



# Blockchain

*Ethereum – an world computer*

*Ethereum, Smart Contract, wallet*



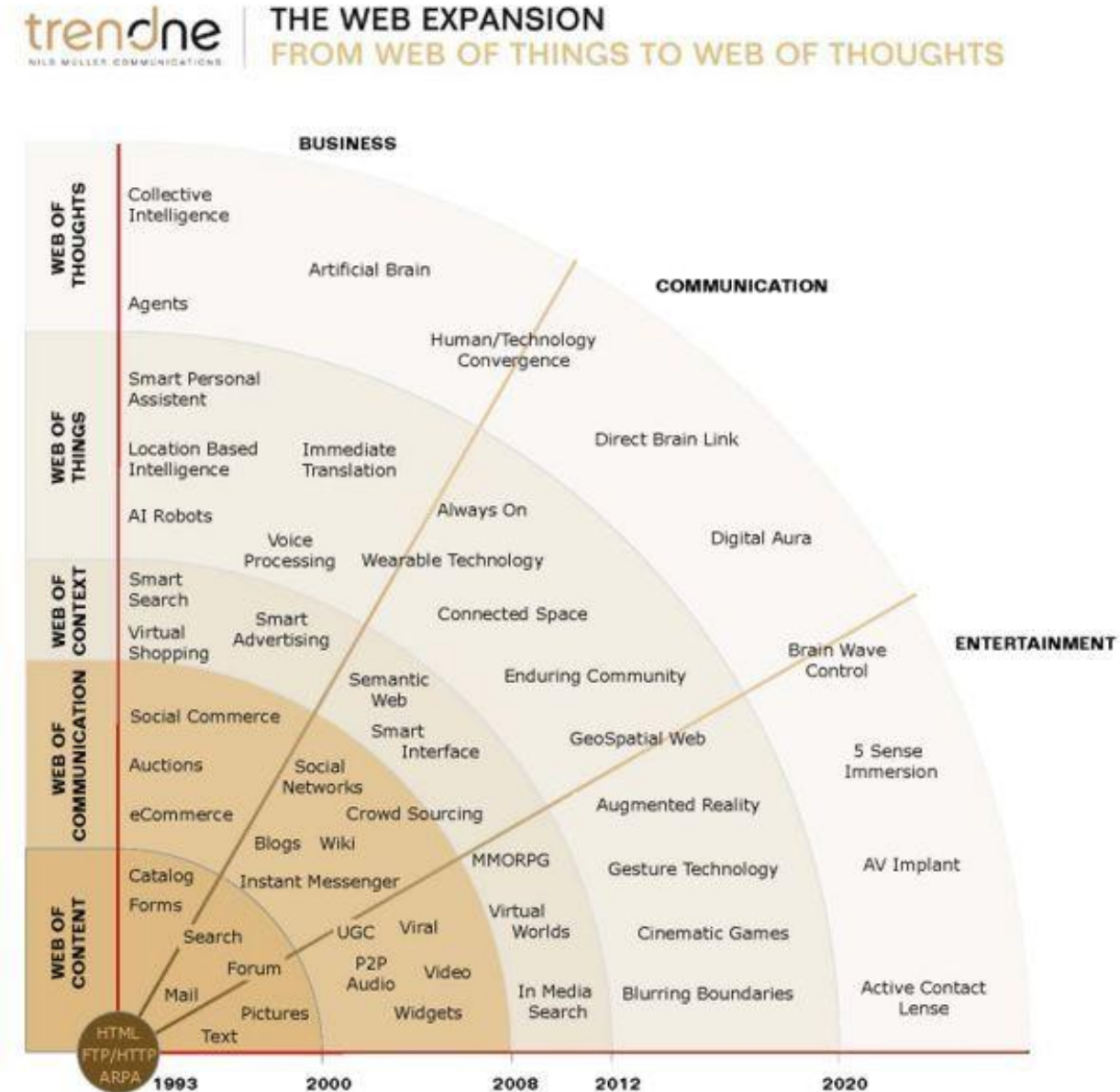
Dr. Sarwan Singh

NIELIT Chandigarh



# Agenda

- Ethereum- introduction, history
- Ethereum Ecosystem
- Smart Contract
- Wallet



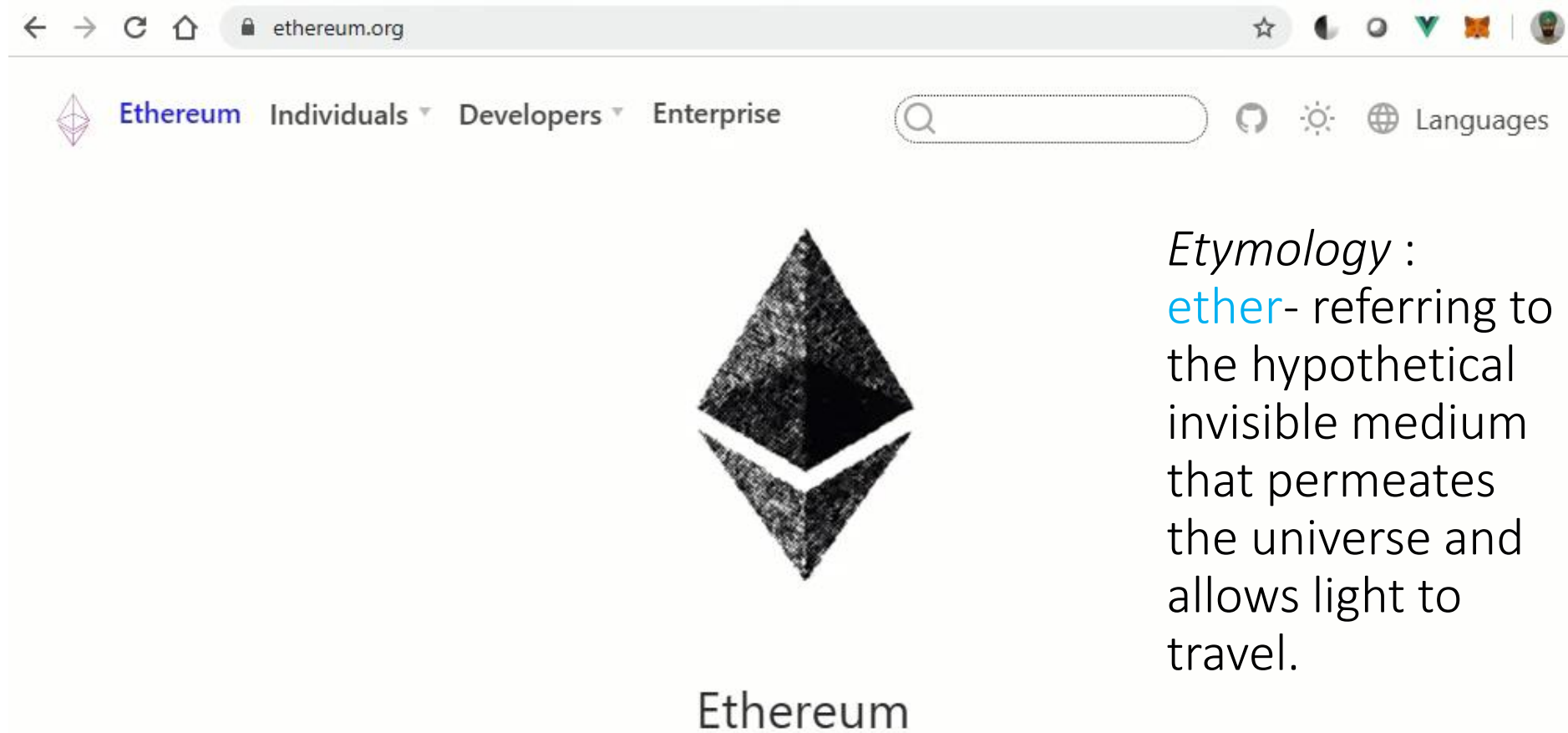


# References

- [Medium.com - Blockchain](#)
- [Quora.com – blockchain, mining](#)
- [en.bitcoin.it](#)
- [Ethereum.org](#)
- [Capgemini.com – Blockchain, databases vs blockchain](#)
- [consensys.net – Blockchain application areas, use-case](#)
- [flatworldbusiness.wordpress.com](#)
- [101blockchains.com](#)

# Ethereum

*Ethereum is a public,  
open-source,  
Blockchain-based  
distributed software  
platform that allows  
developers to build and  
deploy decentralized  
applications*



*Etymology :*  
**ether**- referring to  
the hypothetical  
invisible medium  
that permeates  
the universe and  
allows light to  
travel.

Ethereum is a global, open-source platform for decentralized applications.

On Ethereum, you can write code that controls digital value, runs exactly as programmed, and is accessible anywhere in the world.



# Ethereum

- **Ethereum** is an open source, public, **blockchain**-based distributed computing platform and operating system featuring smart contract (scripting) functionality.
- It supports a modified version of Nakamoto consensus via transaction-based state transitions.

26 years old Vitaly Dmitriyevich "Vitalik" Buterin is a Russian-Canadian programmer and writer primarily known as a co-founder of Ethereum and as a co-founder of Bitcoin Magazine.



Original author(s)	Vitalik Buterin, Gavin Wood
Initial release	30 July 2015
Repository	<a href="https://github.com/ethereum">github.com/ethereum</a>
Written in	C++, Go, Python
Operating system	Cross-platform
Platform	x86-64, ARM
License	open-source licenses
Website	<a href="https://ethereum.org">ethereum.org</a>



# History

- With beginning of blockchain viz. bitcoin in 2008, several developer started watching the development very closely.
- With difference in opinion and usage, several people started their own blockchain
- Vitalik Buterin, co-founder of Bitcoin Magazine and other started feeling that there should be **general purpose blockchain** which can be used as **Decentralized Application Platform** like Internet, whereas everyone should be free to store its own data.
- Vitalik said new framework should be able to perform all operation what bitcoin does.
- Main problem with bitcoin was lack general purpose programming language, it doesn't have loops, and can't store state. *"Lack of Turing-completeness"*
- Vitalik published white paper <https://github.com/ethereum/wiki/wiki/White-Paper>



# History Timeline

Ethereum was initially described in a white paper by Vitalik Buterin, a programmer and co-founder of Bitcoin Magazine, in late 2013 with a goal of building decentralized applications.

---

Buterin had argued that Bitcoin needed a scripting language for application development.

---

Failing to gain agreement, he proposed the development of new platform with more general scripting language.

---

Ethereum was announced at the North American Bitcoin Conference in Miami, in January 2014

---

a group of people rented a house in Miami – project kick-off

---

Six months later the founders met again in a house in Switzerland, where Buterin told the founders that the project would proceed as a non-profit

---



# History ...

- Launched in 2015, Ethereum is the world's leading programmable blockchain.
- Ethereum is the foundation for a new era of the Internet:
  - An Internet where money and payments are built in.
  - An Internet where users can own their data, and your apps don't spy and steal from you.
  - An Internet where everyone has access to an open financial system.
  - An Internet built on neutral, open-access infrastructure, controlled by no company or person.

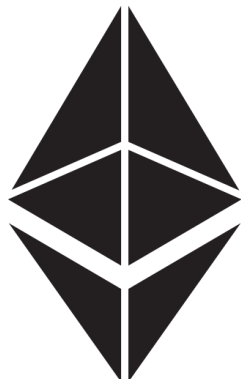




- The **Ethereum community** is the largest and most active blockchain community in the world. It includes core protocol developers, cryptoeconomic researchers, cypherpunks, mining organizations, ETH holders, app developers, ordinary users, anarchists, fortune 500 companies, and, as of now, you.
- There is **no company** or centralized organization that controls Ethereum.



VS



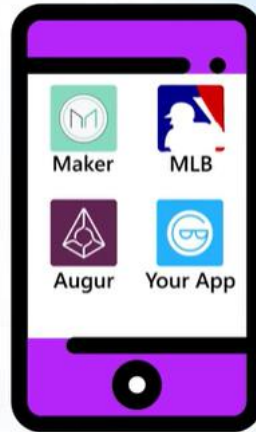
Ethereum : *an programmable blockchain*

Parameter	Bitcoin	Ethereum
Definition	Bitcoin is a digital money	Ethereum is a world computer.
Founder	Satoshi Nakamoto (~18 m)	Vitalik Butarrn (~1 billion)
Hashing algorithms	Bitcoin used SHA-256 algorithm.	Ethereum uses Etash algorithm.
Average Block time	10 minutes	10-15 sec
Release Date	9 Jan 2008	30 July 2015
Blockchain	Proof of work	Proof of work (Planning for POS)
Usage	Digital Currency	Smart Contracts Digital Currency
Cryptocurrency Used	Bitcoin(Satoshi)	Ether
Blocks Time	10 Minutes	12-14 Seconds
Mining	ASIC miners	GPUs
Scalable	Not now	Yes
Concept	Digital money	World Computer/Smart Contract
Cryptocurrency Token	BTC	Ether
Turing	Turing incomplete	Turing complete
Coin Release Method	Early mining	Through ICO
Protocol	Bitcoin still employs the pool mining concept.	It uses a Ghost Protocol.



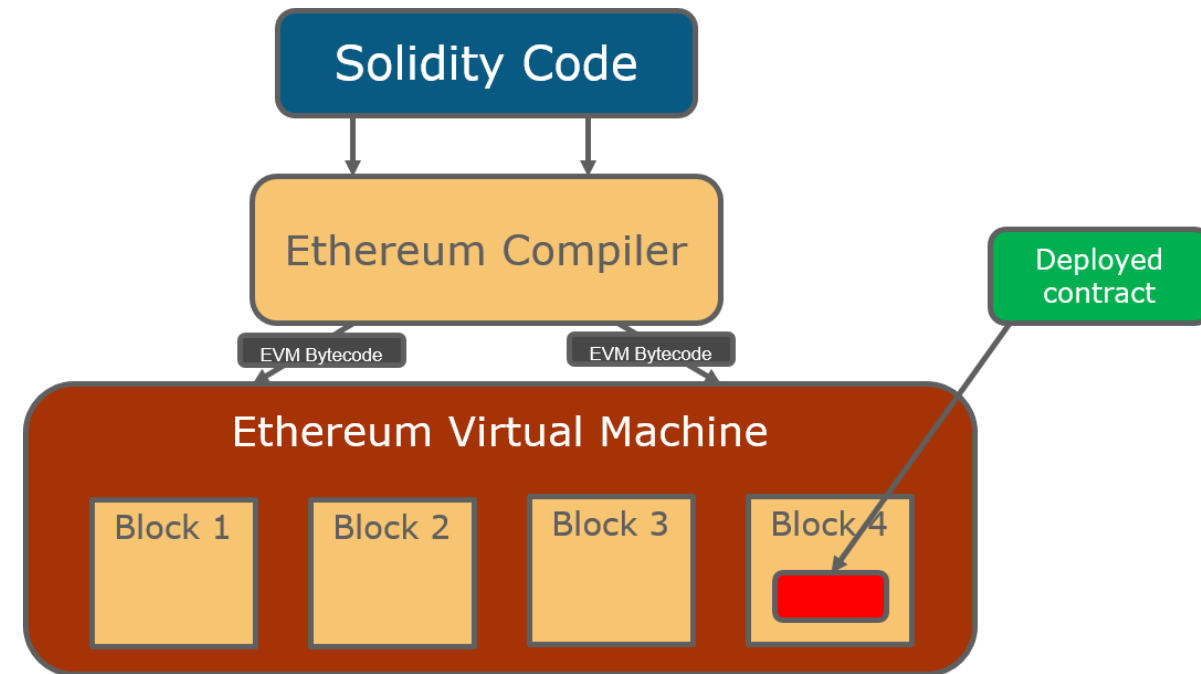
# Bitcoin vs Ethereum

- Bitcoin and Ethereum differ substantially in purpose and capability.
- Bitcoin offers one particular application of blockchain technology, a peer to peer electronic cash system that enables online Bitcoin payments.
- Bitcoin is an **app**, Ethereum is an **app store**
- Bitcoin is used to **track ownership** of **digital currency (bitcoins)**, Ethereum focuses on running the **programming code** of any **decentralized application**.
- Ethereum is platform to store multiple applications data



# Ethereum Virtual Machine (EVM)

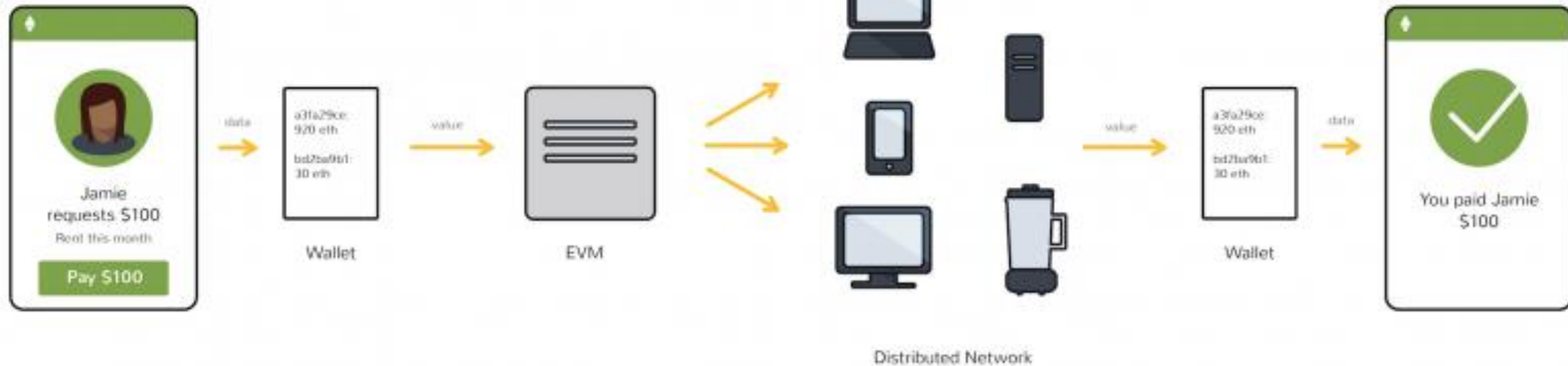
- Like other blockchains, Ethereum has a native cryptocurrency called **Ether (ETH)**. ETH is digital money. It has same features as Bitcoin
- The supply of ETH isn't controlled by any government or company - it is decentralized, and it is scarce.
- But unlike other blockchains, Ethereum can do much more.



# Ethereum Virtual Machine (EVM)

- Ethereum is programmable, which means that developers can use it to build new kinds of applications.
- Runtime environment for smart contracts called **Ethereum Virtual Machine (EVM)**

Ethereum App





# Ether (ETH)

- ETH is the native currency of Ethereum
- It is "digital money" that can be sent over the internet instantly and cheaply, and also be used in many Ethereum-based applications.
- The easiest way to get ETH is to buy some. There are many cryptocurrency exchanges that will allow you to buy ETH, but the one you should use will depend on where you live and how you want to pay.

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
1,000,000,000,000,000,000,000	$10^{18}$	<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 Network

- It is a public blockchain network
- It forms the basis of all decentralized peer-to-peer applications and organizations run on the network.
- The network is comprised of two types of nodes
  - **full nodes** - contain the entire history of transactions since the genesis block. They are a full-fledged proof of the integrity of the blockchain network. Full nodes have to contain each and every transaction that has been verified
  - **light-weight-nodes**- only contain a subset of the entire blockchain. mostly used in e-wallets which have to be light-weight in nature. They do not verify every block or transaction and may not have a copy of the current blockchain state.





# Smart Contract

- The term smart **contract** dates to 1994, defined by Nick Szabo as “a computerized transaction protocol that executes the terms of a contract”.
- A **smart contract** is a collection of code and data (sometimes referred to as functions and state) that is deployed using cryptographically signed transactions on the blockchain network (e.g., Ethereum’s smart contracts, Hyperledger Fabric’s chaincode)



# Not every blockchain can run smart contracts

Blockchain network users can create transactions which send data to public functions offered by a smart contract.

The smart contract executes the appropriate method with the user provided data to perform a service.

The code, being on the blockchain, is also tamper evident and tamper resistant and therefore can be used as a trusted third party.

A smart contract can perform calculations, store information, expose properties to reflect a publicly exposed state and, if appropriate, automatically send funds to other accounts.



# Smart Contract

- Smart contracts must be deterministic, in that given an input they will always produce the same output based on that input.
- Additionally, all the nodes executing the smart contract must agree on the new state that is obtained after the execution. To achieve this, smart contracts cannot operate on data outside of what is directly passed into it (e.g., smart contracts cannot obtain web services data from within the smart contract – it would need to be passed in as a parameter).
- Any smart contract which uses data from outside the context of its own system is said to use an 'Oracle'



# Gas

- To perform a transaction on the Ethereum network, a user requires to make a payment (to the miner) Ether via an intermediary token called 'Gas'.
- It is a unit which allows you to measures the computational work required for running a smart contract or other transactions.
- In Ethereum, the transactions fee is calculated in Ether,

$$\text{Ether} = \text{Tx fees} = \text{Gas Limit} * \text{Gas Price}$$

- Gas Limit= Refers to the amount of gas that is used for the computation
- Gas Price= The amount of Ether a user is required to pay



pragma solidity 0.4.25;

contract Bank{

    int bal;

    constructor () public

    {      bal=1;    }

    function withdraw(int a) public

    {      bal =bal -a;    }

    function deposit(int a) public

    {      bal =bal +a;    }

    function getBalance() view public returns (int)

    {              return bal;    }

}



# Ethereum Ecosystem

Built on Ethereum

Decentralized  
Finance

Decentralized  
Exchanges

Games

Collectibles

Marketplaces

Supply Chain

Developer  
Tools

Identity

Governance

Infrastructure

Enterprise

Oracles

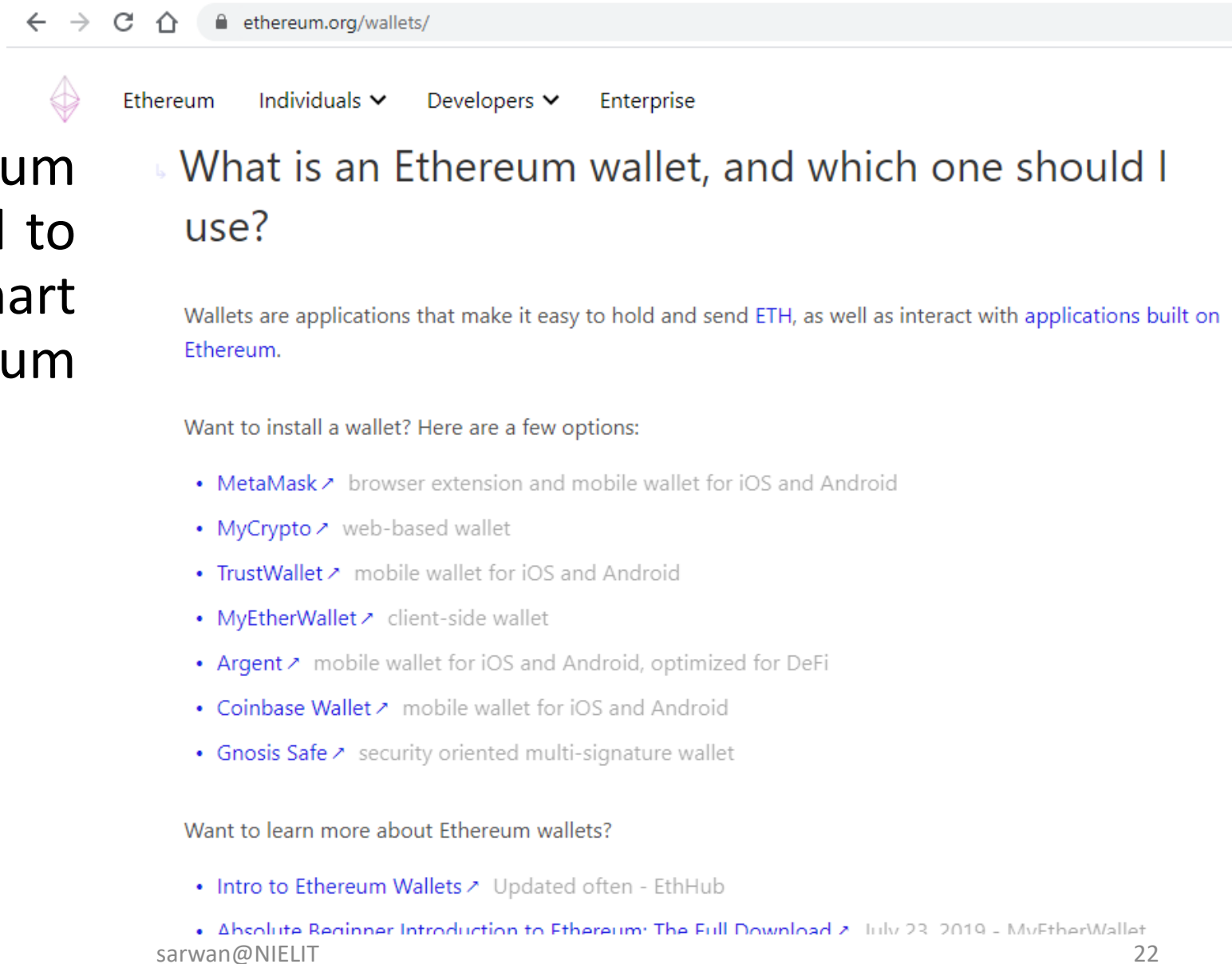
Token Curated  
Registries

ERC Token  
Standards



# Ethereum Wallets

- Wallets allow Ethereum users to store Ether and to interact with smart contracts on the Ethereum network.



The screenshot shows the Ethereum.org/wallets/ page. At the top, there's a navigation bar with the Ethereum logo and links for 'Ethereum', 'Individuals', 'Developers', and 'Enterprise'. The main heading is 'What is an Ethereum wallet, and which one should I use?'. Below this, a paragraph explains that wallets are applications for holding and sending ETH and interacting with dApps. A section titled 'Want to install a wallet? Here are a few options:' lists several wallets: MetaMask, MyCrypto, TrustWallet, MyEtherWallet, Argent, Coinbase Wallet, and Gnosis Safe, each with a brief description. Another section titled 'Want to learn more about Ethereum wallets?' lists two resources: 'Intro to Ethereum Wallets' and 'Absolute Beginner Introduction to Ethereum: The Full Download'.

← → ↺ 🏠 ethereum.org/wallets/

Ethereum Individuals ▾ Developers ▾ Enterprise

## What is an Ethereum wallet, and which one should I use?

Wallets are applications that make it easy to hold and send [ETH](#), as well as interact with [applications built on Ethereum](#).

Want to install a wallet? Here are a few options:

- [MetaMask](#) ↗ browser extension and mobile wallet for iOS and Android
- [MyCrypto](#) ↗ web-based wallet
- [TrustWallet](#) ↗ mobile wallet for iOS and Android
- [MyEtherWallet](#) ↗ client-side wallet
- [Argent](#) ↗ mobile wallet for iOS and Android, optimized for DeFi
- [Coinbase Wallet](#) ↗ mobile wallet for iOS and Android
- [Gnosis Safe](#) ↗ security oriented multi-signature wallet

Want to learn more about Ethereum wallets?

- [Intro to Ethereum Wallets](#) ↗ Updated often - EthHub
- [Absolute Beginner Introduction to Ethereum: The Full Download](#) ↗ July 23, 2019 - MyEtherWallet

sarwan@NIELIT





# Ethereum Wallets

- [Smart Contract Wallets](#) : wallets with unique abilities due to the power of smart contract functionality. They enable additional security and recovery features for users.
  - E.g. gonosis safe, Argent
- [Hardware Wallet](#) : They are the most-secure method for accessing your funds while online, as they do not expose your private key to the internet when signing transactions.
  - E.g. ledger, lattice1, Trezor, keepkey, BitBox



# Ethereum Wallets

- [Mobile](#) : are mobile alternatives to desktop and web wallets.
  - E.g. Alphawallet, Ambo, atomic wallet, balance
- [Desktop Wallets](#) :downloadable apps capable of operating on Windows, MacOS, or Linux that allow users to interact with their funds.
  - E.g. Eidoo, fetch, MyCrypto
- [Web Wallets](#) : wallets hosted on a website, they may be custodial or act as an interface for users to generate and interact with their accounts.
  - MetaMask, Torus, Portis