Introduction to Blockchain

Module-1
Mr. Rupesh Mishra

Introduction to Blockchain

1. What is a blockchain
2. Origin of blockchain
    a. Hash functions
3. Foundation of blockchain
    a. Merkle trees

1. Components of blockchain
2. Block in blockchain
3. Public, Private, and Consortium
4. Consensus Protocol
5. Challenges of blockchain

rupeshmishra@sfit.ac.in

Evolution of WWW

- **Web 1.0**
  - ✓ Readonly Web
  - ✓ HTML pages with Hyperlink
- **Facts and Information**
  - ✓ Frames and Tables
  - ✓ Content from Filesystem

- **Web 2.0**
  - ✓ Read, Write, Alter
  - ✓ Javascript Framework
- **Facts and Information**
  - ✓ Responsive to use input
  - ✓ Content from API, Databases

- **Web 3.0**
  - ✓ Read Write Interact
  - ✓ Decentralised Protocol
- **Facts and Information**
  - ✓ Smart Contract and Sementic Web
  - ✓ Integration of DLT, Blockchain

rupeshmishra@sfit.ac.in

Portable and Personal, Ownership of Content

Social Web, User Generated Content

Small number of content creator for a larger audience

rupeshmishra@sfit.ac.in

Definition

- **Blockchain is an immutable database that records information efficiently on a decentralised network.**
- **Details stored on a blockchain are verifiable**
- **Blockchain provides the process of**
  - ✓ Recording Transactions
  - ✓ Assets Tracking
    - Tangible
    - Intangible

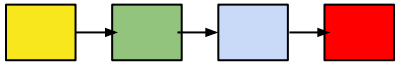
rupeshmishra@sfit.ac.in

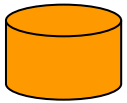
Why Blockchain

- **Issues in Centralisation**
  - ✓ Single point of Failure
    - Centralised | Distributed | Decentralised
  - ✓ Acts as Middle Man
  - ✓ Counterparty risk
  - ✓ Scalability
- **Multiple authority do not trust each other can corporate, coordinate and collaborate**
- **Computation and Information Sharing Platform**

rupeshmishra@sfit.ac.in

Blockchain Based DLT





Blockchain

- Ever Growing
- Hash Chain from prev to next
- Includes set of transection
- Linked List
- Immutable

World State

- Most Recent State (Output of most recent transaction)
- Key - Value Pair
- All changes recorded as transaction on Blockchain

rupeshmishra@sfit.ac.in

- **Block**
  - ✓ Ever Growing List of Records
- **Chain**
  - ✓ Cryptographic hash value
  - ✓ Prev block to link with next blocks securely
- **Genesis Block (Block 0)**
- **Block Content**
  - ✓ Block Header
  - ✓ Block Data

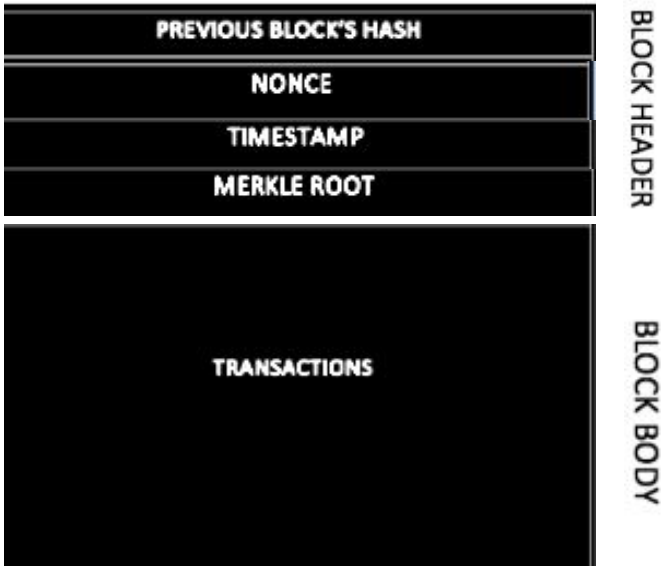


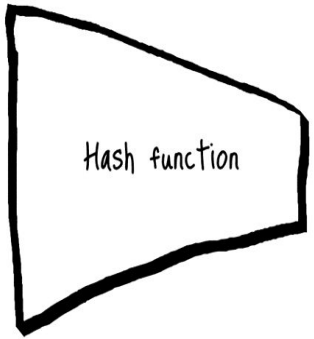
Fig: Generic Structure of Block

rupeshmishra@sfit.ac.in

In the generic structure of Block Header of Genesis Block, which attribute is set to zero?

Origin of Blockchain

Hash Function



- **Cryptographically Secure Hash Function H(x)**
- **Function to map any size of input to fixed size of output**
  - ✓ One way function
    - y = H(x)
    - Compute y if x is known
    - Not possible to compute x if y is known
  - ✓ Deterministic
  - ✓ Different Hash for different data
  - ✓ Avalanche Effect

rupeshmishra@sfit.ac.in

Transaction Data

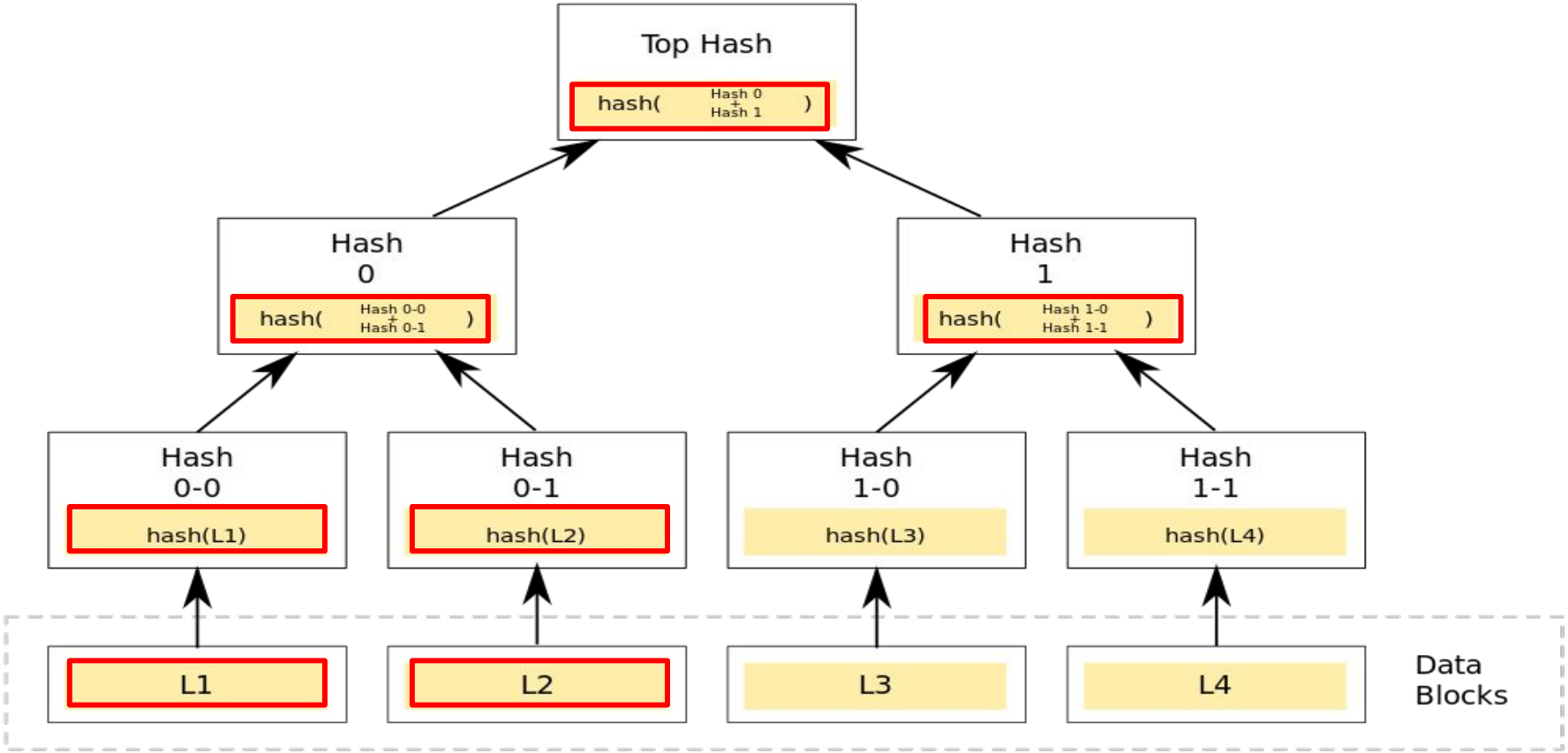
- **Merkle tree**
  - ✓ Binary Tree
  - ✓ Root Node - Commitment
  - ✓ Inner Node - hash of the child nodes
  - ✓ Data Node - Leaf Node
  - ✓ Commitment Scheme
- **Leaf nodes revealed and proven to be part of the original commitment**
- **Efficient and Secure verification of the contents (large data structure)**

rupeshmishra@sfit.ac.in

Uses of Merkle Tree

- **Verification of stored data**
- **Transferring and Managing between computers**
- **Integrity of data received in a peer-to-peer network**
- **Check that the other peers do not lie and send fake blocks**
- **Application**
  - ✓ Bitcoin and Ethereum - Peer-to-peer networks
  - ✓ Git - Revision Control System
  - ✓ Apache Cassandra, Riak, and Dynamo - NoSql Database

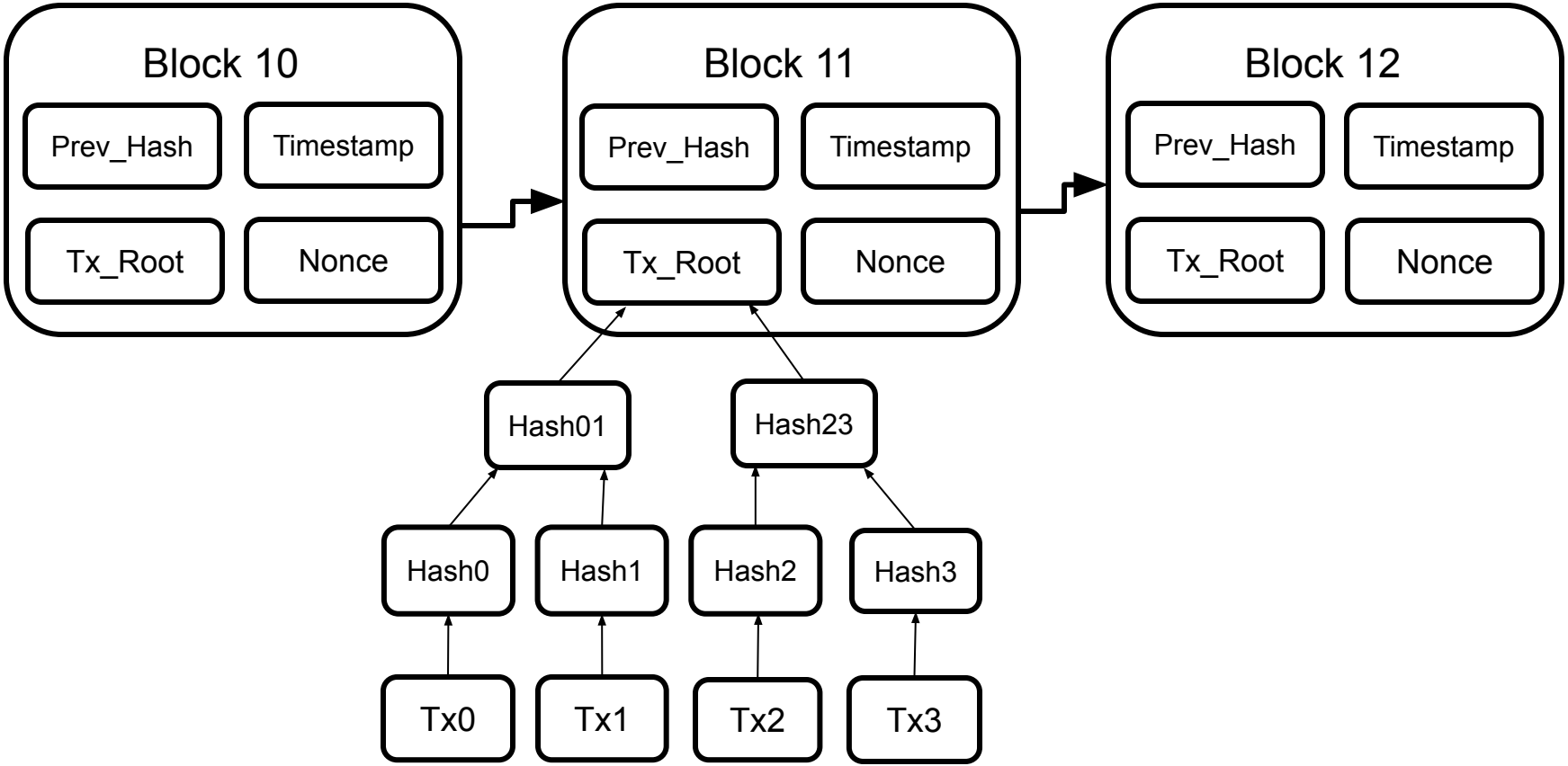
13
rupeshmishra@sfit.ac.in



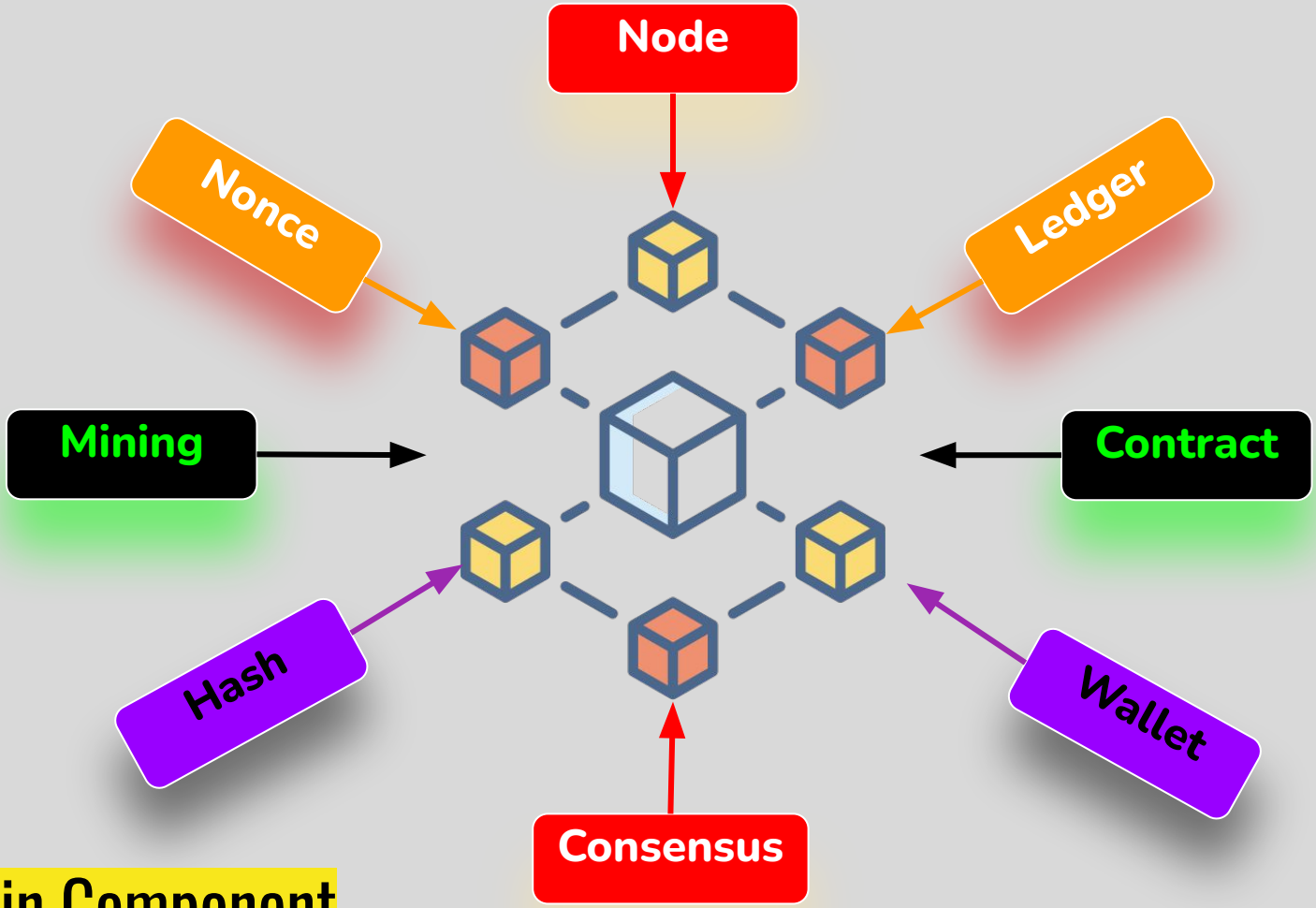
By Azaghal - Own work, CCo, https://commons.wikimedia.org/w/index.php?curid=18157888

rupeshmishra@sfit.ac.in

Merkle Tree Demo



rupeshmishra@sfit.ac.in



Blockchain Component

rupeshmishra@sfit.ac.in

Node

- **Network of computers that run a blockchain**
- **Peer to Peer Network**
- **More number of node → More secure network**
  - ✓ 51 % Attack
- **Two Types**
  - ✓ **Full Node**
    - Maintains full copy of all the transections
    - Validate, accept and reject Transaction
  - ✓ **Partial Node**
    - Light Node
    - Maintains only block header
    - Connected with full node for security

rupeshmishra@sfit.ac.in

Ledger

- **Data structure / Digital database of Information**
- **Application interacts with ledger to read/write its content**
- **Stores records of approved transactions**
  - ✓ **Check that the wallet initiating the transaction has enough funds to send the required amount**
  - ✓ **Be authorized (signed) by the one who's submitting the transaction.**
  - ✓ **Check that the destination account is valid**

rupeshmishra@sfit.ac.in

Contract

- **Smart contract is the business logic**
- **Transaction**
  - ✓ Invocation of functions of smart contract
- **A software to manipulate and read ledger**
- **get and set ledger state**
- **Immutable once deployed on blockchain**
- **Written in High Level Language and compiled to Bytecode**
- **Executed in a sandbox mode**

rupeshmishra@sfit.ac.in

Wallet

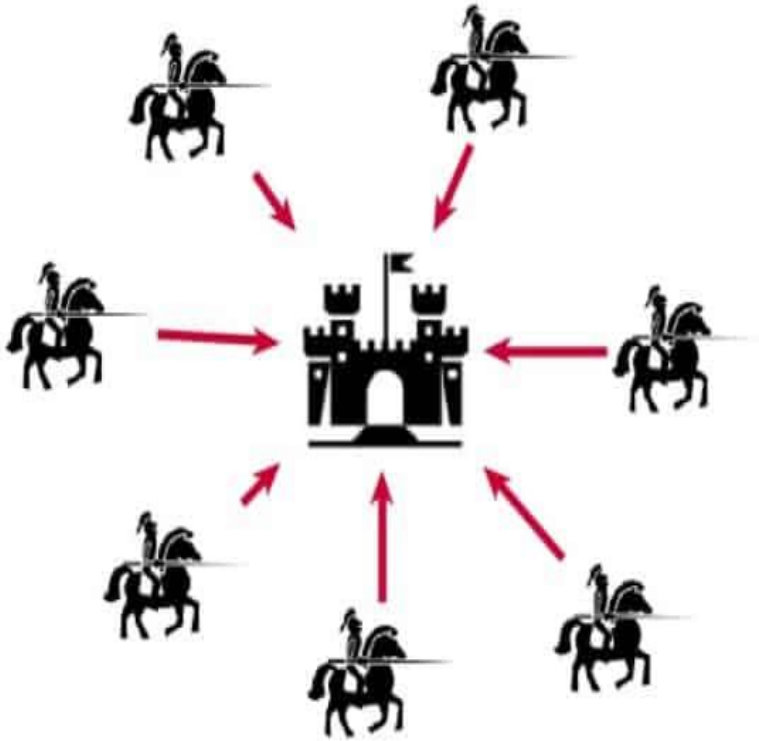
- **Stores Cryptocurrencies and security credentials**
- **Public and Private Key**
- **Digital Identity to perform transactions**
- **Types of Wallet**
  - ✓ **Hot Wallet**
    - Software based
    - Connected to Internet
  - ✓ **Cold Wallet**
    - Hardware based
    - Not Connected to internet

rupeshmishra@sfit.ac.in

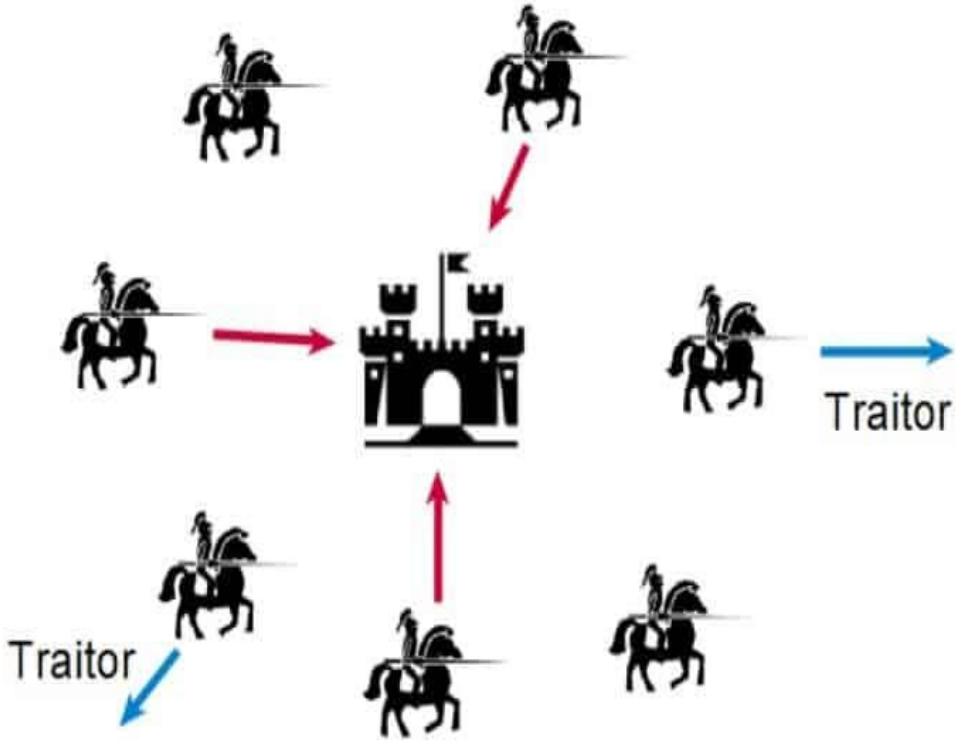
Consensus Protocol in Blockchain

- **Set of rules and procedures for attaining a unified agreement between the participating nodes on the status of the network**
- **The rules defines the process for**
  - ✓ **Authentication and validation of transactions added to a distributed ledger**
  - ✓ **To prevent**
    - Creation of different versions of the ledger
    - Alteration of previous transactions
- **Solution for Byzantine General Problem of Distributed Computing**

rupeshmishra@sfit.ac.in



Coordinated attack leading to victory



Uncoordinated attack leading to defeat

n

Consensus Protocol

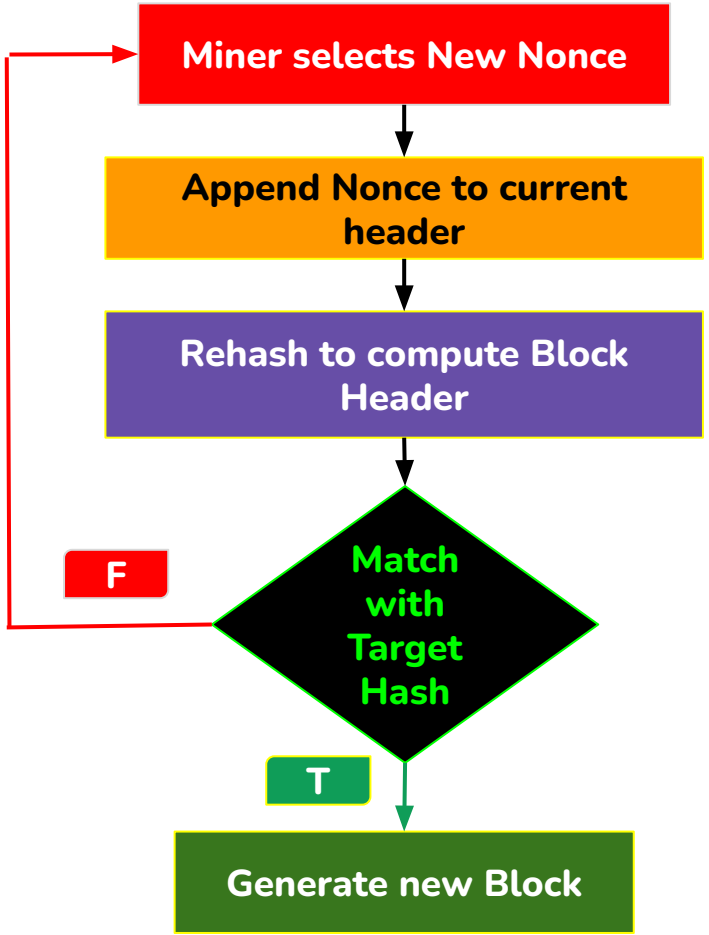
- **Objective**
  - ✓ Unified Agreement
  - ✓ Fault Tolerant
  - ✓ Prevent double spending
  - ✓ Incentivisation
  - ✓ Egalitarian
  - ✓ Collaborative and Participatory

- **Algorithms**
  - ✓ Proof of Work (PoW)
  - ✓ Proof of Stake (PoS)
  - ✓ Proof of Elapsed Time(PoET)
  - ✓ Proof of Burn (PoB)
  - ✓ Proof of Authority (PoA)
  - ✓ PBFT
  - ✓ RAFT

rupeshmishra@sfit.ac.in

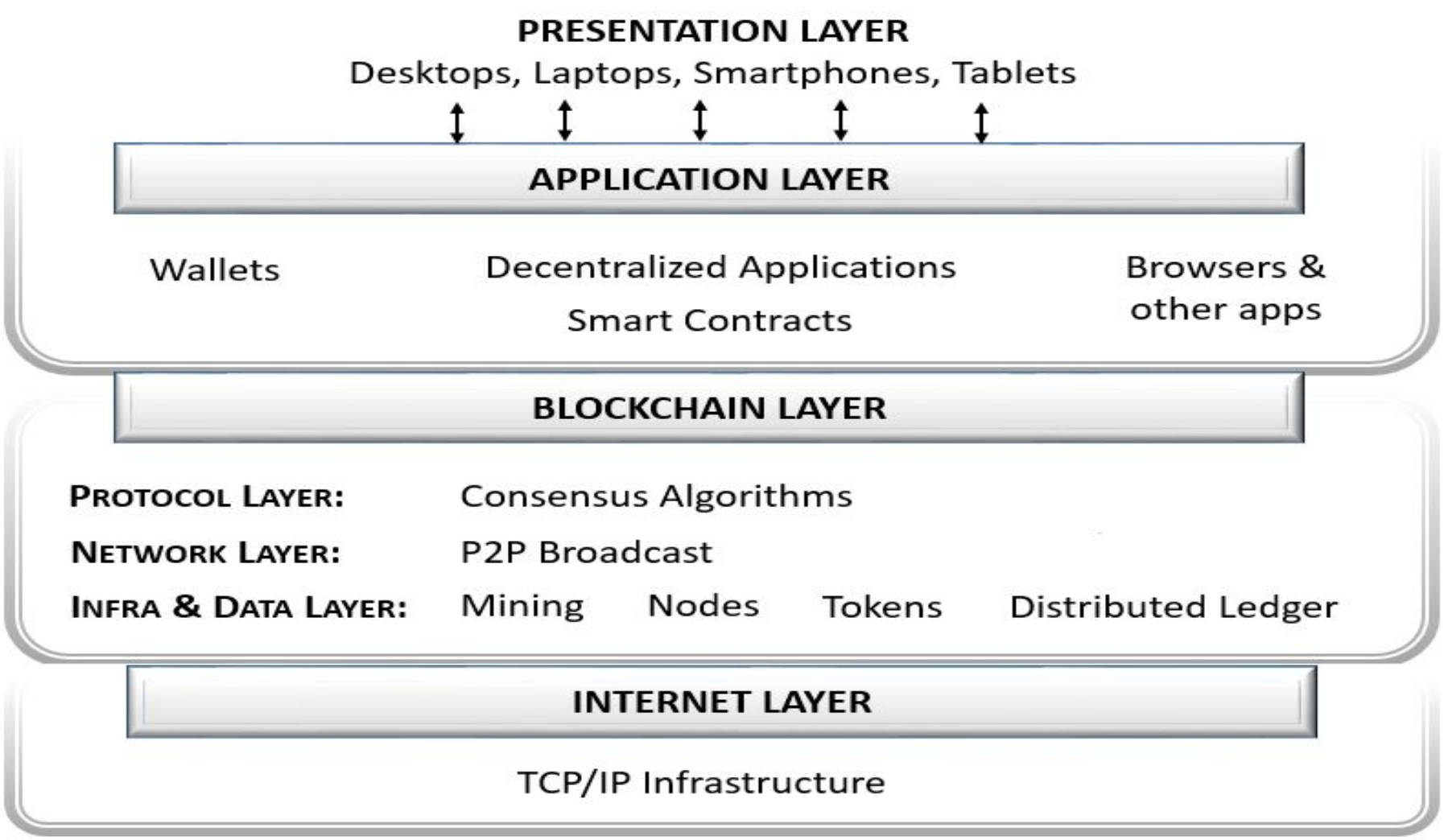
New Block Generation

- **Hash**
  - ✓ Data mapping to fixed size value
  - ✓ Maintain Integrity
  - ✓ Collision resistant and Difficulty
- **Mining**
  - ✓ Special type of node
  - ✓ Calculate new block hash
  - ✓ Helps in maintaining consensus
- **Nonce**
  - ✓ Number used once
  - ✓ Create new block
  - ✓ Validate block hash

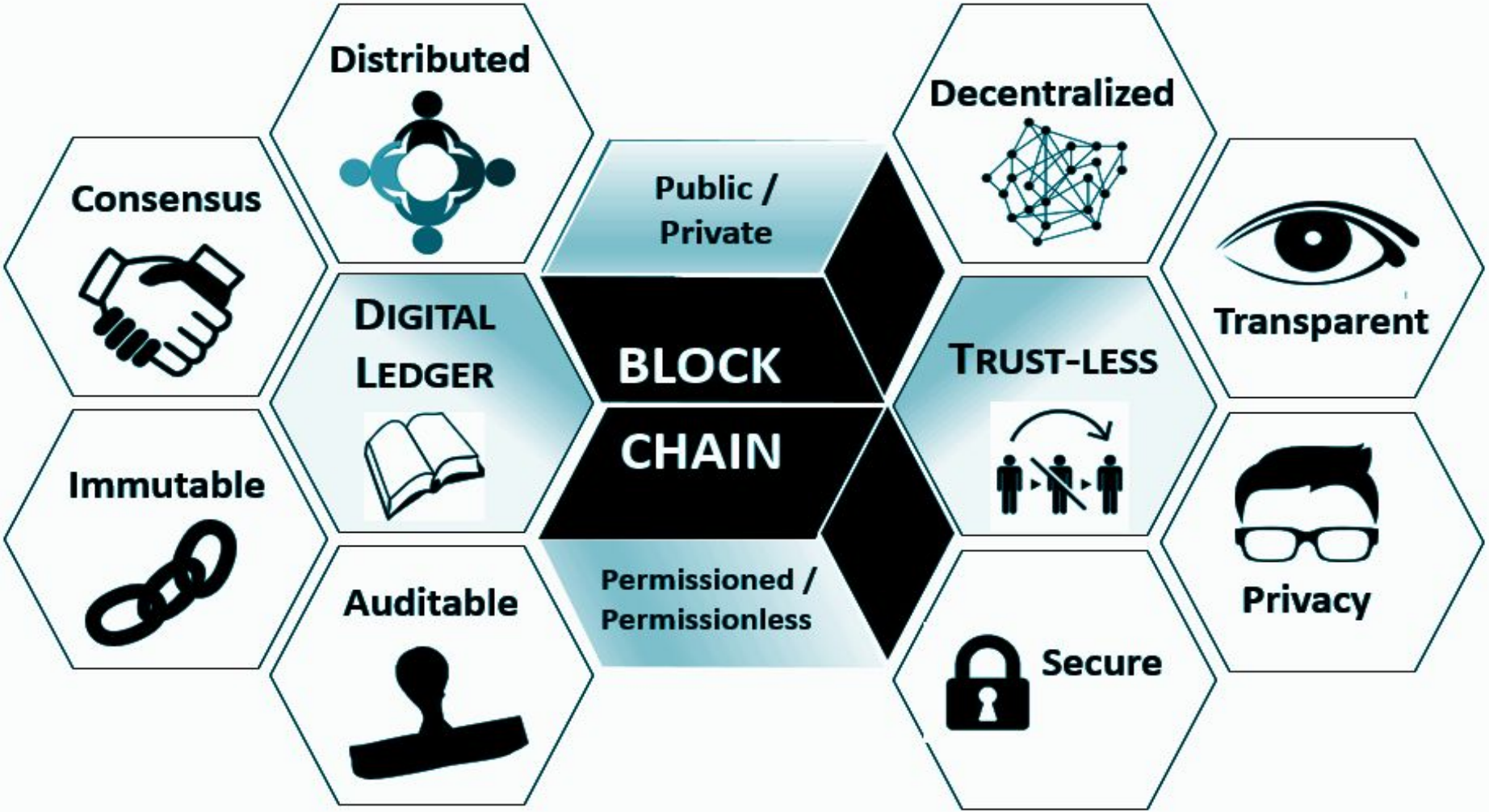


rupeshmishra@sfit.ac.in

Blockchain Layers


PRESENTATION LAYER
Desktops, Laptops, Smartphones, Tablets
APPLICATION LAYER
Wallets
Decentralized Applications
Smart Contracts
Browsers & other apps
BLOCKCHAIN LAYER
PROTOCOL LAYER: Consensus Algorithms
NETWORK LAYER: P2P Broadcast
INFRA & DATA LAYER: Mining Nodes Tokens Distributed Ledger
INTERNET LAYER
TCP/IP Infrastructure

Blockchain Characteristics


Distributed
Decentralized
Consensus
Public / Private
Transparent
DIGITAL LEDGER
BLOCK CHAIN
TRUST-LESS
Immutable
Privacy
Auditable
Permissioned / Permissionless
Secure

Types of Blockchain

Types of Blockchain

- **Public Blockchain**
  - ✓ Decision making done by miner
    - executes decentralized consensus mechanisms such as proof of work (POW) and proof of stake (POS) etc.
  - ✓ Open and transparent
    - Anyone can review anything at a given point of time
  - ✓ Example
    - Bitcoin, Ethereum etc.

rupeshmishra@sfit.ac.in

Types of Blockchain

- **Private Blockchain**
  - ✓ Private property of an individual or an organization.
  - ✓ Central authority to manage
    - Read/Write
    - Authorization
  - ✓ Consensus is achieved on the whims of the central in-charge
  - ✓ Mining rights given to anyone or not give at all
  - ✓ Example
    - Hyperledger

rupeshmishra@sfit.ac.in

Types of Blockchain

- **Consortium Blockchain**
  - ✓ More than one in charge
  - ✓ Consensus
    - A group of companies or representative individuals coming together and making decisions for the best benefit of the whole network.
  - ✓ Such groups are also called consortiums
  - ✓ Example
    - Corda, r3 etc.

rupeshmishra@sfit.ac.in

Types of Blockchain

- **Hybrid Blockchain**
  - ✓ Partially open
    - Private -> Generation of Block
    - Public -> Stored Data
  - ✓ No full control of alteration of transection to any central authority
  - ✓ Example
    - Ripple, XRP, etc.

rupeshmishra@sfit.ac.in

Public	Private	Consortium	Parameter
Permissionless	Permissioned	Permissioned	Join Network
Open	Closed	Partially Open	Ledger
Slow	Fast	Fast	Speed
Decentralised	Centralised	Semi Decentralised	Decentralization
PoW, PoS	Owner	Voting	Consensus
Bitcoin, Ethereum	Hyperledger	Corda, r3	Example

rupeshmishra@sfit.ac.in

	PUBLIC BLOCKCHAIN	PRIVATE BLOCKCHAIN	CONSORTIUM BLOCKCHAIN	HYBRID BLOCKCHAIN
USERS	Anonymous; but web tracking and cookies pose a risk to privacy	Known & trusted participants	Known & trusted participants	Anonymity for public network members; private network members are known within the private network
ACCESS	Open and Transparent to all	Access fully restricted	Selectively open; relevant transparency provided	Centralized control of providing access, hence privacy and confidentiality maintained
NETWORK TYPE	Decentralized; zero points of failure	Centralized; single point of failure	Partially decentralized; multiple points of failure	Zero points of failure
OPERATION	Anyone can read or initiate or receive transaction	Pre-approved participants can read &/or initiate transaction	Pre-approved participants can read &/or initiate transaction	Any combination is possible; Operations are customizable. Central authority decides which transactions can be made public and which are private
VERIFICATION	Anyone can be a node and take part in the consensus process to validate transactions and create a block	Single validator node or central authority to create a block	Only privileged members of the consortium can validate and create a block	The public network verifies the block
IMMUTABILITY	Secured by hashing	Secured by distributed consensus	Secured by distributed consensus	Secured by hashing at the private network and secured by distributed consensus by the public blockchain
CONSENSUS MECHANISM	PoW, PoS, etc.	Voting or variations of PoW/PoS consensus algorithms	Voting or variations of PoW/PoS consensus algorithm	DPoS in public and variations in private
INCENTIVIZATION	Incentivizes miners to grow the network	Users limited to within a company; hence incentivization is not relevant	Limited incentivization	Can incentivize users in the main public network
SECURITY	Security based on consensus protocol and hash functions. Higher the security, lower the performance	Security is dependent on the blockchain architecture	Security is dependent on the blockchain architecture adopted	Very high as hackers or unknown parties cannot access the system
TRUST	Trust-free system; trust is enforced via cryptographic proof	Trusted; central control	Trusted; need to trust the majority	Trust-free system, consensus by blockchain

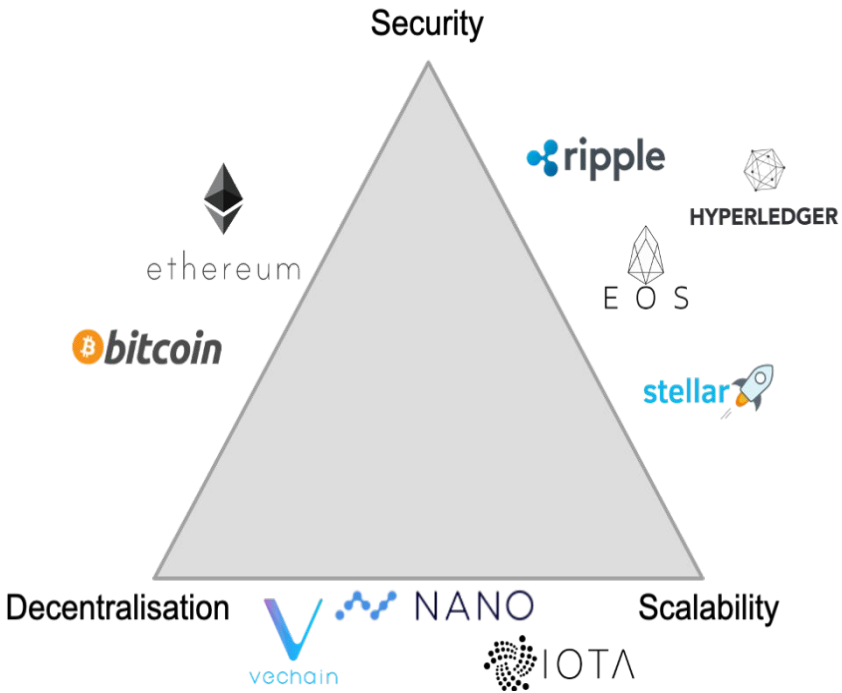
rupeshmishra@sfit.ac.in

Challenges

- **Scalability**
  - ✓ More user using network increases the cost
- **Speed**
  - ✓ Speed of completion of number of transaction is low
- **Interoperability**
  - ✓ Interaction and data sharing among different blockchain platform
- **Regulation**
  - ✓ No regulation for reverse of transection
- **Privacy and Security**
  - ✓ Information is shared with every node
- **Energy Consumption**
  - ✓ High computation
- **Lack of Standardization**
  - ✓ No universal standard
- **Misuse of Anonymity**
  - ✓ Use of technology for criminal activity

rupeshmishra@sfit.ac.in

Blockchain Trilemma



- **Decentralised**
  - ✓ No centralization
  - ✓ Core component
- **Scalability**
  - ✓ High rate of transection
  - ✓ Mass Adoption
- **Security**
  - ✓ Attack, bugs and issues
  - ✓ Improper code security
- **Trade off between three**

rupeshmishra@sfit.ac.in

Scalability

- **Visa 100,000 tx/s**
- **Ethereum 7 to 15 tx/sec**
- **High Fees**
- **Mass Adoption**
- **Solution**
  - ✓ Layer 2

- **Rollups - Bunch Tx and send**
  - ✓ ZK Rollup
    - No smart contract
  - ✓ Optimistic
    - Smart Contract
- **Sidechain**
  - ✓ Connected to main chain
  - ✓ Own security
- **Sharding**
- **Channels**
  - ✓ Only for crypto

rupeshmishra@sfit.ac.in

Reference

[1] https://en.wikipedia.org/wiki/Blockchain#/media/File:Bitcoin_Block_Data.svg

[2] https://etherscan.io/block/0

[3] https://bitcoinchain.com/block_explorer/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f/

[4] https://andersbrownworth.com/blockchain/public-private-keys/keys

rupeshmishra@sfit.ac.in