**Cryptographic Hashing**
Hashing functions are an essential part of cybersecurity and some cryptocurrency protocols such as Bitcoin.

**What is hashing?**
Hashing is a method of cryptography that converts any form of data into a unique string of text. Any piece of data can be hashed, no matter its size or type. In traditional hashing, regardless of the data's size, type, or length, the hash that any data produces is always the same length. A hash is designed to act as a one-way function—you can put data into a hashing algorithm and get a unique string, but if you come upon a new hash, you cannot decipher the input data it represents. A unique piece of data will always produce the same hash.

**How does it work?**
Hashing is a mathematical operation that is easy to perform, but extremely difficult to reverse. (The difference between hashing and encryption is that encryption can be reversed, or decrypted, using a specific key.) The most widely used hashing functions are MD5, SHA1 and SHA-256. Some hashing processes are significantly harder to crack than others.

**Who uses hashing?**
The average user encounters hashing daily in the context of passwords. For example, when you create an email address and password, your email provider likely does not save your password. Rather, the provider runs the password through a hashing algorithm and saves the hash of your password. Every time you attempt to sign in to your email, the email provider hashes the password you enter and compares this hash to the hash it has saved. Only when the two hashes match are you authorized to access your email.

**Hashing in Cryptocurrencies**
In the Bitcoin blockchain, *mining* is essentially conducted by running a series of SHA-256 hashing functions. In cryptocurrency blockchains today, hashing is used to write new transactions, timestamp them, and ultimately to add a reference to them in the previous block. When a block of transactions is added to the blockchain, and consensus is reached among operators of different nodes (validating that all of them have the right and true version of the entire ledger), it is nearly impossible to reverse a transaction due to the enormous computing power that would be required by anyone attempting to tamper with the blockchain, and the one-way nature of the hashing. Hashing is therefore crucial to maintain the cryptographic integrity of the blockchain.

**Hashing and Cybersecurity**
When an organization discovers that a platform's passwords have been compromised, it usually means that hackers have acquired the hashes that represent the passwords. Hackers then run the hashes of common words and combinations of common words and numbers to decipher some of the passwords that users have saved. The cybersecurity industry now uses a mechanism called 'salting'. Salting includes adding random data to a password before hashing it, and then storing that 'salt value' with the hash. This process makes it harder for hackers to use pre-computation techniques and crack passwords of hashed data that they have acquired.
Cryptographic hashing has long played a role in cybersecurity, and is now poised to power the coming wave of blockchain applications.