# Cryptocurrency, Bitcoin and Ethereum

Department of Computer Science and Engineering

Indian Institute of Technology, Jodhpur

# Cryptocurrency

# Cryptocurrency

- **Cryptocurrencies** are the digital or virtual currencies working on the **cryptographic principles**.
- As the name indicates, it doesn't have any physical existence or they are not tangible.
- They merely exist as a set of **programming codes.**
- Yet provides **high security and usability** than many existing currencies.
- Cryptocurrency works on blockchain technology, we have already seen how blockchain works.

# Cryptocurrency

- **In the case of cryptocurrency,** the ledger keeps the track of cryptocurrency that is generated and transacted across the network.
- Every individual in a particular blockchain will have a **unique account Id/address.**
- The cryptocurrency is always associated with this accounts (Currency is Debited and Credited to this account)

# Wallets

- People can manage their account through the **application called wallets.**
- **Through the wallets, anyone can make the transaction to anyone on the network** (both the sender and receiver must have an account).
- The transactions are verified by nodes and added to the blockchain ledger.
- So the immutable and encrypted ledger of blockchain is the backbone of cryptocurrency.

# Example

- Suppose initially, my wallet has credited with 100 units of cryptocurrency.
- From there onwards every movement of every unit of currency will be recorded in the public ledger, every participating node in the network can watch the past as well as the present of each unit of currency in the system.
- Thus it will be a more transparent monetary system.

# Cryptocurrency

- Other notable features of blockchain are also applicable to cryptocurrency; the encryption mechanism, peer to peer network, and no central authority/central server to control.
- Each cryptocurrency will be working on a blockchain protocol.
- One of the most famous cryptocurrency is bitcoin which relies on the bitcoin blockchain.
- And ether is another fast-growing cryptocurrency which runs on Ethereum protocol.
- While comparing with the traditional currencies, the cryptocurrencies provide highly anonymous nature for participants.
- The only visible identity of a user will be his account ID, rest everything will be encrypted.
- The participants will not have any idea about the real identity of a user.

# Advantages

- Transaction Speed
- Anonymity
- No restriction on payments
- Less /No transaction fees
- Immutable transactions
- Government can’t De-monetize
- Secure Payment information

# Disadvantages

- Less Acceptance
- Inconsistent rate
- Government Ban
- Key recovery is impossible
- Supports Money Laundering/Black Market

# Buy Bitcoin

- The easiest way to own Bitcoin is to buy them from a bitcoin exchange.
- There are a number of online bitcoin exchanges which exchange normal currency to bitcoin.
- People can exchange their normal currency for bitcoin and move it to their wallet.
- Another method to own bitcoin is to participate in Bitcoin mining.

# Transactions

- Sending bitcoin from one account to another is called as a transaction. It is usually done through wallets.
- The wallet app will provide an interface where we can input the account Id of the recipient and the amount we wish to transfer.
- Once we have made the transaction, the miners will verify the transaction and add to the blockchain ledger if it is a legitimate one.
- In Bitcoin, the transactions are cost-free. Usually, a transaction validation time is about 10 minutes in bitcoin, but if we give a small transaction fee we can speed up the process.

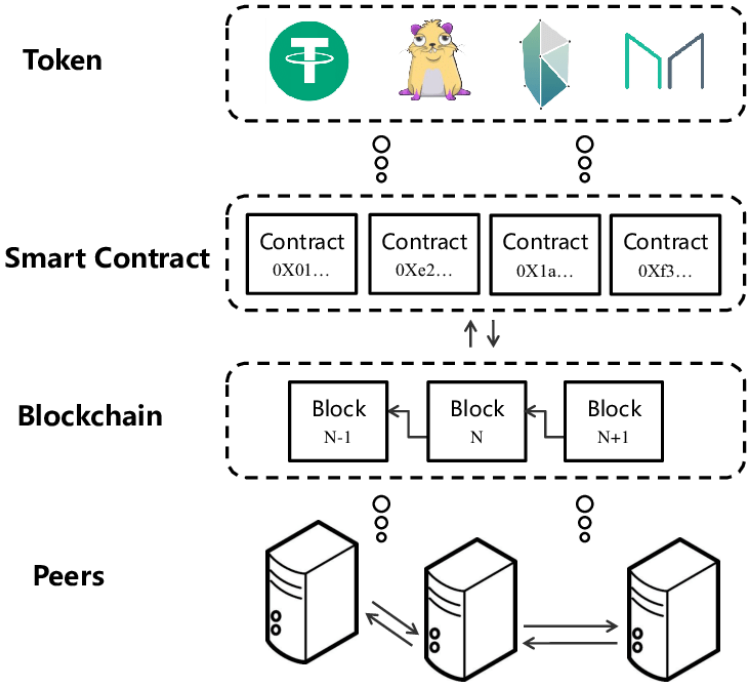
# Bitcoin Mining

- The mining is the most important as well as the interesting topic in bitcoin.
- This is the process by which new transactions are validated and added to the socalled ‘blockchain’.
- This demands dedicated mining hardware and thus, not all nodes are involved in mining.
- Those nodes who are participating in mining process is known as ‘miners’ .
- When a new bitcoin transaction happens in the network that is broadcasted on the network.
- The miners listen to this broadcasting and engage in transaction verification. Once the transactions are verified they are added to a block.

# Ethereum

- Ethereum is an Open Source Blockchain platform which allows anyone to develop and deploy Blockchain based Applications.
- **Any kind of application including cryptocurrency, tokens, wallets, social apps etc. can be developed and deployed in a Distributed Environment of Ethereum.**
- In other words, rather than sticking with the cryptocurrency alone, Ethereum opened the possibilities of the 'blockchain' and 'distributed ledger' technology to other application domains.
- Ethereum is not a single network rather it is more like a protocol for internode communication. Actually, in Ethereum many networks exist alongside.

# Overview of Ethereum Blockchain



# How to be the part of Ethereum?

- Basically, there is two type of users in a typical Ethereum blockchain. The one who issues a DApp (or a smart contract) and others who participates in the contract.
- Every user will have an account in Ethereum, they are called Externally Owned Accounts (EOA).
- Same way every DApp will have an account address in Ethereum known as Contract Accounts.
- User transaction is associated with these unique accounts. Users can make transactions with both other EOA accounts as well as Contract Accounts.

# DApp is the ‘Decentralized Applications

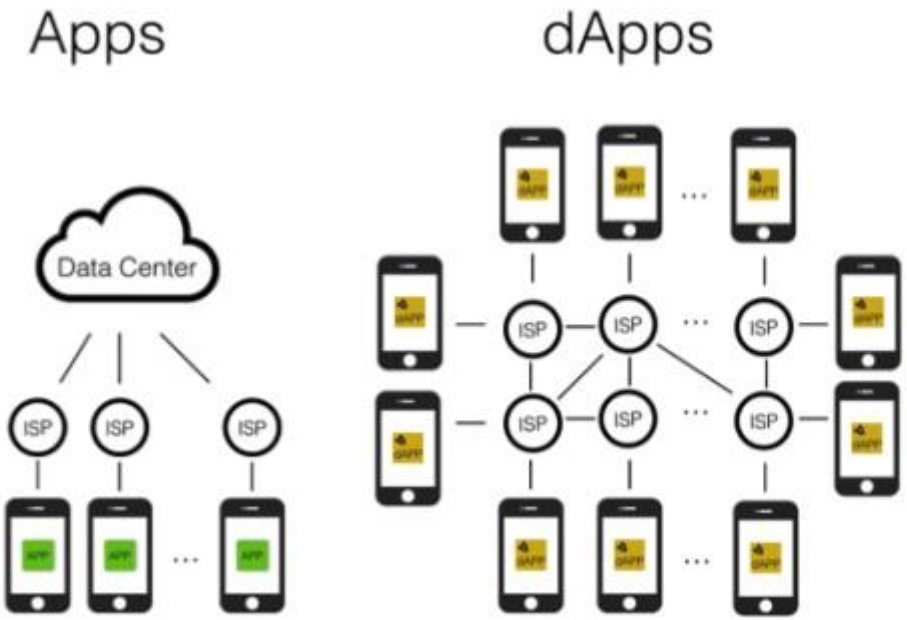
- DApp is the ‘Decentralized Applications’ running on the blockchain.
- They are the applications that run on blockchain without any centralized control.
- We can say bitcoin is a decentralized application that runs on Bitcoin blockchain.
- But it is the Ethereum blockchain that extended the scope of decentralized application and popularized the word DApp.
- DApp uses the shared ledger instead of a server to record and store all the transactions.

# DApp is the ‘Decentralized Applications

- The DApps will have a set of backend codes as well as a user interface.
- In Ethereum, these backend codes will contain the **smart contract** and the front end will provide a **user interface** for the user to interact with the blockchain.
- Once the smart contracts are deployed on the blockchain, then the Dapp will become accessible in the blockchain.
- Then any node in the blockchain network can use the DApp.
- The DApps can be developed for any business use cases.
- Any application that
  is currently running on the client-server model can be implemented as a DApp.

- Some examples of Ethereum DApp:- Green Ether Project, splitcoin, The immortals

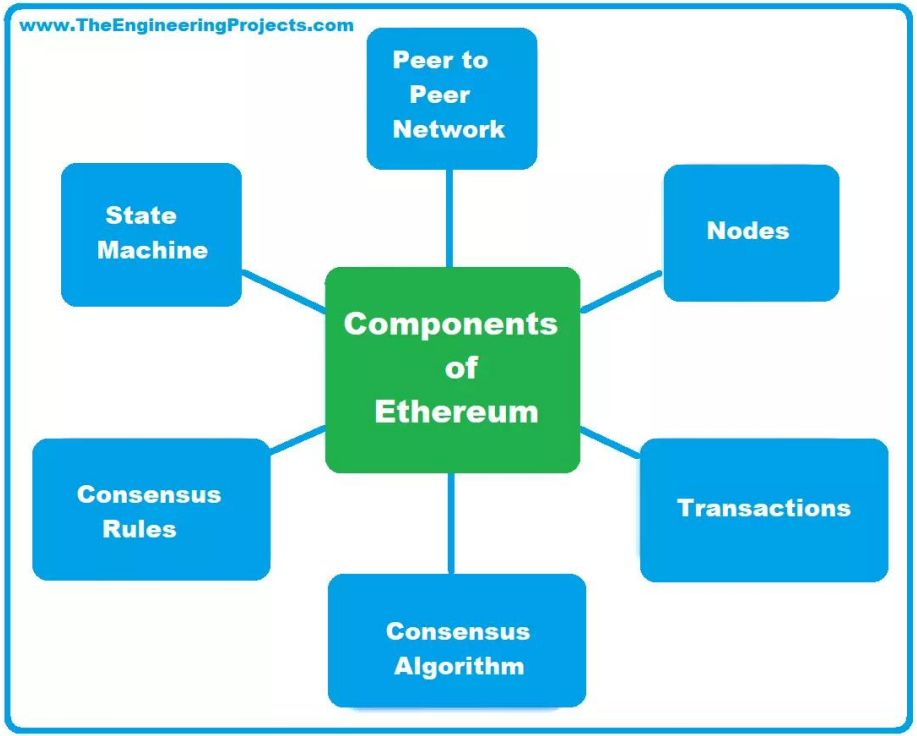
# Apps and dApps



# Components of Ethereum

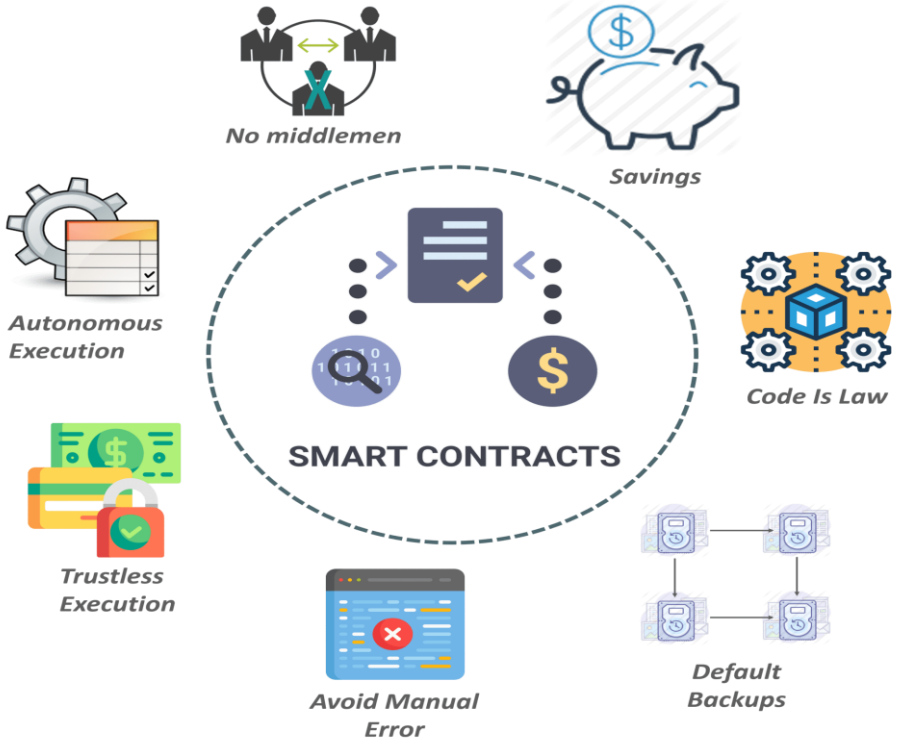
- **Smart contracts**
- **Ether**
- **Ethereum Clients**
- **EVM**
- **Etherscripter**

# Components of Ethereum



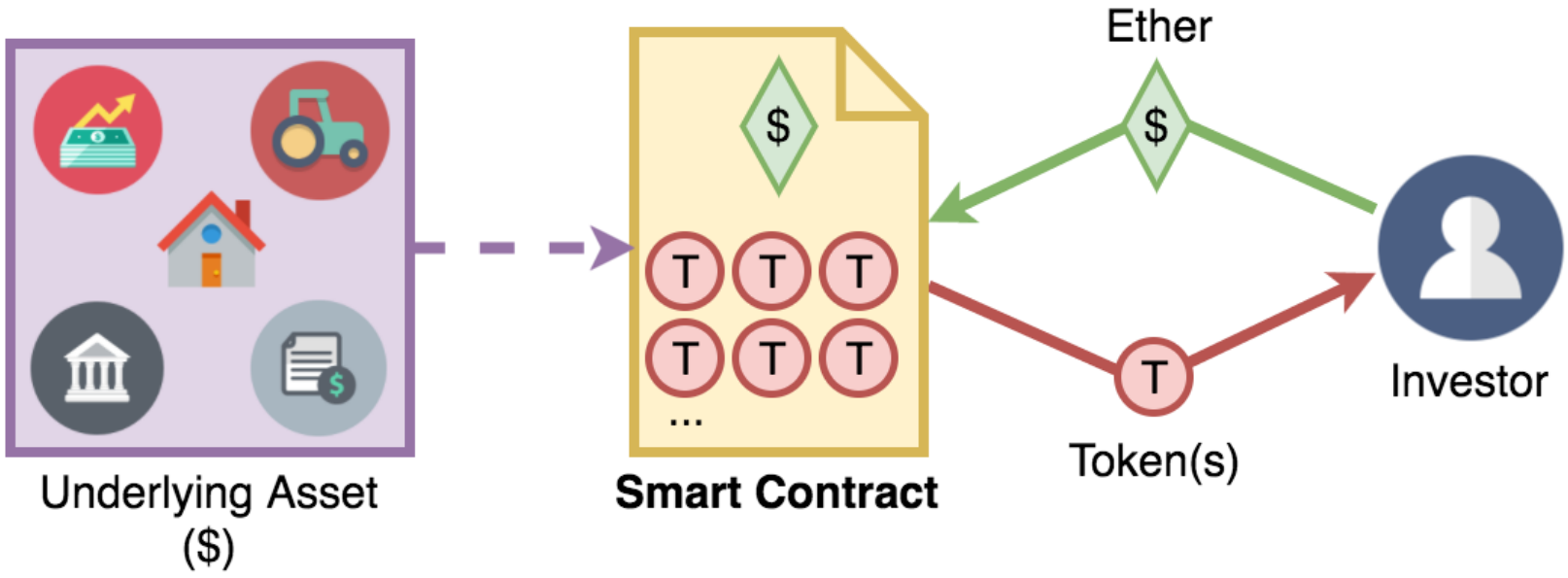
# Smart contracts

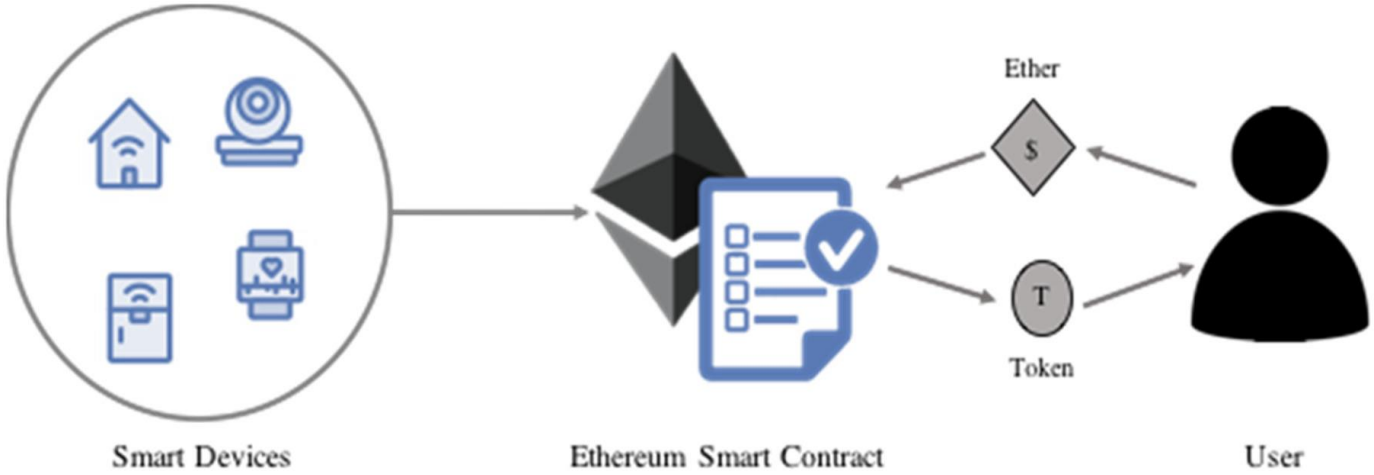
- Smart contracts are the nerves of Ethereum blockchain framework. All the operations in Ethereum are controlled with smart contracts.
- Smart contract is the digital version of contracts; which is executed automatically upon satisfying predefined conditions.
- Of course, they are lines of codes and it is used to exchange anything of value in a more secure and transparent way.
- In Ethereum, these smart contracts are written in solidity programming language.
- The smart contract will provide the direct contract execution between sender and receiver without a middleman.


No middlemen
Savings
Autonomous Execution
SMART CONTRACTS
Code Is Law
Trustless Execution
Avoid Manual Error
Default Backups

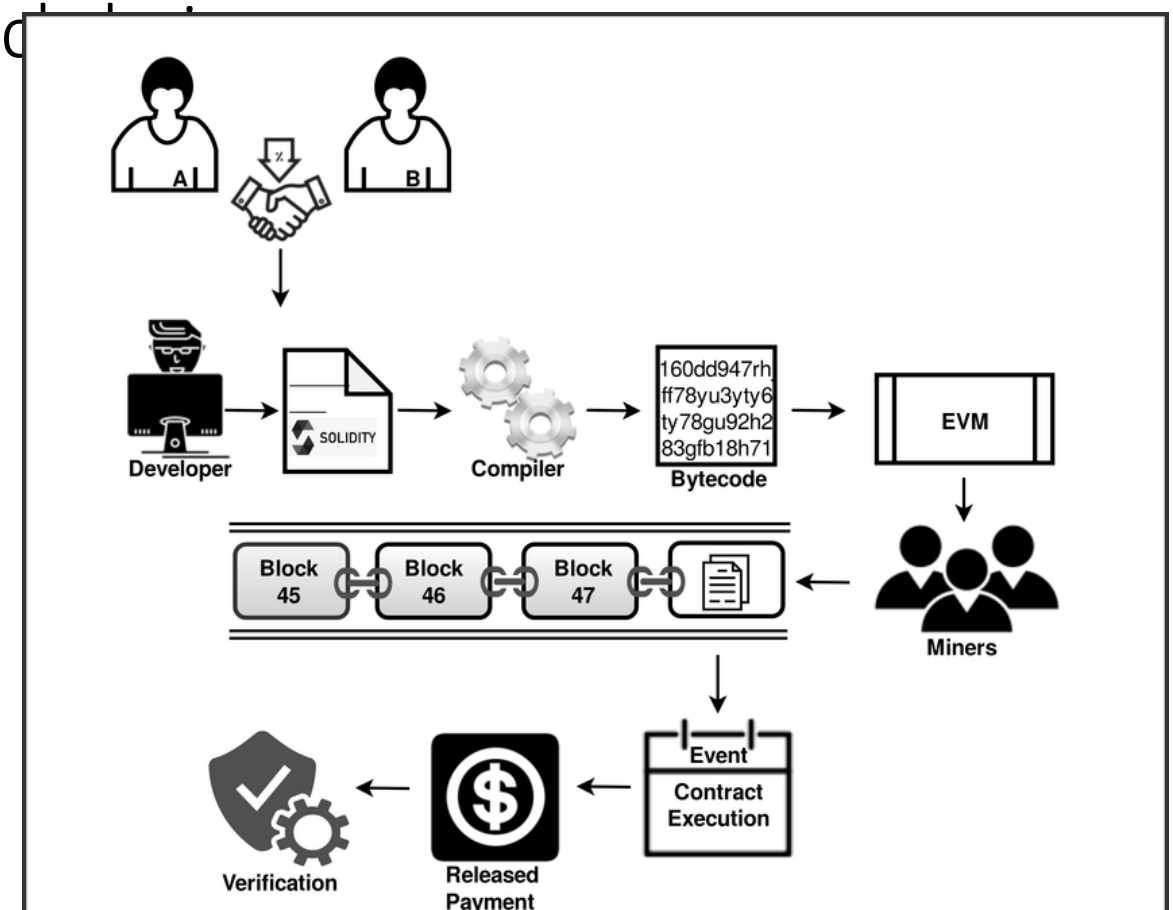
# Working of a Smart Contract.

- First, a contract account is created in Ethereum blockchain. The contract will have specific rules and actions based on that rules
- The contract is then coded. In Ethereum, the smart contract is coded in Solidity; an Ethereum compatible high-level language.
- The coded contract is deployed in Ethereum network. The deployed contract will have a unique public-key address, the address is used to reach the contract in the network. Once the contract is deployed in, it can't be modified even by the Issuer.


Ether
$
$
T
T
T
T
T
T
...
T
Underlying Asset
($)
Smart Contract
Token(s)
Investor


Ether
$
T
Token
Smart Devices
Ethereum Smart Contract
User

# Total cycle of smart contract execution over Ethereum blo



# Ether

- Every collectively run network need some fuel to exist.
- Bitcoin is the fuels of bitcoin network and Ether is the fuel of Ethereum.
- Ether is the cryptocurrency of Ethereum network, and it is the backbone of transactions in Ethereum.
- Ethereum website put it in this way “Ether is a form of payment made by the clients of the platform to the machines executing the requested operations”.
- Similar to the blockchain, the Ethereum network exists in a consistent state because of the computational and other resources spent by individual nodes, Ether is the reward provided to those individual nodes.
- As more people getting interested in Ethereum, the value of Ether is also surging on daily basis. Today, Ether is the most demanded cryptocurrency after Bitcoin.

# Ethereum Clients

- Ethereum Clients are the tools used to connect to the Ethereum blockchain for developmental or mining purposes. Some of the Ethereum clients are listed below :
  - Geth — Geth is an Ethereum client working in GO language. Geth has a command line interface (CLI) tool that communicates with the Ethereum Network and acts as the link between the different nodes in the network.
  - Eth — C++ Eth is a powerful Ethereum client which is more focused on miners.
  - Pyethapp — this client is useful for DApp development using python. 'Pythapp' is also an excellent choice for research and academic purpose in Ethereum blockchain.

# EVM

- The EVM is the engine behind the whole Ethereum blockchain.
- Smart contracts are run on the Ethereum Virtual Machine (EVM) - the decentralized, consensus-driven computer which distinguishes Ethereum from earlier Blockchains.
- This Virtual Machine runs its own language of bytecode.
- For this reason, several languages for writing contracts have been developed.

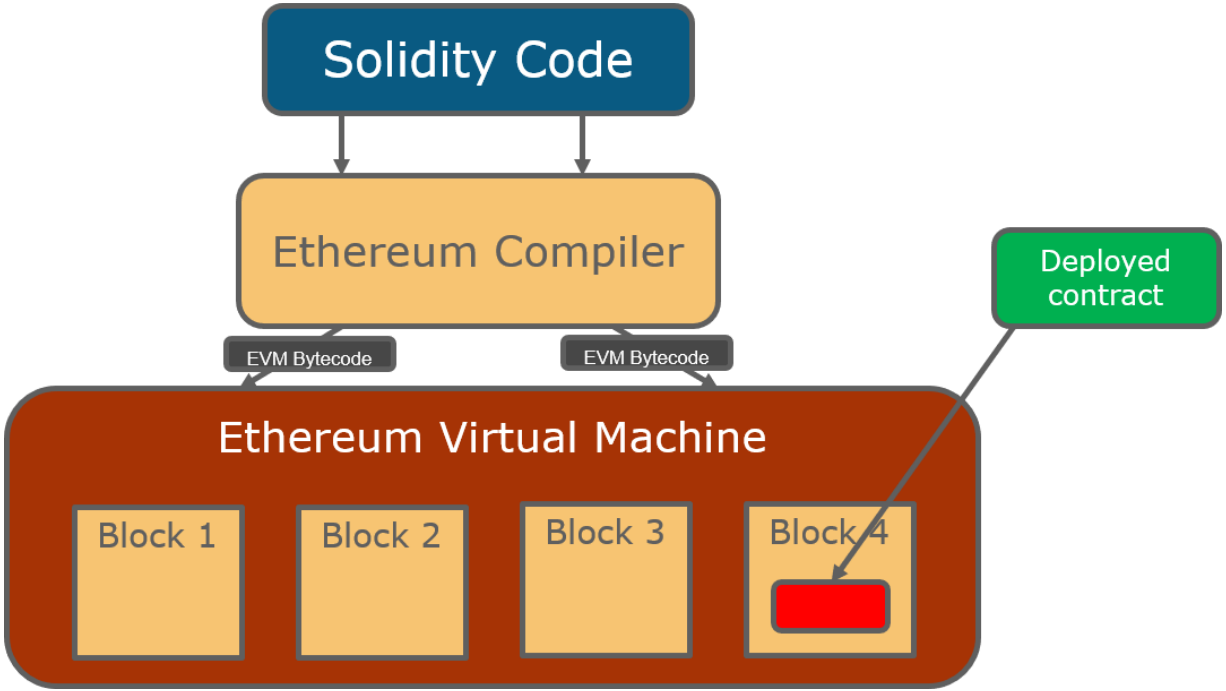
# Solidity

- Of these, the most popular one is Solidity.
- Solidity is a JavaScript-like language developed specifically for writing Ethereum Smart Contracts.
- The Solidity compiler ‘sol-c’ turns this code into Ethereum Virtual Machine bytecode, which can then be sent to the Ethereum network, as a transaction to be given its own address.
- Every participating node will have an EVM installed in it.

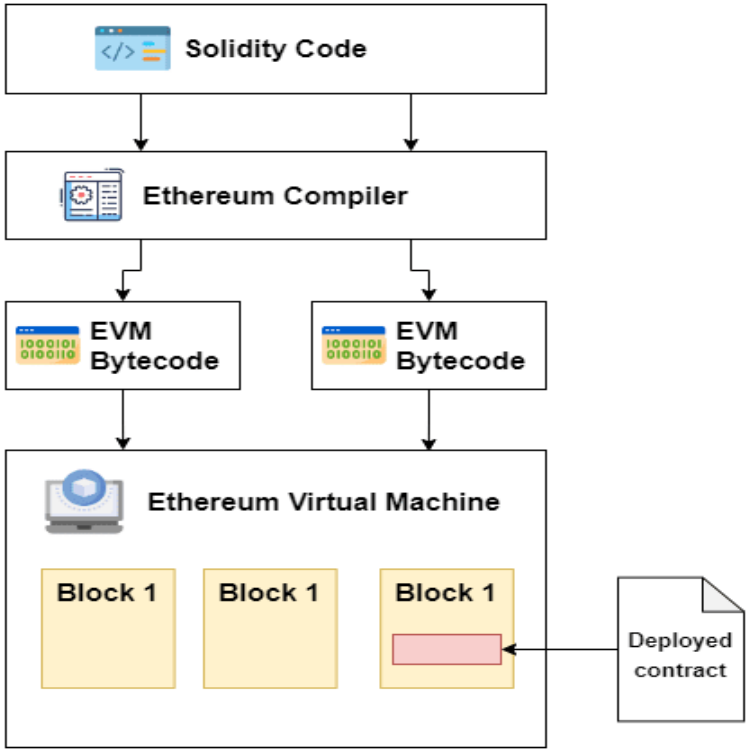
# Etherscripter

- Etherscripter is a visual smart contract builder tool in Ethereum.
- It provides a GUI for creating smart contracts in simple steps.
- Etherscripter provides a simple drag and drop interface where the corresponding backend codes in Serpent, LLL, and XML will be generated automatically.
- Using Etherscripter even a non-programmer can create smart contracts.

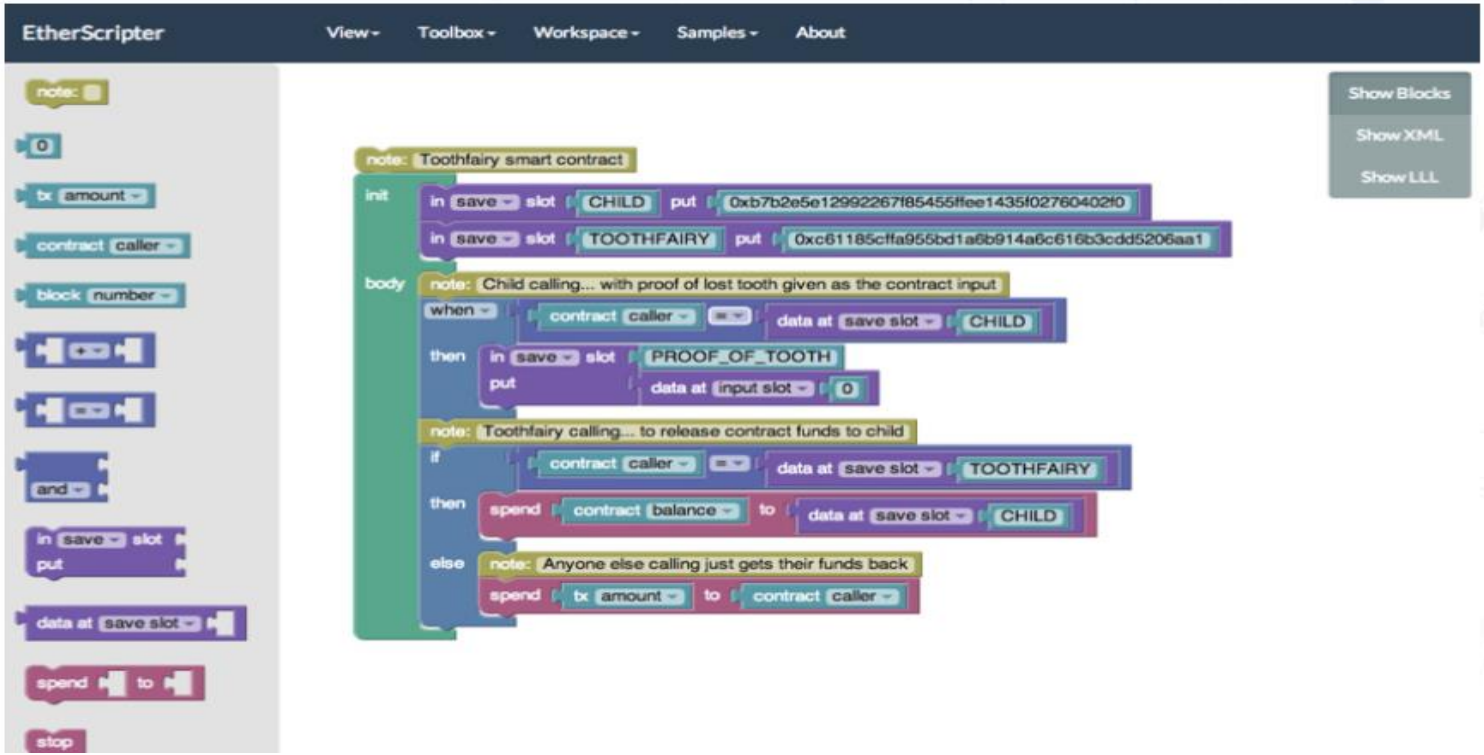
# Ethereum Archicture



# Ethereum Archicture



# Etherscripter




THANK YOU