

The Ethereum Network

Siddhesh V Naik
Anil Dongre

DISCLAIMER

*The opinions presented/stated during this workshop are of the speakers alone.
They are not to be attributed to anyone else.*

AGENDA

- ✓ Reimagining Bitcoin
- ✓ Why Ethereum
- ✓ What is Ethereum
- ✓ The Trilemma
- ✓ Proof Of Stake
- ✓ Private Blockchain

REIMAGINING BITCOIN

Can the supplier customer use case be built upon a bitcoin network?

NO

Why not?

Bitcoin's Script language is intentionally constrained to simple true/false evaluation of spending conditions. It is purpose built only to create a bitcoin, change ownership and burn a bitcoin

But the bitcoin model is powerful when...

Multiple untrusting parties must transact for business reasons and need a ledger that is continuously in sync between transacting parties. Some use cases are...

- Supply chain management
- Trade finance
- Identity management
- Foreign exchange settlement
- Insurance
- Banking and finance

All these are perfect cases for a DLT...

THE BIRTH OF ETHEREUM

2013 Vitalik Buterin started thinking of extending Bitcoin
In October that year he proposed flexible and scriptable contracts

But the approach was not Turing complete

In December Vitalik shared a whitepaper that outlined the idea behind Ethereum:

a Turing-complete, general-purpose blockchain

Vitalik and Dr. Gavin Wood refined and evolved the idea, together building the protocol layer that became Ethereum



WHAT IS ETHEREUM?

Ethereum is often described as "the world computer."
It's a deterministic but practically unbounded state machine, consisting of a globally accessible singleton state and a virtual machine that applies changes to that state.

LET'S BREAKDOWN THE DEFINITION- DETERMINISTIC

Property of the blockchain network required to arrive at a consensus

- ✓ Consensus because the network is decentralized
- ✓ Decentralization requires each participant to validate every transaction
- ✓ Every validation must result in same outcome. Else transaction cannot proceed
- ✓ In a distributed & decentralized system its inefficient to process and commit one transaction at a time hence transactions are collected in blocks
- ✓ Latency causes transactions to arrive at each participant node in an indeterministic manner
- ✓ Consensus includes single transaction validation and agreeing upon the order of transactions in a block
- ✓ Consensus makes the system deterministic




LET'S BREAKDOWN THE DEFINITION- UNBOUNDED

unbounded :

Overview Usage examples Similar and opposite words

Dictionary English ▾

Definitions from [Oxford Languages](#) · [Learn more](#)

 unbounded

adjective

having or appearing to have no limits.
"the possibilities are unbounded"

Similar: unlimited boundless limitless without limit illimitable unrestrained ▾



LET'S BREAKDOWN THE DEFINITION- UNBOUNDED STATE MACHINE

A state machine is a behavior model. It consists of a finite number of states and is therefore also called finite-state machine (FSM). Based on the current state and a given input the machine performs state transitions and produces outputs.

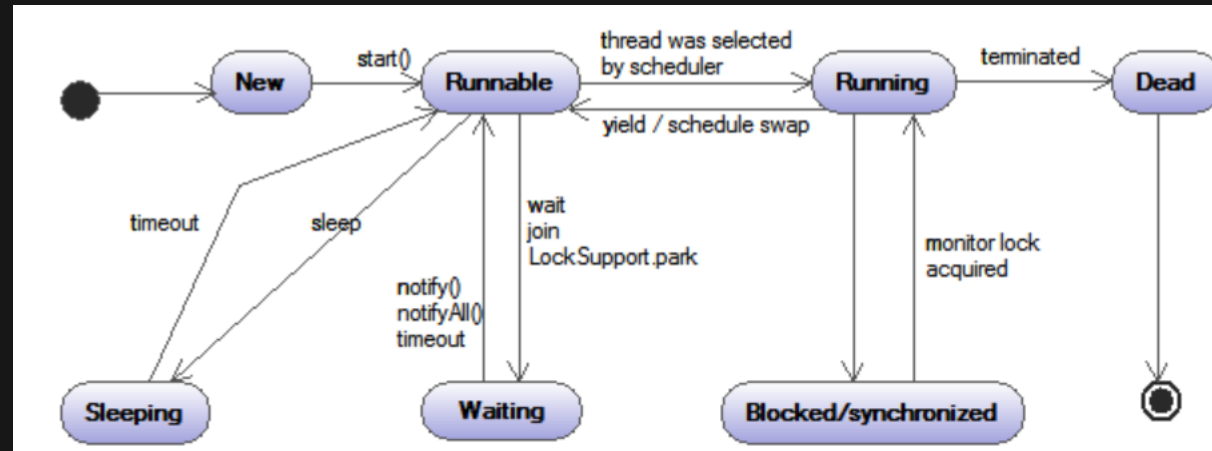


Image Source: [Tec Bar](#)

But ...

Ethereum network by definition and in theory is unbounded



LET'S BREAKDOWN THE DEFINITION-

GLOBALLY ACCESSIBLE SINGLETON STATE

A class that allows only a single instance of itself to be created and gives access to that created instance

But ours is not just a class. It's an unbounded state machine that is global. Which means its spread across the world



LET'S BREAKDOWN THE DEFINITION- VIRTUAL MACHINE THAT APPLIES CHANGES TO THAT STATE

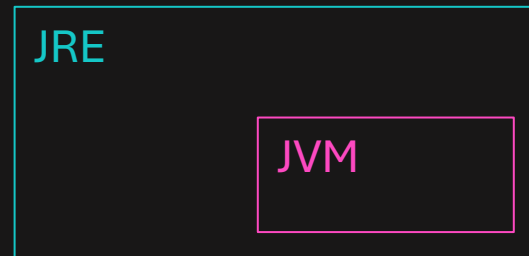
How does this state machine change state?

The system consists of a virtual machine that controls what changes get applied.

How does it do that?

It provides a runtime environment in which smart contracts are executed

Like Java has a JVM, Ethereum has an EVM



Java → Bytecode → JVM → Machine instructions

Solidity → Bytecode → EVM → Machine instructions



WHAT IS ETHEREUM?

Ethereum is an open source, globally decentralized Turing complete computing infrastructure that executes programs called smart contracts. It uses a blockchain to synchronize and store the system's state changes, along with a cryptocurrency called ether to meter and constrain execution resource costs.



LET'S BREAKDOWN THE DEFINITION- TURING COMPLETE

Turing complete describes a programmable system that can solve any computational problem. The concept comes from the Turing machine, a theoretical model of computation devised by English mathematician and cryptographer Alan Turing. Conversely, a non-Turing-complete system is limited to performing limited tasks based on pre-defined instructions..



LET'S BREAKDOWN THE DEFINITION- SMART CONTRACT

A Smart contract is also a piece of code. How is it different from traditional piece of code that runs on let's say an online ticket reservation web application?

- ✓ They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome
- ✓ The execution is not owned by a central party
- ✓ Every participant can see the code/terms of the contract
- ✓ Once deployed this code cannot be altered without the agreement of all the participants in the network
- ✓ Smart contract code runs at the same time (Well, almost at the same time. Network latency does play a role) on more than one server owned by distinct owners
- ✓ The execution is triggered by conditional events and once started no one can intervene in any way
- ✓ The code must be deterministic
- ✓ A transaction is committed only if there is a consensus among all or a pre-configured number of participants in the transaction about the transaction output
- ✓ Smart Contracts cannot access data from outside the blockchain system for ex. an external database or another API. Such data is provided by something called an Oracle



LET'S BREAKDOWN THE DEFINITION - CRYPTOCURRENCY CALLED ETHER

We hear Save Water slogans for water conservation awareness.
But for petrol we would fight if the pump attendant spilled a few drops outside the tank

Though you can live without petrol but not without water

WHY?

Simply because water is cheap

What if transactions in Ethereum were cheap or did not cost?

What is DDOS?

Its possible because its cheap

Infinite loop – A consequence of Turing complete system

Infinite loop is a reality and there must be a mechanism to break it



**So, how does ether help us against
DDOS or infinite loops?**



THE GAS FEES

Gas fees is the amount you pay per transaction in Ethereum. The payment currency obviously is eth.

It's a deciding factor for your transaction to be picked up for processing by the network. The bigger the fee, greater is the chance that your transaction will be picked up.

It also decides how long your transaction can run

Why this peculiar name?

What we call Petrol in India is called Gas in the US

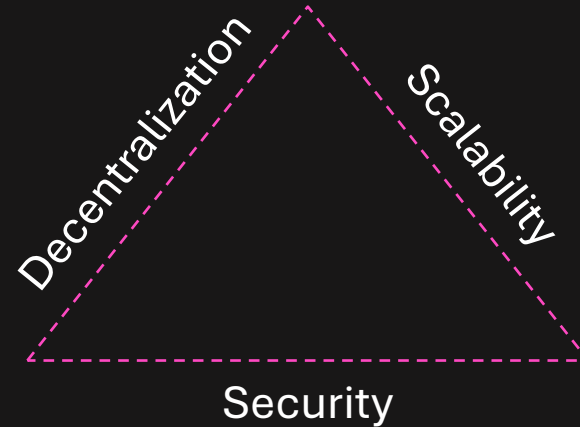
Your car runs only as far as the gas inside its fuel tank allows



What do you think would be the performance of a world computer?



BLOCKCHAIN TRILEMMA



The blockchain trilemma refers to the idea that it's hard for blockchains to achieve optimal levels of all three properties simultaneously. Increasing one usually leads to a weakening of another.

Any guess what compromise Ethereum made?

The compromise is scalability which effects transaction performance.

Why did Ethereum sacrifice scalability?



But real-world applications need all 3

OFF LOAD PERFORMANCE

Sharding

Roll-ups

Plasma

State channels

Side chain

CONSENSUS ALGORITHM – POW TO PROOF OF STAKE

Ethereum started with PoW but changed to PoS algorithm in Sept 2022

WHY?

PoS is more secure, less energy-intensive, and better for implementing new scaling solutions

But what was the problem with PoW?



PHENOMENON BEHIND POS

What's the philosophy behind PoW's that require spending so much electricity?

To ensure good behavior by miners. To prove they have skin in the game...

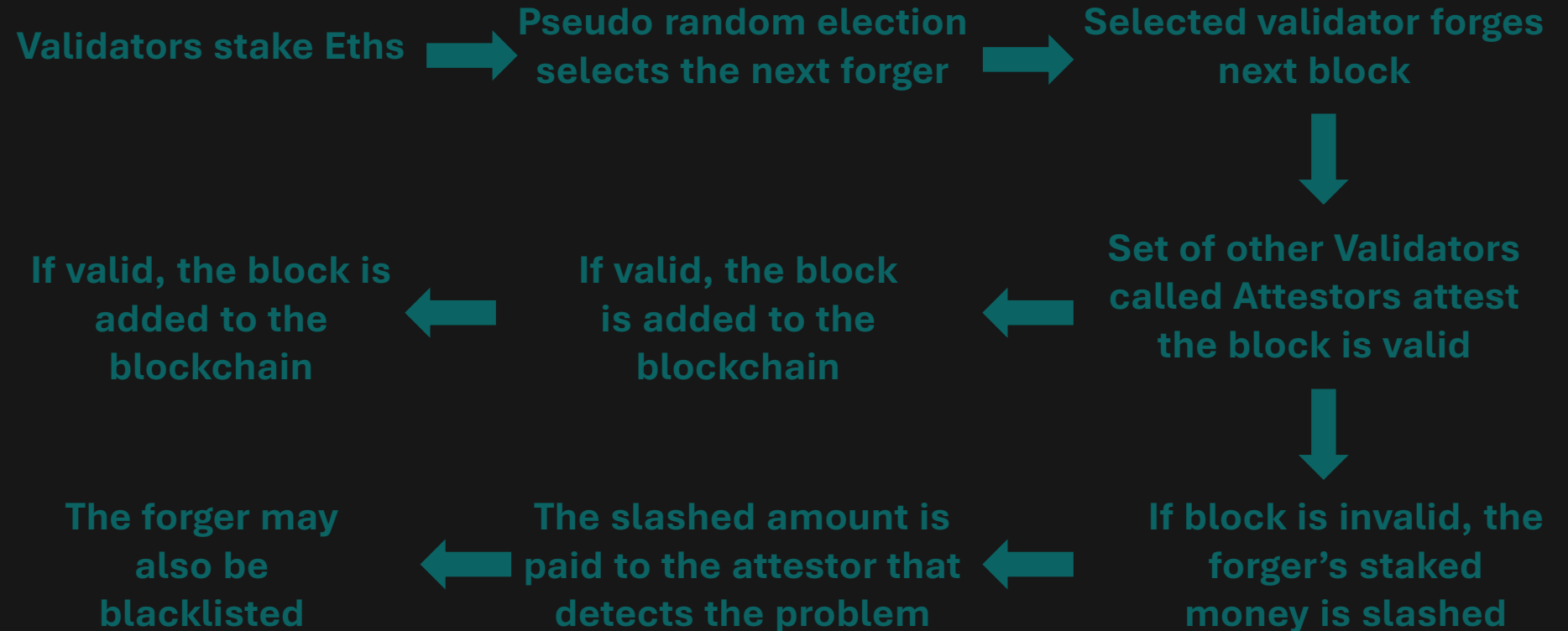
Is there another way to prove skin in the game?

Yes, it's the deposits

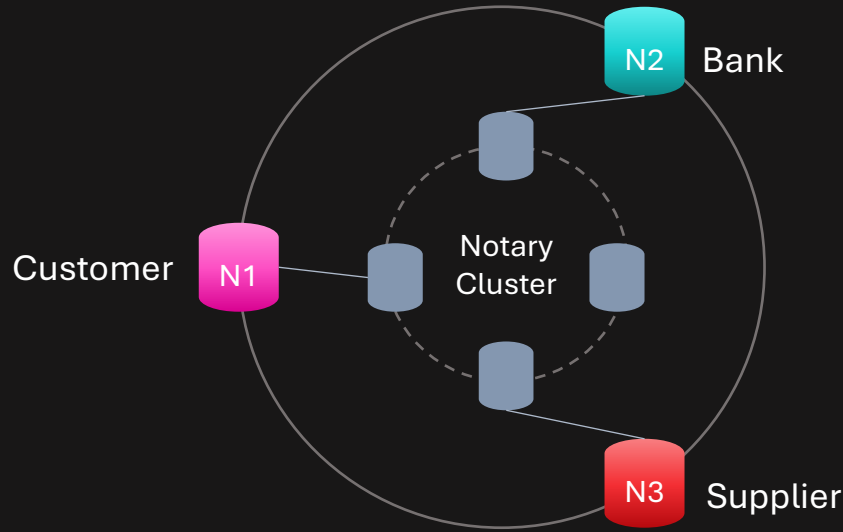
- ✓ Validator nodes validate transactions in a block and propose an order
- ✓ They stake min 32 eths ~100,000 USD
- ✓ Larger the stake better is the chance to be elected to propose a block
- ✓ The block proposer earns from the gas fees paid on each transaction in the block
- ✓ A set of remaining validators known as attestors ensure there are no problems with the proposed block by the elected node
- ✓ If the block is found fraudulent, the proposing validators deposit is slashed, and the forger may be blacklisted



SO, HOW DOES PROOF OF STAKE WORK AFTER ALL?



PRIVATE DLT – R3 CORDA



- ✓ Joining the network is by permission only
- ✓ Notaries are special corda nodes
- ✓ The notary cluster orders transactions and ensures double spend protection
- ✓ Notary nodes are part of every transaction
- ✓ Transactions are not broadcast. They are sent to only the relevant parties on need-to-know basis
- ✓ All this leads to improved performance and privacy

But the trilemma cannot be avoided

Any guess what did R3 sacrifice for performance?

It's the decentralization



Thank You