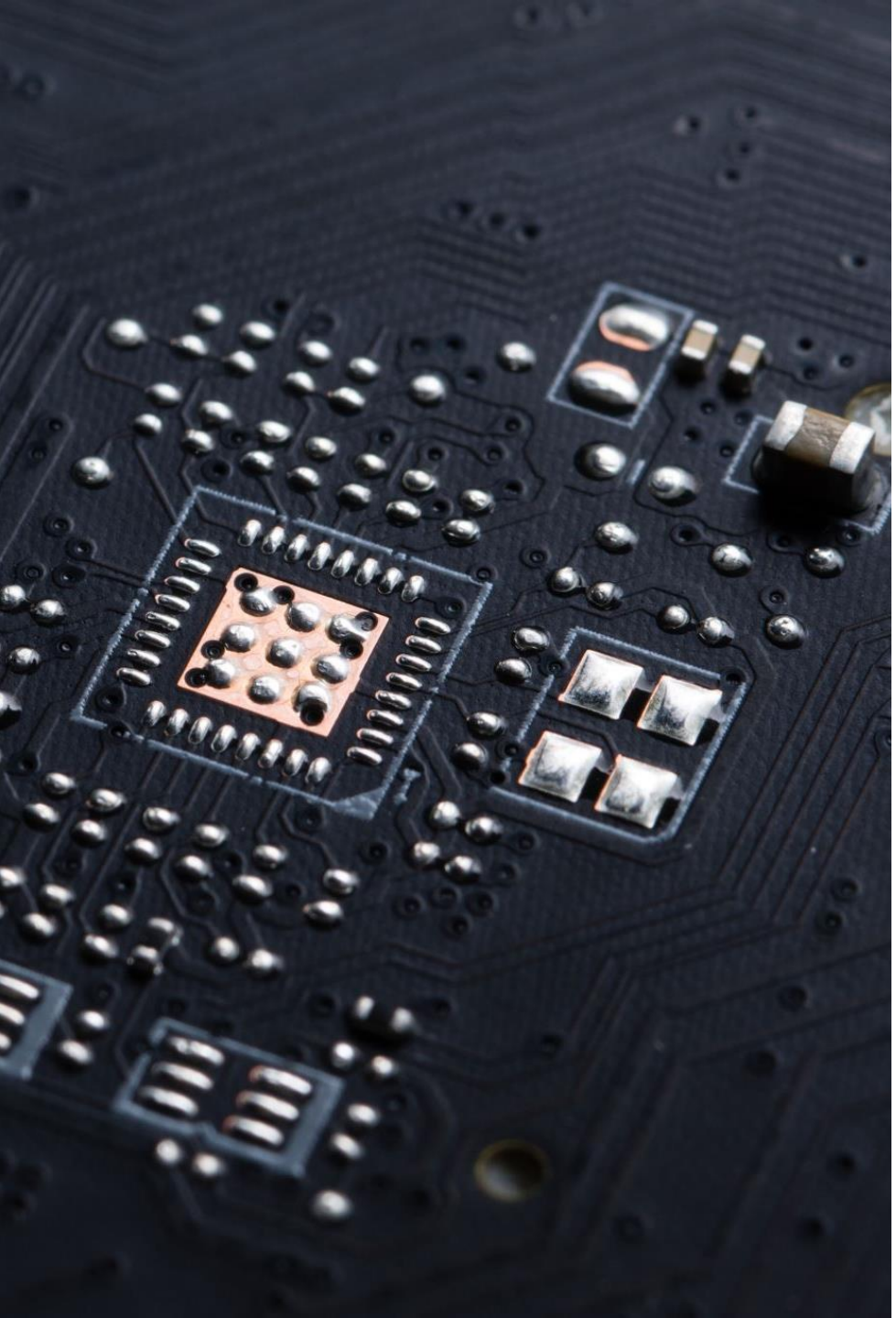
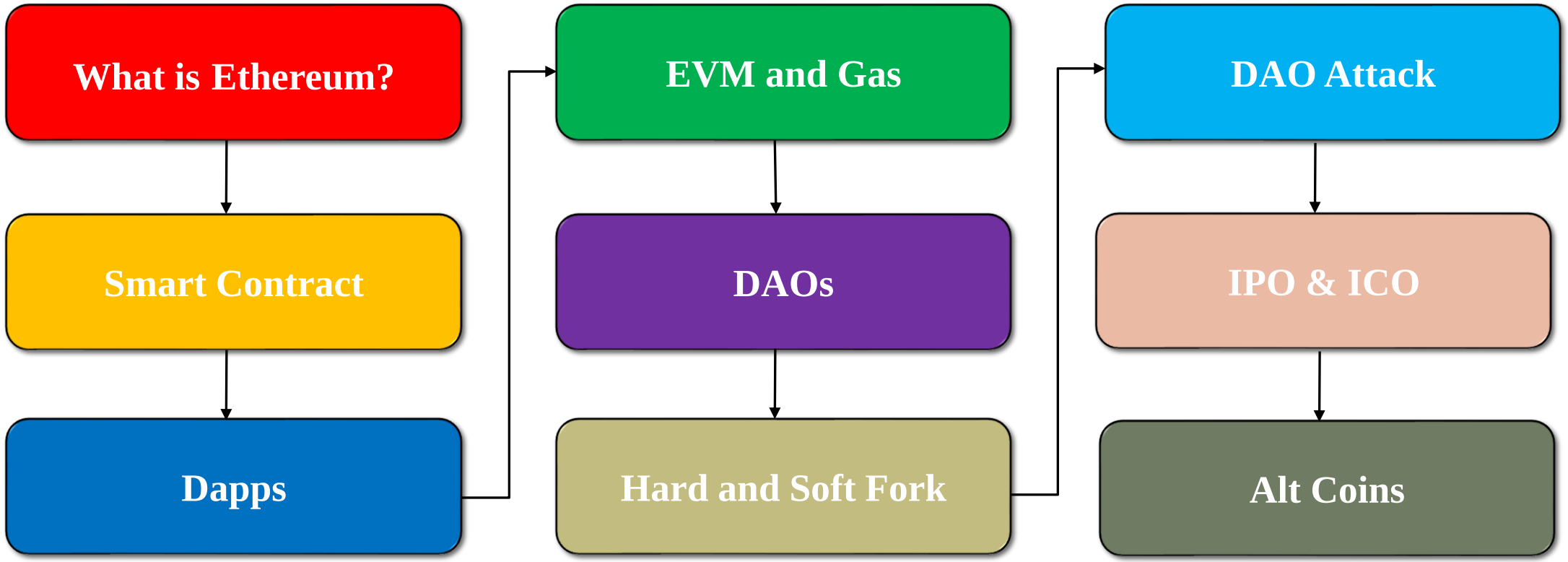
Blockchain

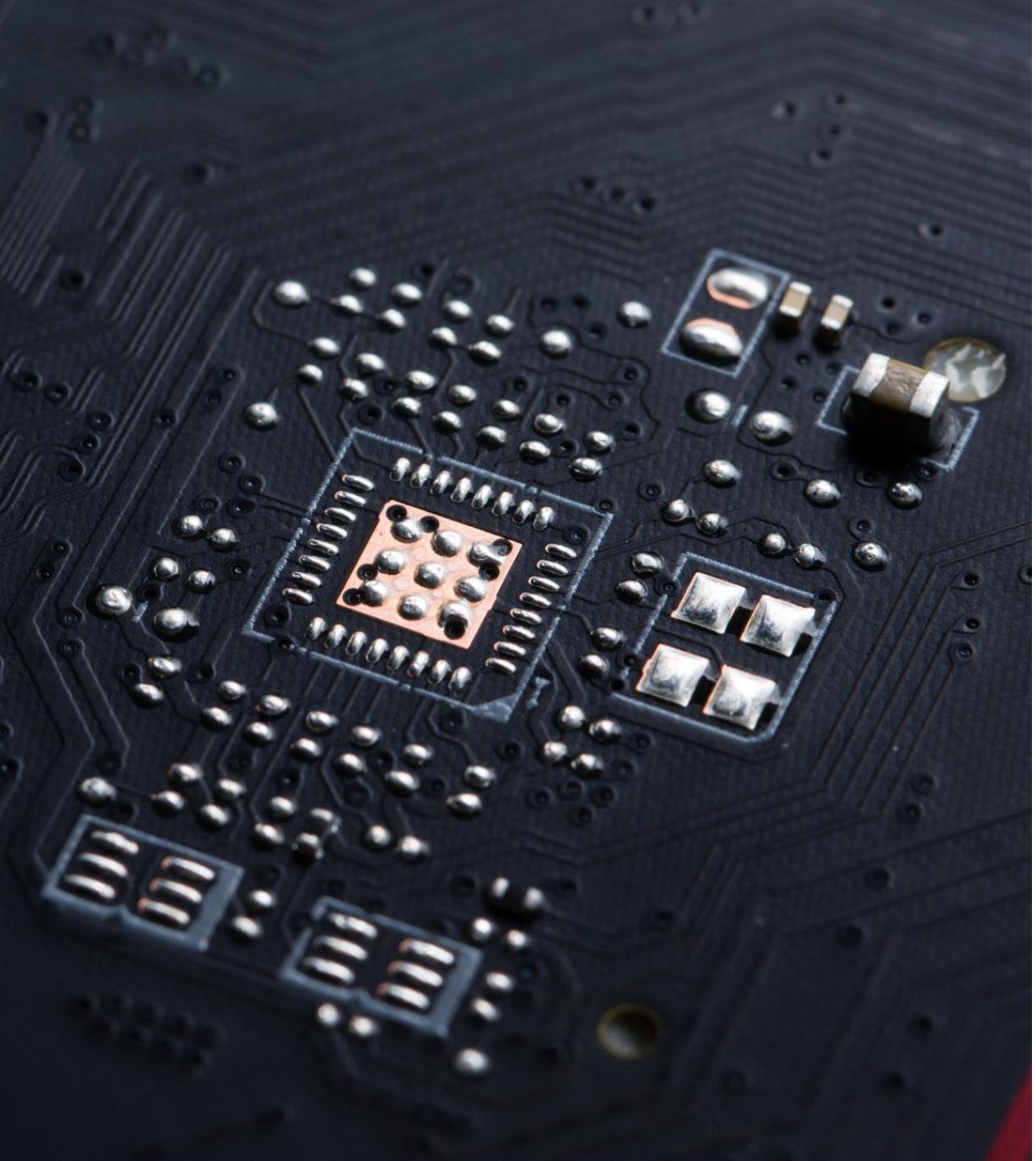
Dr. Bahar Ali
Assistant Professor (CS), National University Of Computer and Emerging Sciences, Peshawar.



Ethereum

Contents – Module C





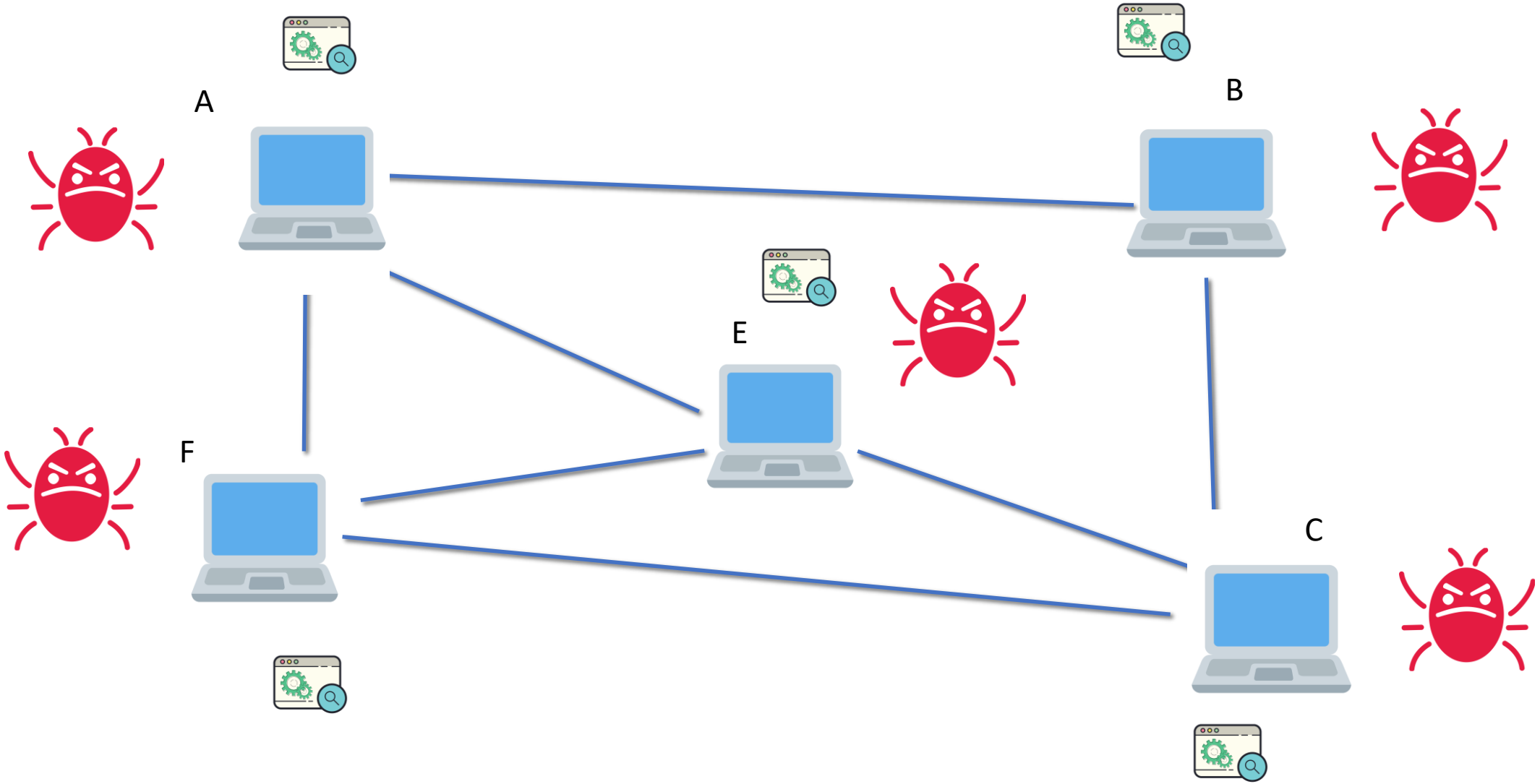
Ethereum Virtual Machine(EVM)

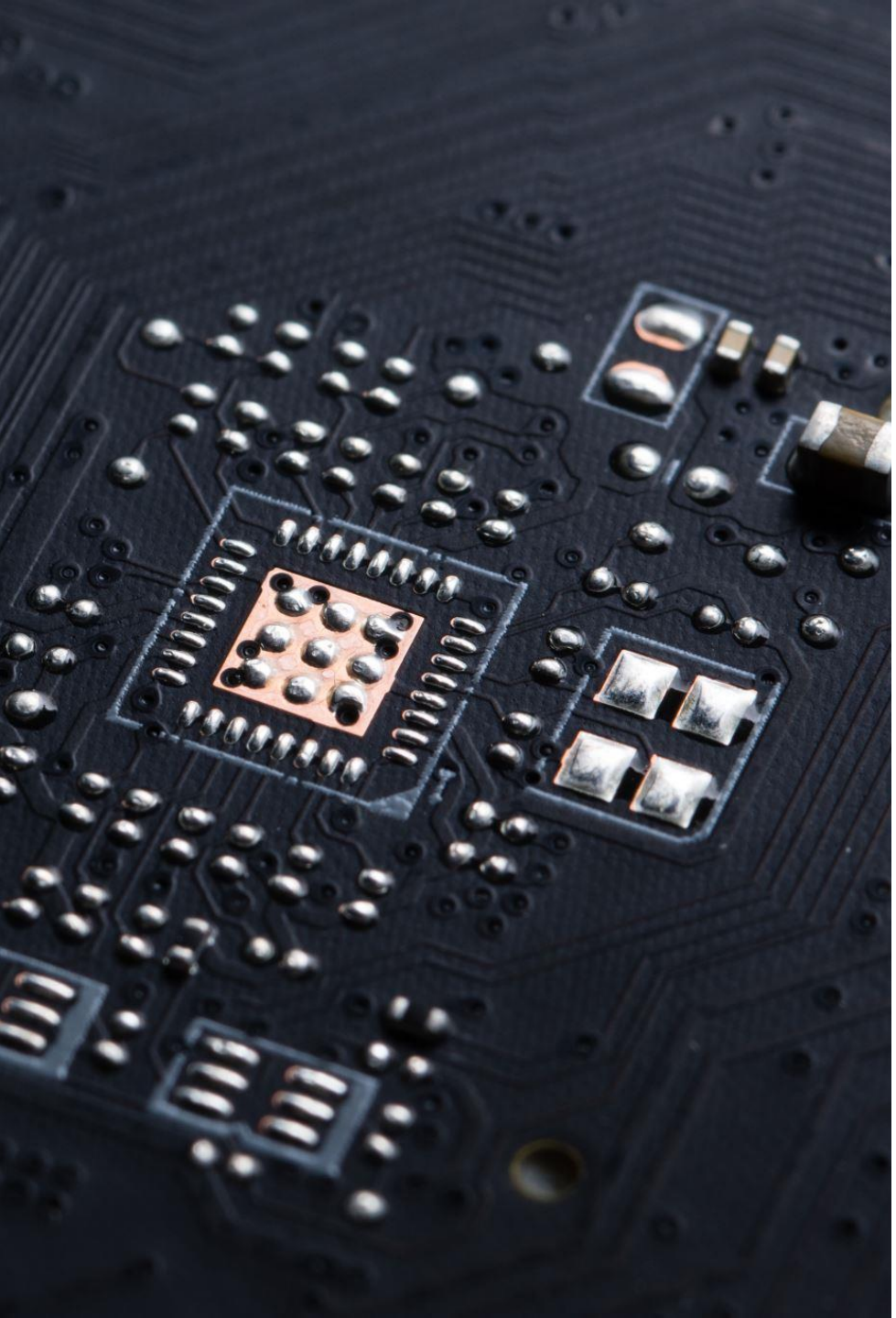
Ethereum Virtual Machine

- A powerful, sandboxed virtual stack embedded within each full Ethereum node
- A decentralized and isolated environment for running smart contracts.
- Isolated, the code it runs has no access to the network, filesystem, or other processes. Thus, If a hacker writes malicious code that runs all over the network, it cannot harm the hard disk, etc.
- Computes the state of the network after each new block is added

Ethereum Virtual Machine

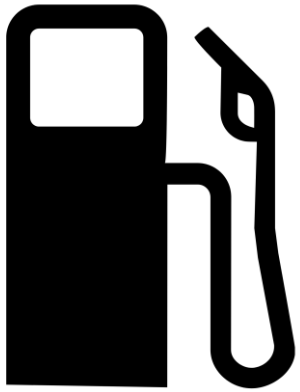
- Contracts are written in high-level languages, like Solidity, and compiled to EVM bytecode, thus EVM executes the contract bytecode
- Supports interoperability between blockchains, EVM can support all types of blockchains that use bytecode-based smart contracts.

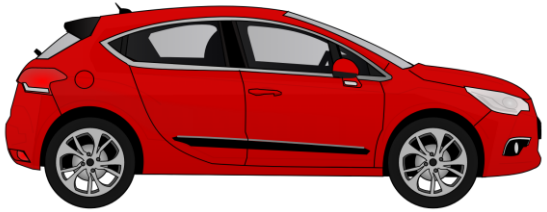

A
B
E
F
C



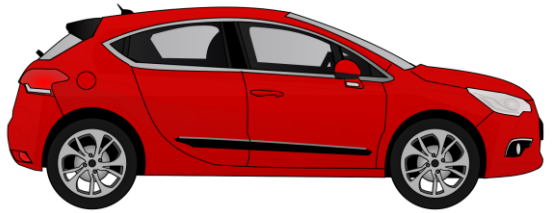
Ethereum Gas

Ethereum Gas



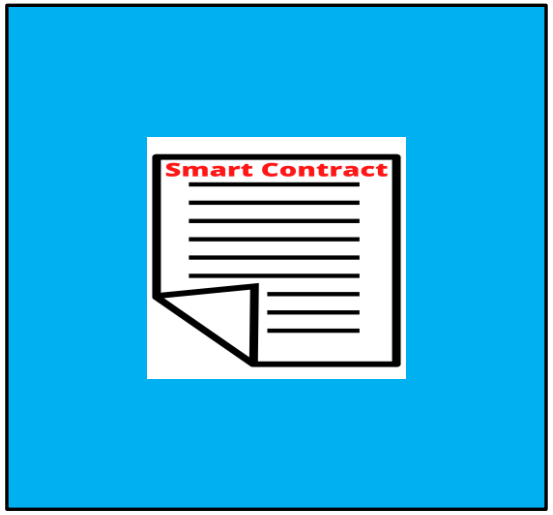


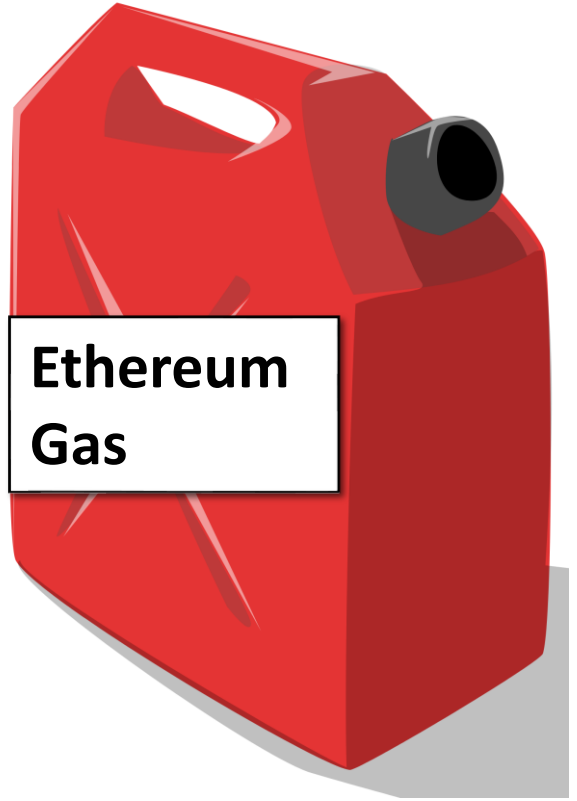
A



B

Ethereum Gas





Ethereum Gas

- A Car needs petrol/ gas to go from one point to another
- The Ethereum needs gas for running smart contracts on Ethereum
- Smart Contract uses different opcodes that have their own gas requirement.

Opcode Gas Cost
https://ethereum.org/en/developers/docs/evm/opcodes/
https://github.com/djrtwo/evm-opcode-gas-costs/blob/master/opcode-gas-costs_EIP-150_revision-1e18248_2017-04-12.csv

Ethereum Gas

10 * 3 – 6 = ?

Multiplication needs 5 gas

Subtraction needs 3 gas

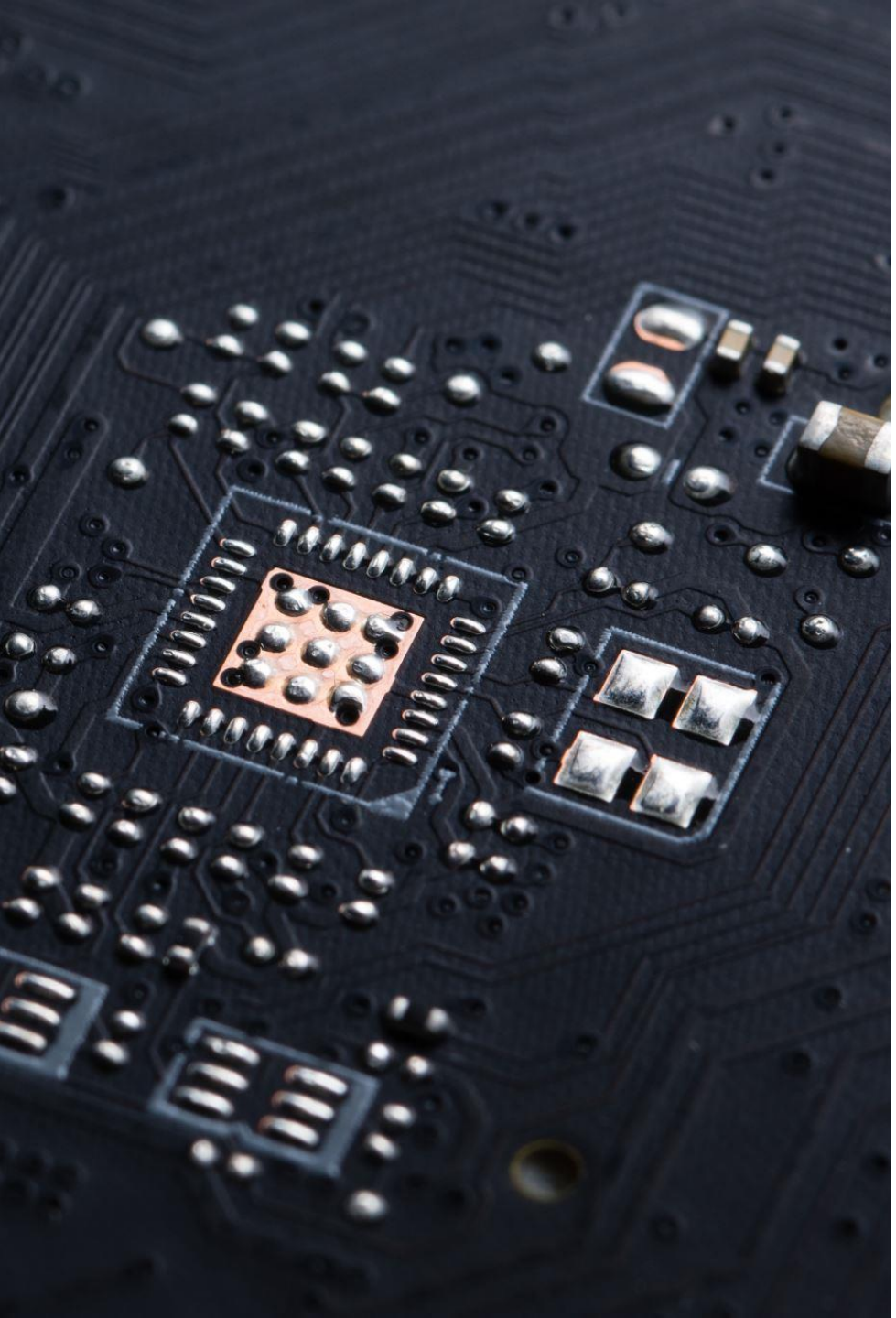
Equal needs 3 gas

Total gas required -> 5 + 3 +3 = 11 Gas

Ethereum Gas

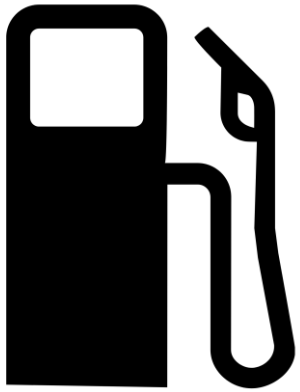
Some important points to note -

- Any transaction that modifies the blockchain costs gas.
- The user that generated the transaction pays for the gas.

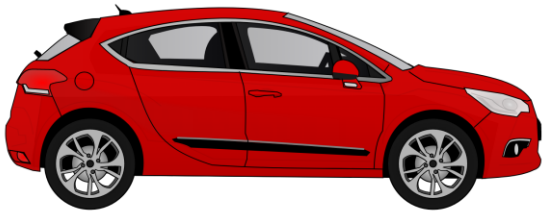


Ethereum Gas Price

Gas Price



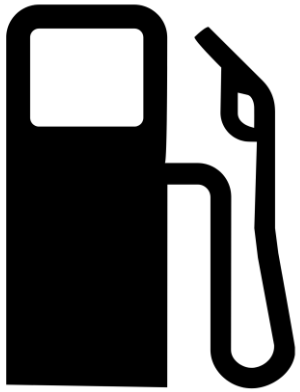
Petrol – 10 liters



A

B

Gas Price

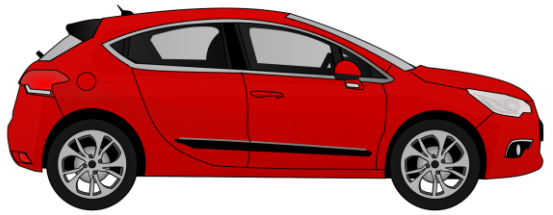


Petrol – 10 liters

Total price= ?

1 liter – Rs.5

Total price= 10x5=
Rs. 50



A

B

Gas Price

10 * 3 – 6 = ?

Multiplication needs 5 gas

Subtraction needs 3 gas

Equal needs 3 gas

Total gas required -> 5 + 3 +3 = 11 Gas

Gas Price

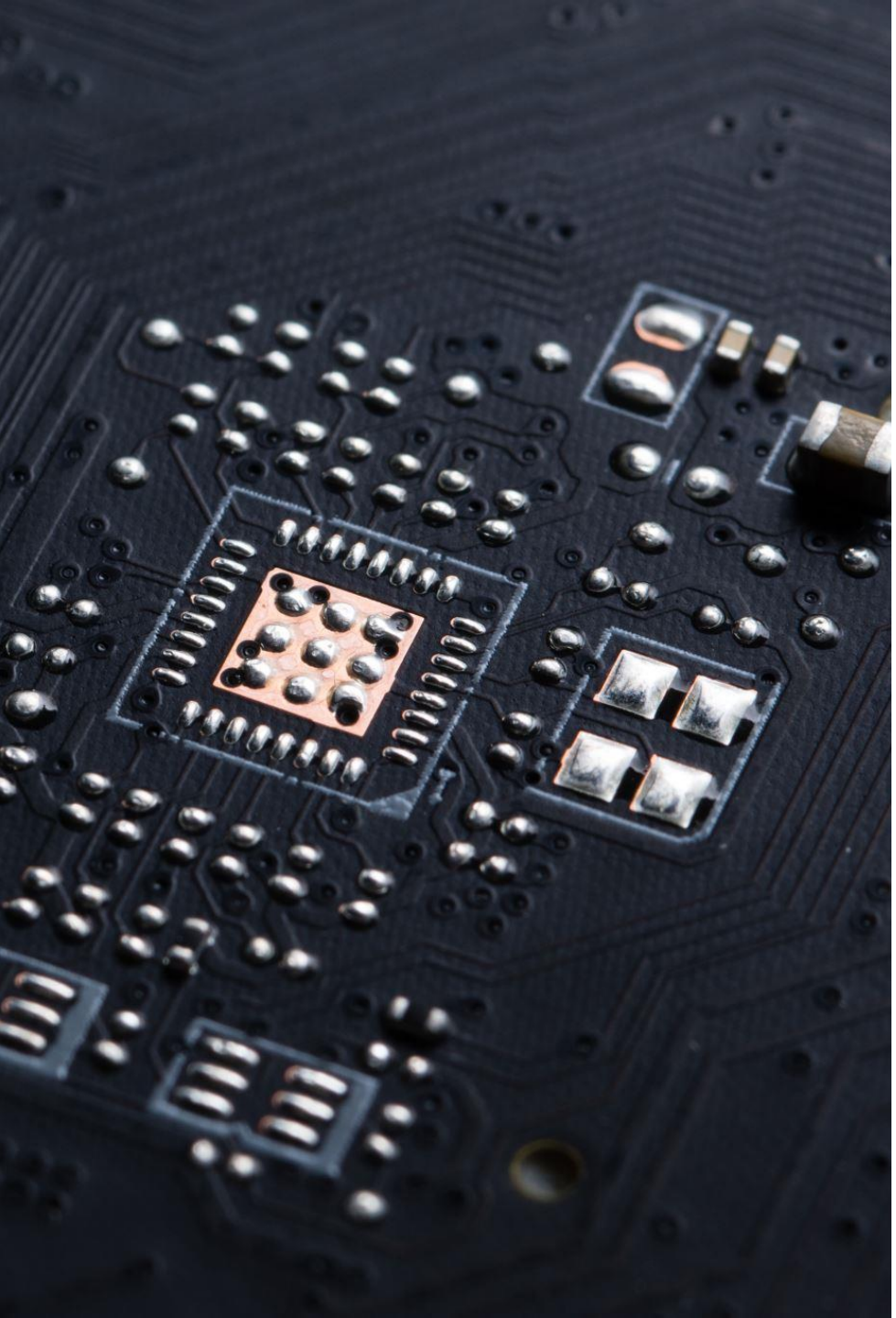
- It is the amount the sender wants to pay per unit of gas to get the transaction mined
- The gas Price is set by the sender.
- Gas prices are denoted in gwei. (1 gwei = 10^-9 ETH)

1 Gas price = 10 gwei

Ethereum Gas Tracker Demo
https://etherscan.io/gasTracker

Gas Price

- **The higher the gas price the faster the transaction will be mined.**
- It is just like the transaction in Bitcoin.



Ethereum Gas Limit

Gas Limit

- It is the maximum gas the transaction can consume
- Set by the sender

- Note: A standard peer-to-peer ETH transfer requires no more than 21,000 units of gas

Gas Limit

Let's say A wants to send B 2 ETH. So, what will be the total fees that A must pay?

Case 1: When transaction gas limit is 21,000 units.

A sets the gas price per unit = 100 gwei.

Transaction gas limit = 21,000 units.

The gas limit value is calculated from the opcode cost

Total fee = Gas units (limit) * Gas price per unit

Total fee will be: `21,000 * 100 = 210,0000 gwei` or 0.0021 ETH

Gas Limit

Let's say A wants to send B 2 ETH. So, what will be the total fees that A must pay?

Case 2: When gas transaction limit < 21000 units.

Transaction gas limit = 20,000 units.

Transaction Fail

However, the transaction fee will be charged, as the sender set less gas for the transaction

Gas Limit

Let's say A wants to send B 2 ETH. So, what will be the total fees that A must pay ?

Case 3: When gas transaction limit > 21000 units.

Transaction gas limit = 22,000 units.

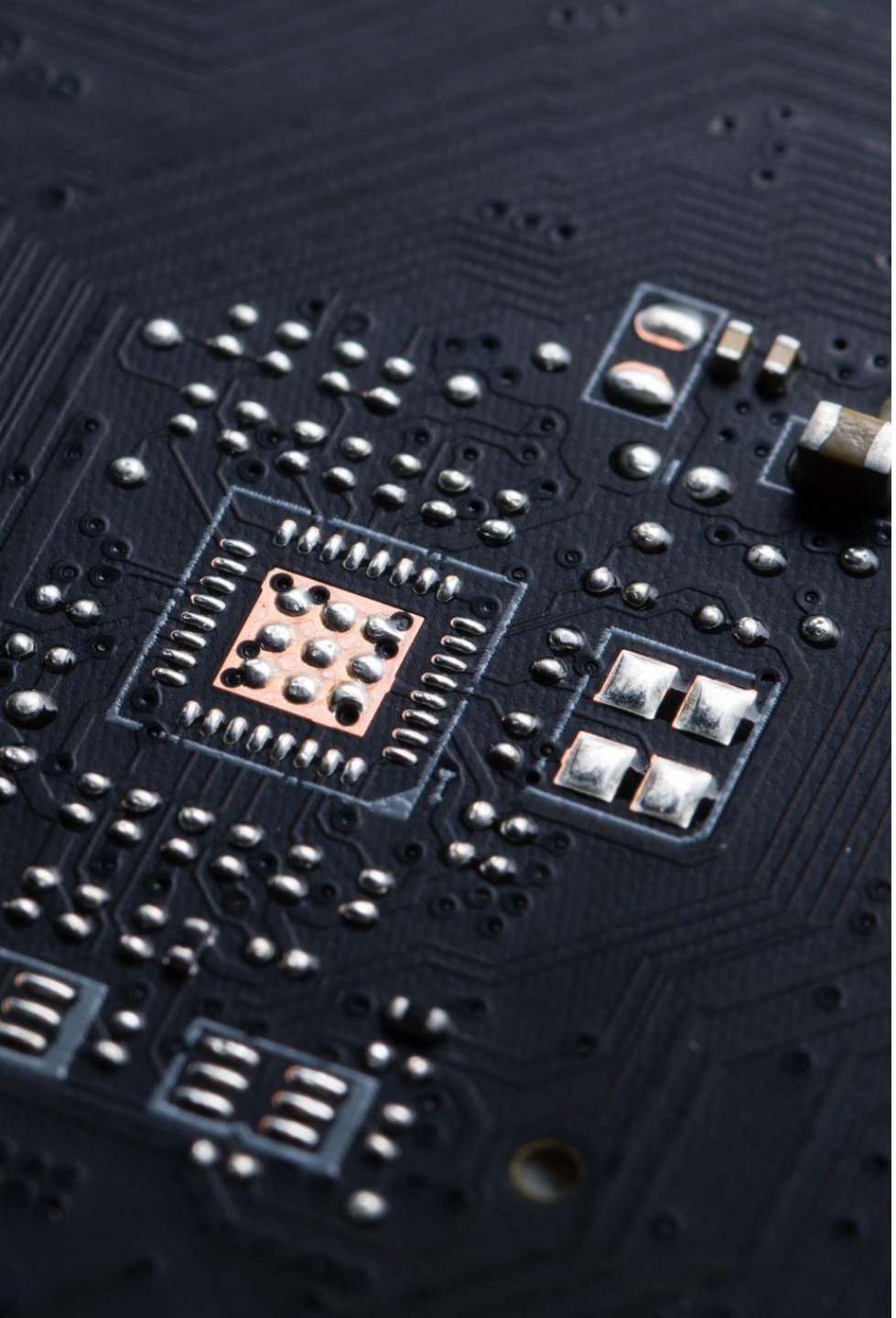
22,000 – 21000 = 1000 will be returned

Gas Limit

Q) The Gas limit can directly be calculated at the time when a smart contract runs. Then what is the use of Gas Limit?

A) A cap is applied, which can be used to

- Stop indefinite loops and saves ethers
- Stop attacks like DoS



Ethereum Demo

Ethereum Demo

Ethereum Demonstration

https://etherscan.io/blocks