Métricas de Software

Maestría en Ingeniería de Sistemas e Informática

Mención: Ingeniería de Software

Docente: Mg. Ing. Félix Melchor Santos López

2020 - I

UNMSM

Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América.

Blockchain Module 2
Blockchain Technology & Architecture

Blockchain Mechanisms
- Node Monitor
- Automated Node Deployer
- Consensus Processor
- Block Maker
- Identity Federator
- Node Placement Monitor
- Hashing Engine
- Chaining Engine
- Node Repository
- Ledger Replicator
- Live Node Migrator
- Identity Verifier

Scalability and Reliability Patterns
- Auto-Scaling Nodes
- Guaranteed Minimum Full Nodes
- Geo Scaling
- Block Size Update

Utility Patterns
- Transaction Tagging
- Lightweight Node
- Node Task Abstraction

Consensus Participation
- Creating Blocks
- Validating Blocks
- Adding Blocks to Chains
- Retaining Copies of Ledger
- Leader Tasks
- Record Creation
- Record Signing
- Voting
- Node Nomination

Integrity and Validation Patterns
- Block Singleton
- Sidechain
- Block Validation Consensus
  - Proof of Work (PoW)
  - Proof of Stake (PoS)
  - Proof of Activity (PoA)
  - Delegated Proof of Stake (DPoS)
  - Leased Proof of Stake (LPoS)
  - Proof of Importance (PoI)
  - Proof of Elapsed Time (PoET)
  - Round Robin
  - Proof of Capacity (PoC)
  - Proof of Burn (PoB)

Security and Privacy Patterns
- Federated Chain
- User Data Protection
- Forced On-Chain Transactions

Clase 9: Patrones de Integridad y Validación

Discusión:

Aplicando sus experiencias y conocimientos previos:

¿Cuáles son los Patrones de Integridad y Validación?

Patrones de Integridad y Validación

Definición

- Block Singleton
- Sidechain
- Block Validation Consensus

Discusión:

Aplicando sus experiencias y conocimientos previos:

¿Qué será el Patrón Block Singleton?

Patrones de Integridad y Validación

Block Singleton

¿Cómo se puede prevenir que un usuario agregue bloques duplicados a la cadena?

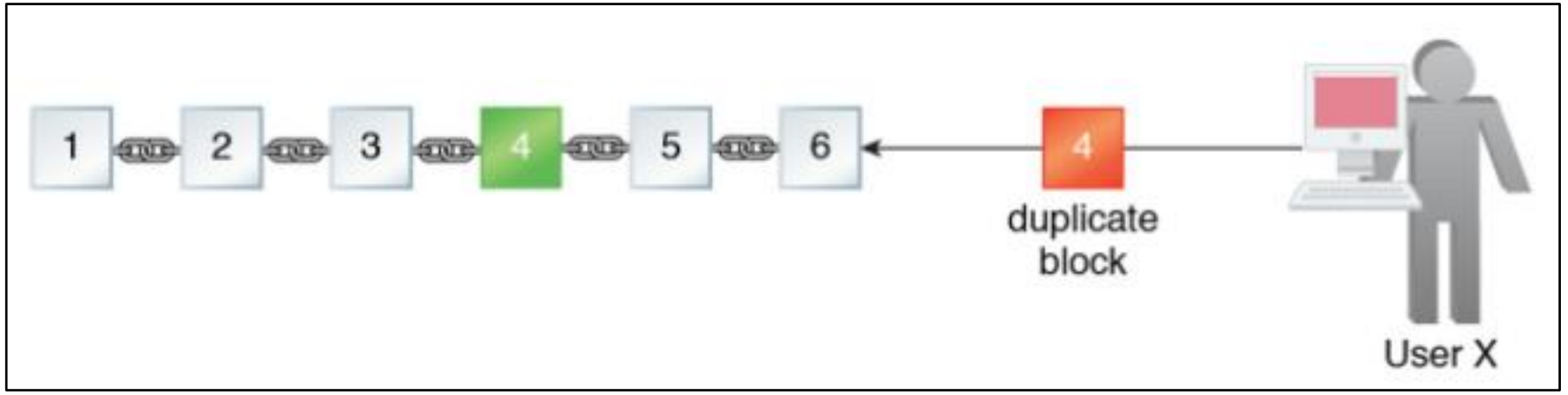
Patrones de Integridad y Validación

Block Singleton

Problema Un usuario malicioso puede intentar crear un bloque duplicado (o un bloque conteniendo registros duplicados) y enviarlo a la Red Blockchain para agregarlo a la cadena principal (main chain), comprometiendo la integridad del Distributed Ledger.
Solución La aplicación Blockchain es diseñada para verificar si los bloques y registros enviados a la Red Blockchain ya existen en la cadena principal.
Aplicación Los mecanismos de Consensus Processor y Hashign Engine son programados para verificar cada nuevo bloque enviado y su contenido, contra los bloques existentes en la cadena, con la finalidad de identificar duplicados.
Mecanismos Block Maker, Consensus Processor, Hashing Engine

Patrones de Integridad y Validación

Block Singleton

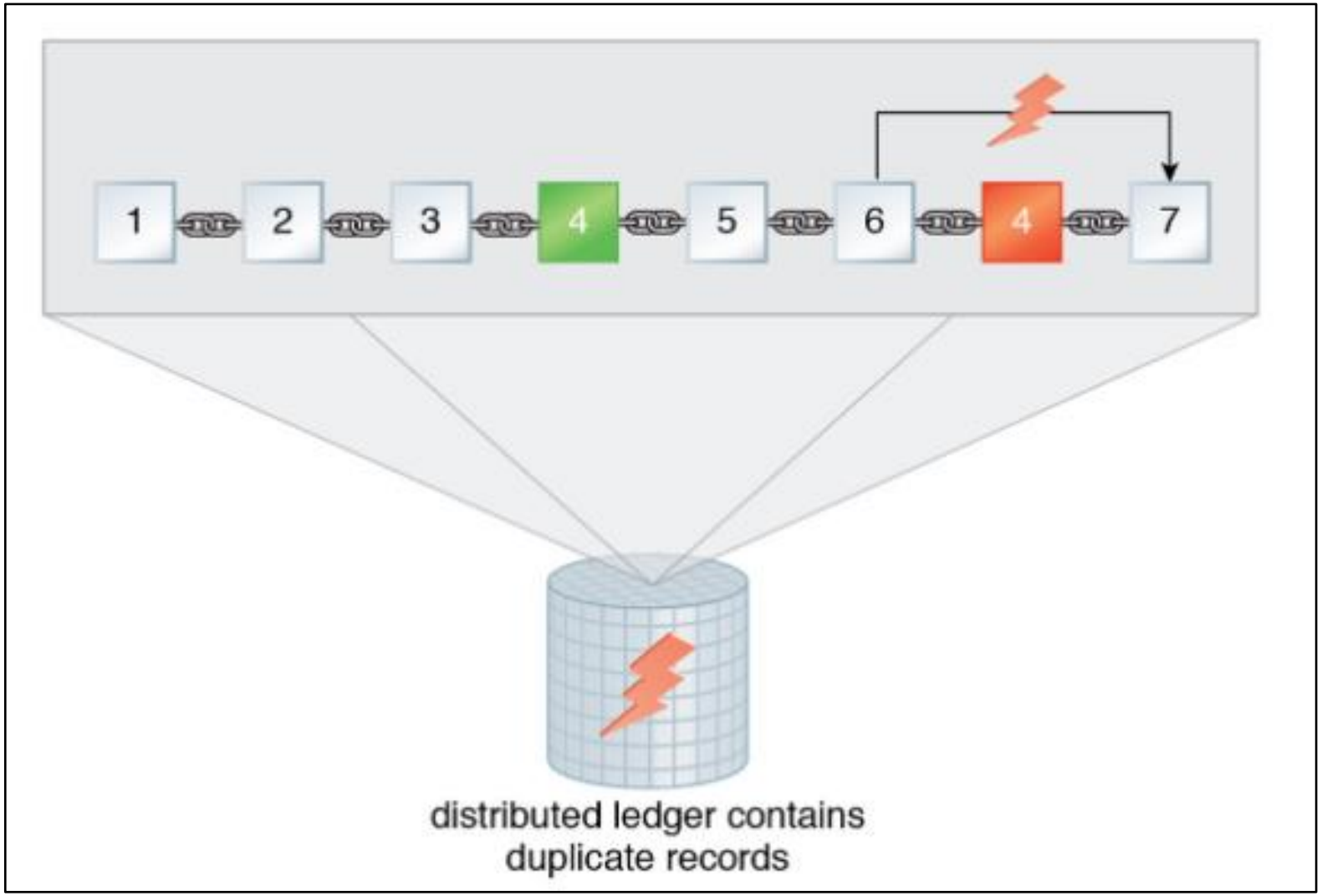


El usuario malicioso X intenta agregar el bloque 4 a la cadena, a pesar de que el mismo bloque 4 ya ha sido agregado a la cadena.

Patrones de Integridad y Validación

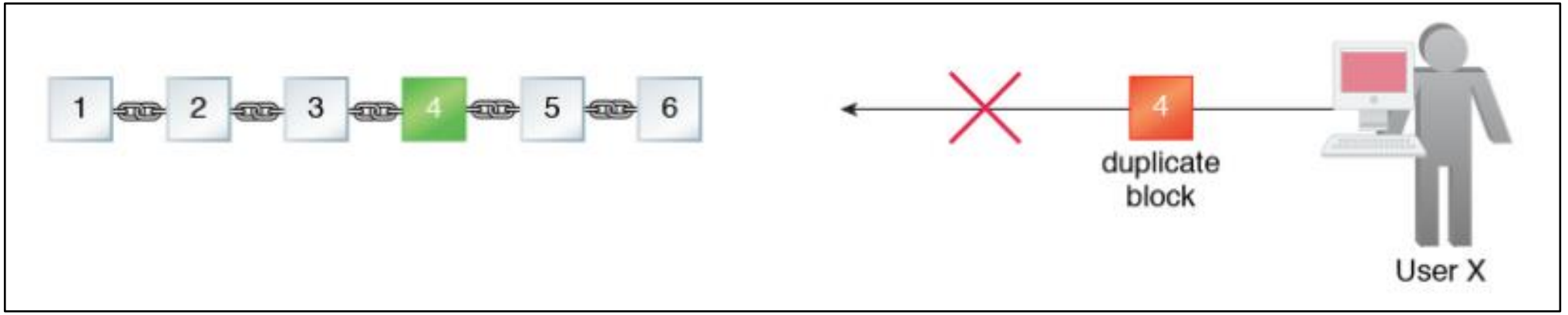
Block Singleton

La Aplicación Blockchain no detecta que el nuevo bloque agregado es un duplicado, y permitió que el nuevo bloque 4 invalido se agregado posterior al bloque 6, y previo al bloque 7. Por tanto, esto compromete la integridad de la cadena y del Ledger.



Patrones de Integridad y Validación

Block Singleton

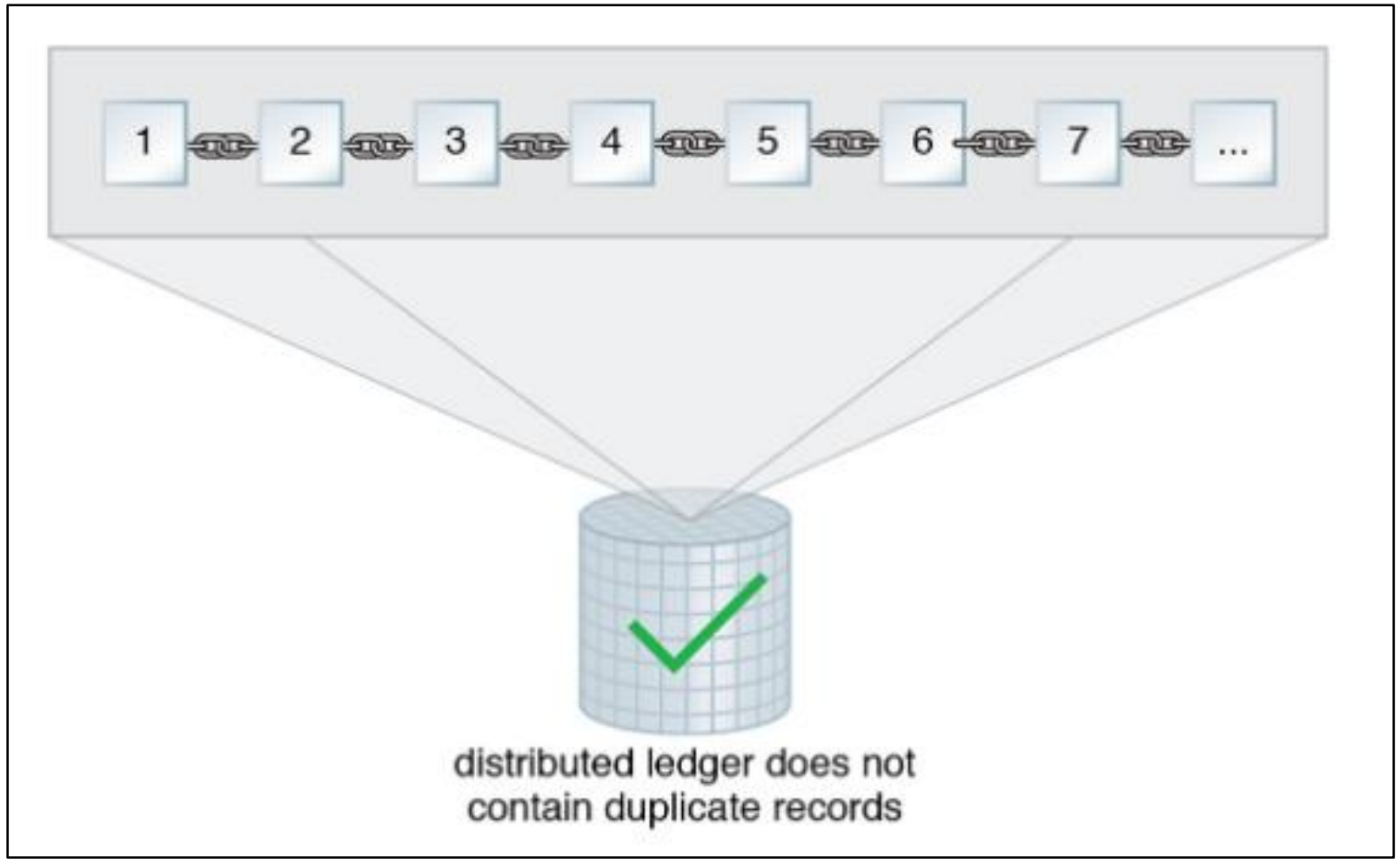


El bloque duplicado es identificado como que ya forma parte de la cadena, y es rechazado.

Patrones de Integridad y Validación

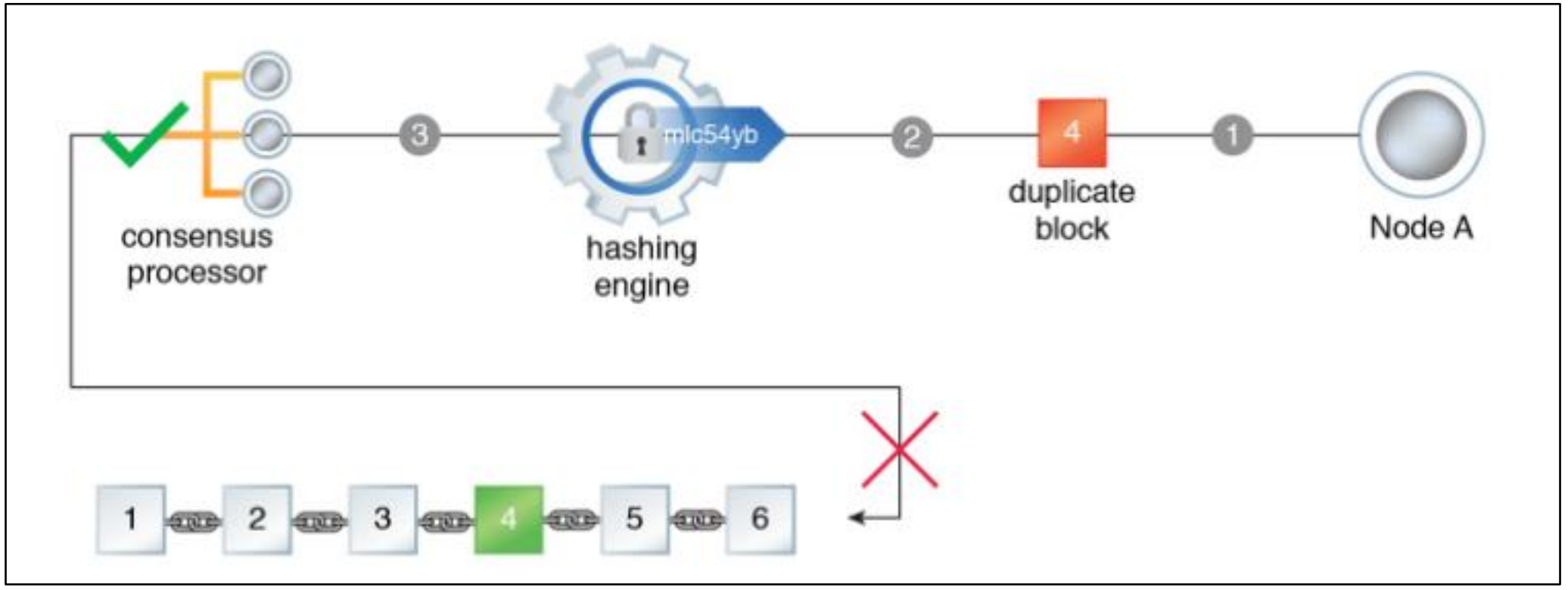
Block Singleton

La cadena continua disponible para agregar nuevos bloques en el correcto orden secuencial sin duplicación, por tanto mantiene la integridad del Distributed Ledger.



Patrones de Integridad y Validación

Block Singleton



Gráfica de la solución

Patrones de Integridad y Validación

Block Singleton

Los mecanismo Hashing Engine y Consensus Processor son programados para establecer una “línea de defensa de dos”.

El Hashing Engine determina si un bloque enviado está ya agregado con el mismo hash. Esto puede ocurrir cuando un usuario malicioso intenta corromper la Blockchain agregando un bloque duplicado mediante un diferente número de ID de Bloque. Ejemplo: duplicar el Bloque 4, utilizando el Bloque 7.

Patrones de Integridad y Validación

Block Singleton

El **Consensus Processor** puede ser programado para habilitar que los nodos participantes en el consenso identifiquen y verifiquen si un registro dado es el duplicado de uno previo. También puede ayudar a verificar cuando el nuevo bloque intenta ocultar registros duplicados mediante la mezcla con nuevos registros o de registros duplicados de bloques existentes.

Patrones de Integridad y Validación

Block Singleton

Cuando un bloque con contenido duplicado es identificado, el mecanismo **Block Maker**, puede ser programado para enviar una notificación a los nodos full participantes para prevenir que el bloque duplicado sea agregado a la cadena. Alternativamente, el **Block Maker** puede ser diseñado para destruir automáticamente un bloque después de que se ha confirmado que es un duplicado.

Discusión:

Aplicando sus experiencias y conocimientos previos:

¿Qué será el Patrón Sidechain?

Patrones de Integridad y Validación

Sidechain

¿Cómo una Aplicación Blockchain para Usuario Final puede sobrellevar una transacción off-chain sin comprometer la integridad de la cadena principal (main-chain)?

Patrones de Integridad y Validación

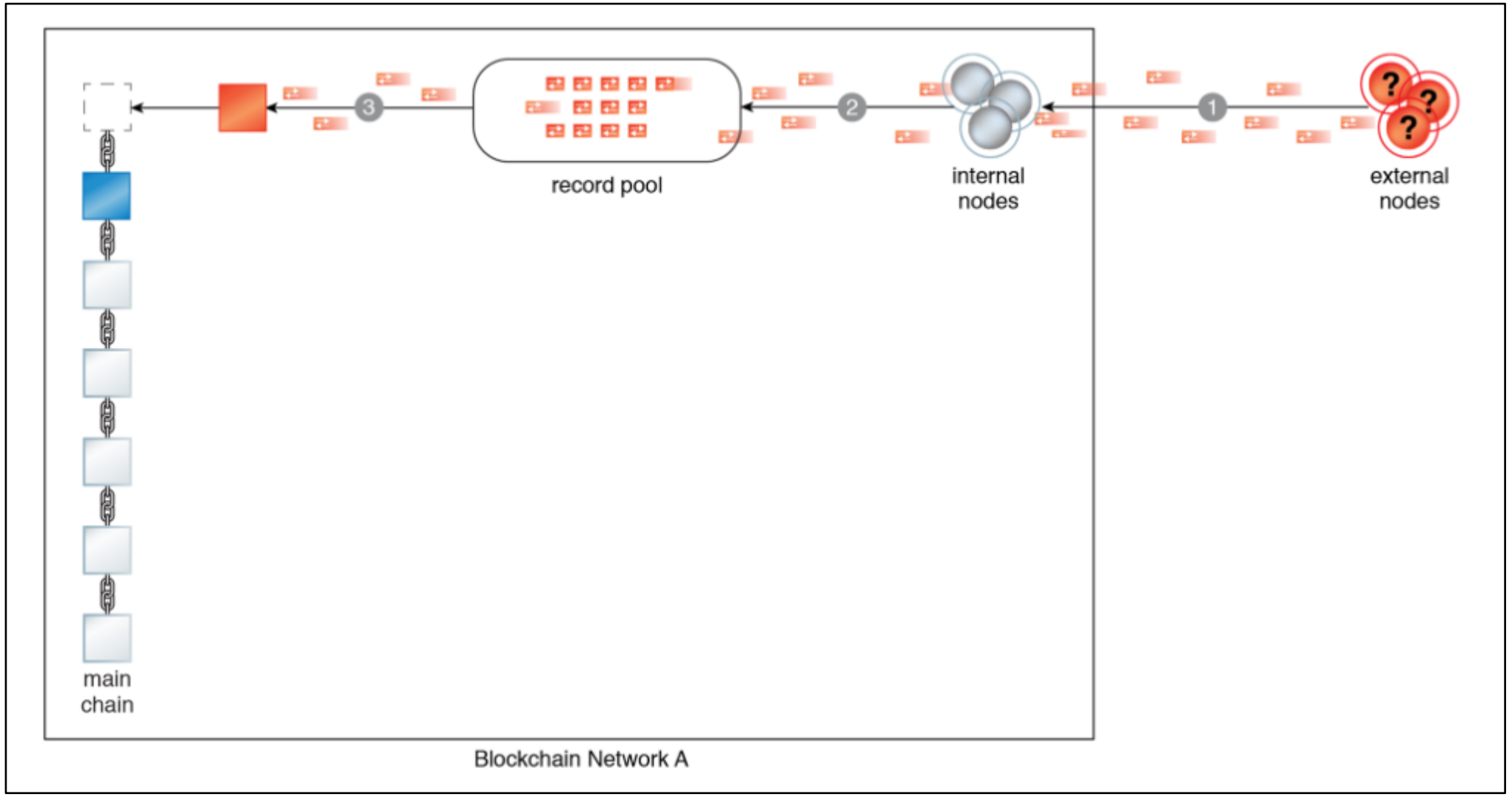
Sidechain

Problema Cuando un usuario de Aplicación Blockchain ejecuta una transacción con otro usuario fuera de la Red Blockchain, la transacción no puede ser completamente validada o sujeta al consenso dentro de la Aplicación Blockchain. Si las transacciones son escritas en la cadena principal (main chain) y luego se torna inválido, eso compromete la integridad del Distributed Ledger.
Solución La Aplicación Blockchain permite que las actividades off-chain sean registradas fuera de la cadena principal hasta que pueda ser seguramente determinado que los registros asociados son válidos.
Aplicación Una Sidechain es creada y enlazada a la cadena principal, pero la composición de bloques son separados hasta que sea considerado seguro para mezclarlos en la cadena principal.
Mecanismos Block Maker, Chaining Engine

UNMSM

Patrones de Integridad y Validación

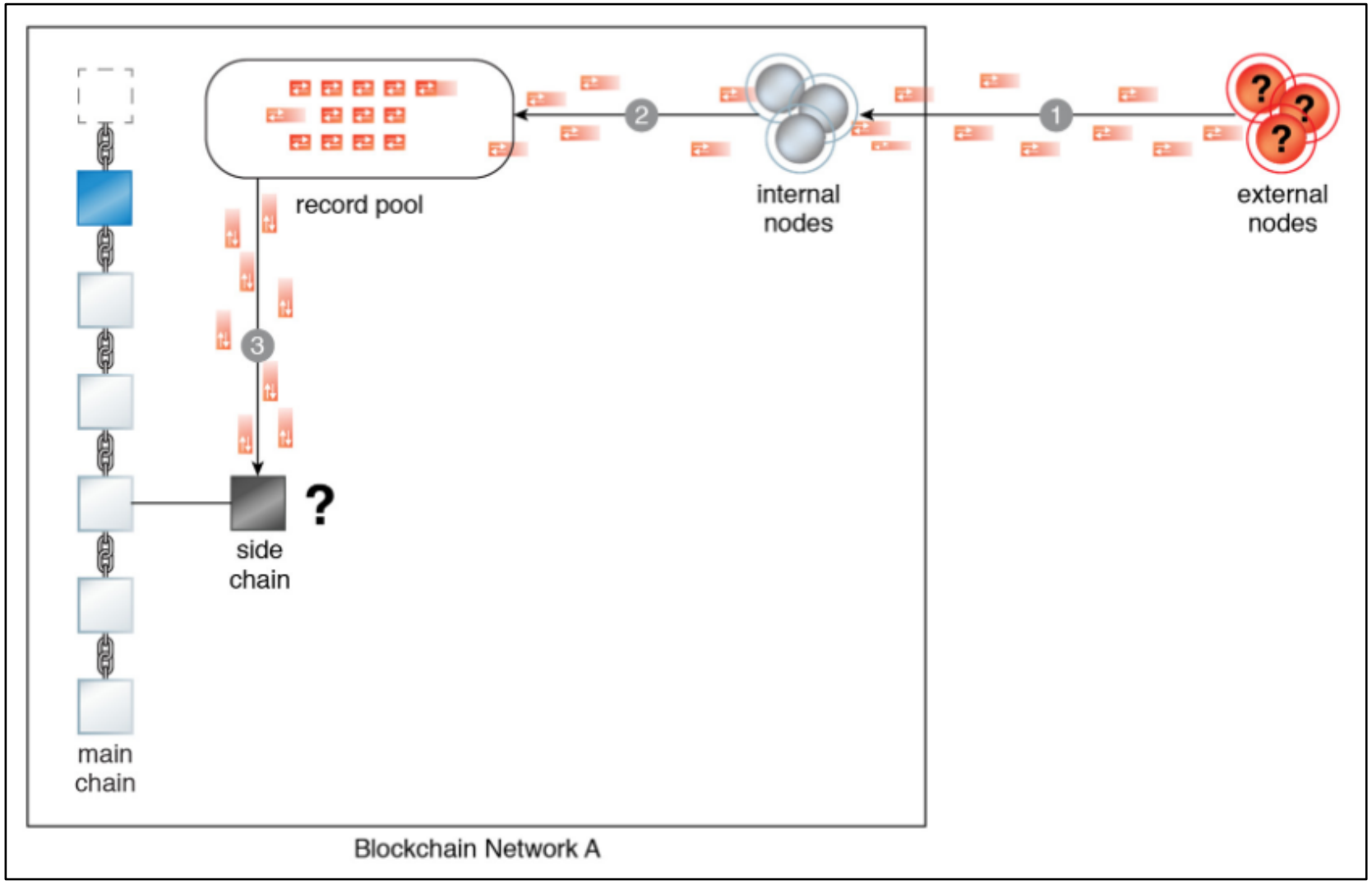
Sidechain



Los bloques validados fuera de la Red Blockchain A (off-chain) se podrían asumir como válidos al interno. Por tanto, hay un riesgo de agregar esos bloques a la cadena principal.

Patrones de Integridad y Validación

Sidechain

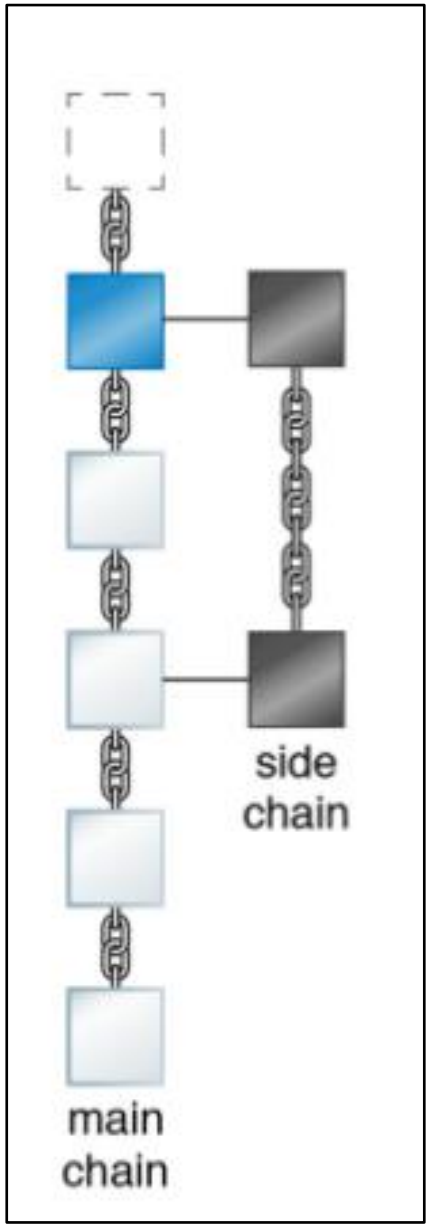


Los registros de la off-chain que no han sido confirmados como válidos, son colocados en la sidechain fuera la cadena principal

Patrones de Integridad y Validación

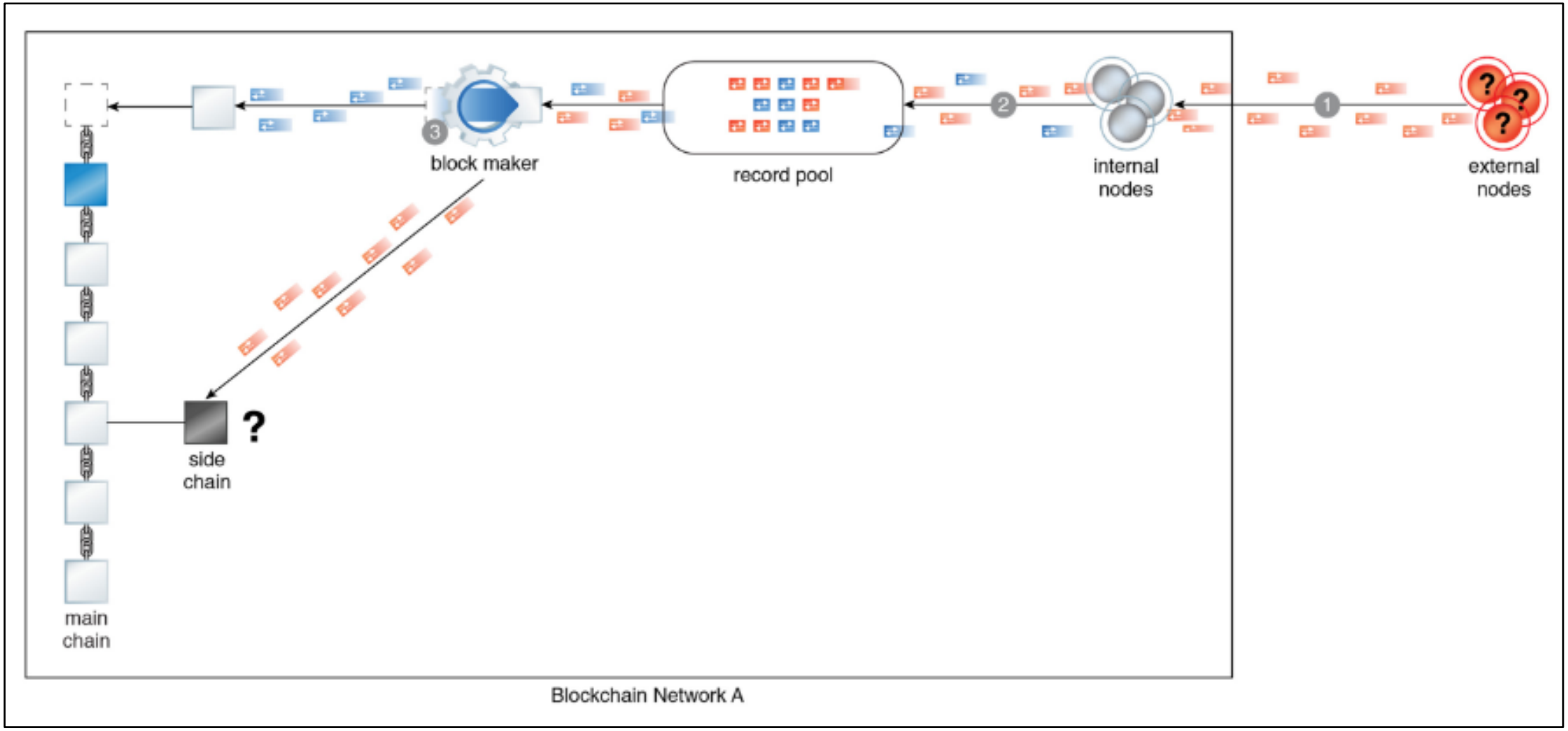
Sidechain

Los bloques sidechain creados en diferentes puntos de tiempo, pueden ser encadenados entre ellos.



Patrones de Integridad y Validación

Sidechain

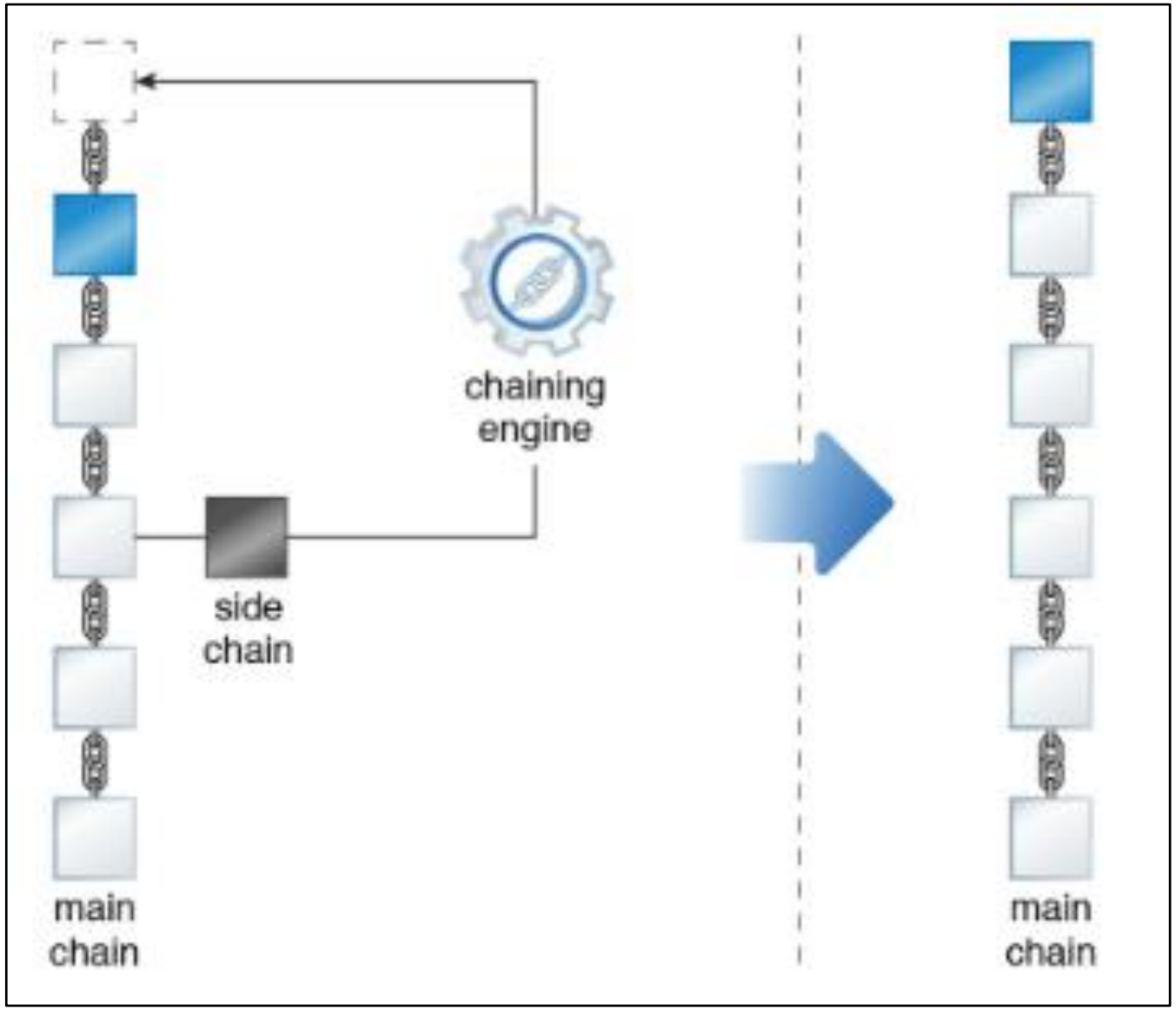


Gráfica de la solución

Patrones de Integridad y Validación

Sidechain

En algún punto la side chain y la cadena principal van a requerir ser combinados. El side chain es considerado válido y el chaining engine los combina, dejado no activo el side chain.



Discusión:

Aplicando sus experiencias y conocimientos previos:

¿Qué será el Patrón Block Validation Consensus?

Patrones de Integridad y Validación

Block Validation Consensus

¿Cómo un bloque de datos puede ser comprensiblemente validados previo a que sean permanentemente escritos al Distributed Ledger?

Patrones de Integridad y Validación

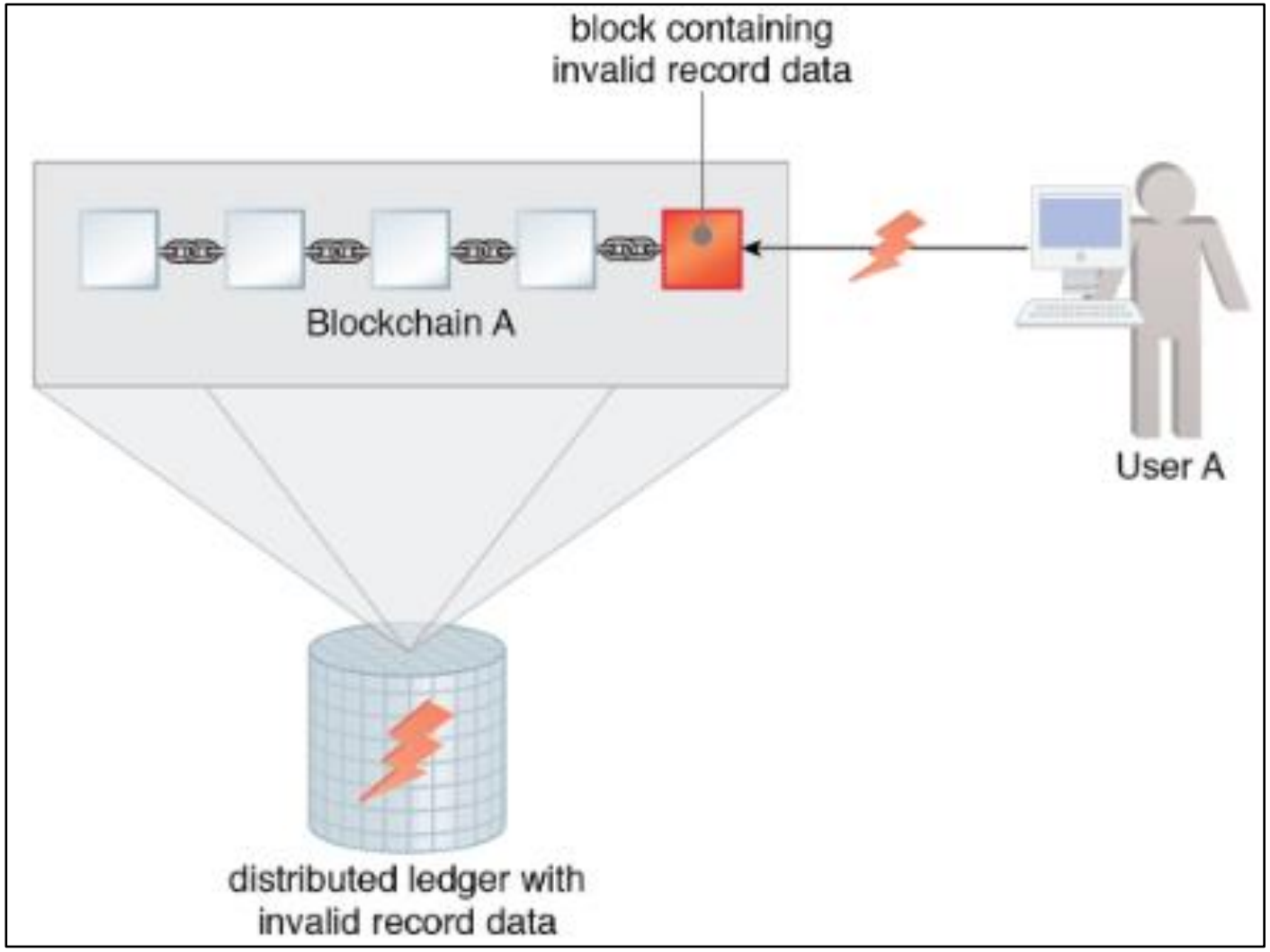
Block Validation Consensus

Problema Si una data invalida es permanente y inmutablemente almacenada en el Distributed Ledger, eso puede comprometer enteramente la integridad de la Aplicación Blockchain y la confianza de sus usuarios.
Solución Un proceso formal de validación se lleva acabo para múltiples nodos antes de enviar los registros de los datos a ser aprobados para su inserción en el **Distributed Ledger**.
Aplicación Un algoritmo de consenso es escogido e implementado vía el **Consensus Processor** para ejecutar el proceso de validación de bloques.
Mecanismos Consensus Procesor

Patrones de Integridad y Validación

Block Validation Consensus

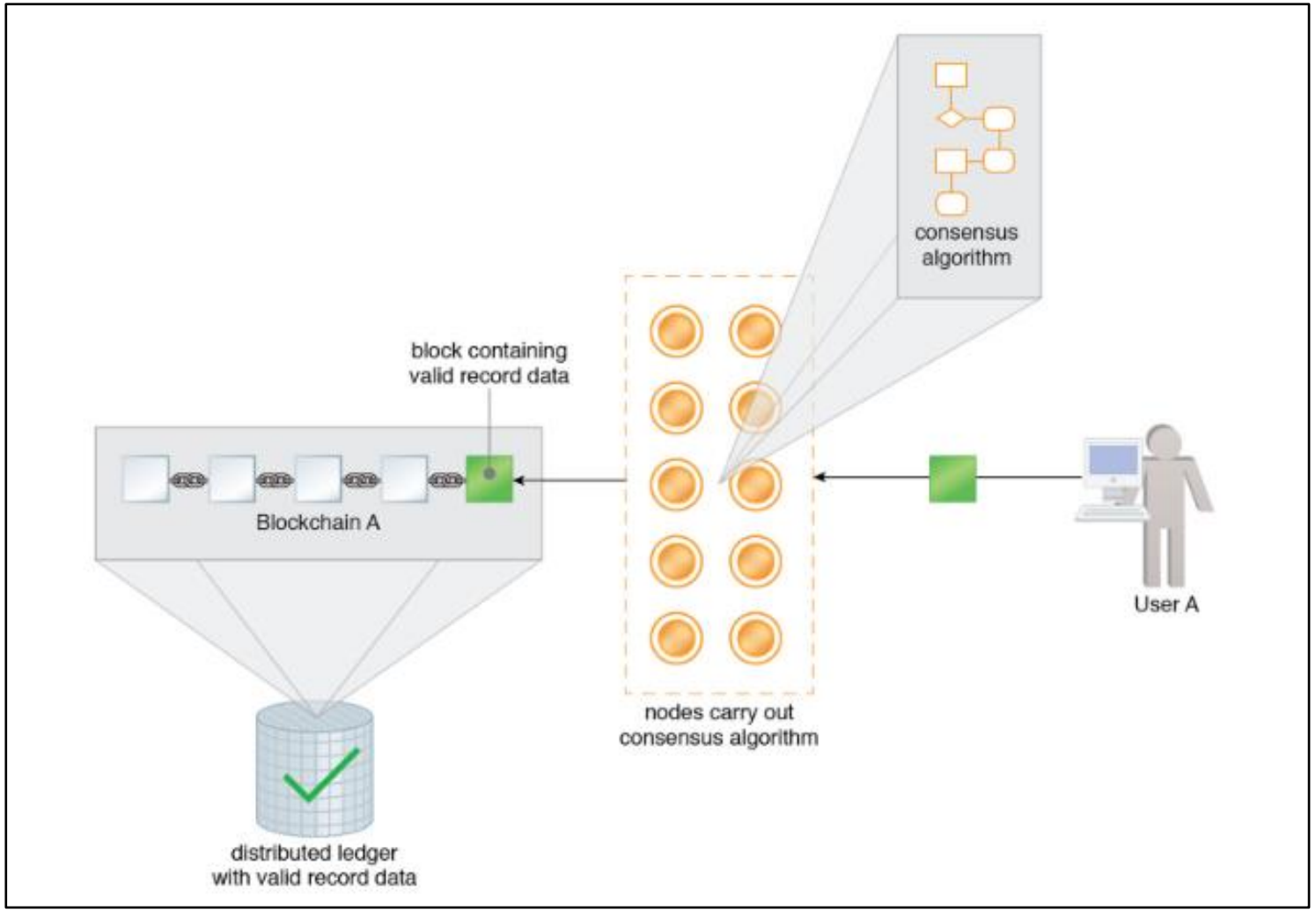
Un usuario envía (inadvertida o deliberadamente) un registro de datos invalido que es permanentemente escrito en el Distributed Ledger, por tanto eso impacta directamente en la confianza como fuente de verdad.



Patrones de Integridad y Validación

Block Validation Consensus

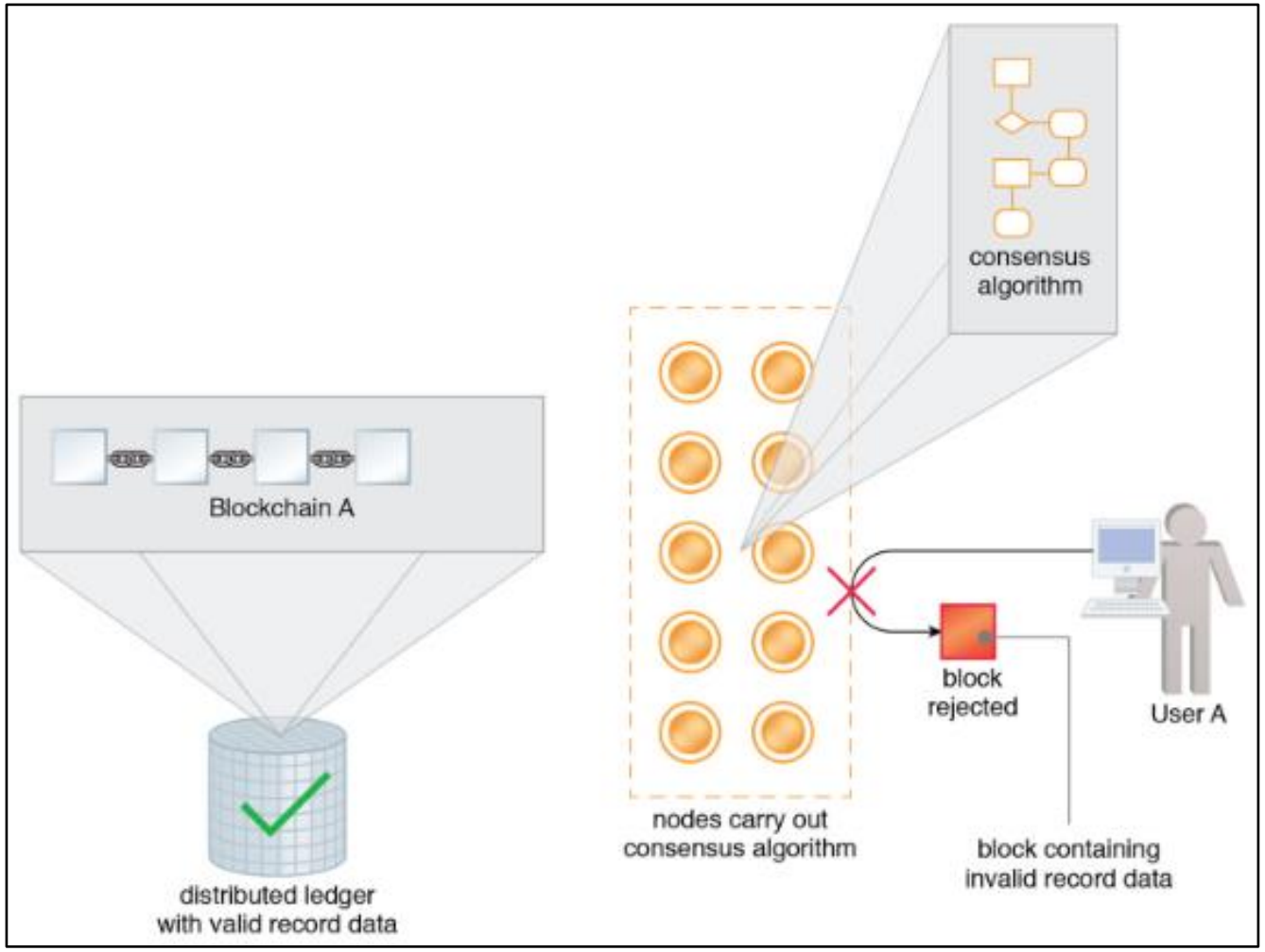
Con solución, previo al registro se debe ejecutar un algoritmo de consenso en múltiples nodos para la validación del bloque, y una vez validado se podrá registrar en el Distributed Ledger.



Patrones de Integridad y Validación

Block Validation Consensus

Si el algoritmo de consenso arroja como resultado una inconsistencia, entonces se evidencia la invalidación y se rechaza el bloque sin registralo en el Distributed Ledger.



Patrones de Integridad y Validación

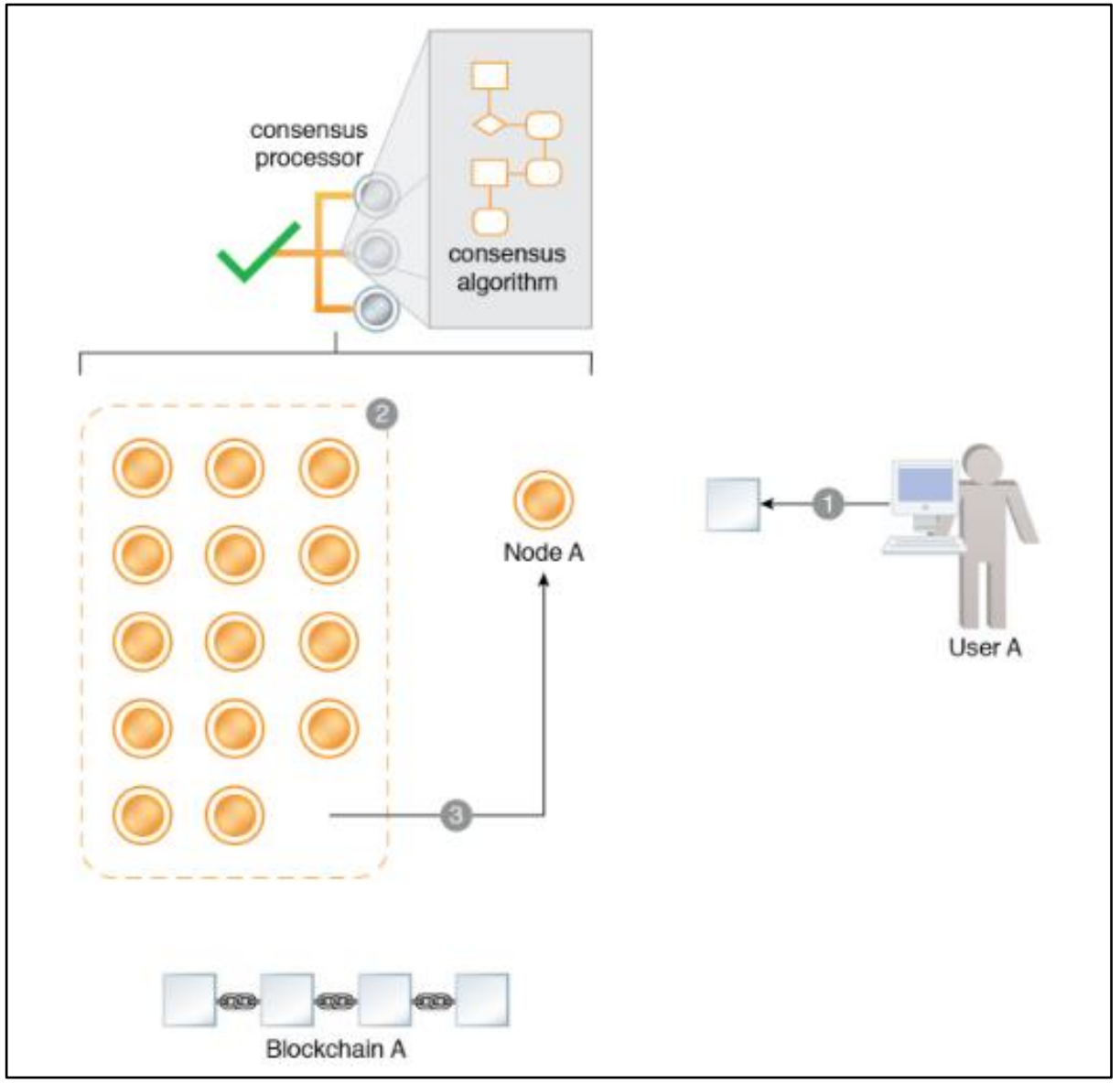
Block Validation Consensus

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Proof of Activity (PoA)
- Delegated Proof of Stake (DPoS)
- Leased Proof of Stake (LPoS)
- Proof of Importance (PoI)
- Proof of Elapsed Time (PoET)
- Round Robin
- Proof of Capacity (PoC)
- Proof of Burn (PoB)

Patrones de Integridad y Validación

Block Validation Consensus

El usuario envía un bloque para su validación, el Nodo A es agregado al pool de validación.



Patrones de Integridad y Validación

Block Validation Consensus

El Nodo A valida el bloque. Además, el bloque es adicionalmente aprobado por los participantes del consenso. Se agrega el bloque a la cadena principal.