P P SAVANI
UNIVERSITY

Module 3

IBM and Blockchain

Outline

P P SAVANI UNIVERSITY

- How IBM can help with a Blockchain Project
- IBM's Blockchain strategy
- The IBM Blockchain Platform
- The Linux Foundation's Hyperledger Project
- Hyperledger Fabric
- Continuing your Blockchain Journey

How IBM can help

P P SAVANI UNIVERSITY

- **Security at scale** – Enterprise grade security and control on a platform where businesses and industries are reinventing themselves.
- **Trusted expertise** – Reinventing business processes through unrivalled industry and technical knowledge as you start, accelerate and innovate your blockchain network.
- **Network convening power** – Bringing together an expansive partner network of innovators, regulators and suppliers to establish, join or run your blockchain network.

IBM Blockchain Strategy

P P SAVANI UNIVERSITY

Services

Collaborate with services teams from ideation all the way to production

Ecosystem

Tap into our diverse ecosystem to develop strategic partnerships and create your competitive advantage

Solutions

Solve critical industry challenges by building and joining new business networks and applications

IBM Blockchain Platform

Build, operate and grow blockchain networks in heterogeneous environments

HYPERLEDGER

A founding, premier member of Hyperledger, IBM is committed to open source, standards & governance

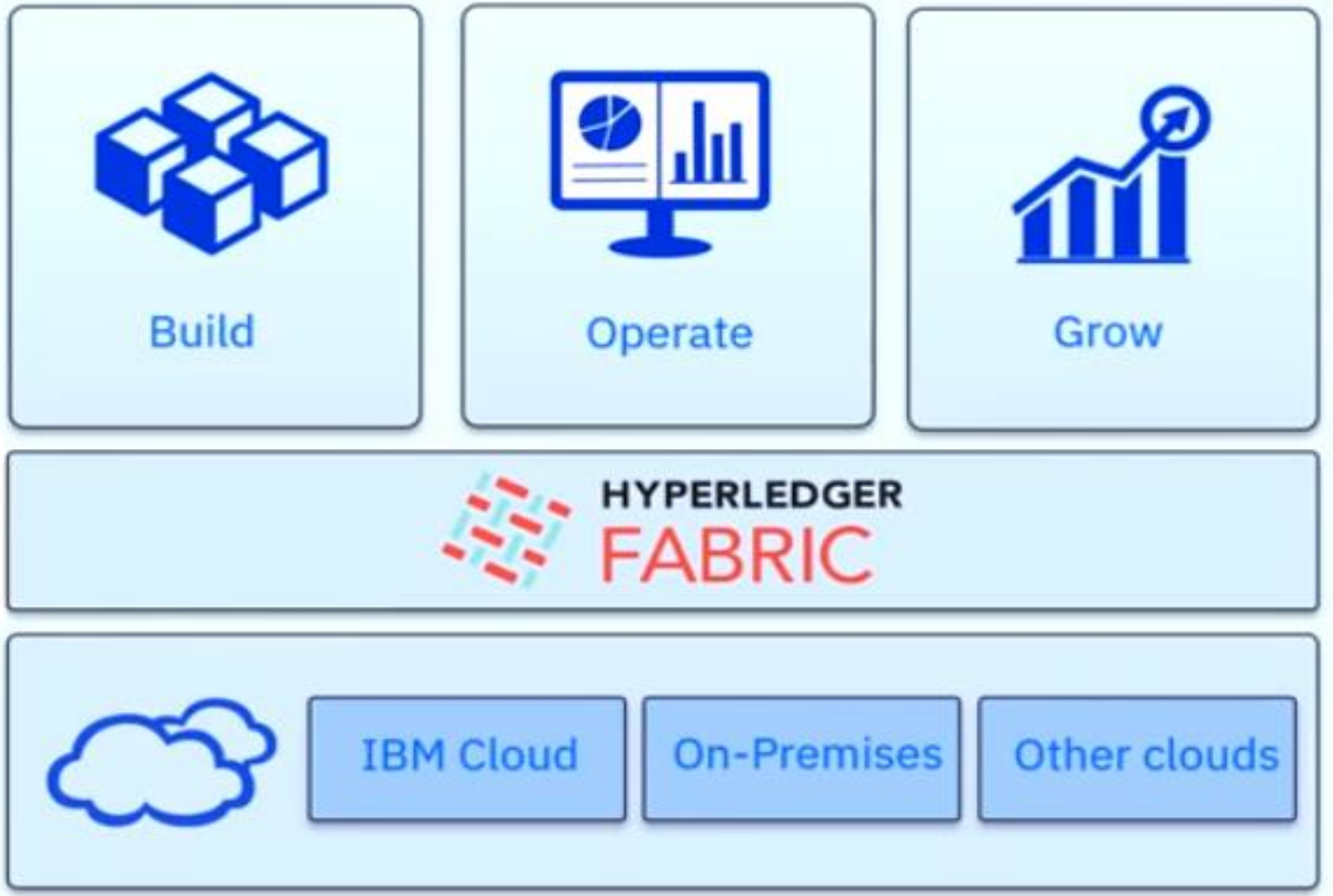
IBM Blockchain Platform

P P SAVANI UNIVERSITY

Advanced tooling
allows you to quickly build, operate and grow blockchain networks

Open technology
uses the popular Hyperledger Fabric distributed ledger

Deploy anywhere
fully managed, or flexible deployment on-premises or on other cloud vendors



Hyperledger is not

P P SAVANI UNIVERSITY

- A Cryptocurrency
- A Blockchain
- A Company

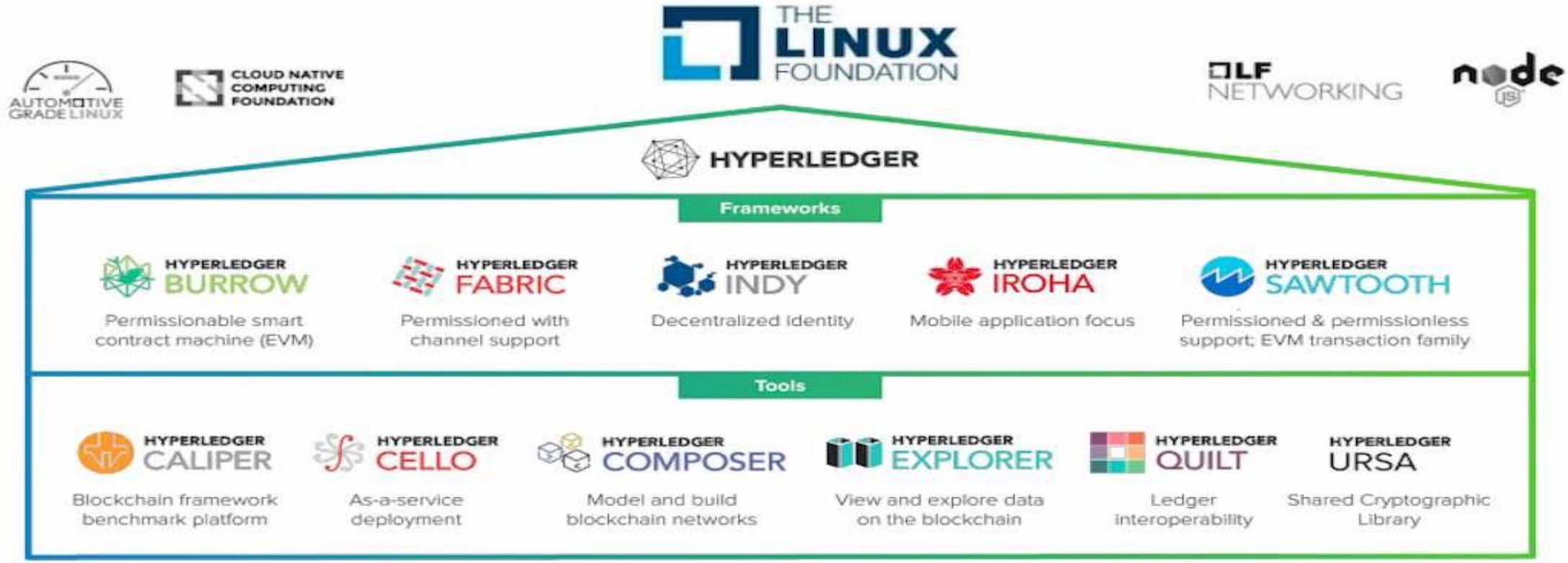
Hyperledger is

- A project under Linux foundation.
- An open source development project.
- An open source community of communities to benefit an ecosystem of Hyperledger based solution providers and users focussed on blockchain related use cases that will work across a variety of industrial sectors.

Hyperledger

- IBM Blockchain Platform is underpinned by technology from the Hyperledger project.
- Hyperledger is an open source collaborative effort created to advance cross industry blockchain technologies.
- The Hyperledger greenhouse includes many projects that anyone can freely use and contribute to.
- Open Source
- Open Standards
- Open governance model.

Hyperledger Greenhouse



Hyperledger Framework

P P SAVANI UNIVERSITY

- Hyperledger Fabric: Hyperledger Fabric is intended as a foundation for developing applications and solutions with modular architecture. It provides many benefits like permissioned networks, confidential transactions, etc.

- Hyperledger Sawtooth: It is an open-source project and used as an enterprise-level blockchain system used for creating and operating distributed ledger applications. Hyperledger sawtooth supports a variety of consensus algorithms like PBFT, and PoET.

- Hyperledger Indy: It is a project that is made for decentralized identity. It offers lots of libraries, tools, and reusable components for creating decentralized identities.

Hyperledger Framework

- Hyperledger Iroha: It is a blockchain platform designed for infrastructure projects that need distributed ledger technology. It is used to build identity management platforms like national IDs. It can integrate with Linux, macOS, and Windows platforms.
- Hyperledger Burrow: It is a framework for executing smart contracts in permissioned blockchains. The goal of Hyperledger burrow is to facilitate cross-industry applications for smart contracts. It is built around the BFT consensus algorithm.
- Hyperledger Caliper: It is a blockchain benchmark tool that allows users to measure the performance of a blockchain implementation with a set of predefined use cases. It will produce reports containing a number of performance indicators to serve as a reference when using the blockchain solutions like Hyperledger Burrow, Hyperledger Fabric, Hyperledger Iroha, and so on.

Hyperledger Framework

P P SAVANI UNIVERSITY

- Hyperledger Cello: It serves as an operational dashboard for Blockchain that reduces the effort required for creating, managing, and using blockchains. It provides an operational console for managing blockchain efficiently.
- Hyperledger Explorer: It is a user-friendly web application tool that is used to view, invoke, deploy, or query blocks, associated data, and network information stored in the ledger. It is regarded as an easy way that allows users to view the necessary network information of the blockchain.
- Hyperledger Besu: It is an Ethereum client designed to be enterprise-friendly for both public and private blockchain network use cases. It offers many useful features like EVM, several proof-of-authority protocols, a privacy transaction manager to ensure the privacy of transactions, etc.

Proof of elapsed time

P P SAVANI UNIVERSITY

- A node downloads PoET code and generates a key.
- This key is verified by the existing participants.
- The new node is given a timer object which is random.
- Each participant in the blockchain network waits a random amount of time.
- The first participant to finish waiting gets to be the leader of the new block.

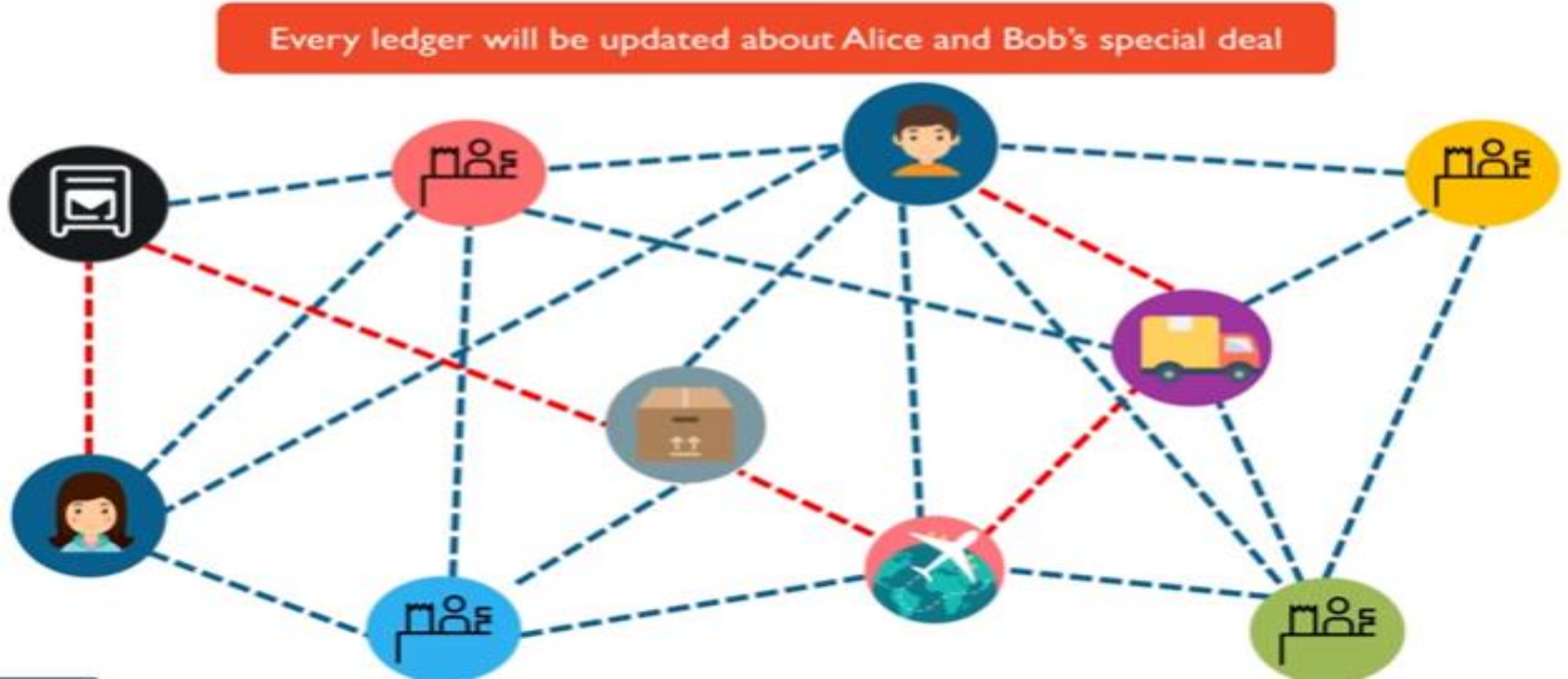
Hyperledger

P P SAVANI UNIVERSITY

In simpler terms, Hyperledger can be thought of as a software which everyone can use to create one's own personalised blockchain service.

Example – Traditional Trading

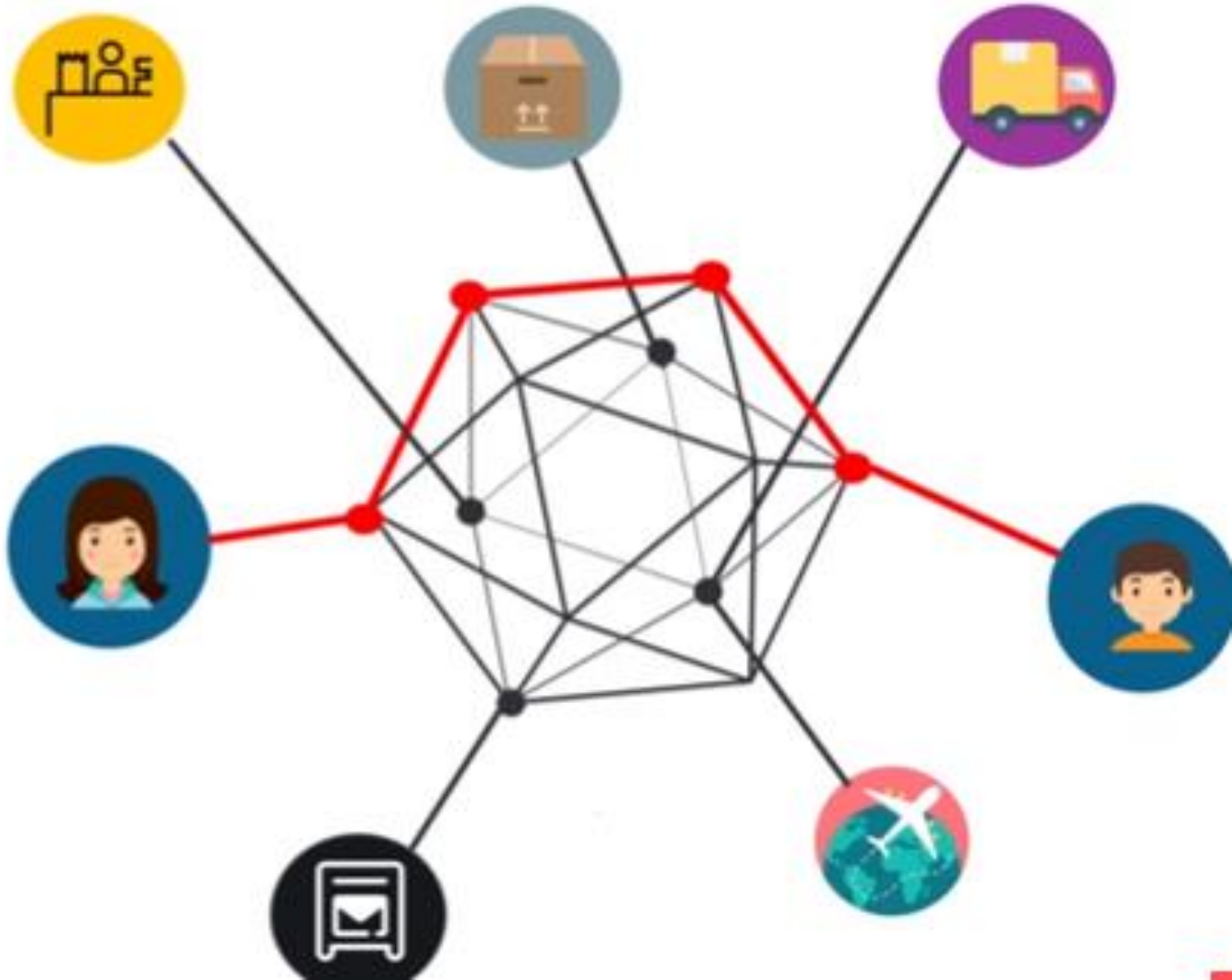
Example – Trading on public blockchain



Example – Hyperledger

P P SAVANI UNIVERSITY

On the Hyperledger network, only parties directly affiliated with the deal are updated on the ledger and notified. Thus maintaining privacy and confidentiality



How this works

P P SAVANI UNIVERSITY

App Query

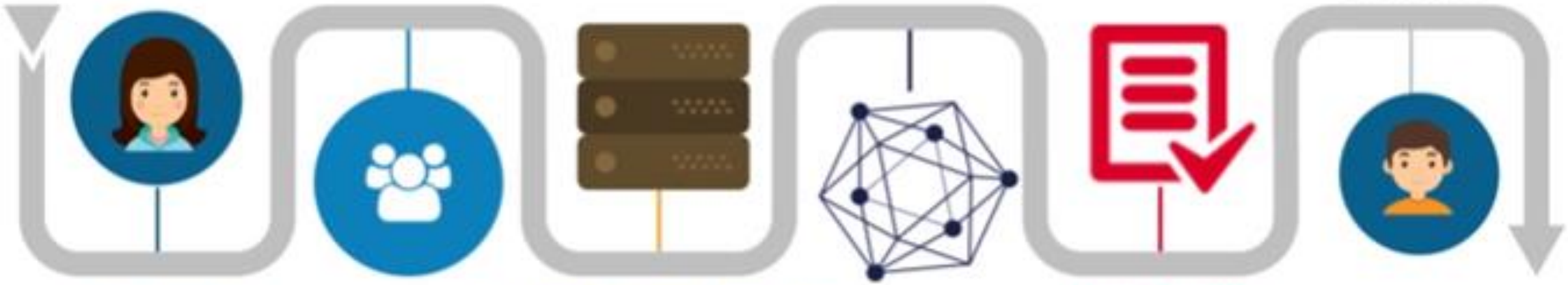
She looks up her app for Bob's address on the network

Hyperledger

The Hyperledger network then connects both parties directly affiliated with the deal

Bob Receives

Once the consensus cloud validates the transaction, Bob receives his product and the transactions are committed to the ledger



Alice Sends

Alice decides to send Bob her product

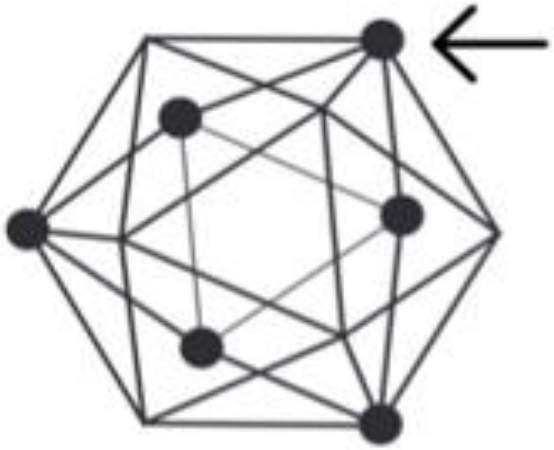
Membership Service

The app looks up a membership service validates Bob's membership

Verification

Both parties generate a result which are then sent to the consensus cloud to be ordered and verified

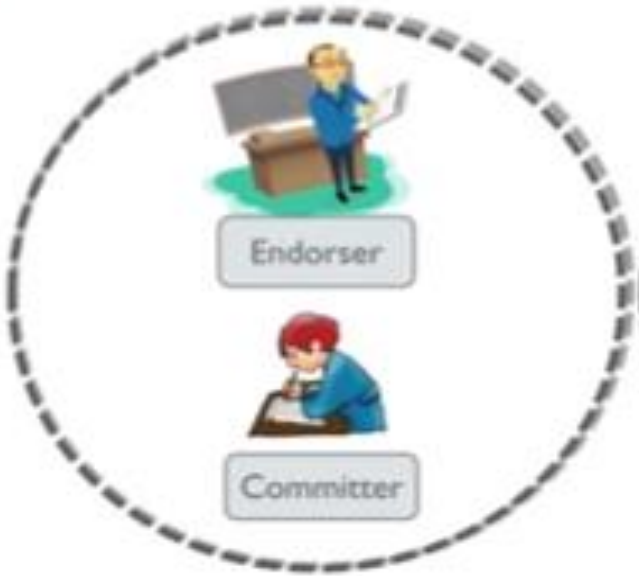
Different from Blockchain



Peers

Two Separate Runtime

Three Distinct Roles



Peer Roles

P P SAVANI UNIVERSITY

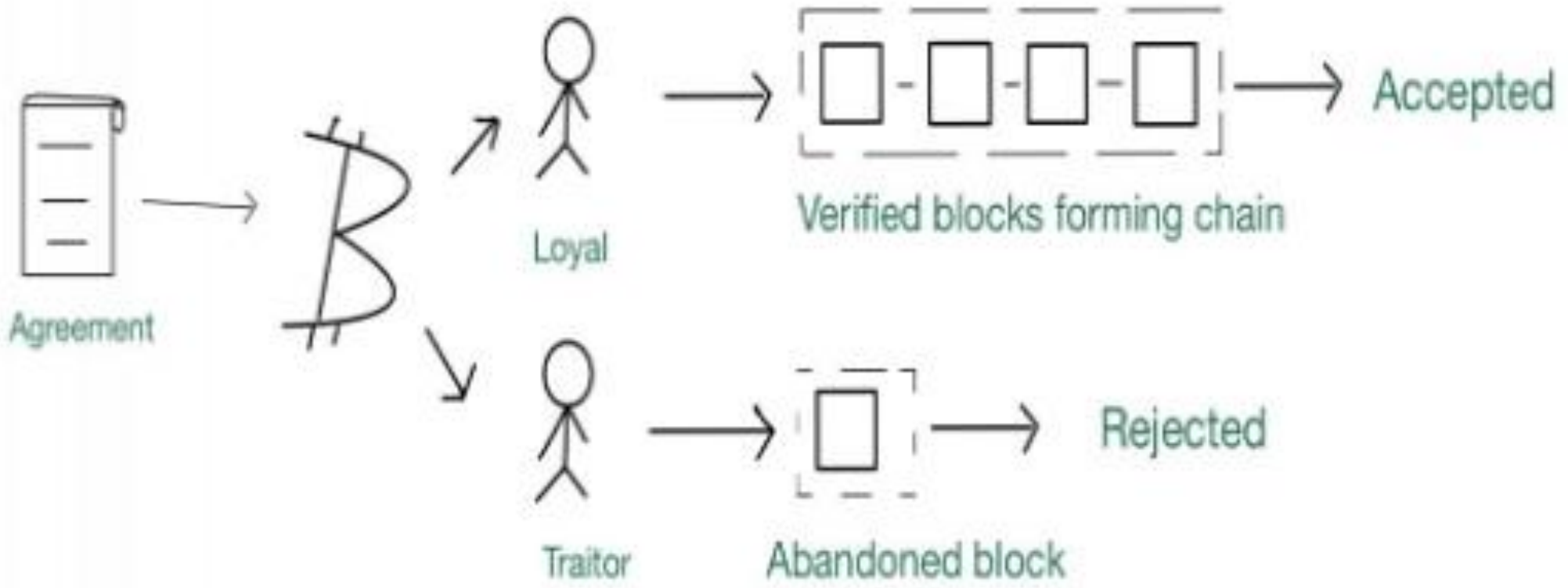
- Committers – Append validated transaction to their specific ledger.
- Endorsers – Simulate the transactions and prevent unstable and non deterministic transactions.
- All endorsers are committers but all committers may or may not be endorsers.
- Consenter – Network consensus service. A collection of consensus service nodes (CSNs) will order transactions into blocks according to the networks chosen ordering implementation.

Comparison

P P SAVANI UNIVERSITY

Parameters	Bitcoin	Ethereum	Hyperledger
Cryptocurrency	Bitcoin	Ether	None, but can be implemented when required
Network	Public	Public	Permissioned
Consensus	Proof of Work (SHA256)	Proof of Work (Ethash)	PBFT (practical byzantine fault tolerance)
Smart Contract	None	Yes (Solidity)	Yes (chaincode)
Language	C++	Golang, Python	Golang, Java

Byzantine Fault Tolerance (BFT)



Pseudo Anonymity

P P SAVANI UNIVERSITY

- Pseudo-anonymity, means that a person will be linked to a public Bitcoin address, but no one will get to know the actual name or address.
- To explain this in simple words, suppose a person sends a sum of money, then the receiver will get to know that the sender is linked to a bitcoin address but will not know the actual address. Hence, we say that bitcoin or any other alt currencies are not entirely anonymous.

	Traditional Database	Public Blockchain	Private Blockchain
How is governance managed?	Centralized	Decentralized	Federated
Who updates the ledger?	Single party	Unrestricted participants	Restricted participants
How is good behavior incentivized?	N/A	Cryptoeconomics	Reputational risk
Who has read-only access?	Users authorized by the database owner	Anyone	A group of selected actors/contributors
Who has writing access?	Users authorized by the database owner	Anyone	A group of selected actors/contributors
Are transactions anonymous to the public?	Yes	No	Yes
Does it require censorship resistance	No	Yes	No
Examples	Experian	Ethereum, Bitcoin blockchain	Enterprise Ethereum, PegaSys Plus

Crime-as-a-service

P P SAVANI UNIVERSITY

- Crime-as-a-Service Could Be the Next Big Threat to Your Business. Crime-as-a-service is when a professional criminal or group of criminals develop advanced tools, “kits” and other packaged services which are then offered up for sale or rent to other criminals who are usually less experienced.
- For example, someone might develop a ransomware kit that’s capable of encrypting important files where the victim must pay a ransom. They will then sell or rent that kit to other lower level cyber criminals, thus enabling them launch attacks.

Sybil attack

P P SAVANI UNIVERSITY

- In a Sybil attack, the attacker subverts the reputation system of a network service by creating a large number of pseudonymous identities and uses them to gain a disproportionately large influence.

- In the world of cryptocurrencies, a more relevant example is where somebody runs multiple nodes on a blockchain network.

Z Cash

P P SAVANI UNIVERSITY

- Zcash is a cryptocurrency aimed at using cryptography to provide enhanced privacy for its users compared to other cryptocurrencies such as Bitcoin. Zcash is based on Bitcoin's codebase.
- Zcash is the first widespread application of zk-SNARKs, a novel form of zero-knowledge cryptography. The strong privacy guarantee of Zcash is derived from the fact that shielded transactions in Zcash can be fully encrypted on the blockchain, yet still be verified as valid under the network’s consensus rules by using zk-SNARK proofs.

zk-SNARKs

P P SAVANI UNIVERSITY

- The acronym zk-SNARK stands for “Zero-Knowledge Succinct Non-Interactive Argument of Knowledge,” and refers to a proof construction where one can prove possession of certain information, e.g. a secret key, without revealing that information.
- “Zero-knowledge” proofs allow one party (the prover) to prove to another (the verifier) that a statement is true, without revealing any information beyond the validity of the statement itself. For example, given the hash of a random number, the prover could convince the verifier that there indeed exists a number with this hash value, without revealing what it is.

zk-SNARKs

P P SAVANI UNIVERSITY

- Example:

  You need to make a purchase and you tell the seller that you have the sufficient amount of money to pay for that without actually telling him your account balance.

- This is made possible by proving the identity using public private key pair.
- If someone had access to the secret randomness used to generate these parameters, they would be able to create false proofs that would look valid to the verifier. For Zcash, this would mean the malicious party could create counterfeit coins. To prevent this from ever happening, Zcash generated the public parameters through an elaborate, multi-party ceremony.

Blockchain Double Spending

P P SAVANI UNIVERSITY

- Double spending means spending the same money twice.
- As we know, any transaction can be processed only in two ways. One is offline, and another is online.

- Offline: A transaction which involves physical currency or cash is known as an offline transaction.

- Online: A transaction which involves digital cash is known as an online transaction.

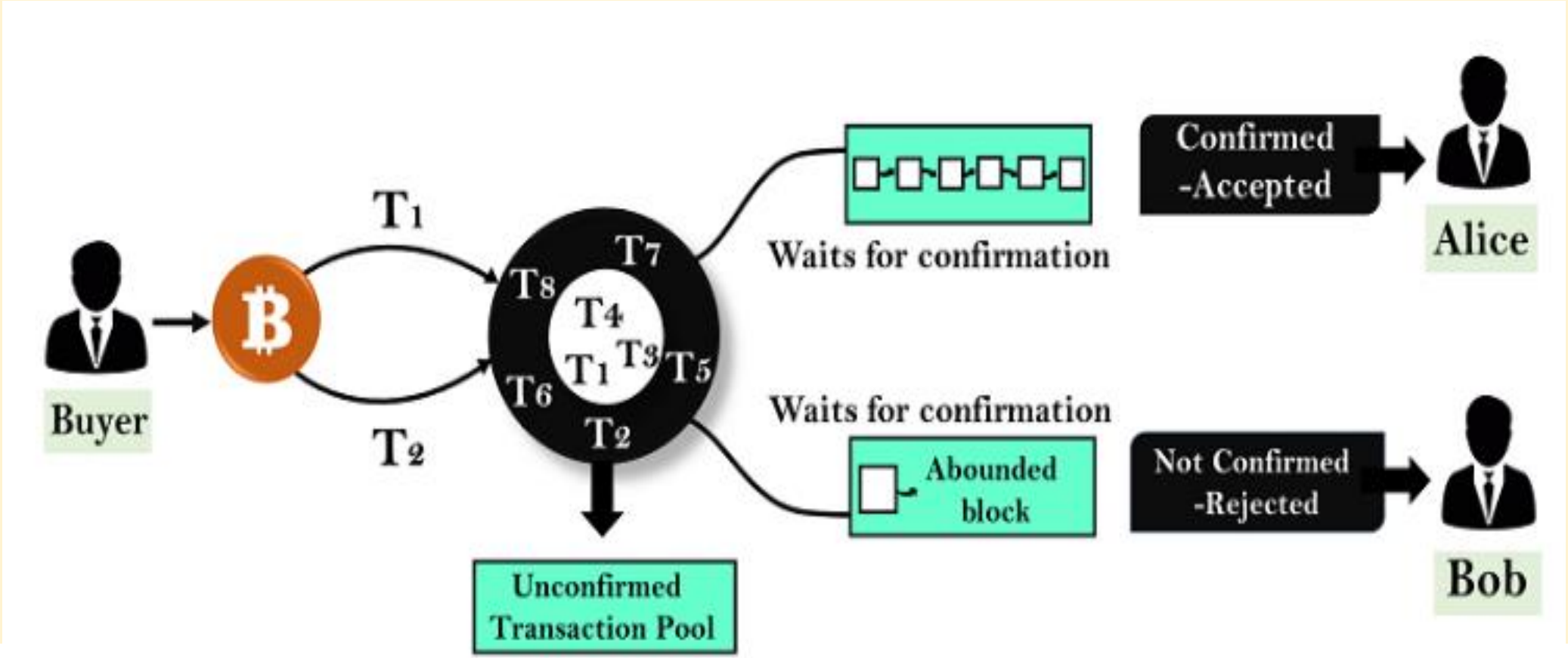
Continue...

P P SAVANI UNIVERSITY

- In a physical currency, the double-spending problem can never arise.

- But in digital cash-like bitcoin, the double-spending problem can arise. Hence, bitcoin transactions have a possibility of being copied and rebroadcasted. It opens up the possibility that the same BTC could be spent twice by its owner.

Example


Buyer
T1
T2
T7
T8
T4
T1
T3
T5
T6
T2
Unconfirmed Transaction Pool
Waits for confirmation
Confirmed -Accepted
Alice
Waits for confirmation
Abounded block
Not Confirmed -Rejected
Bob

Finney Attack

P P SAVANI UNIVERSITY

- The Finney attack is named after Hal Finney.
- The Finney attack is one of the types of double-spending problem.
- In this attack, the attacker is the miner who mines blocks normally.
- In the block, he includes a transaction which sends some of his coins back to himself without broadcasting the transaction. When he finds a pre-mined block, he sends the same coins in a second transaction. The second transaction would be rejected by other miners, but this will take some time.
- To prevent this attack, the seller should wait for at least six blocks confirmation before releasing the goods.

Vector76 Attack

P P SAVANI UNIVERSITY

- The Vector76 attack is a combination of the Race attack and the Finney attack.
- In this attack, a miner creates two nodes, one of which is connected to the exchange node, and the other is connected to well-connected peers in the blockchain network.
- Now, the miner creates two transactions, one high value, and one low value. Then, the attacker pre-mines a high-value transaction to an exchange service.
- When a block is announced, he quickly sends the pre-mined block directly to the exchange service. When exchange service confirms the high-value transaction, the corrupted attacker sends a low-value transaction to the blockchain network that finally rejects the high-value transaction.

Continue...

P P SAVANI UNIVERSITY

- As a result, the corrupted attacker's account is deposited on the amount of the high-value transaction.
- This attack can be protected by disabling the incoming connections and only connecting to well-connected nodes.

Algorand

P P SAVANI UNIVERSITY

- Algorand is a Boston-based open-source software company working
- towards building a borderless economy. They've developed a
- permissionless, Pure Proof-of-Stake (PoS) protocol with open
- participation, scalability, security and transaction finality.
- Proposal phase: a single token is randomlyselected, and its owner
- proposes the next blocks. However, this proposer is only known to the
- whole network during thepropagation phase: it is already too late to
- interfere. In Pure PoS, every token has thesame powerin being
- selected.

- Voting round: a committee of owners of 1,000 random tokens is
- selected, approving the block proposed by the first user. As opposed to
- the fixed committee system in many Proof-of-Work or Proof-of-Stake
- blockchains, this random selection of thecommittee members makes
- the protocol extremely secure against adversary attacks: they simply
- don’t know who to target.

Sharding

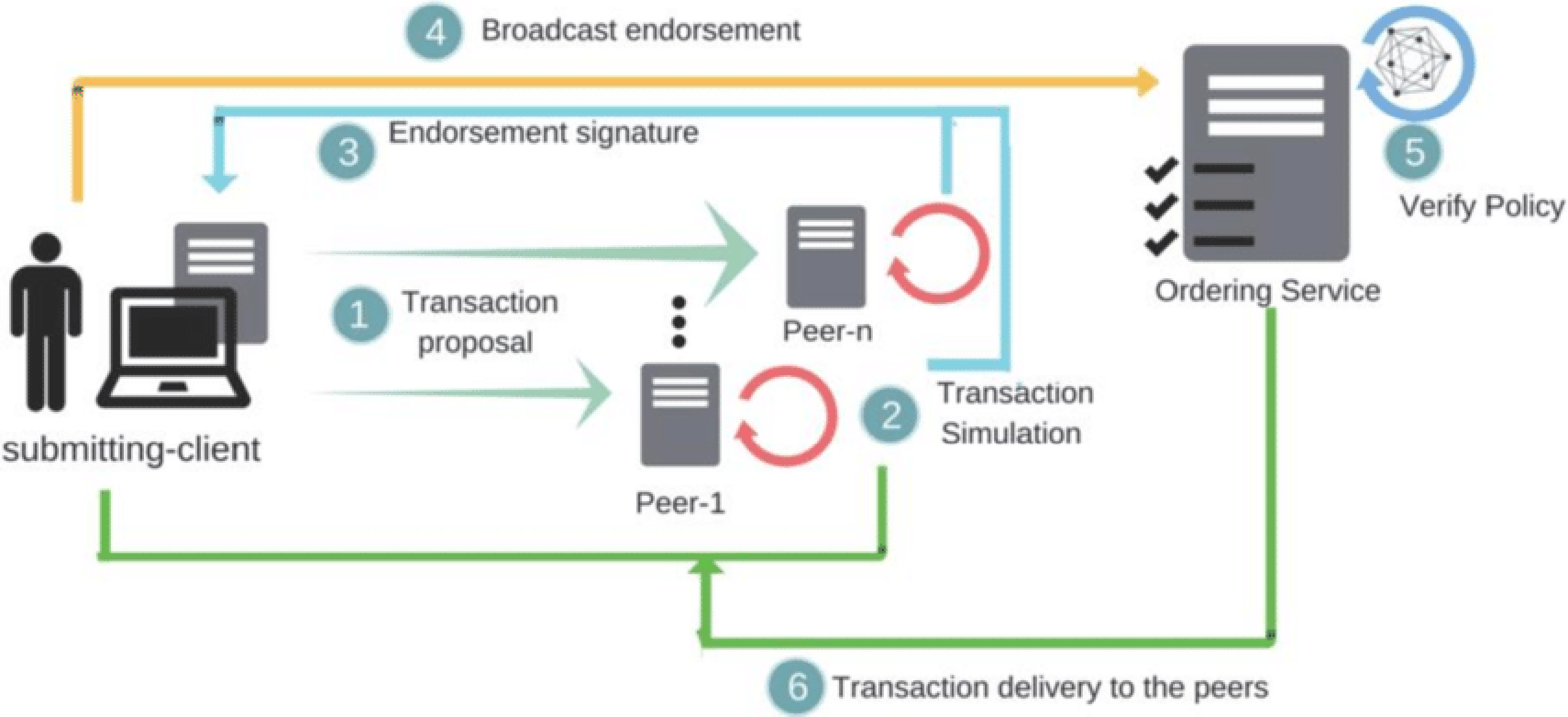
P P SAVANI UNIVERSITY

- Sharding is a type of database partitioning that separates very large databases the into smaller, faster, more easily managed parts called data shards. The word shard means a small part of a whole.
- Sharding could be the key to allowing blockchains to scale, while maintaining the privacy and security features that make the distributed ledger technology so efficient. But there are hurdles that need to be addressed.
- Sharding is a way of partitioning to spread out the computational and storage workload across a peer-to-peer (P2P) network so that each node isn't responsible for processing the entire network's transactional load. Instead, each node only maintains information related to its partition, or shard.

Advantages of Hyperledger

P P SAVANI UNIVERSITY

- Permissioned membership
- Performance, scalability, and levels of trust
- Data on a need-to-know basis
- Rich queries over an immutable distributed ledger
- Modular architecture supporting plug-in components
- Protection of digital keys and sensitive data


4 Broadcast endorsement
3 Endorsement signature
5 Verify Policy
Ordering Service
1 Transaction proposal
Peer-n
Peer-1
2 Transaction Simulation
submitting-client
6 Transaction delivery to the peers