# **LetsUpgrade Blockchain Assignment #1**

Question 1: What is your understanding of Blockchain?

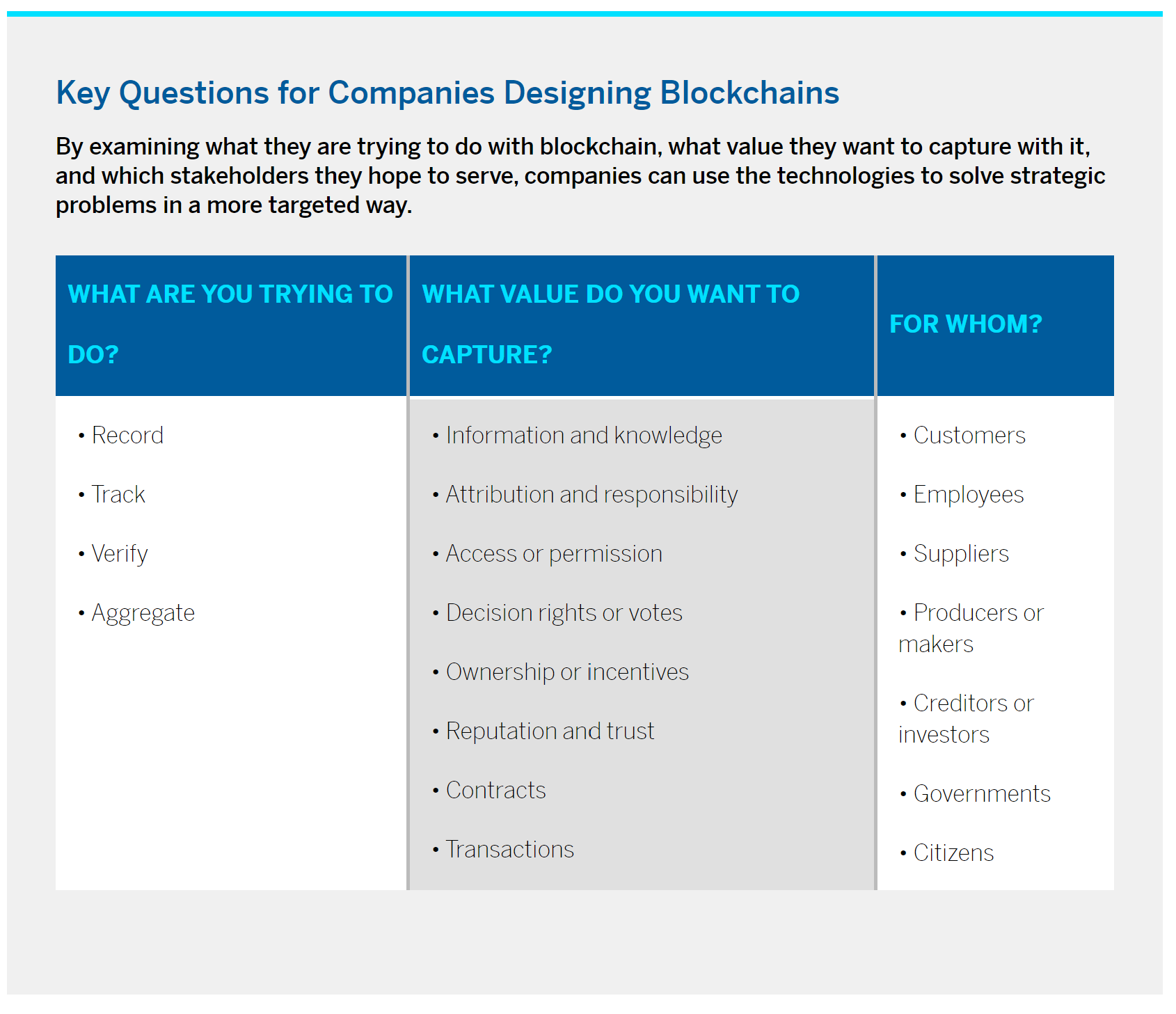
Ref: <https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html>

Ans: A blockchain is a decentralized ledger of all transactions across a peer-to-peer network. Using this technology, participants can confirm transactions without a need for a central clearing authority. Potential applications can include fund transfers, settling trades, voting, and many other issues.

Question 2: What is the core problem Blockchain trying to solve?

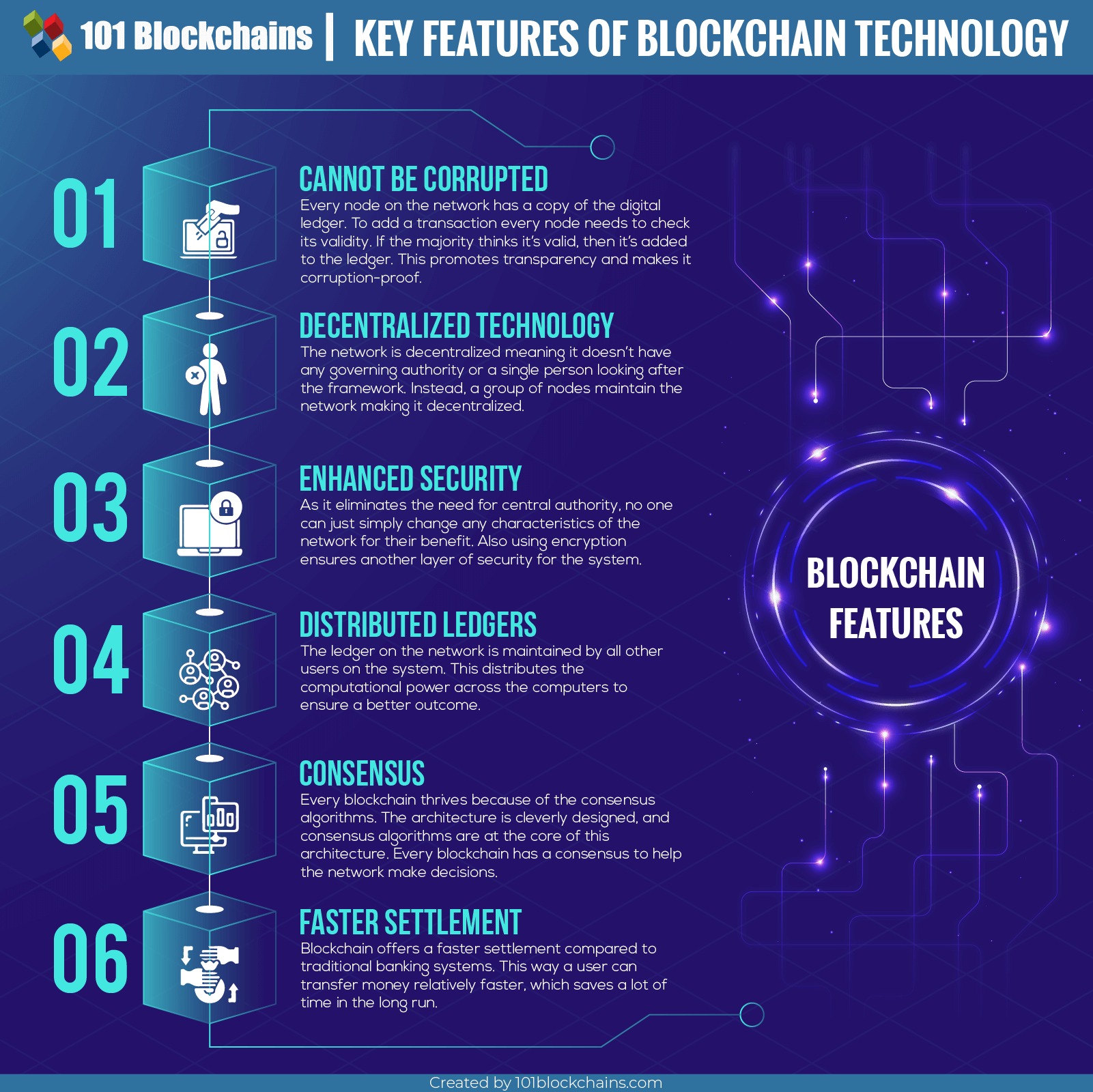
Ref: <https://sloanreview.mit.edu/article/what-problems-will-you-solve-with-blockchain/>

Organizations must determine which transactions or interactions the blockchain should capture and who should have access to which portions.



Question 3: What are the few features which Blockchain will give you?

Ref: <https://101blockchains.com/introduction-to-blockchain-features/>



Question 4: What all things does a Block contain?

Ref 1: <https://www.linkedin.com/pulse/blockchain-data-structure-ronald-chan/>

Ref 2 : <https://www.pluralsight.com/guides/blockchain-architecture>

The blockchain data structure is a back-linked list of blocks of transactions, which is ordered. It can be stored as a flat file or in a simple database. Each block is identifiable by a hash, generated using the SHA256 cryptographic hash algorithm on the header of the block. Each block references a previous block, also known as the parent block, in the “previous block hash” field, in the block header.

Blocks contain a **block header**, which is the metadata that helps verify the **validity** of a block.

Typical block metadata contains:

* version - the current version of the block structure
* previous block header hash - the reference this block's parent block
* merkle root hash - a cryptographic hash of all of the transactions included in this block
* time - the time that this block was created
* nBits - the current difficulty that was used to create this block
* nonce ("number used once") - a random value that the creator of a block is allowed to manipulate however they so choose

Question 5: How is the verifiability of Blockchain has been attained?

Ref 1: <https://www.techvariable.com/how-does-blockchain-verification-work/>

Ref 2 : <https://www.investopedia.com/terms/b/blockchain.asp>

in Blockchain, every user keeps a track record of transactions. This record is regularly updated. When a user introduces a new transaction to the system, the user hashes it once or multiple time. This gives a unique output.

Now other users or nodes or clients do the same thing. They too run it on their respective machines. If the output matches then the transaction is termed as valid. If not, then it is rejected. This is a seemingly simple procedure that the Blockchain technology uses to distinguish between real transactions and fraud ones. It may look like inessential but the importance of this process becomes paramount when sensitive and valuable data, say, Bitcoins are introduced into the mix.