Blockchain Privé VS Blockchain Publique

Christophe Ozcan

BLOCKCHAIN PRIVE VS BLOCKCHAIN PUBLIQUE

BLOCKCHAIN PRIVE ET BLOCKCHAIN PUBLIQUE
(90 min)

Type d'infrastructures Blockchain

Typologie des réseaux

La Blockchain privée

La Blockchain Publique

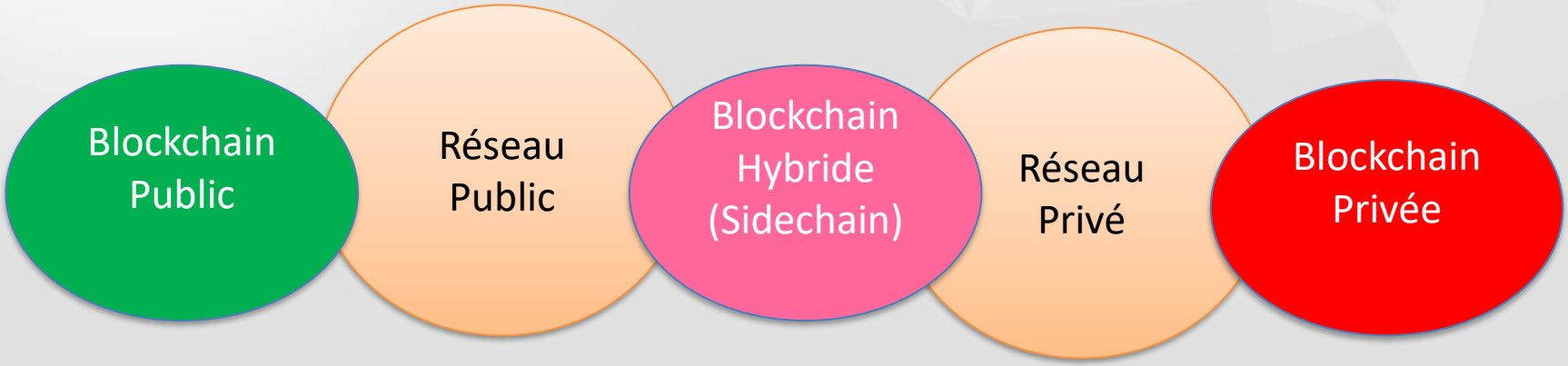
Consensus

Blockhain Privé : Hyperledger

Blockchain Hybride : Ethereum Private Sidechains

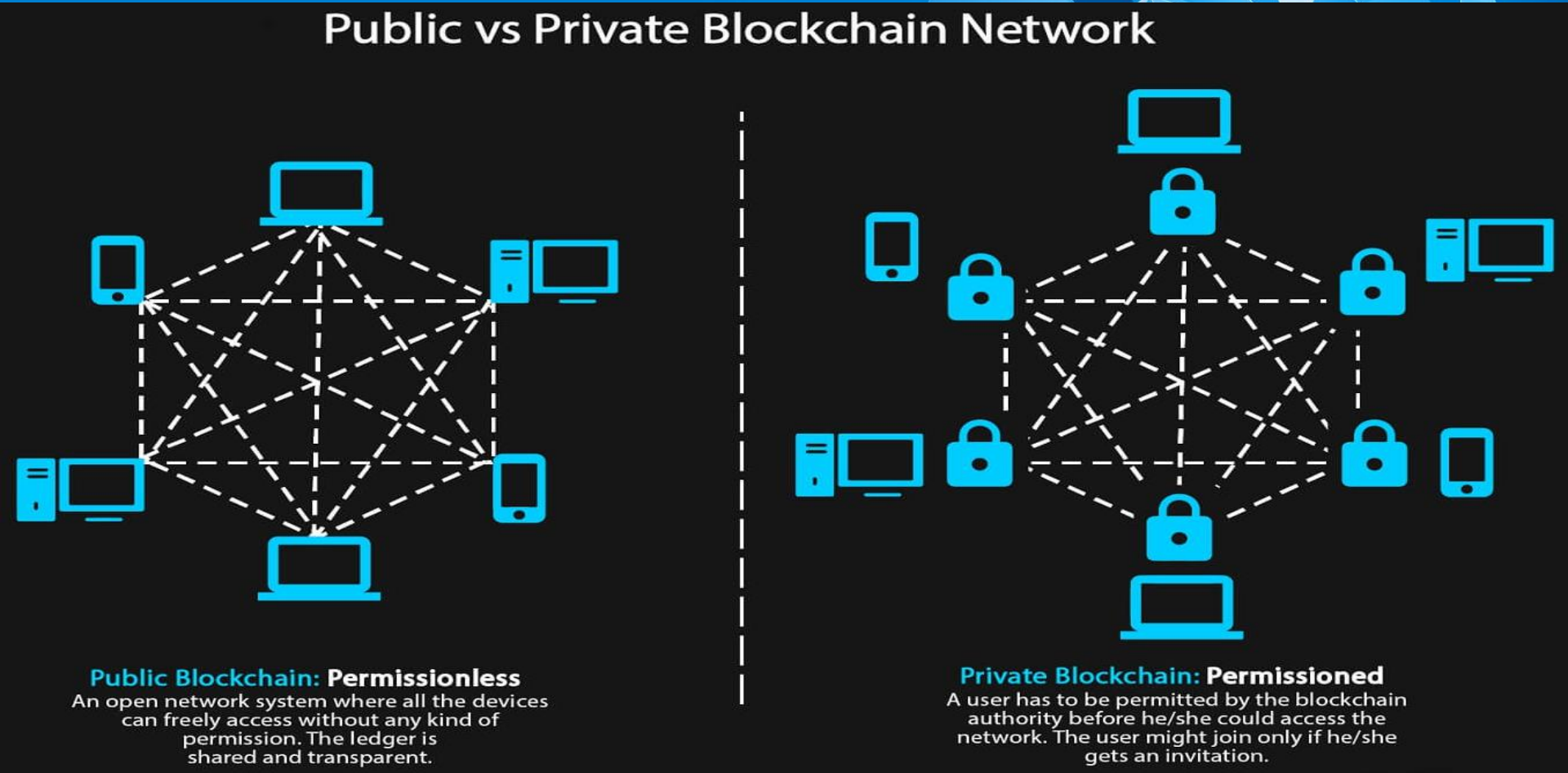
BLOCKCHAIN PRIVE VS BLOCKCHAIN PUBLIQUE
Type d'infrastructures Blockchain

Types d'infrastructure de la Blockchain:



BLOCKCHAIN PRIVE VS BLOCKCHAIN PUBLIQUE

Type de système distribués Blockchain



Blockchain Privée

2. La Blockchain Privée

Une blockchain privée est une blockchain restrictive ou d'autorisation opérant uniquement dans un réseau fermé.

Les blockchains privées sont généralement utilisées au sein d'une organisation ou d'entreprises où seuls les membres sélectionnés sont des participants à un réseau blockchain. Le niveau de sécurité, les autorisations, les permissions, l'accessibilité sont entre les mains de l'organisation de contrôle. Ainsi, les blockchains privées sont utilisées de la même manière qu'une blockchain publique mais ont un réseau petit et restrictif.

Elles ne bénéficient pas de la sécurité d'une Blockchain publique cependant elles sont plus rapide et une transaction n'a pas de coûts.

Aussi impressionnantes que soient les blockchains privées, elles ont leurs propres avantages et inconvénients.

Blockchain Privée

2. Les avantages de la Blockchain Privée

1) Vitesse - Les transactions des blockchains privées se produisent plus rapidement que les blockchains publiques. Cela signifie que le taux de transactions par seconde (TPS) est plus élevé dans le cas des blockchains privées. En effet, il existe un nombre limité de nœuds dans un réseau privé par opposition à un réseau public. Cela accélère le processus de consensus ou de vérification d'une transaction par tous les nœuds d'un réseau. De plus, le taux d'ajout de nouvelles transactions dans un bloc est rapide. Les blockchains privées peuvent faciliter les transactions à un taux allant jusqu'à des milliers ou cent mille TPS à la fois.

2) Évolutivité - Les blockchains privées sont assez évolutives. Autrement dit, vous pouvez choisir la taille de votre blockchain privée selon vos besoins. Par exemple, si une organisation a besoin d'une blockchain de seulement 20 nœuds, elle peut facilement en déployer une. Ensuite, après l'expansion, s'ils ont besoin d'ajouter plus de nœuds, ils peuvent facilement le faire. Cela rend les blockchains privées très évolutives car cela donne à une organisation la flexibilité d'augmenter ou de réduire la taille de son réseau sans trop d'effort.

Blockchain Privée

2. Les inconvénients de la Blockchain Privée

1) Nécessite un renforcement de la confiance - En ce qui concerne une blockchain publique, c'est comme un livre ouvert ou comme nous l'appelons, un registre ouvert. Cela garantit la sécurité et la légitimité de chaque utilisateur. Alors que, dans un réseau privé, il y a des participants limités dans un réseau restreint. Surtout au sein d'une organisation, où les collègues se connaissent. Ils ont besoin de renforcer la confiance pour transmettre des informations confidentielles au sein d'un réseau.

2) Sécurité inférieure - Comme un réseau blockchain privé a moins de nœuds ou de participants, il court un risque plus élevé de faille de sécurité. Si l'un des nœuds accède au système de gestion central, il peut accéder à tous les nœuds du réseau. Cela permet à un nœud malicieux d'altérer plus facilement l'ensemble de la blockchain privée et d'utiliser à mauvais escient les informations.

3) Centralisation - Les blockchains privées sont limitées, c'est-à-dire qu'elles ont besoin d'un système central de gestion des identités et des accès (IAM) pour fonctionner correctement. Ce système possède tous les droits de surveillance et d'administration. Il donne les autorisations pour ajouter un nouveau nœud dans le réseau ou pour décider du niveau d'accès qu'ils obtiennent pour les informations stockées dans la blockchain..

Blockchain Public

La Blockchain publique

Une blockchain publique est un système de grand livre distribué non restrictif et sans autorisation.
Toute personne ayant accès à Internet peut se connecter sur une blockchain public pour devenir un nœud et faire partie du réseau de la blockchain.

Un nœud ou un utilisateur qui fait partie de la blockchain publique est autorisé à accéder aux enregistrements actuels et passés du ledger, à vérifier les transactions ou à faire une preuve de travail pour un bloc entrant à travers le minage par exemple.

Ainsi, les blockchains publiques les plus courantes sont les blockchains Bitcoin et Ethereum.

Les blockchains publiques sont pour la plupart sécurisée du fait du consensus appliqué à grande échelle impactant cependant la rapidité des transactions du réseau.

Blockchain Public

Les Avantages de la blockchain publique

1) Fiable - Contrairement à la blockchain privée, deux nœuds ou participants n'ont pas à se soucier de l'authenticité de l'autre. En d'autres termes, ils n'ont pas besoin de connaître personnellement ou de faire confiance aux autres nœuds, car le consensus garantit qu'il ne peut y avoir de fraude dans les transactions.

2) Sécurisé - Il peut y avoir autant de participants ou de nœuds dans un réseau public, ce qui en fait un réseau sécurisé. Attention toutes les blockchains publiques ne sont pas toutes sécurités par design uniquement celles les plus distribués le sont. Plus le réseau est grand, plus la distribution des enregistrements est grande et plus il est difficile pour les pirates de pirater l'ensemble du réseau.

3) Ouvert et transparent - La blockchain publique est ouverte et les données sont transparentes pour tous les nœuds participants. Une copie des enregistrements de la blockchain ou du registre numérique est disponible sur chaque nœud autorisé. Cela rend l'ensemble du système de blockchain complètement ouvert et transparent.

Blockchain Public

Les inconvénients de la blockchain publique

1) Rapidité faible - Le taux de transactions par seconde (TPS) dans une blockchain publique est très faible. En effet, il s'agit d'un immense réseau avec beaucoup de nœuds et pour chaque nœud, vérifier une transaction et atteindre le consensus prend du temps. C'est pourquoi les blockchains publiques ne peuvent traiter que quelques centaines de transaction par seconde.

2) Couteux – Une blockchain publique a un rythme lent de traitement et de réalisation des transactions souvent assez couteuses du fait de la saturation du réseau qui privilégie les transactions ayant des frais de confirmation plus importante pouvant impacter par exemple le coût d'exécution d'un smart contract (contrat intelligent).

BLOCKCHAIN PRIVE VS BLOCKCHAIN PUBLIQUE

Type de système distribués Blockchain

The differences	Blockchain type	
	Public	Private
Operator	There is no administrator	Only one administrator
System participants	Anyone	Once approved
Data access rights	Anyone	Invited users only
Permission to write data	Anyone	The approved user
Ownership	Nobody	A single organization
Identity confidentiality	Yes	No
Transaction speed	Low	Fast

Blockchain Hybride (Sidechain)

3. Blockchain Hybride (Sidechain)

Une blockchain hybride est une combinaison de la blockchain privée et publique. Elle utilise les fonctionnalités des deux types de blockchains, c'est-à-dire que l'on peut avoir un système privé basé sur des autorisations ainsi qu'un système public sans autorisation. Avec un tel réseau hybride, les utilisateurs peuvent contrôler qui a accès à quelles données stockées dans la blockchain.

Seule une section sélectionnée de données ou d'enregistrements de la blockchain peut être autorisée à devenir publique en gardant le reste confidentiel dans le réseau privé. Le système hybride de blockchain parfois appelé Sidechain est flexible afin que les utilisateurs puissent facilement rejoindre une blockchain privée avec plusieurs blockchains publiques. Une transaction dans un réseau privé d'une blockchain hybride est généralement vérifiée au sein de ce réseau. Mais les utilisateurs peuvent également le publier dans la blockchain publique pour être vérifié. Les blockchains publique impliquent plus de nœuds mais également plus de frais pour la vérification.

Blockchain Hybride (Sidechain)

2. Les avantages de la Blockchain Hybride

1) Vitesse - Les transactions des blockchains hybrides sont aussi rapide que celles opérées par les Blockchain privée cependant elles peuvent être également enregistrés sur une Blockchain publique dans un second temps pour tout ou une partie uniquement des transactions. Cela permet par exemple d'enregistré uniquement sur la Blockchain publique des donnés triées afin qu'elles deviennent immuables.

2) Évolutivité - Les blockchains hybrides sont elles aussi évolutives que les Blockchain privés.

3) Sécurisé – Contrairement à ce que nous pourrions pensée les Blockchains Hybrides sont sécurisé car elles s'appuient principalement sur la sécurité d'une Blockchain publique. Elle est en faite ce que l'on appel une couche de niveau 2 que nous allons étudier par la suite.

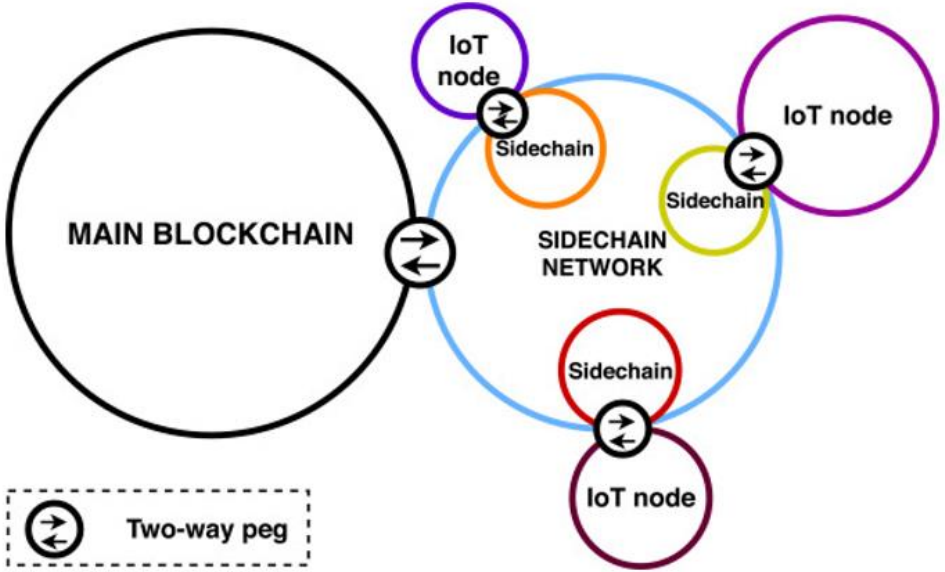
Blockchain Hybride (Sidechain)

2. Les inconvénients de la Blockchain Hybride (Sidechain)

1) Centralisation - Les blockchains hybrides sont par design centralisé et sont limitées d'accès, elles ont besoin également d'un système central de gestion des identités et des accès (IAM) pour fonctionner correctement. Ce système possède tous les droits de surveillance et d'administration. Il donne les autorisations pour ajouter un nouveau nœud dans le réseau ou pour décider du niveau d'accès qu'ils obtiennent pour les informations stockées dans la blockchain..

BLOCKCHAIN PRIVE VS BLOCKCHAIN PUBLIQUE

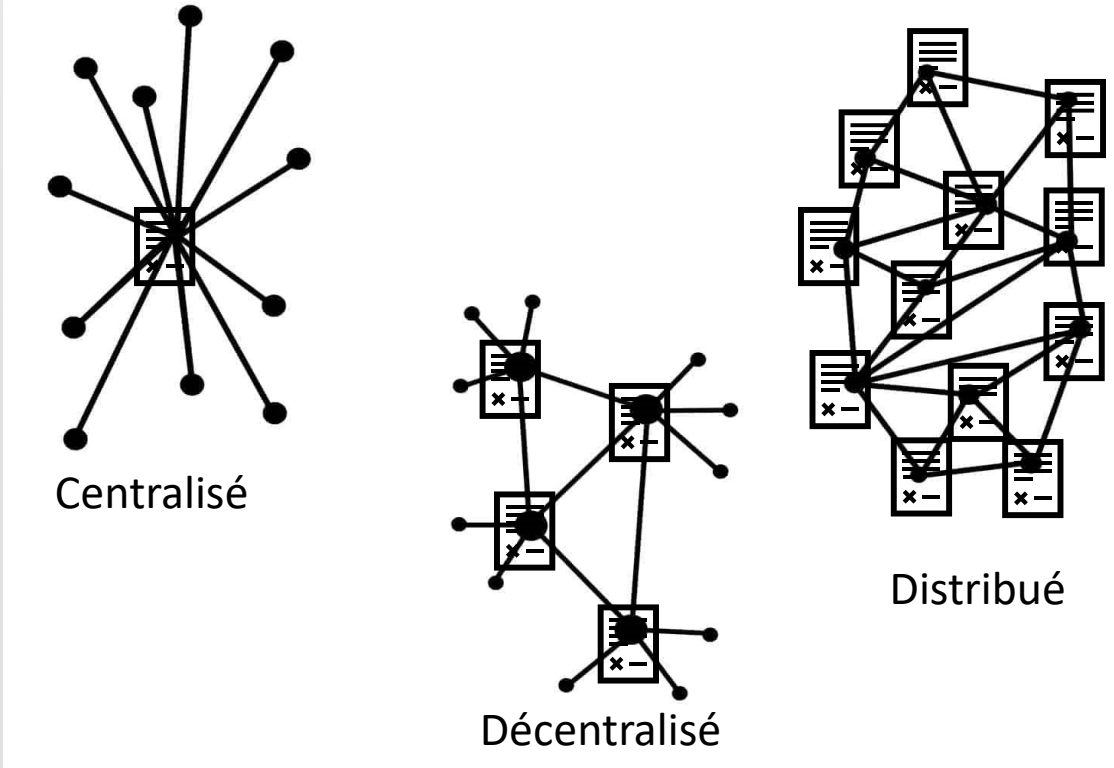
Type de système distribués Blockchain



BLOCKCHAIN PRIVE VS BLOCKCHAIN PUBLIQUE
Typologies des réseaux Blockchain

Typologies des réseaux Blockchain:

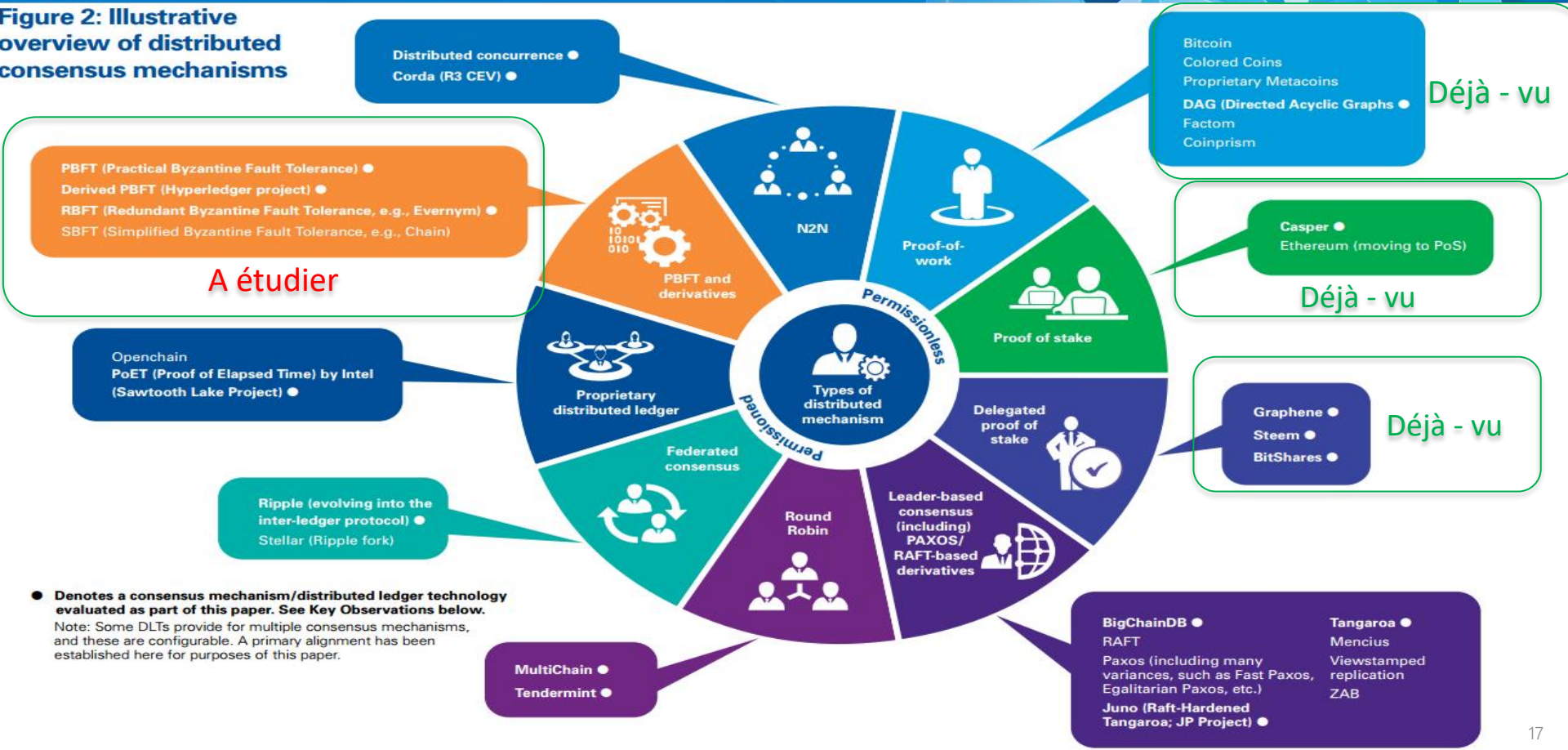
- Centralisé autour d'un registre et d'un nœud hub
- Décentralisé autour de registres répliqués par des nœuds hub
- Distribué autour de registres répliqués par des nœuds



BLOCKCHAIN PRIVE VS BLOCKCHAIN PUBLIQUE

Consensus

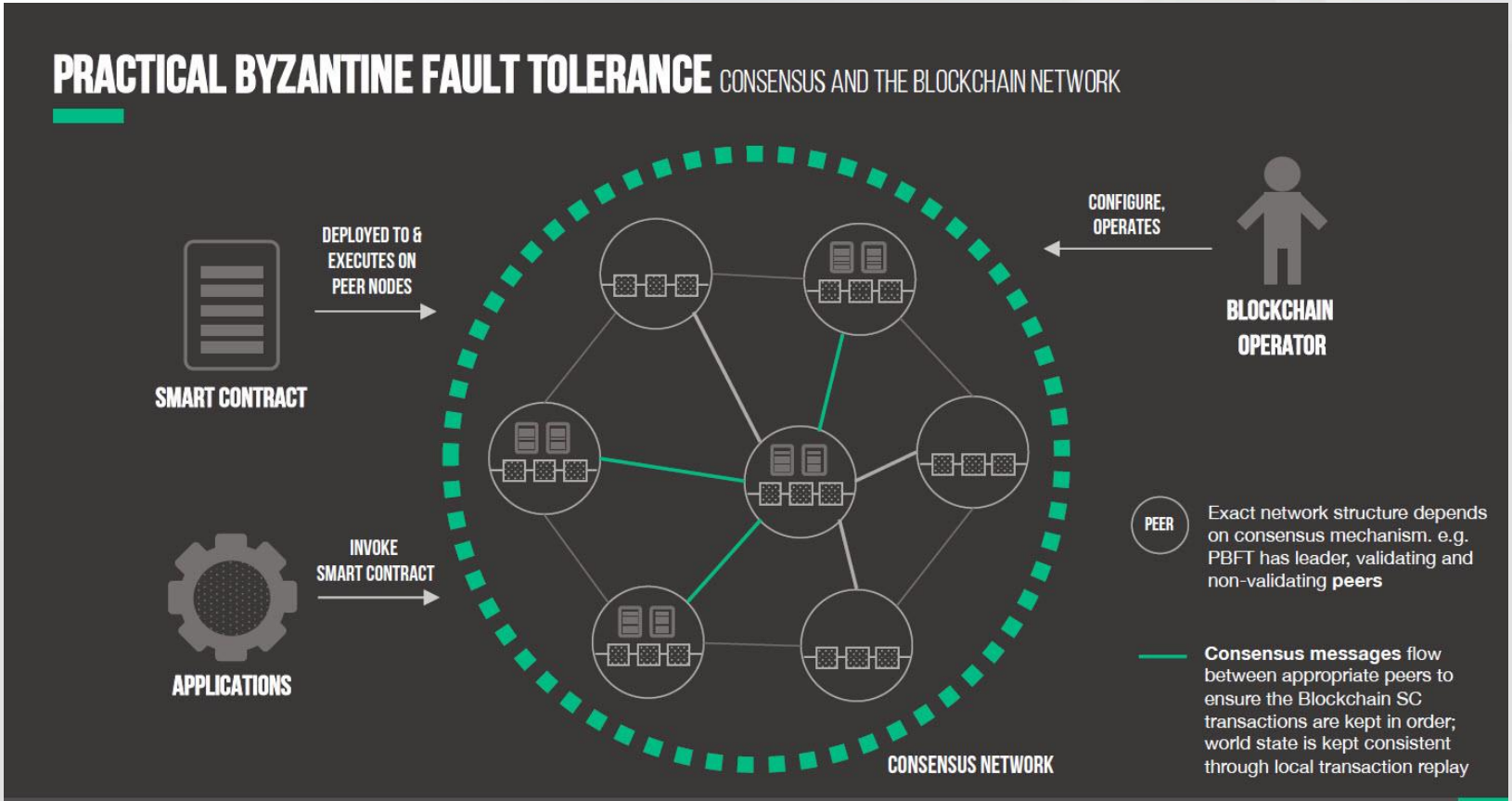
Figure 2: Illustrative overview of distributed consensus mechanisms



● **Denotes a consensus mechanism/distributed ledger technology evaluated as part of this paper. See Key Observations below.**

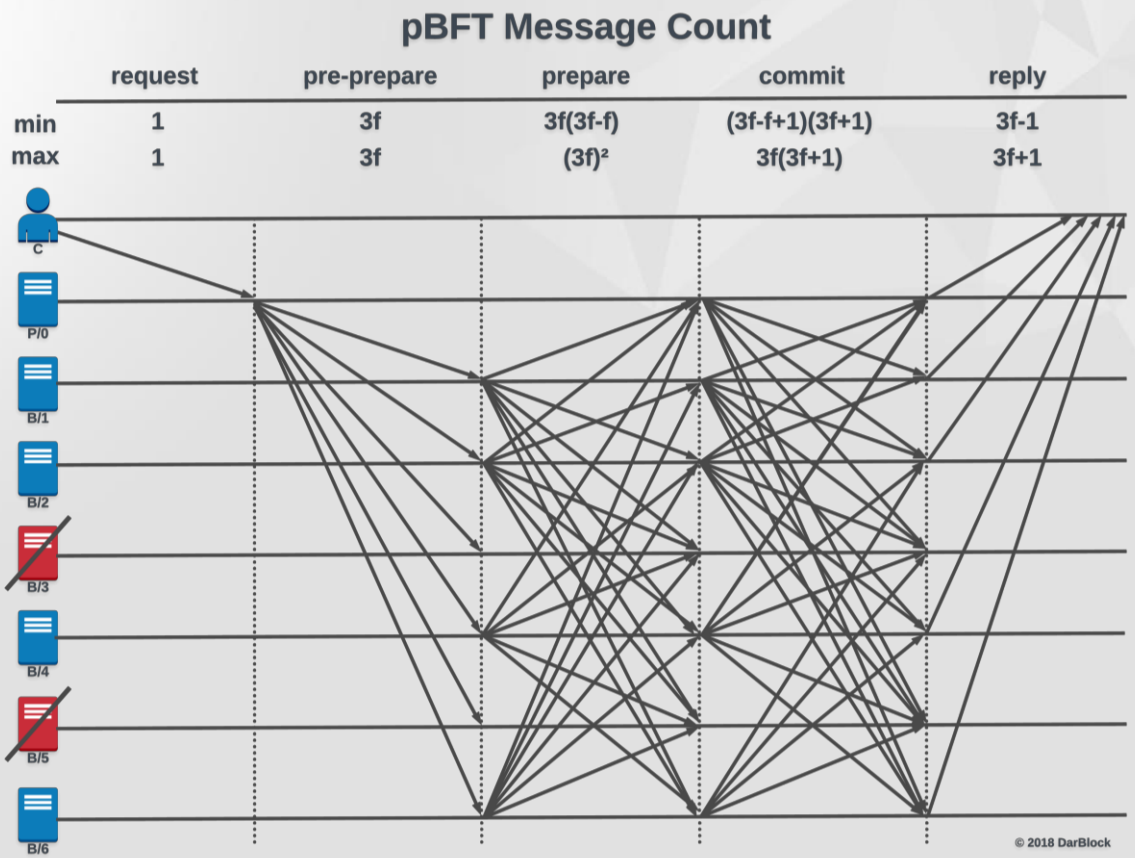
Note: Some DLTs provide for multiple consensus mechanisms, and these are configurable. A primary alignment has been established here for purposes of this paper.

BLOCKCHAIN PRIVE VS BLOCKCHAIN PUBLIQUE
Consensus



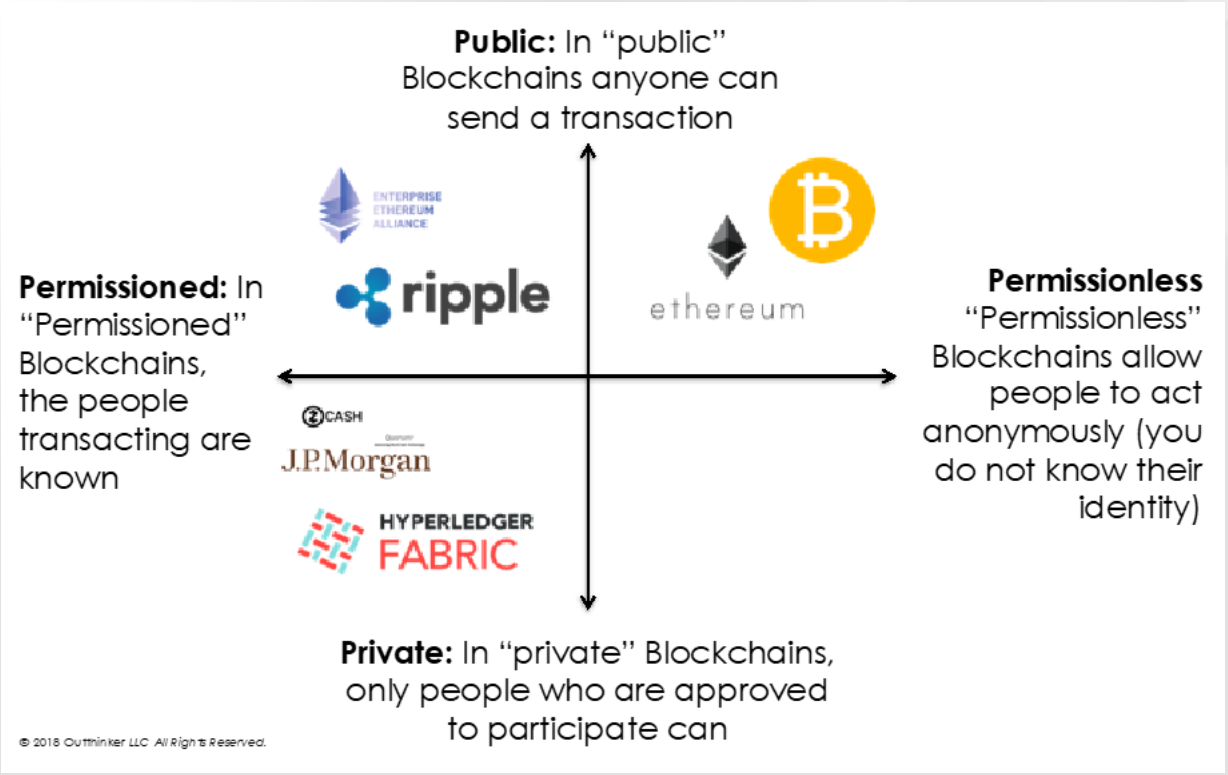
BLOCKCHAIN PRIVE VS BLOCKCHAIN PUBLIQUE

Consensus



BLOCKCHAIN PRIVE VS BLOCKCHAIN PUBLIQUE

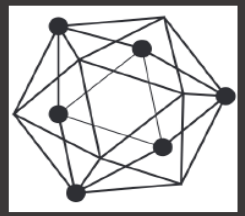
Consensus



HYPERLEDGER BLOCKCHAIN FRAMEWORKS

FABRIC

- IBM CODEBASE
- PLUGGABLE CONSENSUS
- MOST ADVANCED



SAWTOOTH LAKE

- INTEL CODEBASE
- MODULARITY
- POET & QUORUM

IROHA

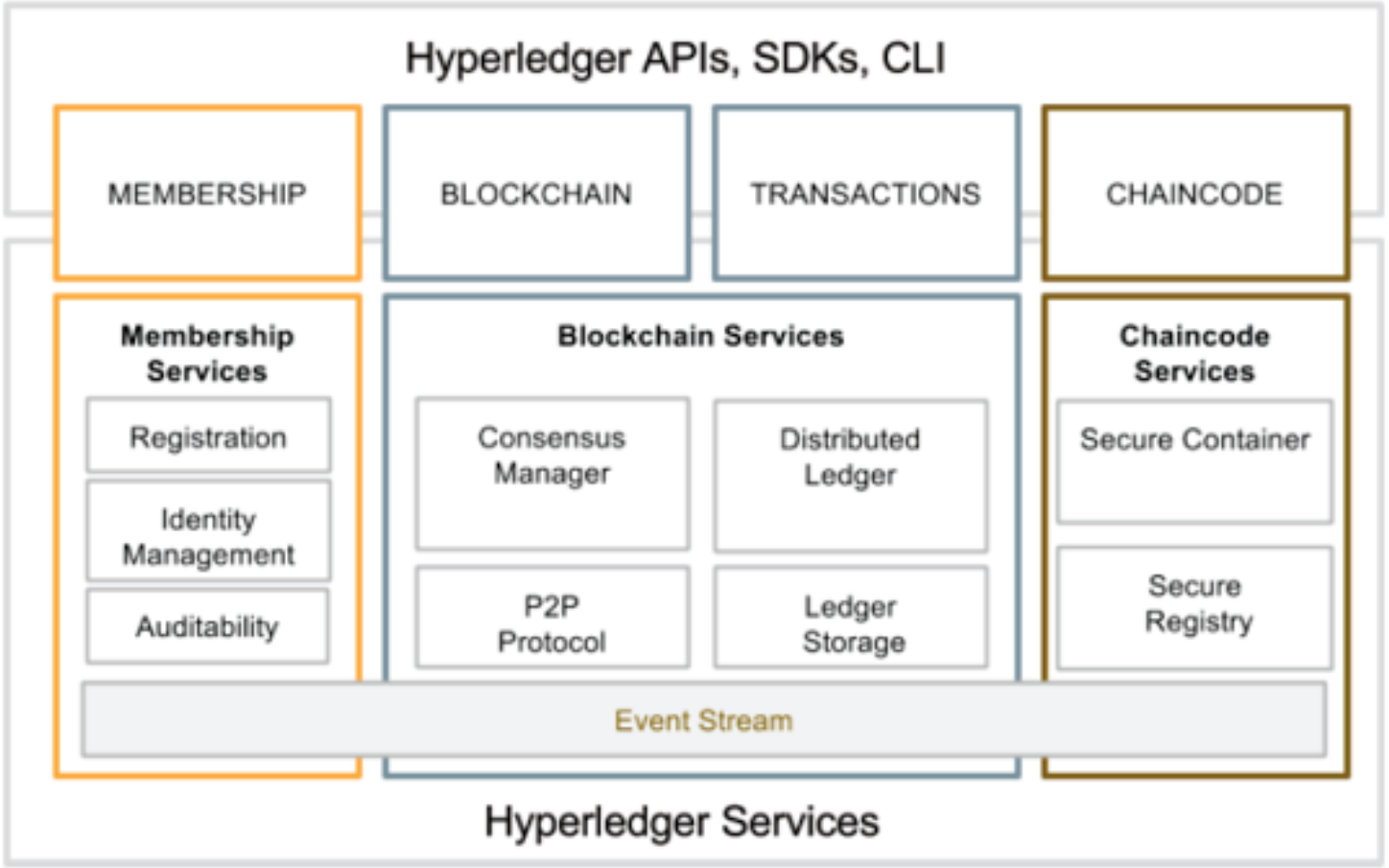
- JAPANESE
- MOBILE LIBRARIES & COMPONENTS

CORDA

- R3 CONSORTIUM
- MULTIPLE LEDGERS
- PRIVATE P2P TRANSACTIONS

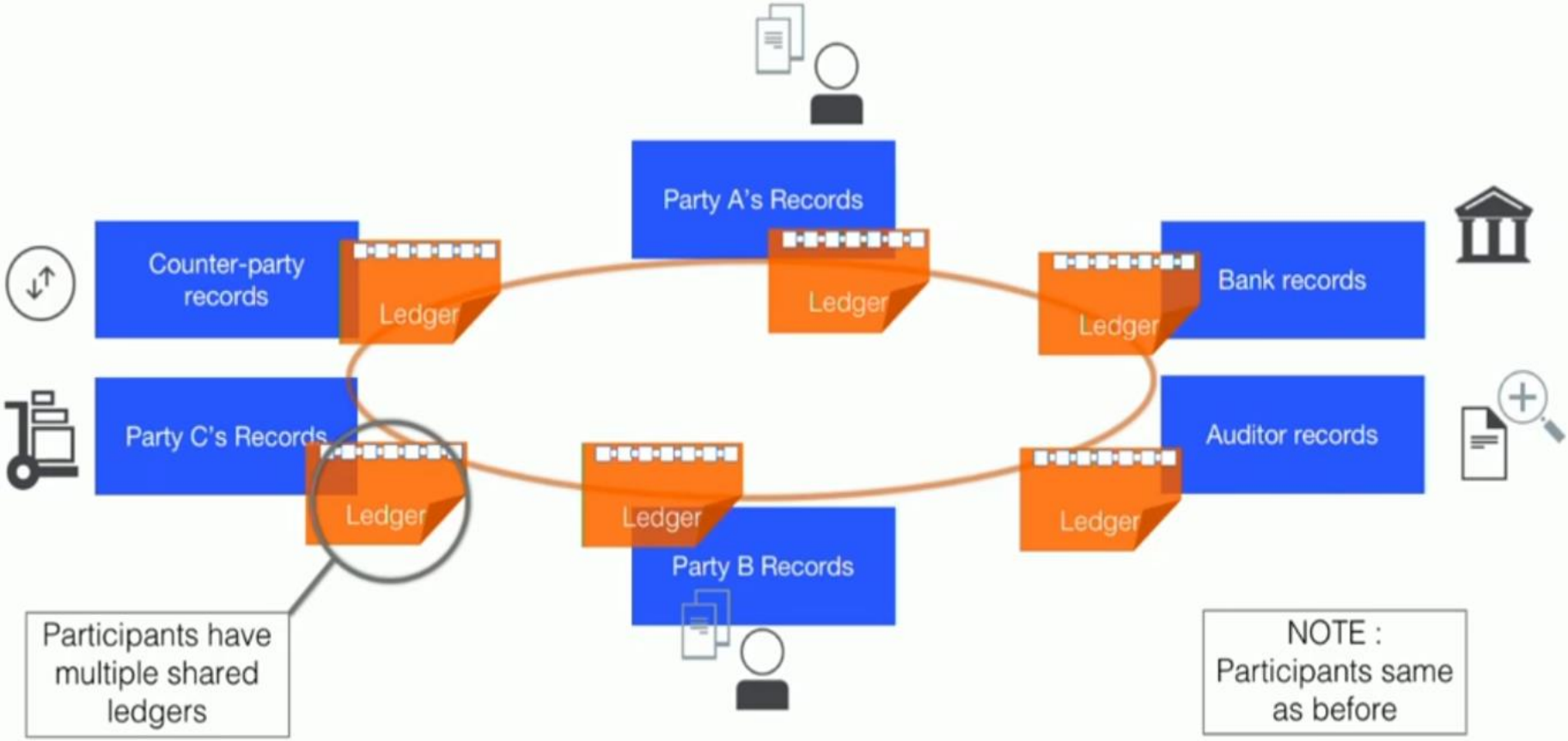
BLOCKCHAIN PRIVE VS BLOCKCHAIN PUBLIQUE

Hyperledger Fabric



BLOCKCHAIN PRIVE VS BLOCKCHAIN PUBLIQUE

Hyperledger Fabric



Nodes and roles

	**Committing Peer:** Maintains ledger and state. Commits transactions. May hold smart contract (chaincode).
	**Endorsing Peer:** Specialized peer also endorses transactions by receiving a transaction proposal and responds by granting or denying endorsement. Must hold smart contract.
	**Ordering Node:** Approves the inclusion of transaction blocks into the ledger and communicates with committing and endorsing peer nodes. Does not hold smart contract. Does not hold ledger.

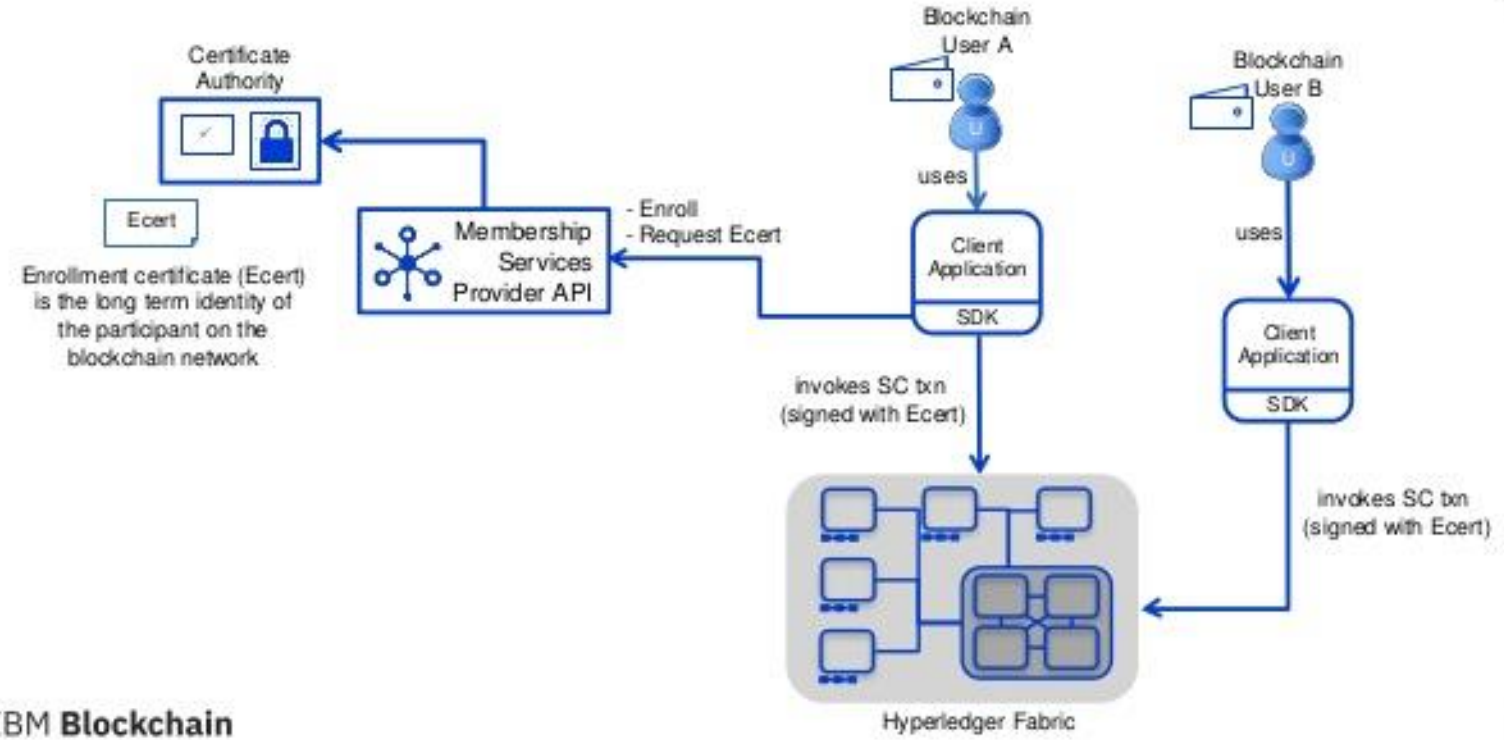
IBM **Blockchain**

Hyperledger Fabric Consensus

Consensus is achieved using the following transaction flow:

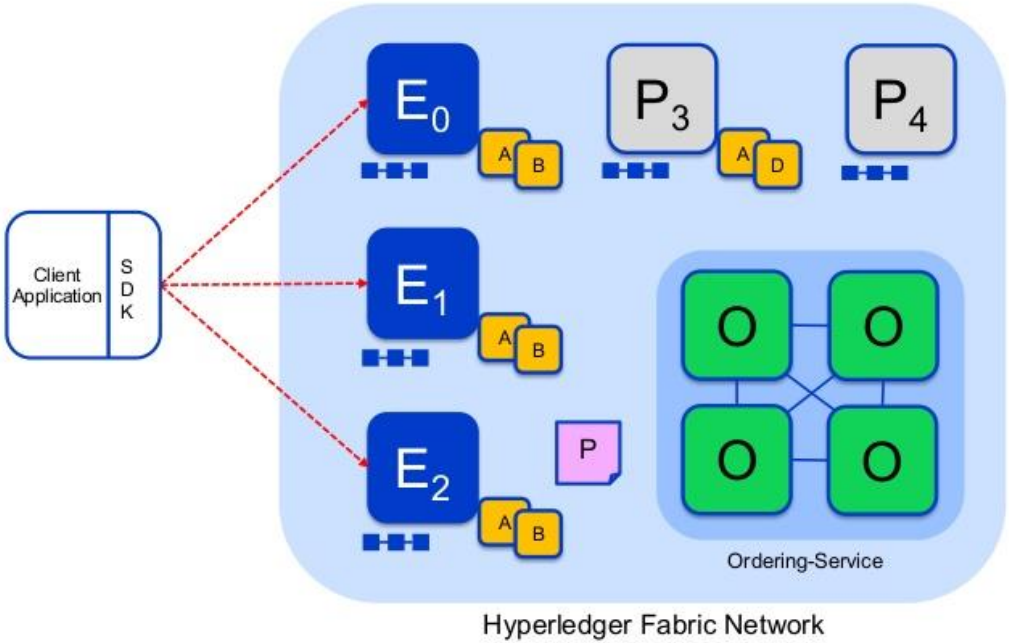
IBM **Blockchain**

Membership Services Overview



IBM **Blockchain**

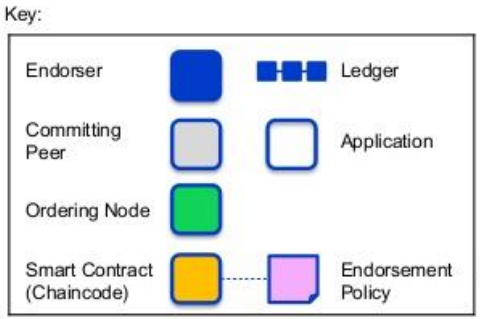
Sample transaction: Step 1/7 – Propose transaction



Application proposes transaction

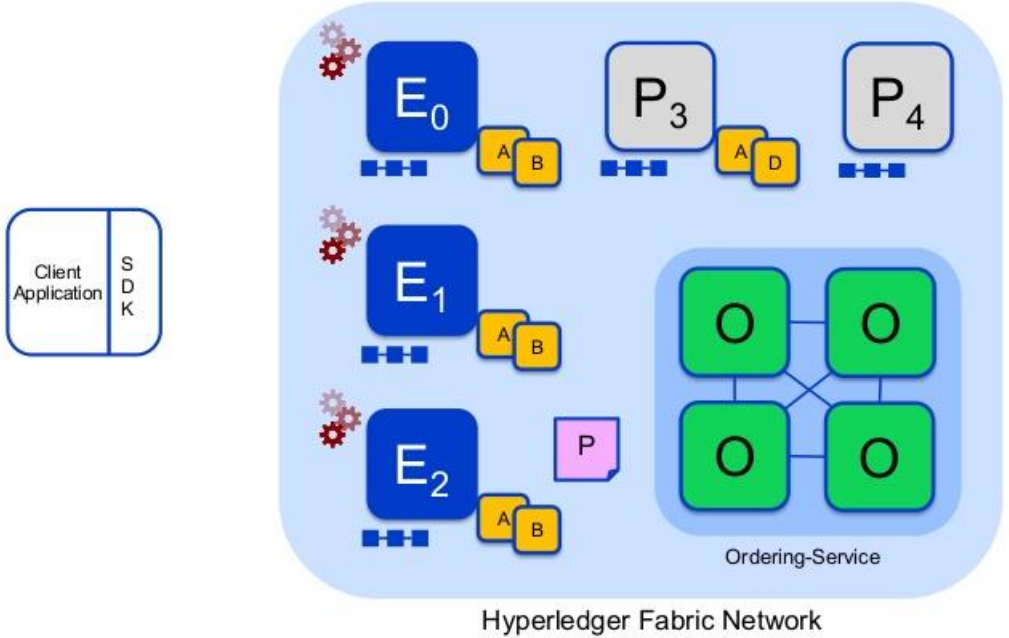
Endorsement policy:
- "E_0, E_1 and E_2 must sign"
- (P_3, P_4 are not part of the policy)

Client application submits a transaction proposal for Smart Contract A. It must target the required peers {E_0, E_1, E_2}



IBM **Blockchain**

Sample transaction: Step 2/7 – Execute proposal

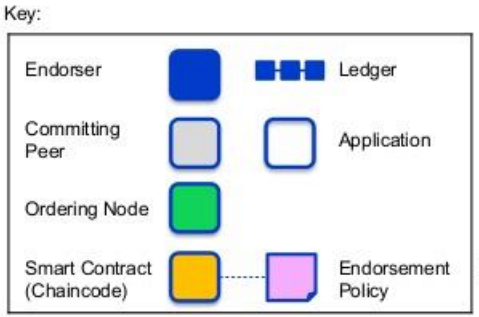


Endorsers Execute Proposals

E_0, E_1 & E_2 will each execute the proposed transaction. None of these executions will update the ledger

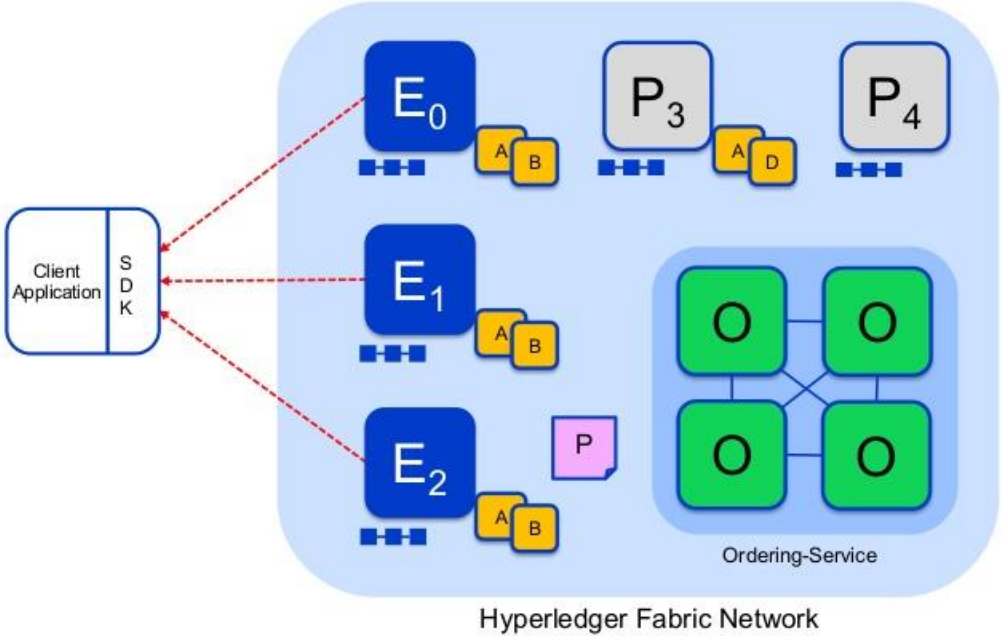
Each execution will capture the set of Read and Written data, called RW sets, which will now flow in the fabric.

Transactions can be signed & encrypted



IBM **Blockchain**

Sample transaction: Step 3/7 – Proposal Response



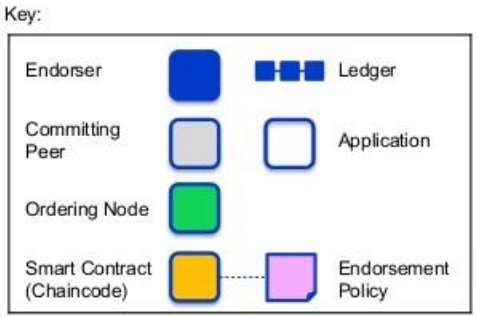
Hyperledger Fabric Network

Application receives responses

RW sets are asynchronously returned to application

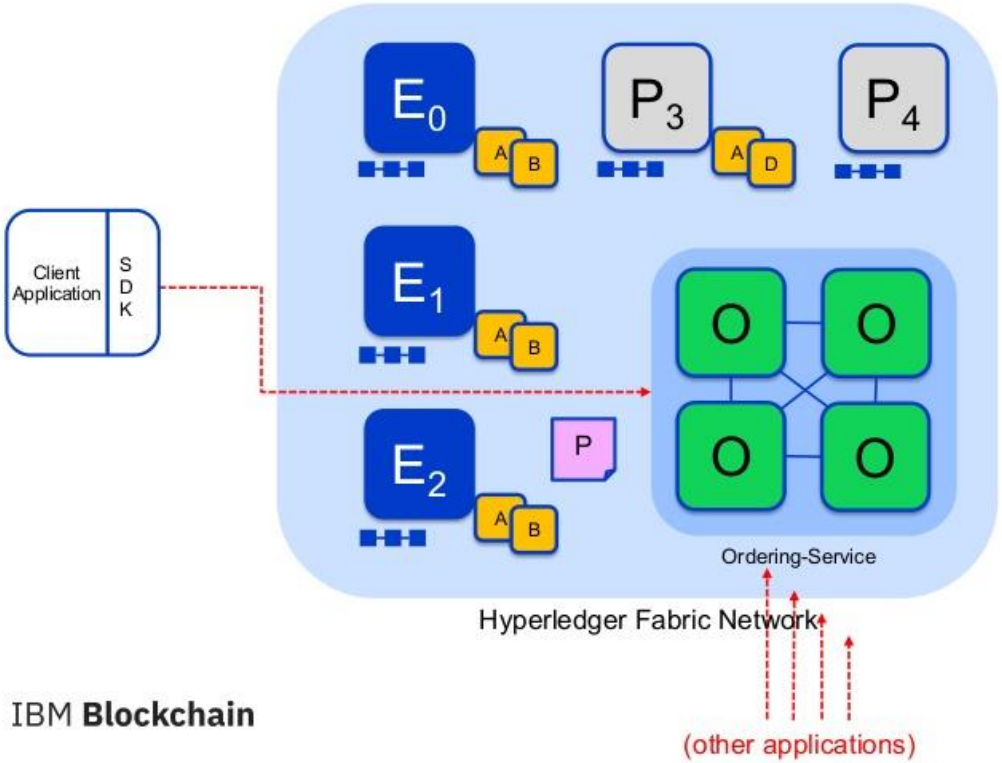
The RW sets are signed by each endorser, and also includes each record version number

(This information will be checked much later in the consensus process)



IBM **Blockchain**

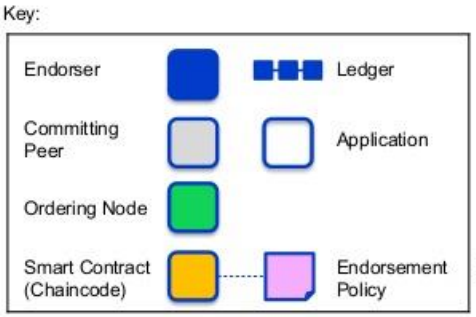
Sample transaction: Step 4/7 – Order Transaction



Responses submitted for ordering

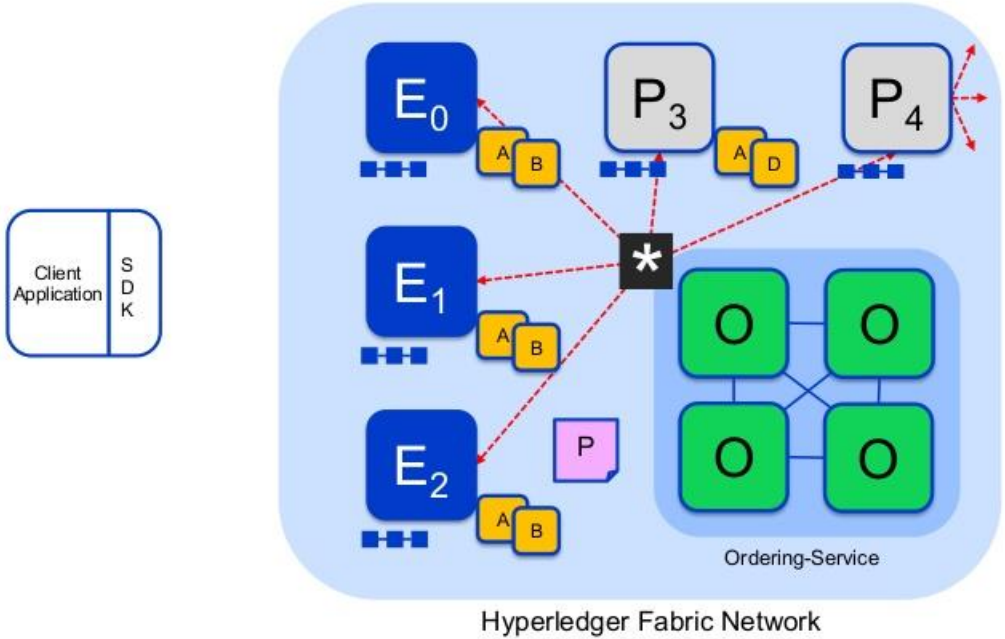
Application submits responses as a transaction to be ordered.

Ordering happens across the fabric in parallel with transactions submitted by other applications



IBM **Blockchain**

Sample transaction: Step 5/7 – Deliver Transaction



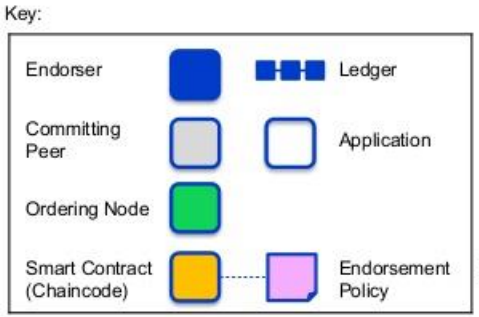
Hyperledger Fabric Network

Orderer delivers to committing peers

Ordering service collects transactions into proposed blocks for distribution to committing peers. Peers can deliver to other peers in a hierarchy (not shown)

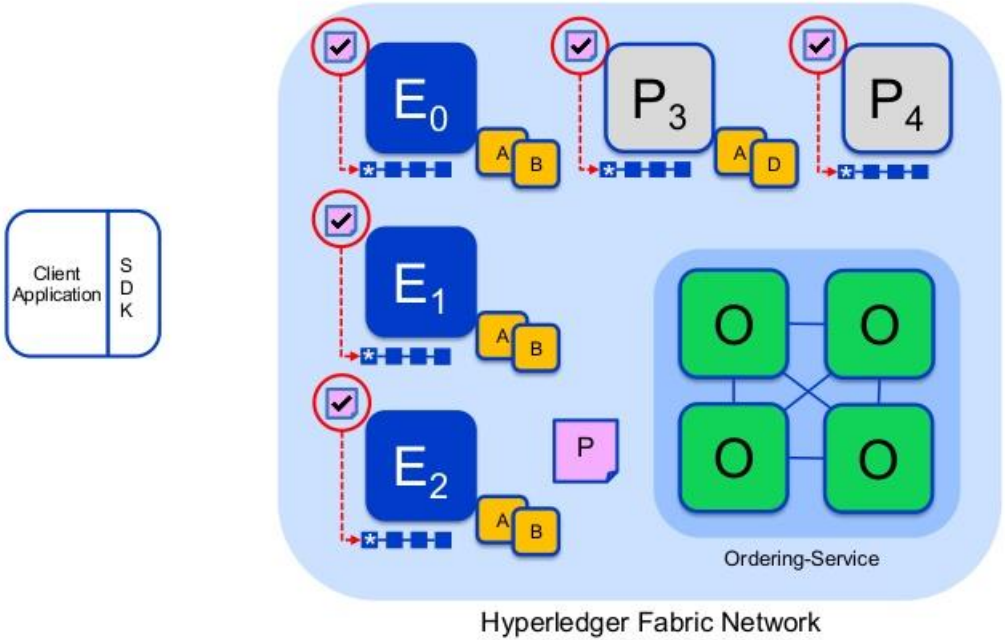
Different ordering algorithms available:

- SOLO (Single node, development)
- Kafka (Crash fault tolerance)



IBM **Blockchain**

Sample transaction: Step 6/7 – Validate Transaction



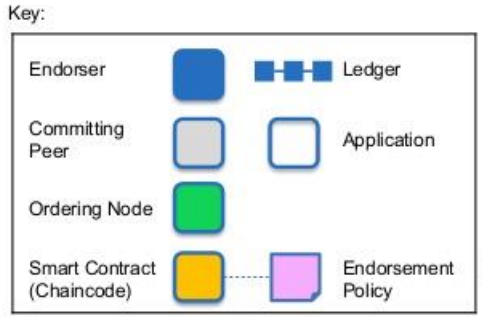
Hyperledger Fabric Network

Committing peers validate transactions

Every committing peer validates against the endorsement policy. Also check RW sets are still valid for current world state

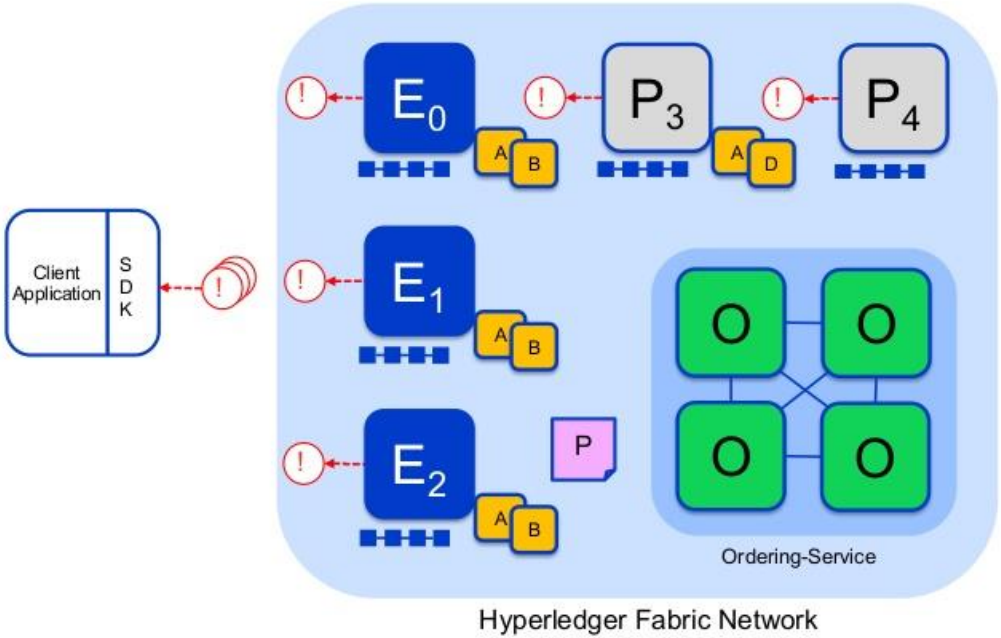
Validated transactions are applied to the world state and retained on the ledger

Invalid transactions are also retained on the ledger but do not update world state



IBM **Blockchain**

Sample transaction: Step 7/7 – Notify Transaction

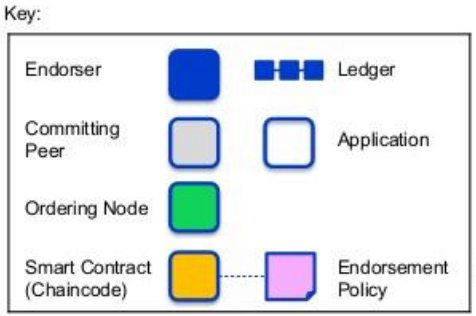


Hyperledger Fabric Network

Committing peers notify applications

Applications can register to be notified when transactions succeed or fail, and when blocks are added to the ledger

Applications will be notified by each peer to which they are connected

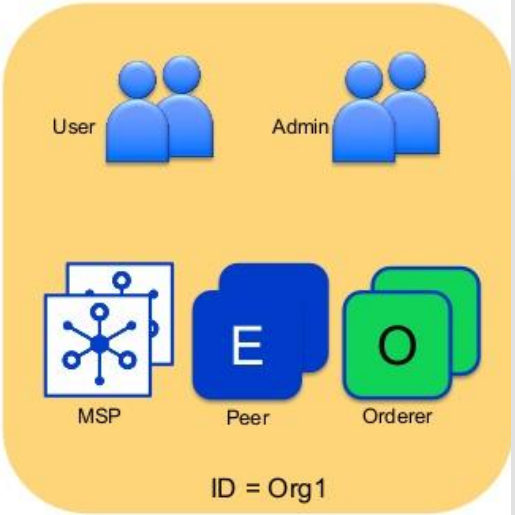


IBM **Blockchain**

Organisations

Organisations define boundaries within a Fabric Blockchain Network

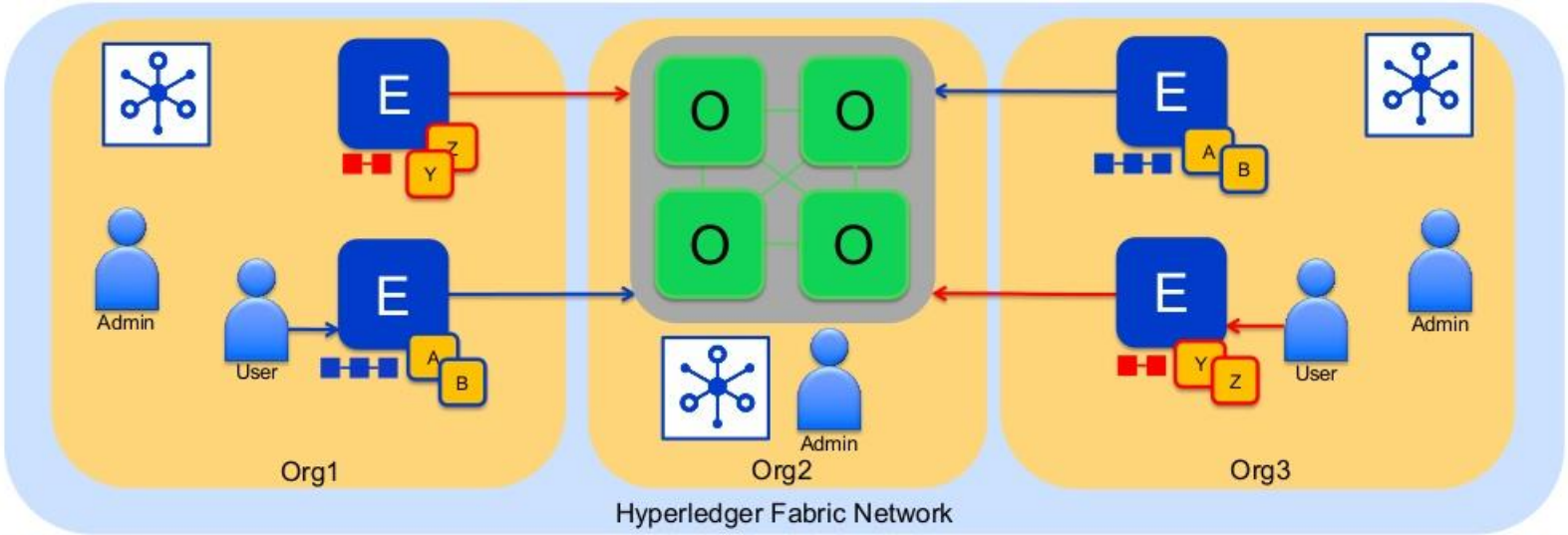
- Each organisation defines:
  - Membership Services Provider (MSP) for identities
  - Administrator(s)
  - Users
  - Peers
  - Orderers (optional)
- A network can include many organisations representing a consortium
- Each organisation has an ID



Consortium Network

An example consortium network of 3 organisations

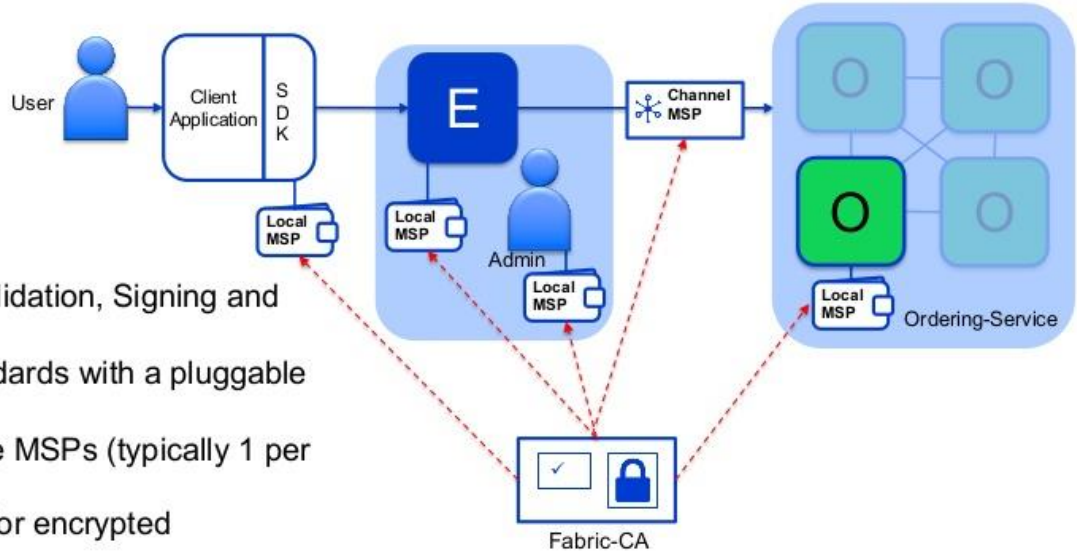
- Orgs 1 and 3 run peers
- Org 2 provides the ordering service only



Membership Services Provider - Overview

A MSP manages a set of identities within a distributed Fabric network

- Provides identity for:
  - Peers and Orderers
  - Client Applications
  - Administrators
- Identities can be issued by:
  - Fabric-CA
  - An external CA
- Provides: Authentication, Validation, Signing and Issuance
- Supports different crypto standards with a pluggable interface
- A network can include multiple MSPs (typically 1 per org)
- Includes TLS crypto material for encrypted communications



IBM **Blockchain**