
BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्
Blockchain @ BITS Pilani
BITS Pilani
Pilani Campus
Name: Jeeten Kapoor Jain
0:00 / 20:12 • Chapters

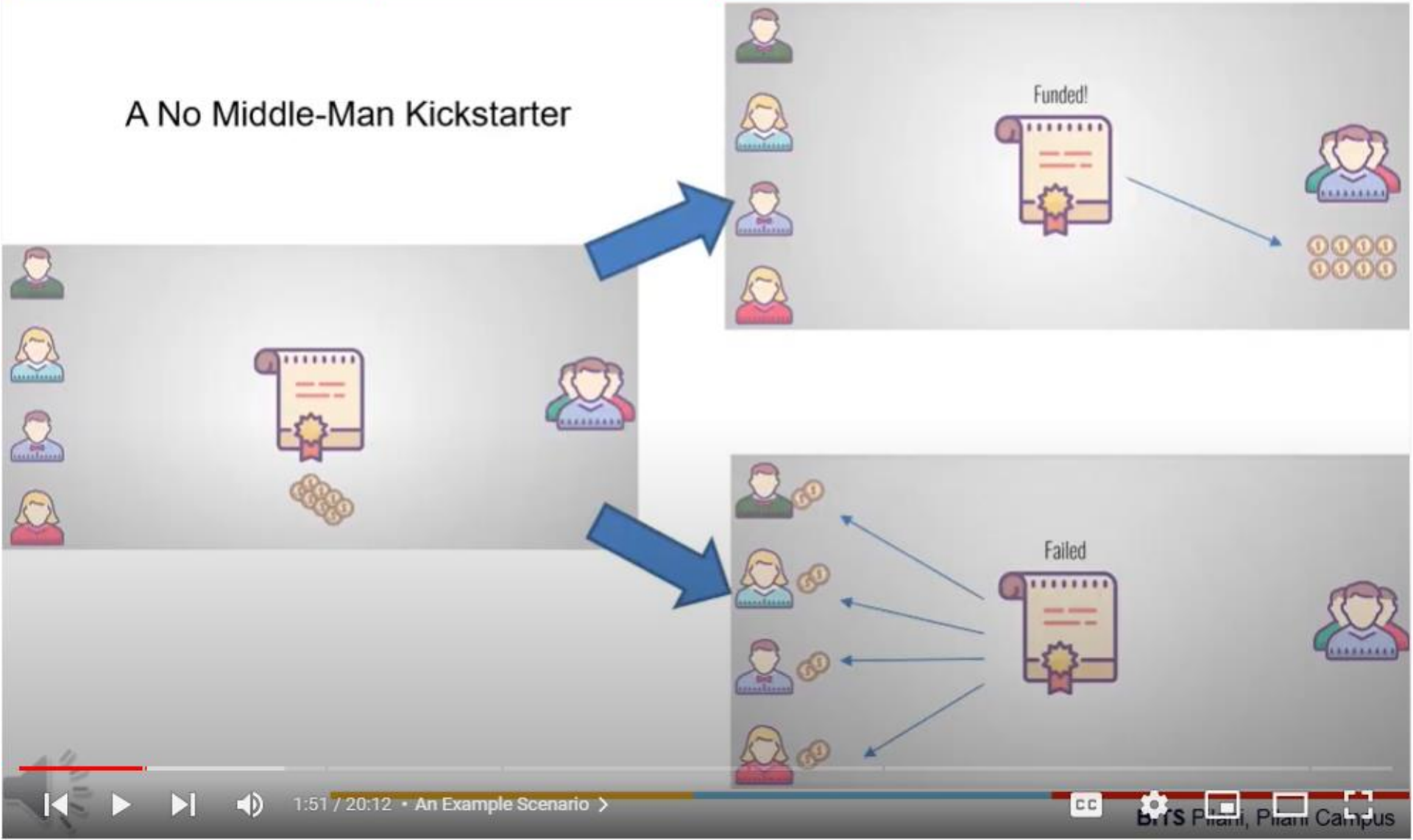
Smart Contracts – Video Lecture from Youtube

Smart Contracts

innovate achieve lead

- Programs/Protocols stored Blockchain
  - because it exists on the blockchain it inherits various security and privacy properties.
- Automatic execution: preprogrammed to when some predetermined conditions is met
- Reduces the need for intermediaries
- Immutability: cannot be changed or updated once they are deployed
- Expanded Blockchain's scope of applications
  - Tokens, DApps, Many more…

An Example Scenario



How Smart Contracts Works

innovate achieve lead

How does a SMART CONTRACT WORK?

Pre-Defined Contract
Terms and conditions are agreed by all the parties involved.

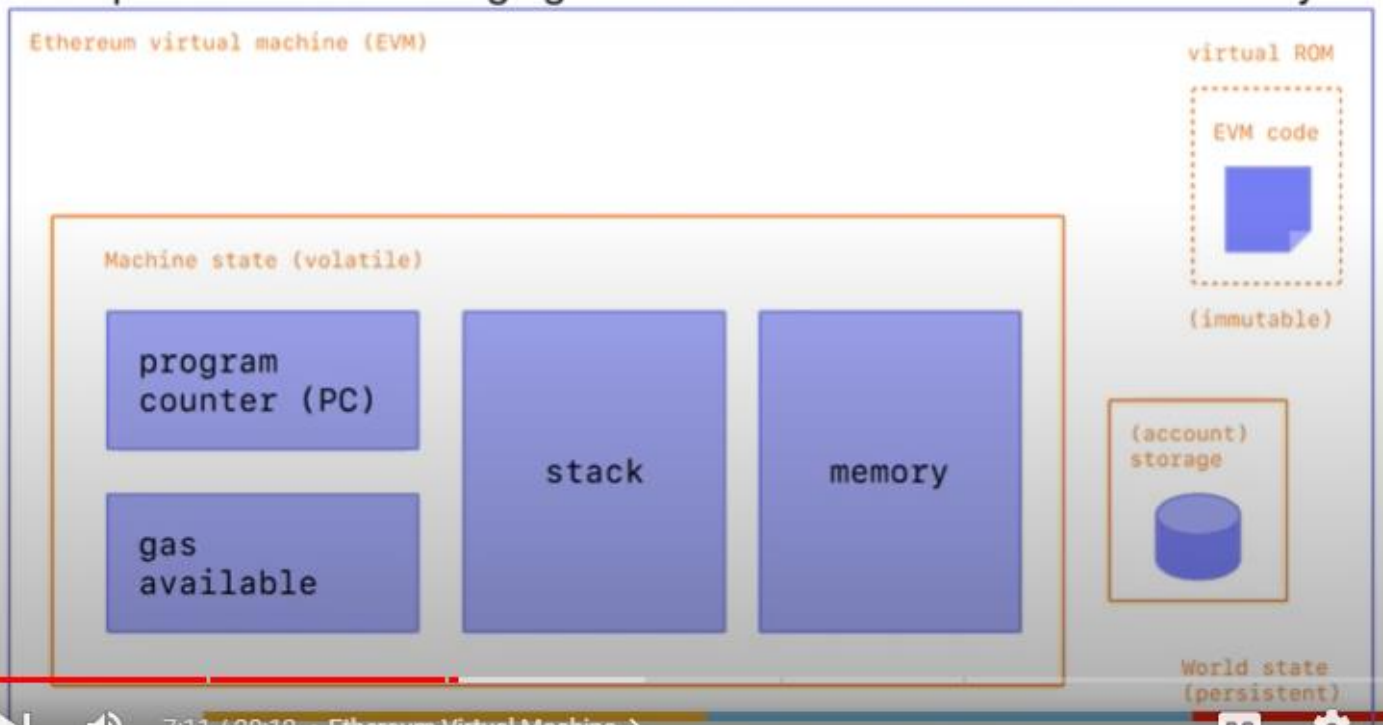
Events
Execution of the contract is triggered by an event.

Execution
The smart contract is executed automatically.

Settlement
All the settlements are executed quickly and eficiently.

Ethereum Virtual Machine

- Physical instantiation can't be described
  - exists as one single entity maintained by thousands of connected computers running an Ethereum client
- Ethereum as a distributed state machine
  - The specific rules of changing state from block to block are defined by the EVM



Smart Contracts on Ethereum

innovate achieve lead

- Smart Contracts are a collection of its code (function) and its data (state)
- They are a type of Ethereum account
  - Like all account it resides at a specific address on the Ethereum blockchain.
  - Like all account they have a balance and can send transactions
- It is Permissionless: Anyone can write a smart contract and deploy it to the network
- Needs certain an amount of gas to deploy and run
  - Deploying a smart contract is technically a transaction, so you need to pay your Gas in the same way

What is Gas and why it exists?

innovate achieve lead

- Unit of computational effort required to execute specific operations on the Ethereum network
- The London Upgrade – 5th August 2021
  - better transaction fee estimation
  - generally quicker transaction inclusion
- Every block has a base fee: calculated by network based on demand for block space
- Variable-size blocks: Block has a target size of 15 million gas, but can go up to 30 million gas based on network demand
- Keeps the network secure: every computation executed requires a fee, preventing spamming of network

An Example

innovate achieve lead

Let's say Alice wants to send a transaction to Bob of 1ETH

The fees and refund is calculated as per the formulas below:

$$Total\ Transaction\ fee = gasLimit \times (baseFee + tip)$$

$$Refund = maxFee - actualFee$$

Alice sets gas limit as 21,000 units and assuming the current base fee as 100 gwei. Alice has included a tip of 10 gwei.

$$21{,}000 \times (100 + 10) = 2{,}310{,}000\ gwei = 0.00231\ ETH$$

No refund in this case!

*As Alice didn't set the optional parameter of maxFeePerGas**

Open Challenges

- Far from perfect: no straight forward way to cater to any requirement for changes in the logic of the code
- No right to remedy
- Bug are visible to all nodes, hence easier to exploit