CRYPTOCURRENCY & CYBER SECURITY

Arjun vankani – 180210107060 GUIDE: Prof. Karshan Kandoriya

WHAT IS CRYPTOCURRENCY?

Cryptocurrency is digital or virtual currency, which is transparent, decentralized, and secured by cryptography.

The global economy is moving toward the digital world, and from investments to money transfer, everything is becoming digital. Here, the newest and most promising digital payment system has come into the market, which is **cryptocurrency**.

Cryptocurrency, also known as crypto, is a type of online payment method that can be exchanged online to purchase goods and services. It is much similar to real-world currency, but it does not have any physical appearance.

It **is encrypted, transparent, and decentralized** digital money, which is based on **blockchain** technology. There are approximately 5000 different types of cryptocurrencies, among which **Bitcoin and Ethereum** are the popular ones.

FEATURES

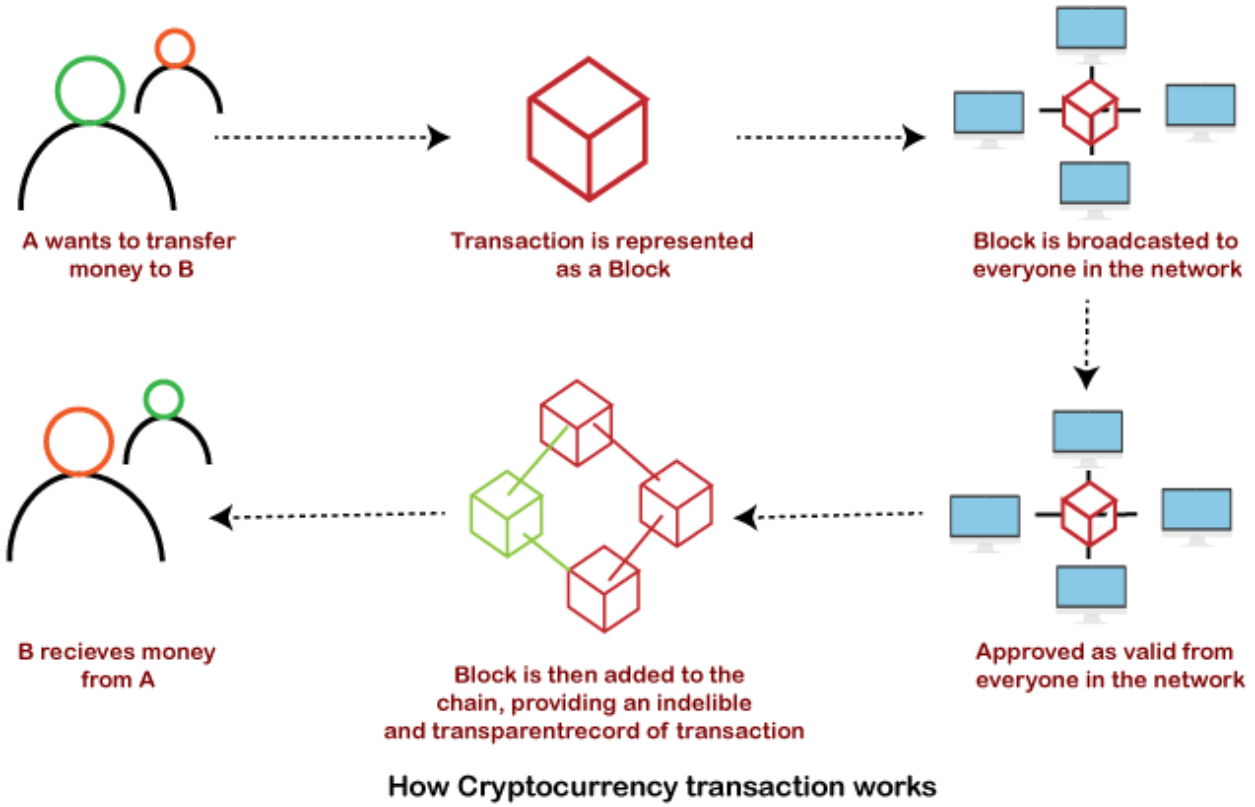
It has a limit to how many units can exist, such that bitcoin has 21 million limits.

It performs easy verification of transfer of funds with the help of hashing algorithms that verify each transaction.

It is independent of any central authority or a bank.

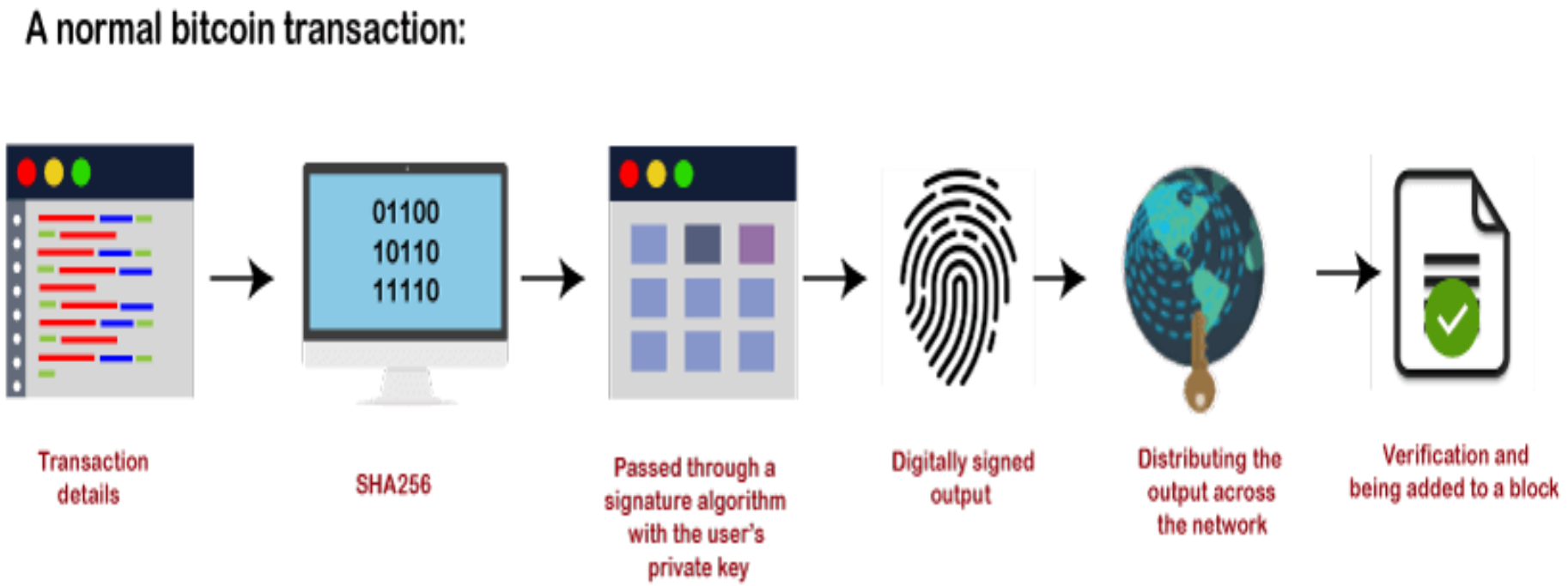
The new units can only be added after certain conditions are met.

HOW DOES CRYPTOCURRENCY WORKS?



How Cryptocurrency transaction works

Crypto is used for cryptography, which is a technique of encryption and decryption for secure communication between two parties. The cryptography technology usually uses a computational algorithm such as **SHA256**, a public key, and a private key. The public key is shared with everyone, and a private key is like the digital signature of the user.



CRYPTOCURRENCY MINING ALGORITHMS:

Cryptocurrencies makes use of different algorithms named as hashing algorithms.

By the way, Hash is a “message digest” -a number generated from a string of text, the hash itself is smaller than the text, it’s almost impossible to generate another string of text with the same hash value.

There are different hashing algorithms used for various cryptocurrencies such as:

1. SHA-256
2. ETHASH
3. SCRYPT
4. EQUIHASH
5. CRYPTONIGHT
6. X11

WHAT IS A BLOCKCHAIN?

A blockchain is a decentralised, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without altering the subsequent blocks and the collusion of the network. Each block contains three things:

1. A cryptographic hash for previous block
2. A timestamp
3. Transaction data

Blockchains makes use of security methods such as public key cryptography.

CRYPTOCURRENCY SECURITY STANDARDS

This includes cryptocurrency exchanges, mobile, and web applications.

For increasing cryptocurrency security, it is better to have an information system having cryptocurrency Security standards. Cryptocurrency Security Standards (CCSS) allow the end-users to make smart choices and decisions for purchasing and investing in the right services.

Cryptocurrency Security Standards:

- Key/seed generation
- Wallet Creation
- Key Storage
- Key Usage
- Key Compromise policy
- Keyholder Grant/ Revoke Policy and Procedures
- Third-party audits
- Data Sanitization Policy
- Proof of Reserve
- Log Audits

RISKS THAT OCCUR ARE AS FOLLOWS

1. Leaving cryptocurrency on a single exchange making it more prone to hackers.
2. Keeping Cryptocurrency locally can have consequences like data can be lost or stolen, as local storage is vulnerable, and someone can track down your transaction and steal it.
3. Another risk is when someone targets you specifically, then Email phishing attacks are prevalent. Also, some standard methods and techniques leading to personal attacks like SIM Swap assaults for clearing the 2-way authentication are used.

WAY TO PROTECT YOUR DIGITAL INVESTMENTS:

- Thorough Run Research on Exchanges
- Store your Cryptocurrency Safely
- Using a Hybrid Strategy will be a wise investment
- Use a strong password
- Use trustworthy wallets

Keep the key secret

STEPS TO PREVENT YOUR CRYPTOCURRENCY FROM CYBER ATTACKS

- Try to avoid storing cryptocurrency on digital storage.
- Invest in buying a cryptocurrency hardware wallet.
- Do not use public WIFI while making transactions.
- Use private and secured internet connection.
- Also, make sure to keep the security level high and do not install any unsecured apps.
- Use 2-stage authentication and verification for better secure transactions.
- Make sure to stay away from the bitcoin gambling sites.
- Hold cryptocurrency privately.
- Put a unique and robust password.
- Do not share your passwords, key, and wallet details with anyone.

THANK YOU SO MUCH