**Q&A**

**Q 1 - How does a timestamp server work in the proposed solution, and what is the role of the hash in the process?**

A 1 - In the proposed solution, a timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash. The hash plays a crucial role in the process as it proves that the data must have existed at the time it was timestamped in order to get into the hash.

**Q 2 - What is the problem with introducing a trusted central authority in electronic transactions, and why is it not a viable solution in the long run?**

A 2 - Introducing a trusted central authority in electronic transactions is not a viable solution in the long run because it requires trust, increases transaction costs, and limits the possibility for small casual transactions. Additionally, it introduces the possibility of fraud and requires merchants to be wary of their customers.

**Q 3 - How does the proposed solution create a chain of timestamps, and how does this chain of timestamps reinforce the previous ones?**

A 3 - The proposed solution creates a chain of timestamps by including the previous timestamp in each subsequent timestamp's hash, forming a chain of blocks. Each additional timestamp reinforces the ones before it as it is computationally impractical to alter the contents of any given timestamp block without altering all subsequent blocks. Therefore, the more timestamps that are added to the chain, the more secure it becomes.

**Q 4 - What kind of system is used to implement a distributed timestamp server on a peer-to-peer basis? O**

A 4 - The system used to implement a distributed timestamp server on a peer-to-peer basis is a proof-of-work system similar to Adam Back's Hashcash.

**Q 5 - How is the proof-of-work system implemented in the timestamp network proposed in the text? O**

A 5 - The proof-of-work system in the timestamp network proposed in the text is implemented by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work.

**Q 6 - What problem does the proof-of-work solve in majority decision making?**

A 6 - The proof-of-work solves the problem of determining representation in majority decision making, as it ensures that the majority decision is represented by the longest chain with the greatest proof-of-work effort invested in it, rather than by one-IP-address-one-vote, which could be subverted by anyone able to allocate many IPs.

**Q 7 - How is the proof-of-work difficulty determined in the timestamp network? O**

A 7 - The proof-of-work difficulty in the timestamp network is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

**Q 8 - What is the purpose of the first transaction in a block in a cryptocurrency network?**

A 8 - The purpose of the first transaction in a block in a cryptocurrency network is to start a new coin owned by the creator of the block, providing an incentive for nodes to support the network and a way to initially distribute coins into circulation

**Q 9 - How does the incentive system in a cryptocurrency network help encourage nodes to stay honest?**

A 9 - • The incentive system in a cryptocurrency network rewards nodes with new coins for their CPU time and electricity expended in adding new blocks to the chain. This steady addition of new coins is analogous to gold miners adding gold to circulation. If a greedy attacker were to try to defraud people by stealing back their payments or undermine the system, they would have to choose between using their CPU power to generate new coins or using it to defraud people. The incentive system encourages nodes to play by the rules and act honestly in order to earn more new coins than anyone else combined.

**Q 10 - What is the purpose of hashing transactions in a Merkle Tree in the Bitcoin blockchain, and how does it facilitate compacting old blocks?**

A 10 - The purpose of hashing transactions in a Merkle Tree in the Bitcoin blockchain is to facilitate discarding spent transactions in old blocks without breaking the block's hash. This is done by including only the root of the Merkle Tree in the block's hash, allowing old blocks to be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored, which helps save disk space.

**Q 11 - What is the simplified method for verifying payments without running a full network node, and how does it work?**

A 11 - The simplified method for verifying payments without running a full network node is to keep a copy of the block headers of the longest proof-of-work chain and obtain the Merkle branch linking the transaction to the block it's timestamped in. This method is reliable as long as honest nodes control the network, but is vulnerable if the network is overpowered by an attacker.

**Q 12 - How does the privacy level of the traditional banking model compare to that of stock exchanges, and how can anonymity of public keys be used to maintain privacy in the context of publicly announced transactions?**

A 12 - The privacy level of the traditional banking model is higher than that of stock exchanges, as the latter only reveals the time and size of individual trades without telling who the parties were. Anonymity of public keys can be used to maintain privacy in the context of publicly announced transactions by keeping public keys anonymous, so that the public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone.