problem. This claim can easily be refuted.
- Bitcoin is a global, decentralized, highly liquid, and pseudo-anonymous asset. Therefore, in any transaction, which requires all these properties, the benefits of using Bitcoin over other currencies are clear. Moreover, that is exactly the reason that most people do not appreciate these properties.
- First, most people are unaware of the damage caused by centralized monetary systems.
- Second, only rarely do they perform international financial transactions in large volumes. Third, most people are against anonymous transactions.
- However, the benefits of Bitcoin are widely recognized in the following cases :
  - (i) Where the centralized monetary system completely collapses.
  - (ii) Where the government confiscates its own citizen's assets.
  - (iii) Among populations, which are excluded from the financial and banking systems.
  - (iv) Among out casted populations.
  - (v) Among people who are keener on their privacy.
  - (vi) Among frequent travelers/flyers.

4.5 DIGITAL TOKENS

GQ. What are digital tokens?

- Digital tokens, simply known as "Tokens," are another market-shaking blockchain-based technology that is trending.
- Tokens are a digital asset that are developed on top of cryptocurrencies of a blockchain network. They are a minor variation of cryptocurrencies.
- The token may be used for a variety of things, including granting rights, paying for services, transferring data, offering incentives, getting access to further services, and many more.
- To put it another way, a token can be utilized anyway the developer or creating company sees fit.
- The tokens are a digital asset that is less liquid than a cryptocurrency and will never be utilised as one. Therefore, the value of every token that is produced will likewise be specified.
- The tokens may be refundable under specific circumstances, allowing us to trade them for cryptocurrencies.
- Wallets are used to maintain tokens, just like they are with cryptocurrencies.
- Most tokens are now produced on the Ethereum network. It is easy to create tokens using the Ethereum network. The establishment of a smart contract is all that is required to create a token in Ethereum.
- All that is required to create the tokens is the addition of the essential codes to the structure. When the token is finished, the Ethereum network can use it.

4.6 TYPES OF CRYPTOCURRENCIES

GQ. State and explain different types of cryptocurrencies.

- Despite the fact that Bitcoin was the first cryptocurrency in use by the general public, there are many different types of cryptocurrencies.

- Depending on its formulation or code design, application or use case, and other characteristics, we may classify cryptocurrencies into different types.
- You might get coins, payment tokens or altcoins, security tokens, non-fungible tokens or NFTs, decentralized finance tokens, utility tokens, and other categories.
- Coins are frequently used interchangeably with cryptocurrencies, despite the concept being used to describe all different kinds of cryptocurrencies or digital currencies.
- Even while many of them do not function as a unit of account, a store of value, or a medium of exchange-Bitcoin does-they are widely perceived as such.
- Coins, however, may be distinguished from altcoins. In addition to Bitcoin, all other cryptocurrencies that are viewed as alternatives to Bitcoin are referred to as altcoins.

(1) **Coins :** As coins are based on their blockchain, they may be distinguished from altcoins. Bitcoin on the Bitcoin blockchain and Ether, or ETH, on the Ethereum blockchain are two good examples. Building or creating a cryptocurrency begins with or follows the creation of a blockchain.

(2) **Altcoins :** They are viewed as alternatives to Bitcoin, the original cryptocurrency, even if they may all be considered coins. Also known as shitcoins, apart from Ethereum, most of the first ones were forked from Bitcoin. These include Namecoin, Peercoin, Litecoin, Dogecoin, and Auroracoin.

3) **Tokens :** In a blockchain, tokens serve as digital representations of specific assets or utilities.Tokens are essential to getting a true grip on cryptocurrencies. They're the amount of digital resources you control on a given platform. As mentioned before, a digital wallet stores them and accessed with a key, which can be reassigned to someone else. Two types of tokens exist. First, is a native token. This type of token has an intrinsic utility. It forms the core part of a blockchain. That is to say, a blockchain could not run without a native token. Often times, they're used as an incentive to validate transactions, or create blocks.Be careful that tokens and coins have different properties. The majority of people frequently use them interchangeably, yet this is incorrect.

(4) **Bitcoin :** The king of the castle. Created in 2008, it housed the original code for blockchain technology. Its creation spurred many other cryptocurrencies. It's easily the most trusted and known virtual currency on the market, even if it has its flaws.

(5) **Ethereum :** Probably the second most well-known cryptocurrency. It allows users to do more than just use it as a virtual currency. It's an open-source blockchain. Money and assets are quickly transferred with the use of smart contracts. Assets include houses, cars, stocks, and other property owned with real-world value.

(6) **Litecoin :** One of the first cryptocurrencies to emerge after Bitcoin's initial release. It has a much shorter processing time-about 2.5 minutes-than Bitcoin's crazy 10-minute timeframe. Litecoin provides more tokens and a different mining algorithm, but it ultimately didn't take off the same way its big brother did.

(7) **Ripple :** Because every single token was mined before its release, it is quite possibly the most despised cryptocurrency by the community. This action is known as pre-mining and is a huge no-no. Essentially, this takes away the community aspect of virtual currencies. It attempts to take a decentralized platform and centralize it.

(8) **Monero :** Solved many of Bitcoin's privacy issues. It adds an additional level on anonymity to transactions. A few darknet markets (networks that require specific software or authorization to access them) started accepting the cryptocurrency in 2016, where it ultimately reached its peak.

4.7 CRYPTOWALLETS

- People dealing with cryptocurrency use a wallet as a safe depository and an instrument for incoming and outgoing payments. Let's analyze the available types of wallets and choose the most suitable one based on your computer's resources and tasks.
- There are hot and cold wallets. There are also warm wallets, but they are used much less often.
- Cold wallets are used to store money, while hot wallets are used to send and receive the currency quickly.

- As a rule, a wallet has a Private key and a Public key. The Private key belongs only to you, and you should never show it to anyone.
- You must keep it in mind as you sign all transactions with this key. At the same time, someone can use public keys to transfer money to your account.

4.8 METAMASK

GQ. Write a short note on: MetaMask.

- MetaMask is a web browser add-on which enables anyone to run the Ethereum DApps without running the Ethereum full node. An Ethereum full node installation
- will take a lot of memory as well as time; so Metamask is a tool that eliminates the overburden of this hectic installation task. Initially, Metamask was available only for Google Chrome, but now it is available for Firefox and other popular web browsers.
- MetaMask add-on for chrome can be added from chrome web store or from 'metamask.io' website. This MetaMask add-on provides a user interface for interacting with the blockchain.
- The user can connect to the Ethereum main network or 'test net' or he may create his own private network and run DApps on the blockchain.
- In normal case, a web3.js (the JavaScript API for Ethereum DApps) must be installed in the local system to interact with the Ethereum DApps. Web3.js is a collection of libraries used to interact with local or remote Ethereum node using Http or IPC connection. But MetaMask will inject the web3.js to each page for accessing the Ethereum blockchain by itself. This approach eliminates the effort of web3.js installation in the local system.
- After adding the Metamask, the user can interact with Ethereum blockchain as normal. The user can create an account, access Ethereum DApps, or deploy once own DApp. MetaMask retrieves data from the blockchain and allows the users to manage the data securely.

- The Metamask provides a vault account for each user, this vault secures, stores and tightly controls access to tokens, password, certificates, API keys and otherelements in blockchain apps. The vault account act as a second level encryption for the user account.

Wallet Seed

- The Metamask will provide a group of 12 words known as "wallet seed" while installing it. It is the user credential and it must be stored somewhere safe.
- The users can also create passwords for their account. The wallet seed or the password is necessary to log in to the MetaMask.
- The vault account willencrypt the user metadata and securely store it in the browser itself.

MetaMask Transactions

- The Metamask user interface has a default buy and send option for buying and sending Ether. The user can access his wallet, buy or send ether, check his balance and transactions from this interface.
- When the user executes a transaction from the Metamask it will send the transaction to the respective blockchain network.
- Then the corresponding validation and confirmation will occur in the blockchain as usual. In the case of 'testnet' and main network, the user can see the transaction details and confirmations in the 'Etherscan.io'.
- Example of a transaction of Ether through Metamask:For sending Ether to an account you have to specify the recipient address and the amount to be transferred in the provided interface.
- Before linking your transactions to the blockchain, the web3.js will ask yourpermission and the transaction will be submitted only after your approval.
- Once the user submits the transaction, it will be sent to the blockchain for validation. The transactions will be broadcasted to the nodes and once the validation is completed you can see the transaction details in the ether scan window. The window will display all the information regarding that transaction i.e.; block number, hash value, sender and recipient address,

number of confirmations, gas units, transaction cost, nonce etc.

- GNOSIS, Maker(MKR), Token Factory, CryptoKitties etc. are some DApps that supports Metamask. Any developer can submit DApp in Ethereum with Metamask support so that the user doesn't need to install the full Ethereum node for accessing the particular app. The Metamask is the very useful tool for accessing Ethereum in low bandwidth networks. Let's hope the tool will expand the reach of 'Ethereum' to more people.

4.9 COINBASE

- Coinbase is a trading platform that allows users to buy, sell and store more than 30 different digital currencies.
- Coinbase is more geared towards beginners while Coinbase Pro, the premium service, is for avid and experienced traders who make high volume transactions and want more trading options.
- The platform is straightforward. Like many trading apps, users can see their balance and a watch list, which allows them to track the prices of different kinds of cryptocurrencies.
- Traders can also check which cryptocurrencies are the biggest movers. Coinbase Cardis also introduced, that users can use to earn rewards for spending the assets in their portfolio.
- Coinbase charges a fee for trading via the platform. Coinbase doesn't charge users to hold their assets in a digital wallet or to transfer cryptocurrency from one wallet to another within the Coinbase network, like from Coinbase to Coinbase Pro.
- Once you have your digital wallet set up, users can trade. Coinbase does not offer trading for all cryptocurrencies, but the exchange does regularly add new coins.

Chapter Ends...

□□□