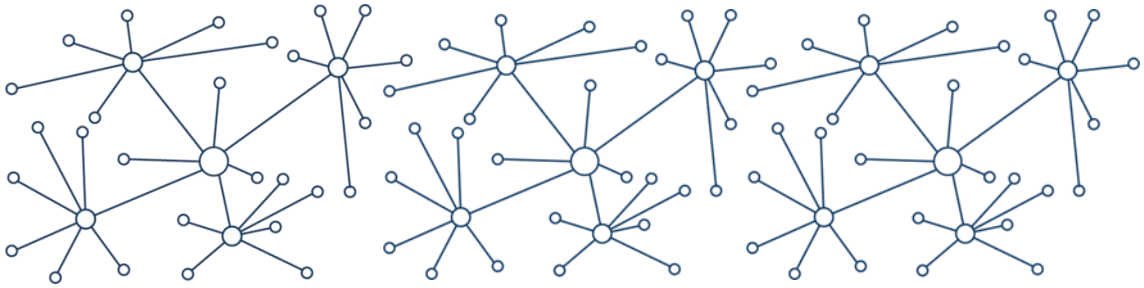


Blockchain Technology

Core Elective 3 – CS423

B. Tech. IV CSE 7th Sem

Lecture#1 and 2 (26-27 July 2022)

Dr. Dhiren Patel

Welcome note

- Digital divide (bandwidth, power, device, platform)
- NEP – New Education Policy
- Capacity building, Re-training, Up-skilling (Deep skilling)
- Personalized Education – Digital way
- As responsible citizens, all of us should fight the pandemic and other hardships, and showcase our capabilities and commitment towards economic progress with social inclusion and environment sustainability for the global good

What is a Blockchain? Why should we learn it?

- Blockchain facilitates peer-to-peer transfer of *digital assets* in a *decentralized network*
- It is a time-stamped series of (immutable) records of data that is managed by a cluster of nodes (computers) not owned by any single entity (?) - **a democratized system**
- A technology originally created to support *cryptocurrency* bitcoin - Founder (pseudo-named) – **Satoshi Nakamoto**
- Blockchain has the potential to improve applications in finance, healthcare, government, manufacturing, and distribution supply chain…
- There is a dire need for designers, developers, and critical thinkers, who can envision and create newer application models on Blockchain to benefit the world

Security primitives and its use

- Hash function (cryptographic) – e.g. SHA2
- Encryption (Block cipher, Stream cipher, Symmetric Key Encryption, Public Key Encryption)
- AES, RSA, Elliptic Curve
- Key management and Key exchange (Security Association)
- Example: Banking – end-of-day reconciliation

Blockchain

- Think of blockchain as a historical fabric underneath recording everything that happens—every digital transaction; exchange of value, goods and services; or private data—exactly as it occurs.
- Then the chain stitches that data into (encrypted??) blocks that can never be modified and scatters the pieces across a worldwide network of distributed computers or "nodes.“
- A blockchain is made up of two primary components: a decentralized network facilitating and verifying transactions, and the immutable ledger that network maintains.
- Welcome aboard in the World of Blockchain!!

Know the Course CS423

- Course scheme (3-0-0) – Core Elective 3 <see next slide>
- Course Objectives, Outcome and Curriculum/Syllabus
- Teaching methodology (Interactions and Hands on)
- Book(s), Reference(s), PPTs, Papers (ACM, IEEE, etc..), MooCs
- Course repository – Google classroom (**Class code: 3wcypqj**)
- Evaluation - **Relative Grading (Open Notes?)**
- **Mid-sem, End-sem, Assignments (coding/math/design), Quizzes/Tests, Attendance requirement (?)**

Teaching Scheme of B.Tech.-IV (CSE) (Semester VII)

Sr. No.	Course	Code	Credit	Teaching Scheme			Examination Scheme			Total
				L	T	P	L	T	P	
1	Software Engineering (Core-15)	CS401	5	3	1	2	100	25	50	175
2	Innovation, Incubation and Entrepreneurship	HU410	3	3	0	0	100	0	0	100
3	Core Elective-3	CS4AA	3	3	0	0	100	0	0	100
4	Core Elective-4	CS4BB	3	3	0	0	100	0	0	100
5	Summer Training*	CS403	2	0	0	0	0	0	50	50
6	Project Preliminaries	CS405	3	0	0	6	0	0	150	150
	Total		**19**	**12**	**1**	**8**	**400**	**25**	**250**	**675**
	Total Contact Hours per week			**21**						

Core Elective-3 (CS4AA):

1	Computer Graphics (CS421)	4	Video Codec standards and Design (CS427)
2	Blockchain Technology (CS423)	5	Computational Geometry (CS429)
3	Smartphone Computing and Applications (CS425)		

B.Tech. IV (CSE) Semester – VII
BLOCKCHAIN TECHNOLOGY (CORE ELECTIVE - 3)
CS423

	L	T	P	Credit
Scheme	**3**	**0**	**0**	**03**

---

1. Course Outcomes (COs):

At the end of the course, students will be able to

CO1	understand the need, functions and challenges of blockchain technology.
CO2	deploy smart contracts for given use cases.
CO3	analyse blockchain based system structure and security offered therein.
CO4	asses functions, benefits and limitations of various blockchain platforms.
CO5	design and develop solution using blockchain technology in various application domains.

Syllabus

- **INTRODUCTION** **(04 Hours)**

  Introduction to Blockchain Technology, Concept of Blocks, Transactions, Distributed Consensus, the Chain and the Longest Chain, Cryptocurrency, Blockchain 2.0, Permissioned Model of Blockchain, Permission less Blockchain.

- **DECENTRALIZATION USING BLOCKCHAIN** **(06 Hours)**

  Methods of Decentralization, Disintermediation, Contest-Driven Decentralization, Routes to Decentralization, the Decentralization Framework Example, Blockchain and Full Ecosystem Decentralization, Storage, Communication, Computing Power and Decentralization, Smart Contracts, Decentralized Autonomous Organizations, Decentralized Applications (DApps), Requirements and Operations of DApps, DApps Examples, Platforms for Decentralizations.

- **CRYPTO PRIMITIVES FOR BLOCKCHAIN** **(04 Hours)**

  Symmetric and Public Key Cryptography, Cryptographic Hard Problems, Key Generation, Secure Hash Algorithms, Hash Pointers, Digital Signatures, Merkle Trees, Patricia trees, Distributed Hash Tables.

Syllabus - cont

- **BITCOINS AND CRYPTOCURRENCY** **(06 Hours)**

  Introduction, Digital Keys and Addresses, Private and Public Keys in Bitcoins, Base58Check Encoding, Vanity Addresses, Multi Signature Addresses, Transaction Lifecycle, Data Structure for Transaction, Types of Transactions, Transaction Verification, The Structure of Block in Blockchain, Mining, Proof of Work, Bitcoin Network and Payments, Bitcoin Clients and APIs, Wallets, Alternative Coins, Proof of Stake, Proof of Storage, Various Stake Types, Difficulty Adjustment and Retargeting Algorithms, Bitcoin Limitations.

- **SMART CONTRACTS** **(02 Hours)**

  Smart Contract Templates, Oracle, Smart Oracle, Deploying Smart Contract on Blockchain.

- **PERMISSIONED BLOCKCHAIN** **(05 Hours)**

  Models and Use-cases, Design Issues, Consensus, Paxos, RAFT Consensus, Byzantine General Problem, Practical Byzantine Fault Tolerance.

Syllabus - cont

- **DEVELOPMENT TOOLS AND FRAMEWORKS** **(05 Hours)**

  Solidity Compilers, IDEs, Ganache, Metamask, Truffle, Contract Development and Deployment, Solidity Language, Types, Value Types, Literals, Enums, Function Types, Reference Types, Global Variables, Control Structures, Layout of Solidity Source Code File.

- **HYPERLEDGER** **(05 Hours)**

  The Reference Architecture, Requirements and Design Goals of Hyperledger Fabric, The Modular Approach, Privacy and Confidentiality, Scalability, Deterministic Transactions, Identity, Auditability, Interoperability, Portability, Membership Services in Fabric, Blockchain Services, Consensus Services, Distributed Ledger, Sawtooth Lake, Corda.

- **BLCOKCHAIN USE-CASES AND CHALLENGES** **(05 Hours)**

  Finances, Government, Supply Chain, Security, Internet of Things, Scalability and Challenges, Network Plane, Consensus Plane, Storage Plane, View Plane, Block Size Increase, Block Interval Reduction, Invertible Bloom Lookup Tables, Private Chains, Sidechains, Privacy Issues, Indistinguishability Obfuscation, Homomorphic Encryption, Zero Knowledge Proofs, State Channels, Secure Multiparty Computation, Confidential Transactions.

(Total Contact Time = 42 Hours)

Course objectives

- Capacity building - Learning through examples/use cases
- Understand technology foundations of Blockchain through protocols, security primitives, token economics, smart contracts, attacks and advances
- Design and implement new ways of using blockchain for applications with cryptocurrency and beyond
- Explore platforms to build applications on blockchain

Course outcome ()

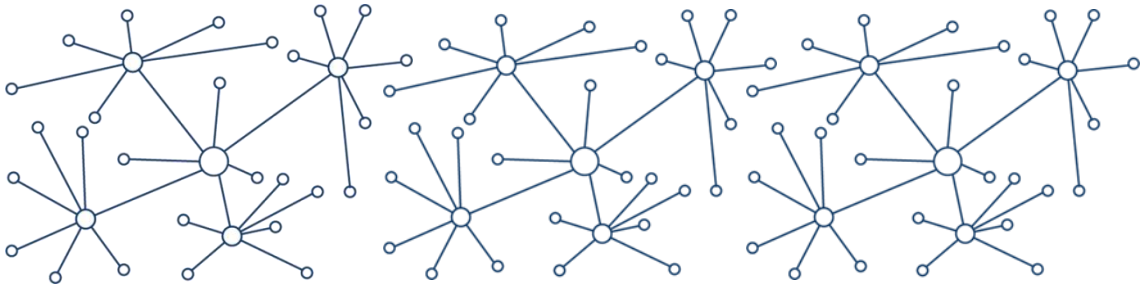
1. Understand blockchain architecture and requisite crypto foundations
2. Understand various consensus protocols and their usage for specific applications
3. Understand and Resolve security concerns in blockchain
4. Explore blockchain advances, use cases and upcoming platforms
5. Learn to write smart contracts
6. Solve problems and create solutions..

Instructor(s)

- Disciplines/Departments/Compartments?? (**NEP**)
- Boundary-less, Flexible, Autonomous education ecosystem
- Instructors (Fall 2022) –
  - Dr Dhiren Patel (2 hrs/week)
  - Himanshu (TA) (1 hr/week)
  - Visiting faculty (on-line/on-campus)
  - Dr Mahesh Shirole (VJTI Mumbai)
  - Dr Yann Busnel (IMT Atlantique Rennes France),
  - Jay Bothra (HSBC London)
  - Mugdha Bhagwat (Morgan Stanley)
  - Sanket Shah (VJTI Mumbai), …. And more

Thank you

for your attention



Blockchain Technology

Core Elective 3 – CS423

B. Tech. IV CSE 7th Sem

Lecture#3 and 4 (2 Aug 2022)

Dr. Dhiren Patel

Bitcoin

- Bitcoin enabled an innovative platform for peer to peer transfer of value without any central authority
- By implementing software programs for validation, verification, consensus in the blockchain
- Recording the transaction in an immutable distributed ledger
- Establishing trust among unknown peers
- BTC price on 17 March 2020 – USD 4.9 k
- BTC price mid-April 2021 – USD 64 k !!!!
- BTC price – USD 31.7 k (19 July 2021)
- BTC price – USD 22.7k (today)

21,075.30 USD

-18,413.40 (46.63%) past year

27 Jul, 3:59 am UTC · Disclaimer

1D | 5D | 1M | 6M | YTD | 1Y | 5Y | Max

Bitcoin price – historical

BTC price – Fall 2021 lecture (ATH – April 2021 USD 64k)

Bitcoin (July 2020)!
(Fall 2020 first lecture)

Why Crypto price fluctuates?

- India Banknote Demonetization (2016)
- Donald Trump's election as President (2016)
- Elon Musk (Tesla BTC investment (Jan 2021), Doge meme coin tweet (Jan 2021))
- Colonial Pipeline Attack (May 2021) and Recovery of Ransom BTC by FBI
- China crack down on Mining Farms (June 2021)
- Mining as a business (abstract view)

Altcoins are generally defined as all cryptocurrencies other than Bitcoin (BTC).

Altcoins

- best-known cryptocurrency Bitcoin – BTC (max. supply 21 M)
- And a selected number of alternative cryptocurrencies known as “Altcoins” (coins that are an alternative to Bitcoin)
- Altcoins that are built using Bitcoin’s original open-source protocol (e.g. Litecoin – LTC, max. supply 84 M)
- //The Litecoin Network aims to process a block every 2.5 minutes, rather than Bitcoin's 10 minutes. This allows Litecoin to confirm transactions much faster than Bitcoin.
- Altcoins that are not based on Bitcoin’s open-source protocol, but that have their own protocol and distributed ledger. (e.g. Ethereum – ETH max. supply – unlimited!, Ripple – XRP max. supply 100 B)
- //**Ethereum** is a decentralized, open-source blockchain with smart contract functionality

Market Cap = Current Price x Circulating Supply (July 2021)

Market cap of BTC ~600 B USD

Circulating supply = 18,759,981 BTC

April 2021 – market cap ~ 1.2 Trillion USD

Why?

BTC - Store of Value – digital gold //Universal currency?

Market cap of Eth ~223 B USD

Ethereum Eth- Utility token

Market cap of BNB ~ 52 B USD

BNB – exchange token used for payment of fees (trading)

Market cap of UNI ~ 10 B USD

UNI – DeFi (landing protocol – governance token)

BAT – (Basic Attention Token)…. digital advertisement industry

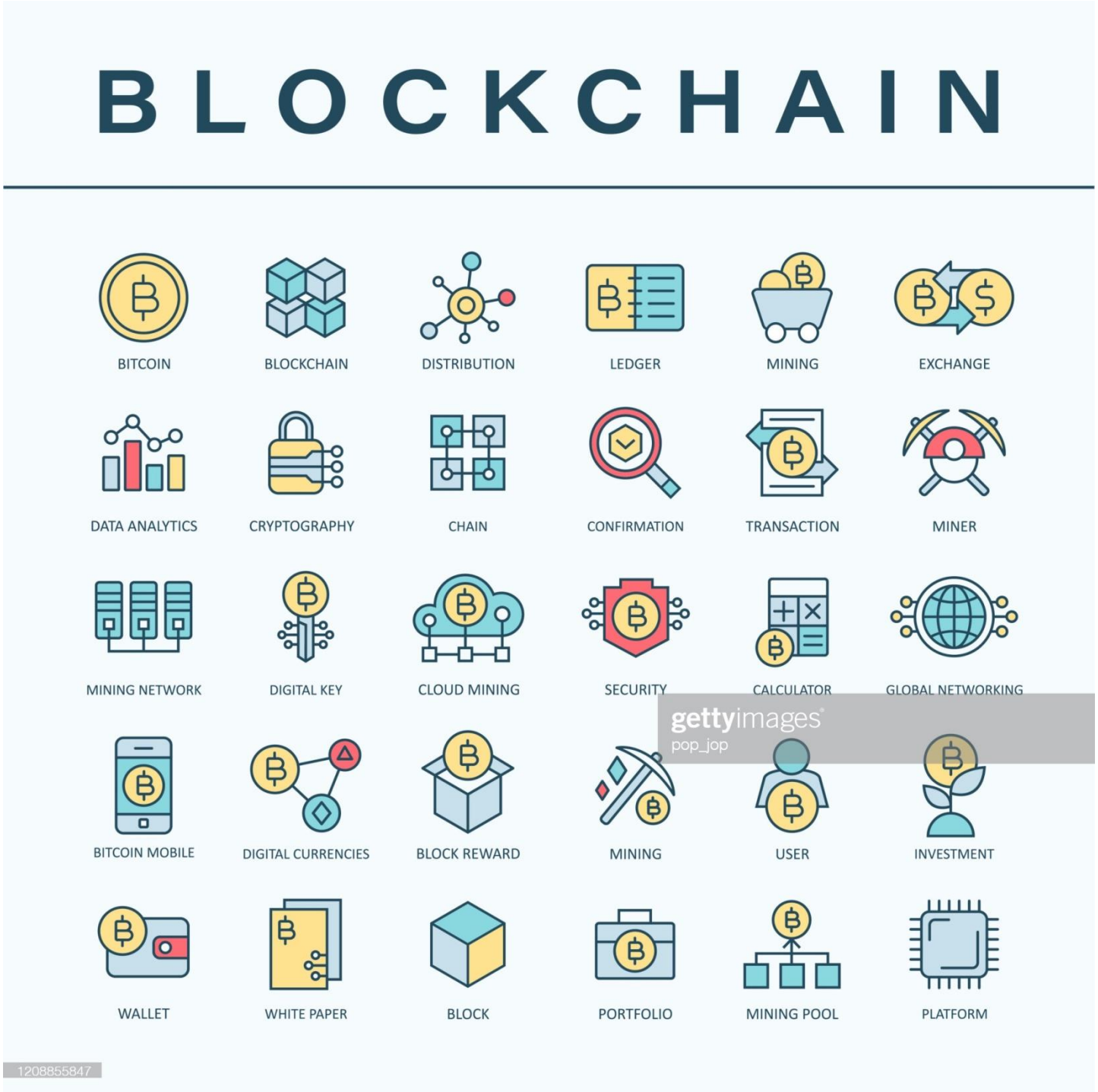
CHIA token - XCH (Proofs of Space and Time - Storage as a Service)….

Why Crypto price fluctuates?

- El Salvador declaring BTC as a legal tender (Sept 2021)
- Wars (US force leaving Afghanistan (Aug 2021), Russian Invasion in Ukraine (Feb 2022)) ….
- Political resistance (old school) across the world ….
- Market movers (Eth2.0, DeFi, NFTs, Gaming and Metaverse, CBDC etc.)

Blockchain Technology (domain, keywords and symbols)

- Cryptocurrency (coins, addresses, wallets and exchanges)
- Transactions, Blocks, Hash function, Public Key Cryptography
- Remittance, Payment system(?), Stable coins,
- Mining, Consensus, Burning, Governance, Fees
- Smart contracts
- Tokenization and Virtual assets
- Supply-chain, Value-chain, Circular economy
- Scalability (Main chain, Side chain, Para chains..)

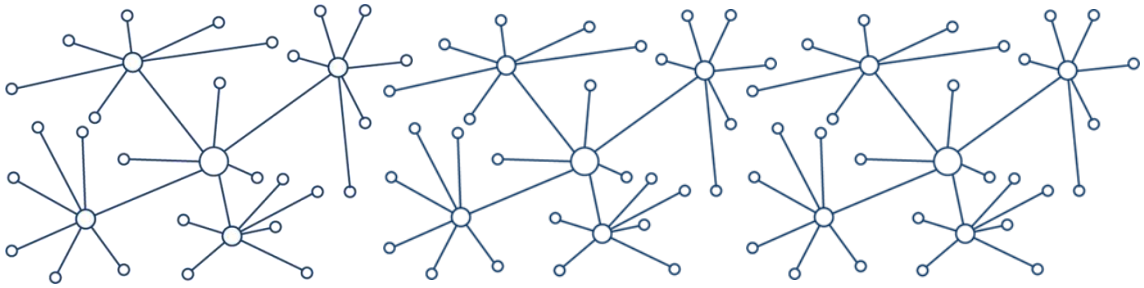

BLOCKCHAIN
BITCOIN
BLOCKCHAIN
DISTRIBUTION
LEDGER
MINING
EXCHANGE
DATA ANALYTICS
CRYPTOGRAPHY
CHAIN
CONFIRMATION
TRANSACTION
MINER
MINING NETWORK
DIGITAL KEY
CLOUD MINING
SECURITY
CALCULATOR
GLOBAL NETWORKING
BITCOIN MOBILE
DIGITAL CURRENCIES
BLOCK REWARD
MINING
USER
INVESTMENT
WALLET
WHITE PAPER
BLOCK
PORTFOLIO
MINING POOL
PLATFORM
gettyimages
pop_jop
1208855847

Pre-test (scheduled at 11:30 AM)

- Google classroom
- Test Link
- Participation is important

Blockchain – visualization – hands on

- https://andersbrownworth.com/blockchain/distributed



Blockchain Technology

Core Elective 3 – CS423

B. Tech. IV CSE 7th Sem

Lecture#5 and 6 (16 Aug 2022)

Dr. Dhiren Patel

Blockchain - visualization

- https://andersbrownworth.com/blockchain/distributed

Blockchain Technology

- Bitcoin components (max. supply 21 M)
- Hash function SHA256
- Puzzle to solve (making x leading bits of block hash to 0)
- Difficulty adjustment (auto – approx. every 2 weeks (time it took to find the last 2,016 blocks) to keep av. time between blocks to 10 min)
- Elliptic curve crypto - Secp256k1 is the name of the elliptic curve used by Bitcoin to implement its public key cryptography (wallets)

Why Crypto price fluctuates?

- Bitcoin halving !!!! (happened on an av. every 4 years so far – reward reduced from 50 BTC → 25 BTC → 12.5 BTC → 6.25 BTC) //last halving happened in May 11, 2020
- Miners runaway when rewards cut into half and mining bill (electricity to run computers to solve puzzle) doesn't fall!!
- El Salvador declaring BTC as a legal tender (Sept 2021)
- Wars (US force leaving Afghanistan (Aug 2021), Russian Invasion in Ukraine (Feb 2022)) ….
- Political resistance (old school) across the world ….
- Market movers (Eth2.0, DeFi, NFTs, Gaming and Metaverse, CBDC etc.)

Cryptocurrency (Wikipedia)

- It is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure transactions, control the creation of units, and verify the transfer of assets
- encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds
- It uses decentralized control as opposed to centralized currency and central banking systems
- (normal (fiat) currency example – exchange, storage, ownership, value, purchase power, trust, production, interoperability..)
- The decentralized control of each cryptocurrency works through DLT, typically a blockchain, that serves as a public financial transaction database (coinbase??)

Money Reimagined (Afghanistan context)

Money Reimagined (Afghanistan context)

Bitcoin could play a very important role (Aug 2021)

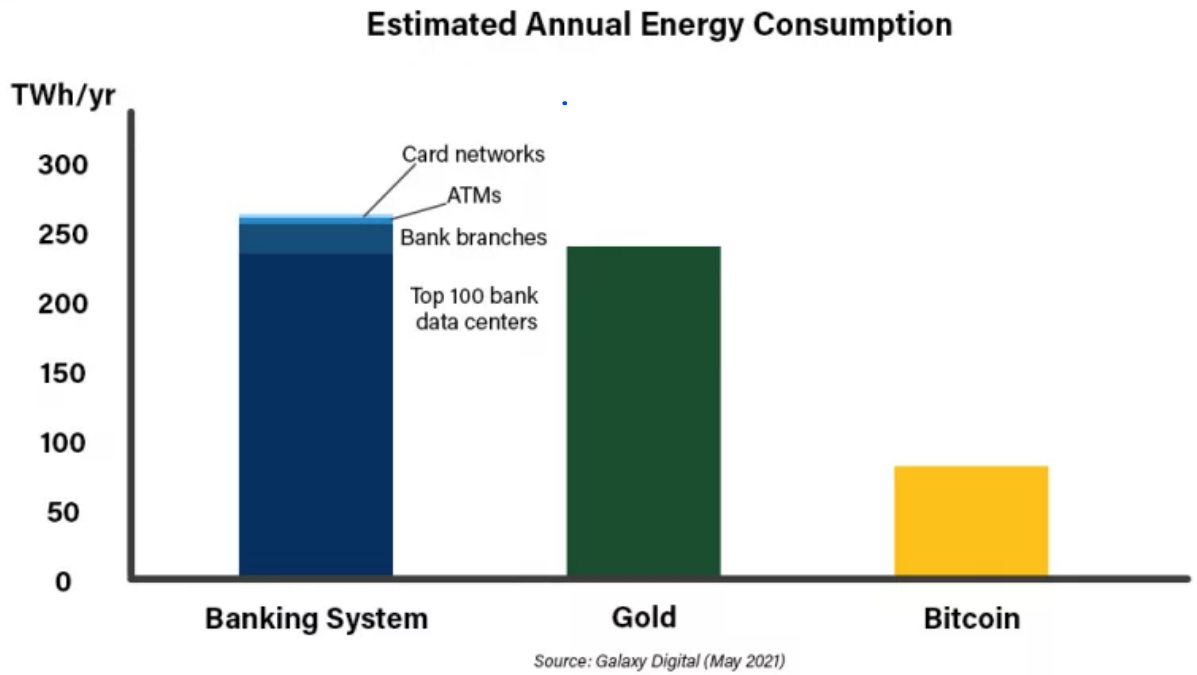
- If Afghans must embark on an arduous and dangerous escape, at least with cryptocurrency they would have a better way to transfer whatever wealth they have across borders.
- In decades past, refugees from war-torn areas would deal with this problem by sewing pieces of gold into the hems of their clothes, running the risk of having them stolen by common thieves or corrupt officials.
- Now, they can simply load up a bitcoin address that's personally accessible anywhere in the world.
- digital literacy and computer education, laying a knowledge foundation upon which bitcoin can now be deployed to bypass the failing legacy system

How Much Energy Does Bitcoin Use?

- Bitcoin uses less than half the energy the banking system consumes, according to recent data.
- Bitcoin's energy usage depends on how many miners are operating on its network at any given time. These miners must compete against each other to win the right to add the next block to the blockchain and earn rewards. The competitive structure results in a lot of wasted energy as only one miner can add a new block every 10 minutes.
- At its present level (Aug 2021), Bitcoin consumes 81.51 terawatt hours (TWh) annually.

Banking system energy consumption

- when you take into account the sheer number of physical branches, printing facilities, ATMs, data centers, card machines and secure transport vehicles required to support the fiat currency system.

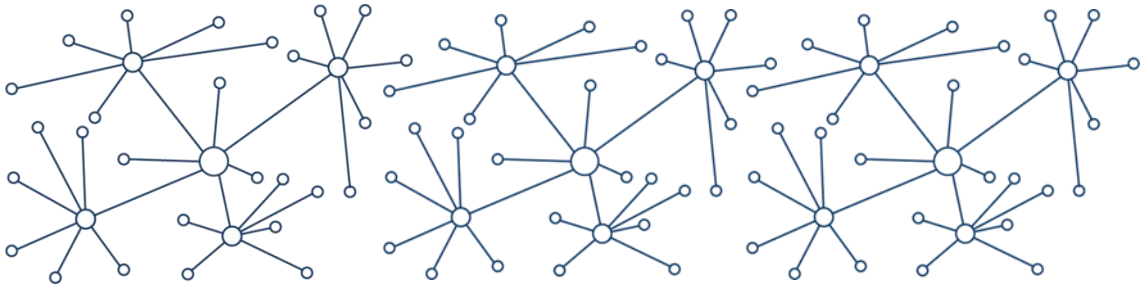


Old → New

- You hand banknotes to the baker or the butcher or the barber, she gives you a bread or a brisket or a buzzcut. No third party gets to second-guess or overrule your choices.
- As commerce moves online, more and more transactions are funnelled through ever-more-powerful intermediaries.
- It would be cheaper for both buyer and seller if the middleman is eliminated from the process

Censorship

- the centralized infrastructure between the buyer and seller, always comes with some sort of fee for the upkeep of the infra[structure] and for the business building and maintaining it to operate.
- the veto power of intermediaries becomes a problem when they block innocuous transactions
- Bitcoin restored censorship resistance to payments in the digital realm



Blockchain Technology

CS423

B. Tech. IV CSE 7th Sem

Lecture#9 and 10 (6 Sept 2022)

Background – Mining and Trust

Dr. Dhiren Patel

Bitcoin Blockchain

- Bitcoin components (max. supply 21 M)
- Hash function SHA256
- Puzzle to solve (making x leading bits of block hash to 0)
- Difficulty adjustment (auto – approx. every 2 weeks (time it took to find the last 2,016 blocks) to keep av. time between blocks to 10 min)
- Elliptic curve crypto - Secp256k1 is the name of the elliptic curve used by Bitcoin to implement its public key cryptography (wallets)

Blockheader in Bitcoin Block

Size	Field	Description
4 bytes	Version	The Bitcoin Version Number
32 bytes	Previous Block Hash	The previous block header hash
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block's transactions
4 bytes	Timestamp	The timestamp of the block in UNIX.
4 bytes	Difficulty Target	The difficulty target for the block.
4 bytes	Nonce	The counter used by miners to generate a correct hash.

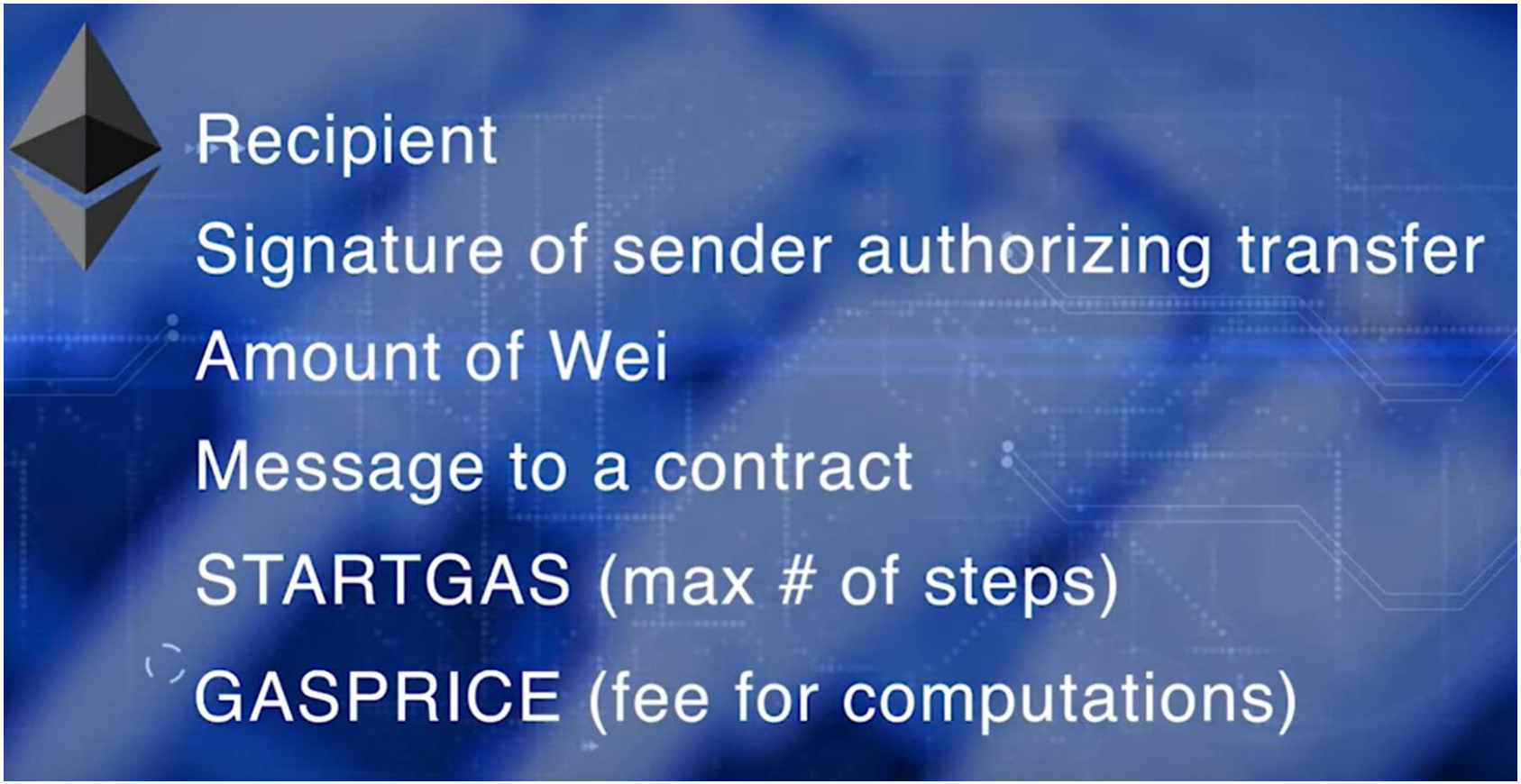
Encryption in Bitcoin Blockchain

- Two techniques are predominantly used for securing the chain and for efficient validation and verification.
- Hashing and asymmetric key encryption (PKC)
- Public-key cryptography, secure hashing, transaction integrity, and block integrity

Ethereum Structure

- Bitcoin blocking state was defined in terms of unspent transaction outputs UTXOs and a reference implementation of the Wallet application
- Ethereum formally introduce the concept of an account as a part of the protocol.
- The account is the originator and the target of a transaction. A transaction directly updates the account balances as opposed to maintaining the state such as in the bitcoin UTXOs.
- It allows for transmit of value and messages and data between the accounts that may result in the state transitions.
- These transfers are implemented using transactions.

Eth transaction



Observe (Ethereum Explorer)

- transaction hash, height of the chain,
- timestamp, from and to accounts,
- value transport, gas limit,
- gas used, transaction receipt,
- success in this case and nonce.

Externally Owned Accounts and Contract Accounts

- There are two types of accounts,
- Externally Owned Accounts and Contract Accounts.
- Externally Owned Accounts or EOA are controlled by private keys.
- Contract Accounts or CA are controlled by the code and can be activated only by an EOA.
- An externally owned account is needed to participate in the Ethereum network.
- It interacts with the blockchain using transactions.
- A Contract Account represents a smart contract.
- Every account has a coin balance.

Ether and Wei

- Both types of transaction require fees.
- An account must have sufficient balance to meet the fees needed for the transactions activated.
- Fees are paid in Wei. Wei is a lower denomination of Ether.
- One Ether 10 to the power of 18 Weis.
- A transaction in Ethereum includes the recipient of the message, digital signature of the sender authorizing the transfer, amount of Wei to transfer, an optional data field or payload that contains a message to a contract,
- STARTGAS which is a value representing the maximum number of computational steps the transaction is allowed.
- Gas price a value representing the fee sender is willing to pay for the computations.

Ethereum Node

- an Ethereum node is a computational system representing a business entity or an individual participant.
- An Ethereum full node hosts the software needed for transaction initiation, validation, mining, block creation, smart contract execution and the Ethereum Virtual Machine (EVM).

Smart Contract Execution

- When the target address in a transaction is a smart contract, the execution code corresponding to the smart contract is activated and executed on the EVM.
- The input needed for this execution is extracted from the payload field of the transaction.
- Current state of the smart contract is the values of the variables defined in it.
- The state of the smart contract may be updated by this execution.
- Results of this execution is told in the receipts.

Benefits of Smart Contract

- Trust between two entities involved in the transaction
- Your documents are encrypted on a shared ledger. There's no way that someone can say they lost it.
- Backup
- Imagine if your bank lost your savings account. On the blockchain, each and every one of your friends have your back. Your documents are duplicated many times over.

Smart Contracts are not Perfect

- What if bugs get in the code? Or how should governments regulate such contracts? Or, how would governments tax these smart contract transactions?
- Smart contracts are not reversible, meaning that if there is a problem with the contract, it can be difficult or impossible to fix.

Validation

- Transaction validation involves checking the time-stamp and the nonce combination to be valid and the availability of sufficient fees for execution.
- Miner nodes in the network receive, verify, gather and execute transactions.
- The in-work smart contract code are executed by all miners.
- Validated transactions are broadcast and gathered for block creation.

Mining

- mining is the process used to secure the network by validating the computations, collecting them to form a block, verifying them, and broadcasting it
- The proof of work puzzle winner, miner that creates a new block, is incentivized with the base fees of three Ethers, and the transaction fees in Ethereum blockchain. (Eth2 – base fees is removed/reduced).

Mining

- A trustless and distributed consensus system means that if you want to send and/or receive money from someone you don't need to trust in third-party services.
- Mining serves as two purposes:
- To verify the legitimacy of a transaction by avoiding the so-called double-spending;
- To create new digital currencies by rewarding miners for performing the previous task.

Mining

- From a technical point of view, the mining process is an operation of inverse hashing: it determines a number (nonce), so the cryptographic hash algorithm of block data results in less than a given threshold.
- This threshold, called difficulty, is what determines the competitive nature of mining

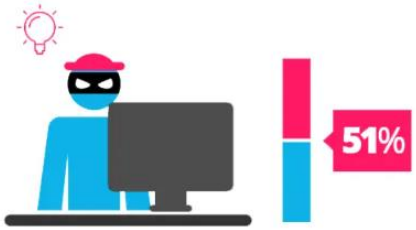
PoW v/s PoS

- In POW, the miners solve cryptographically hard puzzles by using their computational resources.
- In POS, instead of miners, there are validators. The validators lock up some of their Ether as a stake in the ecosystem. Following that, the validators bet on the blocks that they feel will be added next to the chain. When the block gets added, the validators get a block reward in proportion to their stake.
- ethereum community wants to exploit the proof of stake method for a more greener and cheaper distributed form of consensus.

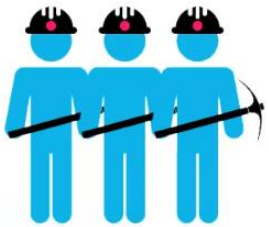
solution to minimize the use of expensive resources spent on mining using proof of work

Proof of Work vs. Proof of Stake

To add each block to the chain, miners must compete to solve a difficult puzzle using their computers processing power.



In order to add a malicious block, you'd have to have a computer more powerful than 51% of the network.



The first miner to solve the puzzle is given a reward for their work.

There is no competition as the block creator is chosen by an algorithm based on the user's stake.

In order to add a malicious block, you'd have to own 51% of all the cryptocurrency on the network.

There is no reward for making a block, so the block creator takes a transaction fee.

PoW v/s PoS

- Using a Proof-of-Work system, bad actors are cut out thanks to technological and economic disincentives.
- programming an attack to a PoW network is very expensive, and you would need more money than you can be able to steal
- the Casper protocol, a bad validator might lose their deposit. (use the set some circumstances)

What? Why?

- blockchains decentralized network participants, are not necessarily known to each other.
- Credentials cannot be checked by the conventional means such as verifying who you are with your driver's license.
- Participants can join and leave the chain as they wish.
- They operate beyond the boundaries of trust.

What? Why?

- Given this context: how do you identify the peer participants?
- How do you authorize and authenticate the transactions?
- How do you detect forged or faulty transactions?
- Private public key pair and hashing are important foundational concepts in decentralized networks that operate beyond trust boundaries.

Hashing

- What is hashing? A hash function or hashing transforms and maps an arbitrary length of input data value to a unique fixed length value.
- Input data can be a document, tree data, or a block data.
- Even a slight difference in the input data would produce a totally different hash output value.

Hashing

- The algorithm chosen for the hash function should be a one-way function and it should be collision free, or exhibit extremely low probability of collision.
- The first requirement is to make certain that no one can derive the original items hashed from the hash value.
- Can you make potatoes out of mashed potatoes?
- The second requirement is to make sure that the hash value uniquely represents the original items hashed.

Hashing

- Odds of a meteor hitting your house is higher than generating two of the same hash values of 256 bits when applying this algorithm!!
- Tree structure helps the efficiency of repeated operations, such as transaction modification and the state changes from one block to the next.
- Log N versus N.


In Ethereum, hashing is used to generate:
Account Addresses
Digital Signatures
Transaction Hash
State Hash
Receipt Hash

Transaction Integrity

- To manage the integrity of a transaction we need number one, secure a unique account address.
- We need a standard approach to uniquely identify the participants in the decentralized network.
- Number two, authorization of the transaction by the sender through digital signing.
- And number three, verification that the content of that transaction is not modified. We use a combination of hashing and public key cryptography.

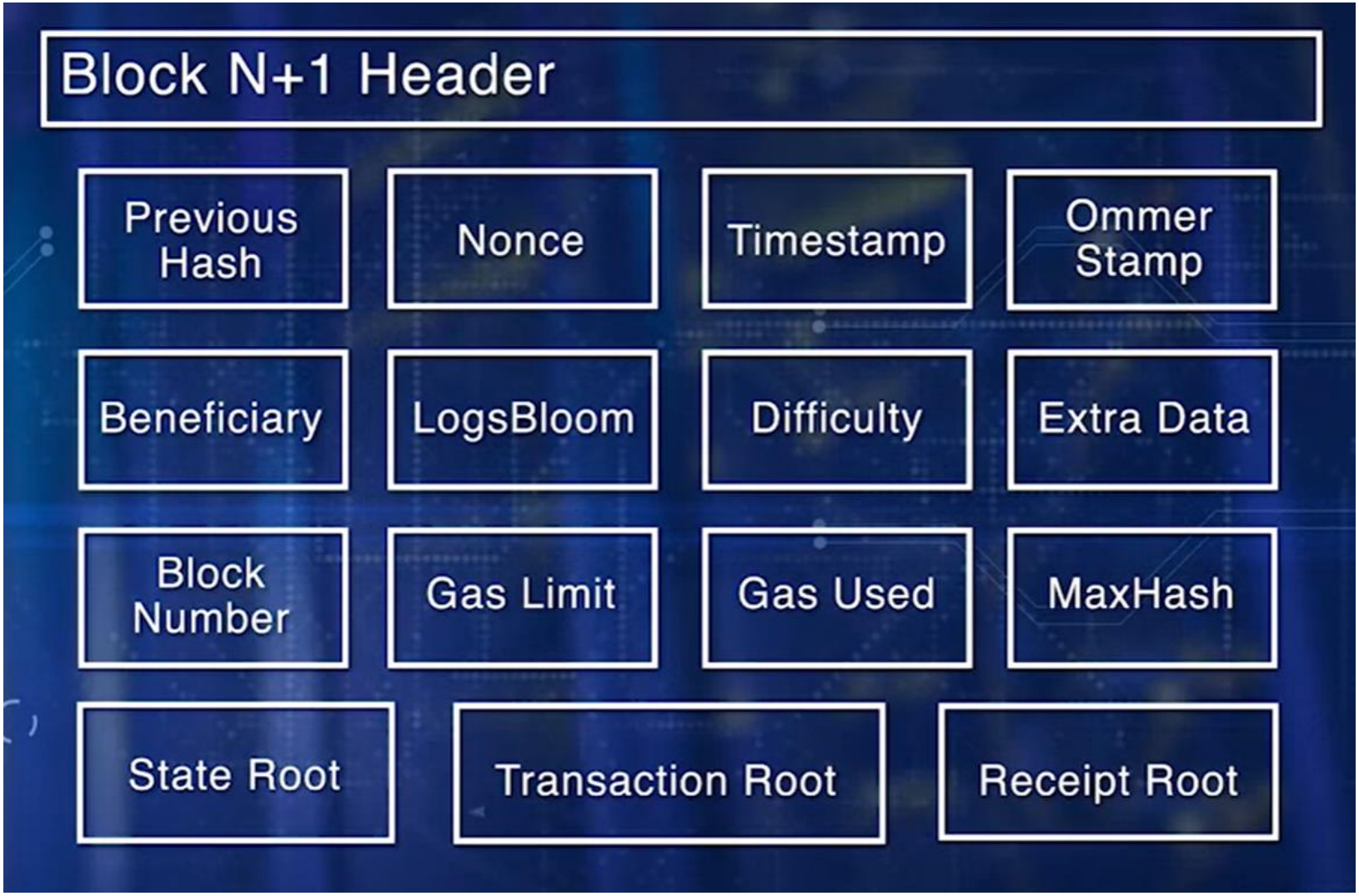
Address of Accounts

- Addresses of accounts are generated using public key, private key pair.
- Step 1, at 256-bit random number is generated, and designated as the private key.
- Kept secure and locked using a passphrase.
- Step 2, an ECC algorithm is applied to the private key, to get a unique public key.
- This is the private public key pair.
- Step 3. Then a hashing function is applied to the public key to obtain account address.
- The address is shorter in size, only 20 bytes or 160 bits.

Non-repudiable

- A transaction for transferring assets will have to be authorized, it has to be non-repudiable, and unmodifiable.
- Step number 1, find the hash of the data fields of the transaction.
- Step number 2, encrypt that hash using the private key of the participant originating the transaction.
- Thus, digitally signing the transaction to authorize and making the transaction non-repudiable.
- Step number 3, this hash just added to the transaction.
- It can be verified by others by decryiptng it using the public key of the sender of the transaction, and recomputing the hash of the transaction.
- Then, compare the computed hash, and the hash received at the digital signature.
- If that is a match, accept the transaction. Otherwise, reject it.

Ethereum Block



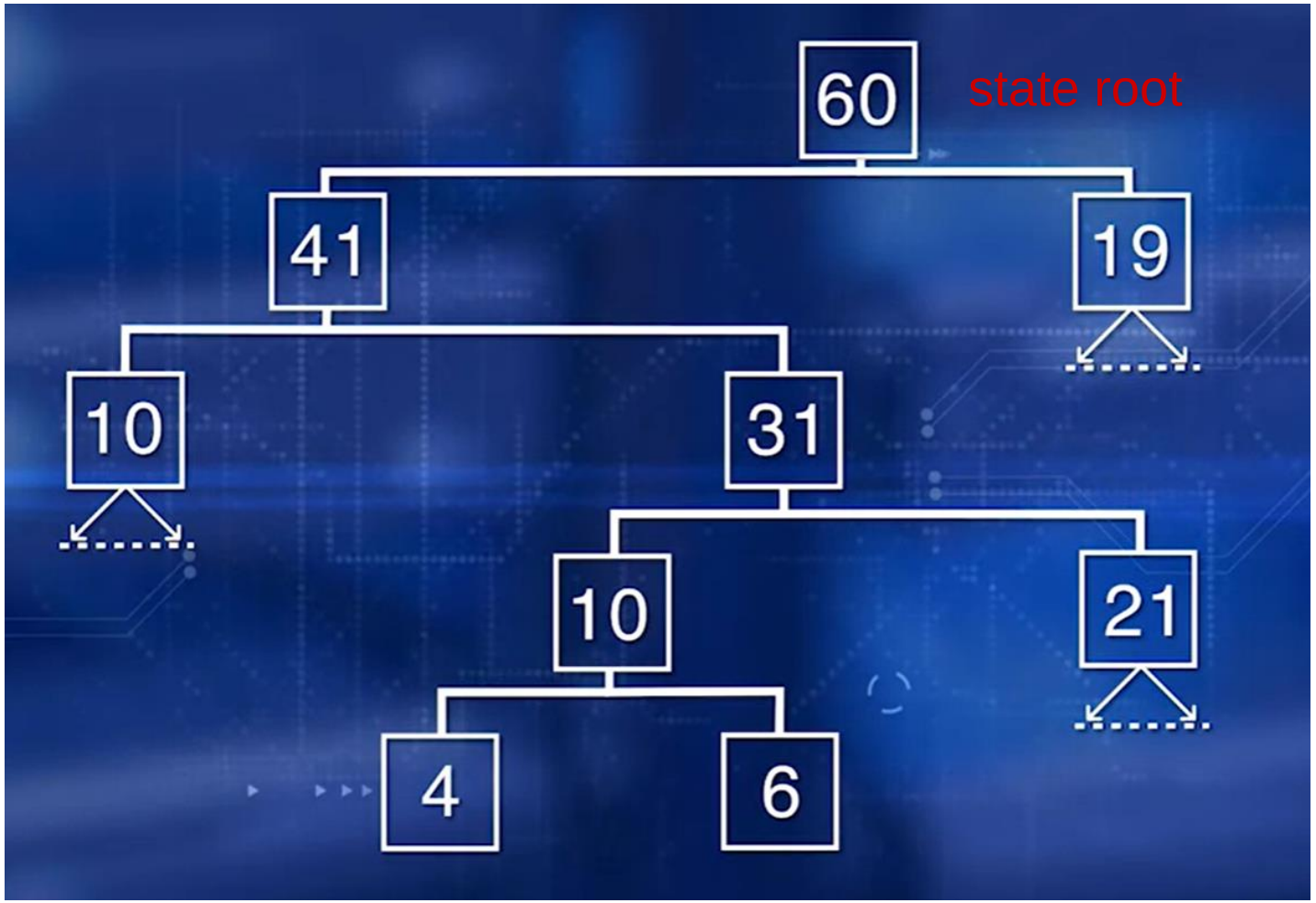
Securing Blockchain

- Integrity of the block is managed by assuring that the block header contents are not tampered with, the transactions are not tempered with, state transitions are efficiently computed, hashed, and verified.
- In Ethereum, the block hash is (the block) of all the elements in the block header, including the transaction root and state root hashes.
- It is computed by applying a variant of SHA-3 algorithm called Keccak and all the items of the block header.

Merkle Tree

- A typical block has about 2,000 transactions in bitcoin and about 100 transaction Ethereum
- Hashes of transaction in a block are processed in a tree structure called Merkle tree hash.
- Merkle tree hash is also used for computing the state root hash, since only the hash of the chained states from block to block have to be re-computed.
- It is also used for receipt hash root.
- The advantage over flat versus tree representation.
- If any transaction is to be verified, only one path to the tree has to be checked. You don't have to go through the entire set of transactions.

Merkle Tree

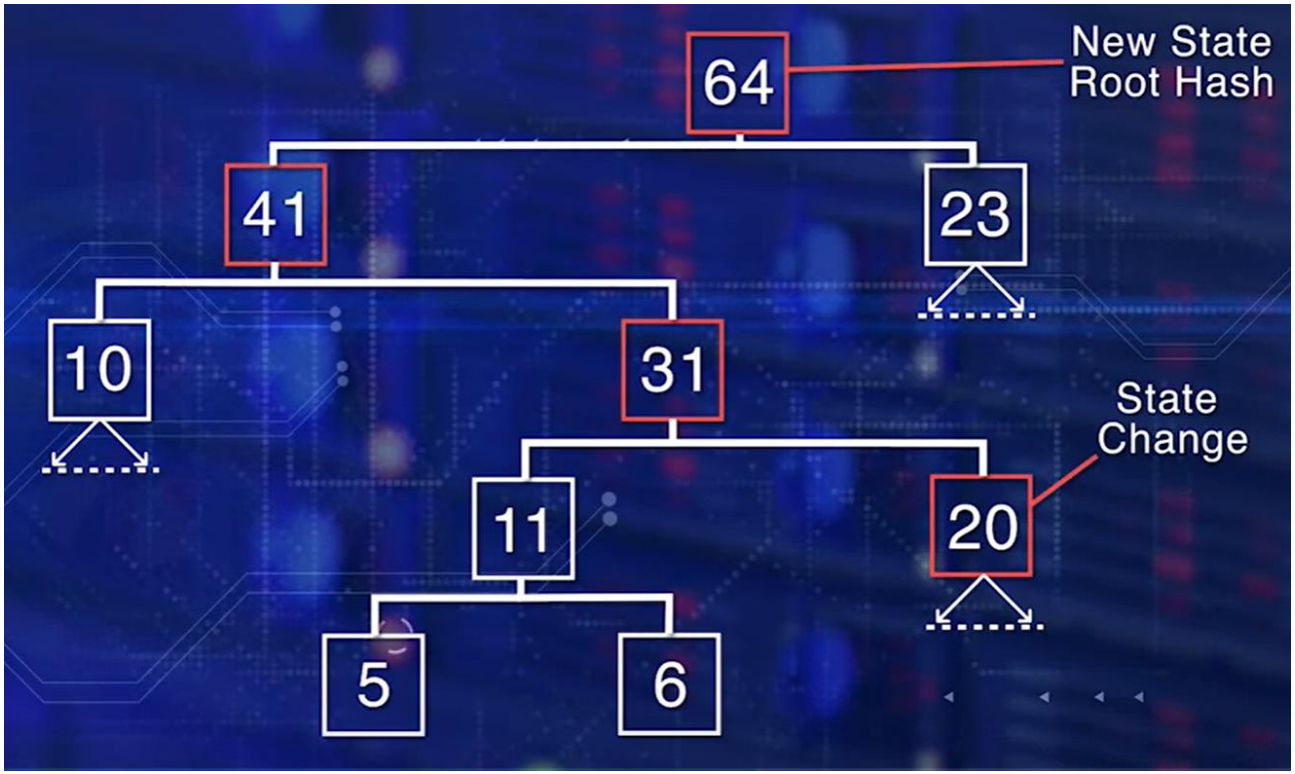


Immutability of Eth Chain

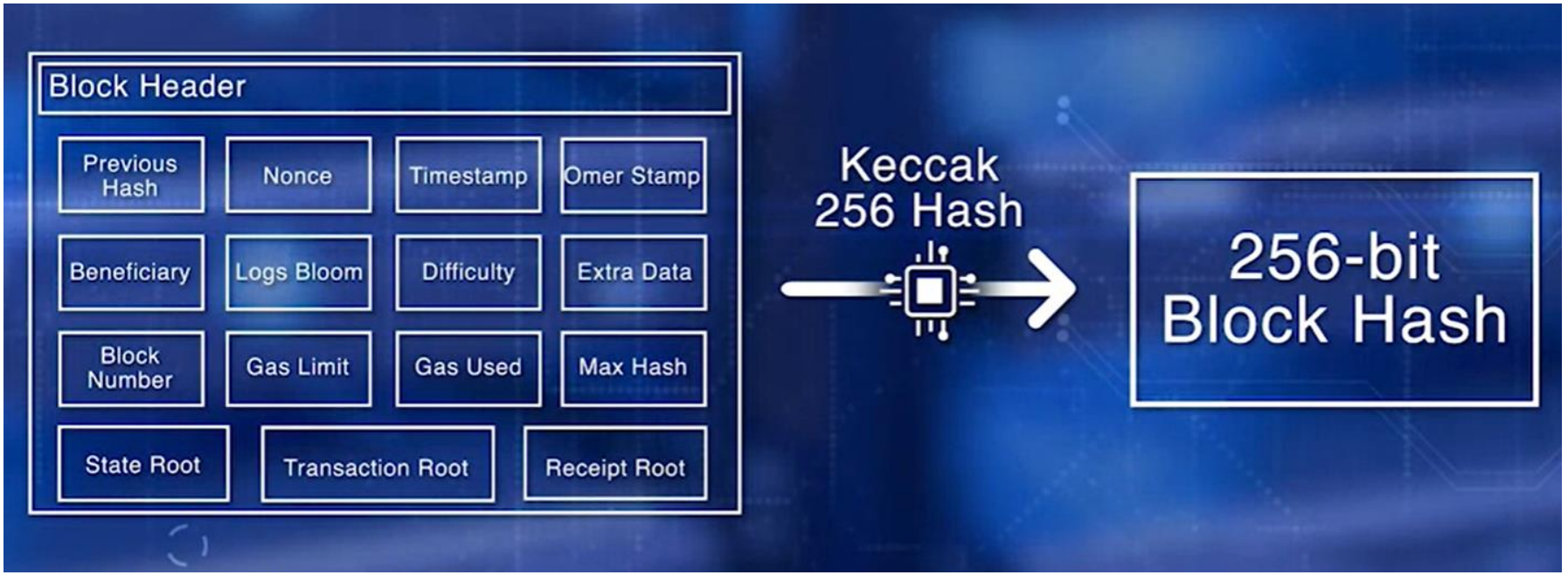
- Block hash serves two important purposes; verification of the integrity of the block and the transactions, formation of the chain link by embedding the previous block hash in the current block header.
- If any participant node tampers with the block, it's hash value changes resulting in the mismatch of the hash values and rendering the local chain of the node in an invalid state.
- Any future blocks initiated by the node would be rejected by other miners due to hash mismatch.
- This enforces the immutability of the chain.

Re-computation

- Every state change requires state root (hash) re-computation



Re-computation, and update



Decentralized Autonomous Organization (DAO)

- The DAO is a leaderless, virtual organization built within a smart contract on the Ethereum blockchain.
- This smart contract sets rules that provide the ability for participants to vote on which ventures would be funded using the Ether (a crypto currency similar to Bitcoin) that each participant contributes to during the creation of the DAO.
- The larger the contribution, the larger the number of votes each participant has.

Blockchain breaches

- blockchain is inherently secure because its principles are founded on cryptography and immutability (i.e., information can be permanently stored on a public ledger without being tampered with).
- But despite its strengths and promise, blockchain is not inherently secure, and even a small oversight can have a significant impact

Trust (Centralized)

- Say, you want to fly out of the Mumbai airport.
- Entry check (only passengers (flyers) with valid tkt and travel document (passport) can enter)
- Check-in Baggage screening (of valid tkt holders)
- Airline counter check-in
- Document verification (of passengers – passport, visa) and boarding pass issue
- Immigration, Border control (passport stamping, visa, support – destination requirements)
- Security check-in (frisking and hand bag screening)
- Boarding Gate security and Aircraft Entry security
- Passenger list to destination (background check)

Trust (decentralized)???

- The airport authority would have pre-established a secure environment for people to arrive and depart.
- This establishes the base trust.
- Then there is additional trust once you - enter and your passport and travel documents are verified, validated, and your baggage is screened.
- Even more trust in you is established when the airline staff checks your boarding pass at the gate and you enter the aircraft to fly.
- < There is nobody checking your credentials and certifying that you are trustworthy. Then, how do you do it?>

Decentralized Trust

- Similar to our airport scenario, trust in a decentralized blockchain is also about securing, validating, verifying, and making sure resources needed for transaction execution are available.
- This is accomplished by securing the chain using specific protocols, validating the transaction and blocks for tamper proofing, verifying the availability of resources for transactions, and executing and confirming the transactions.

Trust

- The Trust Trail is defined by these operations: validate transaction, verify gas and resources, gather transactions, execute transaction to get a new state, form the block, work towards consensus, finalize the block by the bidder, and everyone add the block to their chain and confirm the transactions.

Forks

- debate around whether the network should permit the ability to rewrite history through a “hard fork”
- In that case - the rules of the network would have been bent for a particular scenario and would have set a dangerous precedent for the future
- blockchain is there to stay and hence its adoption will increase, secure implementation is the key!!

Security and Risk management

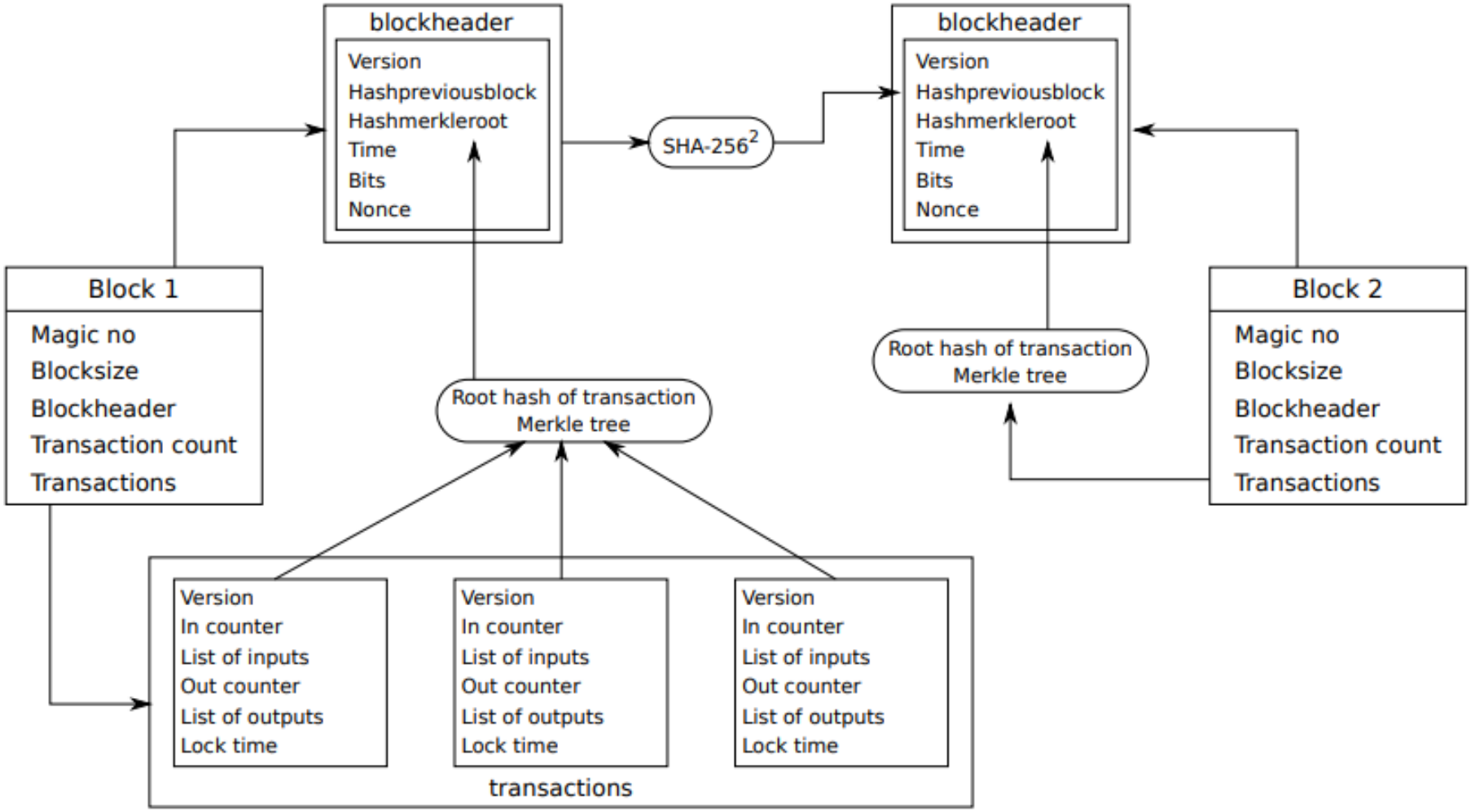
- Poor implementation — inadequate testing creates vulnerabilities in the software code.
- Unauthorized access — inappropriate access to private keys or blockchain related software could be used to steal funds or information.
- Identity management — personally identifiable information may be stolen or a node impersonated to obtain access to a blockchain.

Ethereum check

- The syntax, the transaction signature, time stamp, nonce, gas limit, and sender account balance are validated before execution.
- The fuel, or gas points, and other resources available for smart contract execution, are also validated.
- Transaction signatures and hash are also verified.
- <check - execute transactions>
- Merkle tree hash of the validated transactions is computed.
- This is in Ethereum. This is the transaction root of the block header.
- All miners execute the transaction for either transfer, as well as for execution of smart contracts.
- The state resulting from transaction execution are used in computing the Merkle tree hash of the states, the state root of the block header.
- The receipt root of the block header is also computed.

Blockchain (definition)

- Nakamoto (2008) describes the blockchain as a database modeled by a linear sequence of blocks, each one containing cryptographic hashes corresponding to the previous and current block to ensure continuity and immutability


blockheader
Version
Hashpreviousblock
Hashmerkleroot
Time
Bits
Nonce
SHA-256²
blockheader
Version
Hashpreviousblock
Hashmerkleroot
Time
Bits
Nonce
Block 1
Magic no
Blocksize
Blockheader
Transaction count
Transactions
Root hash of transaction
Merkle tree
Root hash of transaction
Merkle tree
Block 2
Magic no
Blocksize
Blockheader
Transaction count
Transactions
Version
In counter
List of inputs
Out counter
List of outputs
Lock time
Version
In counter
List of inputs
Out counter
List of outputs
Lock time
Version
In counter
List of inputs
Out counter
List of outputs
Lock time
transactions

Why Blockchain and DLT?

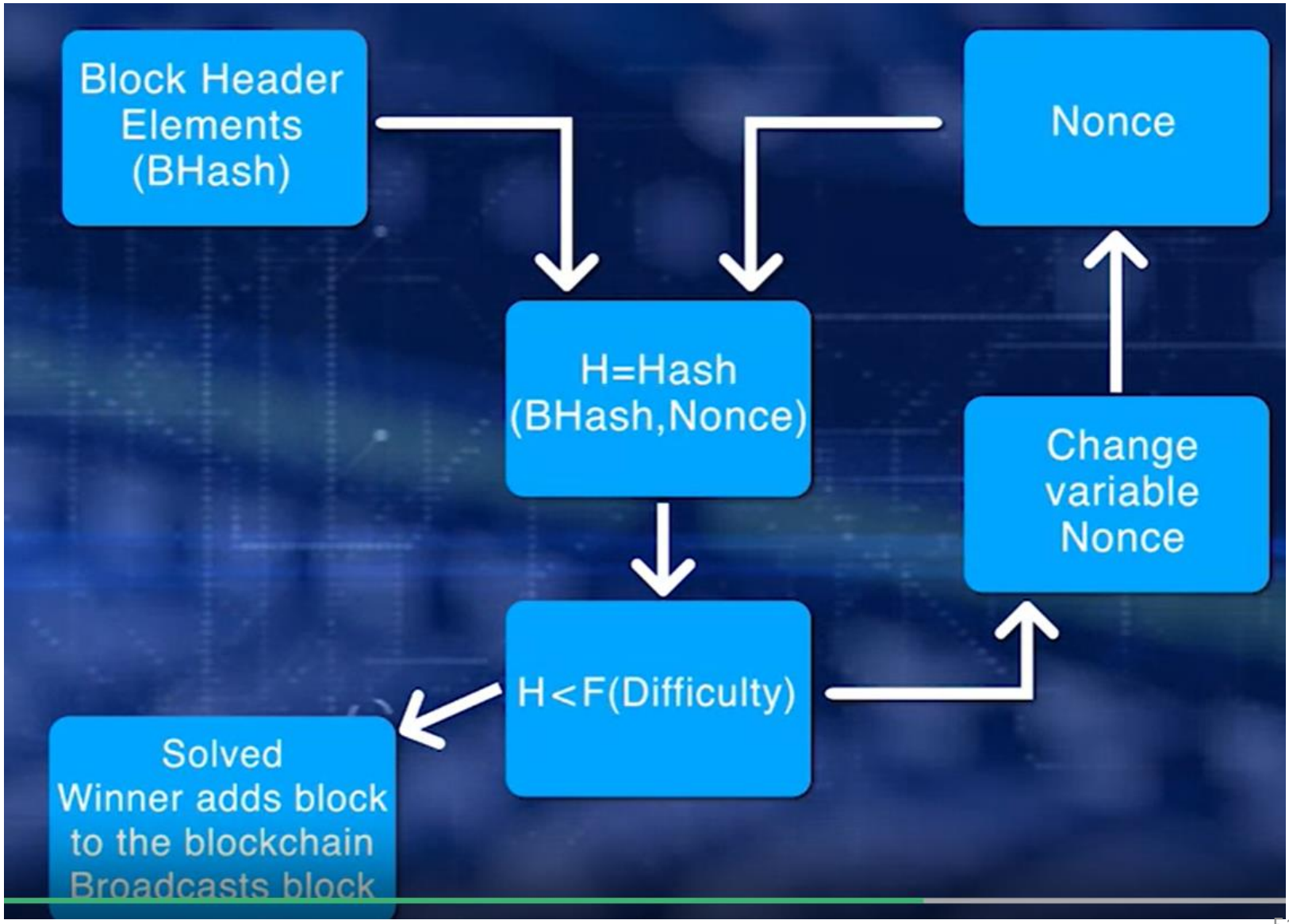
- ledger technologies could save banks $15–20 billion a year by reducing regulatory, settlement and cross-border costs (2017-2022)
- Speed and efficiency are not the only qualities that make distributed ledgers attractive to banks. ‘Regulators will like that blockchain-based transactions can achieve greater transparency and traceability– an “immutable audit trail”.

Consensus Protocol

- A secure chain is a single main chain with a consistent state.
- Every valid block added to this chain, adds to the trust level of the chain.
- What if everyone wants to add their candidate block to the chain?
- Each of the candidate blocks is by a competing miner.
- Which is the next block to be added to the chain?
- Can they agree on the next block?
- Is there a method or a protocol to choose the next block?

Proof of Work (PoW) – BTC and ETH

- Proof of Work uses hashing
- First, compute the hash of the block header elements that is a fixed value, and a nonce that is a variable.
- If hash value is less than 2^128 for bitcoin, and less than function of difficulty for ethereum, the puzzle has been solved.
- If it has not been solved, repeat the process after changing the nonce value.
- If the puzzle has been solved, broadcast the winning block that will be verified by other miners.
- Non-winning miner nodes add the new block to the local copy of the chain, and move on to working on the next block.
- The winner gets an incentive for creating the block.


Block Header Elements (BHash)
Nonce
H=Hash (BHash,Nonce)
Change variable Nonce
H<F(Difficulty)
Solved
Winner adds block to the blockchain
Broadcasts block

Trust and Robustness

- Trust is about executing regular operations correctly and managing exception satisfactory.
- Robustness is the ability to satisfactorily manage exceptional situations.

Double spending

- what if more than one miner solves the consensus puzzle where it close in time to each other?
- What if more than one transaction references as input the same digital asset?
- There's a possibility that digital currency and other consumables are single used digital assets, can be intentionally or inadvertently reused in transactions.
- This situation is called double spending.

Handling exceptions

- In a decentralized network, like a blockchain, there is no intermediary.
- We need a policy and an automatic deterministic way to handle this situation.
- A policy for handling transaction and double spending in Bitcoin is to allow the first transaction that reference the digital asset and reject the rest of the transaction that reference the same digital asset.
- There should be a well-defined processes for handling exception improve trust in the blockchain

Double spending handle solutions
Mining
Timestamp: The confirmed transactions are timestamped, therefore they are irreversible. If a transaction is involved with a bitcoin it is verified and done. But in the future, if other transactions are made with the same bitcoin, the transactions will be canceled.

Fork

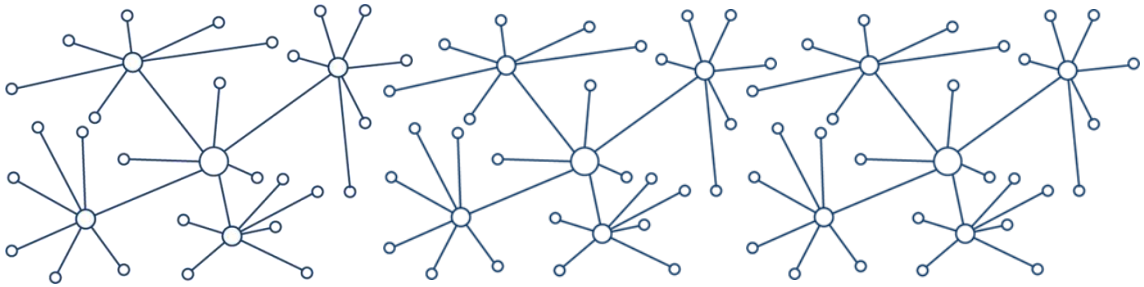
- Background - a minor perturbation in the chain - is handled as a naturally expected occurrence within the block chain.
- On the other hand, occasionally, a minor process adjustment has to be carried out typically by bootstrapping a new software to the already running processes.
- This is soft fork. (sort of - the release of software patches)

Hard fork

- Hard fork implies a major change in the protocol.
- (sort of – a new version of operating system)
- Forks are mechanisms that add to the robustness of the blockchain framework.
- Well-managed forks help build credibility in the blockchain by providing approaches to manage unexpected faults and planned improvements.

Forks

- A **Soft Fork** is a fork where updated versions of the protocol are backwards compatible with previous versions.
- A **Hard Fork** is a change of the protocol that is not backwards compatible with older versions of the client. Participants would absolutely need to upgrade their software in order to recognize new blocks.



Blockchain Technology

Core Elective 3 – CS423

B. Tech. IV CSE 7th Sem

Lecture#7 and 8 (30 Aug 2022)

Ethereum

Dr. Dhiren Patel

SOFT FORK

minor change in the protocol.

backwards compatible

Upgraded versions can interact with previous versions

minor process adjustment has to be carried out typically by bootstrapping a new software to the already running processes

HARD FORK

major change in the protocol.

not backwards compatible

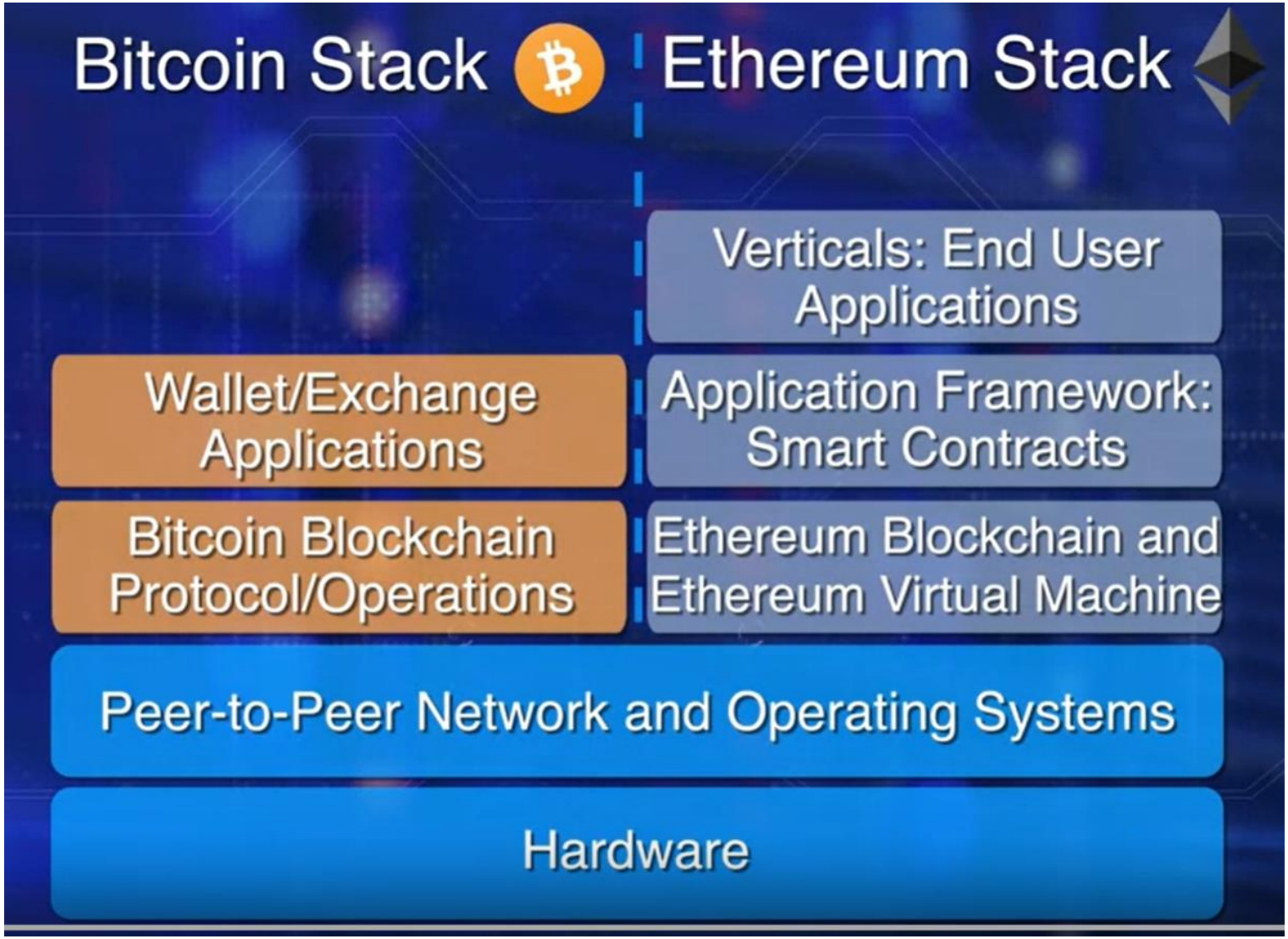
Upgraded versions cannot interact with previous versions

Participants would absolutely need to upgrade their software in order to recognize new blocks.

Ethereum

- Bitcoin blockchain is the mother of all blockchains. (2009)
- It was intended for peer to peer transfer of value and it does that well. ((Digital currency transfer request simple addition and subtraction)
- Around 2013, a framework for code execution was introduced by Ethereum Founders.
- The centerpiece and thrust of this Ethereum blockchain is a smart contract.

Comparison –
Bitcoin v/s Ethereum Blockchain



Smart contracts

- Ethereum supports smart contracts and of virtual machine on which smart contracts execute.
- Smart contracts in turn enable decentralized application that accomplish more than a transfer of value.
- E.g. Efficient automation of decentralized application such as supply chain.

Objectives

- Smart contracts
- Ethereum blockchain protocol – elements and operations
- Concept of gas - the fuel or the payment model for code execution and the incentive model for the Ethereum blockchain.

Smart contract

- A smart contract is a piece of code deployed in the blockchain node.
- Execution of a smart contract is initiated by a message embedded in the transaction.
- Ethereum enables transaction that may carry out more sophisticated operations.
- For example, a transaction could require a conditional transfer,
- it may require some evaluation,
- it may need more than one signature for transfer of assets,
- or it may involve waiting for a specific time or date.

Smart contract

- Structurally, a smart contract resembles a class definition in an object oriented design.
- It has data, functions or methods with modifiers public or private,
- along with getter and set of functions.
- Specific programming languages have been designed for coding smart contracts.
- Solidity is one such language.

Smart contract example

- An auction bidding smart contract could execute this logic -
- If the age of a bidder is greater than 18 and the bid is greater than the minimum bid,
- then, accept the bid,
- or else reject the bid.

Ethereum Virtual Machine

- Every node in Ethereum network should be able to execute the code irrespective of that underlying type of hardware or operating system.
- Enter Ethereum Virtual Machine, EVM.
- An EVM provides a run anywhere abstraction layer for the contract code.
- A smart contract written a high level programming language is translated into EVM byte code, and then, deployed on the Ethereum Virtual Machine, EVM.

Smart contracts

- smart contracts add a layer of logic and computation to the trust infrastructure supported by the blockchain.
- Smart contracts allow for execution of code.
- The code for this smart contract is written in a high level language like Solidity and compiled into byte code.
- The code for the smart contracts is executed on a special structure known as Ethereum Virtual Machine.

What are Smart Contracts?

- A smart contract is a self-executing digital agreement that enables two or more parties to exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the need for a third party.

Smart contract

- With smart contracts, you drop a bitcoin or ether into the vending machine (i.e. ledger), and your escrow, deed, contract, goods, driver's licence, or whatever the contract is for, simply drops into your account.
- The smart contract does all the work to determine whether the conditions of the order were satisfied.
- Smart contracts both define the rules and penalties around an agreement in the same way that a traditional contract does, and also automatically enforces those obligations.

Smart contract

- Smart contracts are verified, executed, and enforced by a computer program that runs on a blockchain network. When both parties involved in the smart contract agree to its terms, the program will automatically execute.
- This eliminates the need for a third party, as the contract is verified and enforced by the blockchain network.
- Because smart contracts are executed by code rather than people, they remove the possibility of human error and can automate many tasks that would traditionally require human interaction.

Smart contract

- In a smart contract approach, an asset or currency is transferred into a program and the program runs this code and at some point it automatically validates a condition and it automatically determines whether the asset should go to one person or back to the other person, or whether it should be immediately refunded to the person who sent it or some combination thereof.
- the decentralized ledger also stores and replicates the document which gives it a certain security and immutability

DeFi

- Decentralized finance is an exit from traditional banking services and norms.
- Smart contracts in DeFi are facilitating the exchange of goods, services, data, funds and so on. Users of centralized financial institutions, such as banks and credit unions, rely on intermediaries to execute a transaction. Whereas, DApps are using smart contracts to ensure that each action is genuine, transparent, and free of human error.

Non Fungible Token

NFTs

- the Market cap of NFTs is closing in at a whopping $40.9 billion in 2021 as they turned out to be the most successful use-case of smart contracts.
- A smart contract is a tool that allows implementing a sale agreement between the NFT owner and the buyer. The smart contract contains information on the NFT, such as the work's creator, other parties who are entitled to royalties each time the NFT is sold, and the work's ownership history.

NFTs

- The majority of NFTs are not recorded on the blockchain since keeping so much data on the blockchain is both costly and energy intensive.
- As a result, smart contracts frequently include a link to the work they represent, which can be viewed by only the owner.

Supply Chain

- “UPS can execute contracts that say, ‘If I receive cash on delivery at this location in a developing, emerging market, then this other [product], many, many links up the supply chain, will trigger a supplier creating a new item since the existing item was just delivered in that developing market.’”
- supply chains are hampered by paper-based systems, where forms have to pass through numerous channels for approval, which increases exposure to loss and fraud. The blockchain nullifies this by providing a secure, accessible digital version to all parties on the chain and automates tasks and payment.

Autonomous cars

- One example is the self-autonomous or self-parking vehicles, where smart contracts could put into play a sort of ‘oracle’ that could detect who was at fault in a crash; the sensor or the driver, as well as countless other variables.
- Using smart contracts, an automobile insurance company could charge rates differently based on where, and under which, conditions customers are operating their vehicles.

Real estate

- A decentralized solution can help cut your costs. All you do is pay via cryptocurrency and encode your contract on a smart contract.
- Everyone sees, and you accomplish automatic fulfilment.
- Brokers, real estate agents, hard money lenders, and anyone associated with the property game can profit.
- Smart contracts are revolutionary in terms of transforming the current real estate practices.

Real estate

- All the parties including the bank, the agent, and the mortgage lender can sign an agreement via smart contracts.
- Because transactions are kept on a blockchain, this shared ledger enables the parties involved to look over the process at any moment and from anywhere.

Autonomy (Benefits of Smart Contract)

- You're the one making the agreement; there's no need to rely on a broker, lawyer, or other intermediaries to confirm.
- Incidentally, this also knocks out the danger of manipulation by a third party, since execution is managed automatically by the network, rather than by one or more, possibly biased, individuals who may err.

Benefits of Smart Contract

- Trust
- Your documents are encrypted on a shared ledger. There's no way that someone can say they lost it.
- Backup
- Imagine if your bank lost your savings account. On the blockchain, each and every one of your friends have your back. Your documents are duplicated many times over.

Problems?

- Much like what happened with The DAO hack in 2016, a mere loophole in a smart contract resulted in the biggest heist of the crypto market.
- Had that loophole been addressed earlier, it could have been prevented.
- But here's the catch, because you can track every movement on a blockchain, the minute the stolen ether/ETH enters circulation, those behind the heist will be exposed. So all that stolen crypto is as good as nothing.

Human Errors and Bugs in programming

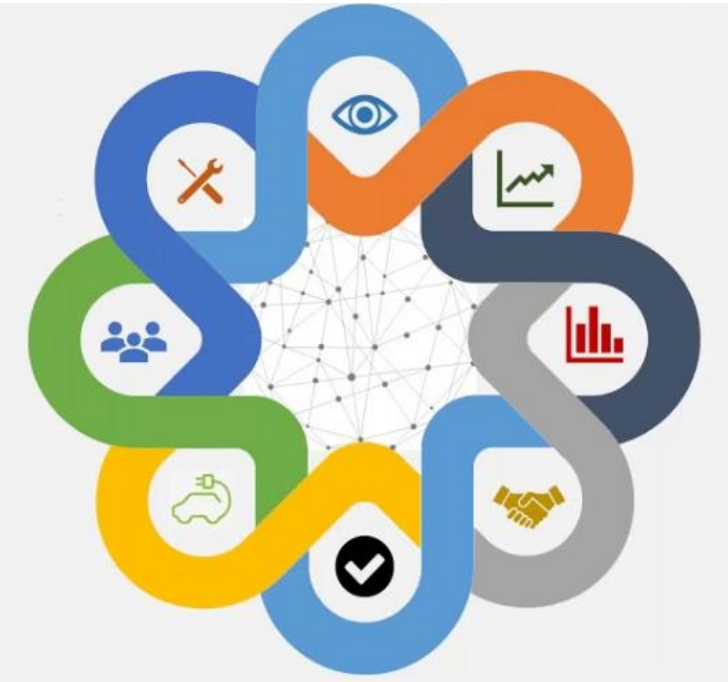
- A simple human-error in writing a smart contract compromised its safety. To prevent that, you will need the right developers who could write a fool-proof smart contract.
- Automated contracts are not only faster and cheaper but also avoid the errors that come from manually filling out heaps of forms

Smart Contracts are not Perfect

- What if bugs get in the code? Or how should governments regulate such contracts? Or, how would governments tax these smart contract transactions?
- Smart contracts are not reversible, meaning that if there is a problem with the contract, it can be difficult or impossible to fix.

Problems??

- Smart contracts theoretically can be subject to downtime and outages, although Ethereum has proven incredibly reliable, newer smart contract networks like Solana have experienced a few outages as the technology is still very much in development
- Smart contracts can be costly to develop and require a high level of technical expertise.
- Smart contracts are not always customizable, meaning that they may not be suitable for all businesses or transactions.



Blockchain use cases

(13 Sept 2022 – Tuesday)

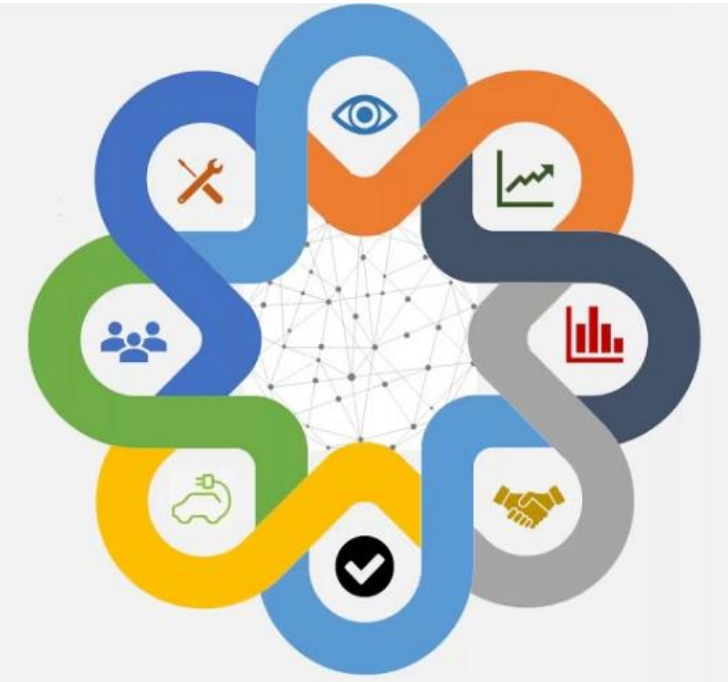
Dhiren Patel

Important properties and definitions

- Integrity - assuring the completeness and accuracy of data
- Authenticity - guaranteeing that a communication partner (a person or an IT component or application) is who he claims to be
- Availability - of services, applications, data - that users can always use them as intended
- Confidentiality - protection against unauthorised disclosure of information
- Anonymity - data or actions of the entity cannot be linked

Some Projects and Examples

- Completeness (E.g. System design – display temperature of a city – wait for all sensors' data, or min. k out of n sensors, or any one sensor, or sending previous result)
- Authenticity (E.g. Dog and monkey at other end of Internet??)
- Availability (E.g. Result Website crashing, internet during early days, email and VSAT at SVNIT)
- Complex system design (E.g. JOSAA admission portal)
- Anonymity (E.g. can you relate bitcoin (transaction) address to someone?) – home assignment!!



Blockchain use cases

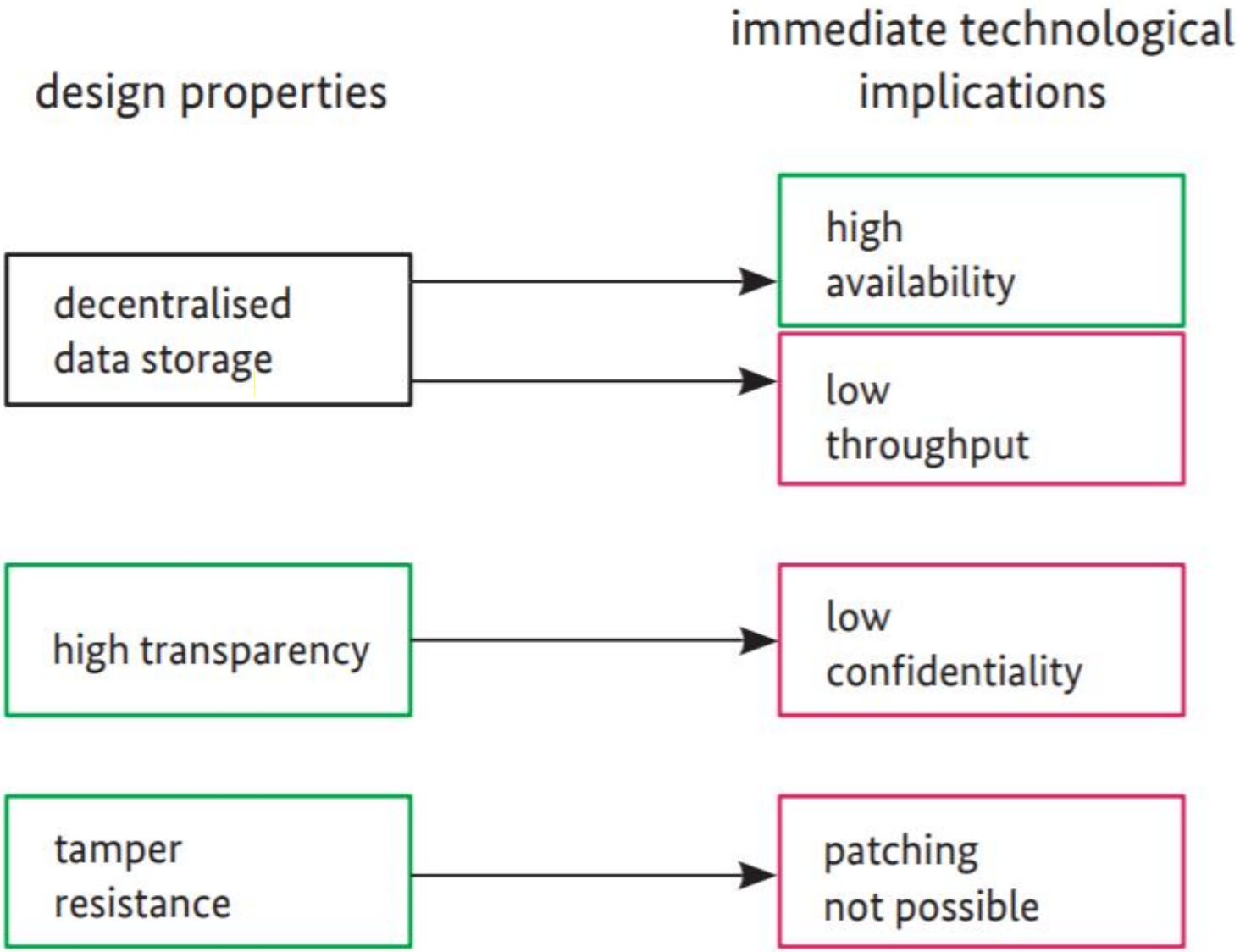
(20 Sept 2022)

Dhiren Patel

Important properties and definitions

- Integrity - assuring the completeness and accuracy of data
- Authenticity - guaranteeing that a communication partner (a person or an IT component or application) is who he claims to be
- Availability - of services, applications, data - that users can always use them as intended
- Confidentiality - protection against unauthorised disclosure of information
- Anonymity - data or actions of the entity cannot be linked

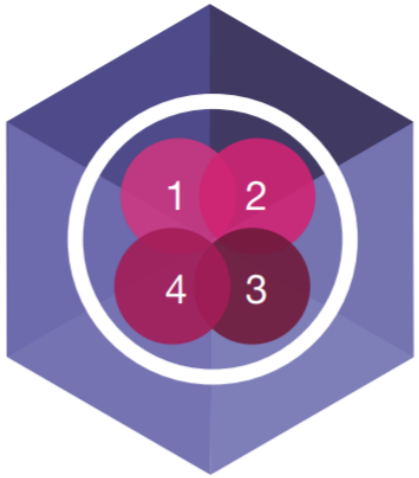
Blockchain USP



Blockchain (Built Businesses)

Improving contract management (legally enforceable smart contracts)

Enabling more transparency (in Supply Chains)



Enabling the infrastructure to combine circular economy (Building Information Management and IoT)

Tamper-proof exchange (of value and information)

Blockchain Use cases

Potential Blockchain Use Cases

Financial Institutions

- International payments
- Capital markets
- Trade finance
- Regulatory compliance & audit
- Anti-money laundering & know your customer
- Insurance
- Peer-to-peer transactions

Corporates

- Supply chain management
- Healthcare
- Real estate
- Media
- Energy

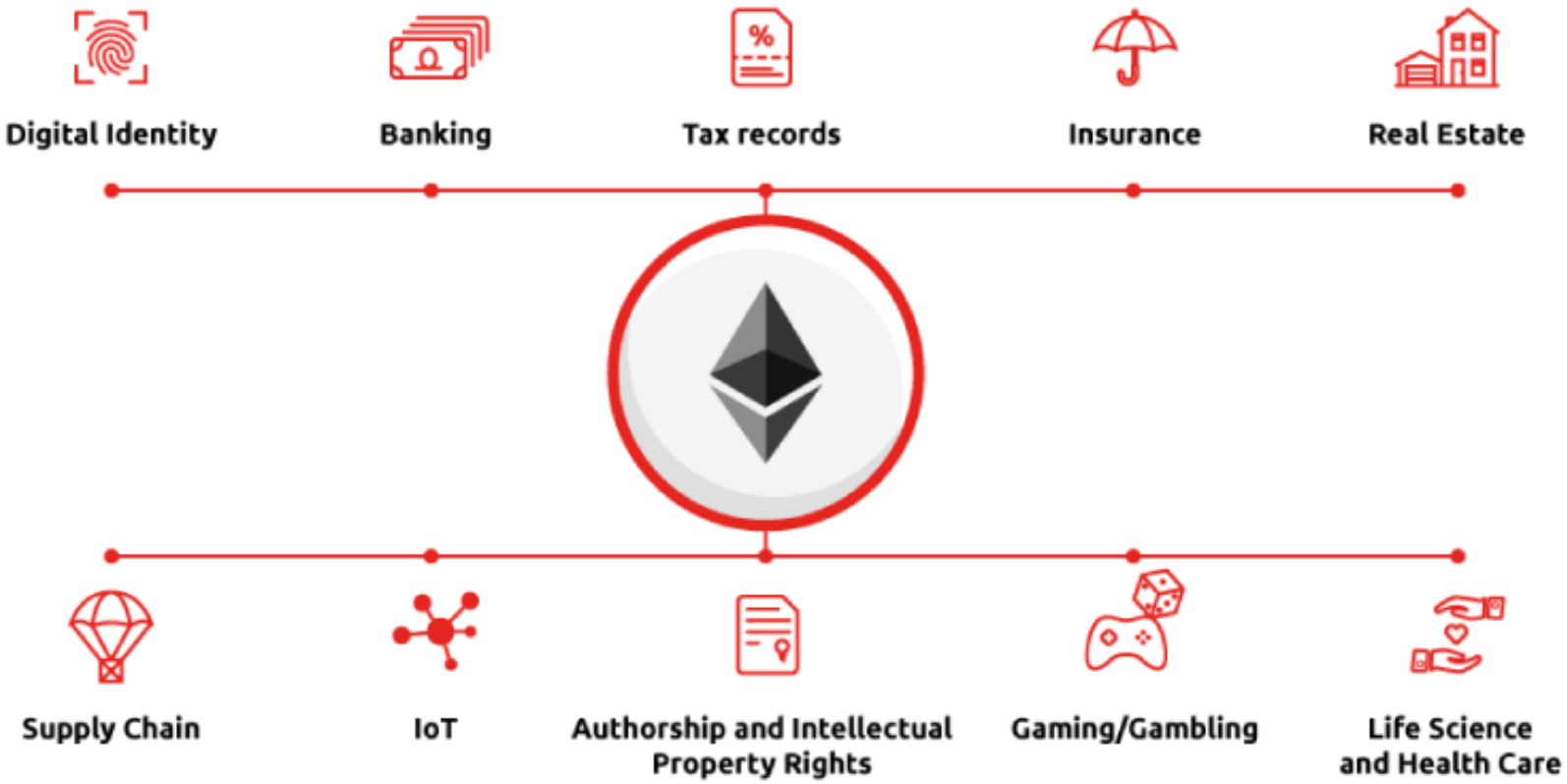
Governments

- Record management
- Identity management
- Voting
- Taxes
- Government & non-profit transparency
- Legislation, compliance & regulatory oversight

Cross-industry

- Financial management & accounting
- Shareholders' voting
- Record management
- Cybersecurity
- Big data
- Data storage
- Internet of Things

Blockchain Smart contracts: Use cases



Use Case: Supply Chain

- Global supply chains are inefficient, poorly tracked, and sometimes exploitative.
- E.g. Paperwork can account for substantial cost of container transport, and products are frequently mis-labeled.
- Create a shared IT infrastructure that streamlines workflows for stakeholders along the supply chain.
- Blockchain platform can facilitate accurate asset tracking, enable enhanced licensing of services, products, and software, and ultimately improves transparency into the provenance of consumer goods, from sourcing all the way to the point of consumption.

E.g. Farm to plate

- the scope is to provide producers, buyers, sellers, and consumers to come to one platform and promote food supply chain transparency
- Transform food supply chain system with Blockchain
- Consumers trust brands that offer 100% transparency on the food journey including product content, food safety process, allergens, and ingredients information.

Farm to Plate

- With all this information on a Blockchain, there is a stronger sense of accountability, transparency, and real-time access to trusted information.
- The information and data stored on **Farm to Plate** are immutable and thus can be trusted, which helps strengthen the quality management process of the produce

designed with Global Food Supply Chain Standards

- Participants can access relevant information that follows a global standard to assure food quality and provides consumers a complete overview of the food journey to enhance brand equity
- QR code scans at each transaction point are recorded on a blockchain that allows tracing locations and activities. Thus damage or spoilage occurrence is identified faster with accuracy.

Design using Hyperledger

- **Hyperledger Fabric** is a Blockchain platform that is best suited for building a permissioned network for enterprises – large, medium, and small
- Being open-source and vendor-neutral, it enables interoperability and easy integration for organizations with their existing or legacy environment.
- An added advantage is, it can be easily adopted by partners and stakeholders even if their technical environment is different from the enterprise adopting Farm to Plate. The web application used for Farm to Plate is **Hyperledger Explorer** which is open source, simple, powerful, and easy to use. **Hyperledger Explorer** allows for browsing activities on the underlying blockchain network.

Features

- Seamless onboarding
- Product registration with an XML file upload
- Easy transfer of dataTwo-factor authentication and authorization
- Identity and Access Management for role allocation
- Publicly accessible URL - through the QR code

Permissioned Blockchain

- Only authorized participants
- Participants are known and trusted
- Secured

Data on a need-to-know basis

- Data stored privately when needed
- Authenticity of data ensured
- Flexibility to determine which data to be private

Modular Architecture

- Plug and play mechanism
- Adherence to consensus protocols, certificate authorities, cryptographic protocols
- Easy integration

Multiple Language Support

- Supports Go, NodeJS, Java, Python
- Developers don't need to learn new languages
- Easy adoption

Open-source

- Available free - no additional cost to host on this platform
- Minimizes cost of adoption of Farm to Plate
- A strong community dedicated to improving performance daily

Deterministic Consensus Algorithm

- Accessibility of participant consensus
- Faster addition of the block to the ledger
- Elimination of bureaucracy

Technology Stack