

# ETHEREUM 2.0 MASTERY PROGRAM

Instructor: Raja Rizwan Saleem





# MODULE-2

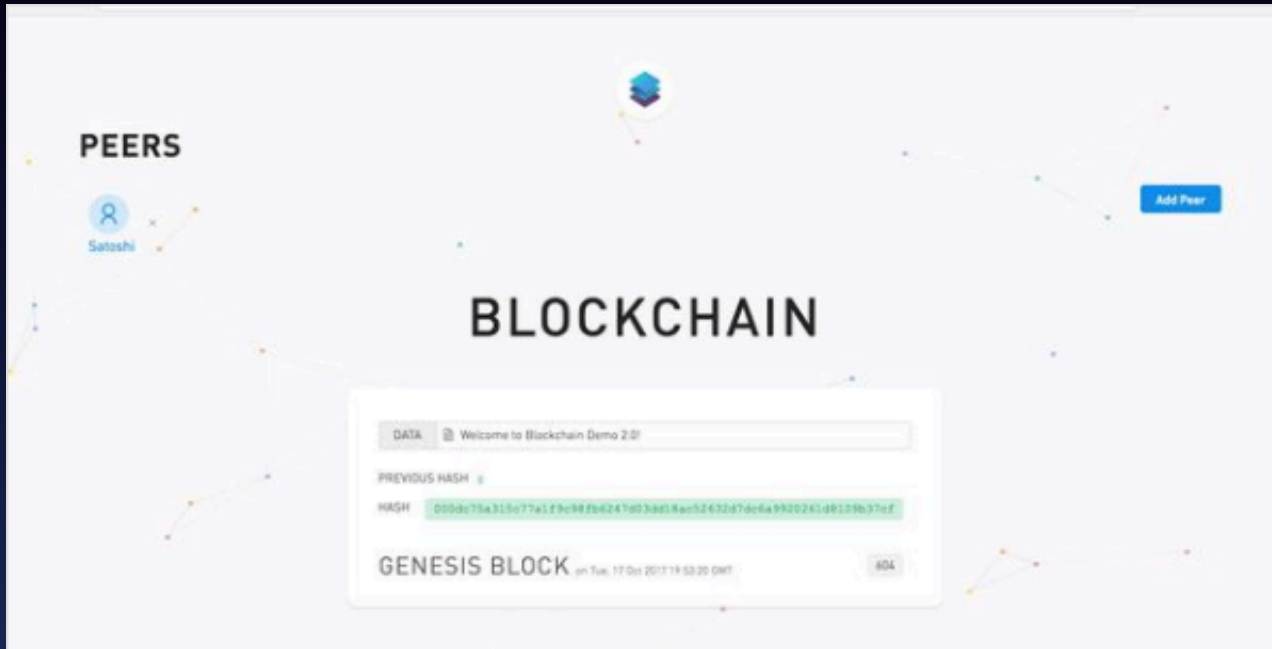
## BLOCKCHAIN AND SMART CONTRACT BASICS

Raja Rizwan Saleem  
Lead Blockchain Trainer

 [www.edversity.com.pk](http://www.edversity.com.pk)



Class-03



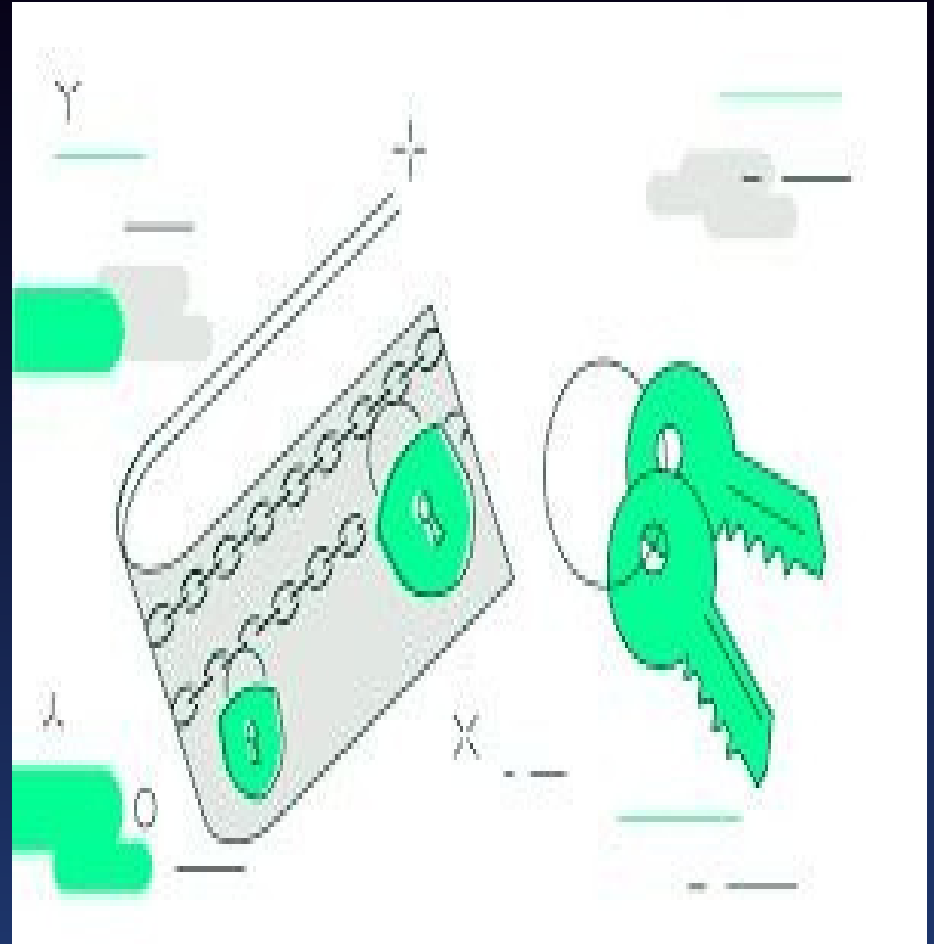
## Blockchain Demo

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



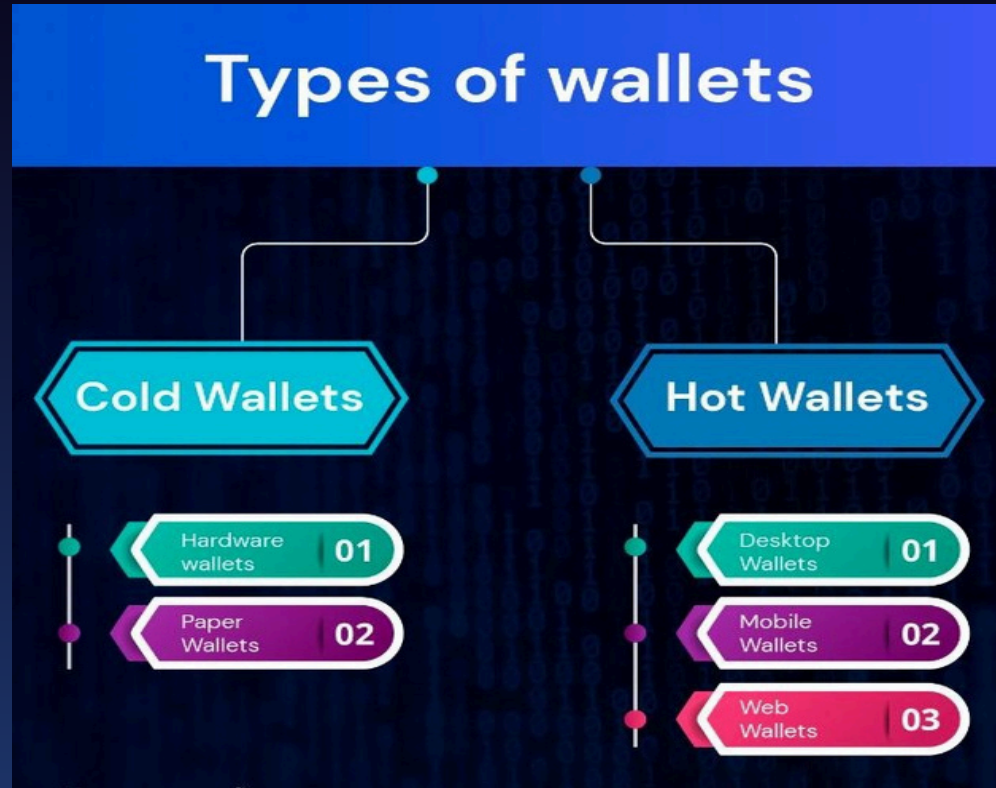
# Wallets

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

A Blockchain wallet has 2 keys



Public key: 099AD..

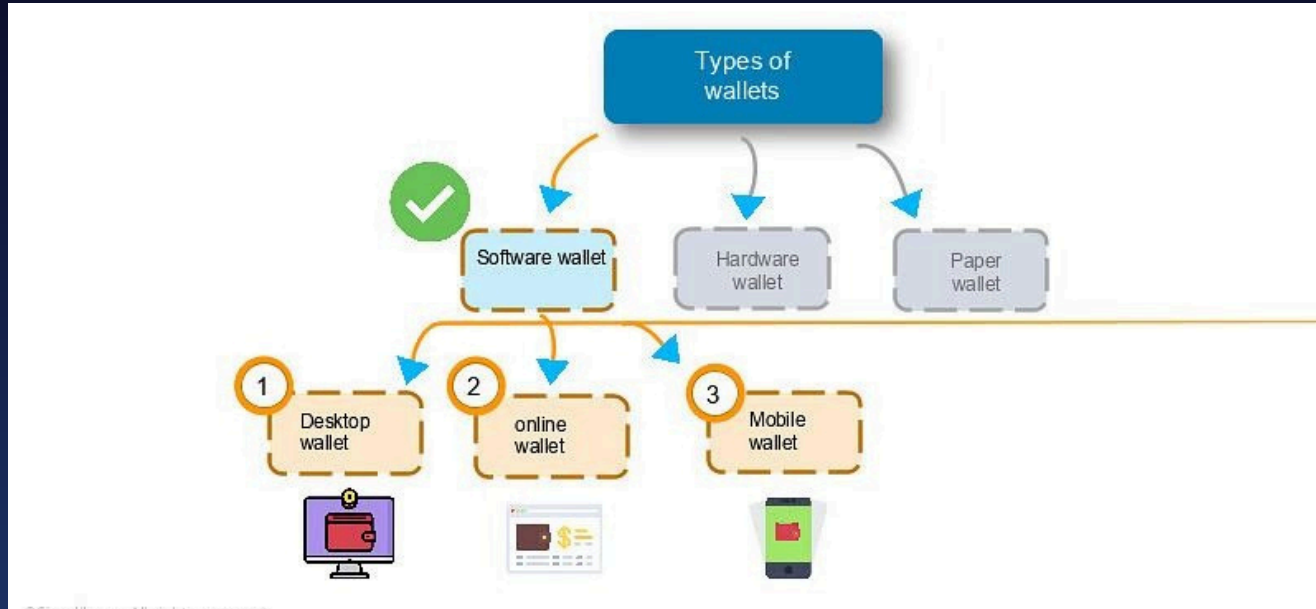
Public key is shared with everyone (just like the e-mail address)



Private key: \*\*\*\*\*

Private key is just like your password which should be kept secret with the sender

# Types of Wallets



# Hardware Wallets



 Ledger

 TREZOR  
 keep key

A hardware wallet is a type of cold storage device which stores the user's private key in a protected hardware device

These wallets are similar to portable devices that can be connected to the computer

It is less prone to malware attacks

For example, Ledger Nano S, TREZOR and KeepKey are the top hardware wallets

**Note:** To make a transaction, the hardware wallet has to be plugged into user's computer system

©Simplilearn. All rights reserved.

# Hardware Wallets



# Paper Wallets



A paper wallet is an offline process of storing cryptocurrencies



This wallet is a printed paper consisting of a private key and a public address (which are accessed using a QR code)



Since these wallets are safe, they are widely used for storing large amounts of cryptocurrencies



For example, Bitcoin paper wallet and MyEtherWallet are one of the widely used paper wallets

mpilearn. All rights reserved.

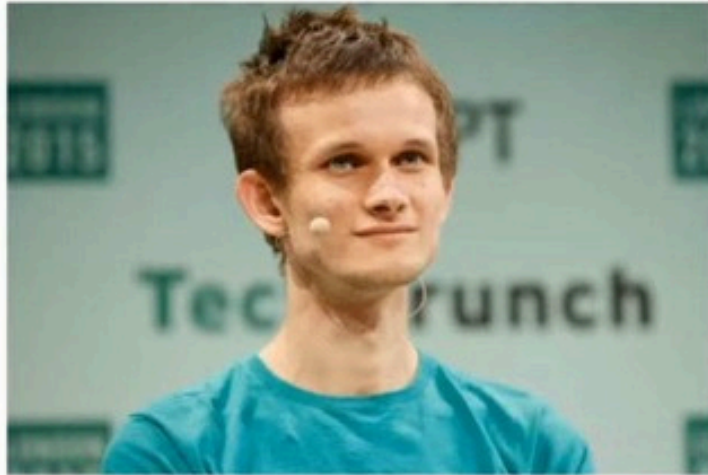


# Prerequisite

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.



Bitcoin



Ethereum



# Ethereum Currency Units

1. Ethereum's currency unit is called *ether*
2. It is identified as "ETH" or with the symbols  $\Xi$  (from the Greek letter "Xi" or, less often, )
3. For example: 1 ether, or 1 ETH, or  $\Xi 1$ , 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	Kiloweï or femtoether
1,000,000	$10^6$	Lovelace	Megaweï or picoether
1,000,000,000	$10^9$	Shannon	Gigaweï 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
<i>1,000,000,000,000,000,000</i>	<i><math>10^{18}</math></i>	<i>Ether</i>	<i>Ether</i>
1,000,000,000,000,000,000,000,000	$10^{21}$	Grand	Kiloether
1,000,000,000,000,000,000,000,000,000	$10^{24}$		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 = 210,000 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

---

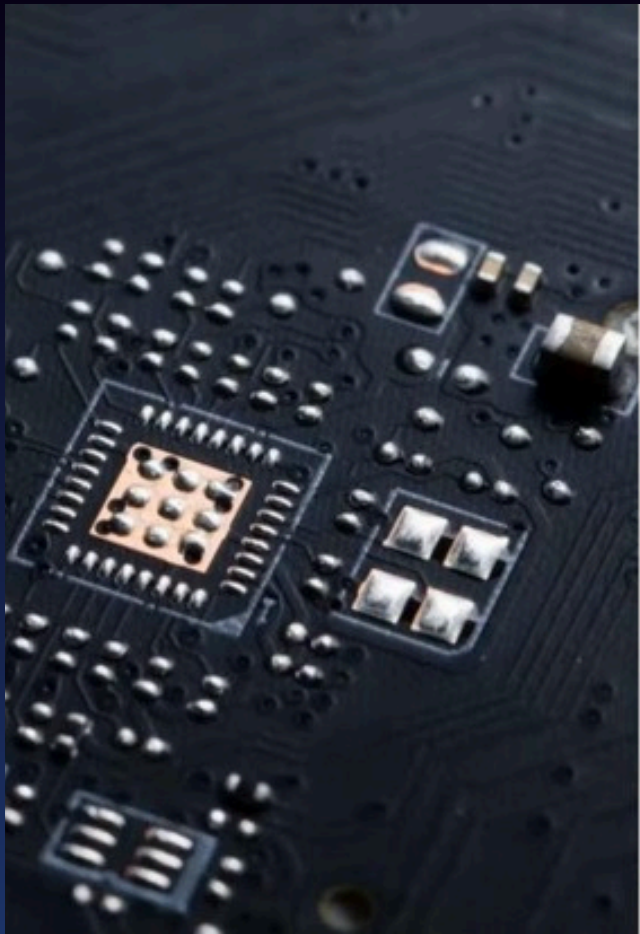
**Q) What is the use of Gas Limit ?**

# 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)**

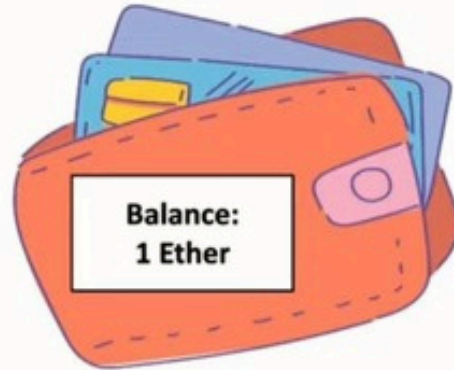
**Contract Account (CA)**

# Externally Owned Account(EOA)

---



**Private Key**



**Wallet**



Send  
Transaction



Receive  
Transaction



Smart  
Contract



# Contract Account (CA)

---

- Controlled by contract code.



# How does the Smart Contract work?



**Pre-defined Contract**



**Business Logic**

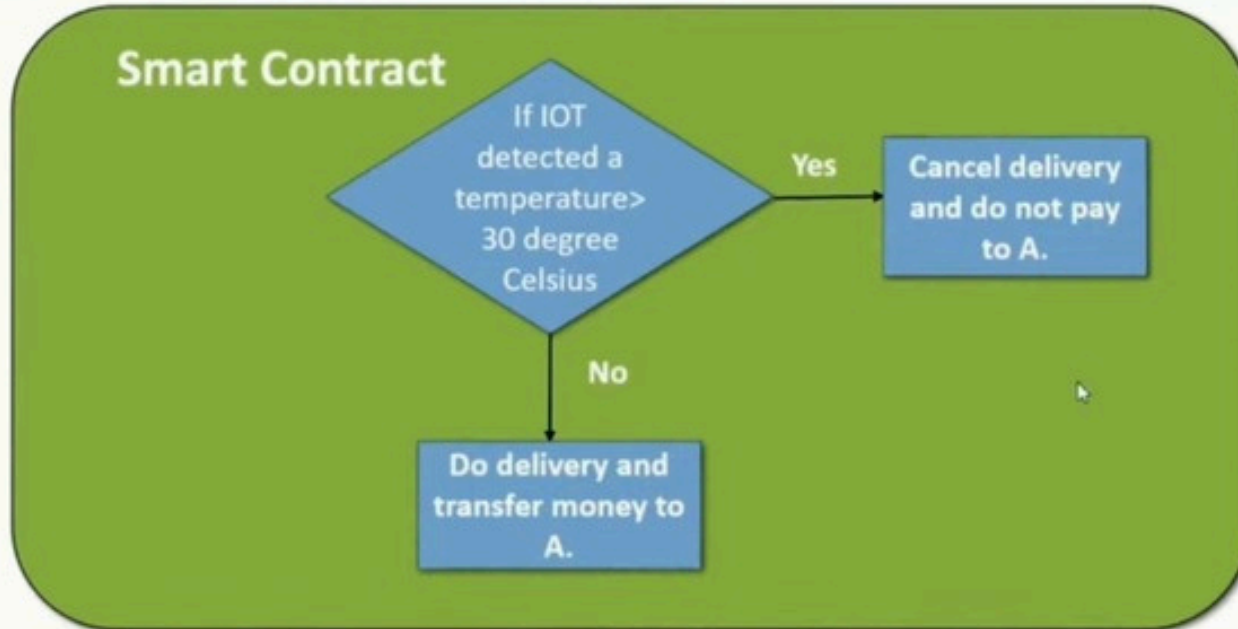


**Execution**



**Settlement**

# 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

