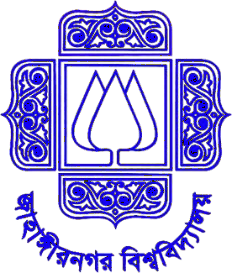
*Course title: Economics*

*Course code: ECO-301*

*3rd Year 1st Semester Examination 2022*

# Date of Submission:



**Submitted to-**

**Md. Adnan Al Nahian**

*Assistant Professor*

*Department of Economics*

*Jahangirnagar University*

*Savar, Dhaka-1342*

| **Sl** | Class Roll | Exam Roll | Name |
| --- | --- | --- | --- |
| 01 | 371 | 202183 | Mamunur Roshid |

**Introduction to crypto and cryptocurrencies:** A cryptocurrency is a digital currency, which is an alternative form of payment created using encryption algorithms. The use of encryption technologies means that cryptocurrencies function both as a currency and as a virtual accounting system. Cryptocurrency, sometimes called crypto-currency or crypto, is any form of currency that exists digitally or virtually and uses cryptography to secure transactions. Cryptocurrencies don't have a central issuing or regulating authority, instead using a decentralized system to record transactions and issue new units.

**List of Cryptocurrencies:** There are many types of crypto currencies. Most popular as follows-

Bitcoin

Litecoin

Dogecoin

Cardano

Ethereum

XRP

Binance Coin

Tether

Bitcoin Cash

**How Bitcoin achieves Decentralization:** Bitcoin is a decentralized digital currency that records transactions in a distributed ledger known as a blockchain. Bitcoin is the most successful out of several attempts to produce virtual money through cryptography. Bitcoin has inspired the advent of other forms of cryptocurrencies. It remains, for the entirety of the past decade, the largest cryptocurrency by market capitalization. The decentralization of Bitcoin is dependent on some of the features in the system. The integrity of transactions is upheld through very secure encryption. When miners verify transactions and add them to the Bitcoin Blockchain, they are rewarded with a newly-created Bitcoin. This, consequently, implies that the processing of transactions is not centralized.

**Mechanics of Bitcoin:** Bitcoin is a decentralized digital currency that operates on a peer-to-peer network and uses cryptographic techniques to secure transactions, control the creation of new units, and verify the transfer of assets. To understand the mechanics of Bitcoin, let's break it down into its key components:

1. **Blockchain:** The Bitcoin blockchain is a public and immutable ledger that contains a record of all transactions ever made on the network. It is a chain of blocks, where each block contains a batch of transactions. Blocks are linked together in chronological order, forming the blockchain.
2. **Transactions:** Transactions are the fundamental building blocks of the Bitcoin system. They represent the transfer of value from one address (Bitcoin wallet) to another. Each transaction includes the sender's public key (address), the recipient's public key, the amount being transferred, and cryptographic signatures to verify the authenticity of the transaction.
3. **Addresses and Wallets:** Bitcoin addresses are alphanumeric strings used to send and receive bitcoins. They are derived from public keys and are meant to be shared publicly. Wallets are software applications that store the private keys needed to access and manage the funds associated with a Bitcoin address.
4. **Miners:** Bitcoin operates on a Proof-of-Work (PoW) consensus mechanism. Miners are participants in the network who use powerful computers to solve complex mathematical puzzles, known as "hashing," to validate and group transactions into blocks. The first miner to solve the puzzle and add a new block to the blockchain is rewarded with newly minted bitcoins and transaction fees from the included transactions.
5. **Mining Reward**: The mining reward is the incentive given to miners for securing the network and validating transactions. Initially set to 50 bitcoins per block, the mining reward is halved approximately every four years in an event called the "halving."
6. **Consensus:** Consensus is achieved when the majority of the network's computational power agrees on the validity of the next block to be added to the blockchain. This ensures that the ledger is accurate and agreed upon by all participants.
7. **Security:** Bitcoin's security is achieved through the use of cryptographic algorithms and the decentralization of the network. Transactions are cryptographically signed to prevent unauthorized tampering, and the decentralized nature of the network makes it resistant to single points of failure or control.
8. **Decentralization:** Bitcoin is decentralized because it operates without a central authority or intermediary. All participants, or nodes, in the network play a role in validating and propagating transactions and blocks. This decentralization enhances the security and resilience of the system.
9. **Halving:** As mentioned earlier, the mining reward is halved approximately every four years or after every 210,000 blocks. This process is known as the "halving" and is programmed into the Bitcoin protocol to control the inflation rate and ultimately limit the total supply of bitcoins to 21 million.

**How to store and use Bitcoins:** No storage method is 100% secure, but here are some ways we can increase our bitcoin and crypto security.

**Types of Storage:**

Custodial Wallet : A custodial wallet is managed by a third party, such as an exchange like Coinbase. In this arrangement, the custodian stores your private keys for you, guaranteeing their safety and sometimes providing insurance on holdings up to a certain amount. Custodial wallets like these have been the target of many attacks since users began using their services; exchanges have taken measures to harden their services, such as moving users' keys into enterprise-level cold storage so that they cannot be accessed.

Custodial wallets can either be hot or cold.

Non-Custodial Wallet: Non-custodial wallets are those you use to store your keys with no one else involved. Non-custodial wallets can also be either hot or cold.

Hot Wallet: Hot wallets are software that stores your keys and have connections to the internet. These wallets create vulnerability because they generate the private and public keys needed to access crypto. While a hot wallet is how most users access and make transactions in bitcoin, they are vulnerable and can be hacked.

Cold Wallet: A cold wallet is a wallet that is not connected to the internet; therefore, it holds far less risk of being compromised. These wallets are also called offline wallets or hardware wallets.

**The Safest Bitcoin Storage:**

Commercial Non-Custodial Cold Wallets

Alternative Non-Custodial Cold Wallets

**Security Precautions:**

Backup

Software Update

Multi-Signature

Seed phrases

**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 receive the bitcoin reward, a new block is created, and the process repeats for the next group of transactions.

**Impact of Cryptocurrency as an alternative monetary system:**

1. **Decentralization:** One of the primary features of cryptocurrencies is their decentralized nature. Traditional fiat currencies are controlled and regulated by central banks and governments, but cryptocurrencies operate on decentralized blockchain technology. This means that no single entity has complete control over the currency, which can have implications for financial sovereignty and independence.
2. **Financial Inclusion:** Cryptocurrencies have the potential to facilitate financial inclusion for individuals who lack access to traditional banking services. All that's needed to participate in the cryptocurrency ecosystem is an internet connection, which opens up possibilities for those in remote or underserved regions.
3. **Borderless Transactions:** Cryptocurrencies can be sent and received across international borders with relative ease, bypassing the need for traditional financial intermediaries like banks or remittance services. This has the potential to reduce transaction costs and time delays associated with cross-border payments.
4. **Security and Anonymity:** Cryptocurrencies employ cryptographic techniques that provide enhanced security for transactions and user identities. While transactions are transparent on the blockchain, users' personal information is generally not required, offering a level of anonymity not found in traditional financial systems.
5. **Investment Opportunities:** The rise of cryptocurrencies has created new investment opportunities for individuals and institutions. Some people have seen substantial returns on their investments, while others have faced significant risks and losses due to the inherent volatility of the cryptocurrency market.
6. **Challenges and Risks:** The impact of cryptocurrencies has not been without challenges and risks. The market's extreme volatility, lack of regulation, and susceptibility to fraud and cyberattacks have caused concerns among policymakers, regulators, and investors. The use of cryptocurrencies for illicit activities, such as money laundering and tax evasion, has also been a point of contention.
7. **Regulatory Responses:** Governments and regulatory bodies worldwide have been grappling with how to address the rise of cryptocurrencies. Some countries have embraced cryptocurrencies, developing regulations to govern their use and protect consumers. Others have taken a more cautious or restrictive approach, leading to varying degrees of acceptance and adoption.
8. **Environmental Concerns:** One significant concern has been the environmental impact of certain cryptocurrency mining operations. Some cryptocurrencies, like Bitcoin, rely on energy-intensive proof-of-work mining algorithms, which have raised questions about their sustainability and carbon footprint.