.What is block chain , its types , adavntages-disadavntages uses ?

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Cryptographer. David Chaum first proposed a blockchain-like protocol in his 1982 dissertation "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups. The blockchain technology was described in **1991** by the research scientist **Stuart Haber** and **W. Scott Stornetta**. They wanted to introduce a computationally practical solution for time-stamping digital documents so that they could not be backdated or tampered. They develop a system using the concept of **cryptographically** secured chain of blocks to store the time-stamped documents . Later Further, in **2008**, **Satoshi Nakamoto** conceptualized the theory of **distributed blockchains**. He improves the design in a unique way to add blocks to the initial chain without requiring them to be signed by trusted parties.

Types of Block chain :-

1.public block chain

2.private block chain

3.hybrid block chain

4.side chain

Advantages :-

* Trustworthy distributed system
* No government interference
* Increase stability
* Instant payment at reduce cost
* Improved security & financial efficiency

Disadvantages :-

* Private key issues
* Extremely volatile
* Issues in scalability
* It consumes more energy
* Data modification is difficult

Uses :-

* Smart contracts
* Crypto currencies
* Energy trading
* Health care

2. What is Linked list ?

A Linked list is a linear data structure , in which the element are not stored at contiguous memory location . The elements in a linked list are linked using pointer .



In simple words, a linked list consist of nodes where each node contains a data field and a reference link to the next node in the list .

Types :-

* Single linked list
* Circular linked list
* Double linked list
* Misc
* Quick links

3.What is SHA 256 hash ?

SHA-256 stands for Secure Hash Algorithm 256-bit and it's used for cryptographic security. Cryptographic hash algorithms produce irreversible and unique hashes.

SHA-2 is a set of cryptographic hash functions designed by the United States National Security Agency and first published in 2001. They are built using the Merkle–Damgård construction, from a one-way compression function itself built using the Davies–Meyer structure from a specialized block cipher. Digit sizes : 224, 256, 384 or 512 bits

4 .Why it is more secure than any other other techniques ?

Actually, its not so easy to decrypt the output from a hash function. There are different types of attacks employed to decrypt SHA. Following are the most famous ones.

1. Preimage attack - identifies a message that has a specific hash value.
   1. Birthday attack is an example of preimage attack. It take O(2^n/2) time where n is the output length of hash function (SHA2 its 512). To put things in context, Assuming 32 byte input (which is reasonable for your case - 20 bytes salt + 12 bytes password) my machine takes ~0,22s (~2^-2s) for 65536 (=2^16) computations. So 2^256 computations would be done in 2^240 \* 2^16 computations which would take

2^240 \* 2^-2 = 2^238 ~ 10^72s ~ 3,17 \* 10^64 years

2. Collision attack

3. Pseudo collision

SHA-1 which employs 256 bits is considered to be broken since, a collision was identified at 2^69 operations much less than 2^80.

None of the above attacks can crack an hash generated by SHA-1 or SHA-2 algo with the best of the hardware available on earth.

Coming to the other question about the tools available online to decrypt. They actually don’t crack the hash given by you. The tools just compare the hash available in their database. They maintain a database with computed hashes for some strings. When you try to test to encrypt your string on any of the websites, they save the hash and plain text in their database. Thus, when you try to decrypt the hash, you will get the result.

5.What is distributed data base ?

A distributed database is basically a database that is not limited to one system, it is spread over different sites, i.e, on multiple computers or over a network of computers. A distributed database system is located on various sites that don’t share physical components. This may be required when a particular database needs to be accessed by various users globally. It needs to be managed such that for the users it looks like one single database.

**Types :-**

**1. Homogeneous Database:**  
In a homogeneous database, all different sites store database identically. The operating system, database management system and the data structures used – all are same at all sites. Hence, they’re easy to manage.

**2. Heterogeneous Database:**  
In a heterogeneous distributed database, different sites can use different schema and software that can lead to problems in query processing and transactions. Also, a particular site might be completely unaware of the other sites. Different computers may use a different operating system, different database application. They may even use different data models for the database. Hence, translations are required for different sites to communicate.

**Distributed Data Storage :**

* **Replication –**
* **Fragmentation-**