A Brief Glance at Cryptography

Original:
https://www.btcc.com/en-US/academy/crypto-basics/a-brief-glance-at-cryptography

What is Cryptography?

The “crypto” in the word “cryptocurrency” means “secret” in Greek – which gives you a clue as to what the field of cryptography is all about. Cryptography is the study and practice of sending secure, encrypted messages or data between two or more parties. The sender “encrypts” the message, which obscures its content to a third party, and the receiver “decrypts” the message, making it legible again.

Cryptocurrencies use cryptography to allow transactions to be anonymous, secure, and “trustless,” which means you don’t need to know anything about a person to safely make transactions with them – and you don’t need bank, credit-card company, government, or any other third party in the middle. And cryptography isn’t just important for digital money — our computer and the networks it’s attached to are encrypting and decrypting data constantly, from every Google search you make to every email you send.

In short, cryptography is the study and practice of sending secure, encrypted messages between two or more parties. Cryptography allows digital currency transactions to be pseudonymous, secure, and “trustless” – with no bank or other intermediary required.

Why is Cryptography Needed?

Cryptocurrencies are entirely based on cryptographic ideas. Bitcoin was invented by a pseudonymous person (or group of people) going by the name of Satoshi Nakamoto, who proposed the idea in the form of a whitepaper posted to a cryptography message board in 2009.

The thorniest issue that Nakamoto solved was something called the double-spend problem. Because Bitcoin is just code, what’s to stop a person from making and spending multiple copies of their money? Nakamoto’s solution was based on a well-known encryption arrangement known as public-private key encryption.

Bitcoin (as well as Ethereum and many other cryptocurrencies) uses a technology called public-private key encryption. This allows them to be “trustless” – and makes secure transactions between strangers possible without a “trusted intermediary” like a bank or Paypal in the middle.

How do Private Key and Public Key Work?

The Bitcoin network issues all users a private key (essentially a really strong password) from which it cryptographically generates a linked public key. You can freely give people your public key – in fact, that’s the only piece of information anyone needs to send you Bitcoin. But to access those funds, the private key is required.

Part of what makes Bitcoin revolutionary is its solution for the double-spend problem: A peer-to-peer network that uses cryptographic methods to verify the authenticity of transactions.

Your public key is generated from your private key via a method called “hashing” – which is taking a string of data and processing it through an algorithm. It’s virtually impossible to reverse this process, so nobody can guess your private key from your public key.

Because your public and private keys are linked, the network knows that your bitcoin belong to you – and will remain yours as long as you have your private key.

Another impact of not having an intermediary is that Bitcoin transactions are irreversible (after all, there is no credit-card company to call if you make a mistake). But this is a feature, not a bug: permanent transactions are a key part of the solution to the double spend problem.

The other half of the solution is the Bitcoin blockchain, which is a giant, decentralized ledger – imagine a bank’s balance books – that documents every transaction and is constantly verified and updated by all the computers in the network.