The Chain of Trust

Agenda

What?

How?

Why?

Types

Security Model

Smart Contracts

Agenda

SOLIDITY

DEMO

PLATFORMS

SCOPE

What?

Blockchain =/= Bitcoin

Blockchain is gold

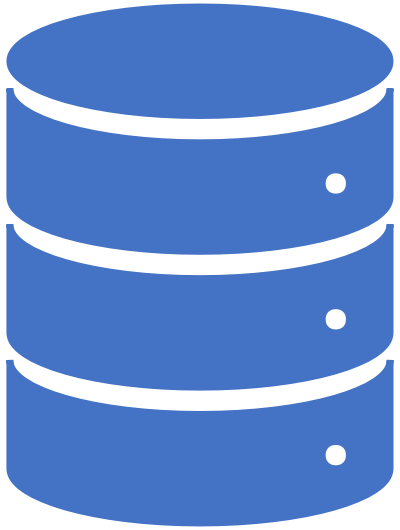
Bitcoin is jewelry

What?

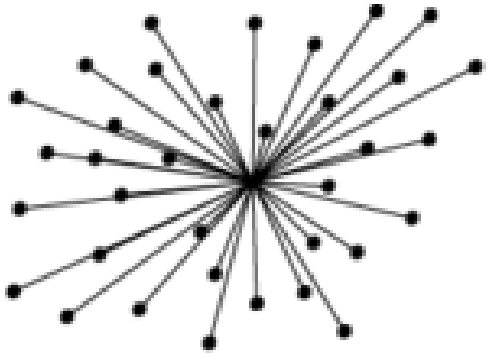
Immutable

Distributed

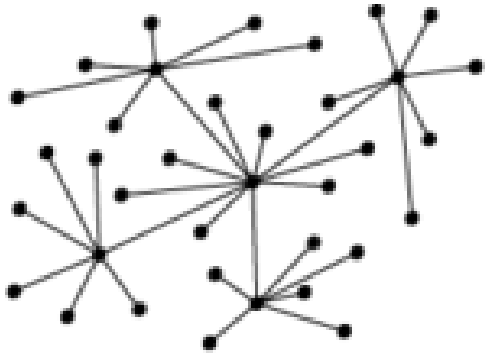
Ledger (Linked List)



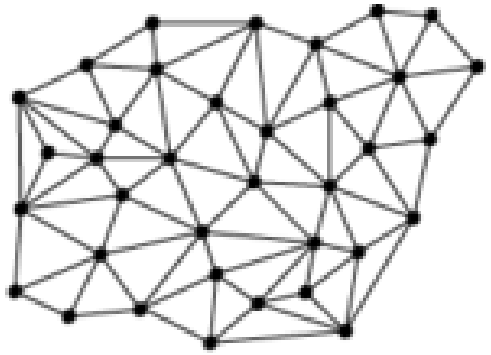
Immutable



centralised



decentralised



distributed

Distributed

Ledger

How?

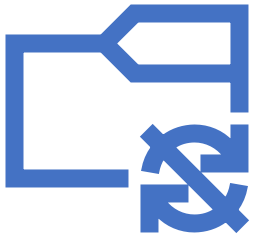
Distributed Computing

P2P Connections

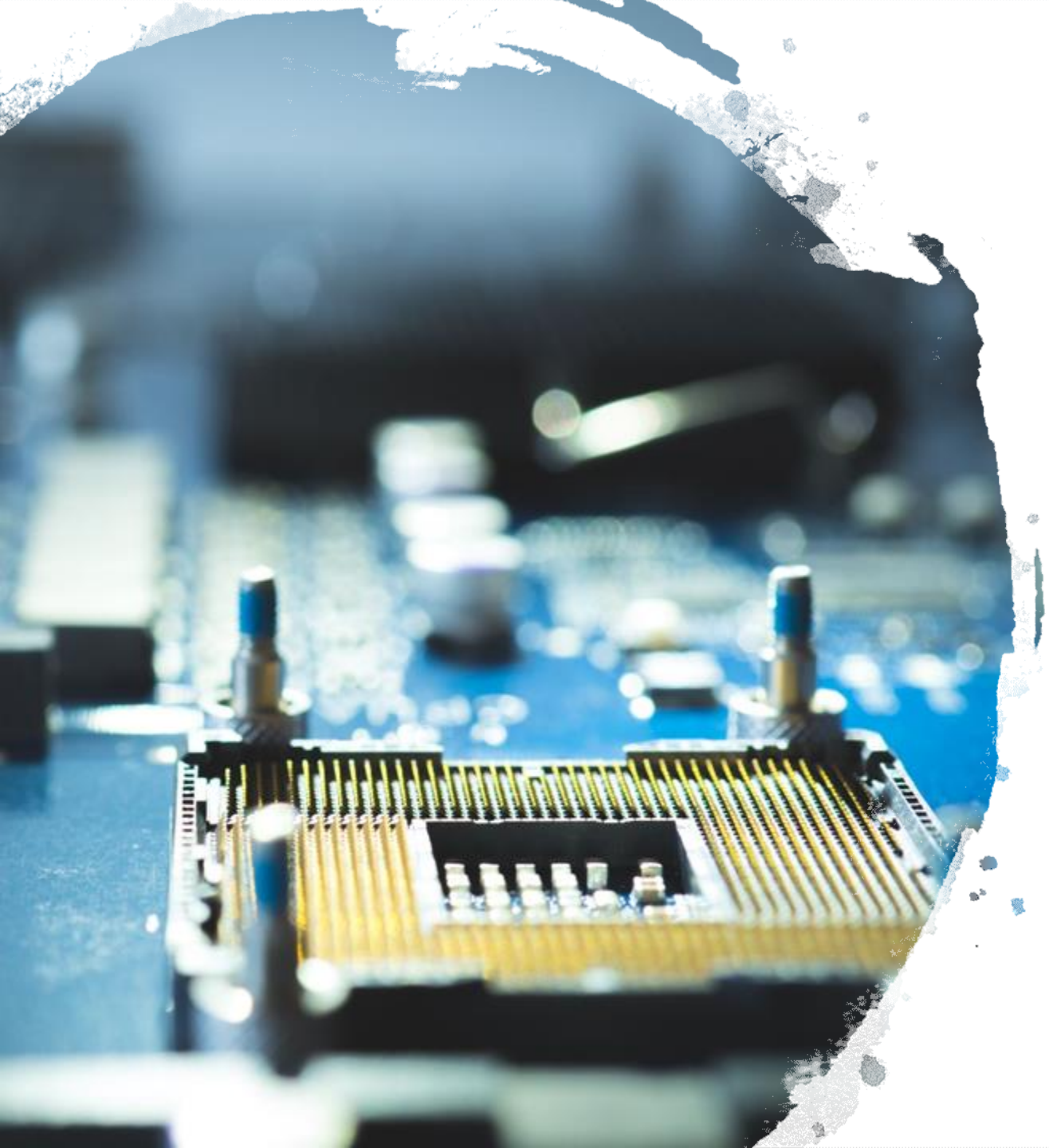
Hashing Algorithms

Merkle Tree

Consensus



Distributed Computing



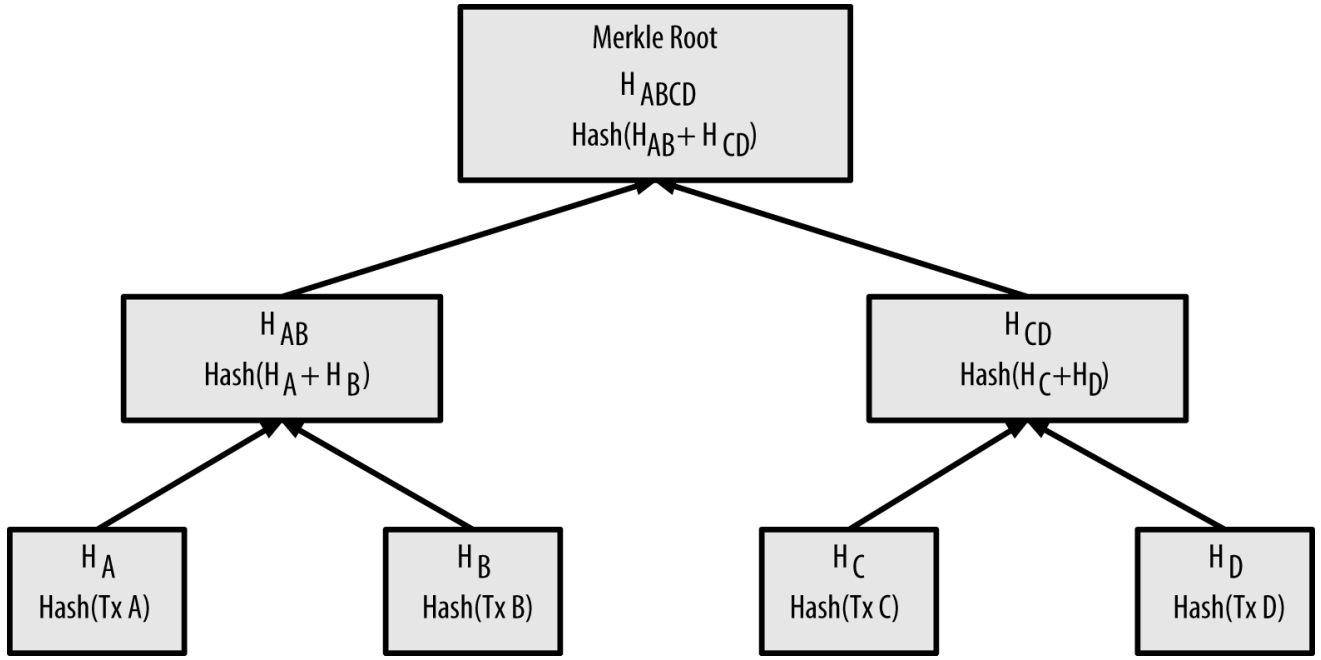
P2P Connections

Hashing Algorithms

One Way Encryption

Avalanche Effect

Pre-Image Resistance


Merkle Root
H ABCD
Hash(H AB + H CD)
H AB
Hash(H A + H B)
H CD
Hash(H C+H D)
H A
Hash(Tx A)
H B
Hash(Tx B)
H C
Hash(Tx C)
H D
Hash(Tx D)

Merkle Tree

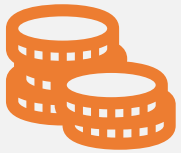
Consensus

Proof of Work

Proof of Stake

Proof of Authority

Why?



Crypto Currencies

IPFS / StorJ

DAPPs

Why?

Freedom

More Control

Democratic Internet

Types

PRIVATE

PUBLIC

Security Model

Byzantine Fault Tolerance

Identity

Cryptography

Byzantine Fault Tolerance

- 2 Generals Problem
- Algorithm OM(m)

2 Generals Problem

Alice & Bob on sides of mountain

Mountain top enemy

Unison Attack

Communication Gap

Algorithm OM(m)

Oral Message Algorithm

Commander Sends message

Lt. Interprets message as 0 or 1

Identity

No Accounts

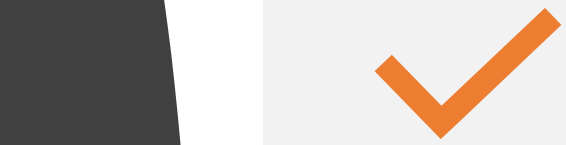
No Balances

No Addresses

No Coins

No PII

Cryptography



AES

ECDSA

SHA

Smart Contracts

Ethereum

Ethereum State

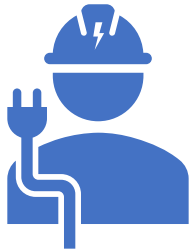
Gas

EVM Simultaneous Computation

Anything can be on blockchain

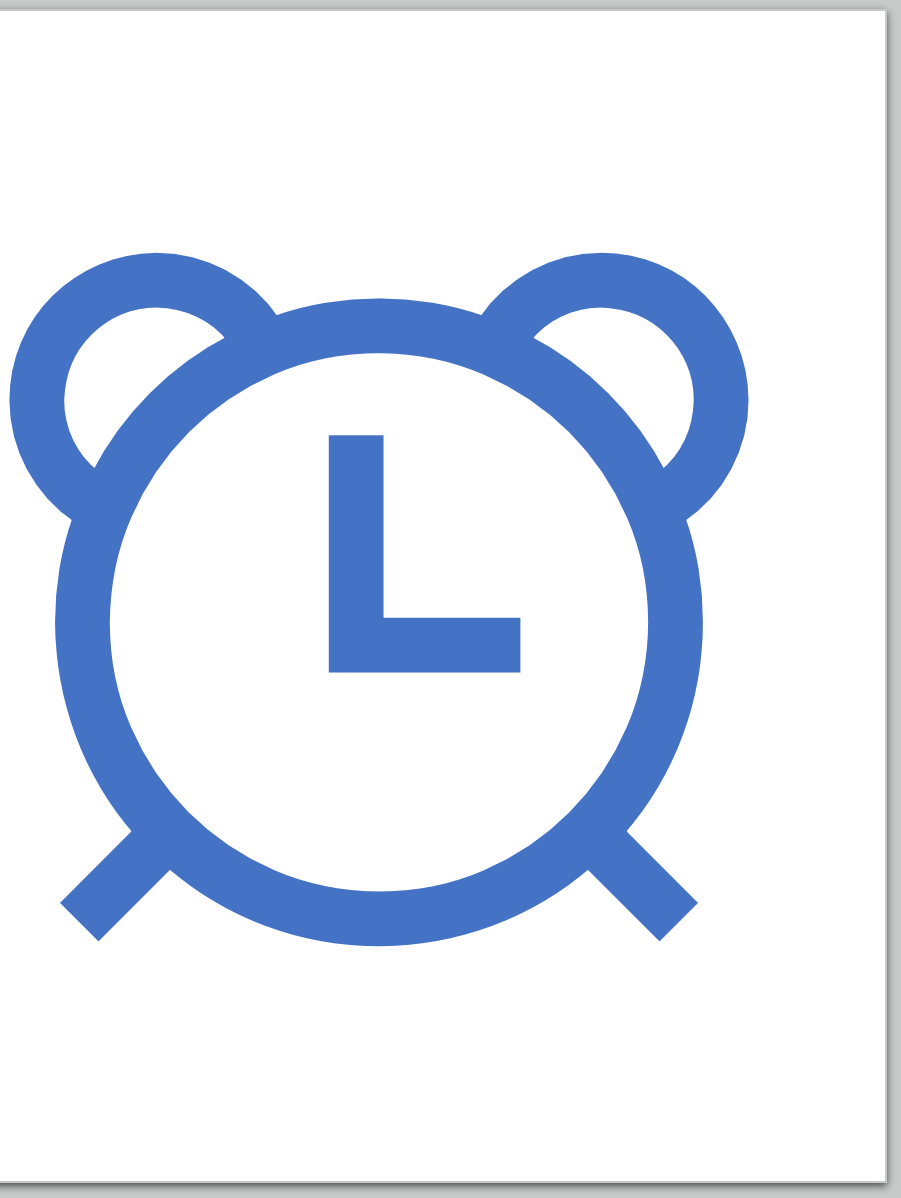
Solidity

Object Oriented



Works on EVM

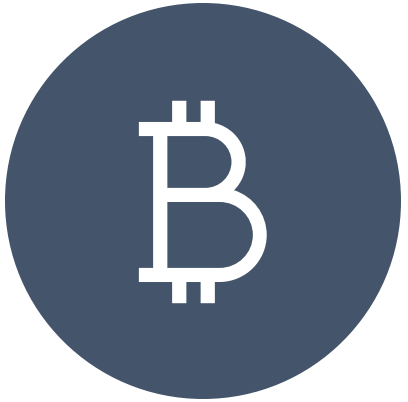
Language for Smart Contracts



Demo Time

Platforms

ETHEREUM



BITCOIN

HYPERLEDGER

Scope

Jobs

Disruption

New Internet

Jobs

SOLULAB

CYBER INFRASTRUCTURE INC.

YES BANK

IPFS

PIXEL CRAYONS

Disruption

Untapped Market

Web 3.0

Identity Management

Distributed AI

New Internet

Q / A

Contact

LinkedIn: /in/gaurav-gogia

GitHub: gaurav-gogia

Email: gaurav-gogia@outlook.com