

Mid term :

Smart contracts are a set of instructions executed in a decentralized way without the need for a centralized or third party intermediary.

With smart contracts, we can eliminate the need for trust. A smart contract is an agreement or a set of instructions that are deployed on a decentralised blockchain. Once deployed, it cannot be altered; it automatically executes, and everyone can see its terms.

1. The core of blockchain and smart contracts lies in creating a trustless system where agreements are transparent, unchangeable, and executed without human intervention. This technology holds the potential to revolutionize industries and everyday agreements by ensuring honesty and fairness.
2. Centralized bodies, like traditional exchanges, have the power to restrict access to financial markets. there is no central authority that can alter or limit market access. This introduces fairness and openness to the financial markets.
 - Traditional Agreements: Require trust in a centralized entity.
 - Smart Contracts: Transparent, decentralized, and tamper-proof.
 - smart contracts can not be altered, execute automatically, everyone sees the terms of agreements.
3. Smart contracts are *the* solution to minimizing the reliance on trust based systems that have historically failed us time and time again.

However, smart contracts face a significant limitation - they cannot interact with or access data from the real world. This is known as the Oracle Problem.

1. Blockchains are deterministic systems, so everything happens within their ecosystem. To make smart contracts more useful and capable of handling real-world data, they need external data and computation. Oracles serve this purpose. They are devices or services that provide data to blockchains or run external computation. To maintain decentralisation, it's necessary to use a decentralized Oracle network rather than relying on a single source. This combination of on-chain logic with off-chain data leads to hybrid smart contracts

1. Common Terms:

- Chainlink is a popular decentralized Oracle network that enables smart contracts to access external data and computation. Chainlink is also blockchain agnostic - so it's going to work with any chain out there.
- Blockchain: In Web3, a blockchain is a digital ledger that records transactions across many computers in a secure and decentralized manner. Each block contains a number of transactions, and every new block is linked to the previous one, forming a chain. This makes the data tamper-resistant. *Example:* Bitcoin's blockchain records all BTC transactions.

- Oracle: Oracles in web3 are intermediaries that provide smart contracts with external data. They act as bridges between blockchains and the outside world, allowing smart contracts to execute based on real-world events and data.
- Layer 2: Layer 2 solutions in web3 are technologies built on top of a blockchain (Layer 1) to improve its scalability and efficiency. These solutions handle transactions off the main chain, reducing congestion and fees,