



El futuro digital
es de todos

MinTIC



Blockchain

& analítica de datos
para industrias digitales





Sesión 16: Requerimientos técnicos de la infraestructura descentralizada



Contenido

- Necesidades
- Capacidad de Transacciones
- Volumen de Información
- Costo de Información
- Escoger la Tecnología
- Blockchain Privada
- Blockchain Publica
- Despliegue de Nodos
- Tamaños de Almacenamiento y tipos de Nodos
- Ancho de banda
- Poder de Procesamiento
- Cantidad de Validadores
- Conclusiones



Necesidades del Proyecto

Dependiendo de las dimensiones del proyecto (cantidad de usuarios, flujo de datos, etc..), se deben establecer unos requerimientos funcionales y económicos con el objetivo de seleccionar la solución tecnológica adecuada.

En algunos casos de uso es pertinente implementar nuevas redes, en otros casos es posible abordar la solución haciendo uso de alguna red existente mediante contratos inteligentes.

Los criterios principales a definir son:

- Capacidad de Transacciones
- Volumen de Información
- Costo de la Información

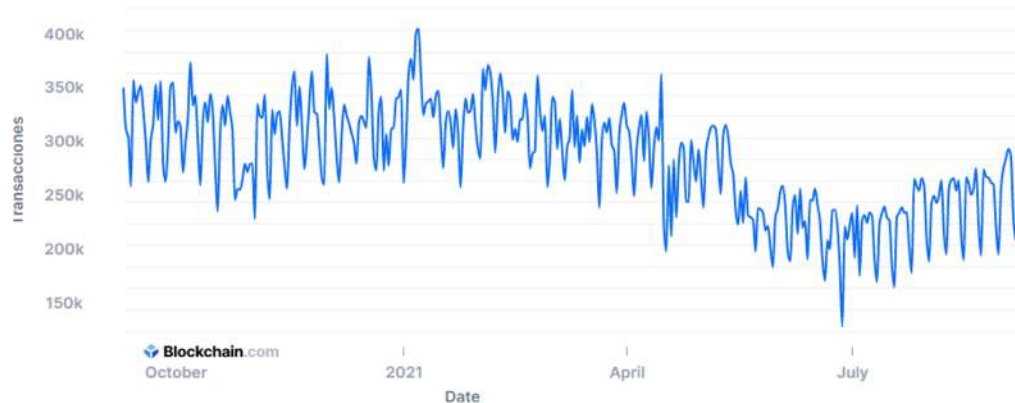




Capacidad de transacciones

Es la velocidad de transacción promedio, la cual proporciona un indicador de la capacidad actual de la red para procesar una transacción. Esto nos asegura que el sistema permanezca en línea, sea utilizable y operativamente consistente. En el caso de bitcoin se realizan 272.360 transacciones al día con un tamaño de bloque de hasta 2 MB dando capacidad para un máximo de 7 transacciones por segundo. Sin un límite, un atacante podría crear un bloque o bloques lo suficientemente grandes como para paralizar la red entera.

Algunos problemas que pueden afectar la velocidad por transacción son: la complejidad de las transacciones (múltiples entradas y salidas), tamaño de bloque (cantidad de transacciones que puedan almacenarse en el mismo bloque) y estado de la red si tienes transacciones en cola o no.



<https://www.blockchain.com/charts/n-transactions>



Capacidad de transacciones

Cryptocurrency	Transactions per Second	Average Transaction Confirmation Time
Bitcoin	3-7	60 min
Ethereum	15-25	6 min
Ripple	1500	4 s
Bitcoin Cash	61	60 min
Stellar	1000	2-5 s
Litecoin	56	30 min
Monero	4	30 min
IOTA	1500	2min
Dash	10-28	15 min

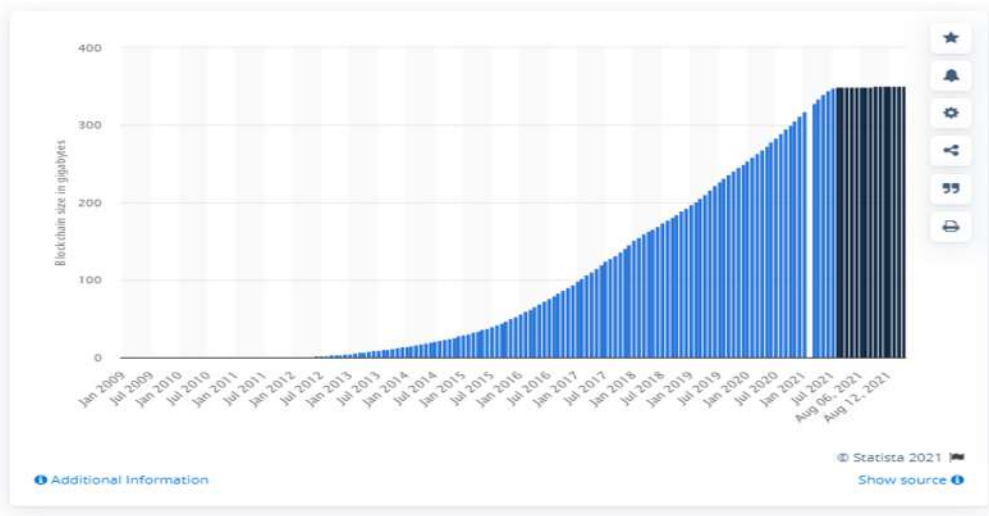
<https://blog.tezro.com/cryptocurrency-transaction-speeds/>



Volumen de Información

Se basa en que a mayor tamaño del bloque más tiempo se necesitará para propagarlo por la red y mayor almacenamiento será consumido a largo plazo a medida que se creen nuevos bloques. Por lo tanto, a mayor capacidad más transacciones podrán almacenarse en un bloque, beneficiando a los usuarios pero perjudicando a los mineros que deben asumir los costos de ese almacenamiento.

Si mi caso de uso requiere grandes volúmenes de información se requiere una Blockchain de mayor escalabilidad o apoyar con sistemas complementarios y usar la Blockchain en los procesos críticos de seguridad.



<https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/>



Costo de la información

Toda información guarda en Blockchain tendrá un costo por eso es importante reconocer si la información que estamos almacenando vale tanto la pena como para pagar una comisión. En una analogía, si compramos una caja fuerte, lo que guardemos en esa caja fuerte debe ser más valioso que la caja para que tenga sentido. El valor que aporta la red al proteger la información debe ser superior al costo de almacenarla para que el caso de uso sea relevante.





Escoger la tecnologías

Es necesario escoger el tipo de red idónea, si se va a crear a partir de un consorcio de empresas privadas o si será una infraestructura pública o privada existente, o si se quiere proponer una nueva infraestructura pública para un ecosistema o comunidad.





Blockchain Privada

- Se denomina privada o “permissioned” cuando depende se convierte en eje central quien define el acceso a la red como validador.
- Este tipo de redes se utiliza en casos de uso específicos donde un grupo de empresas o individuos particulares tienen intereses o procesos compartidos que podrán verificarse y auditoría durante una única red compartida entre los participantes.
- Suelen limitar el número de validadores para conservar la eficiencia y velocidad de la red reduciendo el tiempo de validación o propagación en la misma.
- Algunas redes privadas utilizan protocolos como la prueba de autoridad donde los validadores se autorizan únicamente si cumplen atributos específicos.
- Ejemplo POA network es una red de prueba de autoridad privada, donde los validadores son autorizados por ser notarios verificados en USA y su funcionamiento está basado en la ethereum virtual machine permitiendo migrar proyectos de la red pública de ethereum a la red privada de POA e incluso comunicar ambas redes.





Blockchain Pública

- esta red permite que cualquier usuario pueda hacer parte e incluso modificarla ya que no cuenta con ningún eje o organismo central que regule el funcionamiento de la misma.
- Las actualizaciones y mejoras se realizan por medio de consenso entre los diferentes participantes de la red y su comunidad.
- Las redes públicas representan un mayor grado de seguridad o un mayor nivel de confianza digital debido a su descentralización, sin embargo ese nivel de seguridad tiene un precio a pagar en velocidad y costos de transacción, por lo que su uso no es viable en algunos casos de uso.





Despliegue de un Nodo

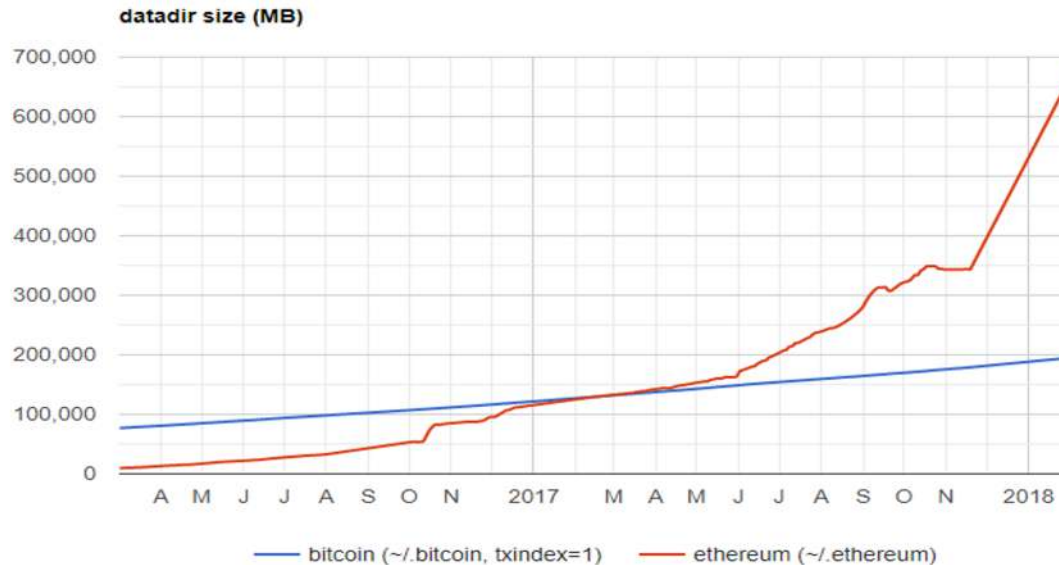
- Cuando se implementan Blockchain nuevas, sean públicas o privadas, o se desea conectarse como nodo directamente a una red existente para leer o registrar información en la misma, se requiere instalar un nodo corriendo el algoritmo de consenso correspondiente.
- Si nuestra implementación se basa en un contrato inteligente se pueden utilizar servicios de terceros como nodos en esa comunicación con la red, pero esto representará vulnerabilidades y centralizará el acceso a la misma al depender de ese único proveedor.





Tamaño de Almacenamiento y Tipos de Nodo

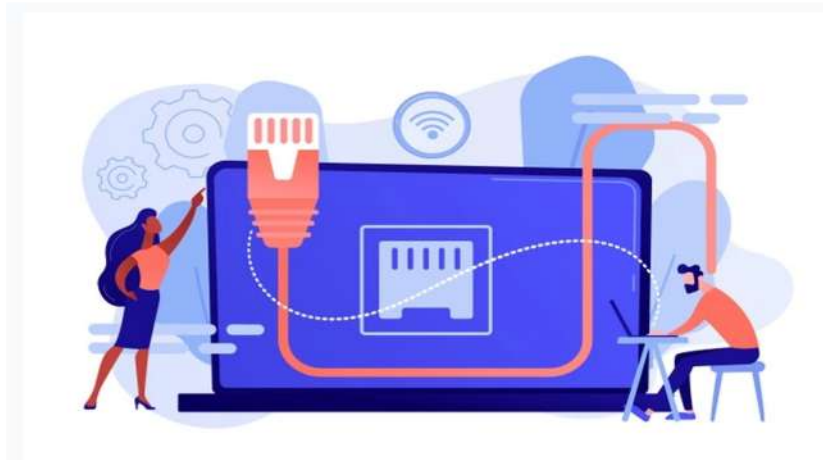
- Existen diferentes tipos de nodos en las Blockchain, algunos llamados nodos mineros o full nodes, deben tener la mayor cantidad de almacenamiento disponible ya que almacenan la información completa (en la Blockchain de Bitcoin 350Gb de memoria disponible). Por otro lado existen nodos ligeros que se conectan a nodos full y permiten validar los datos de este y compararlo con el de los demás nodos utilizando algoritmos hash.





Ancho de banda

- Las redes Blockchain consumen ancho de banda en el proceso de propagación de información a todos los nodos o validadores. Cada nodo debe tener una disponibilidad de ancho de banda específica que aumentará conforme a la cantidad de participantes adicionales tenga la red.
- Los tiempos de propagación de la información y los tiempos de minado de bloques nuevos están correlacionados y afectan el sistema porque las posibles soluciones tienden a la centralización.





Poder de procesamiento (hashpower)

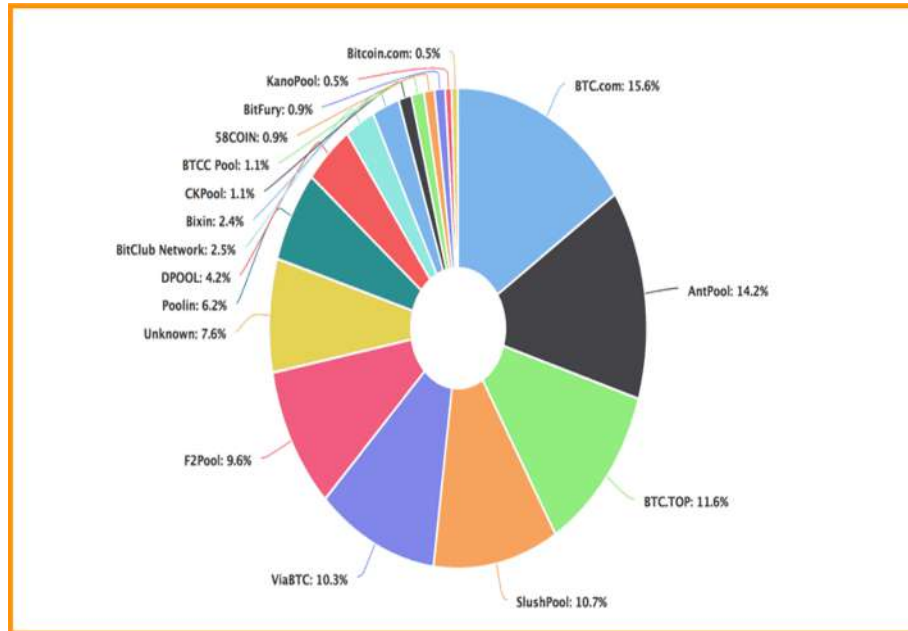
- En las redes blockchain que utilizan la prueba de trabajo, miden su nivel de seguridad y la participación de los nodos en hash/segundo. Entre mayor sea el nivel colectivo de hash power medido en hash/segundo, se considera más difícil vulnerar dicha red.
- Los algoritmos de prueba de trabajo regulan la seguridad y centralización aumentando la dificultad de minado conforme aumenta el poder de minado de la red, por lo que hace económicamente inviable la participación para mineros de bajo poder computacional, para esto existen alternativas llamadas pools de minería donde se juntan varios individuos y se unifica su poder computacional en un representante.





Cantidad de Validadores

- Cuanto más crece la cadena de bloques, mayores se vuelven los requisitos de almacenamiento, ancho de banda y potencia computacional que deben gastar los "nodos completos" en la red, lo que genera un riesgo de centralización mucho mayor si la cadena de bloques se vuelve lo suficientemente grande como para que solo unos pocos nodos puedan procesar un bloque.

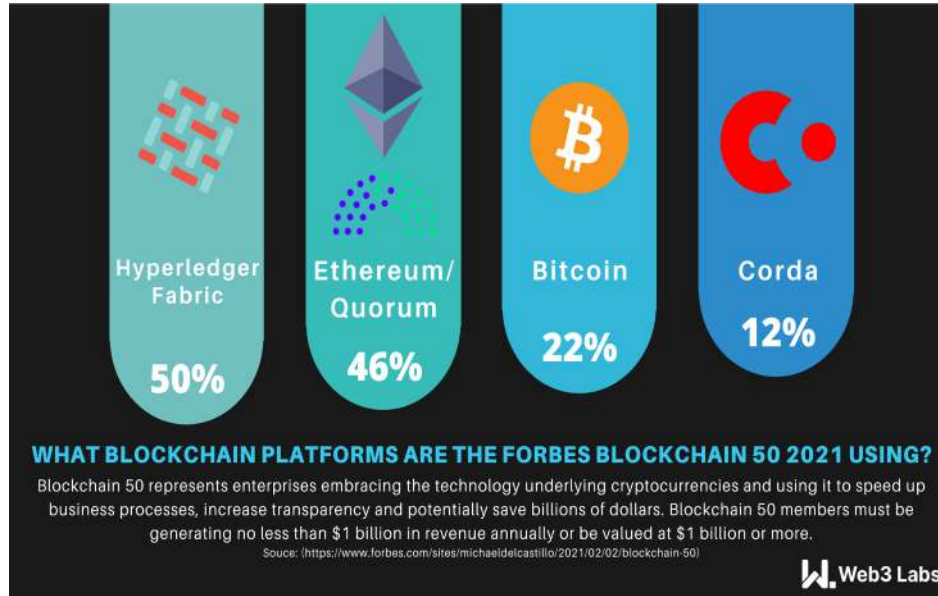


<https://coinsutra.com/hash-rate-or-hash->



Conclusiones

- Para cada caso de uso existe una alternativa que se acomode a sus presupuestos y necesidades según las ventajas o desventajas de cada red o tecnología de registro distribuido. Cada tecnología trae consigo sus propios retos de escalabilidad, consumo de recursos y eficiencia que se relaciona directamente con el nivel de seguridad.



<https://blog.web3labs.com/blockchain-technology->



Agenda

- Notación gráfica estandarizada BPMN.
- Modelación de procesos de negocio.
- Estrategia de modelación de procesos.



Diagramas de Flujo







El futuro digital
es de todos

MinTIC



El BPMN o Business Process Model and Notation es una notación estándar para modelar gráficamente procesos de negocio.



Fue creado por Business Management Initiative, ahora fusionado con Object Management Group (OMG), un grupo de establecimiento de estándares de sistemas de información.





Es un estándar ISO para
modelado de procesos de
negocio ISO / IEC
19510:2013



International
Organization for
Standardization



¿Qué es BPMN?

Business Process Model and Notation

¿Porque es importante BPMN?

Información, actividades y mensajes entre participantes



¿Porque es importante definir nuestros procesos de negocios?



Todas las empresas y organizaciones funcionan con procesos, aunque muchas no los tienen definidos



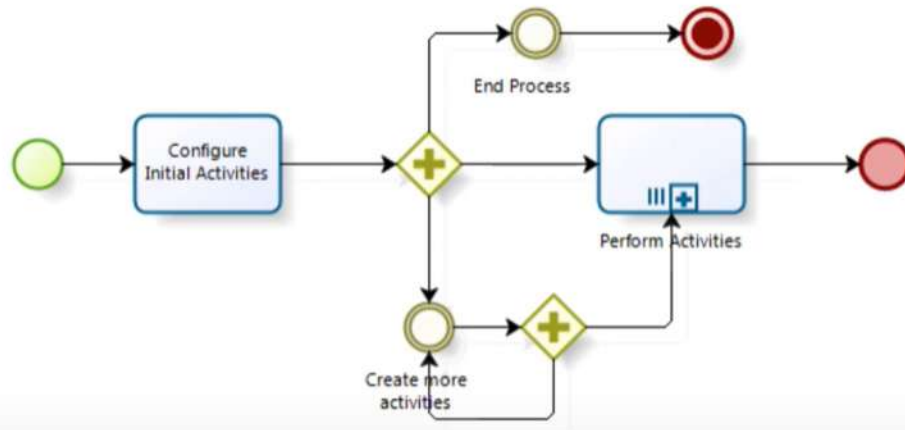
Problemas comunes al no tener definidos nuestros procesos

- Duplicidad de actividades
- Reprocesos
- Desconocimiento de qué hacer
- Burocracia
- Demasiado papel
- Variabilidad para conseguir el mismo resultado
- Demasiado tiempo y esfuerzo
- Alta dependencia de las personas para cumplir
- Bajo nivel de calidad



Problemas comunes al no tener definidos nuestros procesos

Ad hoc

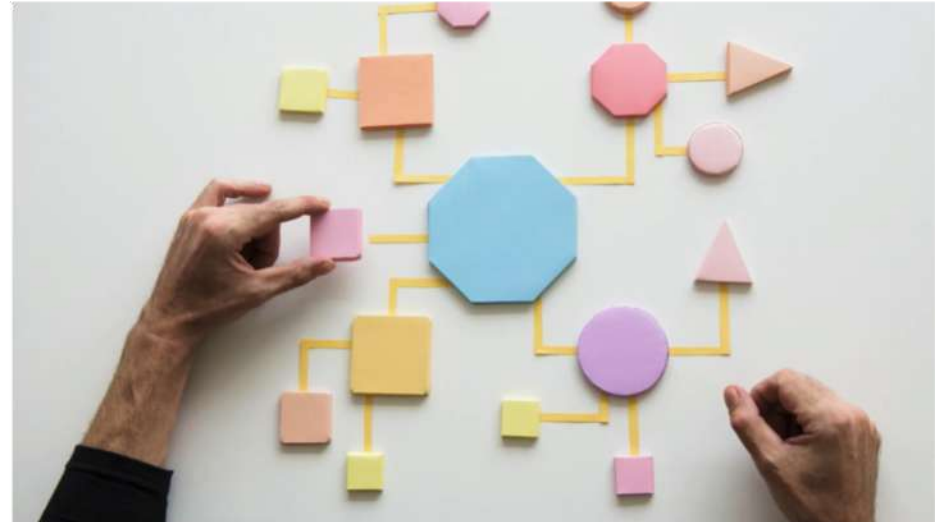


La herramienta más común ayudar a definirlos y entenderlos son los modelos de procesos



¿Cómo definir nuestros procesos?

Un modelo de proceso es la representación analítica o gráfica de los procesos de una organización.





¿Beneficios de modelar procesos?

- Ahorrar dinero reduciendo costos
- Mejorar la calidad
- Reducir tiempo de producción
- Incrementar la productividad
- Reducir tiempos de entrega
- Identificar más fácil las causas de los problemas
- Mantener el conocimiento del procesos
- Estandarizar el desempeño de quienes intervienen en el proceso



¿Cómo se modelan los procesos de negocios?

Los procesos se modelan a través del uso de notaciones y técnicas estándar





Beneficios de la notación BPMN

1. Permite que los profesionales de procesos y TI tengan un mismo conjunto de símbolos, lenguaje y técnicas para representar los procesos.
2. Los procesos son consistentes en forma y significado, facilitando el diseño, análisis y medición
3. Es posible importar y exportar los modelos entre diferentes herramientas.
4. Los modelos gráficos se pueden transformar en aplicaciones de software para su control



Elementos Básicos de Notación BPMN 2.0

1. **Conectores:** elementos de conexión de la secuencia de flujos de trabajo.
2. **Actividades:** representan el trabajo a realizar.
3. **Gateways o Compuertas:** muestran la ramificación y la reunión del flujo de tareas.
4. **Eventos:** indican eventos externos que influyen en el proceso.



1. Conectores:

Flujo de secuencia de las actividades



Flujo de mensajes:



Asociación de artefactos y elementos del flujo





2. Actividades

Tarea:



Tarea de notificación por mensaje:



Subproceso:



Tarea de servicio:



Tarea manual:



Tarea de envío de mensaje:



Tarea de usuario en un sistema de workflow:





3. Eventos

El proceso se inicia con la llegada de un mensaje.



Se debe enviar o recibir un mensaje.



Se enviará un mensaje a otro proceso con el final de este flujo.



Tiempo: el proceso se inicia por una condición de tiempo.



Condicional: una condición lógica determina el comienzo del evento.





Señal: una señal recibida de otro proceso inicia este proceso.



Programación: una excepción de negocio inicia el proceso.



Múltiple: uno de muchos eventos posibles inicia el proceso.



Error: captura la aparición de un fallo.



Múltiple paralelo: deben ocurrir varios eventos para iniciar el proceso.





4. Gateways o Compuertas

Exclusivo basado en los datos: el flujo sigue por una condición exclusiva.



Paralelo: el flujo se divide en otros que ocurren en paralelo.



Inclusivo: el flujo sigue una condición inclusiva





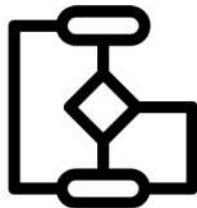
Complejo: Controla condiciones complejas de divergencia y también de convergencia.



Intermediario exclusivo basado en eventos: siempre se utiliza para dividir el flujo



Herramienta que transforma los sistemas legacy para transformar las compañías en organizaciones ágiles, cautivadoras y conectadas con los negocios digitales. **Bizagi**



Adicionalmente: Caso de éxito de emprendimiento Colombiano fundado en 2005.



>Herramienta Bizagi

Crear cuenta - Descargar Bizagi Modeler



Crea una cuenta

Descubra la plataforma que conecta a las personas, aplicaciones, dispositivos e información en su organización.

 Continuar con Microsoft

 Continuar con Google

Email *

p.ej. useremail@domain.com

Contraseña *

- ⊗ 8 caracteres de longitud, máximo 32 caracteres.
- ⊗ 1 letra minúscula, 1 letra mayúscula.
- ⊗ Debe contener 1 caracter(es) especial(es).
- ⊗ Al menos 1 número(s).

Registrarse

¿Tiene una cuenta de Bizagi?

Iniciar sesión

Nuevo Modelo - Bizagi Modeler

Archivo Inicio Formato Vista Publicar Exportar / Importar Herramientas Ayuda Daniel Malaver ES

Pegar Recursos Validar Compartir Vista de simulación Diagrama

Portapapeles Modelar Diagrama

Formato

Buscar Seleccionar Eliminar Ortografía Biblioteca de procesos Ejecutar Workflow Plataforma Bizagi Cursos En Línea

Diagrama 1

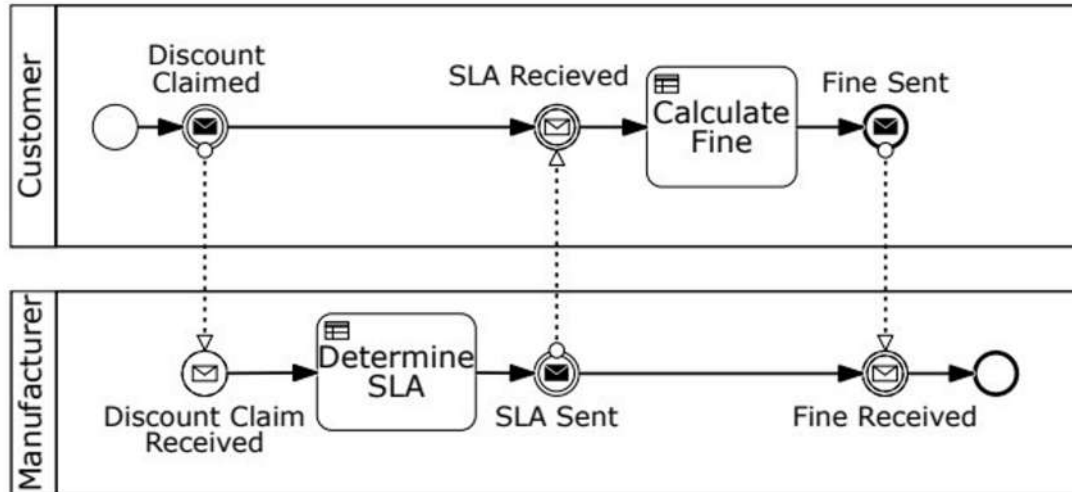
Proceso 1

100%



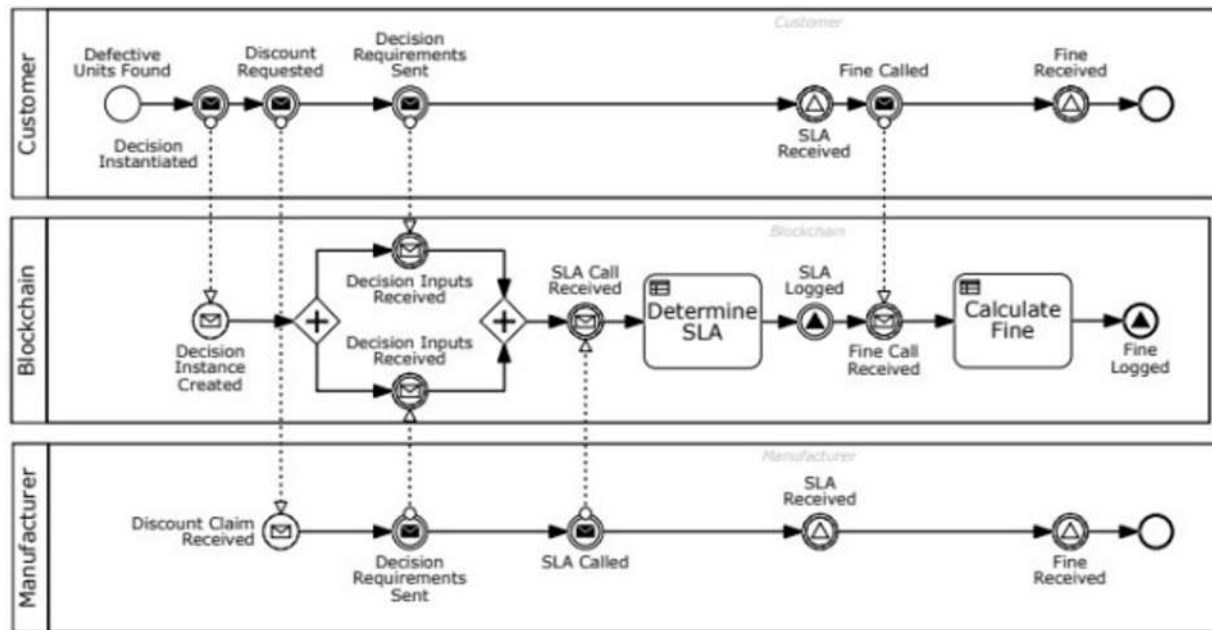
Caso de Ejemplo:

Se observa que un fabricante ofrece a sus clientes un reembolso por las unidades defectuosas entregadas. Una decisión establece la multa como una proporción del precio de compra definido por el SLA (Service Level Agreement) y una cantidad de unidades defectuosas proporcionadas por un cliente. El método tradicional para tomar estas decisiones se ve a continuación:





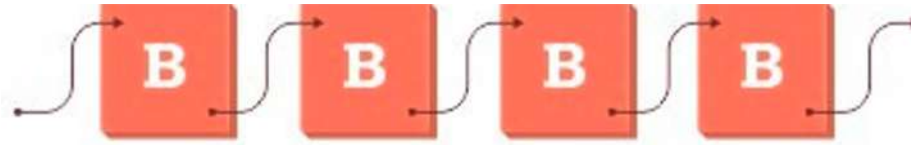
Revisión del proceso





Proceso con Blockchain

Utilización de Blockchain y contratos inteligentes para especificar la lógica de decisión ejecutable. Los participantes pueden contribuir con datos a una decisión a través de transacciones, y los contratos inteligentes ejecutan y registran decisiones.



Conclusión: Basándose en la tecnología blockchain, la confianza se vuelve obsoleta debido a un mecanismo técnico y confiable entre las partes.



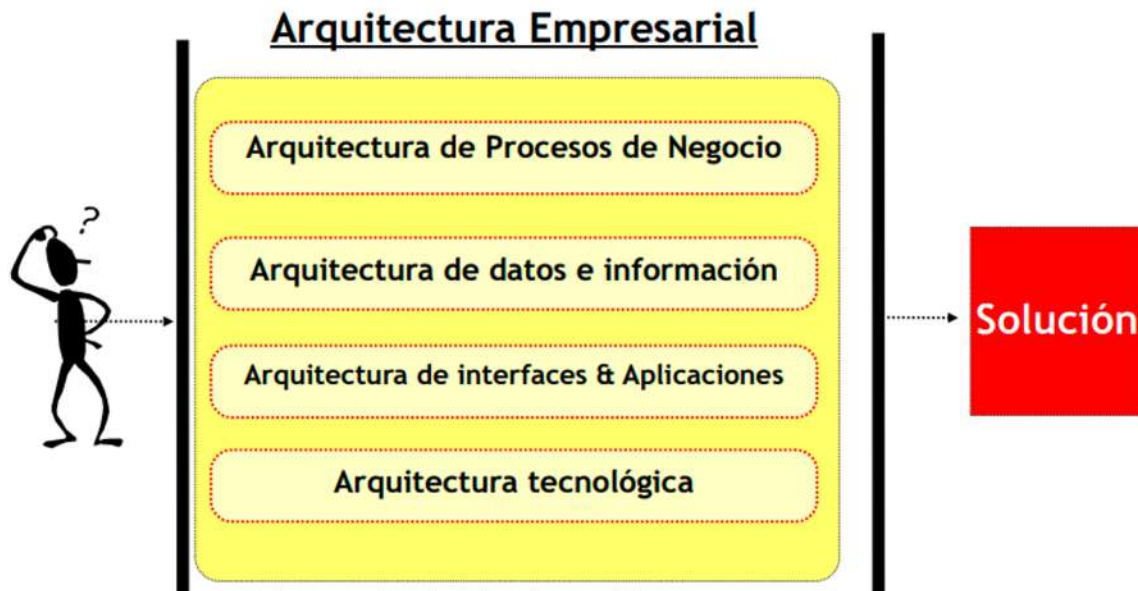
Arquitectura Empresarial

Una Arquitectura Empresarial es una metodología basada en una representación integral de las organizaciones, permite alinear procesos, datos, aplicaciones e infraestructura tecnológica con los objetivos estratégicos del negocio





Necesidad de un enfoque arquitectónico con visión empresarial





Entregas - Grupo

Con miras a facilitar el trabajo en clase y la asesoría con su asesor. Sin embargo, esto no implica la entrega oficial que se debe hacer a través de la plataforma.

Comentario

Tu respuesta

3. Vigilancia tecnológica plantilla

[📎 Añadir archivo](#)

4. Definición de la aplicación

[📎 Añadir archivo](#)

Enviar

Borrar formulario



El futuro digital
es de todos

MinTIC

Gracias

