Ethereum Basics

October 20, 2021

WOMEN WHO CODE®

Rajapandian C
Open Source, Blockchain & Emerging Technologies
rajapandianc@outlook.in
@rajapandianc @crpcodes

Agenda

- Quick Intro to Blockchain
- What makes Blockchain Technology unique
- Blockchain implementations at a glance
- Introducing Ethereum
- Ethereum Fundamentals
- Ethereum Technical Concepts
- Let’s build a Smart Contract
- Q & A

Involve in the Digital Economy

Era	*Disruption*
Web 1.0	Information -> Google, Amazon
Web 2.0	Social -> Facebook, Twitter
Web 3.0	Digital Economy -> Value transfer

Quick Intro to Blockchain

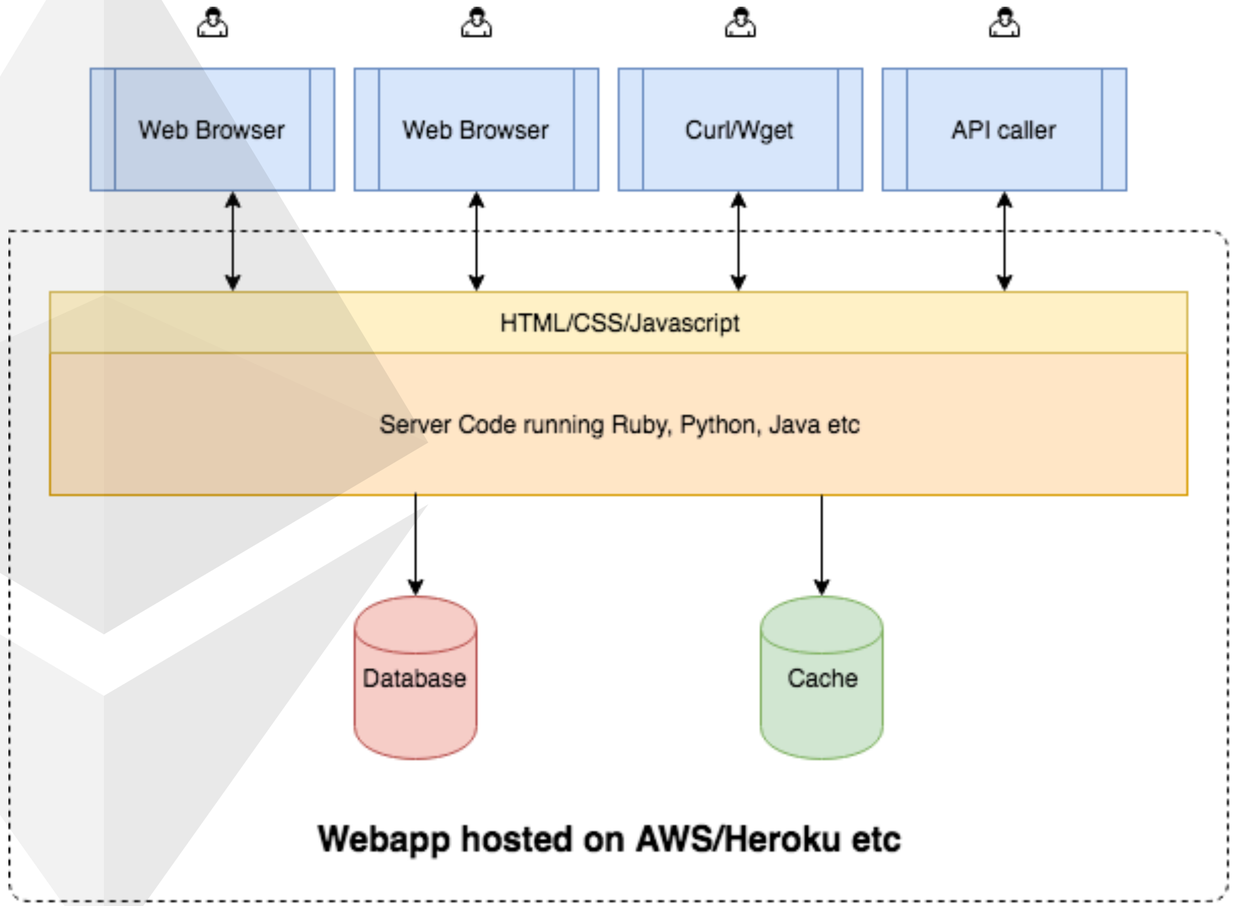
Webapp Architecture

Traits

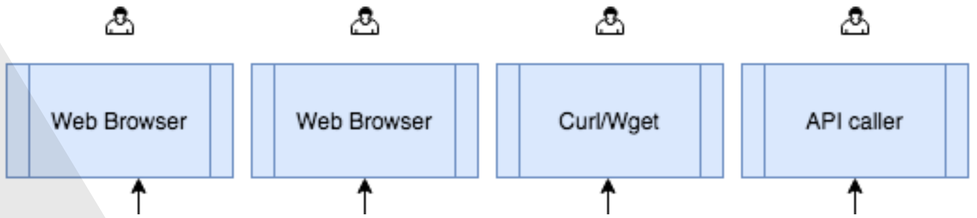
Client-Server Architecture

Centralised Hosting

Data Stored to relational or NoSQL databases



Blockchain Architecture



Traits

Decentralised Hosting

World database - Single Source of Truth

Immutable Digital Ledger

Solves Double-spend

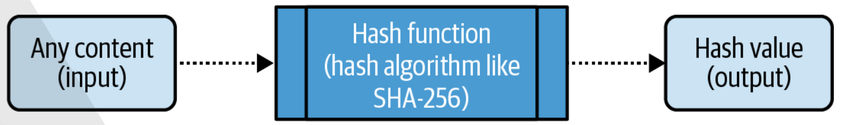
Application deployed to network of nodes

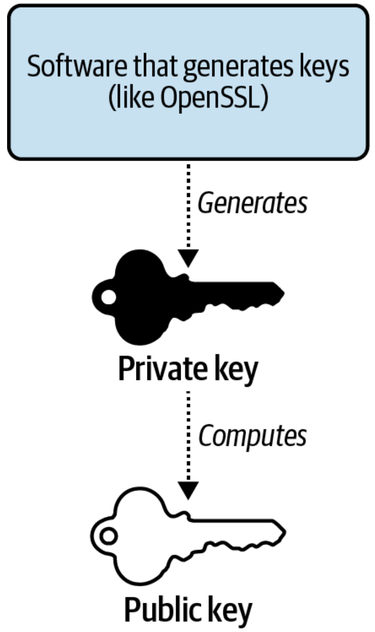
Core Cryptography Concepts

- Hashes
- Public and Private Keys
- Digital Signatures
- Digital Certificates
- Merkle Trees

Foundation

Adds Value



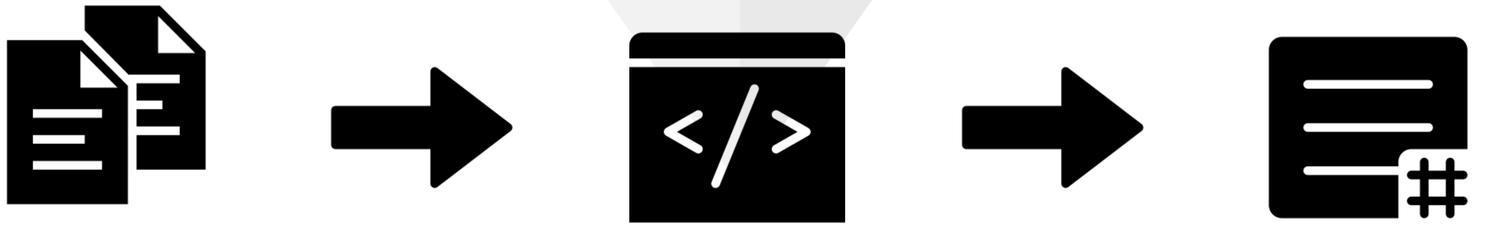


Encryption & Hashing

Encryption
(Used to protect sensitive information)

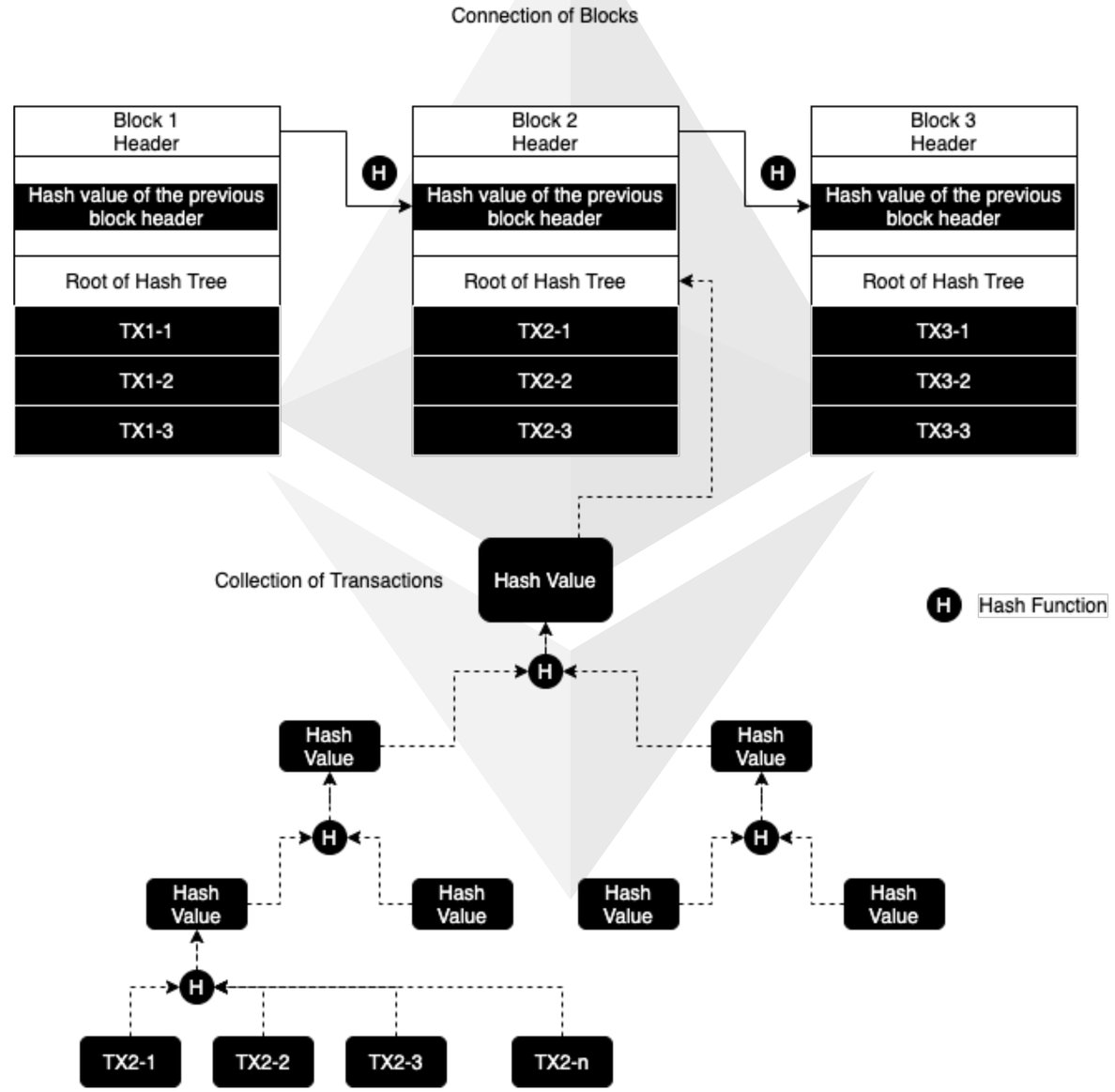
Data — **Encryption** — **Encrypted Data** — **Decryption** — **Data**

Hashing
(Used to validate information)



Data → **Hash Function** → **Hashed Data**

How does a Blockchain look?

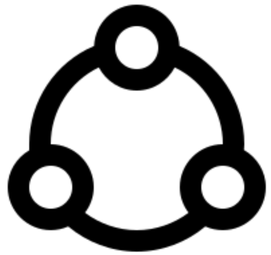


Components of a Blockchain

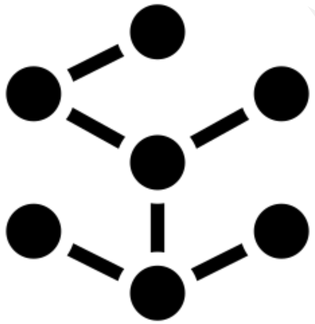
- A ***peer-to-peer (P2P)*** network connecting participants and propagating transactions and blocks of verified transactions, based on a standardized “gossip” protocol
- Messages, in the form of transactions, representing ***state transitions***
- A set of ***consensus rules***, governing what constitutes a transaction and what makes for a valid state transition
- A ***state machine*** that processes transactions according to the consensus rules
- A ***chain of cryptographically secured blocks*** that acts as a journal of all the verified and accepted state transitions
- A consensus algorithm that ***decentralises control*** over the blockchain, by forcing participants to cooperate in the enforcement of the consensus rules
- A game-theoretically sound ***incentivization scheme*** (e.g., proof-of-work costs plus block rewards) to economically secure the state machine in an open environment
- One or more open source software implementations of the above (“clients”)

Traits of a Blockchain

- A digital ledger that maintains a continuously growing list of data records
- Has unique qualities of trust and openness unlike traditional databases



Shared Publicly



Decentralised

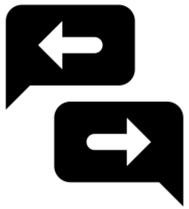
Secure

Trusted

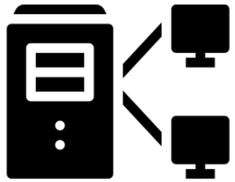
Automated

What makes Blockchain Technology unique?

- Enables trusted P2P communication over a decentralised network of nodes
- Transactions are added to the immutable digital ledger upon consensus among the nodes

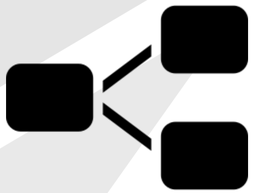


Peer-to-Peer

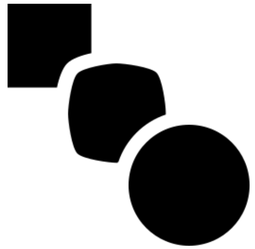


Decentralised Nodes

Consensus



Immutable Ledger



State Transitions

Incentives

Blockchain Implementations

- Bitcoin was the first well known implementation of Blockchain Technology
- Ethereum adds more flavour to Blockchain by enabling Smart-Contracts

Public

Bitcon, Ethereum, Litecoin

Private

Hyperledger, R3 Corda, Quorum

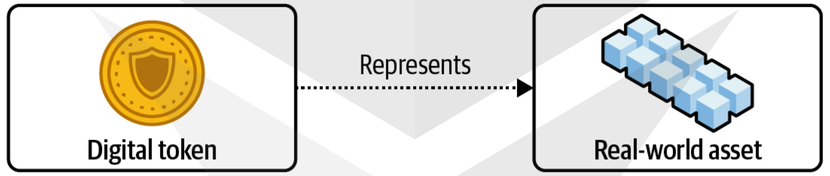
Hybrid

Layer 2 Solutions, Side-chains

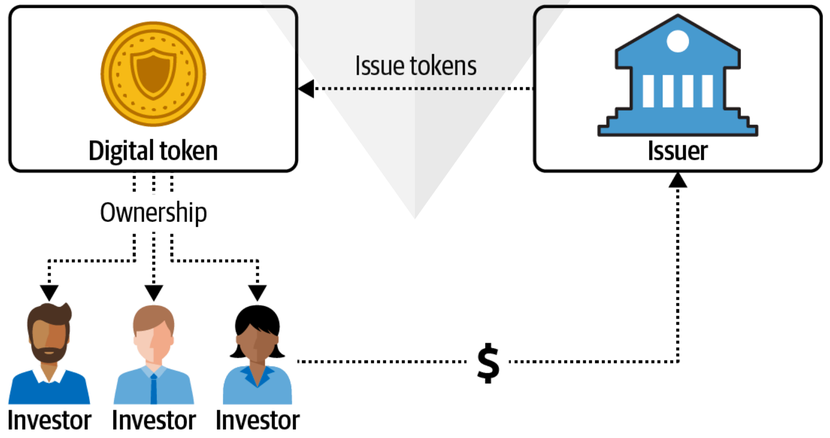
Blockchain Use-cases

- Decentralised Finance and Digital Assets

- Tokenisation

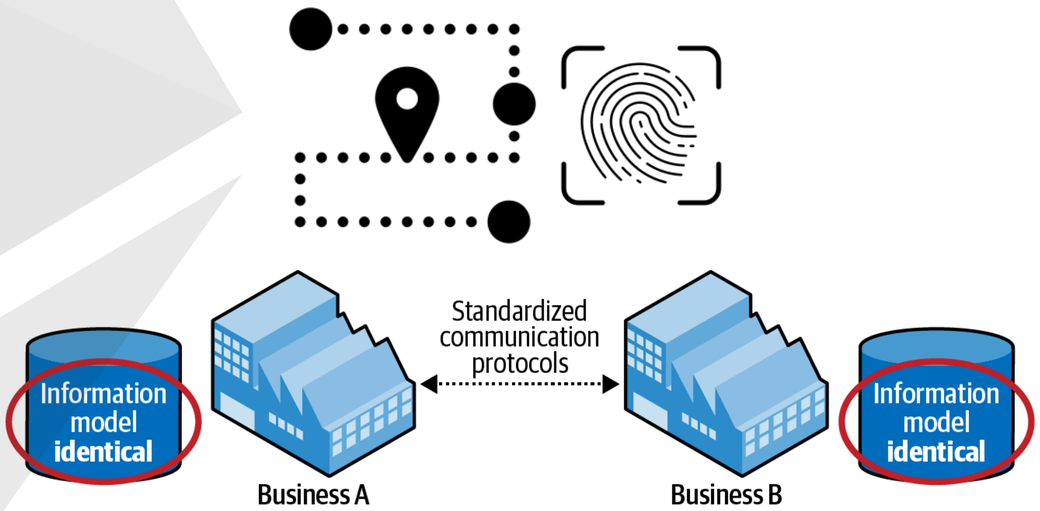


- Capital Raising



Blockchain Use-cases Contd.

- Traceability and Provenance
- Reconciliation Cost Reduction
- Reconciliation Revenue Streams



Ethereum

A General-Purpose Blockchain

Decentralised Payments on Blockchain

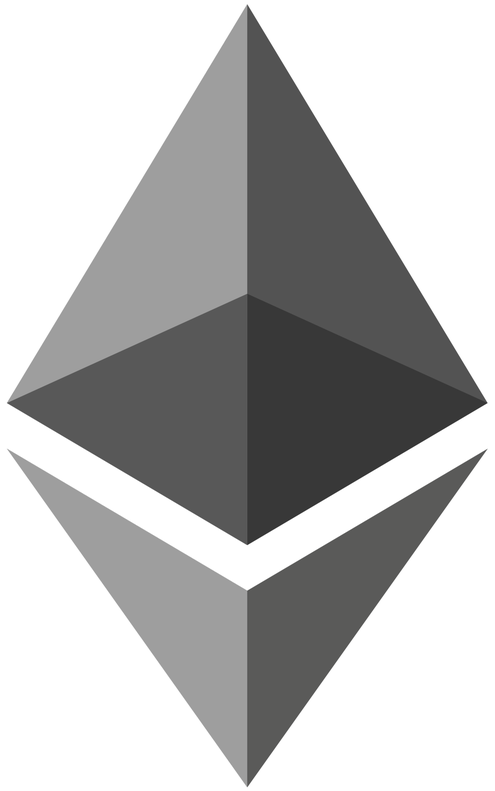
More than just Payments

Introducing Ethereum

- ***Bitcoin*** is primarily used for ***payments on blockchain*** without the need for a central authority

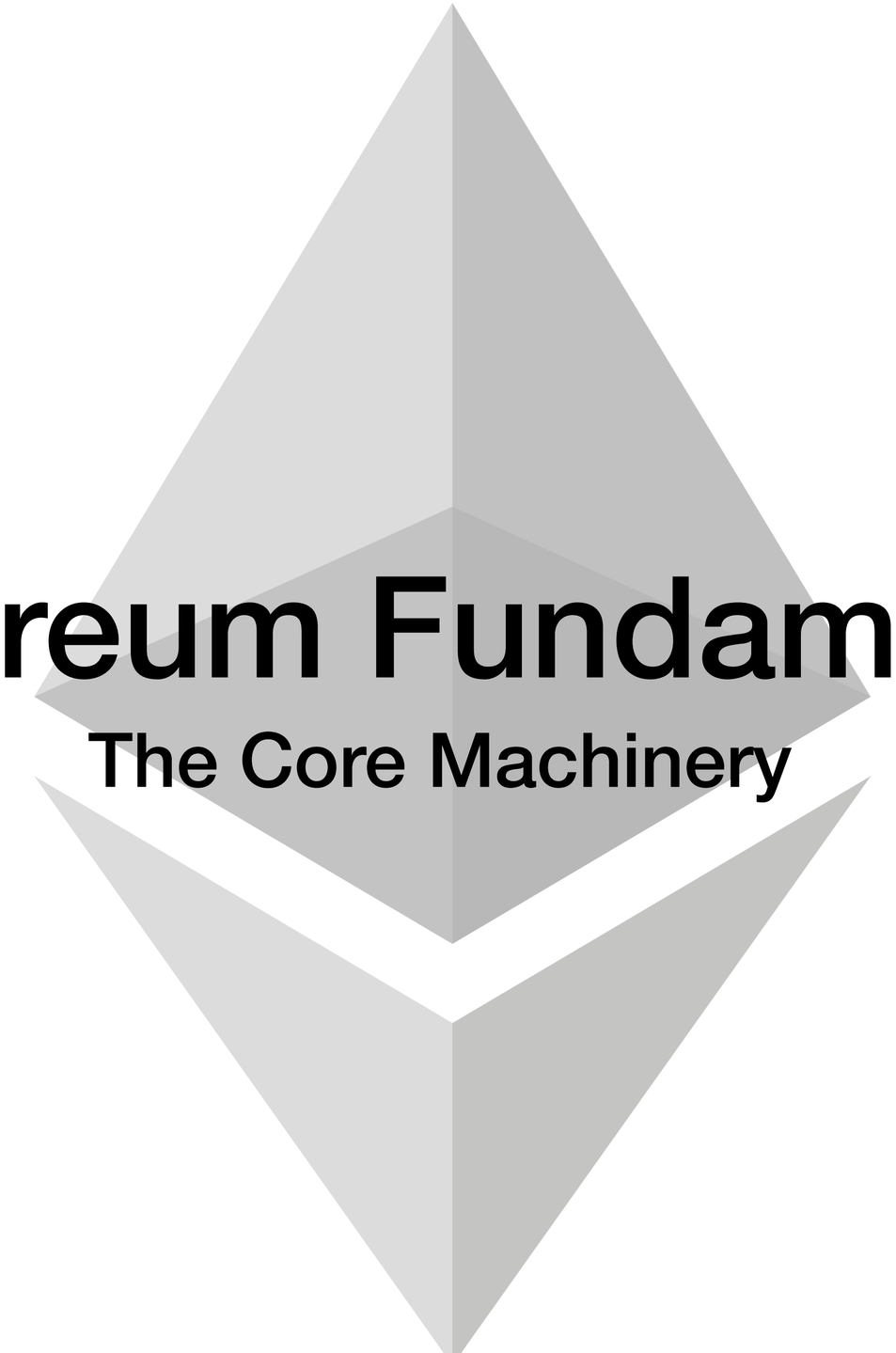
- Vitalik Buterin proposed to add a scripting language to Bitcoin to be able to build applications.

- ***Ethereum*** is a platform ***more than just payments*** that executes the smart-contracts on a virtual machine - Ethereum Virtual Machine (EVM)



White paper - https://github.com/ethereum/wiki/wiki/White-Paper

Yellow paper - https://ethereum.github.io/yellowpaper/paper.pdf



Ethereum Fundaments

The Core Machinery

Ether & Denominations

Ether & Denominations

- Just like in the real world, each country has it's own currency like USD, INR, RNB, GBP, EUR etc, each blockchain has it's own currency. In the case of ***Ethereum blockchain, the native currency is called Ether***

- Ether also has various denominations as shown on the right. The only two you should really remember are ***Ether*** and ***Wei***. ***Wei is the lowest denomination*** and this is the denomination you use in your smart contracts.

Table 1. Ether Denominations and Unit Names

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

Ether & Denominations

Table 1. Ether Denominations and Unit Names

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

What is an Ethereum address?

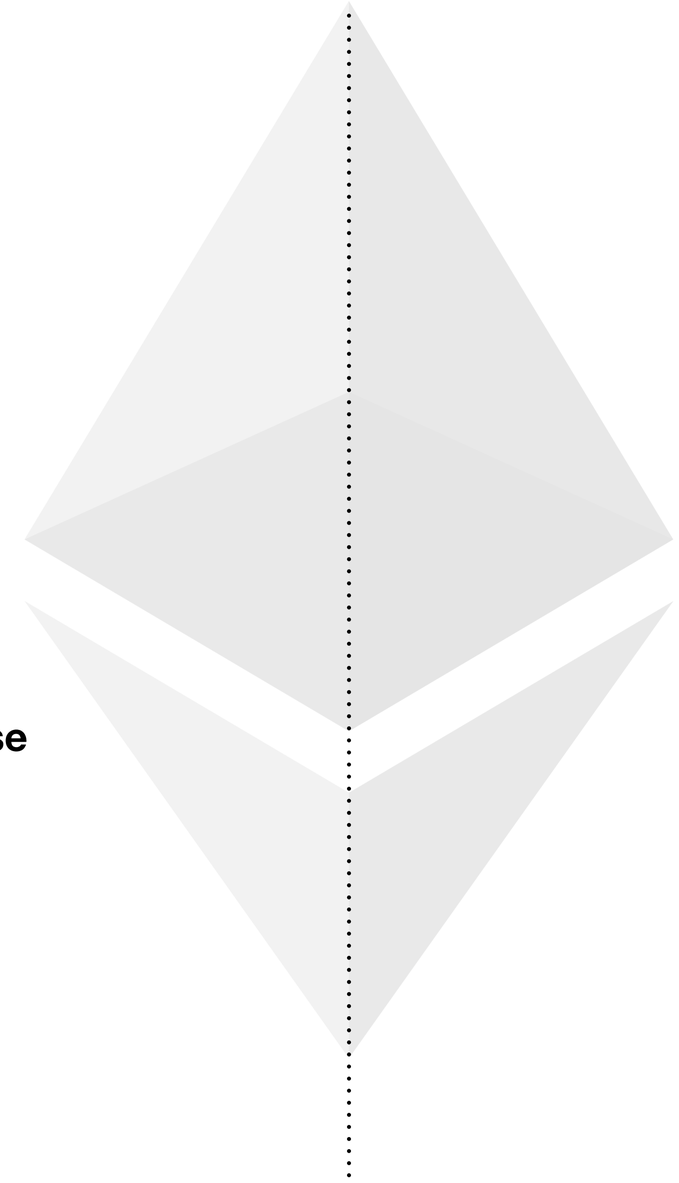
- To login to any website like Facebook, you usually use an ***email/username and password***
- Your ***username is your identity in Facebook*** and you use your username/password to authenticate with Facebook
- In Ethereum blockchain, ***address is your identity***.
- An Ethereum address looks like this: *001d3f1ef827552ae1114027bd3ecf1f086ba0f9*
- An address has a corresponding ***private key***
- You can think of **private key as a password** that only you know
- You need this pair of ***address + private key to interact with the blockchain***
- ***Ethereum address is public and you can share it with anyone in the world***.
- The ***private key should never ever be shared*** with anyone.
- The ***address + private key is not stored*** in any database. Only you are in control of them.

What is an Ethereum address?

Email & Password

Identified by Username

Credentials stored in a Database



Address & Private Key

Identified by Address

Credentials are not stored

What is an Ethereum account?

- The combination of ***Ethereum address and it's private key*** is referred to as an ***account***
- An account in Ethereum ***can hold balance (Ether) and can send transactions***
- Ethereum has 2 types of accounts
- ***Externally owned accounts*** (EOA)
    - EOA is a combination of public address and private key
    - Send and receive Ether to/from another account
    - Send transactions to smart contracts
- ***Contract accounts***
    - Don't have a corresponding private key
    - Generated when you deploy your contract to the blockchain
    - Can send and receive ether just like EOA
    - Have code associated with them unlike EOA
    - Transactions have to be triggered by an EOA or another contract

What is an Ethereum account?

- The combination of ***Ethereum address and it's private key*** is referred to as an ***account***
- An account in Ethereum ***can hold balance (Ether) and can send transactions***
- Ethereum has 2 types of accounts

Externally Owned Account (EOA)

Contract Account

Bytecode & EVM

- ***Bytecode***
  - Smart contract code is usually written in a high level programming language such as ***Solidity***
  - Code gets compiled to something called the ***EVM bytecode*** which gets deployed to the Ethereum blockchain
  - Ethereum runtime environment only understands and can execute the bytecode
- ***Ethereum Virtual Machine (EVM)***
  - Ethereum Virtual Machine is a simple but powerful, ***Turing complete*** 256bit Virtual Machine that allows anyone to execute arbitrary EVM Byte Code
  - EVM is part of the Ethereum Protocol and plays a crucial role in the consensus engine of the Ethereum system
  - Allows anyone to execute arbitrary code in a trust-less environment in which the outcome of an execution can be guaranteed and is fully deterministic

Bytecode & EVM

Solidity Source Code

Compiled Byte Code

Deployed to EVM

Components of an Ethereum Blockchain

- ***P2P network***

  Ethereum runs on the Ethereum main network, which is addressable on TCP port 30303, and runs a protocol called ÐΞVp2p.

- ***Consensus rules***

  Ethereum's consensus rules are defined in the reference specification, the Yellow Paper.

- ***Transactions***

  Ethereum transactions are network messages that include (among other things) a sender, recipient, value, and data payload.

- ***State machine***

  Ethereum state transitions are processed by the Ethereum Virtual Machine (EVM), a stack-based virtual machine that executes bytecode (machine-language instructions). EVM programs, called "smart contracts," are written in high-level languages (e.g., Solidity) and compiled to bytecode for execution on the EVM.

- ***Data structures***

  Ethereum's state is stored locally on each node as a database (usually Google's LevelDB), which contains the transactions and system state in a serialized hashed data structure called a Merkle Patricia Tree.

- ***Consensus algorithm***

  Ethereum uses Bitcoin's consensus model, Nakamoto Consensus, which uses sequential single-signature blocks, weighted in importance by PoW to determine the longest chain and therefore the current state. However, there are plans to move to a PoS weighted voting system, codenamed Casper, in the near future.

- ***Economic security***

  Ethereum currently uses a PoW algorithm called Ethash, but this will eventually be dropped with the move to PoS at some point in the future.

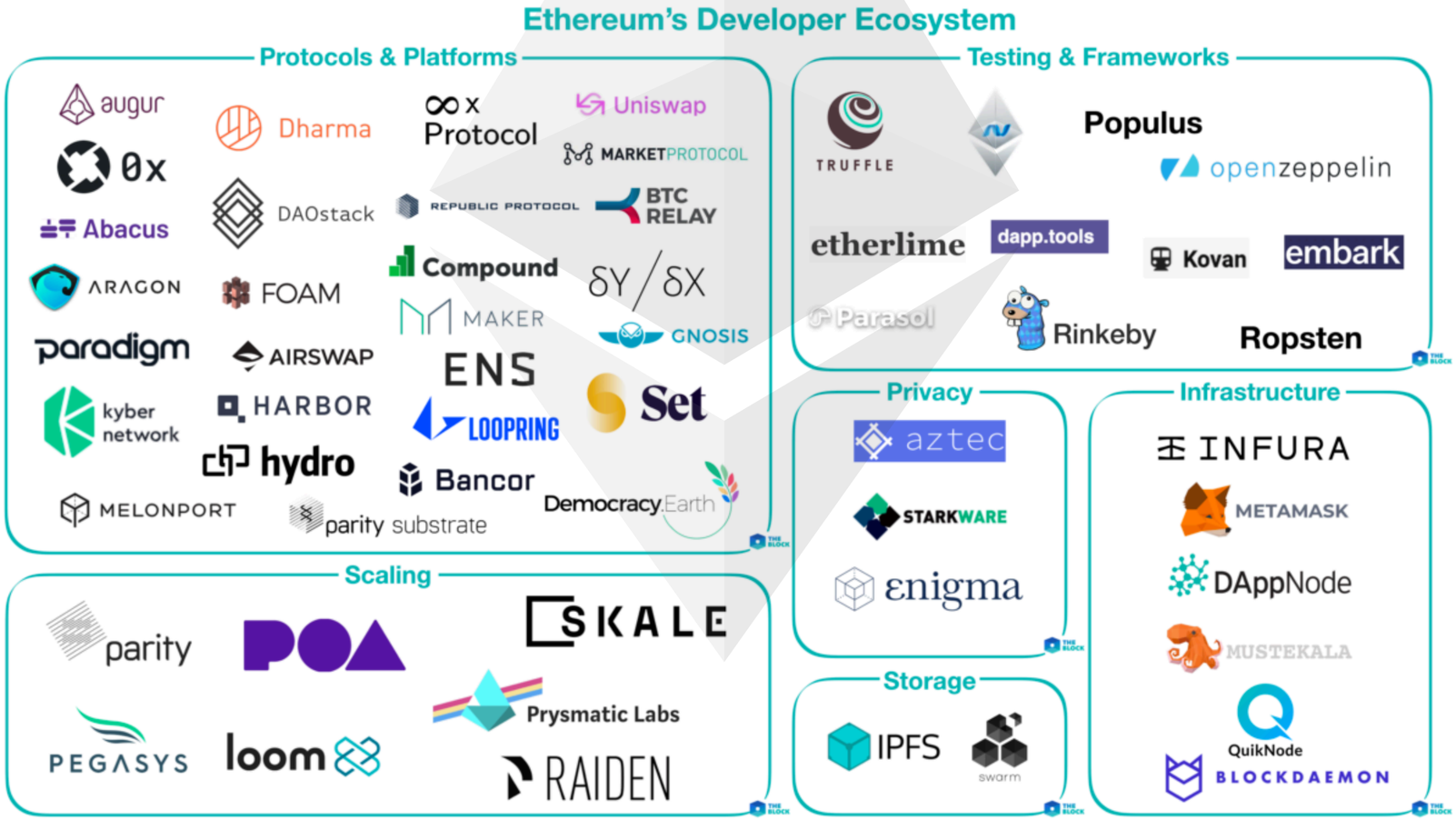
- ***Clients***

  Ethereum has several interoperable implementations of the client software, the most prominent of which are Go-Ethereum (Geth) and Parity.

From General-Purpose Blockchains to Decentralised Applications (DApps)

DApps represent a broader perspective than smart contracts

A DApp is, at the very least, a smart contract and a web user interface



Solidity

Ethereum Technical Concepts

SPDX and Pragma

- Smart-Contracts in Ethereum written in Solidity language has the extension sol

- Every Solidity Smart-Contract starts with a comment indicating its license called ***Software Package Data Exchange (SPDX)***. The comment is optional, however the compiler would complain a warning if not put

- ***pragma*** keyword specifies what version of the compiler are valid to compile this contract file

Contract.sol

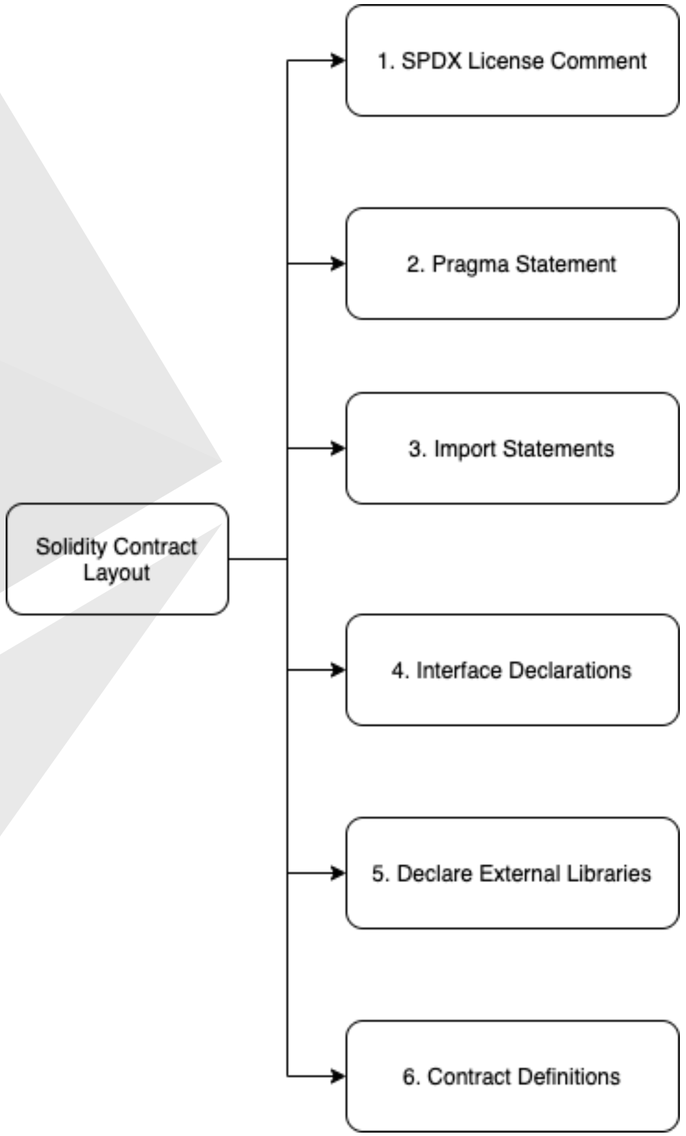
```
// SPDX-License-Identifier: UNLICENSED
pragma solidity >= 0.7.0 <0.8.0;
```

Solidity Contract Layout

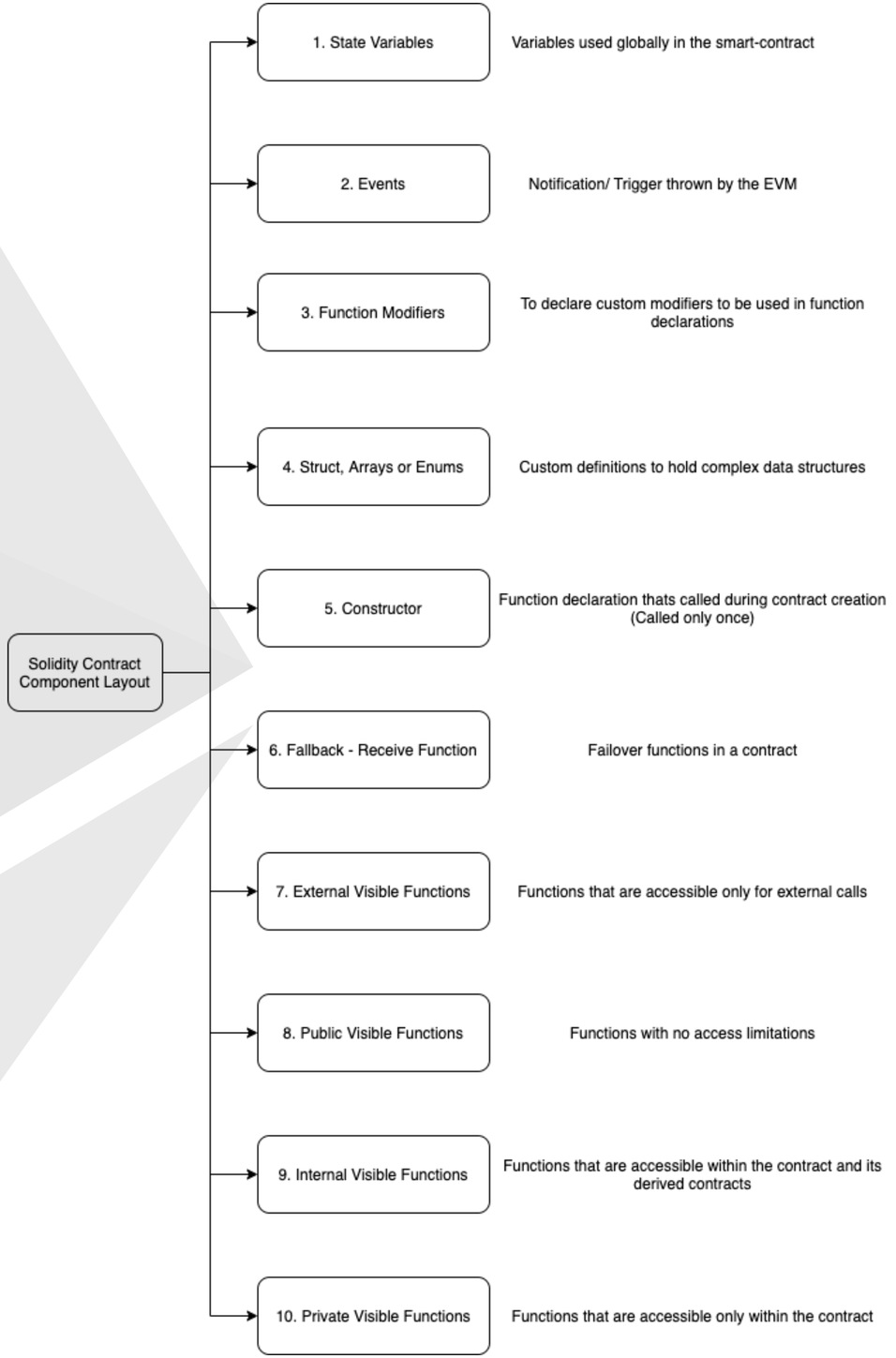
In a Solidity smart-contract, the following are *optional*

- **Import statements**
- **Interface declarations**
- **Usage of External Libraries**

The use-case around the smart-contract developed decides
If the optional elements must be used

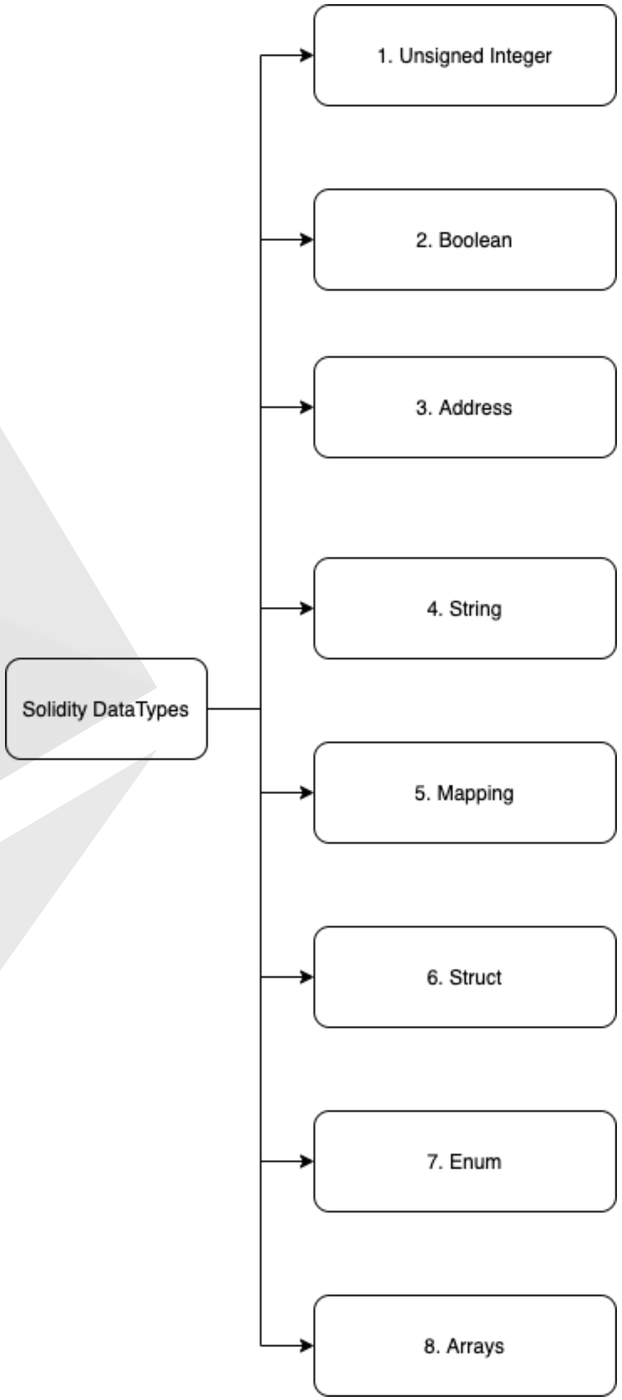


Solidity Contract Component Layout



Solidity DataTypes

- Integers in Solidity are unsigned - ***uint***
- Many variations of uint based on memory requirements
- Boolean - ***bool*** takes true or false
- Address - ***address*** to store the address of the contract or account
- String - ***string*** accepts any character array
- Mapping - ***mapping*** is a key-value datastore
- Struct - ***struct*** to define custom user-defined template
- Enum - ***enum*** to define pre-defined set of values
- Arrays - ***arrays*** to store a list of values of similar type



Let’s Build a Smart-Contract

Implement Event Voting in Solidity using Remix IDE

Workbook:- **https://pie-parmesan-e8a.notion.site/Workbook-Ethereum-Basics-818134253894454 09c9393aa740e0930**


Q & A

*** Learn Solidity - https://cryptozombies.io/en/solidity**