Unit 5 Hyperledger, Security, Emerging Trends

- **Hyperledger Fabric:** Hyperledger architecture, Consensus in Hyperledger, Hyperledger frameworks, Hyperledger Fabric, Sawtooth, Indy, Hyperledger tools Caliper and Hyperledger library Ursa, Blockchain as-a-service deployment model of Hyperledger Cello.
- **Blockchain Security**: Pseudo-anonymity vs. anonymity, Zcash and Zk-SNARKS for anonymity preservation, attacks on Blockchains: Sybil attacks, selfish mining and 51% attacks; Advent of Algorand, and Sharding based consensus algorithms to prevent the attacks
- **Emerging Trends:** Cloud-based blockchain, Multichain, Geth , Stellar , Ripple, R3 Corda, Blockchain API, Blockchain Sandboxes

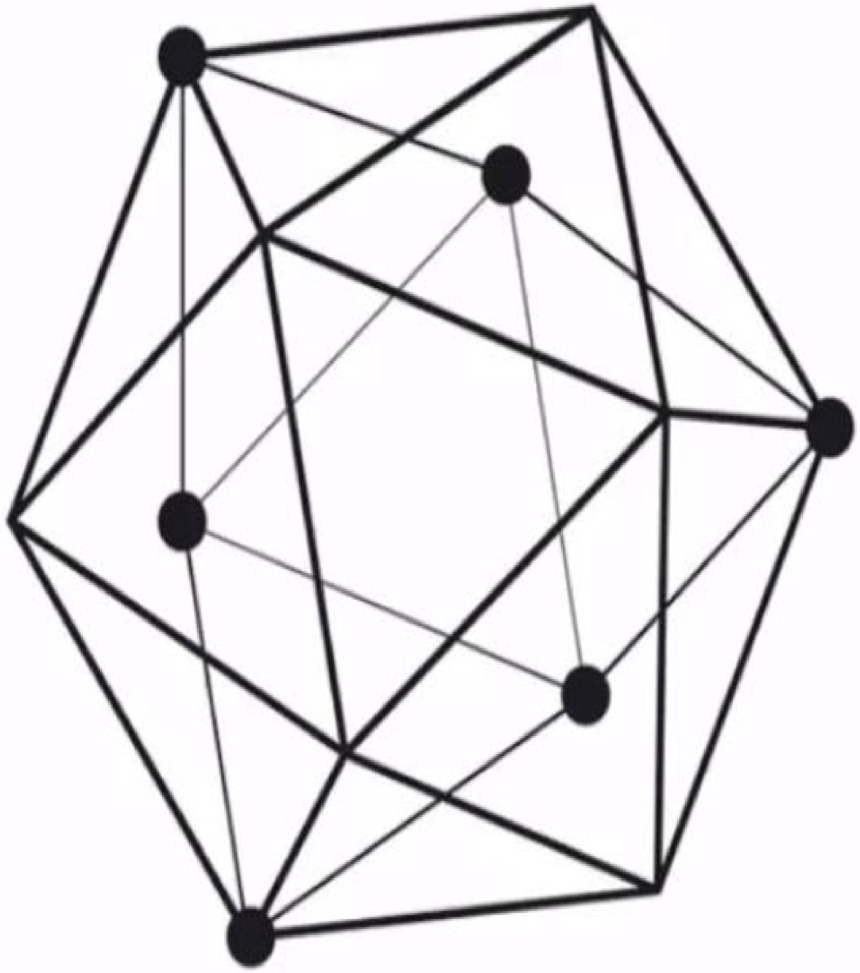
Hyperledger–Greenhouse of BC applications!!

- Linux Foundation first came up with the concept of Hyperledger.
- It’s an umbrella project and also open-source. More so, it comes with loads of free tools and frameworks for you to try out.
- Basically, these tools, libraries are made for enterprises and developers to help them build a new blockchain solution based on that.
- Also, you get access to a very large community that will help you out in terms of developing new revolutionary technologies. Anyhow, Hyperledger came into existence back in 2015, and it came a long way with 16 new projects under it.

“Hyperledger is an open sourced community of communities to benefit an ecosystem of Hyperledger based solution providers and users focused on blockchain related use cases that will work across a variety of industrial sectors.” –

Brian Behlendorf

(Executive Director, Hyperledger)



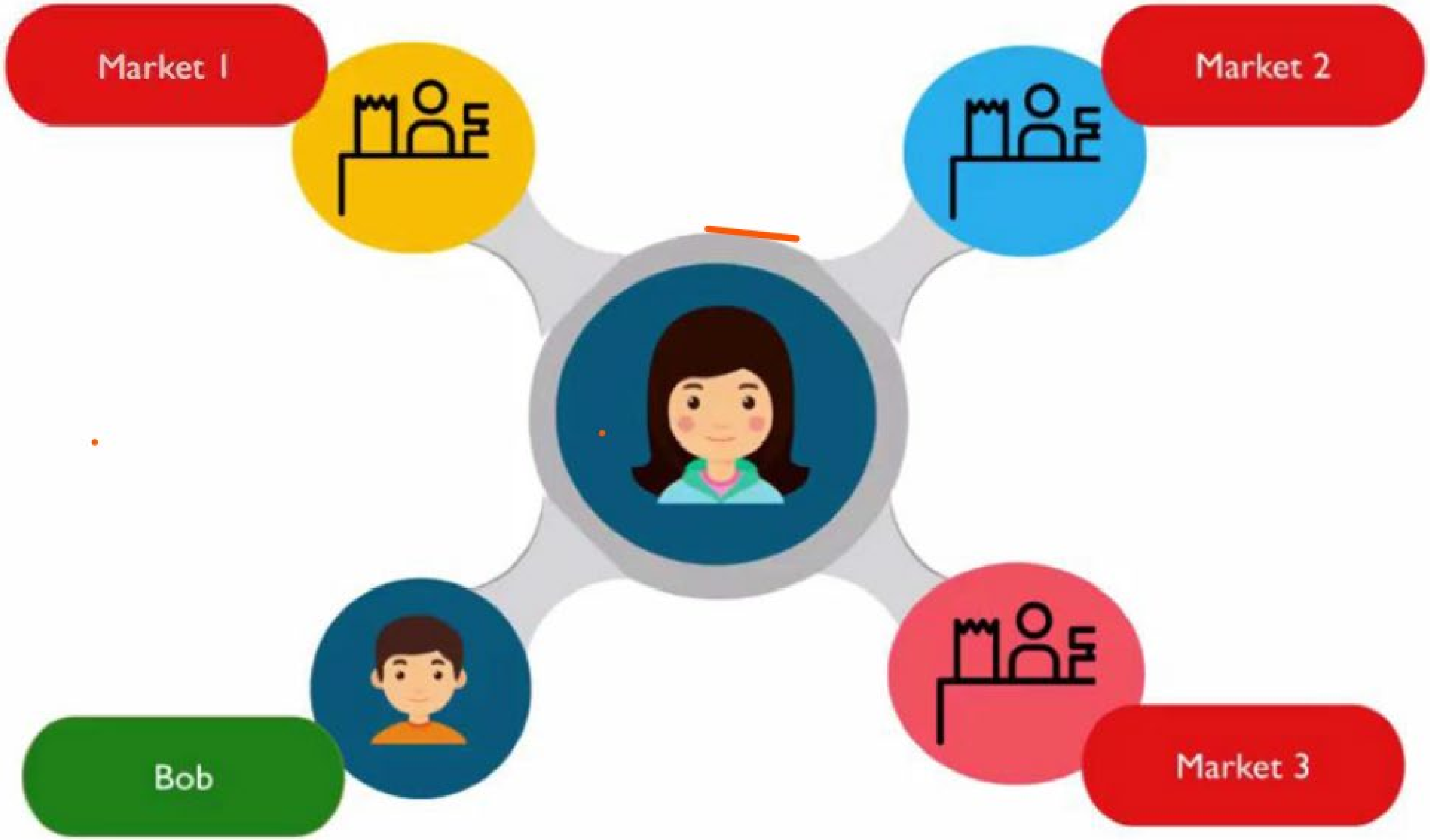
Restrictions

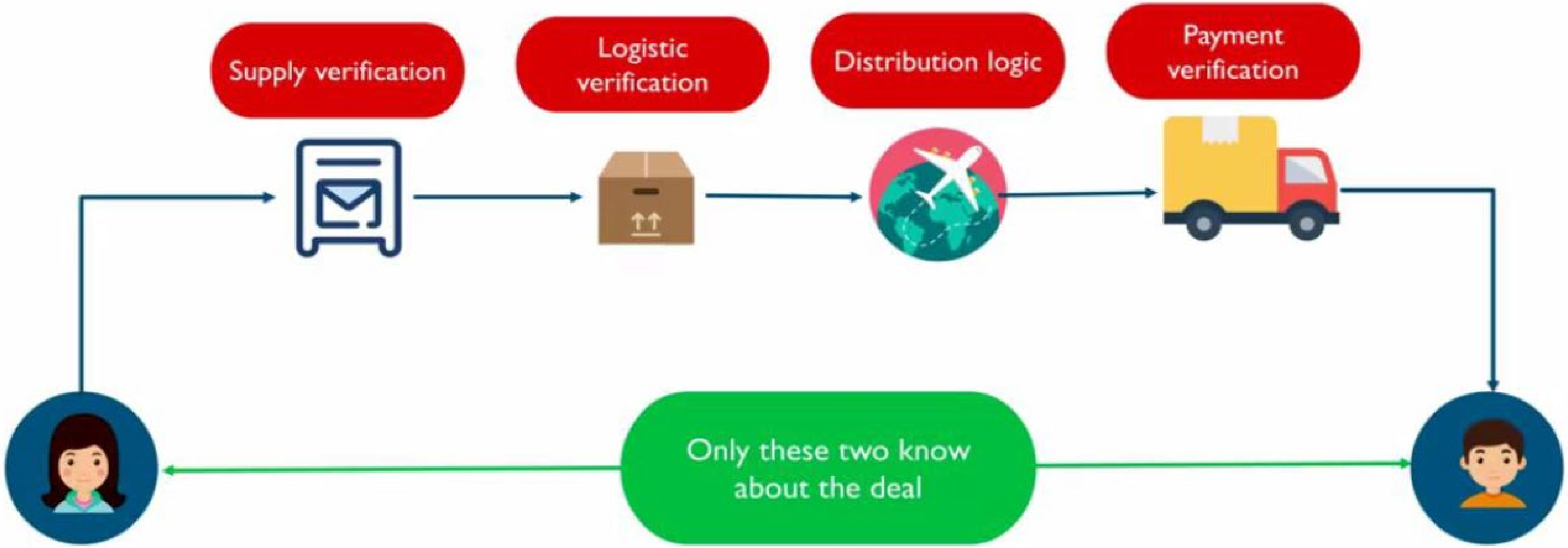
"Public blockchains requires each peer to execute each and every transaction and run 'consensus' at the same time" are….

Not Scalable

Do not support Private and Confidential transactions

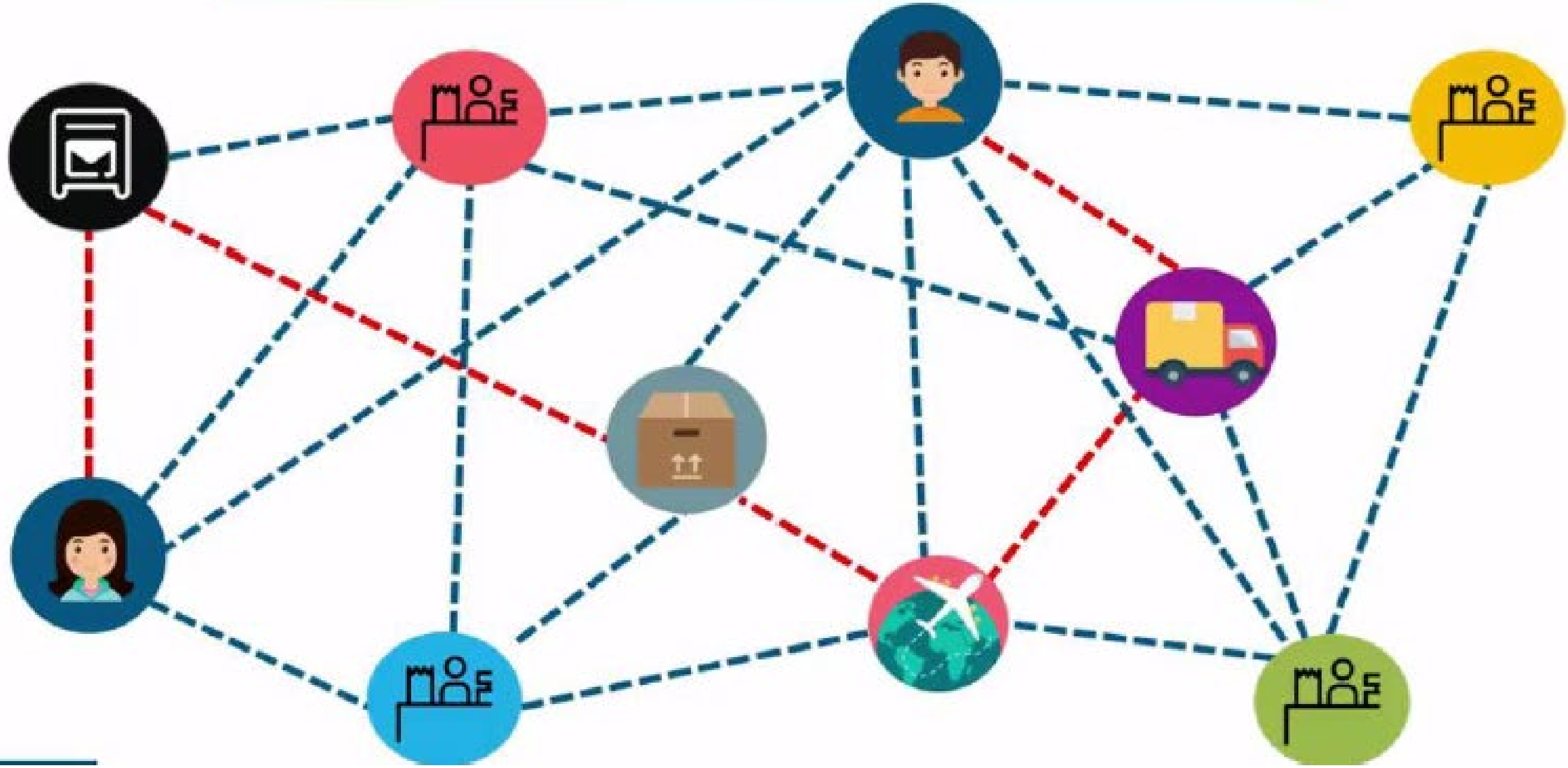
But Alice has a Big Market




Supply verification
Logistic verification
Distribution logic
Payment verification
Only these two know about the deal

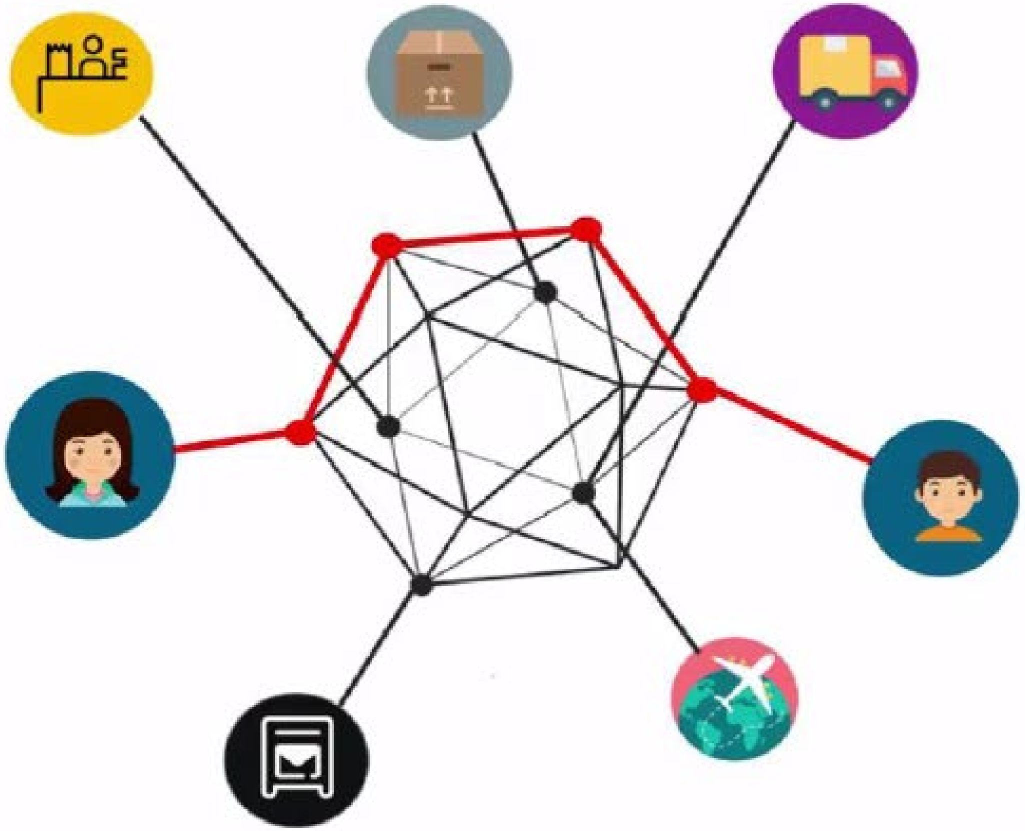
On a Public Blockchain

Every ledger will be updated about Alice and Bob's special deal

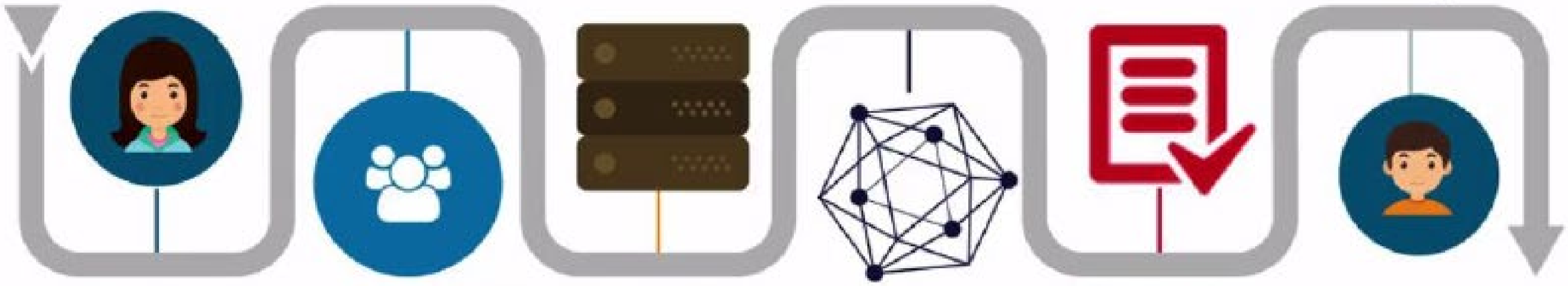


The Hyperledger Way

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



How it works?



Alice Sends

Alice decides to send Bob her product

App Query

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

Membership Service

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

Hyperledger

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

Verification

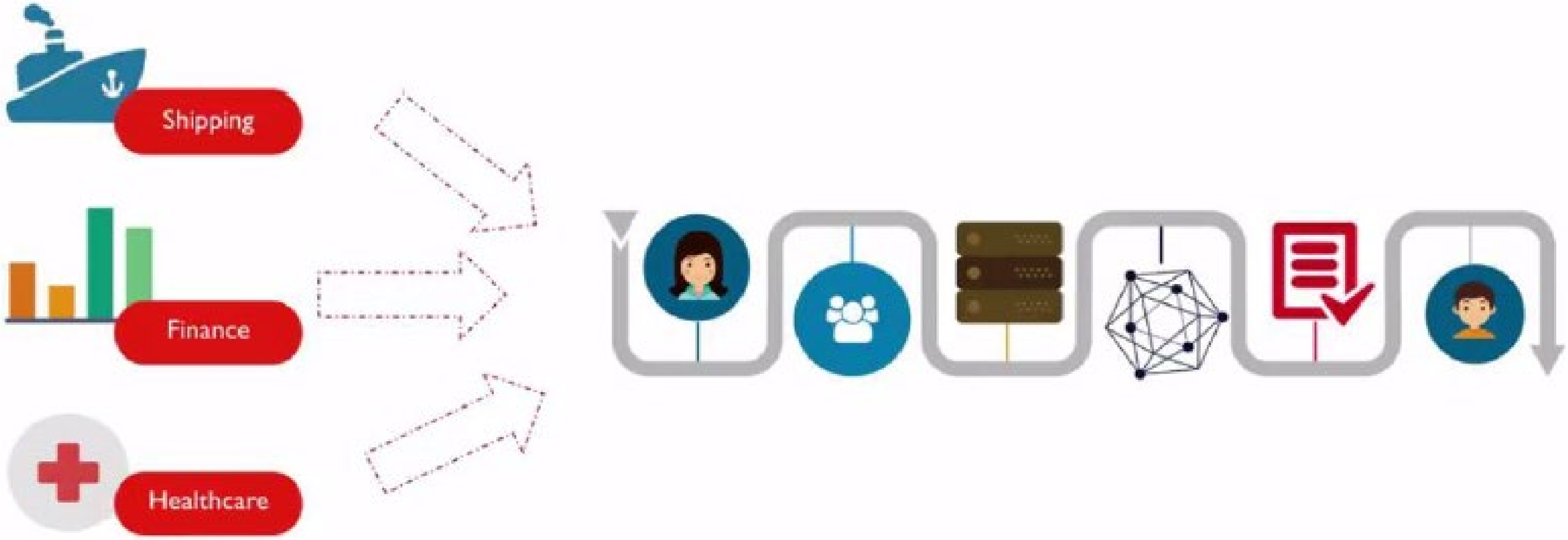
Both parties generate a result which are then sent to the consensus cloud to be ordered and verified

Bob Receives

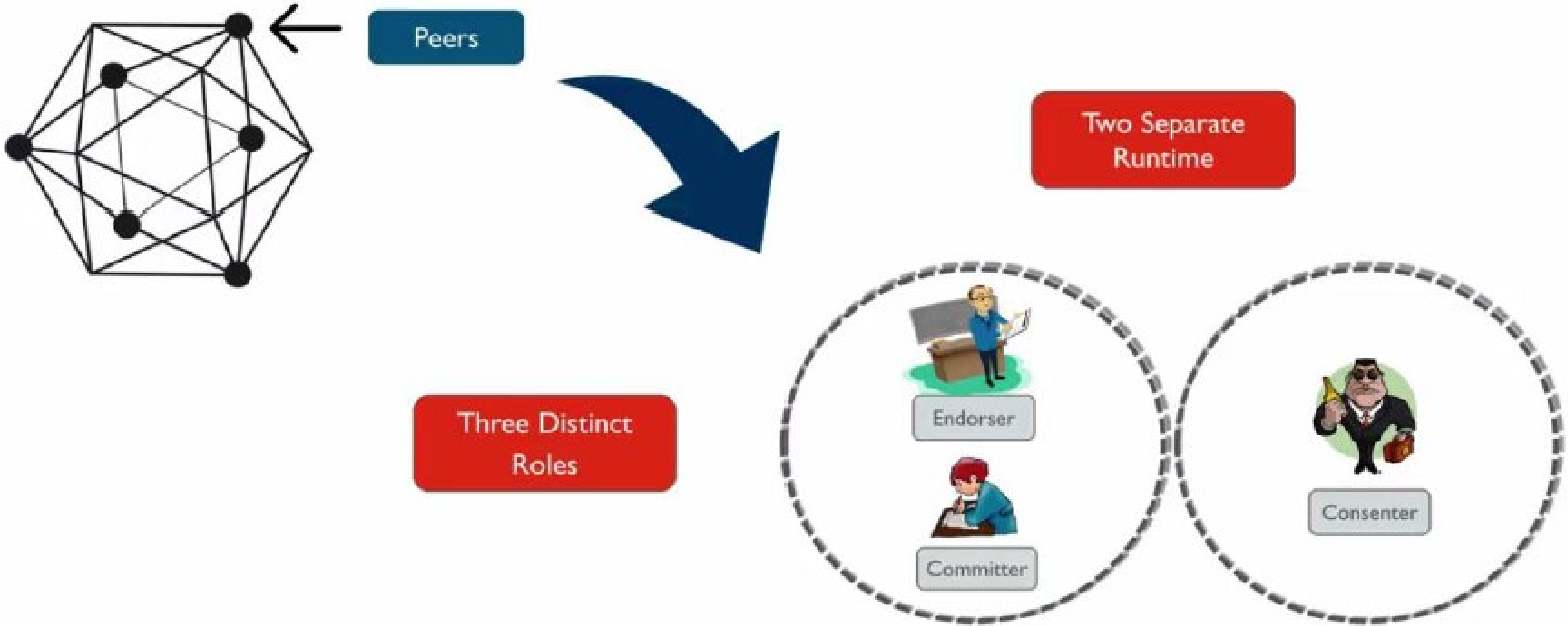
Once the consensus cloud validates the transaction, Bob receives his product and the transactions are committed to the ledger

Pattern Matching

This same pattern is needed by a lot of industries where confidential obligations are need to be met without passing everything through a central authority.



Notable Changes



Peers

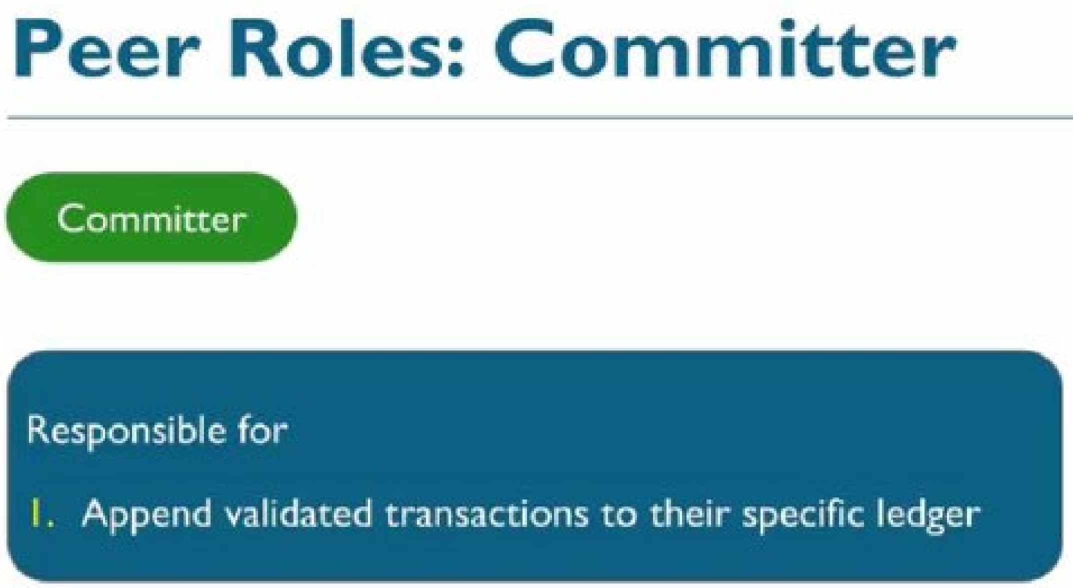
Two Separate Runtime

Three Distinct Roles

Endorser

Committer

Consenter



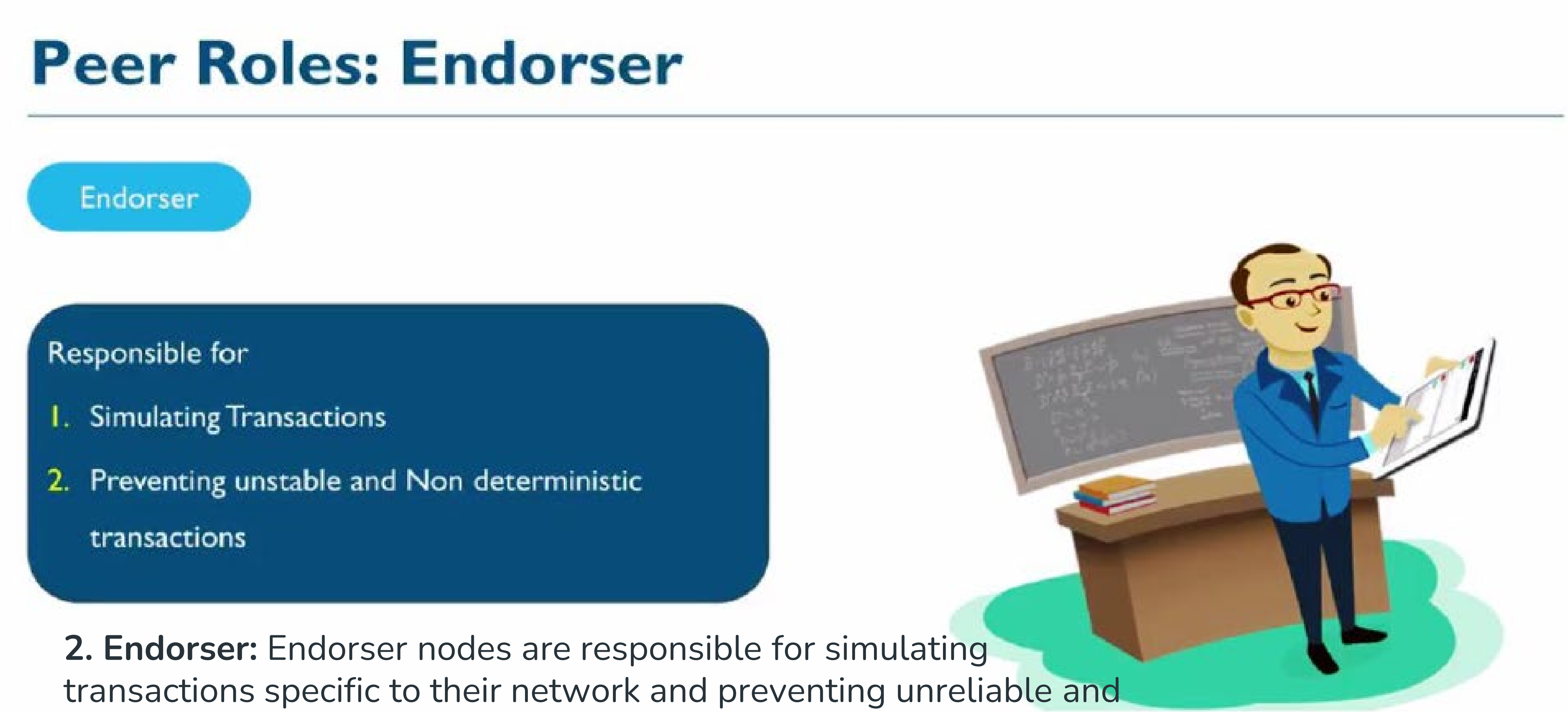
Peer Roles: Committer

Committer

Responsible for

1. Append validated transactions to their specific ledger

1.Committer: Appends validated transactions to their specific ledger. They only add the transaction to the specific ledger once the transaction is returned by the consenter.



Peer Roles: Endorser

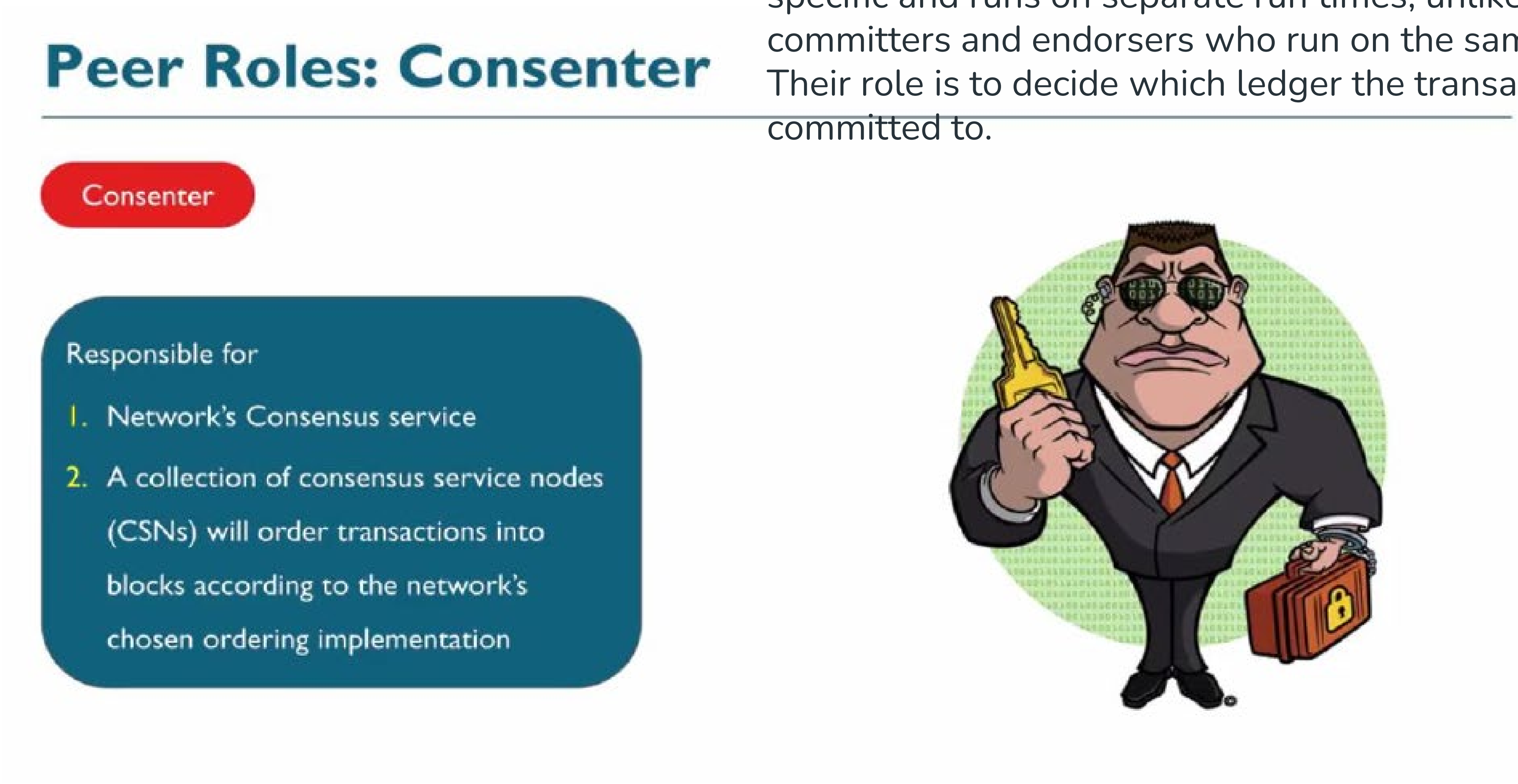
Endorser

Responsible for

1. Simulating Transactions
2. Preventing unstable and Non deterministic transactions

2. Endorser: Endorser nodes are responsible for simulating transactions specific to their network and preventing unreliable and non-deterministic transactions. All endorsers act as committers on the other hand committer may or may not be endorsers depending on network restrictions.

3. Consenter: Their role is to validate the transaction by verifying the result produced by the affiliated peers who want to proceed with a transaction. Their role is very specific and runs on separate run times, unlike committers and endorsers who run on the same run time. Their role is to decide which ledger the transaction be committed to.



Peer Roles: Consenter

Consenter

Responsible for

1. Network's Consensus service
2. A collection of consensus service nodes (CSNs) will order transactions into blocks according to the network's chosen ordering implementation

How Hyperledger Differs

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

Hyperledger Projects

- Hyperledger provides the platform to create personalized blockchain services according to the need of business work. Unlike other platforms for developing blockchain-based software, Hyperledger has the advantage of creating a secured and personalized blockchain network.
- It is created to support the development of blockchain-based distributed ledgers.
- It includes a variety of enterprise-ready permissioned blockchain platforms.
- It is a global collaboration for developing high-performance and reliable blockchain and distributed ledger-based technology frameworks.

https://www.geeksforgeeks.org/introduction-of-hyperledger/

Why Hyperledger Project

Below are some of the reasons stating the need for a hyperledger project:

- To enhance the efficiency, performance, and transactions of various business processes.
- It provides the necessary infrastructure and standards for developing various blockchain-based systems and applications for industrial use.
- It gets rid of the complex nature of contractual agreements, as the legal issues are taken care of.
- Hyperledger offers the physical separation of sensitive data.
- It decreases the need for verification and enhances trust, thus optimizing network performance and scalability.

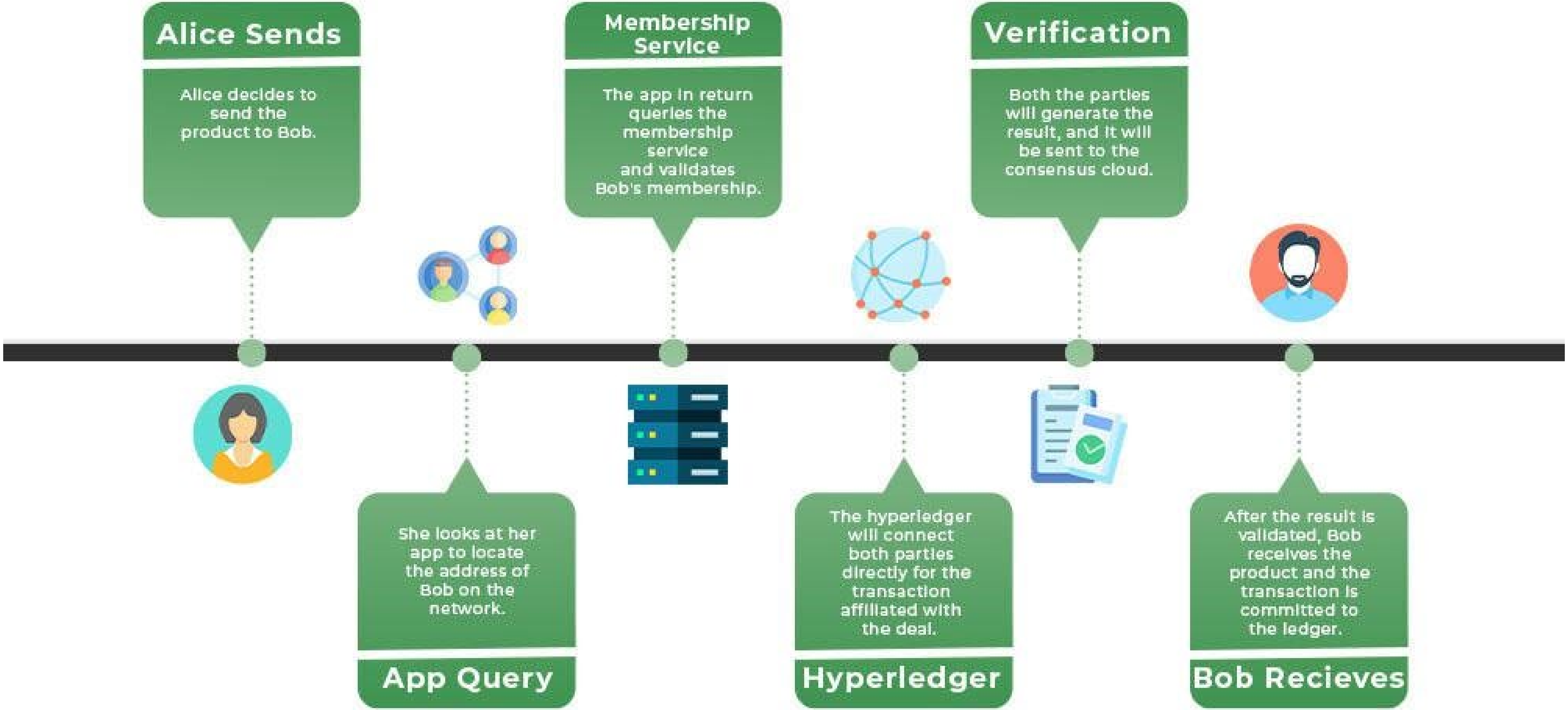
Hyperledger Technology Layers

Hyperledger uses the following key business components:

1. **Consensus layer:** It takes care of creating an agreement on the order and confirming the correctness of the set of transactions that constitute a block.
2. **Smart layer:** This layer is responsible for processing transaction requests and authorizing valid transactions.
3. **Communication layer:** It takes care of peer-to-peer message transport.
4. **Identity management services:** these are important for establishing trust on the blockchain.
5. **API:** It enables external applications and clients to interface with the blockchain.

How Does Hyperledger Work?

- Hyperledger works in a way that a requirement for the contract can be initiated through an application.
- The membership service involved in the network validates the contract.
- The concerned two-peer has to produce a result and then sent it to the consensus cloud.
- The generated result from both the peer has to be the same in order to validate the contract.
- Once it is validated, then the transaction will happen between the affiliated peers and their ledger will be updated.
- When a business requires confidentiality and a private network for its transaction to happen without doing that in a single network, a hyperledger paves the way.



Alice Sends

Alice decides to send the product to Bob.

App Query

She looks at her app to locate the address of Bob on the network.

Membership Service

The app in return queries the membership service and validates Bob's membership.

Hyperledger

The hyperledger will connect both parties directly for the transaction affiliated with the deal.

Verification

Both the parties will generate the result, and it will be sent to the consensus cloud.

Bob Recieves

After the result is validated, Bob receives the product and the transaction is committed to the ledger.

Hyperledger Projects

Hyperledger Architecture

https://101blockchains.com/hyperledger-tutorial/

- **Modular Design**
- All of the projects under Hyperledger come with a modular design. Basically, the modular design makes sure that all of the frameworks are extensible in every way. Anyhow, they typically use common standards in building blocks that are suited for any kind of scenario.
- More so, the modular structure helps in the Hyperledger developer tutorial as they can experiment with it without affecting all other codes.
- It's a great strategy in making the distributed ledger technology as you can reuse any other model previously built.

Hyperledger Architecture

- **Extremely Secure Platform**
- It's one of the important factors of any kind of blockchain platform. In many cases, enterprises deal with a high level of sensitive information. And that information needs a high level of security by all means.
- But it can become difficult to maintain full security when you are dealing with a lot of data flows and codebases. Thus, Hyperledger introduces a new form of security by using the immutability and decentralized nature of the blockchain.
- According to, Hyperledger developer tutorial, all of their projects go through vigorous testing to figure out any loopholes in the system. Thus, it ensures that no hackers can get access to the network and manipulate your data.
- More so, according to their Hyperledger developer tutorial, they also have added layers of blockchain security to help you harness the power.
- Another great news is that all of their codebases go through regular auditing to see any discrepancies in them. If they manage to find any, it's immediately solved.

Hyperledger Architecture

- **Interoperable**
- Blockchain technology needs to be interoperable in order to get into every aspect of our lives. However, without interoperability, there's no chance it can work. So, when multiple networks can communicate with each other and exchange data, all of them can work more efficiently.
- Thus, Hyperledger wants to introduce blockchain interoperability to help make all the applications and other contracts portable to any kind of device. More so, it would connect all of our industries to one hub where everything is connected.
- Using the interconnected data streams, efficiencies would skyrocket, and it would save a lot of time as well.

Hyperledger Architecture

- **Cryptocurrency-agnostic**
- The best part about this platform is that it doesn’t have any kind of cryptocurrency to help run the system. Basically, in other platforms, you see a form of token or cryptocurrency that they use to use certain functions of the network.
- But not in Hyperledger. In reality, all the projects under it are cryptocurrency-agnostic. But why, though? Well, because Hyperledger believes in the core technology and doesn’t want to administrate any cryptocurrencies on the platform.
- However, as many of the enterprises may need a digital form of money, they’ll give you an option to issue your very own token on the platform.

Hyperledger Architecture

- **High-end API Support**
- According to, Hyperledger developer tutorial, all of their projects include high-end API support. More so, every single API from their solutions offers the best of the best blockchain features, and all of them can handle interoperability.
- Anyhow, Hyperledger APIs will help you communicate with their core network from any external client program and network. Most importantly, it helps out all of the distributed ledgers to bloom properly and be capable of handling many other use cases.

Hyperledger Fabric

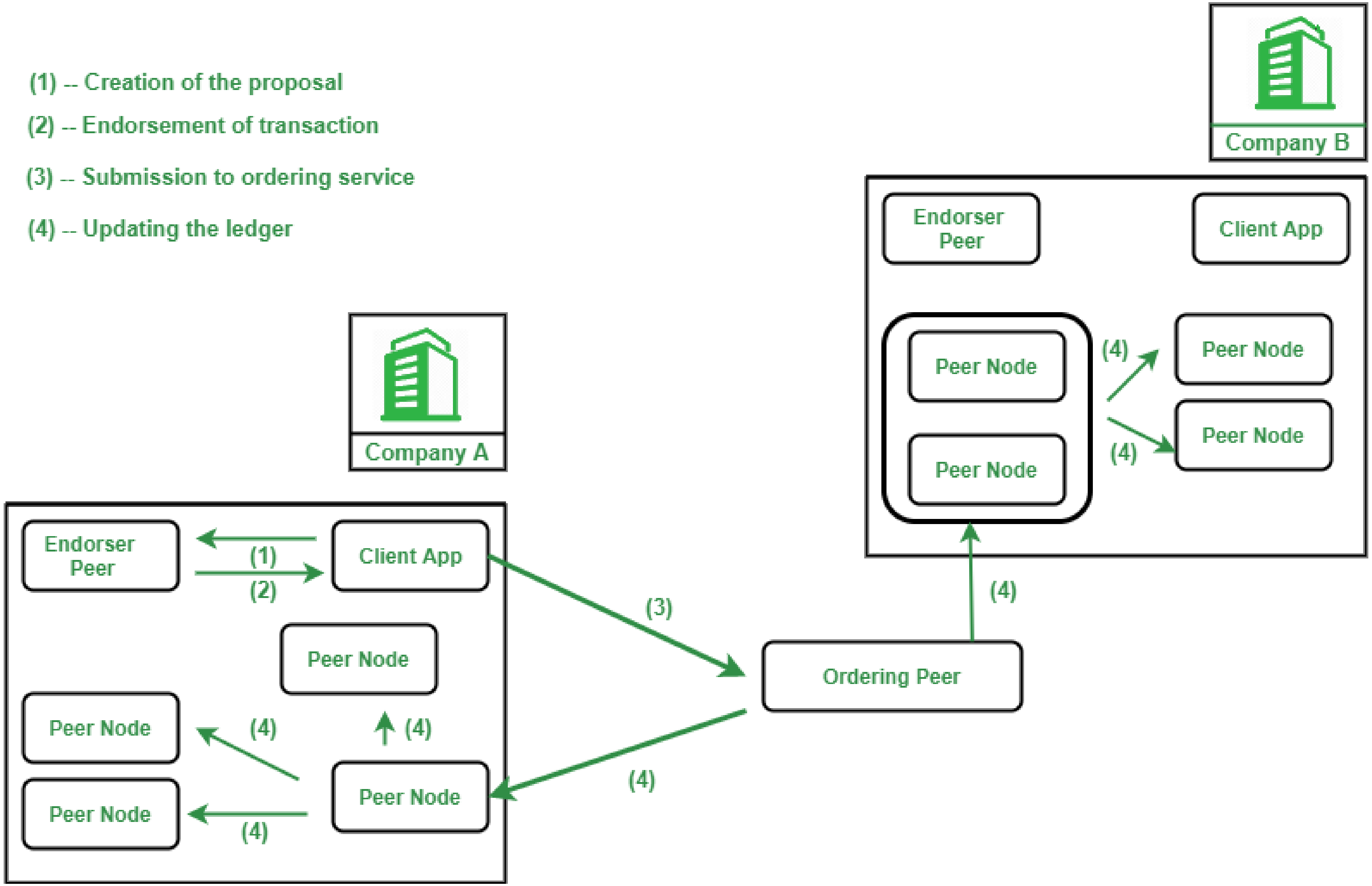
- Hyperledger Fabric is an open-source enterprise-grade framework. It relies on permissioned distributed ledger technology to provide much-needed applications and solutions. Linux Foundation is working on a diverse number of projects, and Hyperledger Fabric is one of them.
- As it is open-source, anyone can join the project and contribute to it. At the core, Hyperledger Fabric is configurable and modular. This means that enterprises can work seamlessly using the framework. All of these desirable features make Hyperledger Fabric a great choice! At the time of writing, you can try out the Hyperledger Fabric 2.0, which comes with new features and functionalities.

(1) -- Creation of the proposal

(2) -- Endorsement of transaction

(3) -- Submission to ordering service

(4) -- Updating the ledger

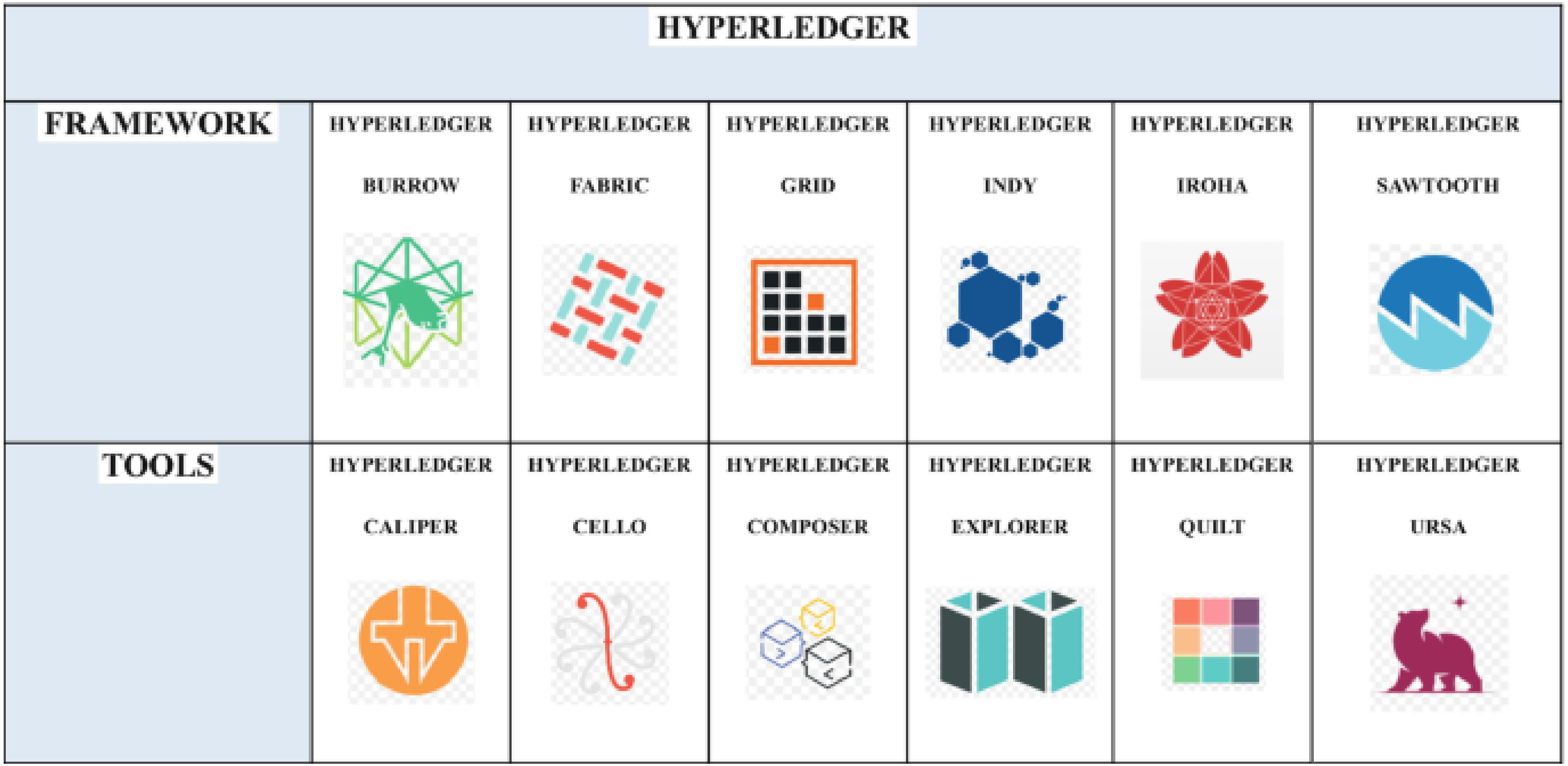


Hyperledger Fabric Features

- **Identity Management:** Identity management is crucial to any permissioned network. That's why digital identity management is one of the crucial features in the Hyperledger Fabric. By giving the administrator to set proper identity management, enterprises can make sure that they employ multiple layers of permission.
- **Efficient processing:** Hyperledger Fabric is efficient. This is because network roles are assigned as node types. The efficiency is also provided by letting transaction execution separately from commitment and ordering.
- **Modular Design:** Hyperledger Fabric utilizes modular design, which means that it is easy to integrate services or other systems into it. This also means that you can specify the consensus algorithm, identity, and so on.
- **Privacy and confidentiality:** Hyperledger Fabric also offers proper confidentiality and privacy, which is very important for enterprises. They offer proper data channels so that information doesn't leak and confidentiality can be maintained at any cost.
- **Chaincode functionality:** Hyperledger Fabric offers chaincode functionality, which enables logic to be invoked only when a specific type of transaction is called.

Fabric Transactions

- The transactions on Hyperledger Fabric can be of two types:
- **Deploy transactions:** This type of transaction is responsible for creating a new chaincode with a parameter as a program. Once done, the chaincode is said to be “installed” on the blockchain.
- **Invoke transactions:** The invoke transactions are transactions that are executed in the context of previous chaincode or smart contracts deployment.



HYPERLEDGER						
FRAMEWORK	HYPERLEDGER BURROW	HYPERLEDGER FABRIC	HYPERLEDGER GRID	HYPERLEDGER INDY	HYPERLEDGER IROHA	HYPERLEDGER SAWTOOTH
TOOLS	HYPERLEDGER CALIPER	HYPERLEDGER CELLO	HYPERLEDGER COMPOSER	HYPERLEDGER EXPLORER	HYPERLEDGER QUILT	HYPERLEDGER URSA

1. **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.
2. **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.
3. **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.

4. 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.

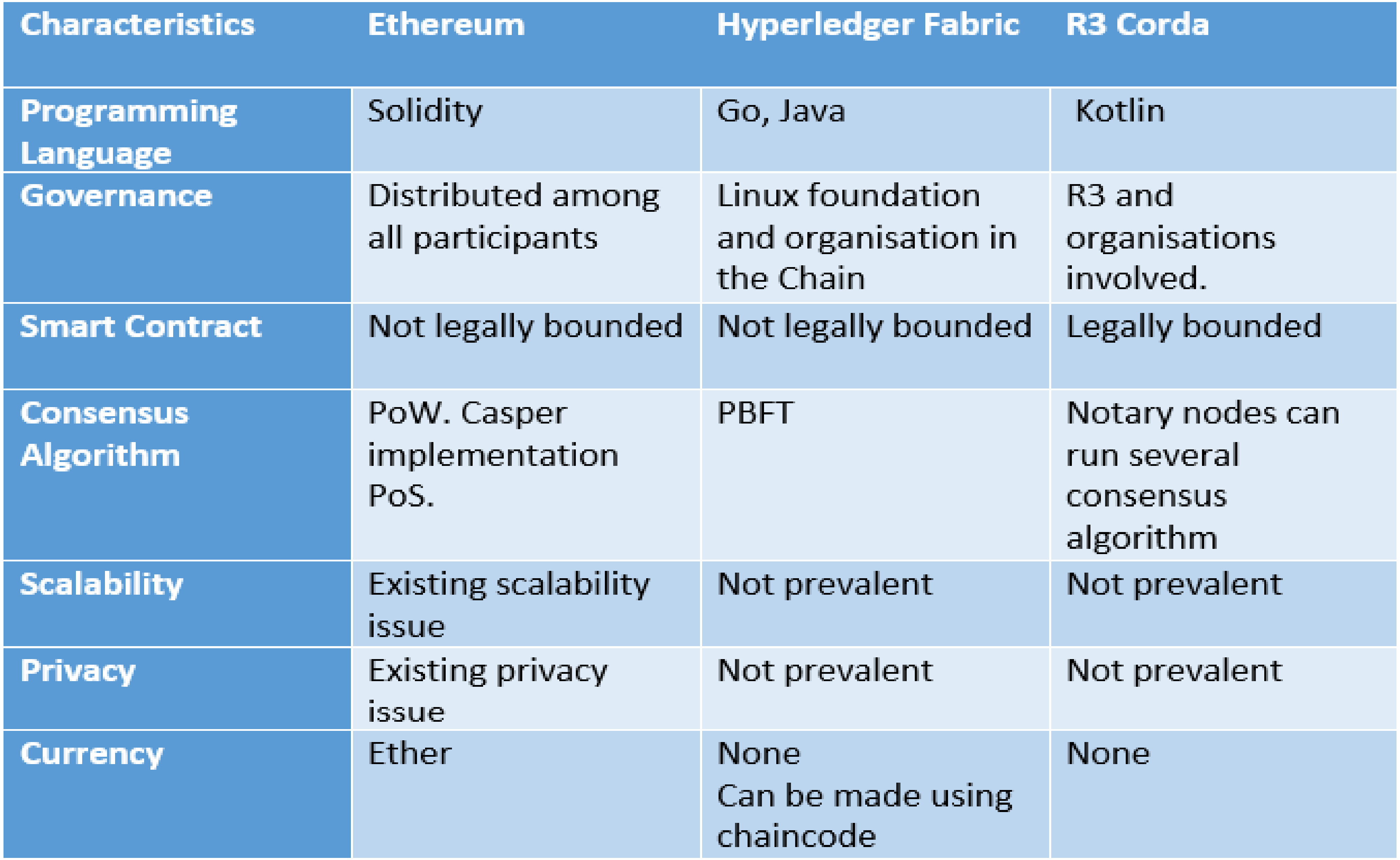
5. **Hyperledger Burrow:** It is a framework for executing smart contracts in permissioned blockchains. The goal of Hyperledger burrow is to facilitate cross-industry applications for smart contracts. It is built around the BFT consensus algorithm.

6. **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.

7. 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.

8.**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.

9. 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.



Characteristics	Ethereum	Hyperledger Fabric	R3 Corda
Programming Language	Solidity	Go, Java	Kotlin
Governance	Distributed among all participants	Linux foundation and organisation in the Chain	R3 and organisations involved.
Smart Contract	Not legally bounded	Not legally bounded	Legally bounded
Consensus Algorithm	PoW. Casper implementation PoS.	PBFT	Notary nodes can run several consensus algorithm
Scalability	Existing scalability issue	Not prevalent	Not prevalent
Privacy	Existing privacy issue	Not prevalent	Not prevalent
Currency	Ether	None Can be made using chaincode	None

Hyperledger Library Ursa

Type: Library

- Hyperledger Ursa is a shared cryptographic library, it enables implementations to avoid duplicating other cryptographic work and hopefully increase security in the process.
- The library is an opt-in repository (for Hyperledger and non Hyperledger projects) to place and use crypto.
- Hyperledger Ursa consists of sub-projects, which are cohesive implementations of cryptographic code or interfaces to cryptographic code.

Hyperledger Library Ursa

- As Hyperledger has matured, the individual projects within Hyperledger have started to find a need for sophisticated cryptographic implementations. Rather than have each project implement its own cryptographic protocols, we think it would be more desirable to collaborate on a shared library. There are many reasons to do this:
- **Avoiding duplication**: crypto implementations are notoriously difficult to get correct (particularly when side channels are taken into account) and often require a lot of work in order to complete with a high level of security. The library would potentially allow projects to share crypto implementations, avoiding unnecessary duplication and extra work.
- **Security**: having most (or all) of the crypto code in a single location would substantially simplify doing a security analysis of the crypto portion of Hyperledger. In addition, the lack of duplication would mean that maintenance would be easier (and thus, hopefully, security bugs would be less numerous). People might also be less likely to “roll their own crypto” if there are easily accessible implementations.

Hyperledger Library Ursa

- **Expert Review**: In addition, the ability to enforce expert review of all cryptographic code should increase security as well. There has already been at least one substantial bug in a Hyperledger DLT platform at a cryptographic algorithm level. We think that having a concentration of cryptographic experts in Hyperledger will help us minimize the risk of this in the future.
- **Cross-platform interoperability**: if two projects use the same crypto libraries, it will simplify (substantially in some cases) cross-platform interoperability, since cryptographic verification will involve the same protocols on both sides.
- **Modularity**: This could be the first common component/module and a step towards modular DLT platforms, which share common components. While we have already outlined most of the advantages this modularity would bring in terms of actual functionality, a successful crypto library could encourage and push forward more modular activities.
- **New Projects**: It would be easier for new projects to get off the ground if they had easy access to well-implemented, modular cryptographic abstractions.

Blockchain-as-a-Service

- KEY TAKEAWAYS
- Blockchain-as-a-service (BaaS) refers to third-party cloud-based infrastructure and management for companies building and operating blockchain apps.
- BaaS functions like a sort of web host, running the back-end operation for a block-chain based app or platform.
- BaaS may be the catalyst that leads to the widespread adoption of blockchain technology.

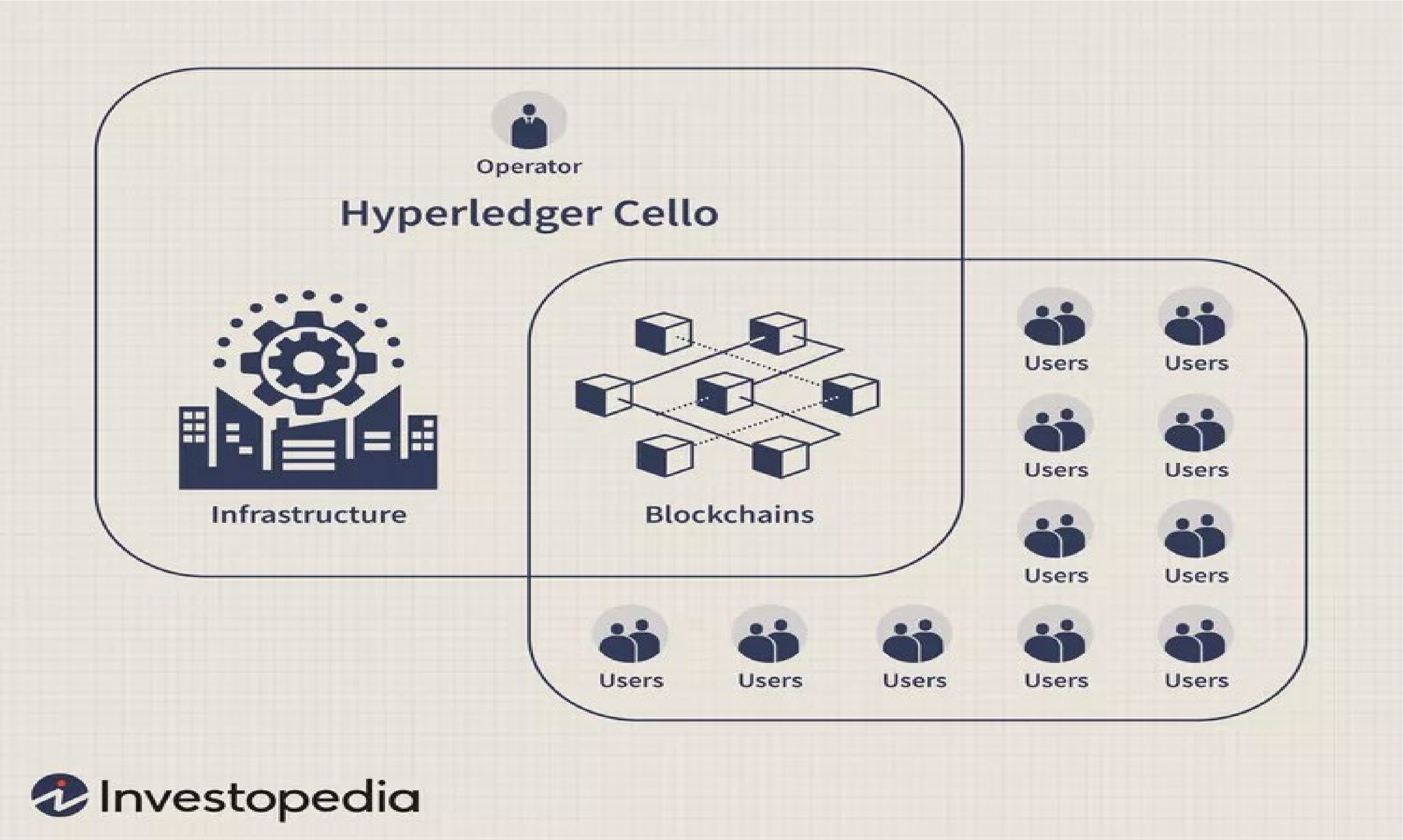
Blockchain-as-a-Service - Providers

- Microsoft, which partnered with ConsenSys to introduce Ethereum blockchain-as-a-service on Microsoft Azure in 2015.[1]
- Amazon, which has introduced Amazon Managed Blockchain, a service that "makes it easy to create and manage scalable blockchain networks" using open source frameworks including Ethereum and Hyperledger Fabric.[2]
- R3, a consortium of global financial institutions that produced a distributed financial ledger called Corda.[3]
- PayStand, which specializes in sending and receiving payments between companies.[4]

Blockchain-as-a-Service

- Consumers and businesses are increasingly willing to adapt to blockchain technology. However, the technical complexities and operational overhead involved in creating, configuring, and operating a blockchain and maintaining its infrastructure often act as a barrier.
- BaaS offers an external service provider to set up all the necessary blockchain technology and infrastructure for a fee. Once created, the provider continues to handle the complex back-end operations for the client.
- The BaaS operator typically offers support activities, such as bandwidth management, suitable allocation of resources, hosting requirements, and data security features. The BaaS operator frees the client to focus on the core job: the functionality of the blockchain.

Example of Blockchain-as-a-Service (BaaS)



Blockchain-as-a-Service - Cello

- In fact, a BaaS’ provider's role is similar to that of a web hosting provider. The website creators create and run all the website content on their own personal computers. They may hire support staff or sign up with an external hosting provider like Amazon Web Services or HostGator. These third-party companies take care of the infrastructure and maintenance issues.
- BaaS may be the catalyst that leads to a wider and deeper penetration of blockchain technology across various industry sectors and businesses. Instead of creating and running their own blockchains, a business, large or small, can now simply outsource the technically complex work and focus on its core activities.

Blockchain Security

Like in real life, your wallet must be secured. Bitcoin makes it possible to transfer value anywhere in a very easy way and it allows you to be in control of your money. Such great features also come with great security concerns. At the same time, Bitcoin can provide very high levels of security if used correctly.

Always remember that it is your responsibility to adopt good practices in order to protect your money.

Bitcoin Attacks Reality

- Bitcoins and other cryptocurrencies have cryptography built into their protocol, meaning that they use strong encryption to verify transactions and to guard against cheats trying to manipulate the system.
- But there are security issues that you need to be aware of before you starting buying bitcoins.
- The protocol may be secure, but not all of the services that deal in bitcoin can be trusted to be secure – or honest.
- There have been several high profile security breaches that have resulted in huge amounts of bitcoins being stolen.
- In 2013, a bitcoin wallet service called inputs.io was hacked. Using a social engineering attack, hackers gained access to their system and stole 4,100 bitcoins, worth at the time about $1.2 million.
- In 2014, bitcoin exchange server Mt. Gox was the largest bitcoin intermediary in the world. Then it announced that approximately 850,000 bitcoins had been lost. While it later managed to retrieve 200,000 of the missing coins, the company went bankrupt and its users were left out of pocket.
- In 2016, Hong Kong-based exchange Bitfinex lost about $65m in a cyber-attack.
- Bitcoin wallets are also vulnerable. In July 2017 ethereum, the second largest cryptocurrency, was attacked by hackers who exploited a programming flaw in the currency’s wallets to steal the equivalent of $31m.

Bitcoin Security Threats

Wallet Attacks

❑ All Bitcoins are stored in digital software called a wallet. There are several of these wallets that people can use, ranging from online, desktop, mobile, and hardware ones.

❑ One of the major security issues facing BTC is the wallets, especially the online ones that are very vulnerable to attacks, thereby requiring encryption and offline backup.

❑ The available backup systems enable users to recover old wallet files. Hackers can quickly attack these wallets using their high-tech malware knowledge and steal massive amounts of Bitcoin.

❑ This affects users as their funds can be sidetracked to different accounts.

❑ Hardware wallets are less vulnerable to such attacks and are considered the safest for BTC storage.

❑ All you need to access them is your private key, and since they're offline, no one can access them from the internet.

Bitcoin Security Threats

Timejacking Attacks

- These occur when an attacker broadcasts incorrect timestamps when linking to a transaction node.
- The node’s network time counter is changed, and it may accept a different blockchain.
- This action results in severe impacts like double-spending and loss of mining computational resources.
- Though very hard to happen as it involves breaking into the blockchain, Bitcoin’s most secure system when it does occur, the consequences are enormous.

Bitcoin Security Threats

Over 50% Attack = 51% attack

❑ The >50% attack, also called the 51% attack, is an issue that affects Bitcoin, though, with limited possibility to occur. It targets the mining process mainly. It results when any user or group obtains over 50% of the mining process's computing power. The user or group can then transform, eliminate, and undo transactions and bar some or all mining of authentic blocks for their benefit.

❑ The mining difficulty has made it necessary for it to be done in pools. Some of these have high computational power, meaning if they reach the 51% mark, they can misuse it and manipulate transactions through mining void blocks or double-spending. This can make stand-alone miners or those in small pools to shy away. It also declines the consensus protocol.

❑ A possible remedy to this security concern is to create checkpoints to prevent altering the blocks before checkpoints. If the attack succeeds, others can be launched too, and the changes made will be permanent and difficult to handle. Double spending alerts can also be relayed among peers, and large pools disincentivized to reduce this type of attack.

Bitcoin Security Threats

Double Spending

- ❑ It’s also called the Race attack and involves spending the same BTCs in numerous transactions and sending two conflicting transactions successively. It majorly targets sellers or merchants, leading to the loss of their products. It also scares honest users from exploiting the investment and establishes blockchain forks.
- ❑ The severe threat is most likely to happen in the “fast payment” mode. The hacker makes a transaction with Coin B to a receiver and another one with the same coin to a different address or receiving node in his control. Making the fraud real involves varying the timestamp. No Bitcoin peer accepts numerous transactions with the same input, meaning that the first transaction to reach the peer will be validated, while others invalidated. The original receiver won’t confirm the transaction, and there’s no way to adjust this once the validation process is complete.
- ❑ Some possible solutions include; – introducing “observers” in the network, peer double-spending communication notifications, and disabling any direct incoming connections by merchants. It’s noteworthy that Bitcoin is increasing its sturdiness against this threat and has reinforced some measures to mitigate it.

Bitcoin Security Threats

Selfish Mining

❑Bitcoin’s continued use of proof-of-work consensus mechanism has another underlying threat. With some mining pools becoming powerful enough to command significant mining ratios, they may engage in selfish mining.

❑Also called block withholding, a pool may use their computational power to mine a block and then hide it from honest miners instead of broadcasting the new block to the network.

❑The selfish pool then attempts to find the second block while the rest grope in the dark. If the greedy miners manage to find a new block before the other miners, then broadcasting the two blocks makes the forked chain the longest. The selfish miners will be ahead of the other miners, getting all the rewards.

❑Such conspiracies, on a large scale, can be combined with the Sybil attack to cause considerable harm to mining because selfish miners can then use their power to invalidate transactions on the network.

Bitcoin Security Threats

Distributed Denial of Service (DDoS) Attacks and Cyber-Attacks

- ❑ Bitcoin is also surrounded by security issues that target exchanges and online platforms.
- ❑ These cyber-attacks can cripple the currency more than any other since most users transact and even store their coins on some platforms.
- ❑ Like the Bitcoin heists that have occurred in the past, possible hacking of exchanges means a massive loss of Bitcoins.
- ❑ It leaves the exchanges bankrupt as the funds stolen are never recoverable.
- ❑ Most exchanges have also become targets of DDoS attacks, with some reporting having faced such occurrences repeatedly.

Bitcoin Security Threats

Fraudulent Exchanges

❑ There are numerous online exchanges or sites for buying and selling Bitcoin.

❑ Are all of them legit? Not all exchanges you see on the internet are legitimate. Some operate fraudulently and are havens for financial scams.

❑ It’s prudent to always research on the trusted Bitcoin platforms before engaging with any. Some of the reliable and authentic ones are CoinBase, Binance, CoinMama, and Bitifinex; you can’t get anything wrong with them.

❑ This threat isn’t a major one, but if you’re new into the investment, you can be a real target of such scams.

Bitcoin Defense Be careful with online services

- ❑You should be wary of any service designed to store your money online.
- ❑Many exchanges and online wallets suffered from security breaches in the past and such services generally still do not provide enough insurance and security to be used to store money like a bank.
- ❑ Accordingly, you might want to use other types of Bitcoin wallets.
- ❑ Otherwise, you should choose such services very carefully. Additionally, using two-factor authentication is recommended.

Bitcoin Defense Small amounts for everyday uses

- ❑A Bitcoin wallet is like a wallet with cash. If you wouldn't keep a thousand dollars in your pocket, you might want to have the same consideration for your Bitcoin wallet.
- ❑In general, it is a good practice to keep only small amounts of bitcoins on your computer, mobile, or server for everyday uses and to keep the remaining part of your funds in a safer environment.

Bitcoin Defense Backup your Wallets

- ❑ Stored in a safe place, a backup of your wallet can protect you against computer failures and many human mistakes. It can also allow you to recover your wallet after your mobile or computer was stolen if you keep your wallet encrypted.
- ❑ Backup your entire wallet
- ❑ Some wallets use many hidden private keys internally. If you only have a backup of the private keys for your visible Bitcoin addresses, you might not be able to recover a great part of your funds with your backup.
- ❑ Encrypt online backups
- ❑ Any backup that is stored online is highly vulnerable to theft. Even a computer that is connected to the Internet is vulnerable to malicious software. As such, encrypting any backup that is exposed to the network is a good security practice.
- ❑ Use many secure locations
- ❑ Single points of failure are bad for security. If your backup is not dependent of a single location, it is less likely that any bad event will prevent you to recover your wallet. You might also want to consider using different medias like USB keys, papers and CDs.
- ❑ Make regular backups
- ❑ You need to backup your wallet on a regular basis to make sure that all recent Bitcoin change addresses and all new Bitcoin addresses you created are included in your backup. However, all applications will be soon using wallets that only need to be backed up once.

Bitcoin Defense Encrypt your Wallets

❑ Encrypting your wallet or your smartphone allows you to set a password for anyone trying to withdraw any funds. This helps protect against thieves, though it cannot protect against keylogging hardware or software.

❑ Never forget your password

You should make sure you never forget the password or your funds will be permanently lost. Unlike your bank, there are very limited password recovery options with Bitcoin. In fact, you should be able to remember your password even after many years without using it. In doubt, you might want to keep a paper copy of your password in a safe place like a vault.

❑ Use a strong password

Any password that contains only letters or recognizable words can be considered very weak and easy to break. A strong password must contain letters, numbers, punctuation marks and must be at least 16 characters long. The most secure passwords are those generated by programs designed specifically for that purpose. Strong passwords are usually harder to remember, so you should take care in memorizing it.

Bitcoin Defense Offline Wallets for Savings

❑ An offline wallet, also known as cold storage, provides the highest level of security for savings. It involves storing a wallet in a secured place that is not connected to the network. When done properly, it can offer a very good protection against computer vulnerabilities. Using an offline wallet in conjunction with backups and encryption is also a good practice. Here is an overview of some approaches.

❑ Offline transaction signing

This approach involves having two computers sharing some parts of the same wallet. The first one must be disconnected from any network. It is the only one that holds the entire wallet and is able to sign transactions. The second computer is connected to the network and only has a watching wallet that can only create unsigned transactions. This way, you can securely issue new transactions with the following steps.

- ❑ **Create a new transaction on the online computer and save it on an USB key.**
- ❑ **Sign the transaction with the offline computer.**
- ❑ **Send the signed transaction with the online computer.**
- ❑ **Because the computer that is connected to the network cannot sign transactions, it cannot be used to withdraw any funds if it is compromised. Armory can be used to do offline transaction signature.**

❑ Hardware wallets

Hardware wallets are the best balance between very high security and ease of use. These are little devices that are designed from the root to be a wallet and nothing else. No software can be installed on them, making them very secure against computer vulnerabilities and online thieves. Because they can allow backup, you can recover your funds if you lose the device.

Bitcoin Defense Software and Signatures

❑ Keep your software up to date

Using the latest version of your Bitcoin software allows you to receive important stability and security fixes. Updates can prevent problems of various severity, include new useful features and help keep your wallet safe. Installing updates for all other software on your computer or mobile is also important to keep your wallet environment safer.

❑ Multi-signature to protect against theft

Bitcoin includes a multi-signature feature that allows a transaction to require multiple independent approvals to be spent. This can be used by an organization to give its members access to its treasury while only allowing a withdrawal if 3 of 5 members sign the transaction. Some web wallets also provide multi-signature wallets, allowing the user to keep control over their money while preventing a thief from stealing funds by compromising a single device or server.

❑ Think about your testament

Your bitcoins can be lost forever if you don't have a backup plan for your peers and family. If the location of your wallets or your passwords are not known by anyone when you are gone, there is no hope that your funds will ever be recovered. Taking a bit of time on these matters can make a huge difference.

Bitcoin Security

Securing bitcoin is challenging because bitcoin is not an abstract reference to value, like a balance in a bank account. Bitcoin is very much like digital cash or gold.

Possession of the keys to unlock the bitcoin is equivalent to possession of cash or a chunk of precious metal.

You can lose it, misplace it, have it stolen, or accidentally give the wrong amount to someone. In every one of these cases, users have no recourse, just as if they dropped cash on a public sidewalk.

However, bitcoin has capabilities that cash, gold, and bank accounts do not. A bitcoin wallet, containing your keys, can be backed up like any file. It can be stored in multiple copies, even printed on paper for hard-copy backup.

You can't "back up" cash, gold, or bank accounts. Bitcoin is different enough from anything that has come before that we need to think about bitcoin security in a novel way too.

Security Principles

The core principle in bitcoin is decentralization and it has important implications for security. A centralized model, such as a traditional bank or payment network, depends on access control and vetting to keep bad actors out of the system.

By comparison, a decentralized system like bitcoin pushes the responsibility and control to the users. Because security of the network is based on proof of work, not access control, the network can be open and no encryption is required for bitcoin traffic.

Traditional payments

- ❑On a traditional payment network, such as a credit card system, the payment is open-ended because it contains the user’s private identifier (the credit card number).
- ❑After the initial charge, anyone with access to the identifier can “pull” funds and charge the owner again and again.
- ❑Thus, the payment network has to be secured end-to-end with encryption and must ensure that no eavesdroppers or intermediaries can compromise the payment traffic, in transit or when it is stored (at rest).
- ❑If a bad actor gains access to the system, he can compromise current transactions *and* payment tokens that can be used to create new transactions.
- ❑Worse, when customer data is compromised, the customers are exposed to identity theft and must take action to prevent fraudulent use of the compromised accounts.

How different in bitcoin!!

- ❑Bitcoin is dramatically different. A bitcoin transaction authorizes only a specific value to a specific recipient and cannot be forged or modified.
- ❑It does not reveal any private information, such as the identities of the parties, and cannot be used to authorize additional payments.
- ❑Therefore, a bitcoin payment network does not need to be encrypted or protected from eavesdropping.
- ❑In fact, you can broadcast bitcoin transactions over an open public channel, such as unsecured WiFi or Bluetooth, with no loss of security.

Bitcoin decentralized power!!

Bitcoin’s decentralized security model puts a lot of power in the hands of the users.
With that power comes responsibility for maintaining the secrecy of the keys. For most users that is not easy to do, especially on general-purpose computing devices such as Internet-connected smartphones or laptops.
Although bitcoin’s decentralized model prevents the type of mass compromise seen with credit cards, many users are not able to adequately secure their keys and get hacked, one by one.

Developing Bitcoin Systems Securely

- ❑The most important principle for bitcoin developers is decentralization. Most developers will be familiar with centralized security models and might be tempted to apply these models to their bitcoin applications, with disastrous results.
- ❑Bitcoin’s security relies on decentralized control over keys and on independent transaction validation by miners. If you want to leverage Bitcoin’s security, you need to ensure that you remain within the Bitcoin security model. In simple terms: don’t take control of keys away from users and don’t take transactions off the blockchain.

Developing Bitcoin Systems Securely

❑For example, many early bitcoin exchanges concentrated all user funds in a single “hot” wallet with keys stored on a single server.

❑Such a design removes control from users and centralizes control over keys in a single system. Many such systems have been hacked, with disastrous consequences for their customers.

Developing Bitcoin Systems Securely

- ❑Another common mistake is to take transactions “off blockchain” in a misguided effort to reduce transaction fees or accelerate transaction processing.
- ❑An “off blockchain” system will record transactions on an internal, centralized ledger and only occasionally synchronize them to the bitcoin blockchain.
- ❑This practice, again, substitutes decentralized bitcoin security with a proprietary and centralized approach.
- ❑When transactions are off blockchain, improperly secured centralized ledgers can be falsified, diverting funds and depleting reserves, unnoticed.

- ❑To take advantage of Bitcoin’s unique decentralized security model, you have to avoid the temptation of centralized architectures that might feel familiar but ultimately subvert Bitcoin’s security.

The Root of Trust –Traditionally!!

- Traditional security architecture is based upon a concept called the *root of trust*, which is a trusted core used as the foundation for the security of the overall system or application.
- Security architecture is developed around the root of trust as a series of concentric circles, like layers in an onion, extending trust outward from the center.
- Each layer builds upon the more-trusted inner layer using access controls, digital signatures, encryption, and other security primitives

The Root of Trust –in Bitcoin !!

- ❑Bitcoin security architecture is different. In Bitcoin, the consensus system creates a trusted public ledger that is completely decentralized.
- ❑A correctly validated blockchain uses the genesis block as the root of trust, building a chain of trust up to the current block. Bitcoin systems can and should use the blockchain as their root of trust.
- ❑When designing a complex bitcoin application that consists of services on many different systems, you should carefully examine the security architecture in order to ascertain where trust is being placed.
- ❑Ultimately, the only thing that should be explicitly trusted is a fully validated blockchain.

The Root of Trust –in Bitcoin !!

- ❑If your application explicitly or implicitly vests trust in anything but the blockchain, that should be a source of concern because it introduces vulnerability.
- ❑A good method to evaluate the security architecture of your application is to consider each individual component and evaluate a hypothetical scenario where that component is completely compromised and under the control of a malicious actor.
- ❑Take each component of your application, in turn, and assess the impacts on the overall security if that component is compromised.
- ❑If your application is no longer secure when components are compromised, that shows you have misplaced trust in those components.
- ❑A bitcoin application without vulnerabilities should be vulnerable only to a compromise of the bitcoin consensus mechanism, meaning that its root of trust is based on the strongest part of the bitcoin security architecture.

User Security Best Practices

❑Fortunately, bitcoin also creates the incentives to improve computer security. Whereas previously the risk of computer compromise was vague and indirect, bitcoin makes these risks clear and obvious. Holding bitcoin on a computer serves to focus the user’s mind on the need for improved computer security.

❑Over the past three years, as a direct result of bitcoin adoption, we have seen tremendous innovation in the realm of information security in the form of hardware encryption, key storage and hardware wallets, multi-signature technology, and digital escrow.

❑In the following sections we will examine various best practices for practical user security.

Practices - Physical Bitcoin Storage

- Because most users are far more comfortable with physical security than information security, a very effective method for protecting bitcoins is to convert them into physical form.
- Bitcoin keys are nothing more than long numbers. This means that they can be stored in a physical form, such as printed on paper or etched on a metal coin.
- Securing the keys then becomes as simple as physically securing the printed copy of the bitcoin keys.

Practices - Hardware Wallets

❑ In the long term, bitcoin security increasingly will take the form of hardware tamper-proof wallets.

❑ Unlike a smartphone or desktop computer, a bitcoin hardware wallet has just one purpose: to hold bitcoins securely.

❑ Without general-purpose software to compromise and with limited interfaces, hardware wallets can deliver an almost foolproof level of security to nonexpert users.

❑ I expect to see hardware wallets become the predominant method of bitcoin storage. For an example of such a hardware wallet, see the Trezor.

Practices - Balancing Risk

- ❑Although most users are rightly concerned about bitcoin theft, there is an even bigger risk.
- ❑Data files get lost all the time. If they contain bitcoin, the loss is much more painful. In the effort to secure their bitcoin wallets, users must be very careful not to go too far and end up losing the bitcoin.
- ❑In the summer of 2010, a well-known bitcoin awareness and education project lost almost 7,000 bitcoins. In their effort to prevent theft, the owners had implemented a complex series of encrypted backups.
- ❑In the end they accidentally lost the encryption keys, making the backups worthless and losing a fortune. Like hiding money by burying it in the desert, if you secure your bitcoin too well you might not be able to find it again.

Practices 一 Diversifying the risk

- Would you carry your entire net worth in cash in your wallet? Most people would consider that reckless, yet bitcoin users often keep all their bitcoin in a single wallet.
- Instead, users should spread the risk among multiple and diverse bitcoin wallets. Prudent users will keep only a small fraction, perhaps less than 5%, of their bitcoins in an online or mobile wallet as “pocket change.”
- The rest should be split between a few different storage mechanisms, such as a desktop wallet and offline (cold storage).

Practices — Multisig and Governance

- ❑Whenever a company or individual stores large amounts of bitcoin, they should consider using a multi-signature bitcoin address.
- ❑Multi-signature addresses secure funds by requiring more than one signature to make a payment.
- ❑The signing keys should be stored in a number of different locations and under the control of different people.
- ❑ In a corporate environment, for example, the keys should be generated independently and held by several company executives, to ensure no single person can compromise the funds.
- ❑Multi-signature addresses can also offer redundancy, where a single person holds several keys that are stored in different locations.

Practices — Survivability

❑One important security consideration that is often overlooked is availability, especially in the context of incapacity or death of the key holder.

❑Bitcoin users are told to use complex passwords and keep their keys secure and private, not sharing them with anyone.

❑Unfortunately, that practice makes it almost impossible for the user’s family to recover any funds if the user is not available to unlock them.

❑In most cases, in fact, the families of bitcoin users might be completely unaware of the existence of the bitcoin funds.

❑If you have a lot of bitcoin, you should consider sharing access details with a trusted relative or lawyer.

❑A more complex survivability scheme can be set up with multi-signature access and estate planning through a lawyer specialized as a “digital asset executor.”

Consensus Protocol- PBFT

- PBFT can be very beneficial for low latency storage systems.
- This type of model is often used in digital assets backed platforms that don’t need a great amount of capacity, but carry out a large number of transactions.
- PBFT makes sure that the transaction records within the network are accurate.
- A few examples of permissioned blockchains that use this model are Hyperledger and Chain.

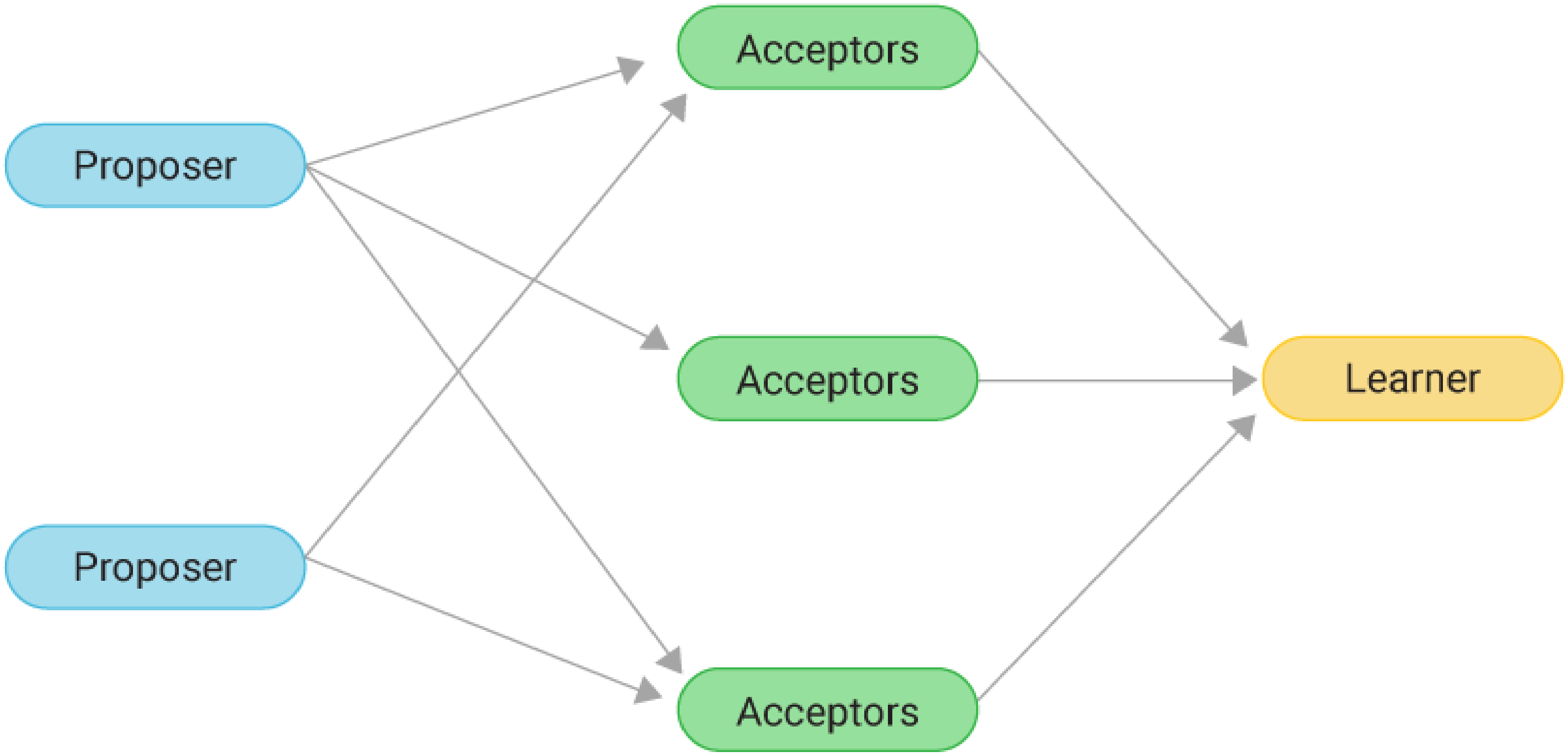
Federated Consensus

- This model guarantees security and transparency . It is ideal for use cases such as cross border remittance, real time KYC etc. Common examples of blockchains that use this model are Stellar and Ripple.

Round Robin Consensus

- Round robin consensus process doesn’t rely on a single participant for the block validation process.
- In this model, several nodes play a major role in validating and signing transactions, which makes this process more secure when compared to other consensus processes.
- There are also lower chances of double spend attacks due to the voting power distribution among trusted nodes.
- Round robin consensus mechanism is ideal for the trade, finance and supply chain industries.
- Some well known permissioned blockchains that use the Round Robin consensus method include Multichain and Tendermint

Paxos Consensus


Proposer
Proposer
Acceptors
Acceptors
Acceptors
Learner