INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Introduction to Blockchain

Dr. Ashok Kumar Das

IEEE Senior Member
Associate Professor
Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad
(Formerly **Indian Institute of Information Technology, Hyderabad**)

E-mail: *ashok.das@iiit.ac.in*
Homepage: http://www.iiit.ac.in/people/faculty/ashokkdas
Personal Homepage: https://sites.google.com/view/iitkgpakdas/

October 26, 2022

What is Blockchain?

- A blockchain is considered as a chain of blocks that are created from several blocks and it potentially consists of information.
- By the words “block” and “chain”, we actually specify in the context of digital information (“block”) which is stored in a public domain say database (“chain”).
- Since the digital information is stored in the form of “block” and it is linked in a “chain” form, the linked blocks constitute a chain, and hence, the name “blockchain”.
- The blockchain’s first block is known as the **Genesis block**.

What is Blockchain?

The reasons why the blockchain have gained so much admiration are that:

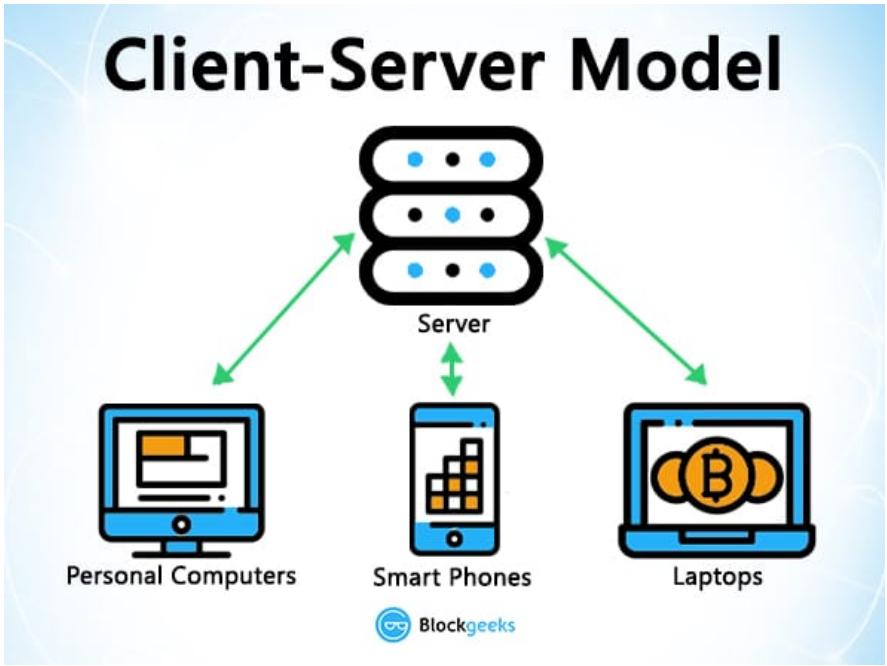
- It is not owned by a single entity, hence it is **decentralized**
- The data is **cryptographically** stored inside
- The blockchain is **immutable**, so no one can tamper with the data that is inside the blockchain
- The blockchain is **transparent** so one can track the data if they want to

Three Pillars of Blockchain Technology

- Decentralization
- Transparency
- Immutability

Pillar #1 : Decentralization

- Example of a centralized system is banks. They store all your money, and the only way that you can pay someone is by going through the bank.
- The traditional client-server model is a perfect example of this.
- When you google search for something, you send a query to the server who then gets back at you with the relevant information. That is simple client-server.



Pillar #1 : Decentralization

The centralized systems have treated us well for many years, however, they have several vulnerabilities.

- Firstly, because they are centralized, all the data is stored in one spot. This makes them easy target spots for potential hackers.
- If the centralized system was to go through a software upgrade, it would halt the entire system
- What if the centralized entity somehow shut down for whatever reason? That way nobody will be able to access the information that it possesses
- Worst case scenario, what if this entity gets corrupted and malicious? If that happens then all the data that is inside the blockchain will be compromised.

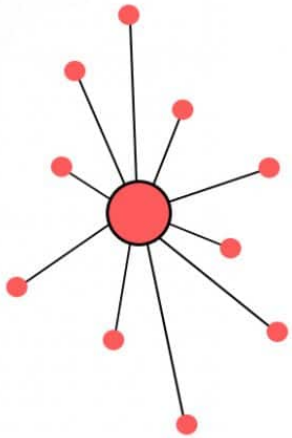
Pillar #1 : Decentralization

- In a decentralized system, the information is not stored by one single entity. In fact, everyone in the network owns the information.
- In a decentralized network, if you wanted to interact with your friend then you can do so directly without going through a third party.
- That was the main ideology behind Bitcoins. You and only you alone are in charge of your money. You can send your money to anyone you want without having to go through a bank.

Pillar #1 : Decentralization

The New Networks

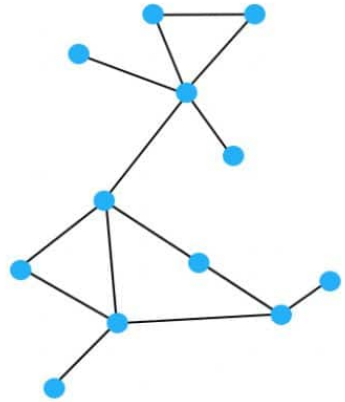
Centralized



Centralized systems have a core authority that dictates the truth to the other participants in the network.

Only priveleged users or institutions can access the history of transactions or confirm new transactions.

Decentralized



Decentralized systems have no core authority to dictate the truth to other participants in the network.

Every participant in the network can access the history of transactions or confirm new transactions.

Blockgeeks

Pillar #2 : Transparency

- While the person's real identity is secure, you will still see all the transactions that were done by their public address.
- This level of transparency has never existed before within a financial system.
- It adds that extra, and much needed, level of accountability which is required by some of these biggest institutions.

Pillar #3 : Immutability

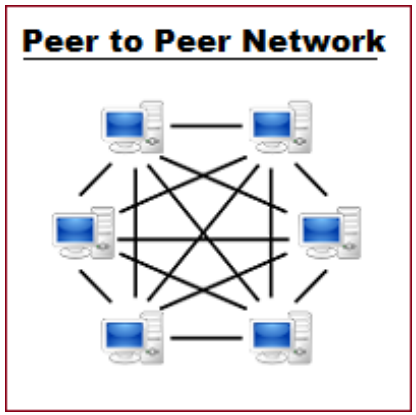
- Immutability, in the context of the blockchain, means that once something has been entered into the blockchain, it cannot be tampered with.
- The reason why the blockchain gets this property is that of cryptographic hash function.

INPUT	HASH
Hi	3639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome to blockgeeks. Glad to have you here.	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

INPUT	HASH
This is a test	C7BE1ED902FB8DD4D48997C6452F5D7E509FBCDBE2808B16BCF4EDCE4C07D14E
this is a test	2E99758548972A8E8822AD47FA1017FF72F06F3FF6A016851F45C398732BC50C

Maintaining the Blockchain – Network and Nodes

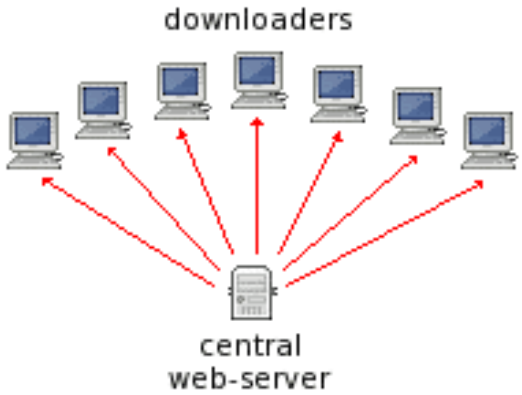
- The blockchain is maintained by a peer-to-peer (P2P) network.
- The network is a collection of nodes which are interconnected to one another.
- Nodes are individual computers which take in input and performs a function on them and gives an output.
- The blockchain uses a special kind of network called *peer-to-peer network* which partitions its entire workload between participants, who are all equally privileged, called *peers*.
- There is no longer one central server, now there are several distributed and decentralized peers.



Maintaining the Blockchain – Network and Nodes

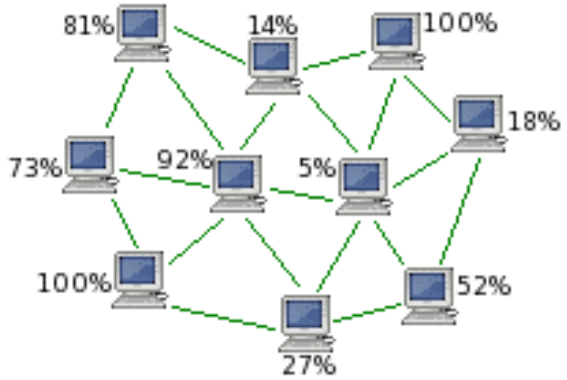
- One of the main uses of the peer-to-peer network is file sharing, also called torrenting.

Traditional Centralized Downloading



- Slow
- Single point of failure
- High bandwidth usage for server

Decentralized Peer-to-Peer Downloading

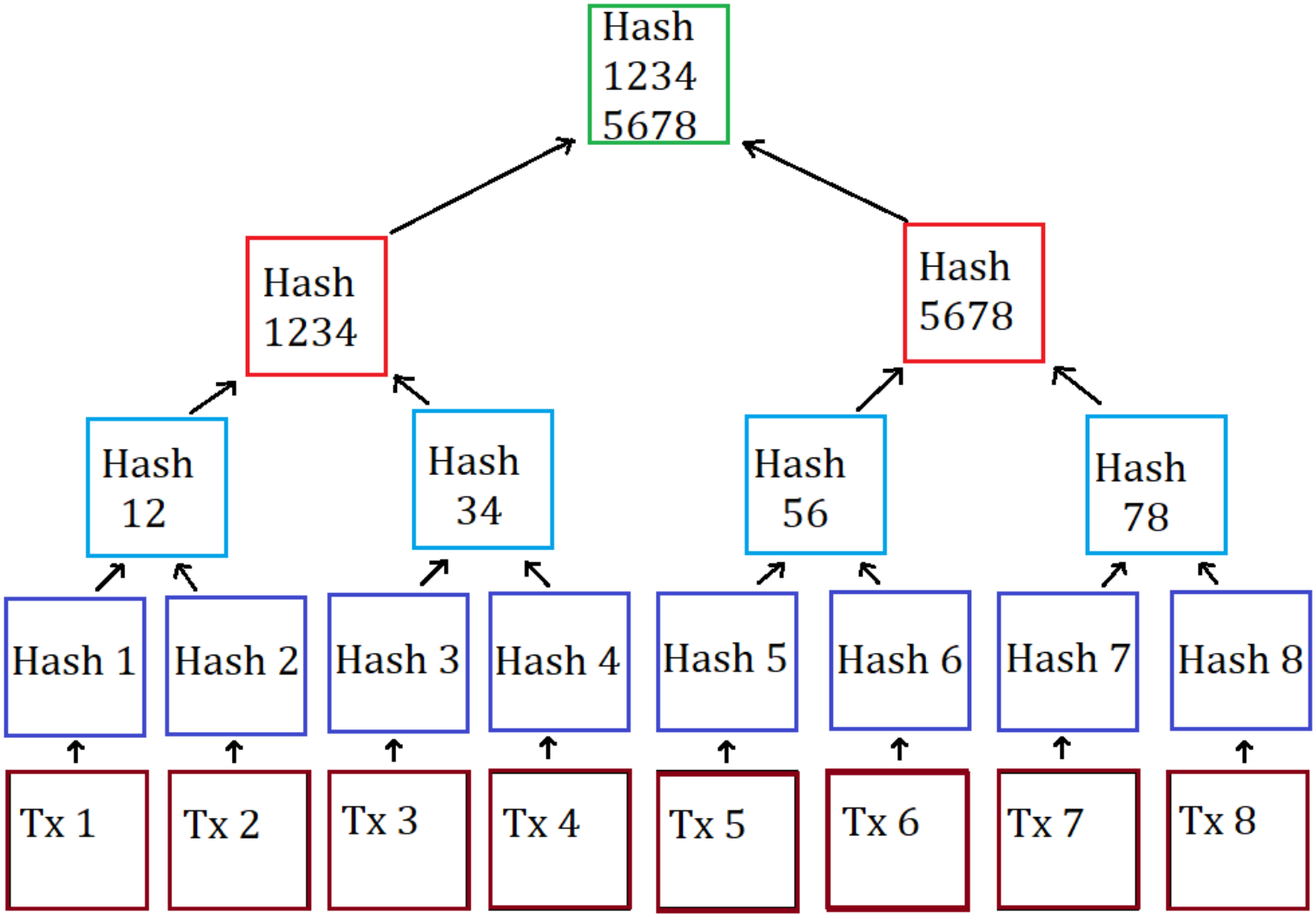


- Fast
- No single point of failure
- All downloaders are also uploaders

Types of blockchain

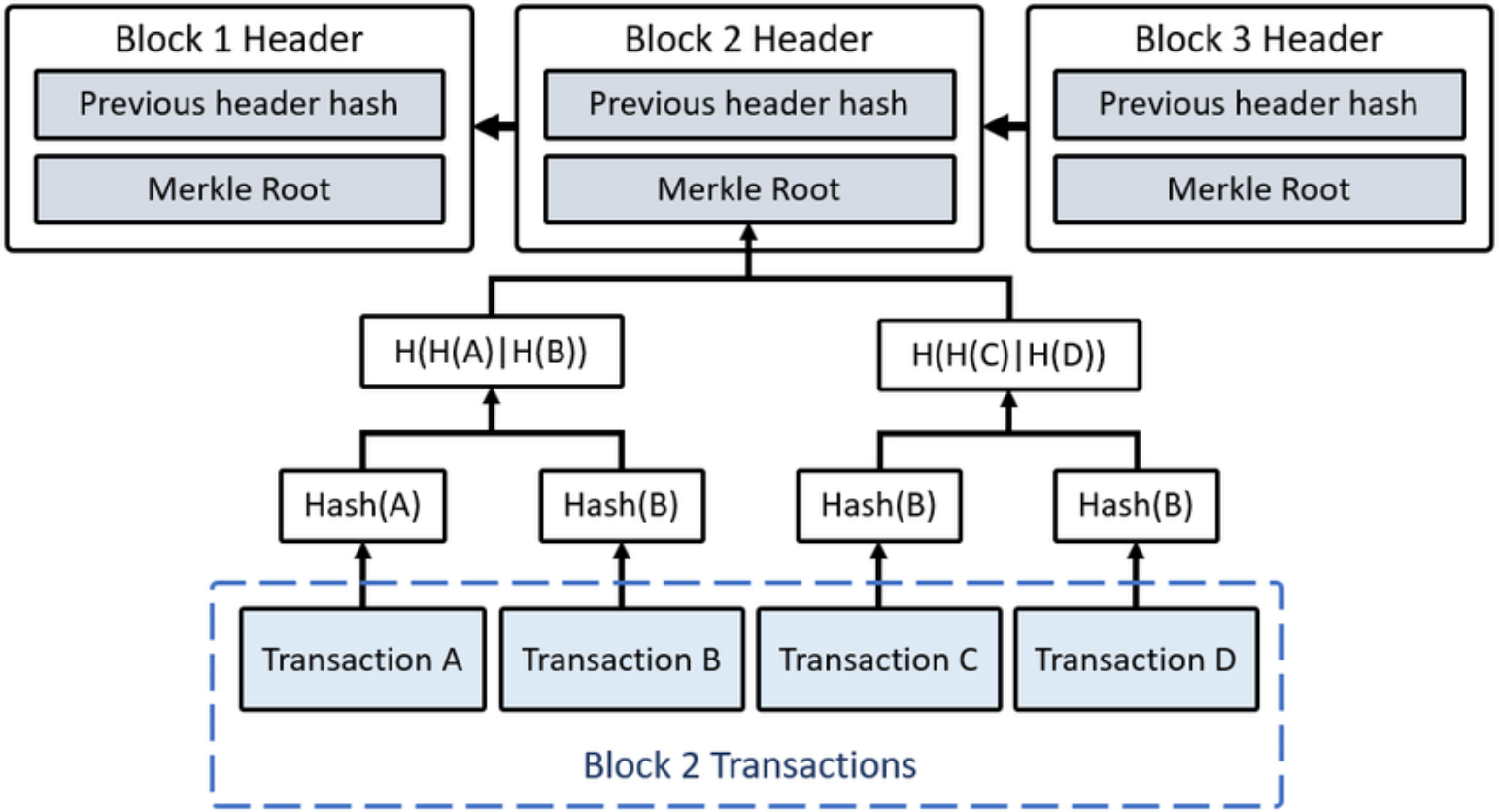
- **Public (Permissionless) Blockchain**: Everyone has the right to join, access, send, verify and receive transactions of the blocks in the blockchain to create a consensus. One widely successful permissionless blockchain is *bitcoin*.
- **Private (Permissioned) Blockchain**: The owner of the network decides which node to assign the right to access, send, receive, join and verify the block for creating an agreement between the nodes. Example: Healthcare Applications
- **Consortium or Hybrid Blockchain**: Internet of Vehicles (IoV) application

How to Make a Merkle Tree?

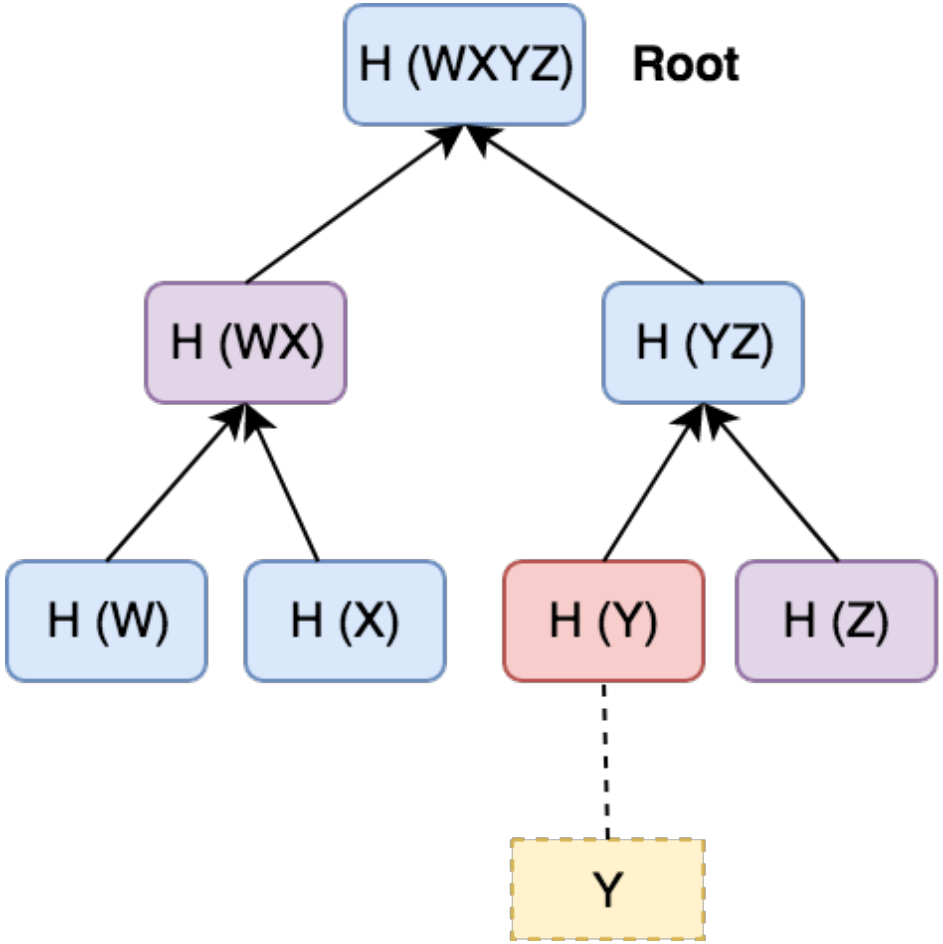


Tx_i: i^{th} transaction; H_i: Hash of i^{th} transaction ($H_{Tx_i} = H(Tx_i)$);
$H_{Tx_1\,Tx_2} = H_{Tx_1} \oplus H_{Tx_2}$; $H_{12345678}$: Merkle root

Use of Merkle Tree in Blockchain



Verifying Transactions Using the Merkle Root



To confirm transaction Y, one only needs to know: $H(WX)$, $H(Y)$, $H(Z)$ and $H(WXYZ)$; $H(\cdot)$: hash function

Types of blockchain

Block Header	
Block Version	BV
Previous Block Hash	PBHash
Merkle Tree Root	MTR
Block Type	Public
Timestamp	TS
Owner of Block	ES_l
Public key of signer (ES_l)	Pub_{ES_l}
Block Payload (Transactions)	
Transaction #1	Tx_1
Transaction #2	Tx_2
⋮	⋮
Transaction #n_t	Tx_{n_t}
Current Block Hash	CBHash
Signature on block using ECDSA	BSign

a) Formation of a block on public blockchain

Block Header	
Block Version	BV
Previous Block Hash	PBHash
Merkle Tree Root	MTR
Block Type	Private
Timestamp	TS
Owner of Block	ES_l
Public key of signer (ES_l)	Pub_{ES_l}
Block Payload (Encrypted Transactions)	
Encrypted Transaction #1	$E_{Pub_{ES_l}}(Tx_1)$
Encrypted Transaction #2	$E_{Pub_{ES_l}}(Tx_2)$
⋮	⋮
Encrypted Transaction #n_t	$E_{Pub_{ES_l}}(Tx_{n_t})$
Current Block Hash	CBHash
Signature on block using ECDSA	BSign

b) Formation of a block on private blockchain

Block Header	
Block Version	BV
Previous Block Hash	PBHash
Merkle Tree Root	MTR
Block Type	Hybrid
Timestamp	TS
Owner of Block	ES_l
Public key of signer (ES_l)	Pub_{ES_l}
Block Payload	
Encrypted Transaction #1	$E_{Pub_{ES_l}}(Tx_1)$
Transaction #2	Tx_2
⋮	⋮
Encrypted Transaction #n_t	$E_{Pub_{ES_l}}(Tx_{n_t})$
Current Block Hash	CBHash
Signature on block using ECDSA	BSign

c) Formation of a block on consortium blockchain

Consensus mechanisms

Consensus mechanisms are used to verify transactional data between the nodes in a P2P network.

- **Byzantine Fault Tolerance (BFT)**: An agreement protocol which helps to tolerate the Byzantine failures in a network. BFT maintains the reliable record of transactions in a transparent and tamper-proof way, as long as the number of traitors does not exceed one-third of the general network nodes.
- **Practical Byzantine Fault Tolerance (PBFT)**: This consensus mechanism is used when BFT fails to tolerate the faults in a network system. The algorithm for PBFT works in asynchronous systems and is optimized to achieve high performance along with an impressive overhead runtime.

Practical Byzantine Fault Tolerance (PBFT)

For adding a block in the blockchain, the following procedures in PBFT are required:

- A leader acting as a miner will select by the leader selection algorithm for adding a block.
- Leader receives a block with block adding request from any nodes (or client) into the blockchain.
- Leader sends this block to every node in the network for verifying the transactions.
- After successful verification of the transaction in the block, each received node sends a valid reply for adding that block.
- Leader counts the received reply and checks the number of counts (say, RCount) if it is greater that the twice number of the faulty nodes, i.e., $RCount > 2n_f + 1$ or the two-third nodes give the same reply. The $2n_f + 1$ non-faulty or valid replies provide the liveness of the system, that is, the message delay need to be bounded in due course. If this condition is satisfied, the leader will add the block into the blockchain and broadcasts a commit for adding the block into their respective blockchain for backup purposes.

Consensus mechanisms

- **Proof-of-Work (PoW):** This is the original consensus mechanism used to verify the transactions and produce new blocks in the blockchain. Mining is a complex process, and miners need to demonstrate that they can validate the transaction block. Here, the miners are financially rewarded if they perform verification. Thus, as the complexity increases in the mining process over time, the power consumption also increases. In other words, PoW is a costly process as the miners compete with each other to solve a mathematical problem.
- **Proof-of-Stake (PoS)**: In 2017, Ethereum began the process of switching from a PoW mechanism to a PoS system. The latter was designed to mitigate the limitations of PoW, in terms of energy, cost, and processing time. Specifically, it adopts a forging process rather than the mining process to validate transaction blocks.

Consensus mechanisms

- **Delegated Proof-of-Stake (DPoS):** This is a fast, efficient, flexible and most decentralized consensus mechanism. DPoS holds the power of stakeholder for the approval of voting and resolving the consensus issues in an honest and representative way. The deterministic selection of witnesses allows the transactions to be confirmed on an average of just 1 second. This consensus mechanism is designed to protect all the participants in a free, fair, and transparent environment.
- **Proof-of-Burn (PoB)**: An alternative consensus protocol for PoS and PoW. In PoB mechanism, the miners prove that they burn one cryptocurrency to create another currency, i.e., they are sent to a bitcoin address which is unsupendable. Its significance depends on the burning tokens in an unrecoverable manner. As comparative to PoW/PoS, it is easily verifiable and hard to undo.

Ripple Protocol Consensus Algorithm (RPCA)

- It is a voting based consensus algorithm proposed in the literature in order to achieve high accuracy of a correct agreement for adding a block into a blockchain over unreliable distributed network.
- RPCA achieves an agreement in the voting process.
- Every participant node in the voting process maintains a unique node list (UNL), where each node in the list is considered as trusted one.
- The protocol executes with the help of the following steps [Wang et al. [2019]]:
  - In voting process, every participant node constantly receives the transaction. If the transaction is valid, the node integrates the transactions into a set or list, called a “candidate set”.
  - Every participant node dispatches its own candidate set to other participant node as a proposal.

Ripple Protocol Consensus Algorithm (RPCA) (Continued...)

- The remaining steps are as follows [Wang et al. [2019]]:
  - The participant node receives the proposal from other nodes. The node will then check whether the sender node belongs to its UNL list or not. If it is there, the node will verify the transactions with its own local candidate set. If all are valid, the transactions will gain a vote. Only when the transaction gets more than 50% of vote, the transaction will enter into the next round.
  - Next, the participant node sends the transaction that it gains more than 50% of the votes than the others and if it increases to 60% of vote, it needs to wait until it reaches to the threshold of 80% of the votes.
  - Finally, the participant node records the transaction confirmed by the 80% UNL nodes to be added into its ledger data.

The transaction is accepted only if 80% of the votes in the UNL of a participant node agrees with it. Thus, 80% of the UNL is honest, that is, the percentage of the faulty nodes in the UNL is less that for the 20% of the UNL. When the UNL contains d number of nodes in the network, and the RPCA will maintain its correctness as long as $n_f \leq \frac{d-1}{5}$, i.e., $d \geq 5n_f + 1$ where n_f is the Byzantine failure persisted nodes in the network.

Table: Blockchain consensus mechanisms and their applications

Consensus mechanism	**Concept**	**Resource**	**Applications**
Ripple	Voting in multiple rounds	No resource	XRP ledger xrp [2014]
PBFT	Voting	No resource	Tendermint Kwon [2014]
PoW	Hashing	Computations	Bitcoin Nakamoto [2009] Ethereum Wood et al. [2014]
PoS	Digital signatures	Currency	PeerCoin King and Nadal [2012] SnowWhite Bentov et al. [2016] Ouroboros Kiayias et al. [2017]
DPoS	Voting	Currency	BitShared Ark EOS
PoB	Address suspension	Currency	SlimCoin sli [2014]

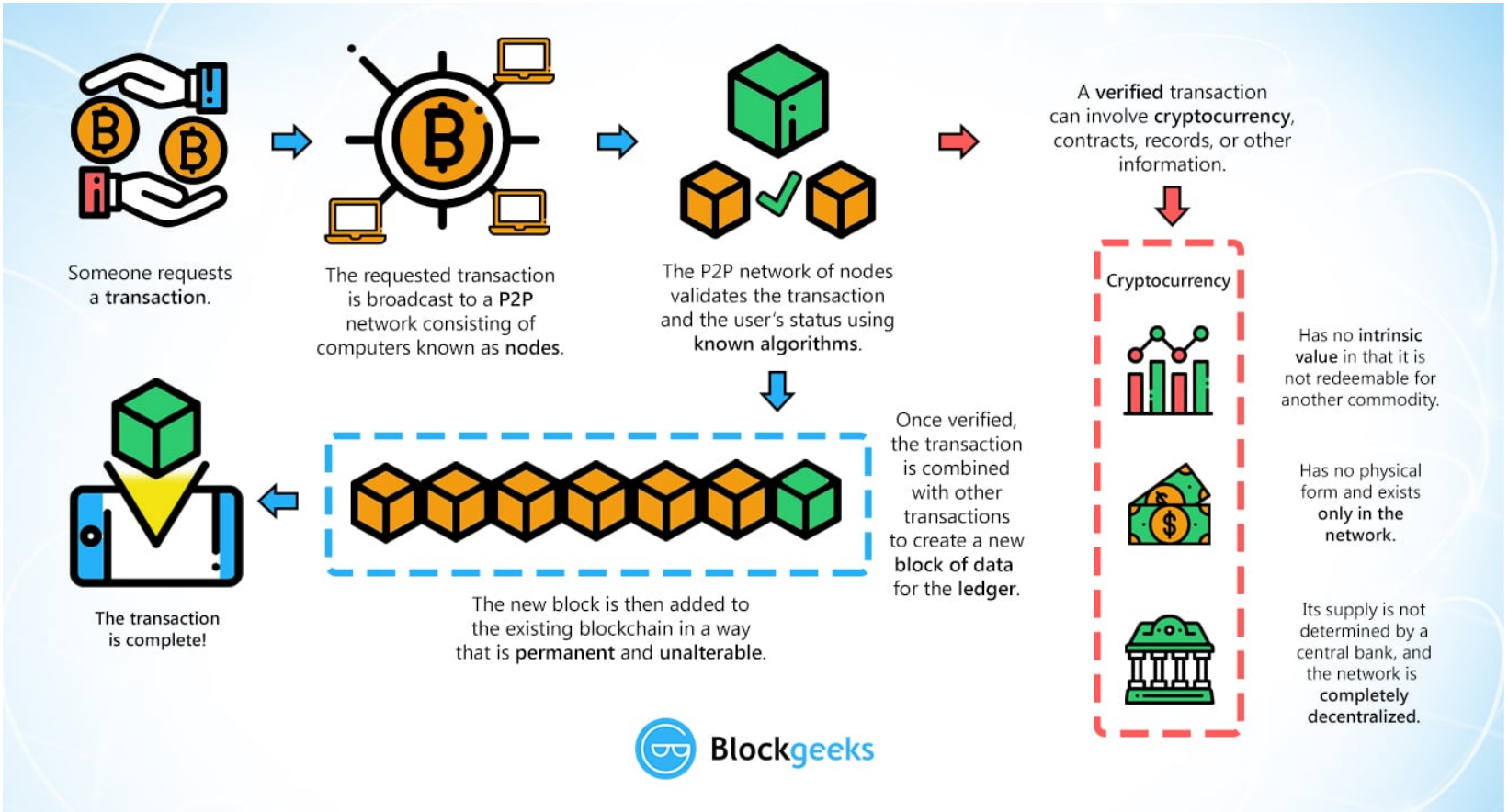
Ref. Anusha Vangala, Ashok Kumar Das, Neeraj Kumar, and Mamoun Alazab. "Smart Secure Sensing for IoT-Based Agriculture: Blockchain Perspective," in *IEEE Sensors Journal*, 2020, DOI: 10.1109/JSEN.2020.3009382. (2019 SCI Impact Factor: 3.073)

Table: Attacks on consensus mechanisms

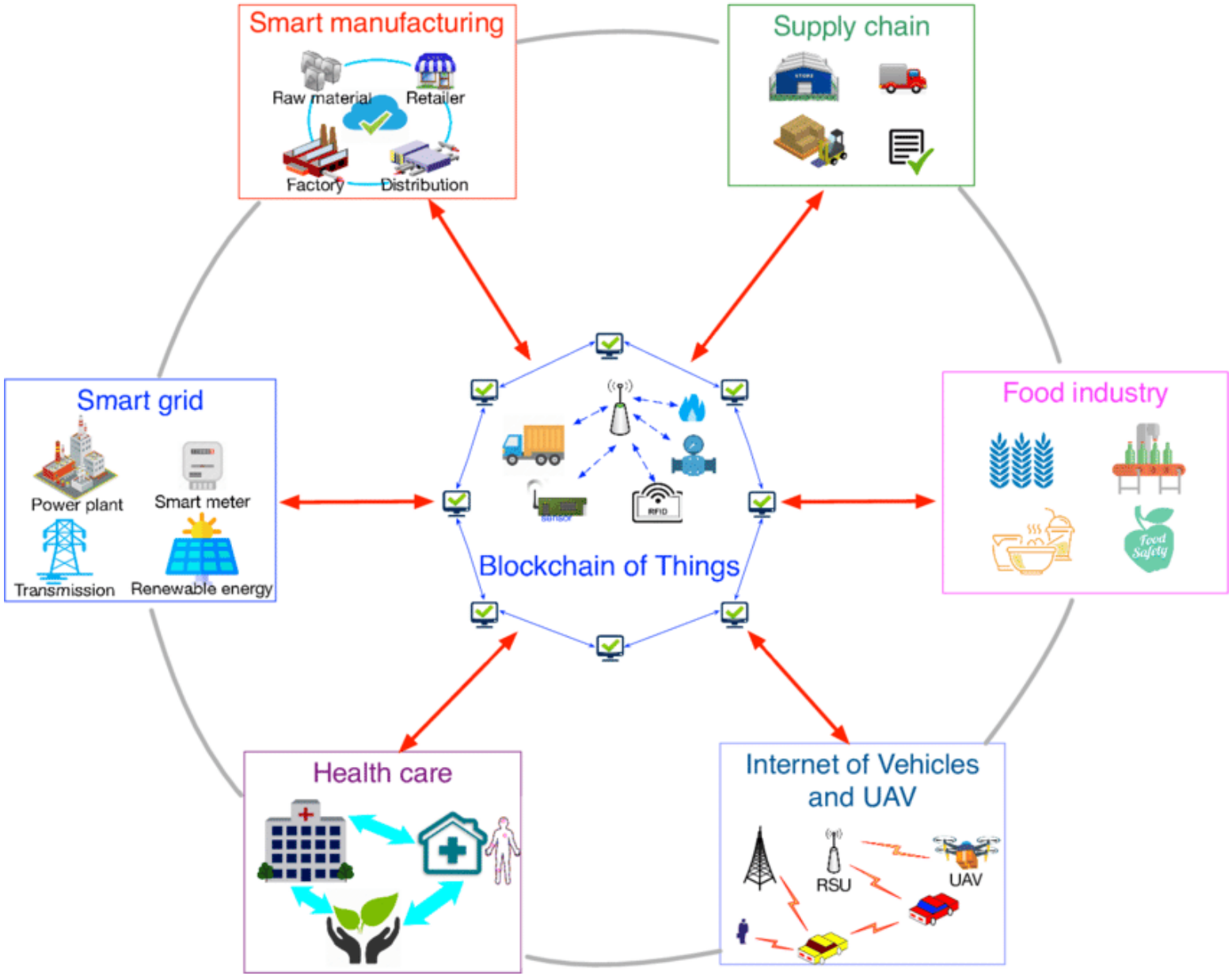
Attack	Affected consensus protocols	Description
Double spending	Most protocols	Repeated usage of token
Selfish mining	PoW	Gain profits by generating blocks privately in a mining pool
Nothing at stake	PoS	Blocks added to all branches in a fork
Bribe attack	PoS	Honest nodes are given incentive to add blocks on private fork
Stake bleeding attack	PoS	Broadcast transactions copied from main chain onto private fork to earn extra fees and increase stake
Fake stake attack	PoS	Increase the smaller valued stakes to higher valued stakes

Ref. S. Zhang and J. Lee, "A Group Signature and Authentication Scheme for Blockchain-Based Mobile-Edge Computing," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4557-4565, 2020. (2019 SCI Impact Factor: 9.936).

Block creation and addition using consensus mechanism in a blockchain



Applications of Blockchain Technology



References

Slimcoin : A Peer-to-Peer Crypto-Currency with Proof-of-Burn - Mining without Powerful Hardware, 2014. URL https://github.com/slimcoin-project/slimcoin-project.github.io/raw/master/whitepaperSLM.pdf.

The XRP Ledger, 2014. URL https://xrpl.org/consensus-principles-and-rules.html.

Iddo Bentov, Rafael Pass, and Elaine Shi. Snow White: Provably Secure Proofs of Stake. *IACR Cryptology ePrint Archive*, 2016(919), 2016.

Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Advances in Cryptology (CRYPTO'17)*, pages 357–388, Santa Barbara, CA, USA, 2017.

Sunny King and Scott Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, 2012.

Jae Kwon. Tendermint: Consensus without mining. *Self-Published Paper (Draft v.0.6)*, 1(11), 2014. URL https://tendermint.com/static/docs/tendermint.pdf.

Satoshi Nakamoto. Bitcoin open source implementation of p2p currency. *P2P foundation*, 18, 2009.

X. Wang, P. Zeng, N. Patterson, F. Jiang, and R. Doss. An Improved Authentication Scheme for Internet of Vehicles Based on Blockchain Technology. *IEEE access*, 7:45061–45072, 2019.

Gavin Wood et al. Ethereum: A Secure Decentralised Generalised Transaction Ledger. *Ethereum project yellow paper*, 151(2014):1–32, 2014.