BLOCKCHAIN CLUB SVCT

SRI VENKATESWARAA
COLLEGE OF TECHNOLOGY
*Approved by* AICTE, New Delhi
*Affiliated to* Anna University, Chennai
*An Autonomous Institution*
*(Confered Autonomous Status by UGC)*

GITATHON
SVCT-BLOCKCHAIN CLUB

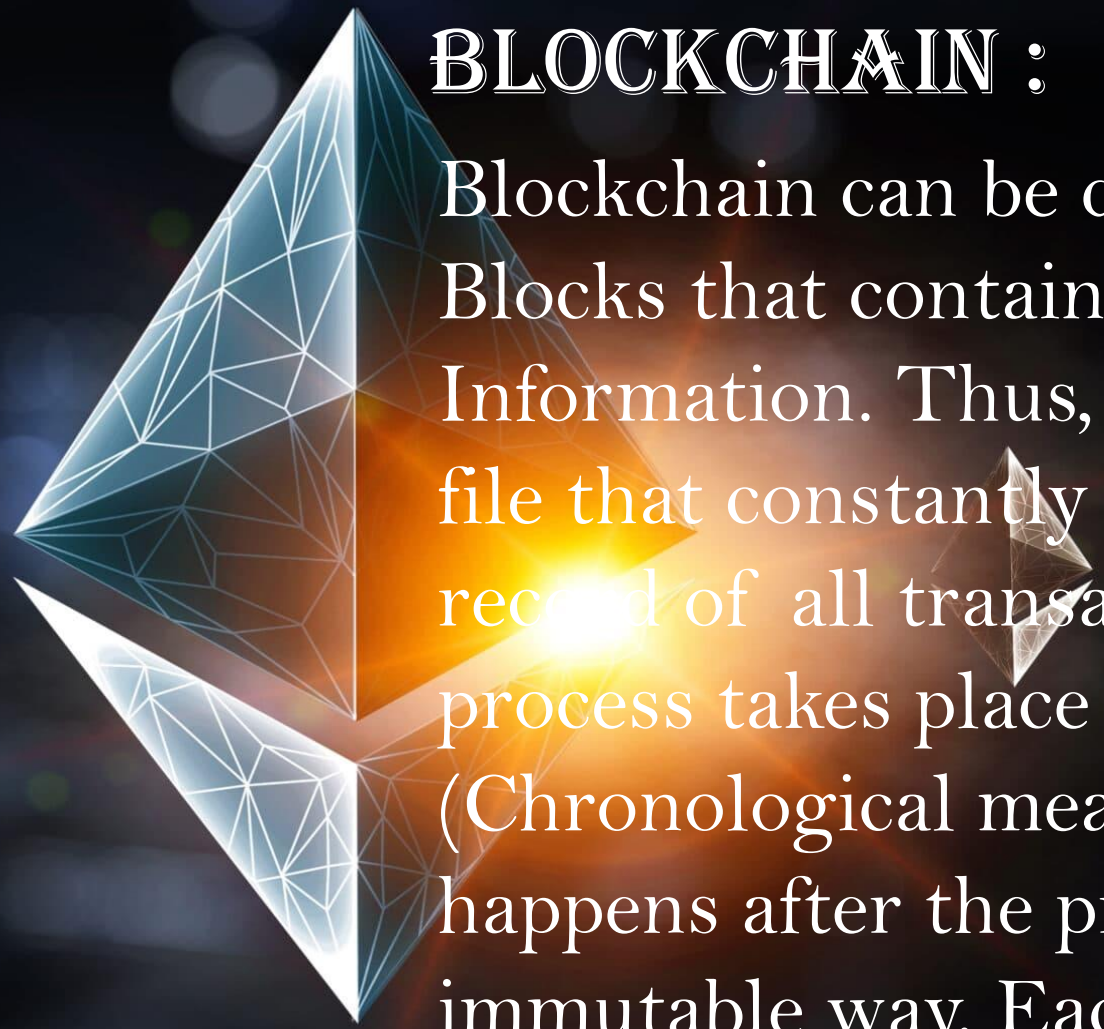
ethereum

# BLOCKCHAIN AND SMART CONTRACTS

Presented by:
R.Lakshmi Sravya
1st Year-AI&DS
SVCT-BLOCKCHAIN CLUB

# TOPICS

1.History of Blockchain
2.Consensus Algorithm
    Proof of Work (PoW)
    Proof of Stake (PoS)
3.ETHEREUM
4.Basics of Ethereum
5.Binance Smart Contracts (BSC)
6.Structure and Solidity Features



- # HISTORY OF BLOCKCHAIN :

Blockchain can be defined as the Chain of Blocks that contain some specific Information. Thus, a Blockchain is a ledger i., file that constantly grows and keeps the record of all transactions permanently. This process takes place a secure,chronological (Chronological means every transaction happens after the previous one) and immutable way. Each time when a block is completed in storing information, a new block is generated.

# WHAT IS MEANT BY CONSENSUS ALGORITHM??

A Consensus algorithm is a process in computer science used to achieve agreement on a single data value among distributed processes or systems. Consensus algorithm has two types which are Proof of Work (PoW) and Proof of Stake (PoS).

# PROOF OF WORK (POW) :

Proof of work is a blockchain consensus mechanism that incentivizes network validation by rewarding miners for adding computational power and difficulty to the network.

## BENEFITS OF POW:

- A Hard-to-find solution.Yet , easy verification.
- It is easy to implement when compare with other blockchain machanisms.
- It is fault-tolent.

## LIMITATIONS OF POW:

PoW is a time and energy-consuming process.

- It needed heavy expenses for hardware'
- Risk of denial of service attacks by intruders.

# Proof of Stake (PoS):

Proof of Stake is a cryptocurrency consensus mechanism for processing transactions and creating new blocks in a blockchain.A consensus mechanism is a method for validating entries into a distributed database and keeping the database secure.

## Key points of PoW:

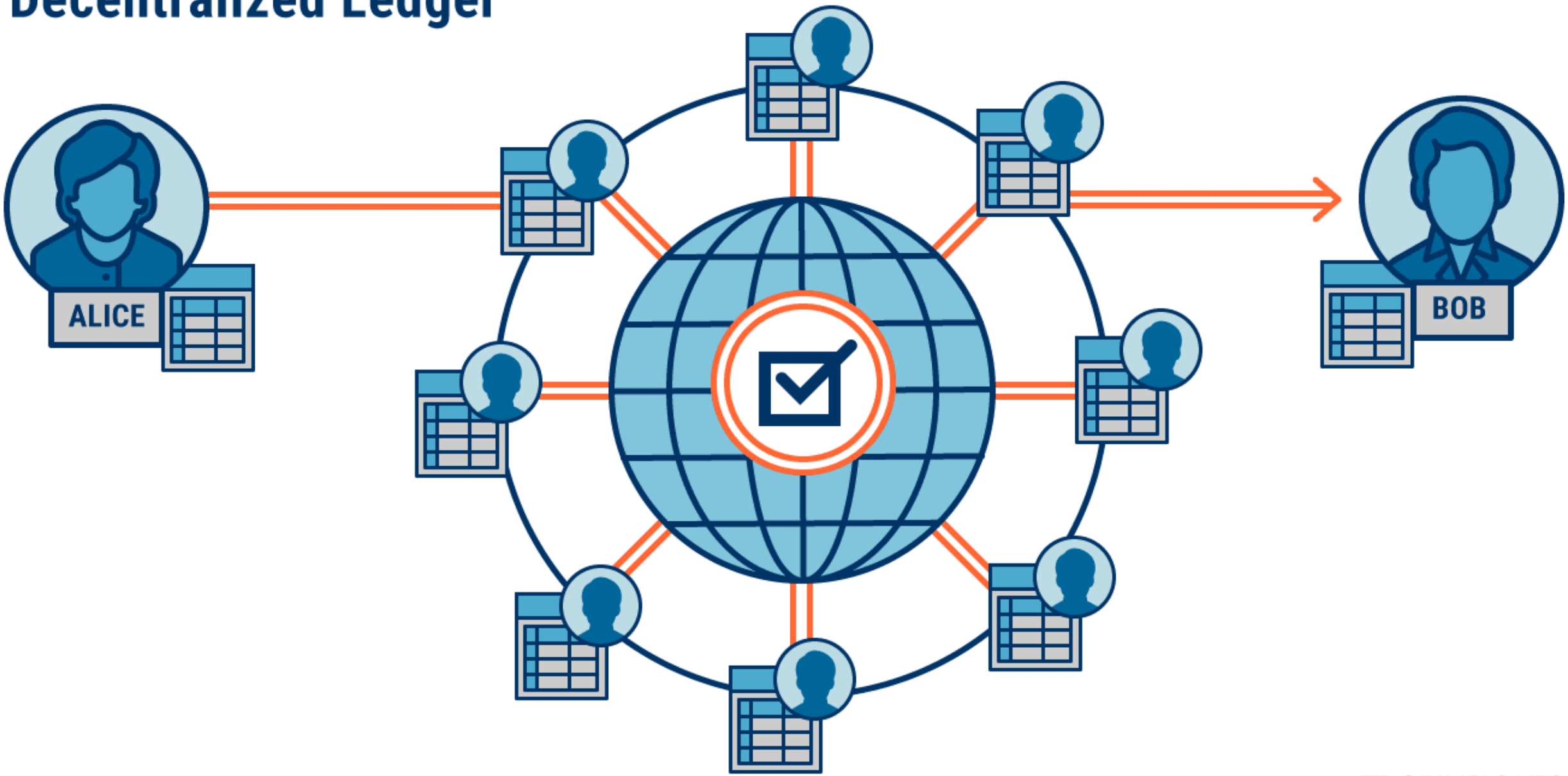
- Under Proof of Stake ,validators are chosen based on the number of staked coins they have.
- Proof of Stake was created as an alternative to proof of work, the original consensus mechanism used to validate transactions and open new blocks.
- Proof of Stake is seen as less risky regarding the potential for an attack on the network, as it structures compensation in a way that makes an attack less advantages.

# Ethereum

*[i-ˈthir-ē-əm]*

An open-source blockchain that is known for its smart contracts functionality, and which serves as the basis for the cryptocurrency ether (ETH).

# Decentralized Ledger



# Ethereum: The Go-To Blockchain Technology for Business Solutions

Flourishing Ethereum Ecosystem: A Six-Year Snapshot


**8,670**
Nodes Running on Ethereum Network

**150M+**
Total Unique Addresses

**116M+**
Total Ethereum supply

**3,000+**
Total Dapps

**500K**
Daily Active Dapp Users

**9.3M**
Total Eth Locked in DeFi

**Global Processes**
1.183M
Transactions/Day

**Tens of Thousands of Developers**
Growing Global Community

Stats as of July 15, 2021

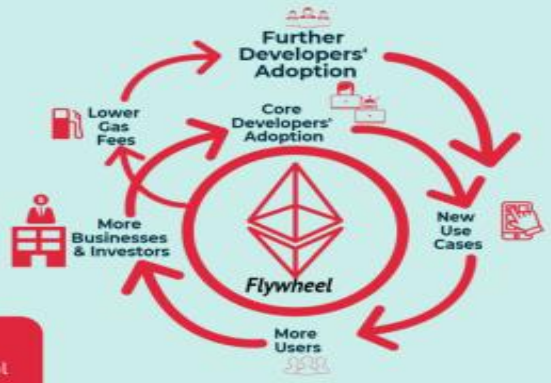
Nevina Infotech
Delivering Innovative Technology Solutions

# Advantages of Ethereum

1. Immutable
2. Decentralized
3. Fast transactions
4. Secure
5. Reliable

# Ethereum Ecosystem And Its Business Models

Ethereum was launched in 2015 with its cryptocurrency, Ether, as an open-source, blockchain-based, decentralized platform software. Smart contracts are enabled, and Distributed Applications (dApps) get built without downtime or third-party disturbance. It also helps developers build and publish applications as it is also a programming language running on a blockchain.




**Mission**
Enable the development of a decentralized web via decentralized applications, decentralized autonomous organizations, and decentralized finance (and many other use cases).

**Vision**
Create a new model for the web, there no single entity is in charge.

**Value Propositions**
**Simplicity**: the Ethereum protocol should be as simple as possible, even at the cost of some data storage or time inefficiency.
**Universality:** a fundamental part of Ethereum's design philosophy is that Ethereum does not have "features".
**Modularity**: the parts of the Ethereum protocol should be designed to be as modular and separable as possible.
**Agility**: details of the Ethereum protocol are not set in stone.
**Non-discrimination and non-**

**Value Model**

**Economic Model**

- Mining Incentives (Eth
- Tokenization and ICOs
- Staking Incentives (Eth 2.0)
- Platform for decentralization

**Blockchain Model**

- Proof-of-Work (Eth 1.0)
- Proof-of-Stake (Eth 2.0)

**Distribution Model**

- Core Development Team lead by the foundation
- Fast-evolving protocol, with thousands of potential commercial use cases
- Institutional and enterprise partnerships on top of Ethereum
- Ability to launch own token on top of Ethereum

# Binance Coin (BNB)

Network currency of Binance ecosystem, in top 5 list, and an excellent investment.

**Network**
Binance Smart Chain

**Founder**
Changpeng Zhao

**Growth since launch**
610125.55% (Aug 2023)

**Launched**
July 2017 on ERC
Sept 2019 on BSC

**Launch Price**
$0.17 / BNB

**ICO Round**
Raised $15 million
Sold 100M BNB for 15 C

**Market cap**
$37,261,183,213 (2023)

**Market Dominance**
3.093%

**Circulating Supply**
153.86 million

**Max Supply**
200 million

**All Time High**
$690(May 10, 2021)

**All Time Low**
$0.096 (Aug 01, 2017)

**Events**
Migration from ERC to BSC chain.
Rally to 1062.26% in Dec 2021.
$575M of burning in Jan 2023

**Use Cases**
Goods & Services Payment
Less Transaction Fees
Participate Sales in DeFi

**Social Media**
- Twitter – 10.6 M
- Youtube – 606 K
- Instagram – 3.7 M
- Telegram – 550 K

**Products**
Binance Exchange,
BEP20 Smart contracts

**Price Prediction**
2025–$606.00/BNB
2030–$2081.00/BNB
2035–$2,657.35/BNB
2050–$4,343.68/BNB

CoinPedia.

www.coinpedia.org

# STRUCTURES AND SOLIDITY FEATURES:

A struct is a creative data structure format in Solidity where variables of diverse data types can be bundled into one variable or a custom-made type. Once the data types are grouped into a struct, the struct name represents the subsets of variables in it.

# What is SOLIDITY Blockchain

## Solidity Smart Contracts

## Features of Solidity

- Contract-oriented
- Static typing
- Modifiers
- Events
- Library functions
- Ethereum Virtual Machine (EVM) compatibility

@contractsaudit

# Concepts You Should Know to Understand Solidity

## Ethereum

Ethereum is an open-source blockchain platform that offers smart contract facilities. Solidity was first introduced as a new type of programing language for the Ethereum platform.

Ether is the primary token for the platform. This platform is dedicated to developers for helping them develop and deploy decentralized applications.

101 Blockchains

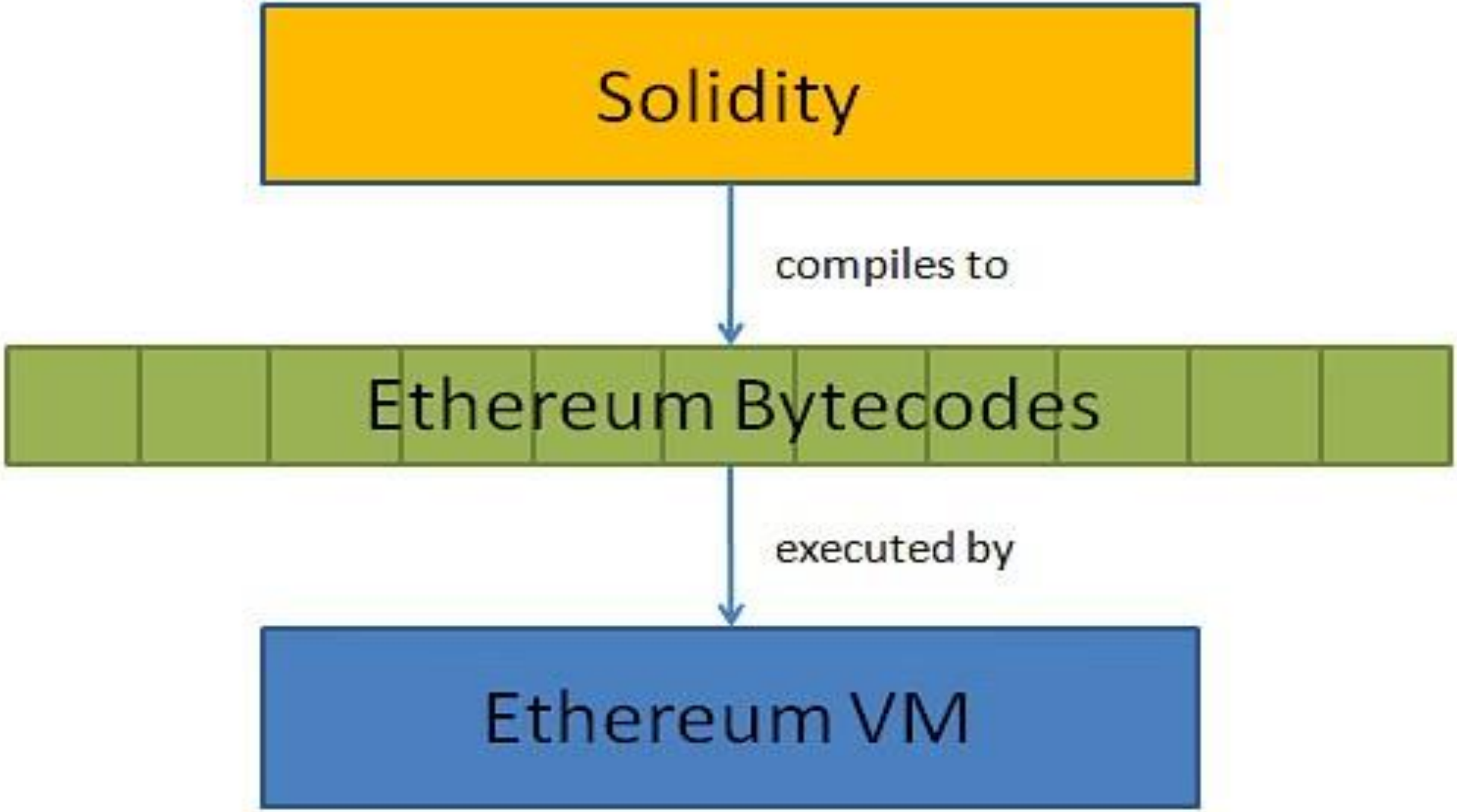
# Understanding the Solidity Syntax

- **Pragma:** In Solidity, a pragma language will specify how the compiler will process any type of input. Typically, the first line of code in Solidity based smart contracts contains the pragma.
- **Contract:** uintstoredData component within the code will denote the Solidity contract. This part will contain all the data and code needed for locating a particular address within the blockchain.
- **File Importing:** Solidity offers similar support for file import systems like JavaScript.

# Solidity

## Smart Contract Developer

## For EVM-Compatible Blockchain



Solidity
compiles to
Ethereum Bytecodes
executed by
Ethereum VM

101 Blockchains

# TOP 10 SOLIDITY ISSUES

## UNCHECKED EXTERNAL CALL

The send and call function will return a Boolean value which return a false value in terms of exceptions but will not revert the transaction.

## REENTRANCY

External calls from a contract are vulnerable and hackers can misuse the code to re-enter the contract to perform malicious activities.

## COSTLY LOOPS AND GAS LIMIT


An attacker can include infinite loops within an array to exhaust the Gas limit mimicking a DoS attack and freeing the transaction.

## CLEARING MAPPINGS

Deleting a dynamic storage array that uses Mapping as the base type won't clear the Mapping as it's a storage-only key-value data structure.

## UNEXPECTED ETHER

Contracts that rely on code execution for every single Ether transaction are vulnerable because it can send Ether forcibly to another contract.

## ARITHMETIC PRECISION

Solidity does not support any floating or fixed-point numbers. Thus, the 256 bits Ethereum Virtual Machine packets data types shorter than 32 bytes into the 32 bytes slot.

## RELYING ON TX.ORIGIN

Attacker can hide a withdraw function within the tx.origin variable to create a phishable contract and invoke a fallback function to steal all the funds.

## DEFAULT VISIBILITIES

Default visibility of functions are public so without visibility specifiers any external user can call that function to receive funds from a contract.

## OVERFLOW AND UNDERFLOW

The underflow or overflow issues happen when a user is trying to store a value that is out of the Solidity data type's range.

## TIMESTAMP MANIPULATION

Miner's have the freedom to change the timestamp, which is risky if they're using it incorrectly in the smart contract.

# THANK YOU ALL...!!!


**Presented by:**
**R.Lakshmi Sravya**
**1st Year-B.Tech**
**Dept:AI&DS**
**SVCT Blockchain Club.**