



OPEN SOURCE BLOCKCHAIN

Desarrollo de Tecnologías Emergentes - TG2



9 DE ABRIL DE 2018

GRUPO T1

Contenido

1. Autores del trabajo, planificación y entrega.....	3
1.1 Autores.....	3
1.2 Planificación	3
1.3 Entrega	3
2. Descripción de las tecnologías	4
2.1 Descripción de la tecnología Multichain.....	4
2.2 Descripción de la tecnología Monax.....	4
3. Criterios de comparación	5
3.1 Categoría A: Generales.....	5
3.1.1 Criterio A.1: Precio.....	5
3.1.2 Criterio A.2: Tamaño.....	5
3.1.3 Criterio A.3: Sector al que va dirigido	5
3.1.4 Criterio A.4: Comodidad de desarrollo	5
3.1.5 Criterio A.5: Precio de cursos de formación	5
3.2 Categoría B: Hardware.....	5
3.2.1 Criterio B.1: Memoria RAM	5
3.2.2 Criterio B.2: Almacenamiento externo.....	5
3.3 Categoría C: Software de implementación	6
3.3.1 Criterio C.1: Sistemas Operativos	6
3.3.2 Criterio C.2: Lenguaje de programación.....	6
3.4 Categoría D: Software de la tecnología Blockchain	6
3.4.1 Criterio D.1: Almacenamiento de datos por transacción.....	6
3.4.2 Criterio D.2: Versiones.....	6
3.4.3 Criterio D.3: Mecanismo de consenso.....	6
3.4.4 Criterio D.4: Tipo de protocolo	6
3.4.5 Criterio D.5: Tipo de confirmación de transacciones	6
3.4.6 Criterio D.6: Madurez.....	6
3.5 Categoría E: Calidad y privacidad	7
3.5.1 Criterio E.1: Fiabilidad de la empresa	7
3.5.2 Criterio E.2: Privacidad	7
3.5.3 Criterio E.3: Tamaño comunidad y respaldo	7
3.6 Categoría F: Versatilidad.....	7
3.6.1 Criterio F.1: Lenguaje de programación	7
3.6.2 Criterio F.2: Usos	7
3.6.3 Criterio F.3: Carácter privado o público.....	7
3.7 Categoría G: Soporte y mantenimiento	7

3.7.1 Criterio G.1: Mantenimiento	7
3.7.2 Criterio G.2: Soporte/Formación	8
4. Evaluación de los criterios por tecnología	9
4.1 Evaluación de los criterios para la tecnología Multichain	9
4.2 Evaluación de los criterios para la tecnología Monax	10
5. Comparación de las tecnologías	11
6. Recomendaciones	15
6.1 Nómina.....	15
6.1.1 Descripción de la situación	15
6.1.2 Recomendación de tecnología a utilizar	15
6.2 Sistema de votación	16
6.2.1 Descripción de la situación	16
6.2.2 Recomendación de tecnología a utilizar	17
7. Conclusión	18

1. Autores del trabajo, planificación y entrega

1.1 Autores

Este grupo es el T1 y está formado por:

- Alejandro Díaz Moreno (Coordinación del grupo T1)
- Daniel Ortega Expósito
- Daniela Guzmán Pisfil
- María Castro Vaquerizo
- Paula Hernández Jordá

1.2 Planificación

Como la herramienta GanttPro ya no permite compartir mediante URL la planificación hemos tenido que añadir al profesor de la asignatura a la misma.

URL → <https://app.ganttpro.com/#!/app/home>

1.3 Entrega

Indicamos el enlace (URL) a un repositorio en GitHub:

https://github.com/alex7dm/DTE_T1_OpenSourceBlockchain

En dicho repositorio encontraremos:

- El trabajo terminado con el nombre **TG2_final.pdf**
- La presentación del trabajo con el nombre **TG2_final.pptx**

.

2. Descripción de las tecnologías

2.1 Descripción de la tecnología Multichain

Es un software de acceso gratuito que permite la creación y puesta en marcha de aplicaciones Blockchain con el objetivo de ayudar a las organizaciones a construir y desplegar dichas aplicaciones con velocidad.

Algunas de las características más importantes de esta tecnología:

- **Rápido despliegue:** permite crear una nueva cadena de bloques en dos simples pasos y conectarlos a la cadena existente en tres y esto nos permite implementar BlockChains ilimitados por servidor para aplicaciones de cadena cruzada.
- **Activos ilimitados:** permite emitir millones de activos en una cadena de bloques, todos rastreados y verificados a nivel de red. Además, se pueden realizar transacciones de intercambio atómico seguro de múltiples activos y multipartes.
- **Flujos de datos:** permite crear múltiples bases de datos de valores clave, series de tiempo o identidades en una cadena de bloques. Es ideal para el intercambio de datos, la marca de tiempo y el archivo encriptado.
- **Permisos detallados:** opcionalmente se puede controlar quien puede conectar, enviar y recibir transacciones, crear archivos, secuencias y bloques. Cada Blockchain será tan abierto o cerrado como se necesite.

Esta herramienta fue diseñada para permitir a los desarrolladores crear Blockchain y aplicaciones causando la mínima molestia y, además, provee de un total control sobre la personalización total de cada aspecto de la cadena de bloques y de la aplicación Blockchain.

Es importante destacar la seguridad flexible que ofrece, admitiendo nombres múltiples, claves primarias externas, nodos fríos y administración con consenso.

2.2 Descripción de la tecnología Monax

Monax es una plataforma abierta dirigida a desarrolladores y devops para que construyan, envíen y ejecuten aplicaciones basadas en Blockchain para ecosistemas empresariales.

Es una plataforma completa ya que permite realizar aplicaciones de nivel empresarial, es madura, gratuita y de código abierto utilizando componentes modulares.

Dicha plataforma está diseñada para el soporte de múltiples nodos conectados a múltiples redes de Blockchain, cada una de ellas con diferentes intérpretes.

La plataforma también permite la construcción de redes BlockChains de múltiples usos tanto corporativo como público. Además de lo citado dota la posibilidad de ejecución de contratos inteligentes, creación y configuración de tokens.

3. Criterios de comparación

3.1 Categoría A: Generales

3.1.1 Criterio A.1: Precio

Descripción: Coste monetario de la adquisición de la tecnología.

Tipo de valor: Numérico (€)

3.1.2 Criterio A.2: Tamaño

Descripción: Tamaño de la tecnología.

Tipo de valor: Numérico (MB)

3.1.3 Criterio A.3: Sector al que va dirigido

Descripción: Sector y mercado al que va dirigido el producto o servicio.

Tipo de valor: Texto libre

3.1.4 Criterio A.4: Comodidad de desarrollo

Descripción: Facilidad en la implementación. En la valoración, 1 es una tecnología difícil de implementar, lo que conlleva el cumplimiento de ciertos requisitos de gran dificultad. El 5 representa una tecnología que facilita en la medida de lo posible su implementación. Los recursos y requisitos en el nivel 5 serían más que asequibles.

Tipo de valor: Escala (1-5)

3.1.5 Criterio A.5: Precio de cursos de formación

Descripción: Coste monetario de la adquisición de la formación necesaria para implementar de manera óptima la tecnología.

Tipo de valor: Numérico (€).

3.2 Categoría B: Hardware

3.2.1 Criterio B.1: Memoria RAM

Descripción: Cantidad de memoria necesaria para implementar la solución.

Tipo de valor: Numérico (MB)

3.2.2 Criterio B.2: Almacenamiento externo

Descripción: Espacio mínimo necesario en el ordenador para poder implementar la tecnología.

Tipo de valor: Numérico (MB)

3.3 Categoría C: Software de implementación

3.3.1 Criterio C.1: Sistemas Operativos

Descripción: Sistemas operativos que se pueden utilizar para implementar la plataforma.

Tipo de valor: Texto libre (Enumeración de sistema operativos)

3.3.2 Criterio C.2: Lenguaje de programación

Descripción: Necesidad de programación para implementar la plataforma.

Tipo de valor: Booleano (Si/No)

3.4 Categoría D: Software de la tecnología Blockchain

3.4.1 Criterio D.1: Almacenamiento de datos por transacción

Descripción: Cantidad de datos que se pueden almacenar por cada una de las transacciones.

Tipo de valor: Numérico (MB)

3.4.2 Criterio D.2: Versiones

Descripción: Versiones existentes del producto.

Tipo de valor: Numérico

3.4.3 Criterio D.3: Mecanismo de consenso

Descripción: Mecanismo que utiliza la propia tecnología para crear un consenso entre los mineros en caso de que dos de los bloques apunten al mismo bloque precedente.

Tipo de valor: Texto libre

3.4.4 Criterio D.4: Tipo de protocolo

Descripción: Tipo de protocolo utilizado por la tecnología en la validación.

Tipo de valor: Texto libre

3.4.5 Criterio D.5: Tipo de confirmación de transacciones

Descripción: Tiempo que tarda la tecnología en confirmar cada una de las transacciones.

Tipo de valor: Numérico

3.4.6 Criterio D.6: Madurez

Descripción: Existencia de una mayor realización de cambios corrigiendo los fallos.

Tipo de valor: Escala (1-5)

3.5 Categoría E: Calidad y privacidad

3.5.1 Criterio E.1: Fiabilidad de la empresa

Descripción: Confianza en las empresas desarrolladoras de estas tecnologías, por ejemplo, si tiene buenas referencias en internet o buenas referencias de otras empresas o personas que las haya utilizado.

Tipo de valor: Booleano (Si/No)

3.5.2 Criterio E.2: Privacidad

Descripción: Si se permite la visibilidad de transacciones a todo el público o no.

Tipo de valor: Booleano (Si/No)

3.5.3 Criterio E.3: Tamaño comunidad y respaldo

Descripción: Se tiene en cuenta el valor de la empresa y el volumen de esta que utiliza la tecnología en cuestión. En la valoración, 1 representa cero volumen y empresas con nulo poder empresarial. El 5 representa un volumen de empresas muy alto con gran valor en su correspondiente sector.

Tipo de valor: Escala (1-5)

3.6 Categoría F: Versatilidad

3.6.1 Criterio F.1: Lenguaje de programación

Descripción: Compatibilidad con varios lenguajes de programación.

Tipo de valor: Booleano (Si/No)

3.6.2 Criterio F.2: Usos

Descripción: Cantidad de aplicaciones que se podrían desarrollar con la tecnología. En la valoración, 1 hace referencia a un único uso y 5 a un amplio rango de usos.

Tipo de valor: Escala (1-5)

3.6.3 Criterio F.3: Carácter privado o público

Descripción: Posibilidad de colaboración con otras redes Blockchain.

Tipo de valor: Texto libre

3.7 Categoría G: Soporte y mantenimiento

3.7.1 Criterio G.1: Mantenimiento

Descripción: Si la empresa desarrolladora ofrece mantenimiento adicional al adquirir la tecnología.

Tipo de valor: Booleano (Si/No)

3.7.2 Criterio G.2: Soporte/Formación

Descripción: Si la empresa desarrolladora ofrece soporte o cursos de formación adicionales para el uso de la tecnología al adquirirla.

Tipo de valor: Booleano (Si/No)

4. Evaluación de los criterios por tecnología

4.1 Evaluación de los criterios para la tecnología Multichain

CRITERIO	RESULTADO
A.1: Precio por tecnología	0€
A.2: Tamaño de descarga del software	40,5 MB
A.3: Sector al que va dirigido	Empresarial y público
A.4: Comodidad de desarrollo	3, personas con cierta formación en esta tecnología consideran que es una plataforma simple, potente y bien documentada. También es verdad que, para personas con bajos conocimientos en este ámbito, puede resultar complicado de implementar.
A.5: Precio de cursos de formación	717€ de media
B.1: Memoria RAM	512 MB
B.2: Almacenamiento externo	1024 MB
C.1: Sistemas Operativos	Windows, Linux y Mac (todos de 64 bits)
C.2: Lenguaje de programación	NO
D.1: Almacenamiento de datos por transacción	64 MB
D.2: Versiones	37 versiones
D.3: Mecanismo de consenso	Propio
D.4: Tipo de protocolo	Proof of work o proof of stake (preferiblemente el 2º)
D.5: Tiempo de confirmación de transacciones	2 seg.
D.6: Madurez	3.
E.1: Fiabilidad de la empresa	SI. Cuenta con el apoyo de grandes empresas
E.2: Privacidad	SI. MultiChain si implementa privacidad en la red, todos pueden ver todas las transacciones de los demás.
E.3: Tamaño y comunidad de respaldo	4, debido a que actualmente grandes empresas tecnológicas (Indra, Accenture, BCG, WOLFRAM y PWC) lo utilizan. En el último año el número de descargas asciende a 50000
F.1: Lenguaje de programación	SI (C#, Java, Javascript, Python, Python 3, Ruby y PHP)
F.2: Usos	4. 4 casos de uso: Lightweight financial systems, provenance tracking, interorganizational record keeping, multiparty aggregation.
F.3: Carácter privado o público	Privado
G.1: Mantenimiento	SI
G.2: Soporte/Formación	Si (gratis y de pago)

4.2 Evaluación de los criterios para la tecnología Monax

CRITERIO	RESULTADO
A.1: Precio por tecnología	0€
A.2: Tamaño de descarga del software	17,8 MB
A.3: Sector al que va dirigido	Empresarial
A.4: Comodidad de desarrollo	3, personas con cierta formación en esta tecnología consideran que es una plataforma simple, potente y bien documentada. También es verdad que, para personas con bajos conocimientos en este ámbito, puede resultar complicado de implementar.
A.5: Precio de cursos de formación	12.059€ de media
B.1: Memoria RAM	No aplica
B.2: Almacenamiento externo	No aplica
C.1: Sistemas Operativos	Windows, Linux y Mac
C.2: Lenguaje de programación	SI (Smart Contracts)
D.1: Almacenamiento de datos por transacción	64 MB
D.2: Versiones	18 versiones RC.
D.3: Mecanismo de consenso	Tendermint
D.4: Tipo de protocolo	Proof of stake
D.5: Tiempo de confirmación de transacciones	~ 0 (Instantáneo).
D.6: Madurez	4.
E.1: Fiabilidad de la empresa	SI. Cuenta con el apoyo de grandes empresas
E.2: Privacidad	NO. Monax no implementa privacidad en la red, todos pueden ver todas las transacciones de los demás.
E.3: Tamaño y comunidad de respaldo	4, debido a que actualmente grandes empresas tecnológicas (Indra, Accenture, Delloitte, Swift, Microsoft, Amazon y PWC) lo utilizan.
F.1: Lenguaje de programación	SI (C/C++ y Java)
F.2: Usos	5. 8 usos englobados en 3 categorías: financiero, seguros y logística.
F.3: Carácter privado o público	Publico
G.1: Mantenimiento	Si (de pago)
G.2: Soporte/Formación	Si (solo de pago)

5. Comparación de las tecnologías

CRITERIOS	MultiChain	Monax	COMENTARIOS
Generales			
A.1: Precio por tecnología	0€	0€	Ambos son gratuitos por lo que nos es indiferente su elección.
A.2: Tamaño de descarga del software	40,5 MB	17,8 MB	Preferimos Monax ya que el software ocupa menos.
A.3: Sector al que va dirigido	Empresarial y público	Empresarial	Preferimos MultiChain ya que tiene más versatilidad a la hora de enfocar su producto.
A.4: Comodidad de desarrollo	3, personas con cierta formación en esta tecnología consideran que es una plataforma simple, potente y bien documentada. También es verdad que, para personas con bajos conocimientos en este ámbito, puede resultar complicado de implementar.	3, personas con cierta formación en esta tecnología consideran que es una plataforma simple, potente y bien documentada. También es verdad que, para personas con bajos conocimientos en este ámbito, puede resultar complicado de implementar.	Creemos que ambas plataformas tienen el mismo nivel de complejidad a la hora de implementarlas.
A.5: Precio de cursos de formación	717€ de media	12.059€ de media	MultiChain es más barato. También nos proporcionan descuentos en una serie de cursos de formación. Además, hay más cursos gratuitos que en Monax.
Hardware			
B.1: Memoria RAM	512 MB	No aplica	Al no saber qué requisitos necesitamos con Monax, preferimos MultiChain.
B.2: Almacenamiento externo	1024 MB	No aplica	Al no saber qué requisitos necesitamos con Monax, preferimos MultiChain.
Software de implementación			
C.1: Sistemas Operativos	Windows, Linux y Mac (todos de 64 bits)	Windows, Linux y Mac	Aunque ambos permiten su implementación en los mismos SSOO, MultiChain tiene la restricción de que solo es apto para ordenadores de 64 bits.

C.2: Lenguaje de programación	NO	SI (Smart Contracts)	Preferimos MultiChain ya que nos proporciona Smart Contracts ya programados. Monax solo es necesario un lenguaje de programación en los Smart contracts.
Software de la tecnología BlockChain			
D.1: Almacenamiento de datos por transacción	64 MB	64 MB	Ambos transacciones tienen la misma capacidad.
D.2: Versiones	37 versiones	18 versiones RC.	MultiChain ha lanzado un mayor número de versiones.
D.3: Mecanismo de consenso	Propio	Tendermint	Conocemos más el mecanismo de consenso Tendermint que el propio de MultiChain.
D.4: Tipo de protocolo	Proof of work o proof of stake (preferiblemente el 2º)	Proof of stake	A priori, nos es indiferente un protocolo u otro.
D.5: Tiempo de confirmación de transacciones	2 seg.	~ 0 (Instantáneo).	La confirmación de transacción es más rápida con Monax.
D.6: Madurez	3	4	Ambas plataformas han lanzado gran número de versiones, pero Monax ha lanzado 18 versiones RC mientras que MultiChain solo ha lanzado 5 versiones RC.
Calidad y privacidad			
E.1: Fiabilidad de la empresa	SI. Cuenta con el apoyo de grandes empresas	SI. Cuenta con el apoyo de grandes empresas	Ambas empresas son conocidas en el sector y tienen gran popularidad por la funcionalidad y fiabilidad de sus productos.
E.2: Privacidad	SI. MultiChain si implementa privacidad en la red, no todos pueden ver todas las transacciones de los demás.	NO. Monax no implementa privacidad en la red, todos pueden ver todas las transacciones de los demás.	MultiChain ya que podemos elegir si queremos que los demás vean las transacciones o no.
E.3: Tamaño y de comunidad respaldo	4, debido a que actualmente grandes empresas tecnológicas (Indra, Accenture, BCG, WOLFRAM y PWC) lo	4, debido a que actualmente grandes empresas tecnológicas (Indra, Accenture, Delloitte, Swift, Microsoft, Amazon y PWC) lo utilizan.	Ambas plataformas cuentan con el apoyo de grandes empresas.

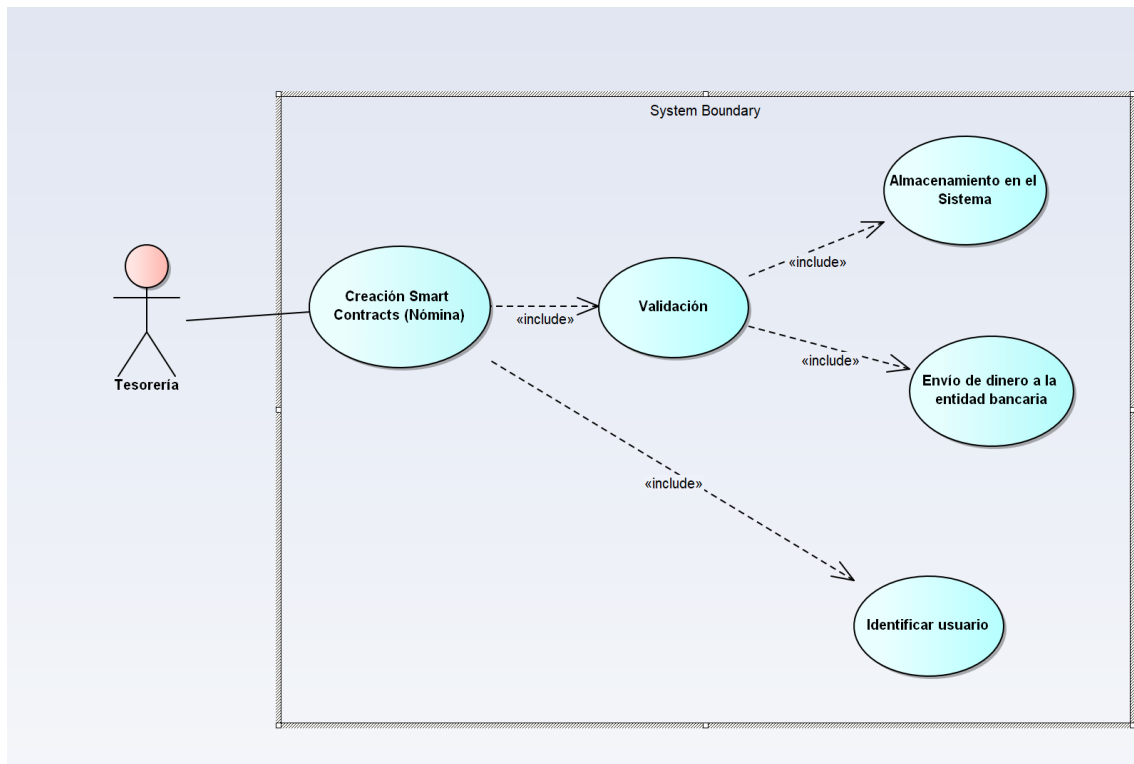
	utilizan. En el último año el número de descargas asciende a X		
Versatilidad			
F.1: Lenguaje de programación	SI (C#, Java, Javascript, Python, Python 3, Ruby y PHP)	SI (C/C++ y Java)	Ambas plataformas son versátiles en este aspecto, pero preferimos MultiChain ya que es compatible con más lenguajes de programación (la gran mayoría)
F.2: Usos	4. 4 casos de uso: Lightweight financial systems, provenance tracking, interorganizational record keeping, multiparty aggregation.	5. 8 usos englobados en 3 categorías: financiero, seguros y logística.	Monax ya que puede se puede implementar en más soluciones.
F.3: Carácter privado o público	Privado	Publico	Preferimos una blockchain colaborativa, por lo tanto, Monax.
Soporte y mantenimiento			
G.1: Mantenimiento	SI	Si (de pago)	El mantenimiento que ofrece MultiChain es gratuito
G.2: Soporte/Formación	Si (gratis y de pago)	Si (solo de pago)	El soporte y formación que ofrece MultiChain es gratuito o de pago, sin embargo, Monax solo lo ofrece de pago.

6. Recomendaciones

6.1 Nómina

6.1.1 Descripción de la situación

La situación ideada ha sido la creación de una nómina con un contrato inteligente (smart contract). Se ingresará el día 1 de cada mes la nómina en la cuenta del cliente sin intermediarios. El contrato deberá detectar variaciones en el pago como dietas, horas extra o incluso sanciones económicas. La idea es que la empresa que posee el Blockchain pueda prescindir de tener un banco.



6.1.2 Recomendación de tecnología a utilizar

Criterios relevantes para la decisión	Multichain	Monax
A.1: Precio por tecnología	X	X
A.2: Tamaño de descarga del software	X	X
A.3: Sector al que va dirigido	X	
A.4: Comodidad de desarrollo	X	
A.5: Precio de cursos de formación	X	X
B.1: Memoria RAM	X	X
B.2: Almacenamiento externo	X	X
C.1: Sistemas Operativos	X	X

C.2: Lenguaje de programación	X	
D.1: Almacenamiento de datos por transacción	X	X
D.2: Versiones	X	X
D.3: Mecanismo de consenso		X
D.4: Tipo de protocolo	X	
D.5: Tiempo de confirmación de transacciones		X
D.6: Madurez	X	X
E.1: Fiabilidad de la empresa	X	X
E.2: Privacidad	X	
E.3: Tamaño y comunidad de respaldo	X	X
F.1: Lenguaje de programación	X	
F.2: Usos	X	
F.3: Carácter privado o público	X	X
G.1: Mantenimiento	X	
G.2: Soporte/Formación	X	

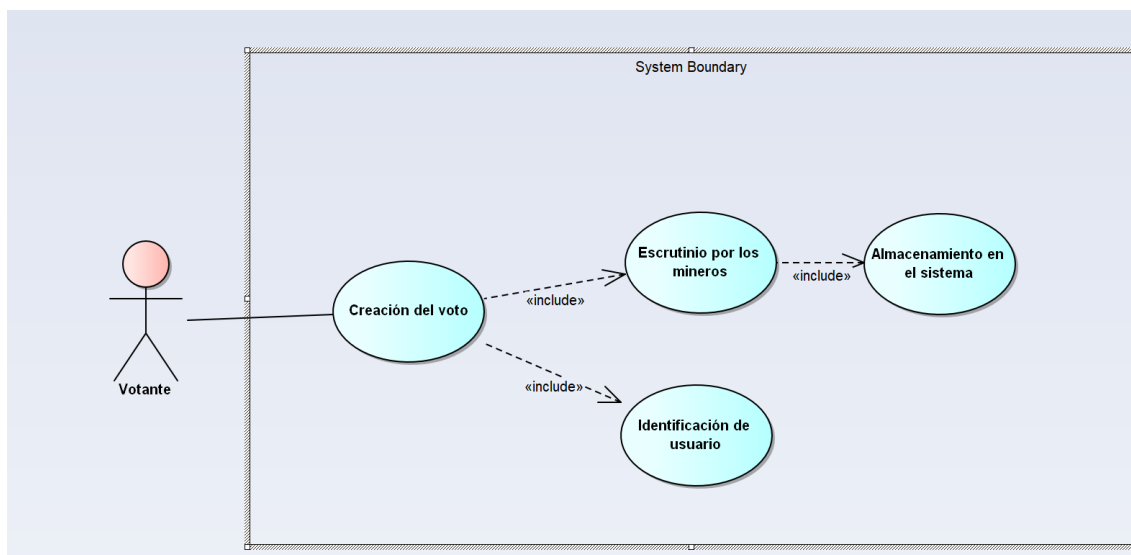
Como podemos ver en la anterior tabla hay varios criterios en común. La diferencia básica entre una tecnología u otra es el hecho de que usando Multichain obtendremos smart contracts descargables que pueden ser rellenos, por lo tanto, no costaría tanto como en Monax en el que habría que programar tu propio contrato y luego rellenarlo. Otro punto importante es que en los Smart contracts hay datos personales que no quieres que nadie sepa, entonces en cuanto a privacidad Multichain también es mejor.

Estos junto con el mantenimiento gratuito es lo que hace que Multichain sea mejor para la creación de Smart contracts.

6.2 Sistema de votación

6.2.1 Descripción de la situación

La situación ideada ha sido la creación de un sistema de votación que proporcione un nivel óptimo de privacidad y funcionalidad a través del Blockchain. Según vayan llegando transacciones (votos) se irá realizando el escrutinio por los “mineros”. Tras la validación de la transacción, esta se unirá a la cadena de bloques. La idea es prescindir de colegios electorales y mejorar la privacidad y seguridad del sistema de votación.



6.2.2 Recomendación de tecnología a utilizar

Criterios relevantes para la decisión	Multichain	Monax
A.1: Precio por tecnología	X	X
A.2: Tamaño de descarga del software	X	X
A.3: Sector al que va dirigido	X	
A.4: Comodidad de desarrollo	X	X
A.5: Precio de cursos de formación	X	X
B.1: Memoria RAM	X	X
B.2: Almacenamiento externo	X	X
C.1: Sistemas Operativos	X	X
C.2: Lenguaje de programación	X	X
D.1: Almacenamiento de datos por transacción	X	X
D.2: Versiones	X	X
D.3: Mecanismo de consenso		X
D.4: Tipo de protocolo		X
D.5: Tiempo de confirmación de transacciones		X
D.6: Madurez	X	X
E.1: Fiabilidad de la empresa	X	X
E.2: Privacidad	X	
E.3: Tamaño y comunidad de respaldo	X	X
F.1: Lenguaje de programación	X	

F.2: Usos		X
F.3: Carácter privado o público		X
G.1: Mantenimiento	X	
G.2: Soporte/Formación		X

En la tabla de arriba podemos ver que en cuanto a criterios están ambas tecnologías muy parejas. Multichain es buena por la privacidad y que está más ligada al sector público, pero Monax tiene una cartera de usos mejor para llevar a cabo este proyecto. También Monax debido a su mecanismo de consenso es mejor para contabilizar los votos, y pasa lo mismo con su protocolo de confirmación, a parte que tiene una capacidad de combinarse con otras blockchain públicas lo que puede facilitar mucho el proceso de escrutinio.

Debido a lo dicho anteriormente creemos que es más conveniente usar Monax para realizar este proyecto.

7. Conclusión

Tras un análisis exhaustivo hemos llegado a la conclusión que ambas plataformas son eficaces para la realización de diferentes aplicaciones blockchain, son asequibles ya que ambas son gratuitas y además cada una tiene sus puntos más fuertes y sus puntos más débiles, lo cual no significa que una sea mejor que otra a la hora de hacer algo con ellas. Y si se está buscando aprender sobre la tecnología blockchain, cada una enseña algo diferente.

Mientras que Multichain destaca por su rápida puesta en marcha y por el control total del acceso de quien puede conectarse, enviar y recibir transacciones; Monax destaca por contar con un mayor número de posibilidades para implementar soluciones, además de destacar por el tiempo de confirmación de transacción.

En definitiva, es simplemente una cuestión de averiguar lo que se quiere hacer. Ambas plataformas destacan de formas diferentes.