Smart Contract Creation.

*Smart Contract :-

* Smart Contract are written in Codes and stored on the blockchain.
* It Ensures that they are immutable and cannot be altered after being deployed.
* It is used to automate various agreements.
* Agreements such as financial transaction, real estate transaction, supply chain management & more.
* Typically used in D-apps.

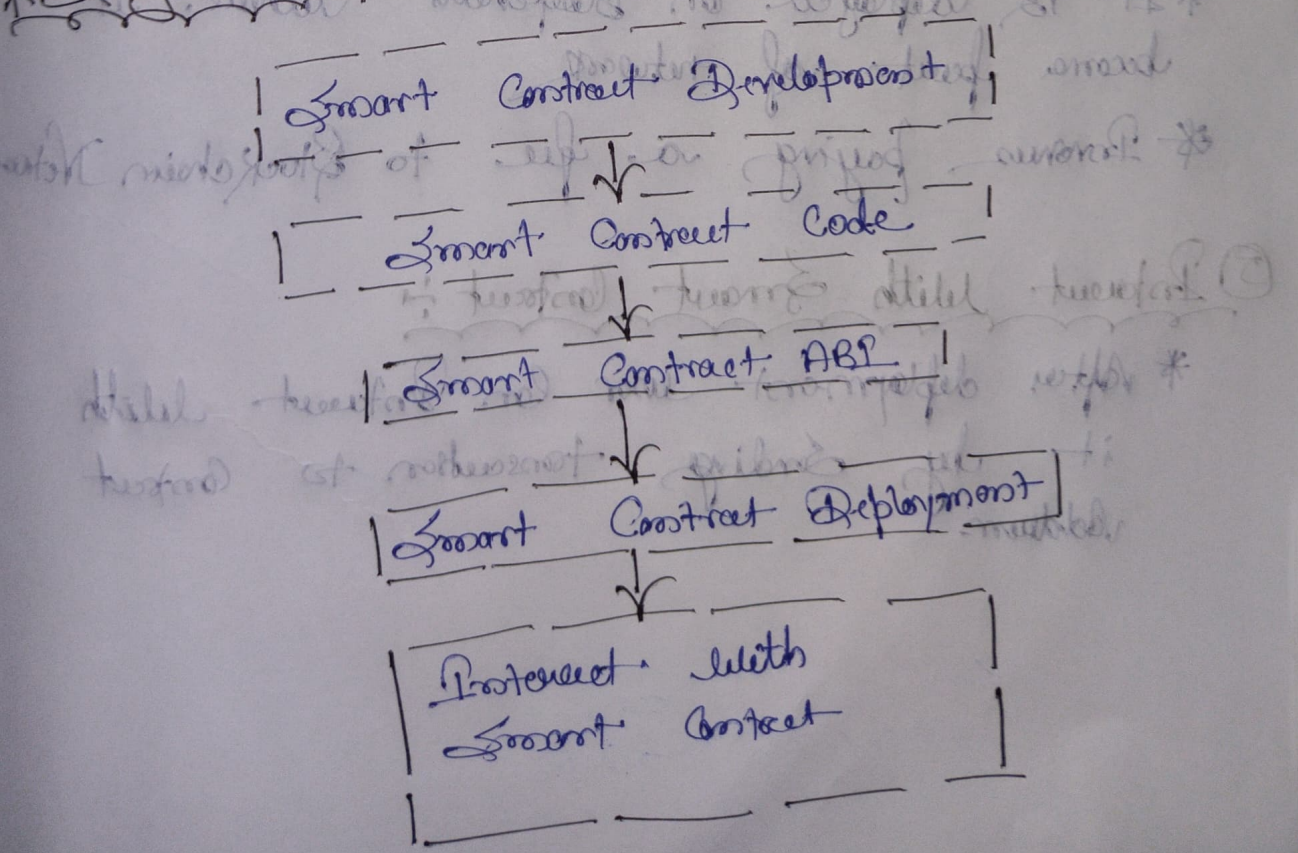
*Advantage of Smart Contract :-

* It provide several benefits like :-
  ① Efficiency ② Transparency & ③ Security.
* Reduce risk of fraud and Error.
* Powerful tool for automating and enforcing agreements.
* It have revolutionized many industries by streamling process and reducing cost.

* Creating Smart Contract :-

1. Connect to Ethereum Network
2. Create your app
3. Create an ethereum account
4. Add Ether
5. Check your Balance
6. Initialize project
7. Download Ganache
8. Create project
9. Add project folder
10. Write Contract
11. Connect Alchemy to project
12. Compile Contract
13. Deploy Contract.

* Diagram Representing Creation of Smart Contract :-



*. Working of Smart Contract Creation :-

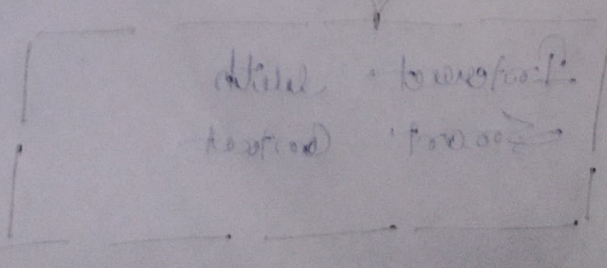
1. Smart Contract Development :- process of creating Smart Contract like writing of code and all.

2. Smart Contract Code :-
   - Codes are written in specific programming language like Solidity

3. Smart Contract ABI :-
   - Application Binary Interface is specification that define how to interact with Smart Contract.

4. Smart Contract Deployment :-
   * It is deployed on Blockchain where it become part of network
   * Persons paying a fee to Blockchain Netwo

5. Interact with Smart Contract :-
   * After deployment user can interact with it by sending transaction to Contract Address.

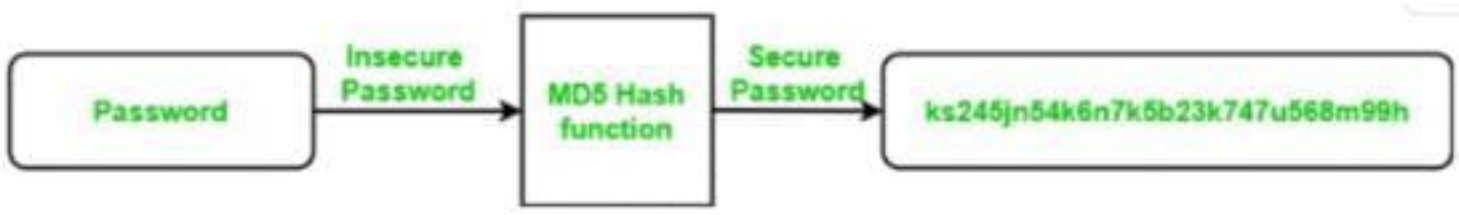


MD5 Algorithm Smart Contract:

MD5 is a cryptographic hash function algorithm that takes the message as input of any length and changes it into a fixed-length message of 16 bytes. MD5 algorithm stands for the message-digest algorithm. MD5 was developed as an improvement of MD4, with advanced security purposes. The output of MD5 (Digest size) is always 128 bits. MD5 was developed in 1991 by Ronald Rivest.

Use Of MD5 Algorithm:

- It is used for file authentication.
- In a web application, it is used for security purposes. e.g. Secure password of users etc.
- Using this algorithm, We can store our password in 128 bits format.



MD5 Algorithm

Working of the MD5 Algorithm:

- MD5 algorithm follows the following steps

1. **Append Padding Bits:** In the first step, we add padding bits in the original message in such a way that the total length of the message is 64 bits less than the exact multiple of 512.

Suppose we are given a message of 1000 bits. Now we have to add padding bits to the original message. Here we will add 472 padding bits to the original message. After adding the padding bits the size of the original message/output of the first step will be 1472 i.e. 64 bits less than an exact multiple of 512 (i.e. 512*3 = 1536).
Length(original message + padding bits) = 512 * i – 64 where i = 1,2,3 . . .

2. **Append Length Bits:** In this step, we add the length bit in the output of the first step in such a way that the total number of the bits is the perfect multiple of 512. Simply, here we add the 64-bit as a length bit in the output of the first step.
i.e. output of first step = 512 * n – 64
length bits = 64.
After adding both we will get **512 * n** i.e. the exact multiple of 512.

3. **Initialize MD buffer:** Here, we use the 4 buffers i.e. J, K, L, and M. The size of each buffer is 32 bits.
   - J = 0x67425301
   - K = 0xEDFCBA45
   - L = 0x98CBADFE
   - M = 0x13DCE476

4. **Process Each 512-bit Block:** This is the most important step of the MD5 algorithm. Here, a total of 64 operations are performed in 4 rounds. In the 1st round, 16 operations will be performed, 2nd round 16 operations will be performed, 3rd round 16 operations will be performed, and in the 4th round, 16 operations will be performed. We apply a different function on each round i.e. for the 1st round we apply the F function, for the 2nd G function, 3rd for the H function, and 4th for the I function.

Application Of MD5 Algorithm:

- We use message digest to verify the integrity of files/ authenticates files.
- MD5 was used for data security and encryption.
- It is used to Digest the message of any size and also used for Password verification.
- For Game Boards and Graphics.

Advantages of MD5 Algorithm:

Advantages of MD5 Algorithm:

- MD5 is faster and simple to understand.
- MD5 algorithm generates a strong password in 16 bytes format. All developers like web developers etc use the MD5 algorithm to secure the password of users.
- To integrate the MD5 algorithm, relatively low memory is necessary.
- It is very easy and faster to generate a digest message of the original message.

Disadvantages of MD5 Algorithm:

- MD5 generates the same hash function for different inputs.
- MD5 provides poor security over SHA1.
- MD5 has been considered an insecure algorithm. So now we are using SHA256 instead of MD5

- MD5 is neither a symmetric nor asymmetric algorithm.