HASHING : WHAT,WHY,HOW?

Did you ever thought how when you logged in any app you access your profile rather than another one or when you repeat the log in but an error shows that either your email or password is incorrect in this article we will talk about how hashing help identifying user credentials with ease and how we use them to store their data in the database.

WHAT IS HASHING ?

in simple words hashing is giving a unique value to any data (sentence,image,video...) for example :

To explain : the text Hello, World! have dffd6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f as a unique value that unique value is specific to that data they can't be two different data have one unique value this value is called a hash of the text Hello, World

HASH FUNCTION

To hash a data you must use a program called a hash function, this function will give a data as an input that data can be arbitrary size and will output a fixed size unique value there a lot of hash functions like Message Digest(MD) ,Secure Hash Function(SHA),BLAKE2...

5 RULES TO IDENTIFY IF A HASH FUNCTION IS CRYPTOGRAPHIC

For making the life more secure we must use hash functions that cryptographic to not let our data be tampered by third party, so we have to follow these 5 rules:

- **Deterministic** : The same input always will return the same output
- **Intractability** : The input can't be found from the output expect by trying gargantuan amount of possbile inputs
- **Colision-Safety** : The output is specific to one input they can't be two input with the same output
- **Avalanche Effect** : The smallest change in input return a different hash than the old one
- **Speed** : The hashing must be fast

SOME USE CASES FOR HASHING ?

Hashing can be important in a lot of cases from securing password to transfering money in the blockchain system, we will talk in this section about some of cases that we implement hashing at:

- Password Hashing : in this new world of social media passwords are important and can be easily trackable so the right solution to secure password is storing the hash of them in the database to not hackers see the password when the database is hacked
- Verifying User Credentials : when the password's hash is stored in the database we must verify if the user who logged in is the right one so we get the email and the password from the application and we hash them then we do the same to the credintials in the database then we compare the two hashes if it's compatible then the user logged in if not we show an error that either the email or password or both is incorrect