BIDISHA CHAKRABORTY — Published On July 22, 2022

Beginner Blockchain

This article was published as a part of the Data Science Blogathon.

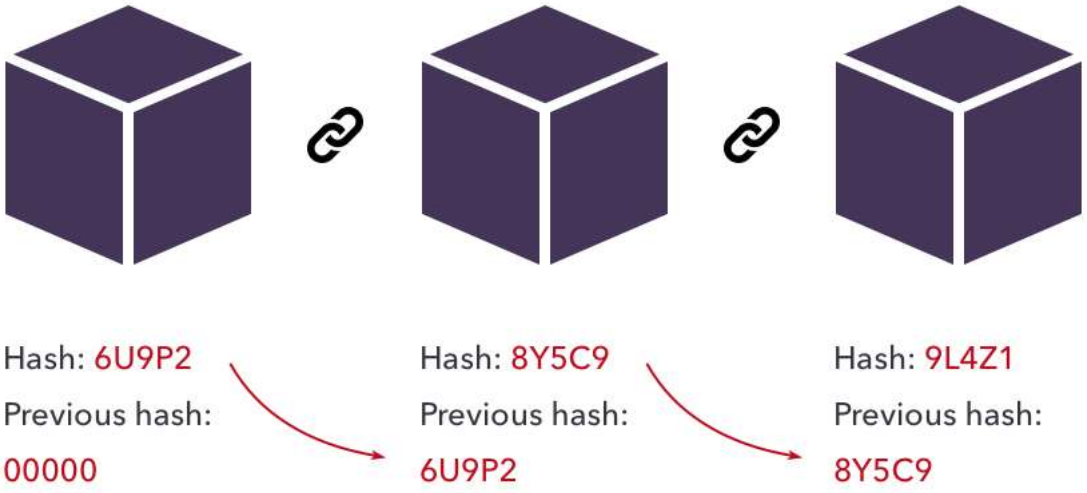
Introduction

Blockchain is a decentralized, distributed ledger that comprises blocks. The Blocks are connected to form a long chain. Each block comprises an address to the previous block and some information. The address part is done with the help of hashing. The information comprises data such as transactions and is encrypted. Blockchain was first implemented in the year 2008 by a group of people named Satoshi Nakamoto. Blockchain uses strong cryptographic methods to manage the whole network.

Terms Related to Blockchain

Before diving deep into more, let us be familiar with the five most important things: Block, miner, node, Block Reward and Cryptography.

1. Block: A block is the unit of blockchain that contains information in encrypted form. The blocks are connected. It is also called an immutable record as it cannot be reverted once created. There are three types of Blocks: Genesis Block, Valid Block and Orphan Blocks. Genesis Block is the first block that is created at the start of the blockchain. Valid Blocks are the blocks validated by miners and added to the blockchain. Orphan Blocks, as the name suggests, they are not added to any blockchain.
2. Miner: Blockchain Mining comprises of verification of transactions. Since blockchain is highly decentralized, no authority can verify and secure the transactions. Miners are the users of the technology who verify the transactions. After successful verification, they get incentives.
3. Node: Nodes are devices in which blocks are stored. The nodes also have a database that stores the history of transactions and is connected.
4. Block Reward: A block reward is an incentive that is given to miners when they participate in the validation of the blocking process. It has two parts: block subsidy and transaction fees.
5. Cryptography: It is a practice used in this technology to encode and decode data. The aim is to protect data with the help of codes. The techniques used are a part of security protocols to prevent unauthorized access from third parties. The word is made up of two terms ‘Krypto’ means ‘hidden’ and ‘Graphy’ means ‘written’.



Structure of Blockchain

Source:https://www.velotio.com/engineering-blog/introduction-to-blockchain-and-how-bitcoin-works

Working of Blockchain

The working is a multistep process, but it involves four phases: the creation of the block, verification of the block, the addition of the block and updation of the database. The steps are as follows:

- An authentic user requests a transaction.
- A block is created in which the transaction or any other data is specified.
- The block is circulated all over the network. Blockchain protocols do this.
- Miners verify the block. Upon successful verification, the miners get incentives.
- After the successful transaction, the database is added.

Cryptographic Primitives

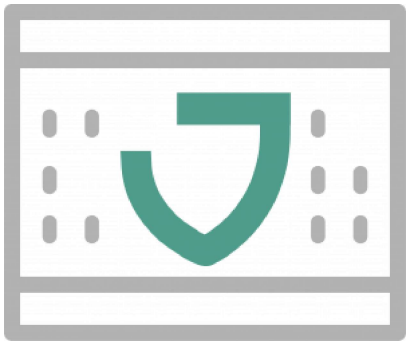
primitives

Cryptographic Primitives are the tools used to build security protocols, which comprise low-level algorithms. Security protocols are nothing but algorithms that are developed by Cryptographic designers using Cryptographic Primitives as tools, and these protocols are executed when certain conditions are met. Since Blockchain is highly decentralized in nature, the security of data is of utmost importance. For example: Suppose two users want to exchange information on a public Blockchain. In Public Blockchain, everybody can see the transaction process. To secure the data, encryption algorithms are used. For decrypting, the data decryption algorithms are used. These cryptographic primitives are used to develop these high-level secured algorithms.

protocols

Block Cipher and Stream Cipher belongs to the symmetric key cipher. These two block ciphers and stream cipher are the methods used for converting the plain text into ciphertext.

The main difference between a Block cipher and a Stream cipher is that a block cipher converts the plain text into cipher text by taking plain text's block at a time. While stream cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time.



Cryptographic Primitive

Source:https://credential.eu/trustee/trustee-primitives-and-components/trustee-components-cryptographic-primitives/

Cryptographic Protocols

the rules that secure the whole blockchain network. The rules are made using cryptographic primitives as the base. They are transparent as they are programmed. The goal of these protocols is to provide data integrity, secure the exchange of data, and maintain the security of the whole network. Hence they are often known as security protocols. Commonly used cryptographic protocols are Bitcoin, Hyperledger, Ethereum, Corda etc.

Combining Cryptographic Primitives

As we all know, each cryptographic primitive is highly specific, and they are the building blocks of any crypto protocols. So each crypto protocol performs a single task. The primitives are limited, and developing them is a tedious task. This is because they are low-level programs and requires complex mathematical analysis. So designers usually combine one or more cryptographic primitives to establish strong crypto protocols so that the protocols can at least tackle the other small problems besides the main problem. For instance, hashing and encryption methods can be combined.

Commonly used Cryptographic Primitives

There are many cryptographic primitives, but we will discuss the most commonly used ones. They are as follows:

1. **One-way hash function:** It is a mathematical function which converts an input of any length to a binary sequence of fixed length. It cannot be reverted, which means the original string cannot be retrieved back from the hash. It is to be noted that even a small change in the input can change the meaning of the whole output. For example, SHA256 is a hash function. It generates 32-byte strings for any input.
2. **Symmetric Key Cryptography**: It is a popular encryption algorithm and is also known as symmetric encryption. The principle of this algorithm is a shared key. For example, a person wants to send some confidential data. He/She encrypts the data and 'locks' it with a key. The same key is used to decrypt or 'unlock' the data when the message is received. This algorithm is mostly used when large amounts of data are sent. The problem is sharing the key. The sender and receiver parties should have the same key. Examples of Symmetric key Cryptography are AES, DES, and 3DES.
3. **Asymmetric key cryptography**: It is also known as public key cryptography. This method has been developed to cope with the disadvantage of Symmetric Key Cryptography. Two types of keys are used: Public key and private key. The public key is used to encrypt the message, whereas the private key decrypts the message. Examples are: Diffie-Hellman, DSA and RSA
4. **Digital Signature**: This is used in blockchains to authenticate transactions or other data. Whenever a digital signature is used, it establishes that the rightful owner has sent it and the message has not been altered. The here private key is used as a digital signature by the user, and once it has been sent to the receivers, the receivers validate the message using the public key.
5. **Private Information Retrieval:** This protocol allows users to retrieve information from the database without other users knowing about it. Here the user can anonymously retrieve the information from another server.

Conclusion

Let us recap important points from the article here:

- Cryptographic Primitives are building blocks of Blockchain security. They form the baseline of the security protocols.
- Although complex, these are highly reliable and can be used to develop any security protocols with certain changes.
- The crypto designers must choose and combine the primitives so that there are no flaws and the whole tech is completely safe and secure.

blockchain blogathon