“New Approach as Blockchain and Cryptography Combination” : Combo Nature System

SYNOPSIS

Blockchain is a peer-to-peer network; the word ‘blockchain‘ is made up of two separate terms, ‘block’ and ‘chain’. A block being referred to a collection of data, alias data records, and chain being referred to a public database of these blocks, stored as a list.

These lists are linked using cryptography, making it the most essential and fundamental requirement for creating a blockchain. Blockchain is a growing list of records, and the blocks get appended to the list with time. Cryptography in blockchain can be a tricky concept, but we have tried to simplify it for your better understanding.

Cryptography is a method of developing techniques and protocols to prevent a third party from accessing and gaining knowledge of the data from the private messages during a communication process. Cryptography is also made up of two ancient Greek terms, Kryptos and Graphein, the former meaning “hidden” and latter being “to write”. There are several terms related to cryptography, which are stated as follows:

Encryption: It is a process of plaintext (normal text) to a ciphertext (random sequence of bits).

Decryption: The inverse process of encryption, conversion of ciphertext to plaintext.

Use of Cryptography in Blockchain

Blockchains make use of two types of cryptographic algorithms, asymmetric-key algorithms, and hash functions. Hash functions are used to provide the functionality of a single view of blockchain to every participant. Blockchains generally use the SHA-256 hashing algorithm as their hash function.

Cryptographic hash functions provide the following benefits to the blockchain:

- Avalanche effect – A slight change in the data can result in a significantly different output.
- Uniqueness – Every input has a unique output.
- Deterministic – Any input will always have the same output if passed through the hash function.
- Quickness – The output can be generated in a very small amount of time.
- Reverse engineering is not possible, i.e. we cannot generate the input by having the output and the hash function.

Hash functions have a major role in linking the blocks to one another and also to maintain the integrity of the data stored inside each block. Any alteration in the block data can lead to inconsistency and break the blockchain, making it invalid. This requirement is achieved by the property of the hash functions, called the ‘avalanche effect’.

According to this, if we make even a slight change in the input to the hash function, we will end up getting a totally unrelated output as compared to the original output. Let us take an example of an SHA-256 hash function, and compare their outputs,

Input: Blockchain at myfort

Output:
04f0ecc95159533982d7571eada5f8d76592b6e97ead964467c603d31b9e7a9c

Input with a slight difference: Blockchain at myfort

Output:
80b069904b6a8db46ed94e7091ff4e5fc72fae5422d46cc57d8f66db7abf4781

You can notice the huge difference in output after changing a single character at the input from lowercase to uppercase. This makes the data reliable and secure on the blockchain; any changes in the block data will

lead to this difference in hash value and make the blockchain invalid, making it immutable.

One of the major parts of asymmetric-key cryptography is digital signatures. Digital signatures provide integrity to the process; they are easily verifiable and cannot be corrupted. They also hold the quality of non-repudiation, making them similar to the signatures in the real-world. The digital signatures ensure that the blockchain is valid and the data is verified and correct.

Hashing, public-private key pairs, and the digital signatures together constitute the foundation for the blockchain. These cryptographic features make it possible for blocks to get securely linked by other blocks, and also ensure the reliability and immutability of the data stored on the blockchain.

There are a huge number of applications of blockchain technology, and cryptography makes it possible. One of the major real-world applications of cryptography in the blockchain is cryptocurrencies.

One of the major parts of asymmetric-key cryptography is digital signatures. Digital signatures provide integrity to the process; they are easily verifiable and cannot be corrupted. They also hold the quality of non-repudiation, making them similar to the signatures in the real-world.

The digital signatures ensure that the blockchain is valid and the data is verified and correct.

Hashing, public-private key pairs, and the digital signatures together constitute the foundation for the blockchain. These cryptographic features make it possible for blocks to get securely linked by other blocks, and also ensure the reliability and immutability of the data stored on the blockchain.

There are a huge number of applications of blockchain technology, and cryptography makes it possible. One of the major real-world applications of cryptography in the blockchain is cryptocurrencies.

Conclusion

Blockchain technology has been in the key focus areas of development for all the multinational companies and also a huge number of startups are emerging in this technology from the past few years. Blockchain is yet to witness its mainstream usage in society, yet there are numerous opportunities for professionals to explore and develop their careers in this field; one of which is cryptography in blockchain for sure.

Software Requirements:

Python IDE(Online/Offline)
* We will Mainly use Google Collab for better performance, easy execution and platform Independent.

Hardware Requirements:

Any Hardware as Mobile, Ipad, Laptop or Desktop will work

Programming:

Project will be in Python Programming.