**Q1. Attempt any four.**

**a. Explain Simplified Payment Verification (SPV) and write down its key features. // ye** sikhaya hai kya apan ko? //I don’t think so. Jawrang can answer better. Wo jyada lec baitha apne se // Riyal Shit [2021.gaurang.raorane@ves.ac.in](mailto:2021.gaurang.raorane@ves.ac.in)bata bhai haila tag bhi hota yaha se

SPV or **simplified payment verification** is a method for verifying particular trans‐

actions were included in a block without downloading the entire block. The

method is used by some lightweight Bitcoin clients.

A **lightweight client**, also known as a simple-payment-verification (SPV) client,

connects to bitcoin full nodes for access to the bitcoin transaction information, but stores the user wallet locally and independently cre‐ates, validates, and transmits transactions. Lightweight clients interact directly with the bitcoin network, without an intermediary.

Not all nodes have the ability to store the full blockchain. Many bitcoin clients are

designed to run on space- and power-constrained devices, such as smartphones, tab‐

lets, or embedded systems. For such devices, a simplified payment verification (SPV)

method is used to allow them to operate without storing the full blockchain. These

types of clients are called SPV clients or lightweight clients. As bitcoin adoption

surges, the SPV node is becoming the most common form of bitcoin node, especially

for bitcoin wallets.

Features(GPT) **Lightweight Verification:** SPV allows users to verify the validity of transactions and their inclusion in a block with relatively minimal computational and storage resources. Instead of downloading the entire blockchain, SPV clients only need to download block headers and a small subset of data.

**Block Header Validation:** SPV clients primarily rely on the block headers of the blockchain. These headers contain important information like the Merkle root of all transactions in the block and the proof-of-work difficulty, which makes it challenging for attackers to tamper with the data.

**Reduced Data Storage**: SPV clients do not store the full transaction history of the blockchain. They only store a small portion of the blockchain, which includes the block headers and a filter that identifies transactions relevant to the user's wallet.

**Privacy-Preserving:** SPV offers a certain level of privacy as it doesn't require users to share their full transaction history with network nodes. However, it's important to note that SPV doesn't provide the same level of privacy as running a full node.

**b. What is mining and what is the need of Mining in Blockchain?**

The bitcoin system of trust is based on computation. Transactions are bundled into

blocks, which require an enormous amount of computation to prove, but only a small

amount of computation to verify as proven. The mining process serves two purposes

in bitcoin:

• Mining nodes validate all transactions by reference to bitcoin’s consensus rules.

Therefore, mining provides security for bitcoin transactions by rejecting invalid

or malformed transactions.

• Mining creates new bitcoin in each block, almost like a central bank printing new

money. The amount of bitcoin created per block is limited and diminishes with

time, following a fixed issuance schedule.

Mining achieves a fine balance between cost and reward. Mining uses electricity to

solve a mathematical problem. A successful miner will collect a reward in the form of

new bitcoin and transaction fees. However, the reward will only be collected if the

miner has correctly validated all the transactions, to the satisfaction of the rules of

consensus. This delicate balance provides security for bitcoin without a central

authority.

**c. Explain how Bitcoin Transaction works.**

**d. Explain Public Key and Private key in bitcoin wallet with its generation process.**

**e. Explain peer to peer network architecture in Blockchain.**

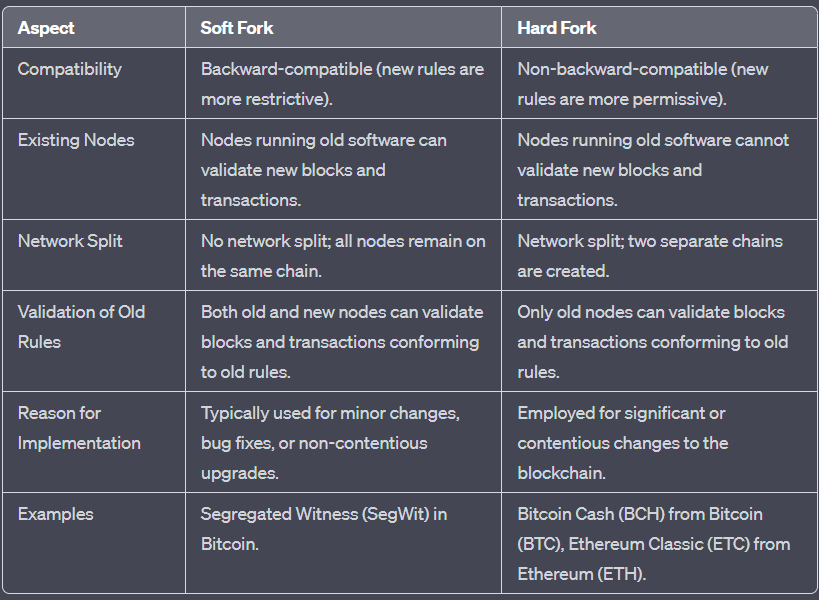
**Q2 a. Explain Merkle trees also explain what is importance of Merkle in Blockchain?**

**b. What is decentralized consensus? Explain Byzantine General's Problem detail.**

**Q3 a. What is need of fork in Blockchain; differentiate between soft fork and hard fork.**

In blockchain technology, a fork is a fundamental concept that refers to a change or divergence in the protocol's rules and consensus mechanism. Forks are necessary for various reasons, including upgrading the blockchain, resolving conflicts, and making improvements to the network. There are two main types of forks: soft forks and hard forks, which differ in their compatibility with the existing blockchain.

Difference b/w



**b. Explain different types of wallets along with their merits and demerits; also explain factors which decide which type of wallets are used for any particular application.**

In blockchain, a wallet is a software or hardware tool that allows users to manage their cryptocurrency holdings, store private keys, and interact with the blockchain network. There are several types of wallets, each with its own merits and demerits. The choice of wallet type for a particular application depends on various factors, including security, convenience, and usage requirements. Here are the different types of wallets, along with their merits and demerits:

Software Wallets:

Merits:

Accessibility: They are easily accessible on computers, smartphones, and tablets, making them convenient for everyday transactions.

User-Friendly: Most software wallets have user-friendly interfaces and are suitable for beginners.

Features: They often offer additional features such as the ability to exchange cryptocurrencies within the wallet.

Demerits:

Security: They are susceptible to malware and phishing attacks, especially on computers and smartphones.

Dependence on Third Parties: Some software wallets rely on third-party services, which may pose security and privacy risks.

Factors for Use: Software wallets are suitable for everyday use and transactions where accessibility and convenience are essential. They are often chosen for small to moderate cryptocurrency holdings.

Hardware Wallets:

Merits:

High Security: Hardware wallets are considered one of the most secure options as they store private keys offline, making them immune to online attacks.

Cold Storage: They offer "cold storage" for long-term holding of cryptocurrencies, protecting them from hacking.

Independence: Hardware wallets do not rely on third-party services or internet connectivity.

Demerits:

Cost: They are relatively expensive compared to software wallets.

Limited Functionality: Hardware wallets are designed primarily for storage and may lack the features of software wallets.

Factors for Use: Hardware wallets are ideal for users looking to secure significant amounts of cryptocurrency or for long-term holding. They are the preferred choice for individuals who prioritize security.

Paper Wallets:

Merits:

High Security: Paper wallets store private keys offline, providing strong security against online threats.

No Cost: They are cost-effective and can be created for free.

Demerits:

Physical Vulnerability: Paper wallets can be damaged or lost, and they require safe storage.

Lack of Usability: Redeeming funds from a paper wallet can be less user-friendly and might require technical knowledge.

Factors for Use: Paper wallets are often used for long-term storage and as a form of secure backup. They are suitable for users who prioritize security and do not require frequent access to their cryptocurrency.

Mobile Wallets:

Merits:

Convenience: Mobile wallets are easy to use and allow users to make on-the-go transactions.

Portability: They can be accessed from anywhere, making them suitable for mobile users.

Demerits:

Security Risks: Mobile devices are susceptible to loss, theft, and malware attacks.

Limited Storage: Mobile wallets may have limited storage capacity.

Factors for Use: Mobile wallets are a good choice for users who need quick and easy access to their cryptocurrency for daily transactions. They are suitable for holding smaller amounts of cryptocurrency.

Web Wallets:

Merits:

Accessibility: Web wallets can be accessed from any internet-connected device.

User-Friendly: They often have user-friendly interfaces.

Demerits:

Security Risks: Web wallets are vulnerable to online attacks and phishing attempts.

Dependence on Third Parties: They rely on third-party services, which can be a security and privacy concern.

Factors for Use: Web wallets are convenient for users who need accessible and easy-to-use wallets for small to moderate cryptocurrency holdings. However, they may not be suitable for long-term storage.

Multisignature Wallets:

Merits:

Enhanced Security: Multisignature wallets require multiple private keys to authorize transactions, making them more secure against single points of failure.

Shared Control: They are suitable for businesses or groups that require shared control over funds.

Demerits:

Complexity: Setting up and managing multisignature wallets can be more complex than single-signature wallets.

Recovery Challenges: If keyholders lose access or fail to cooperate, accessing funds can be challenging.

Factors for Use: Multisignature wallets are used when enhanced security and shared control are essential, especially for business or organizational use cases.

The choice of wallet type depends on various factors, including:

Security Requirements: If security is a top priority, hardware wallets or paper wallets may be preferred.

Usage Frequency: For everyday transactions, software wallets and mobile wallets are more convenient, while cold storage solutions like hardware or paper wallets are suitable for long-term storage.

Accessibility: Some users may prioritize accessibility and may choose web or mobile wallets, even with potential security trade-offs.

Technical Proficiency: Users with more technical expertise might opt for paper wallets or multisignature wallets.

Business or Group Needs: Multisignature wallets are used when multiple parties need to jointly control funds.

Cost Considerations: The budget available for a wallet can also influence the choice, with some options being more cost-effective than others.

Ultimately, the choice of a wallet type should align with the user's specific needs, preferences, and priorities, with careful consideration of the security and usability trade-offs.

**Q4 a. Explain transaction in detail with example.**

**b. Which cryptographic algorithm is used in Blockchain explain with example.**

**Q5 a. What is a node in Blockchain network? List and explain various types node in Blockchain.**

**b. Explain SVP nodes and privacy in detail**

**Q6 Write a short note on any four.**

**a. Assembling and selecting a chain of blocks.**

**b. Bitcoin relay network**

**c. Blockchain Technology in Supply chain & logistics**

**d. Blockchain Technology in Energy**

**e. Bitcoin Transaction**

A Bitcoin transaction is a fundamental operation within the Bitcoin blockchain network, allowing users to transfer ownership of Bitcoin cryptocurrency from one wallet address to another. Bitcoin transactions play a central role in facilitating the peer-to-peer transfer of digital value within the decentralized and trustless blockchain system. To elaborate on this topic for a 10-mark university examination answer, one can provide a comprehensive overview of Bitcoin transactions, covering their structure, purpose, validation process, and significance.

Introduction to Bitcoin Transactions (1 Mark):

A Bitcoin transaction is a digital record stored on the Bitcoin blockchain, which represents the transfer of ownership of a certain amount of Bitcoin from one party to another. These transactions are the core mechanism through which value is transferred within the Bitcoin network, serving as a secure and transparent ledger of financial activities.

Structure of a Bitcoin Transaction (2 Marks):

A standard Bitcoin transaction consists of several key components:

Input: This section specifies the source of the funds, typically referring to the previous transaction's output (known as the Unspent Transaction Output or UTXO) that the sender is spending.

Output: The output section defines the recipient's Bitcoin address and the amount being transferred.

Digital Signature: A cryptographic signature is provided by the sender to prove ownership of the funds and ensure the security of the transaction.

Transaction Fee: The sender may include a transaction fee to incentivize miners to process the transaction.

Purpose of Bitcoin Transactions (2 Marks):

Bitcoin transactions serve various purposes within the network:

Peer-to-Peer Transfers: They enable users to send and receive Bitcoin directly, facilitating financial transactions without the need for intermediaries such as banks.

Verification and Consensus: Transactions are validated by network nodes through a consensus mechanism, ensuring the integrity and security of the Bitcoin ledger.

Ownership Transfer: Bitcoin transactions prove the transfer of ownership rights, enabling users to demonstrate control over their funds.

Validation of Bitcoin Transactions (3 Marks):

The validation process of Bitcoin transactions involves the following steps:

Propagation: When a user initiates a transaction, it is broadcast to the Bitcoin network, allowing nodes to verify its authenticity.

Inclusion in a Block: Transactions are collected into blocks by miners. Miners compete to solve a complex mathematical puzzle to add a new block to the blockchain.

Consensus: Transactions must be confirmed by a network of distributed nodes, ensuring that they meet the network's rules, including double-spending prevention.

Mining Reward: Miners receive a reward (in the form of newly created Bitcoins and transaction fees) for successfully adding a block to the blockchain.

Significance of Bitcoin Transactions (2 Marks):

Bitcoin transactions are significant for several reasons:

Decentralization: They are the foundation of a peer-to-peer, decentralized financial system, eliminating the need for intermediaries and providing financial autonomy to users.

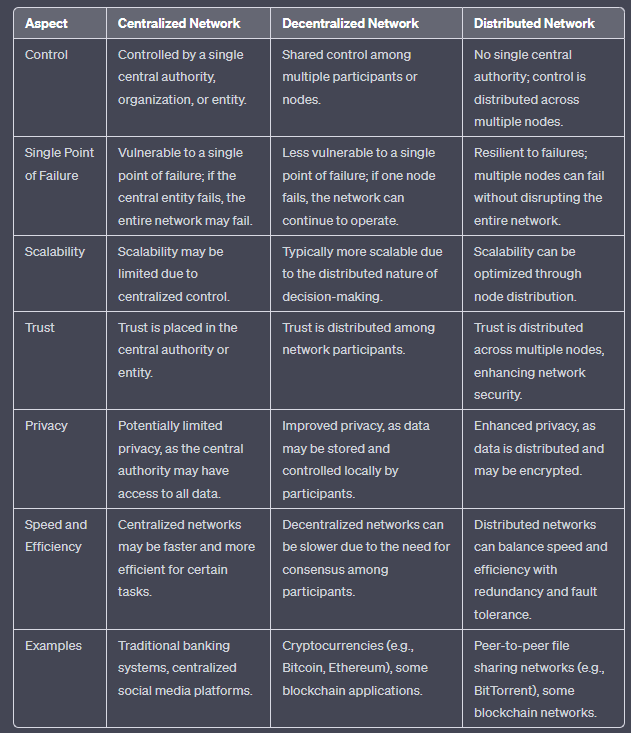
Security: Bitcoin transactions rely on strong cryptographic techniques, making them secure and resistant to fraud.

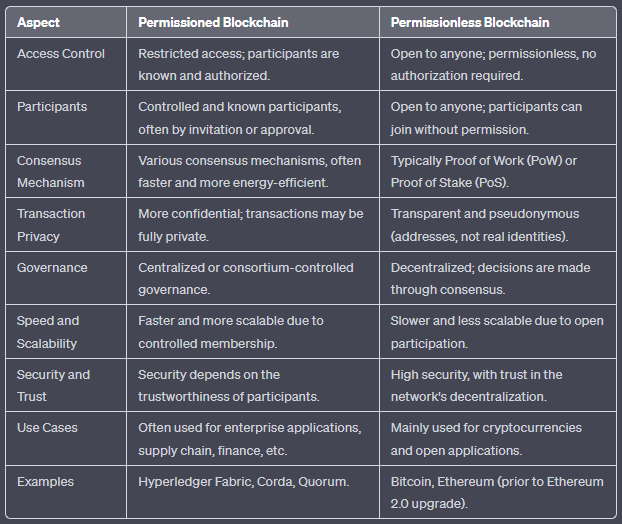
Transparency: The public ledger aspect of Bitcoin transactions ensures transparency and accountability, as all transactions are publicly recorded and can be audited by anyone.

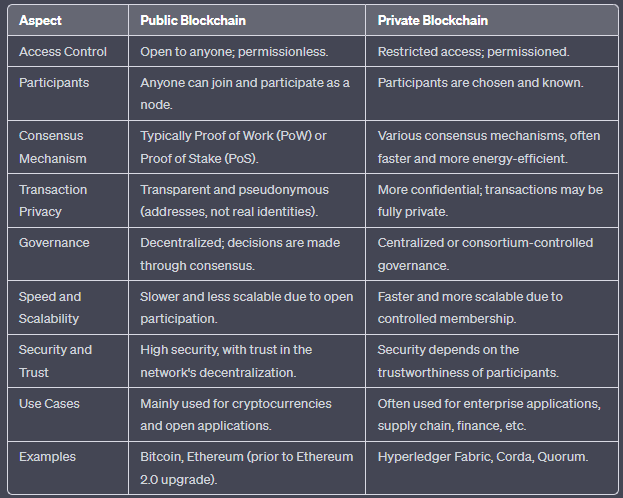
Global Accessibility: Bitcoin transactions can be conducted worldwide, enabling cross-border transfers without the need for traditional banking systems.

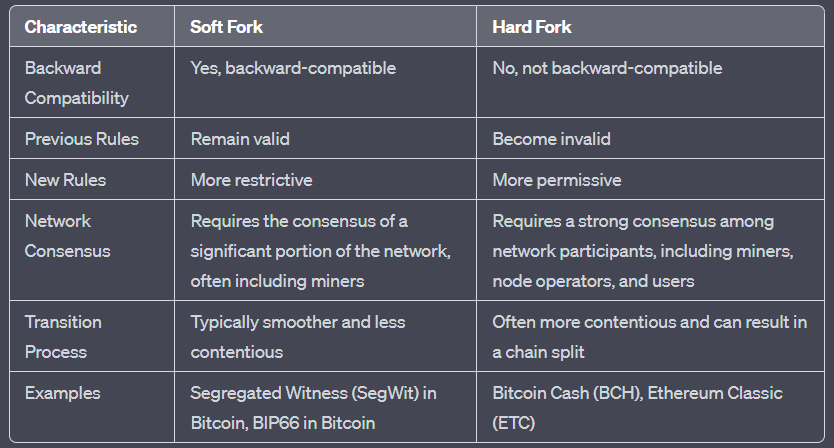
In conclusion, Bitcoin transactions are the lifeblood of the Bitcoin blockchain network, serving as a secure, transparent, and decentralized means of transferring value. They play a pivotal role in ensuring the integrity of the ledger and provide users with financial sovereignty and global accessibility. Understanding the structure, validation process, and significance of Bitcoin transactions is essential for anyone looking to participate in the world of cryptocurrencies.

**IMP TOPICS**

****

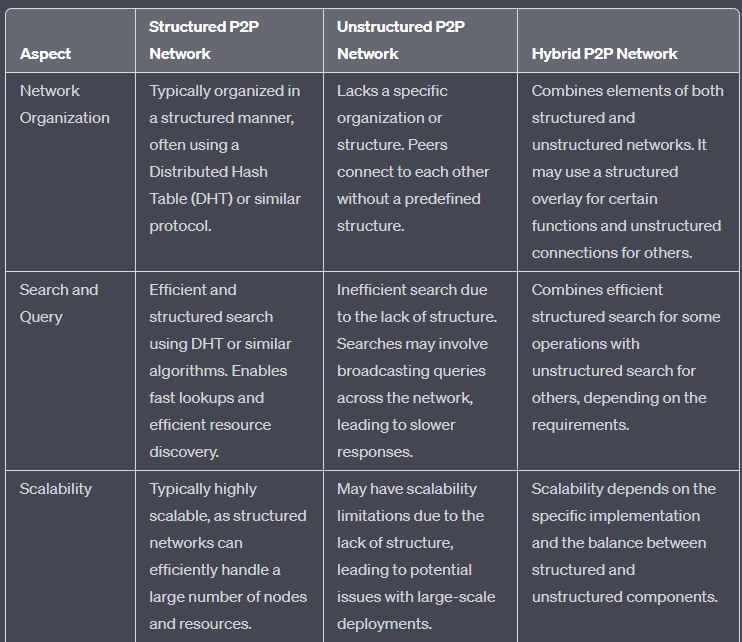
****

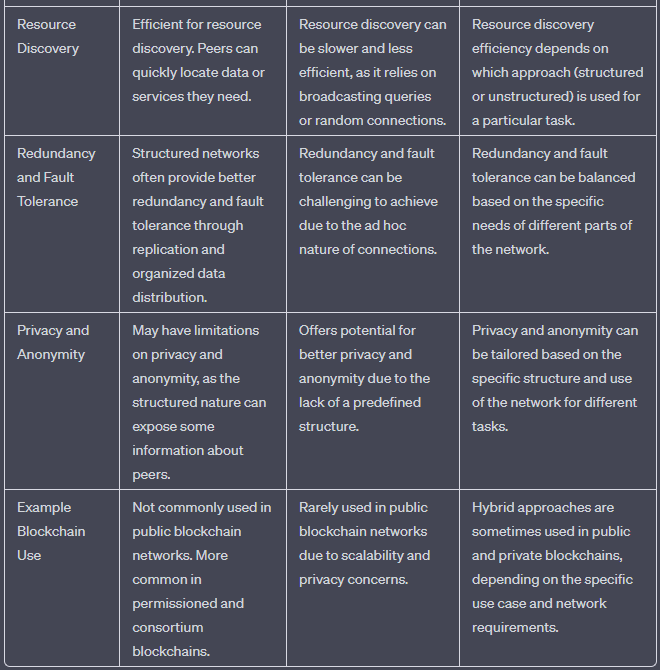
****

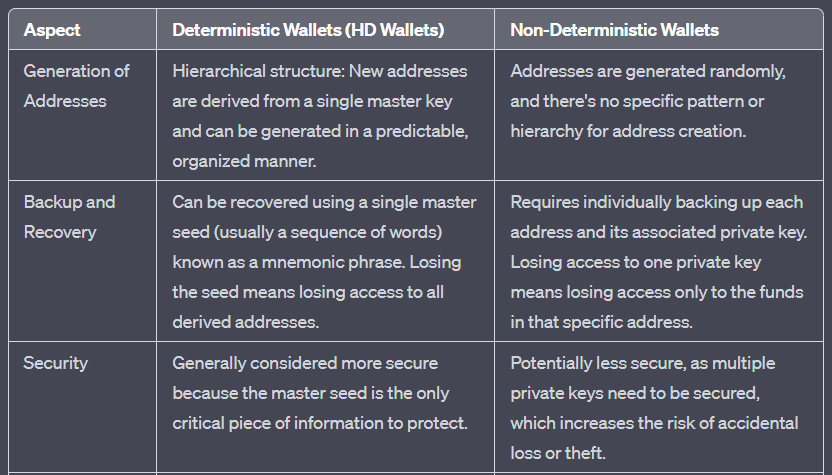
****

**Mod5**

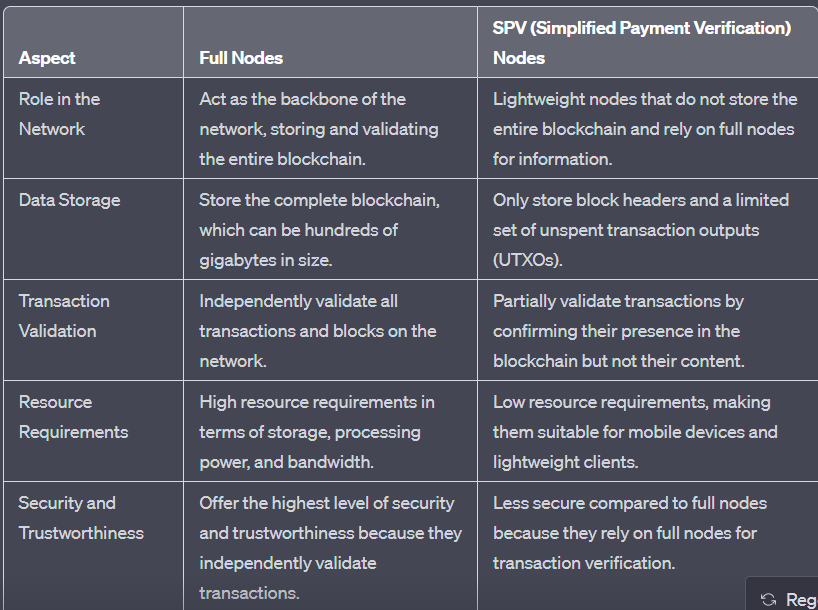
[**https://www.geeksforgeeks.org/what-is-p2p-peer-to-peer-process/**](https://www.geeksforgeeks.org/what-is-p2p-peer-to-peer-process/)

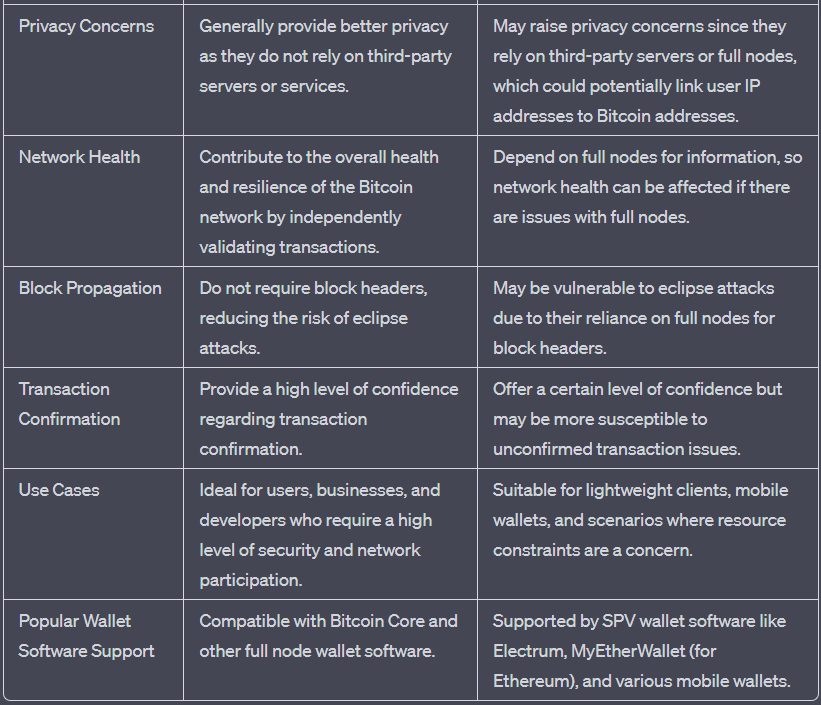
****

****

****

****

****

****