ETHEREUM 2.0 MASTERY PROGRAM

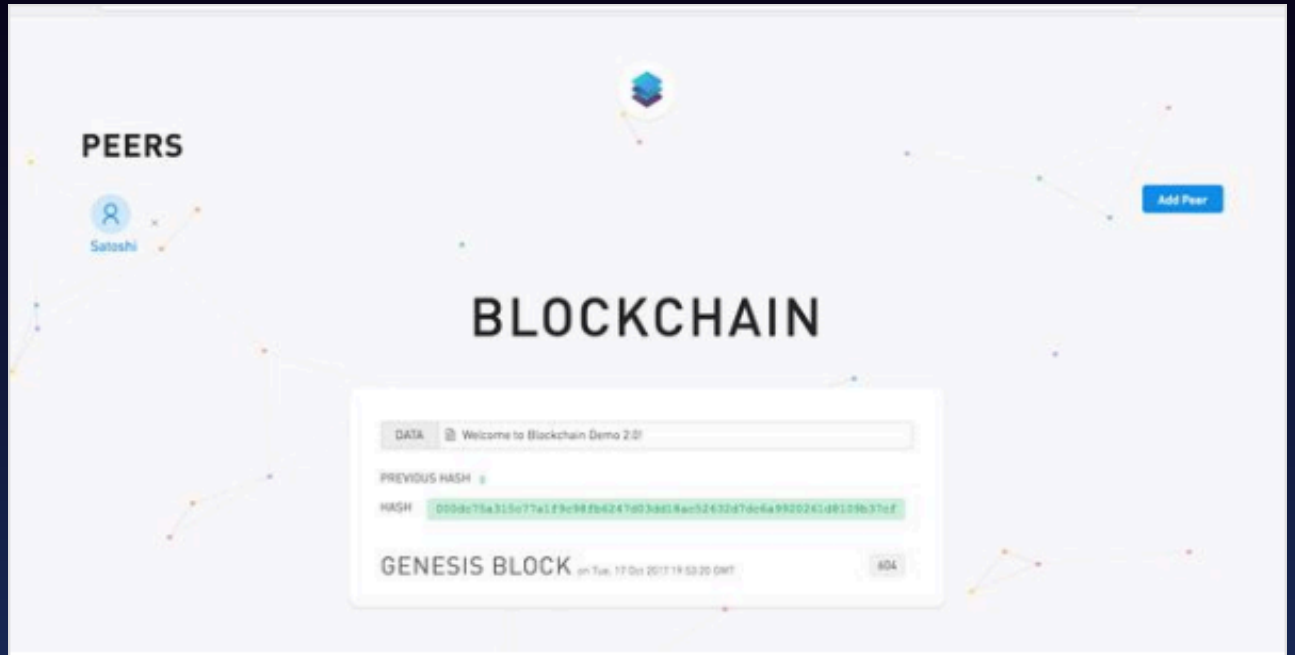
Instructor: Raja Rizwan Saleem

MODULE-2

BLOCKCHAIN AND SMART CONTRACT BASICS

Raja Rizwan Saleem
Lead Blockchain Trainer

Class-03

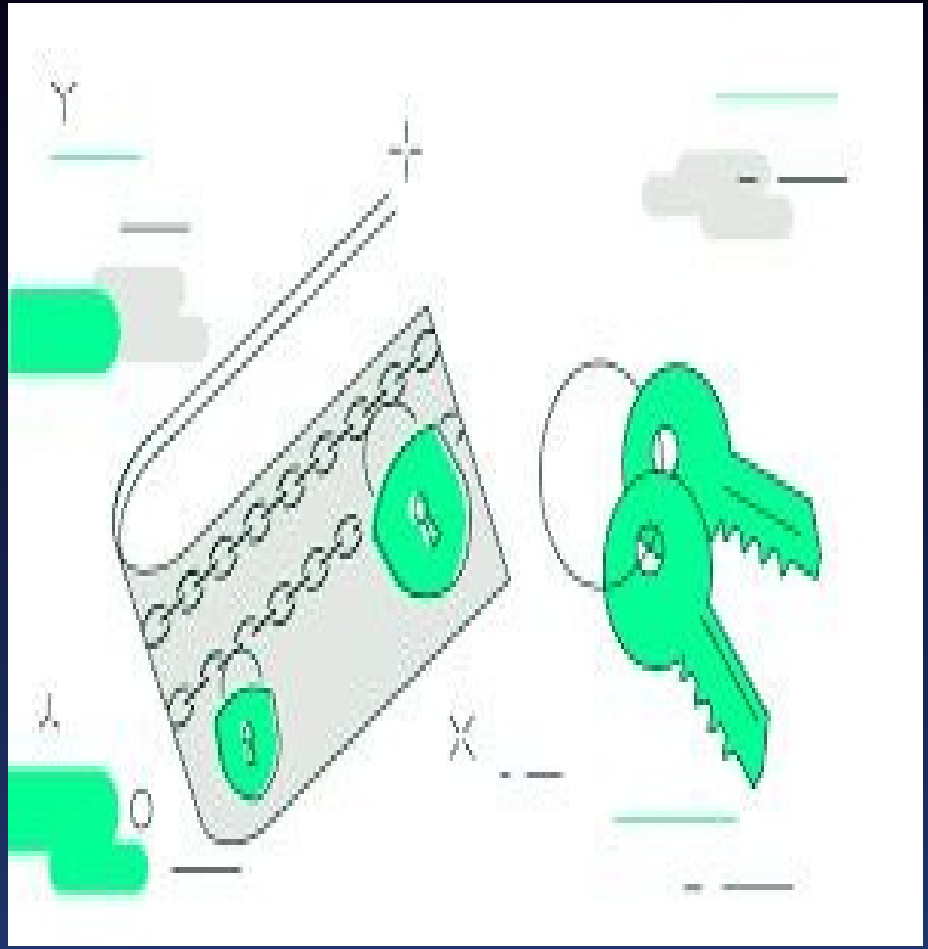


Blockchain Demo

A visual demo of the blockchain data structure

sean_j_han

Wallet & Keys



Wallet & Keys


EVERY CRYPTO WALLET HAS
A PUBLIC KEY
A public key allows users to receive cryptocurrency transactions. It is public and open to anyone in the system.
A PRIVATE KEY
A user's private key proves ownership of their respective public key. It must be stored separately and kept secret.

Wallet & Keys


Private Key
(only visible to you)
Algorithmic
Transformation
Public Key
Hash
Function
Address
(visible to everyone)

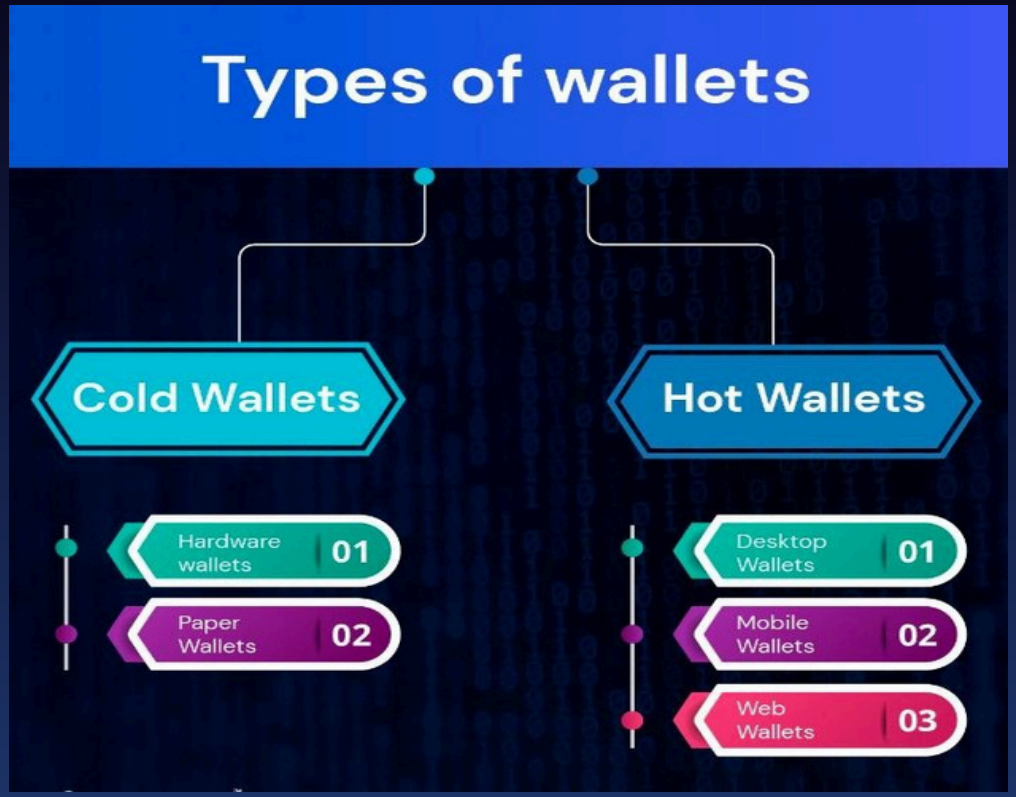
Wallets

A digital wallet (or electronic wallet) is a software-based system or an application that runs on any connected device. It stores your payment information and passwords of numerous payment methods and websites. Digital wallets run primarily on mobile devices but may be accessible from a computer — mobile wallets, which are a subset, are primarily used on mobile devices.

Wallets in Blockchain

- A wallet is software that keeps one or more cryptographic private and public keys.
- Using these keys, you can interact with different blockchains and are allowed to send and receive digital currencies.
- You can also interact with smart contracts using any of the accounts present in your wallet.

Types of Wallets



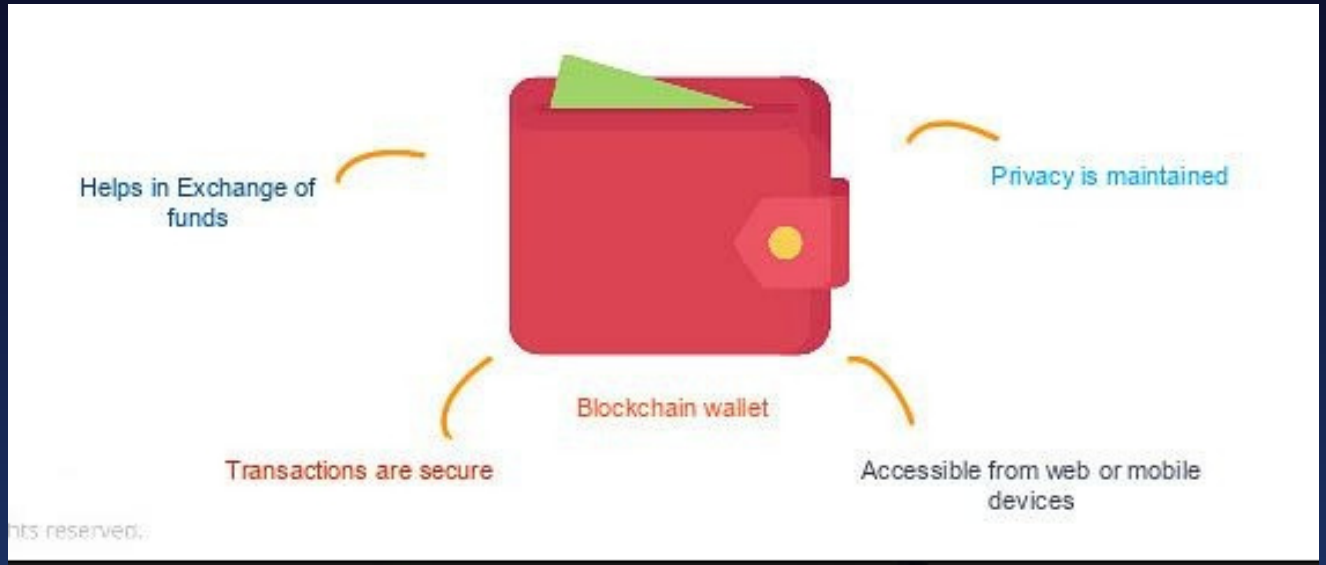
Digital Wallets

- Digital wallets are financial applications that allow you to store funds, make transactions, and track payment histories on devices like phones and tablets.
- You can store all of your financial information in a digital wallet; some even let you store identification cards and driver's licenses.
- Digital wallets may be included in a bank's mobile app or payment apps like PayPal or Alipay.
- Digital wallets allow people in financially underserved parts of the world to access financial services they may not have been able to before.

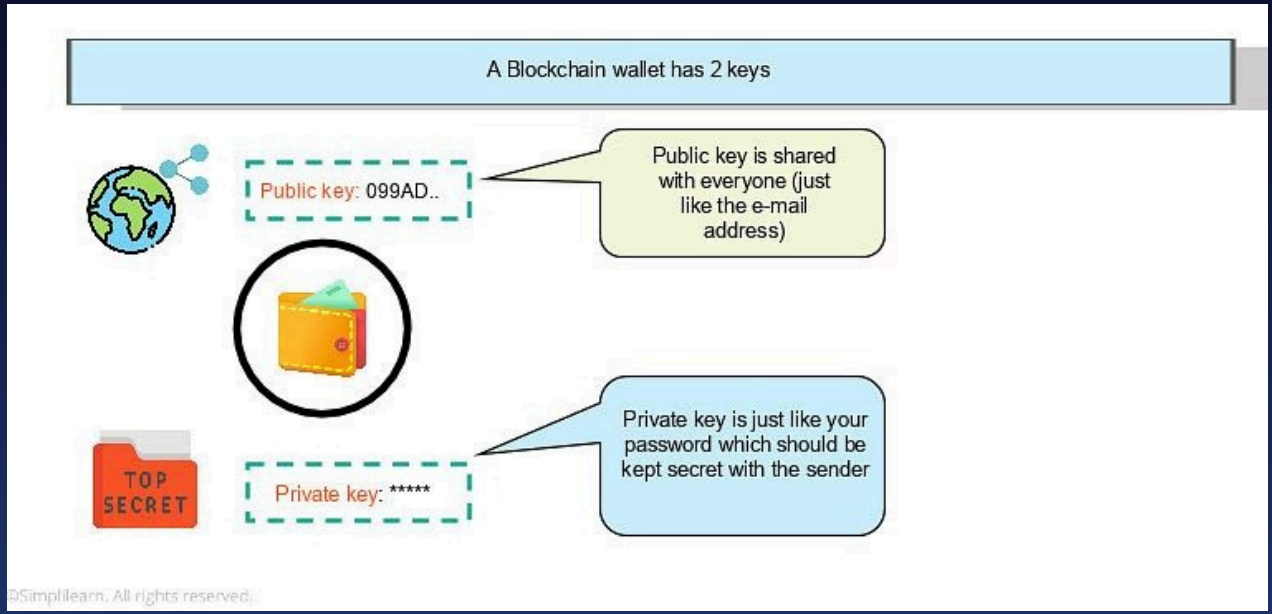
Digital Wallets

- Digital Wallet is simply an E-Wallet
- You are even using it without Bitcoin, like your digital bank applications, Apple Pay & Google Pay (with your credit / debit card)
- But through Digital Wallet you are ready to spend digital cash
- Purpose of the wallets is to save your passwords
- Type of Digital Wallets
    - Desktop
    - Online
    - Mobile
    - Hardware (Flash Drive USB)
    - Paper Wallet

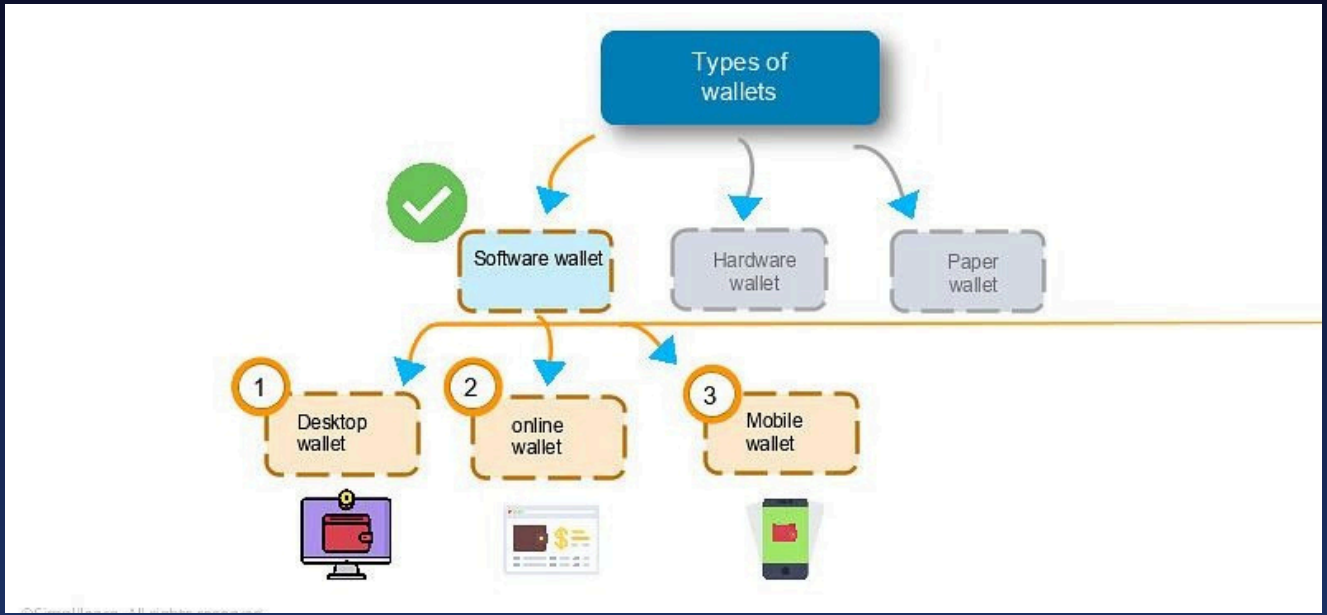
Blockchain Wallet



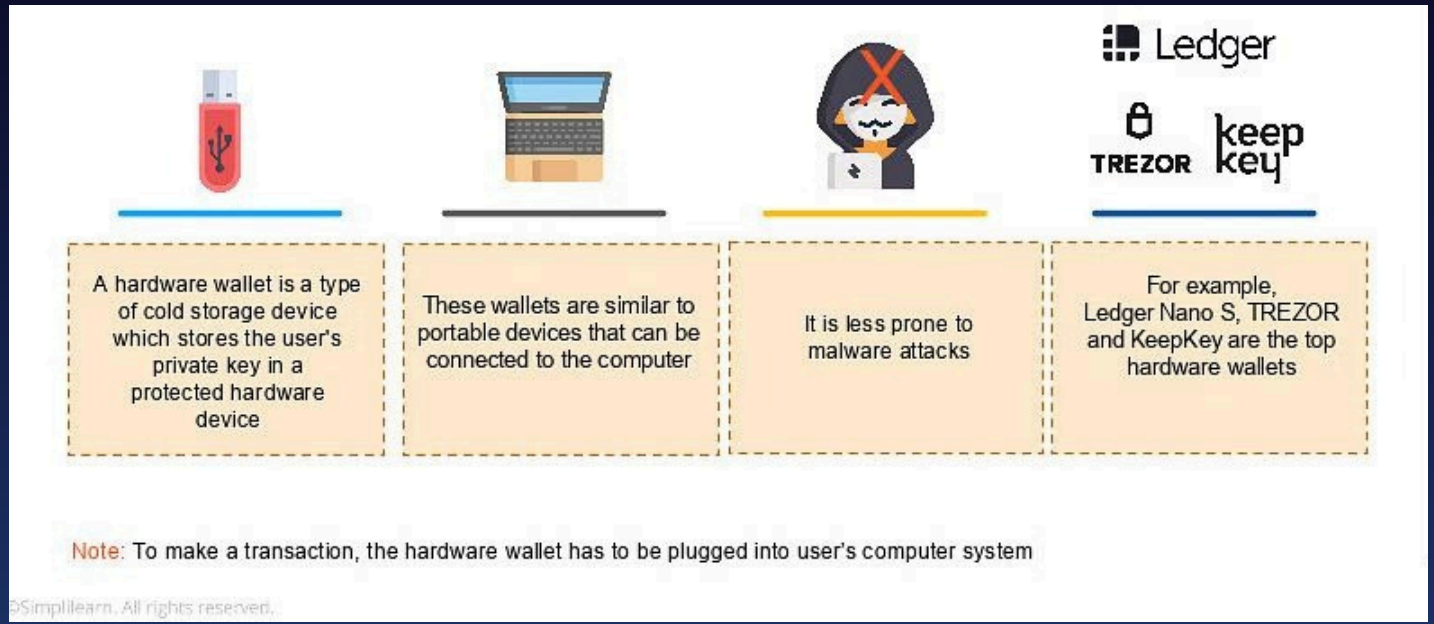
Blockchain Wallet



Types of Wallets

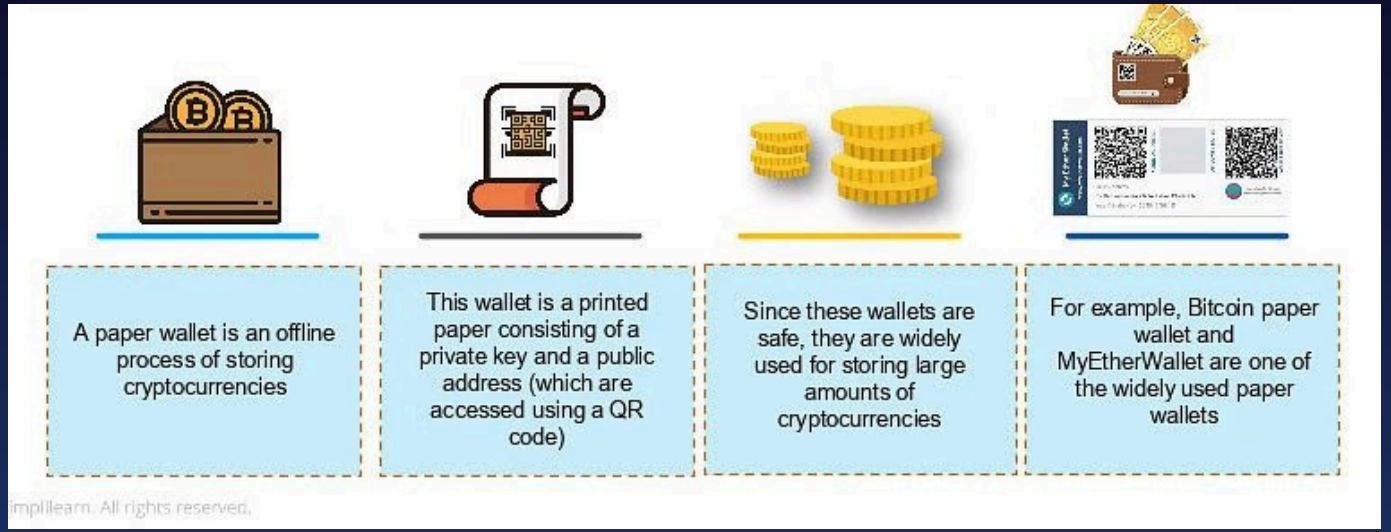


Hardware Wallets



Hardware Wallets

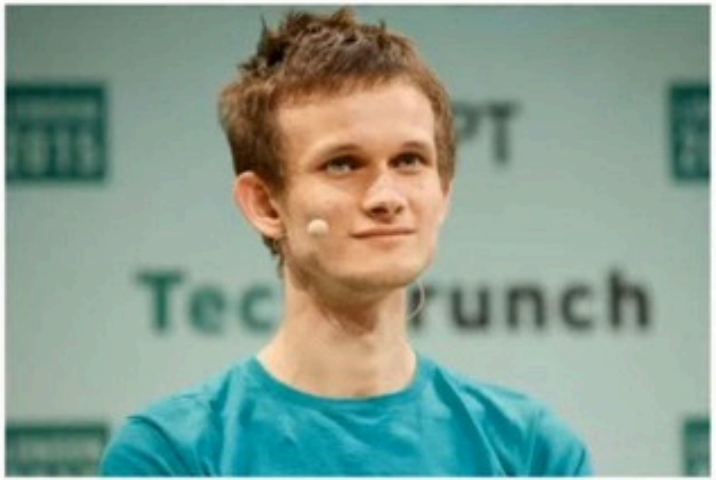
Paper Wallets



Prerequisite

1. Understanding of Blockchain
2. Understanding of Ethereum Blockchain
3. Fundamentals of Programming

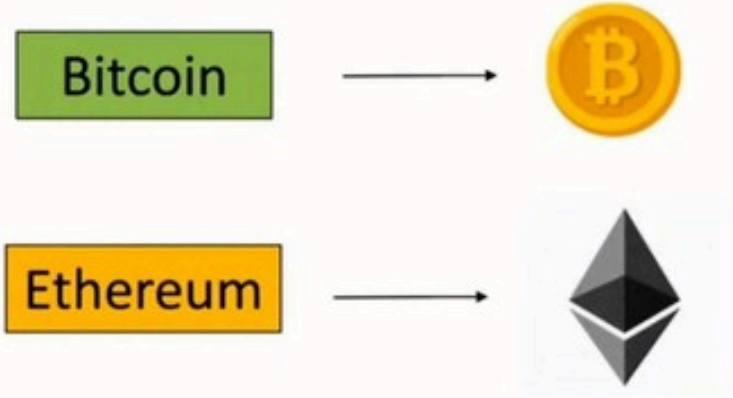
Ethereum



Vitalik Buterin

What is Ethereum?

- **Ethereum** is an open-source blockchain-based platform.



Ethereum Currency Units

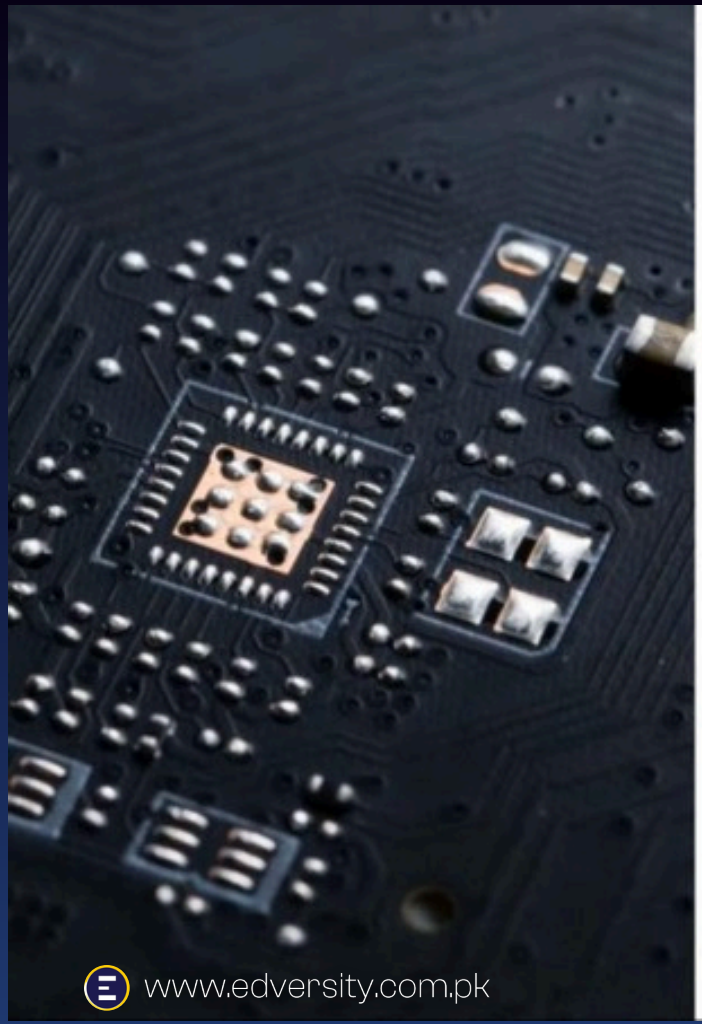
1. Ethereum's currency unit is called *ether*
2. It identified as "ETH" or with the symbols Ξ (from the Greek letter "Xi" or, less often, ♦
3. For example: 1 ether, or 1 ETH, or Ξ1, or ♦1

Ether Smallest Unit = WEI

ethereum

1. Ether is subdivided into smaller units, *wei*.
2. One ether is 1 quintillion wei (10^18 or 1,000,000,000,000,000,000).
3. Ethereum is the system, ether is the currency.
4. When you transact 1 ether, the transaction encodes 1,000,000,000,000,000,000 wei as the value.

Value (in wei)	Exponent	Common name	SI name
1	1	wei	Wei
1,000	10^3	Babbage	Kilowei or femtoether
1,000,000	10^6	Lovelace	Megawei or picoether
1,000,000,000	10^9	Shannon	Gigawei or nanoether
1,000,000,000,000	10^{12}	Szabo	Microether or micro
1,000,000,000,000,000	10^{15}	Finney	Milliether or milli
1,000,000,000,000,000,000	*10^{18}*	*Ether*	*Ether*
1,000,000,000,000,000,000,000	10^{21}	Grand	Kiloether
1,000,000,000,000,000,000,000,000	10^{24}		Megaether



Ethereum Gas Limit

Gas Limit

Let say A wants to send B 2 ETH. So what will be the total fees A that has to pay ?

A sets the gas price per unit = 100 gwei.

Transaction gas limit = 21,000 units.

Total fee will be: Gas units(limit) * Gas price per unit

Total fee will be: `21,000 * 100 = 210,0000` gwei or 0.0021 ETH

Gas Limit

Let say A wants to send B 2 ETH. So what will be the total fees A that has to pay ?

Case 2: When gas transaction limit < 21000 units.

Transaction gas limit = 20,000 units.

Transaction Fail

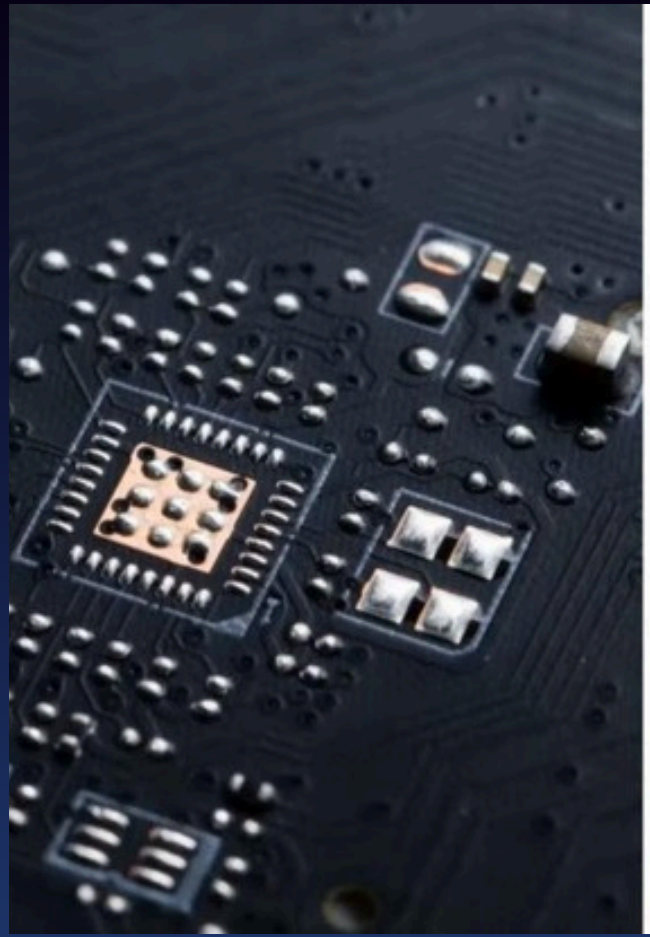
Gas Limit

Q) What is the use of Gas Limit ?

Ethereum Gas

Some important points to note -

- Any transaction that modifies the blockchain costs gas.
- The user that generated the transaction pays for the gas.

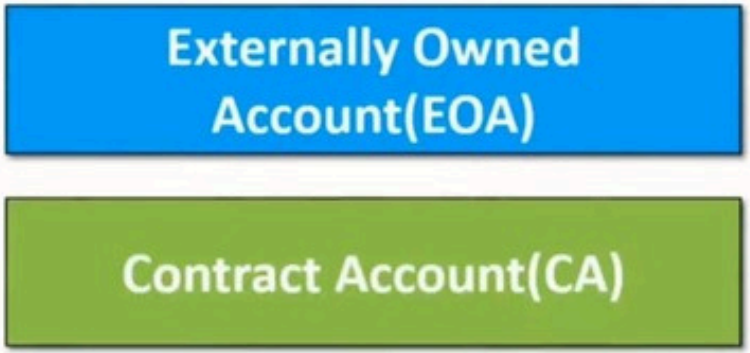


Ethereum Accounts

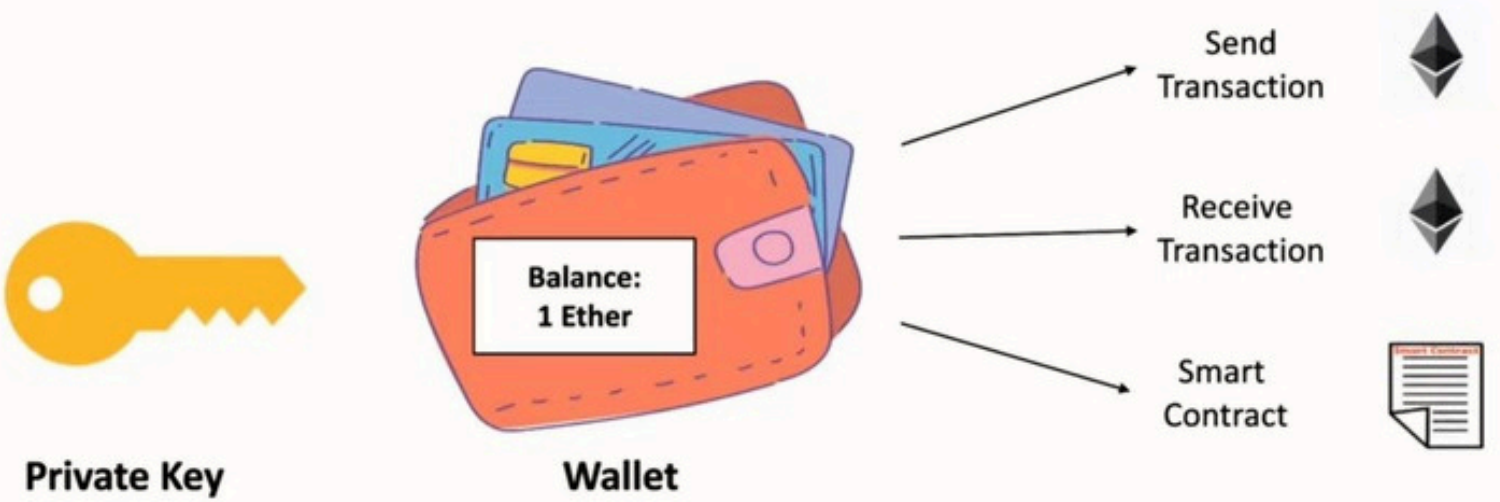
Ethereum Accounts

- An Ethereum account is an entity with an ether (ETH) balance that can send or receive transactions on Ethereum.

Types of Ethereum Accounts



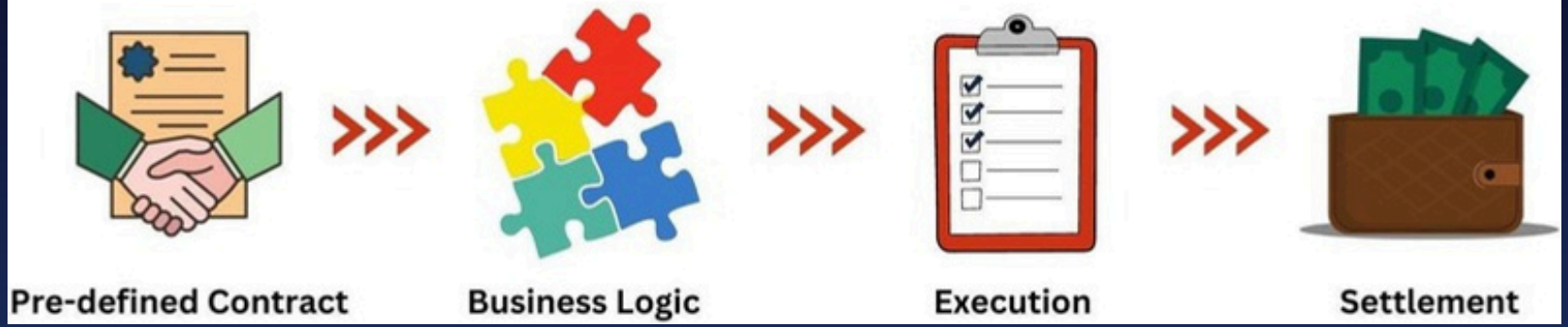
Externally Owned Account(EOA)



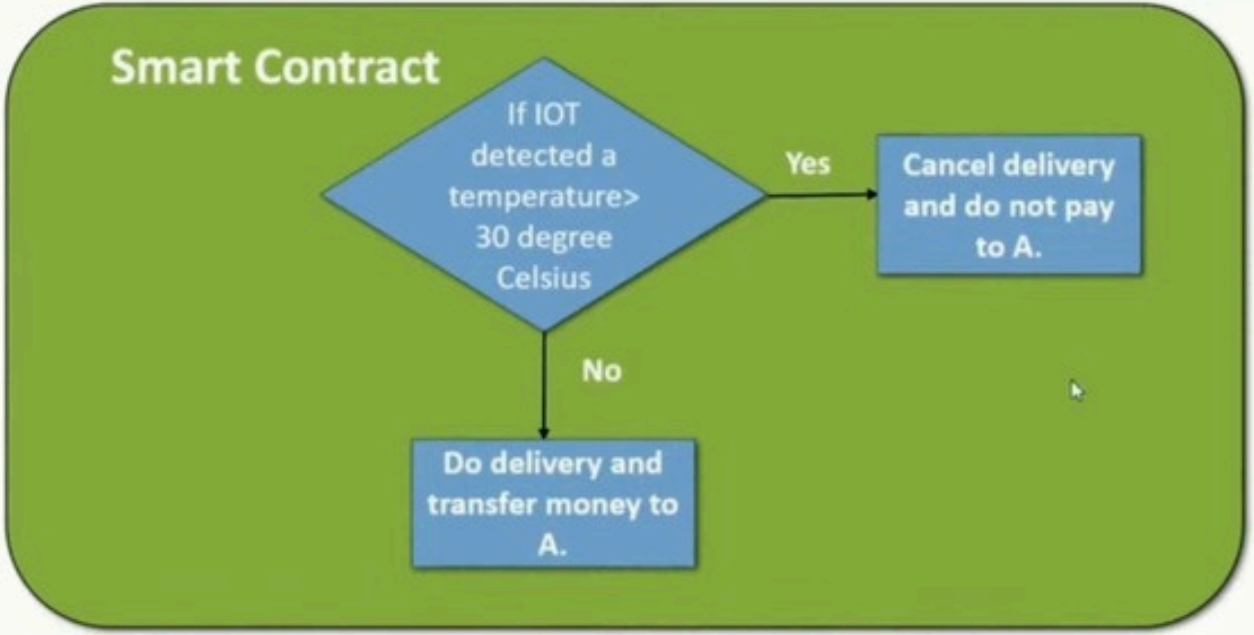
Contract Account (CA)

- Controlled by contract code.

How does the Smart Contract work?



Smart Contract



Note-Assuming optimum temperature <30 degree Celsius.

EOA VS CA

EOA	CA
Private Key is needed	No private or public key is needed.
Controlled by Human	Controlled by Contract code
No gas is associated	Gas is associated
Has a unique address	Has a unique address
Holds ETH balance	Holds ETH balance

THANK-YOU