BLOCK CHAIN TECHNOLOGIES - UNIT – III – MID 1 - ANSWERS

1. Explain Bitcoin Crypto Currency with a suitable diagram and its use cases of Bitcoin

Bitcoin is a decentralized digital currency that was invented in 2008 by an anonymous person or group of people using the pseudonym Satoshi Nakamoto. It operates on a technology called blockchain, which is a distributed ledger that records all transactions across a network of computers. Here are the key components and concepts

Bitcoin was introduced in a whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" in 2008 by an anonymous person or group known as Satoshi Nakamoto. It was launched as an open-source software project in January 2009.

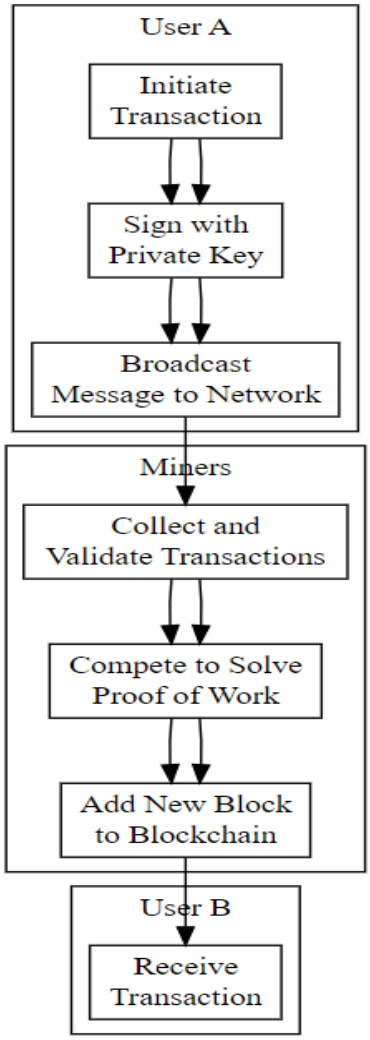
- Bitcoin is a **decentralized digital currency** that operates on a **peer-to-peer network** known as the blockchain.
- Bitcoin transactions are recorded on a public ledger, the blockchain, which is maintained by a distributed network of computers (nodes) without the need for a central authority.
- Bitcoin is often referred to as "**digital gold**" due to its limited supply and potential to serve as a store of value.
- It introduced the concept of cryptocurrencies and blockchain technology

BITCOIN HISTORY:

- **Genesis of Bitcoin (2008-2009):** Bitcoin's origins can be traced back to a whitepaper titled "**Bitcoin: A Peer-to-Peer Electronic Cash System**," published by an individual or group using the pseudonym Satoshi Nakamoto in October 2008.
- **Early Adoption and Mining (2009-2011):** The **first recorded commercial transaction** involving Bitcoin was in May 2010
- **Wider Recognition and Mt. Gox (2011-2013):** In 2011, the first major exchange, Mt. Gox, was established. It became the **dominant exchange for Bitcoin trading**.
- **Media Attention and Price Surge (2013-2014):** Bitcoin gained significant media coverage, drawing attention to its potential as **both a currency and an investment**. In late 2013, its price experienced a dramatic surge, **reaching over $1,000 per BTC**
- **Maturing Ecosystem and Regulatory Developments (2014-2017):** The concept of blockchain technology gained attraction in various industries. Governments and regulatory bodies around the world began to address **Bitcoin's legal and tax status**.
- **Segregated Witness and Scaling Debate (2017):** The **Bitcoin network faced scalability challenges, leading to debates within the community**. A solution called Segregated Witness (SegWit) was activated in August 2017. This upgrade aimed to increase transaction capacity and enable the development of the Lightning Network.
- **All-Time High and Increased Mainstream Interest (2017-2018):** In late 2017, Bitcoin's **price skyrocketed to nearly $20,000 per BTC**, driven by speculative interest.
- **Bear Market and Institutional Involvement (2018-2019):** Following the peak, Bitcoin entered a prolonged bear market. Despite the price decline, the cryptocurrency space continued to develop, with **increasing interest from institutional investors and the growth of various use cases and projects**.
- **2020 and Beyond:** Bitcoin's price saw a resurgence in 2020, attributed to factors such as macroeconomic uncertainty and growing institutional adoption. Companies like **MicroStrategy and Tesla** made headlines by announcing Bitcoin purchases for their corporate treasuries. The concept of Bitcoin as "digital gold" gained further prominence.

BLOCK CHAIN TECHNOLOGIES - UNIT – III – MID 1 - ANSWERS

Bitcoin Transaction Process Flowchart



1. User A initiates a Bitcoin transaction by creating a digital message specifying the recipient (User B) and the amount to be sent.
2. User A signs this message with their private key, creating a digital signature.
3. The transaction message, along with the digital signature, is broadcast to the Bitcoin network.
4. Miners on the network collect and validate pending transactions.
5. Miners compete to solve a mathematical puzzle (Proof of Work) to add a new block of transactions to the blockchain.
6. Once a miner successfully adds a block, the transaction is confirmed and recorded on the blockchain.
7. User B can now see the incoming transaction in their wallet and access the newly received Bitcoins.
8. This process ensures the security and transparency of Bitcoin transactions, making it a trustless and decentralized form of digital currency.

Use cases of Bitcoin:

- Peer-to-peer payments:
- Investment
- Speculation
- E-commerce
- Micropayments
- Charity
- Darknet markets
- Decentralization
- Security
- Transparency
- Speed

BLOCK CHAIN TECHNOLOGIES - UNIT – III – MID 1 - ANSWERS

2. How does Bitcoin's scripting language support micropayments?

Bitcoin's scripting language supports micropayments through a feature known as "Bitcoin Script" and the use of payment channels

In computer programming, a script is a **program or sequence of instructions that is interpreted**

In Bitcoin,

- Scripts are a **fundamental part of its transaction process**.
- They are simple programs that define the conditions under which a certain transaction output can be spent.
- These scripts are written in a programming language called Script.

The combination of blockchain technology and scripts in Bitcoin provides a secure and programmable way to manage and transfer digital assets, going beyond traditional currency systems.

Blockchain scripting:

Blockchain scripting is a programming language used to create smart contracts and other applications on blockchain networks. Blockchain scripting is a powerful tool that can be used to create a wide variety of applications. As blockchain technology continues to evolve, blockchain scripting languages will become even **more sophisticated and powerful**.

- It is a stack-based language, which means that **instructions are executed one at a time**, and the values of variables are **stored on a stack**.
- Blockchain scripting languages are typically Turing-complete, meaning that they can be used to create any program that can be **theoretically executed by a computer.**
- The most common blockchain scripting language is **Bitcoin Script**, which is used to create **transactions on the Bitcoin blockchain**.
- Other popular blockchain scripting languages include **Ethereum Solidity, Hyperledger Fabric Chaincode, and EOS C++.**

Benefits of Blockchain scripting:

- **Security**: Blockchain scripting is a secure way to store and execute code. The code is stored on the blockchain, which is a distributed ledger that is secured by cryptography.
- **Transparency**: The code is transparent and can be audited by anyone. This makes it difficult to fraud or manipulate the code.
- **Scalability**: Blockchain scripting is scalable and can be used to create applications that can handle a large number of transactions.
- **Flexibility**: Blockchain scripting is flexible and can be used to create a wide variety of applications.

Micropayment:

Micropayments are small financial transactions, typically involving very small amounts of money, often fractions of a cent or a few cents, that are conducted electronically. These tiny transactions are used for various purposes, such as purchasing digital content, accessing online services, or making small payments for goods and services.

A Micropayment Channel or Payment Channel is class of techniques designed to allow users to make multiple Bitcoin transactions without commiting all of the transactions to the Bitcoin block chain.

BLOCK CHAIN TECHNOLOGIES - UNIT – III – MID 1 - ANSWERS

Micropayment Examples

- Subscriber fees from streaming services. Subscribers pay a fixed fee at the beginning of each month to access digital goods. ...
- Freelance income through gig sites. ...
- Google ads that monetize user-generated content (UGC).

Advantages of micropayment

- Autonomous transactions. M2M transactions can take place without human intervention. ...
- Time saving. Autonomous payments accelerate transactions because there is no need to wait for human input. ...
- Cost savings.

Disadvantages of micropayment:

- No guaranteed revenue from month to month, week to week, or even hour to hour.
- Provides little impetus for users to return.
- Can lead to low overall lifetime value for users.

3. What are the practical applications of Bitcoin's scripting language, particularly in escrow transactions?

Escrow transactions involve a trusted third party holding funds or assets on behalf of two or more parties until specific conditions are met. Bitcoin escrow script is a ready-made escrow enabled p2p exchange software that helps you to launch a secure P2P crypto exchange platform. Bitcoin escrow script is crafted with advanced coding languages and blockchain technology

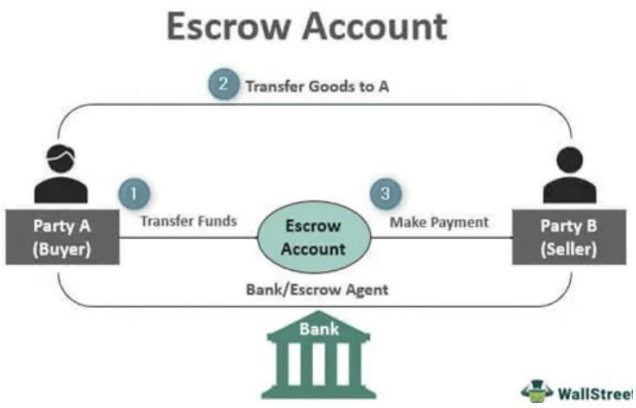
- Bitcoin's scripting language allows for the creation of smart contracts that can facilitate and automate escrow arrangements.
- Bitcoin's scripting language is a powerful tool that can be used to create a wide variety of complex transactions, including escrow transactions.
- Escrow transactions can be used to buy and sell goods and services, to pay freelancers, and to bet on online games without having to trust the other party involved in the transaction.
- As Bitcoin becomes more widely adopted, we can expect to see even more innovative and disruptive applications of Bitcoin's scripting language emerge.

Practical applications of Bitcoin's scripting language in escrow transactions:

1. **Online Marketplaces:** Bitcoin's scripting language can be used in online marketplaces to facilitate secure transactions between buyers and sellers. In this scenario, a multi-signature escrow address is created, and funds from the buyer are locked into this address. The seller and a trusted mediator hold the necessary private keys. When the buyer receives the product and is satisfied, they and the seller can jointly sign a transaction to release the funds from escrow. If there's a dispute, the mediator can step in to resolve it.
2. **Real Estate** Transactions**:** Bitcoin's scripting language can be applied in real estate transactions, particularly for property purchases. A multi-signature escrow address is established, with the buyer, seller, and a neutral third party (e.g., a title company) each holding a private key. The buyer deposits the purchase amount into this address. The transaction is only completed when all parties agree that the conditions, such as property inspections and document verifications, have been met.

3. **Gambling and Betting:** Bitcoin's scripting language can be used to create escrow contracts for gambling and betting applications. Wagers are placed into an escrow address, and the funds are automatically distributed to the winning party based on predefined rules and the outcome of an event.
4. **Smart Contracts for Freelancers**: Freelancers and clients can use Bitcoin's scripting language to create smart contracts for work agreements. The agreed-upon payment is held in escrow, and it's automatically released to the freelancer when the work is completed and accepted by the client.

Escrow Account Process



The buyer and the seller enter a deal through an escrow, and both agree to comply with the contract's terms and conditions. Upon agreement, the following steps:

1. The buyer pays the transaction amount to the escrow account. Consequently, the third party notifies the seller.
2. Next, the seller delivers the product to the buyer. Upon which, the buyer verifies the the product.
3. Finally, the escrow transfers the sum to the seller's account on receiving confirmation from the buyer.

Advantages

1. Safe and Secure Transactions: An escrow ensures that the contracting parties sincerely fulfill commitments. Thus, the transaction is virtually risk-free.
2. Builds Trust: Dealing via an escrow facilitate a higher degree of trust between parties. This further leads to more future dealings where both the parties make a profit.
3. Facilitates Monthly Tax and Insurance Payments: The homeowners hire escrows; home loan providers or mortgage firms. This arrangement helps homeowners pay loans and mortgage in time.
4. Customized Transactions: Such an account includes tailor-made conditions in context to the contract between two parties.
5. Money-Back Assurance: If the seller fails to supply the goods or services or meet the desired standards, the money will be repaid to the buyer.

Disadvantages

1. An escrow account, when opened for insurance and tax purposes, it has various disadvantages. The escrow may calculate the tax amount incorrectly. This could be caused by property value changes. Besides, monthly mortgage payments can be pretty high when it includes tax and insurance charges.
2. Moreover, there are chances of being trapped in escrow fraud. Some miscreants create fake accounts to fool the parties and steal their money. Additionally, escrow fees can be hefty at times; this varies depending on the mode of payment.