Introduction to Blockchain and Ethereum

NIKHIL V CHANDRAN
R&D Engineer

About KBA

A **Center of Excellence** under **Digital University of Kerala** with many International collaborations to explore the disruptive potential of the Blockchain Technology for achieving public good through capacity building to promote Research, Development and Entrepreneurship. Since its inception in 2017, the vibrant ecosystem of KBA offering Certification Programs, R&D activities and Consultancy, has attracted International attention.

Key Facts

- ➔ Associate Member and Official Training Partner of **Linux Foundation Decentralized Trust**
- ➔ General Partner - **R3 Consortium**
- ➔ Associate Member - **InterWork Alliance**
- ➔ Content Partner – **Blockchain Education Network**
- ➔ Knowledge Partner – **IBF NET**

Certification Programs

- ➔ Certified Blockchain Associate (CBA)
- ➔ Certified Blockchain Startup Program (CBS)
- ➔ Certified Ethereum Developer (CED)
- ➔ Certified Hyperledger Fabric Developer (CHF)
- ➔ Bootcamps - Ethereum/Fabric
- ➔ Internship Programs.
- ➔ Certified Blockchain Architect (CBR)
- ➔ Blockchain Excellency Programme (BEP)
- ➔ Free Foundation Programs - Blockchain, Ethereum, Fabric, Corda.

- Our programs are offered in classroom-based, instructor-led model as well as through Online Mode (https://kba.ai/)
- Our Certificates are issued on Blockchain which makes it tamper-proof and easily verifiable. First Academy in India to start this initiative.

Evolution of Web

Web1 - Static Web

Read only

Web2: Social Web

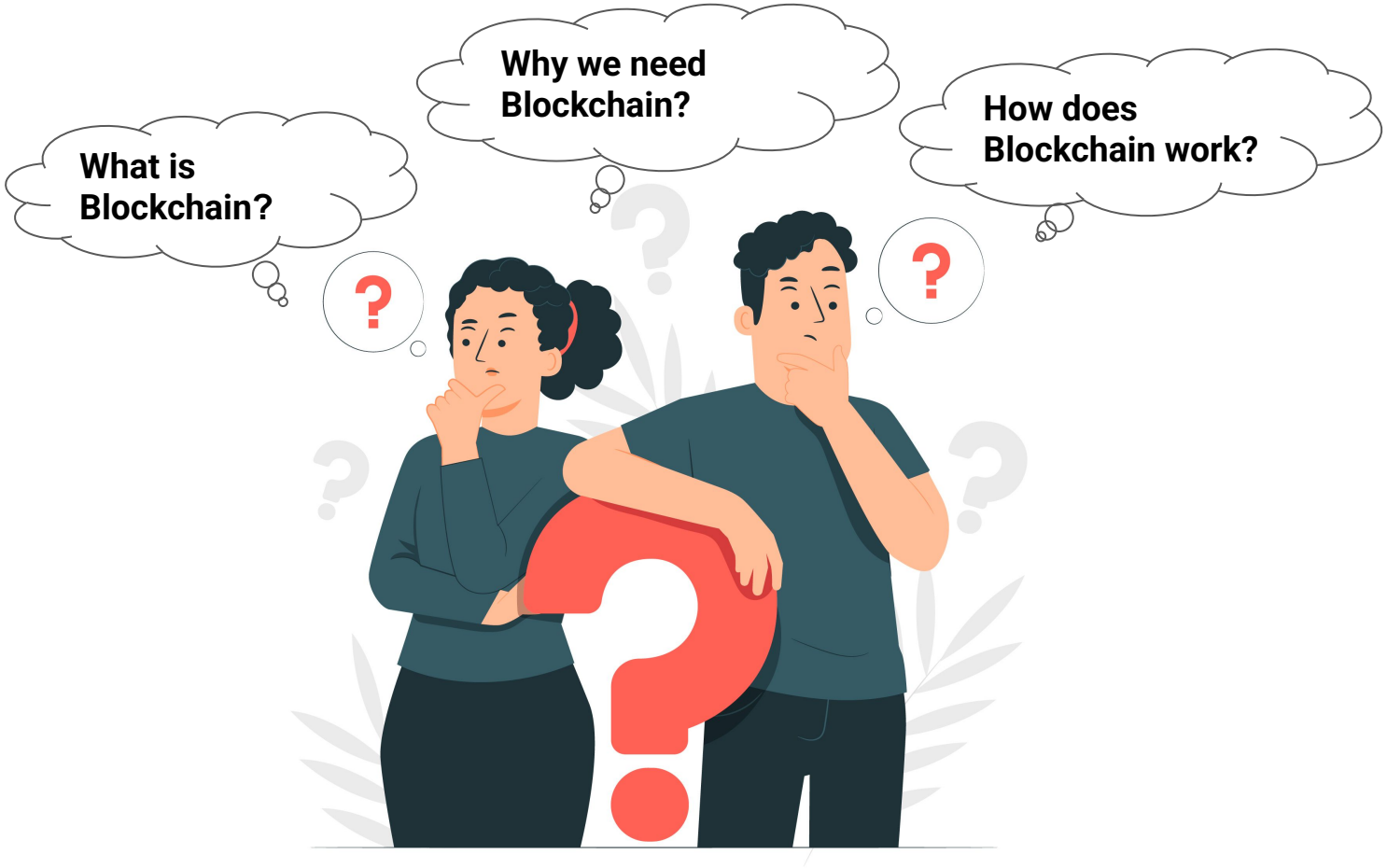
Read-Write

Web3: The New Internet?

Read-Write-Own

CENTRALIZED

DECENTRALIZED


What is Blockchain?
Why we need Blockchain?
How does Blockchain work?

2008

“Bitcoin: A peer to peer electronic cash system” by an anonymous entity called Satoshi Nakamoto

2009

Satoshi launches Bitcoin as an alternative to current financial system

2010

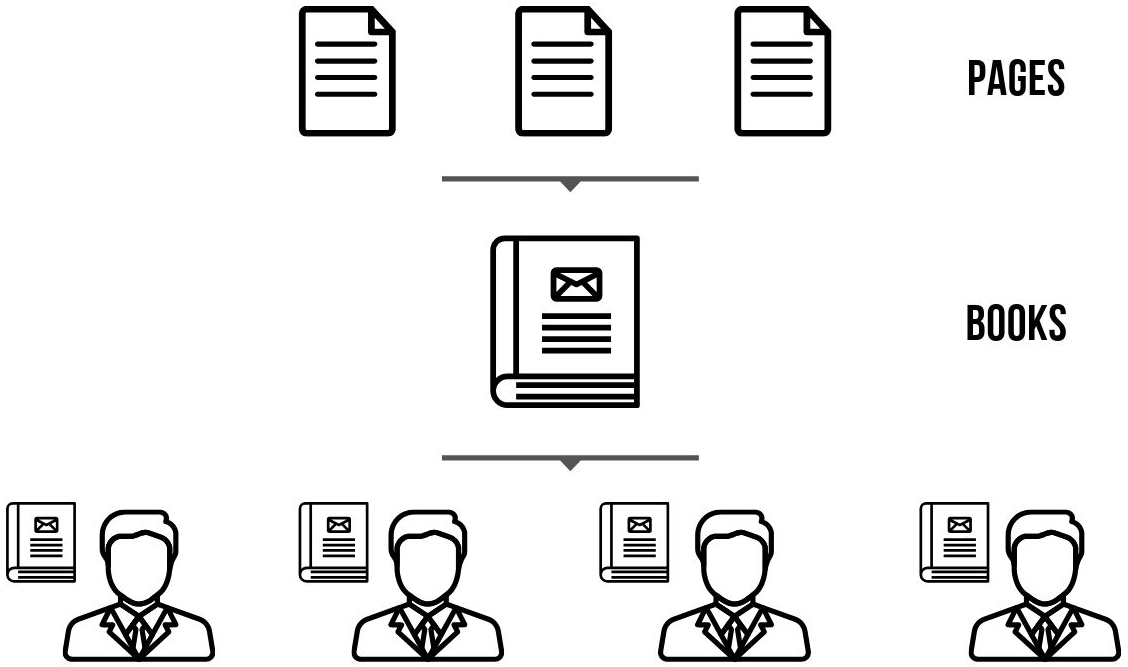
Laszlo Hanyecz bought 2 pizzas for 10,000 bitcoins (BTC). As per current price, it amounts to 29366956230 INR (Nov, 2023)

2023

Bitcoin consumes an estimated 150 terra watt- hours of electricity annually, more than the annual consumption of Netherlands

WHAT LIES UNDER THE HOOD ?

BREAKING IT DOWN...



DEFINING A CHAIN

WHAT ?

BLOCKCHAIN TECHNOLOGY IS A DECENTRALIZED , DISTRIBUTED ,IMMUTABLE ,LEDGER TECHNOLOGY

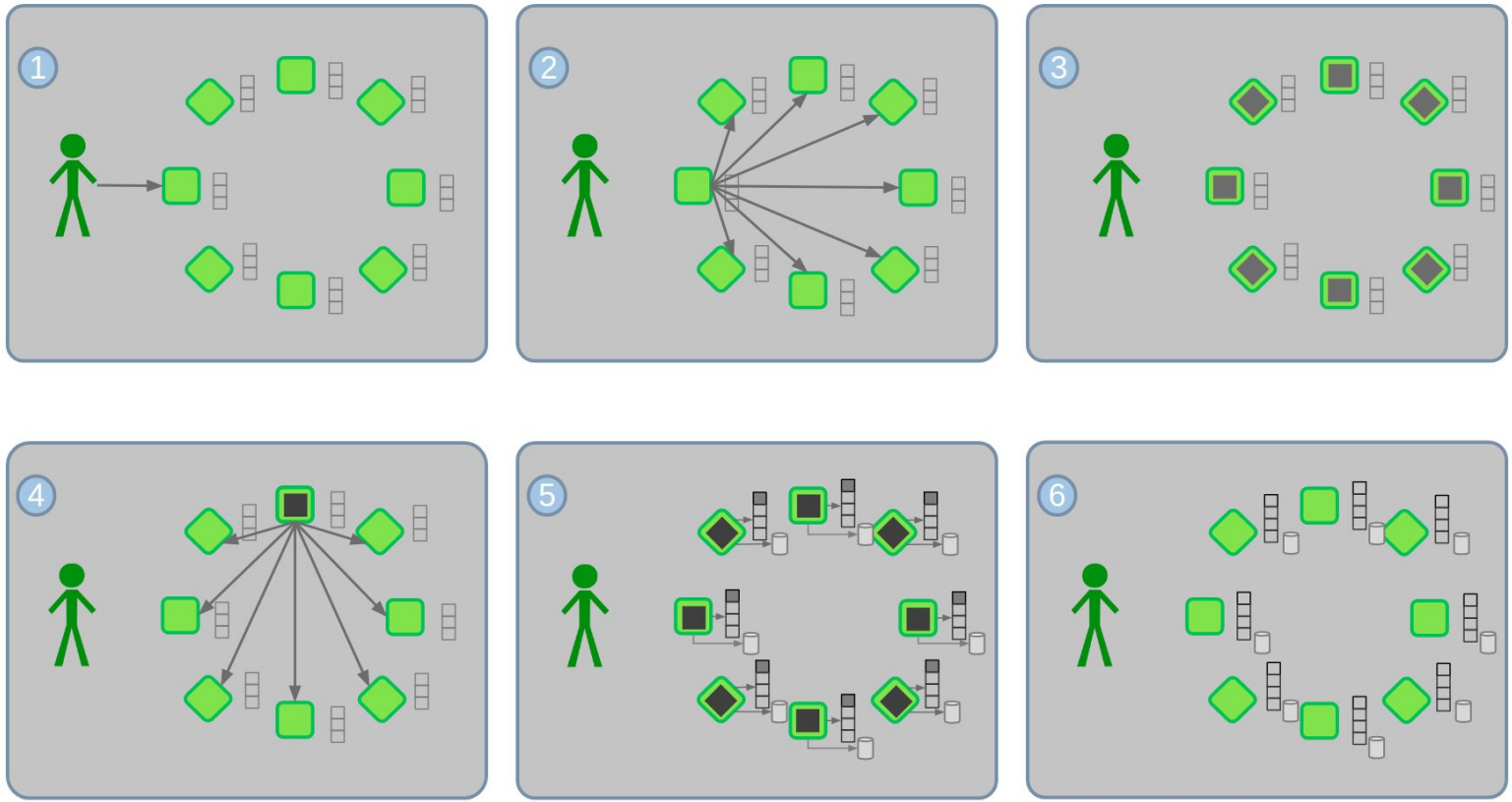
WHY ?

A REAL-TIME OPEN LEDGER FOR RECORDING ANY TYPE OF TRANSACTION(DATA) WITH NO SINGLE OWNER

WHEN ?

CAME IN A DOCUMENT, OR WHITEPAPER PUBLISHED IN 2008 BY SATHOSHI NAKAMOTO

Transaction Flow - Blockchain Network



Consensus

Dictionary

Search for a word

consensus

/kənˈsɛnsəs/

noun

a general agreement.
"there is a growing consensus that the current regime has failed"

Similar: agreement harmony concord like-mindedness concurrence

Translations, word origin and more definitions

Definitions from Oxford Languages Feedback

Programmable Blockchains: Ethereum

Vitalik Buterin (OP)
Sr. Member

Activity: 330
Merit: 394

[ANN] Ethereum: Welcome to the Beginning
January 23, 2014, 11:33:17 AM

Merited by BayAreaCoins (10), tk808 (10), notbatman (8), suchmoon (7), IncludeBeer (7), Kda2018 (7), Abiky (5), nutildah (5), alani123 (5), redsn0w (5), klintay (5), dragonvslinux (5), zork (5), somacoin (5), vapourminer (4), Mrpumperitis (3), goldcoinminer (3), Cloudpost (3), Northa (3), OmegaStarScream (2), pangu (2), julerz12 (2), PuertoLibre (2), bitcampaign (2), V1saya (2), Eddyc (2), batang_bitcoin (1), Jcga (1), Husna QA (1), wmaurik (1), Raja_MBZ (1), mandor (1), Easteregg69 (1), bubbalex (1), kopisusu (1), HBKMusiK (1), FreedomCoin (1), Financisto (1), Tyr808 (1), iwantmyhomepaidwithbtc2 (1), CrowdFunder (1), tammuz (1), safexscam (1), NeStore (1), gabbello (1), heyspongebob (1), Neo Baudrillard (1)

#1

Welcome to the New Beginning

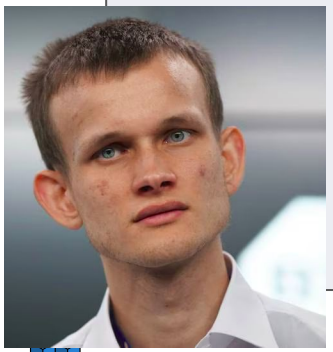
When the grand experiment that is bitcoin began, the anonymous wizard desired to test two parameters- a trustless, decentralized database enjoying security enforced by the austere relentlessness of cryptography and a robust transaction system capable of sending value across the world without intermediaries. Yet the past five years years have painfully demonstrated a third missing feature: a sufficiently powerful Turing-complete scripting language. Up until this point, most innovation in advanced applications such as domain and identity registration, user-issued currencies, smart property, smart contracts, and decentralized exchange has been highly fragmented, and implementing any of these technologies has required creating an entire meta-protocol layer or even a specialized blockchain. Theoretically, however, each and every one of these innovations and more can potentially be made hundreds of times easier to implement, and easier to scale, if only there was a stronger foundational layer with a powerful scripting language for all of these protocols to build upon. And this need is what we seek to satisfy.

Ethereum is a modular, stateful, Turing-complete contract scripting system married to a blockchain and developed with a philosophy of simplicity, universal accessibility and generalization. Our goal is to provide a platform for decentralized applications - an android of the cryptocurrency world, where all efforts can share a common set of APIs, trustless interactions and no compromises. We ask for the community to join us as volunteers, developers, investors and evangelists seeking to enable a fundamentally different paradigm for the internet and the relationships it provides.

Who is Behind Ethereum?

Our primary core devs are:

- Vitalik Buterin → Inventor of Ethereum, protocol developer and researcher
- Gavin Wood →Lead C++ developer
- Jeffrey Wilcke → Lead Go developer



What is Ethereum?

- Ethereum is a Decentralized Distributed Ledger.
- Improvised on the innovations of Bitcoin.
- World’s first programmable blockchain.
- Ethereum aims to reinvent the internet.
- Ethereum is a global, open-source platform for decentralized applications.

Ethereum World Computer

Ethereum Vision: One Computer (blockchain) for the entire world

Ethereum World Computer - Key Properties

Deterministic

{ A + B = C
2 + 3 = 5 }

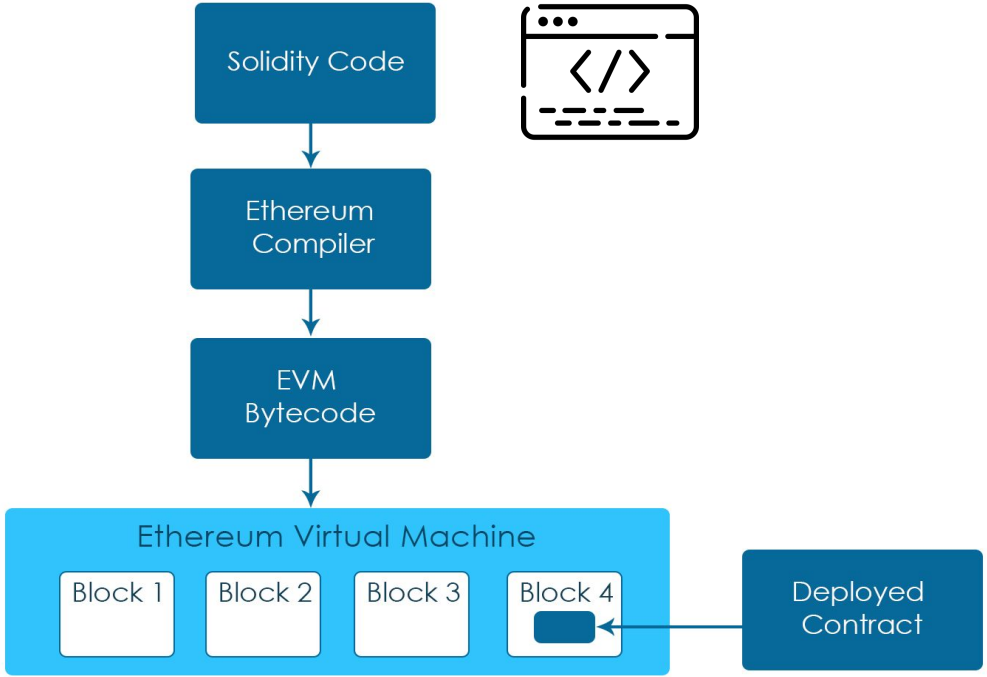
Terminable

Timer
Step Counter
Fee Meter - Ether

Isolated

Virtual Machine

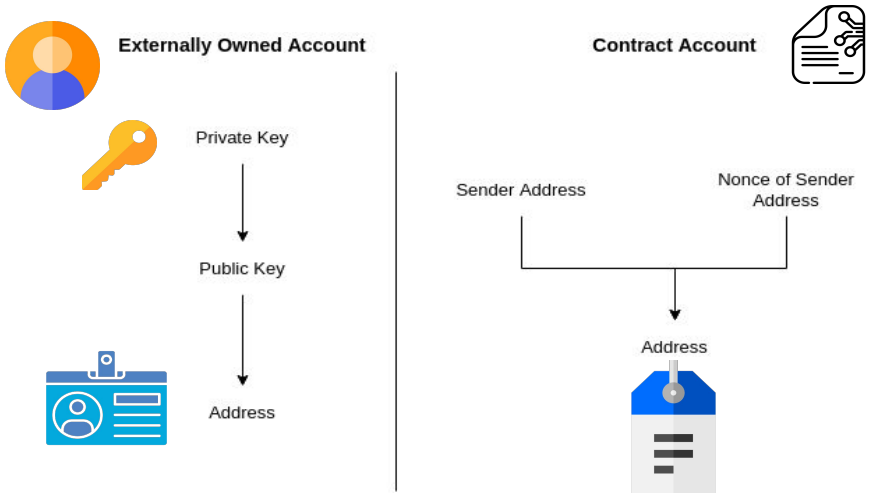
About Ethereum Virtual Machine



Identity: Accounts

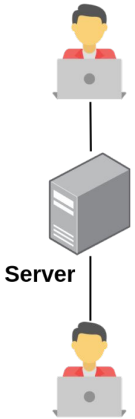
An identity to interact with Ethereum network

0x6eB27Ca7727b7B57dE81df53b27B87b319c94E52

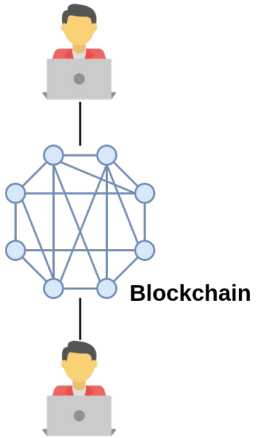


Decentralized Applications (DApps)

- Applications built on top of decentralized network, like Ethereum
- Distributed and shared control among the network participants
- Open and Transparent code
- Code Reusability



	App	DApp
End user Experience	Not Affected	
Communication	Centralized	Peer to Peer
Data Store	Centralized	Distributed



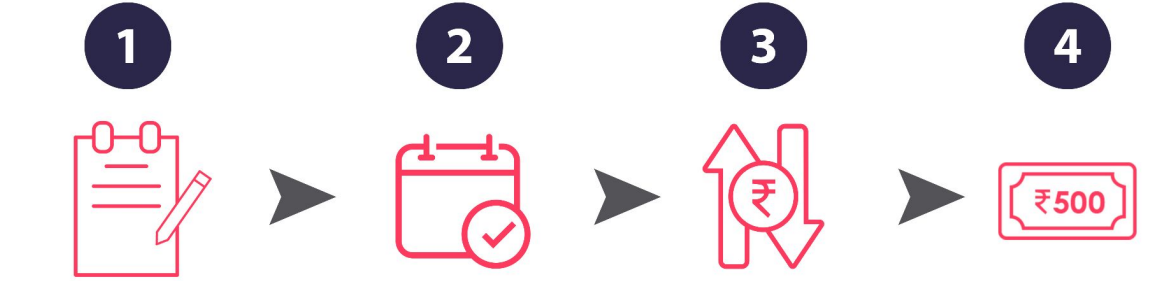
The Smart Contract

- A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract.
- Smart contracts allow the performance of credible transactions without third parties.
- These transactions are trackable and irreversible.

Smart Contracts - Heart of Programmability

- ➔ Introduced by Nick Szabo in 1994.
- ➔ Agreement between two or more people in the form of computer program
- ➔ Business logic / protocol.
- ➔ Immutable and tamper-proof agreement with no intermediaries / third parties.

How do smart contracts work:



Pre-programmed Contracts

A line of code is established by all counterparties defining the rules, terms and conditions of the agreement.

Chain of Events

If the events specified by pre-defined conditions takes place, the code automatically gets executed.

Value Transfer

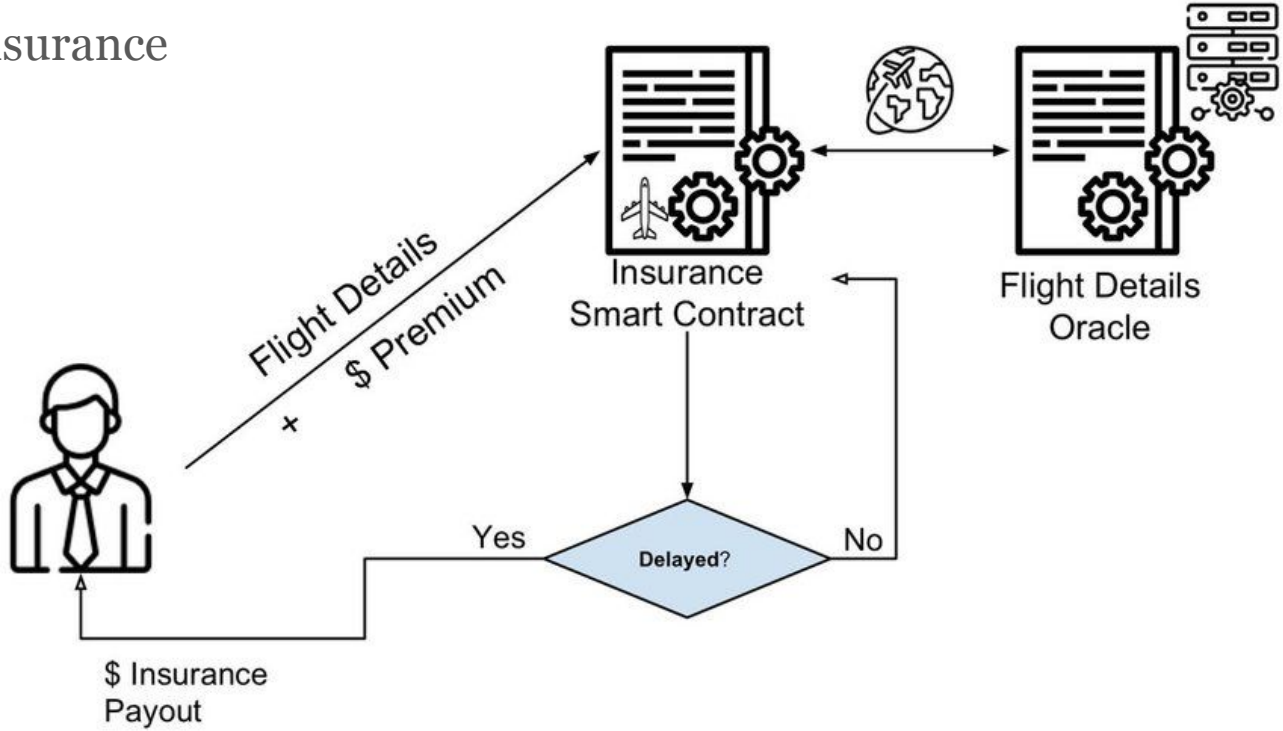
Once the code gets executed, the terms of contract makes sure that the transfer is made to the relevant parties.

Settlement

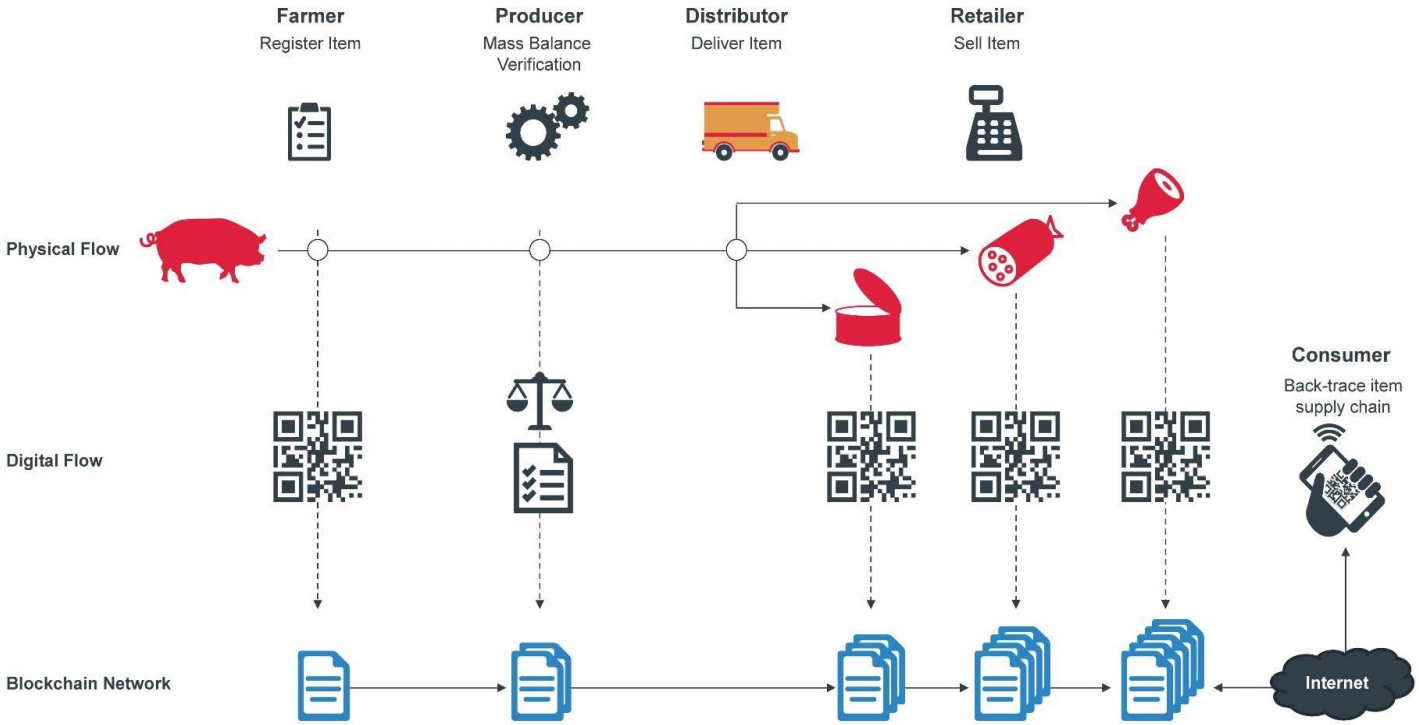
Once the transfer of value to the counterparties takes place, the transaction gets recorded on the blockchain.

A Use Case

Flight Delay Insurance



Supply Chain



Evolution of Chain

The Currency

The implementation of distributed ledger technology led to its first and obvious application: **Cryptocurrencies**

Smart Contracts

An extension of blockchain into privacy, smart contracts and the emergence of non-native asset blockchain tokens and capabilities

Decentralized Applications

Adoption to mainscale applications, blockchain scaling. Improves speed without sacrificing security

Blockchain Variants

Permission-less

- Anyone can join the network and participate in consensus
- No need to prove identity.
- Proof of Work and Proof of Stake are some of the consensus used.
- Eg: Bitcoin and Ethereum

Permissioned

- Only a restricted set of users have the rights to validate the block transactions
- Paxos, Raft, PBFT consensus : Only approved actors participate in consensus
- Eg: Hyperledger Fabric, Corda

HYPERLEDGER FABRIC

c·rda

Why Industry loves Blockchain ?

Traceability

Enhanced Security & Availability

Auditability

Universal record

Third party elimination

Where does the chain fit ?

DIGITAL IDENTITY

A SELF SOVEREIGN ID CAN BE USED TO VERIFY IDENTITY WITHOUT NEEDING AN INDIVIDUAL TO PRODUCE NUMEROUS DOCUMENTS

SUPPLY CHAIN MANAGEMENT

BLOCKCHAINS ALLOW MULTIPLE PARTIES TO ACCESS A DATABASE TO ACT AS THE SINGLE SOURCE OF TRUTH. RECORDED TRANSACTIONS ARE IMMUTABLE, ARE APPEND ONLY AND PROVIDE A TIME STAMPED AUDIT TRAIL .

HEALTHCARE

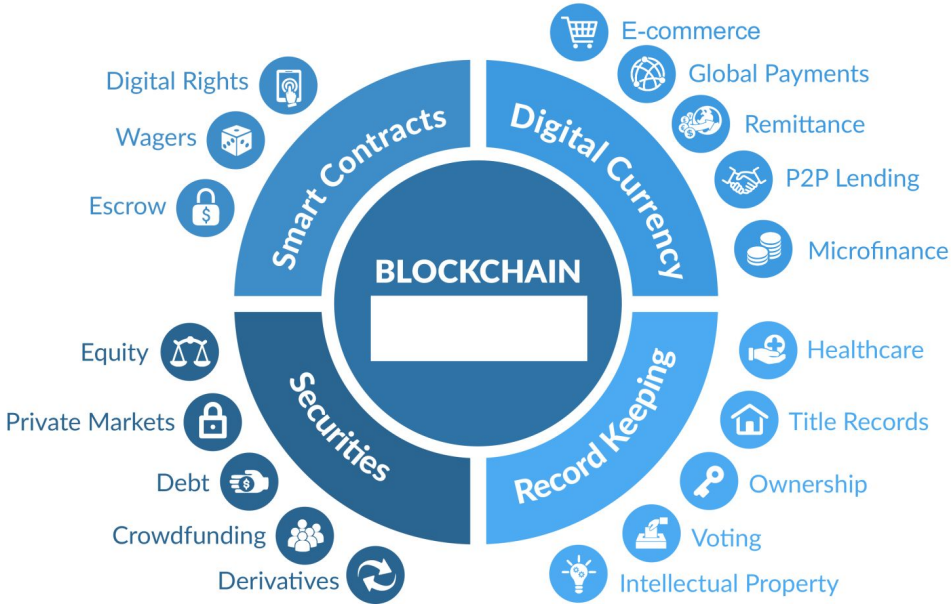
USING BLOCKCHAIN TECHNOLOGY TO RECORD PATIENT INFORMATION ON A DISTRIBUTED LEDGER CAN ALLOW DIFFERENT STAKEHOLDERS CONDITIONAL ACCESS TO A SINGLE SOURCE OF TRUTH

REAL ESTATE

BLOCKCHAIN ALLOWS PEOPLE TO TRANSFER FUNDS, PROPERTY TITLES AND DATA IN A MORE PEER-TO-PEER MANNER THAT IS DIGITAL AND OPEN SOURCE

Value of Blockchain

- Distributed environment.
- Trust-free consensus based transactions.
- Auditable public ledger system.
- Resilient systems.
- Reduction in cost and complexity.
- Trace intruders and attackers.



Decentralized Applications & Smart Contracts

Ethereum Wallets

- Software application that helps you manage your Ethereum account.
- It holds your keys and can create and broadcast transactions on your behalf.
- **MetaMask** is a browser extension wallet that runs in your browser.
- https://metamask.io/

Solidity

- Contract-oriented, high-level programming language for implementing smart contracts.
- Similar to *C++*, *Python* and *JavaScript*
- Supports inheritance, Libraries…..
- EVM Compatible.
- Ref: https://soliditylang.org/

Remix IDE

- IDE for coding smart contracts in Solidity.
- Remix has an inbuilt ethereum node where you can deploy the contract and test it.
- https://remix.ethereum.org/
- By default files are stored in browser's local storage.
- Refer https://remix-ide.readthedocs.io/en/latest/

Remix IDE: Deploy & Run Options

Environment: The environment to which the contract is deployed, can be one of the below.

Remix VM: A simulation of the Ethereum node by Remix developers for testing purposes inside the Remix IDE.

Injected Web3: Establish a connection to Metamask or similar wallet applications, which provides a connection object.

Web3 Provider: Connect to an Ethereum node (eg: Geth.) running on a computer. This option can also be used to connect to Ethereum node simulation tools.

<L2> Provider: Connect to layer 2 solutions.

Account: Shows the list of unlocked accounts in the connected environment.

Gas Limit: The maximum gas that can be used for a transaction. .

Value: When you are required to transfer ether to contract, the ether value can be given here.

Decentralized Applications Tech Stack

Queries?