X.Blockchain

Yongseok Kwon

2017-05-23 Rev 1.

Abstracto

El advenimiento de Bitcoin y la proliferación de trasnacciones que lo usan han demostrado que la tecnología de la cadena de bloques es suficientemente segura como para ser confiable como el director comercial.
La razón principal por la cual la tecnología de la cadena de bloque ha sido notada es que la tercera parte confiada(Trusted Third Party, TTP) ha sido eliminada en términos de seguridad a diferencia del método existente, y que todos los detalles de la transacción se transmiten a todos los participantes en la red, por lo cual la manipulación de los contenidos de la transacción se hace prácticamente imposible.
Los conceptos principales de la tecnología de la cadena de bloque son los conceptos de ‘descentralización’ y ‘libro mayor distribuido’. En el método convencional, todas las transacciones se registran en un servidor central centralizado, y este servidor central(la tercera institución de confianza) ‘garantiza’ la confianza de las transacciones. Sin embargo, las transacciones que se producen en la cadena de bloques se transmiten a todos los participantes en la red para ser ‘verificado’ y ‘acordado’, y se agrupan en unidades de ‘bloque’ para ser conectado de forma secuencial(lineal).

El tamaño de la cadena de bloque en el que se registran todas las transacciones se aumenta a medida que se aumenta el número de transacciones acumuladas, es decir, se aumenta con el tiempo. Esto significa que un día se llegará el momento que se hace prácticamente imposible que todos los participantes en la red almacenen y gestionen toda la cadena de bloques. En otras palabras, un sistema(nodo) capaz de almacenar y gestionar toda la cadena de bloques es probable que se convierte en un número relativamente pequeño de nodos debido a la cantidad reducida de nodos. Y ésto dará lugar a otra forma de centralización. En una situación en la que un número relativamente pqueño de grupos de nodos gestiona toda la cadena de bloques, la fiabilidad de la transacción se ve obligada a depender de este pequeño número de grupos de nodos. Es decir, la ‘descentralización’, que es el concepto fundamental de la cadena de bloques, puede verse seriamente dañada.

En este document, proponemos X. Blockchain que transforma la estructura de conexión de la cadena de bloques de la estructura lineal existente a ka estructura multidimensional en la aplicación de tecnología de cadena de bloques para la protección de documentos electrónicos, y queremos encontrar una solución para el problema del tamaño de toda la cadena de bloques y para el problema de descentralización de nodos.

Problemas

El tamaño de la cadena de bloques se aumenta constantemente en proporción al número acumulado de transacciones a lo largo del tiempo. Si queremos ser fieles al concepto básico de la cadena de bloques que el libro mayor se distribuye y aduministra a todos los nodos que participan en la red de la cadena de bloques y que es posible asegurar la confianza con la transacción sin la tercera institución fiduciaria, el problema de tamaño de la cadena de bloque que se aumenta constantemente genera una situación límite en la participación del nodo. En otras palabras, para participar como un nodo completo que almacena y administra una enorme cadena de bloques, se requiere un rendimiento igual o superior a un cierto nivel, como asegurar el espacio de almacenamiento. Este nivel de rendimiento se incrementará en proporción al tamaño de la cadena de bloques, por lo que la reducción numérica de los nodos participantes se vuelve inevitables, y se volverá a realizar otro tipo de 'centralización'. A partir de mayo de 2017, el tamaño total de la cadena de bloques, incluidos los datos de transacción de Bitcoin, ya ha excedido 115G[1], y la cadena de bloques Ethereum también ha superado recientemente 20g.

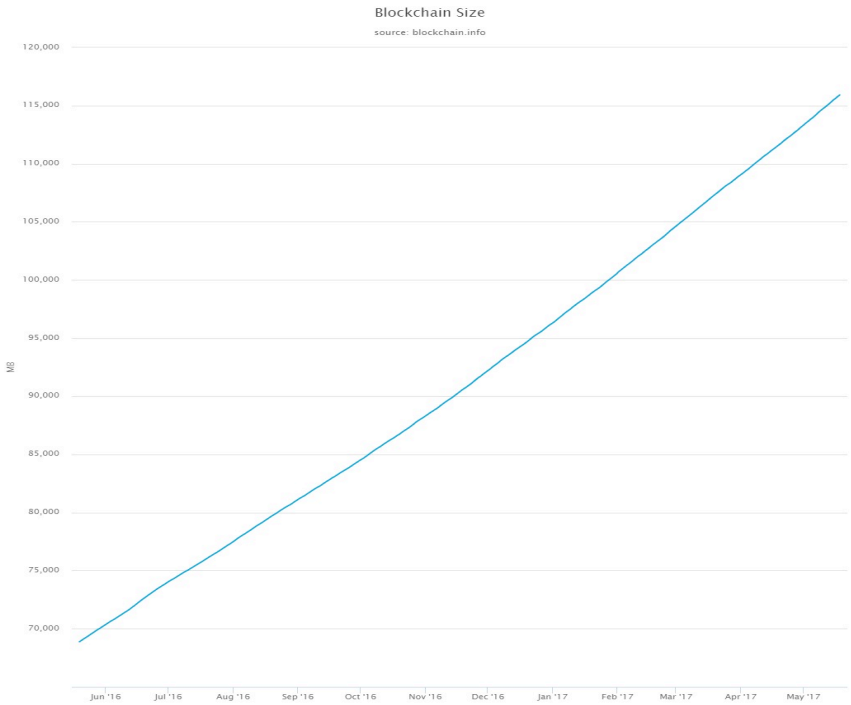

Figura 1. Tamaño total de la cadena de bloques de Bitcoin

Además, la cantidad de nodos completos que existen actualmente en todo el mundo con base en Bitcoin es aproximadamente 5,000 ~ 7,000.

---

[1] El tamaño total de la cadena de bloque, que incluye todos los datos de transacción y la información del encabezado de bloque que describen la transacción

[2.] Bitcoin está proponiendo SPV como una solución a este problema. Ésto es un método para minimizar los recursos requeridos al realizar la verificación de transacciones utilizando solo la información del encabezado del bloque, excluyendo los datos de transacción, lo cual es esencial en una aplicación de cadena de bloque para los documentos electrónicos. Si la transacción consiste en una transacción en la criptomoneda, los datos del documento electrónico se convierten en la parte principal de la transacción en la aplicación del documento electrónico. En este momento, el tamaño del documento es tan grande que no se puede comparar con el historial de transacciones de la criptomoneda, por lo que la cadena de bloque no incluye los datos del documento en sí.
A menos que se especifique lo contrario en este documento, el 'tamaño de cadena de bloque' significa el 'tamaño de encabezado de cadena de bloque'.

[3] El tamaño total de la cadena de bloque, que incluye todos los datos de transacción y la información del encabezado de bloque que describe la transacción.

Por otro lado, una gran cantidad de clients de usuario(incluidos los dispositivos móviles) que no alcanzan cierto nivel están restringidos de participación como los nodos completos. Como resultado, es necesario que el cliente usuario la 'solicite' a este número de grupo relativamente pequeño sin juzgar la confianza de la transacción misma(sin la tercera institución fiduciaria), y que 'acepte' unilateralmente su resultado. Aquí, un pequeño grupo de nodos completos actúa como una ´tercera institución fiduciaria'.

Este problema de 'centralización de nodos completos' es causado por la alta potencia de cómputo requerida para almacenar todas las cadenas de bloques agrandecidas y construir(excavar) los bloques como se mencionó anteriormente.
Aquí, la razón por la cual se requiere almacenar toda la cadena de bloques nuevamente es que dado que la estructura de la cadena de bloques está compuesta por una estructura de conexión lineal, no tiene sentido separar solo los bloques necesarios. Un conjunto de bloques intermedios interrumpidos no puede confirmar ninguna confianza y no tiene ningún valor.

Este problema es inevitable en la 'transacción' como la moneda de cifrado. No es posible ninguna restricción o clasificación al registrar cuánto dinero se mueve de una cuenta a otra. No puede clasificar transacciones basadas en la 'cantidad' de la moneda o la 'cuenta' utilizada para mover la moneda. Como todas las transacciones tienen el mismo significado y todas las transacciones con el mismo significado no pueden clasificarse por ningún estándar, parece virtualmente imposible romper la estructura lineal al tratar con los registros de esta naturaleza.

Por otro lado, en el caso de 'documento electrónico', varios registros sobre el documento se centran en el 'documento' correspondiente, a diferencia de los de la moneda cifrada. Todos los registros, incluida la creación, modificación, transmisión, visualización y descarte de documentos, están cubiertos por el 'documento' correspondiente.
Esto significa que el documento mismo y sus registros asociados se pueden categorizer sobre la base del 'documento', lo que significa que las cadenas en una cadena de bloques se pueden clasificar en múltiples cadenas en lugar de una estructura lineal.

N-Cadena de Bloque Dimensional – X.Blockchain

X.Blockchain clasifica todos los registros de un documento(transacción) en un 'documento' o una 'referencia' que no se vincula con una estructura lineal, reflejando las características del documento electrónico anteriormente mencionado. Y proponemos una cadena de bloques multiimensional mediante la construcción de cadenas múltiples de acuerdo con este criterio.
Por ejemplo, cuando se utilize el 'documento' como referencia, la 'creación inicial' de cada documento se registra en una cadena de bloques(cadena principal)que tiene la misma estructura lineal que la cadena de bloque existente. Sin embargo, los registros adicionales(transacción) como los cambiados realizados en un documento específico ya registrado en la cadena principal se registran en una subcadena, que es otra cadena de bloque que hace que el bloque correspondiente en la cadena principal no la cadena principal sea un bloque de genesis.

[4]. El primer bloque de la cadena de bloque

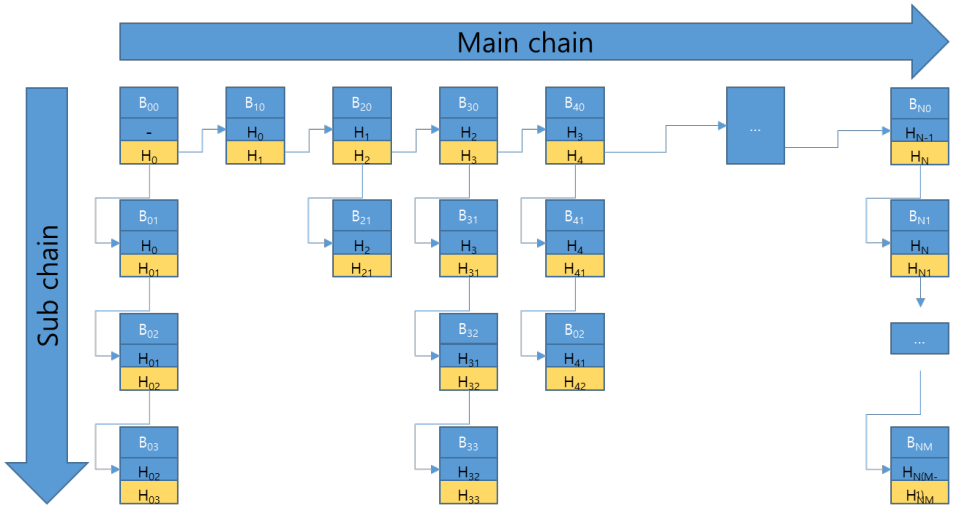

Figura 2. X.Blockchain

La figura anterior muestra el X.Blockchain con una estructura bidimensional. Cuando el 'documento' anteriormente mencionado se toma sobre la base de la cadena principal, cada bloque (B_{00} ~ B_{n0}) que constituye la cadena principal incluye el registro de creación del Nuevo documento y, al mismo tiempo, puede ser el bloque de genesis de cada subcadena. Por ejemplo, si se genera una modificación inicial de un documento electrónico E_{20} cuya creación fue registrada en B_{20}, se registra en B_{21} en la subcadena con B_{20} como el bloque de genesis no B_{30}, el siguiente bloque en la cadena principal.

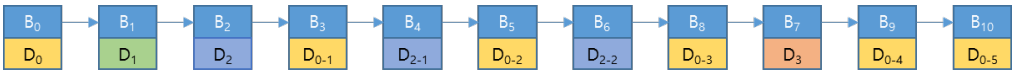

Figura 3. Cadena de Bloque Lineal

En la estructura de cadena de bloque lineal, incluso si el documento es el mismo documento, el registro adicional como la modificación del documento requiere los bloques adicionales de la cadena de bloques.
La figura anterior es un ejemplo de construcción lineal de una situación en la que los documentos D_0 ~ D_3 se agregan a la cadena de bloques. En este ejemplo, D_n significa la creación, y D_{n-m} significa un registro adicional tal como la modificación y transferencia, etc. que aparece en el documento D_n. Se generaron un total de 6 registros(~ D_{0-5}), incluida la generación del documento D_0 en caso del documento D_0 , y se generaron un total de 3 registros(~ D_{2-2}) en el caso del documento D_2.
En la cadena de bloque lineal anterior, todos los clients deben adquirir y almacenar todos los bloques para verificar la confianza de un documento específico. En otras palabras, incluso si el cliente solo necesita el documento D_2, se necesita un total de 11 bloques que incluyen los bloques D_0, D_1, D_3 prácticamente innecesarios y D_{0-1} ~ D_{0-5} que contienen los registros adicionales de D_0.

Sin embargo, si construimos la misma situación con X.Blockchain, se convierte en lo siguiente.

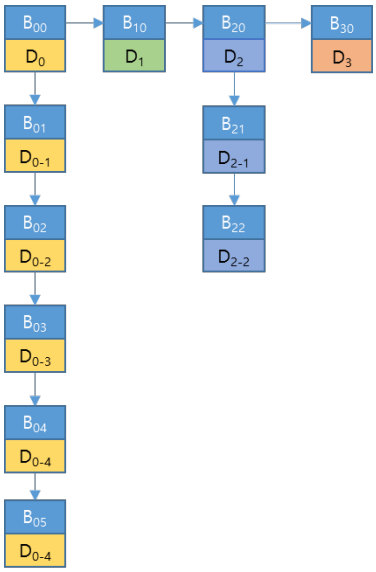

Figura 4. X.Blockchain

En la figura anterior, $B_{00} \sim B_{30}$ constituye la cadena principal, y cada subcadena está constituido que hace B_{00} y B_{20} como el bloque de genesis. En una cadena de bloque multidimensional de este tipo, no todos los clients necesitan tener todas las cadenas de bloque. Si solo se necesita el documento D_2 como en el ejemplo anterior, puede juzgar si el documento D_2 es confiable o no al mantener solo la subcadena que tiene D_2 como un bloque de genesis, y su cadena principal superior en lugar de toda la cadena de bloques. Es decir, es suficiente para mantener un total de 6 de información de bloques compuestas por los bloques $B_{00} \sim B_{30}$ de la cadena principal y los bloques $B_{21} \sim B_{22}$ de la subcadena.

Aquí, los 'criterios de clasificación' aplicados a la cadena principal no necesariamente tienen que ser el 'documento. Dependiendo de la configuración del servicio, la unidad 'departamento' se puede aplicar como el criterio, o un conjunto de documentos que tiene una asociación se puede aplicar como un criterio de clasificación.
Dependiendo de la situación, la subcadena se puede configurar para ser la cadena principal de otra subcadena. En el caso del registro de tierras, si un amplio rango de 'area' se define como una referencia de cadena principal y unidades más pequeñas como la ciudad, gun y gu se clasifican en una subcadena primaria y una unidad de clasificación de tierra se clasifica en una subcadena secundaria, es posible construir una estructura tridimensional como se muestra en la figura siguiente, en lugar de la estructura bidimensional que se muestra en la figura anterior.

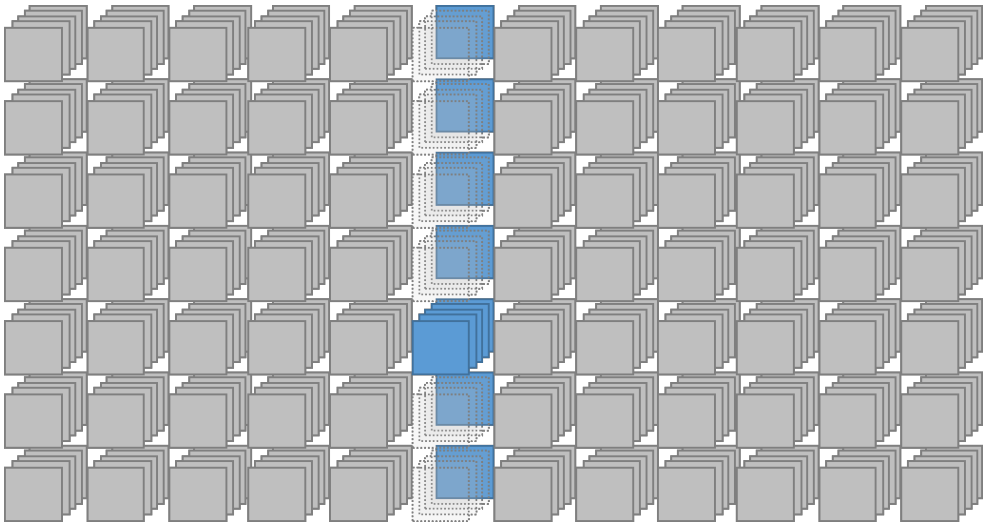

Figura 5. X.Blockchain de la estructura tridimensional

El nodo complete responsable de la nueva explotación de bloques en X.Blockchain todavia debe tener la información sobre todos los bloques. Sin embargo, el cliente(equipo de usuario) no necesita tener un bloque completo para decidir si confiar en el documento, no en la explotación. Cada usuario puede verificar la confianza del documento sin una 'tercera institución fiduciaria' al asegurar que la subcadena que contiene los documentos que necesitan ser verificados, y su cadena principal superior. Aquí, el nodo completo solo juega un papel de 'explotación' en lugar de la tercera institución fiduciaria que confirma la confianza.

Procesamiento de Transacciones en Paralelo

En una estructura de cadena de bloque lineal, todas las transacciones que se producen durante la creación de un bloque permanecerán en estado de espera hasta que se explota el siguiente bloque. [2]Además, en algunos casos, puede ser necesario esperar hasta que se explota no el siguiente bloque sino el otro bloque siguiente, ya que no permite que el tamaño de un bloque[2] crezca indefinidamente. El tiempo de espera hasta que la transacción que se distribuye a la red de la cadena de bloques se incliye en el bloque reduce el 'procesamiento de transacción por segundo(TPS[3])' y se retrasa el procesamiento de transacción en consecuencia.
En X.Blockchain, sin embargo, es posible realizar simultáneamente explotación de bloques para cada subcadena. Por ejemplo, una explotación de bloque B_{n0} en la cadena principal y la explotación de bloque B_{2m} en la subcadena pueden realizar simultáneamente. B_{n0} y B_{2m} pertenecen a una cadena de bloques separados entre sí, y no tienen una relación de conexión mutua.

[5] En Bitcoin, el tamaño del bloque está limitado a 1MB. La restricción de tamaño de bloque se hace para el número de transacciones que puede contener un bloque, lo que disminuye el número de transacciones por segundo(Transacción por segundo:TPS). Actualmente, se está discutiendo el problema de extender el tamaño de bloque de Bitcoin, y algunas implementaciones como Bitcoin Classic usan un tamaño de bloque de 2MB pero no son apoyados por los explotadores.
[6]. Actualmente, el TPS de Bitcoin es aproximadamente de 7 TPS.

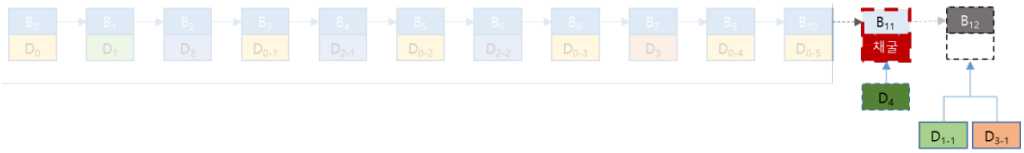

Figura 6. Procesamiento de Transacción - Cadena de Bloque Lineal

La figura anterior se basa en la suposición de que D_4 se creó recientemente en la situación de ejemplo anterior, y que se generaron posteriormente los registros de modificación sobre los documentos D_1 y D_3. En una cadena de bloque lineal, los registros de modificación de D_1 y D_3 permanecen en el estado de espera durante la explotación para la creación nueva de D_4 en curso. Después de que se completa la explotación del bloque de D_4, B_{11}, y cuando se inicia la explotación del siguiente bloque de B_{12}, las modificaciones de D_1 y D_3 에 se incluyen en el bloque de B_{12}, y cuando se completa la explotación y finalmente se conecta a la cadena de bloques, se completa el registro en la cadena de bloque.

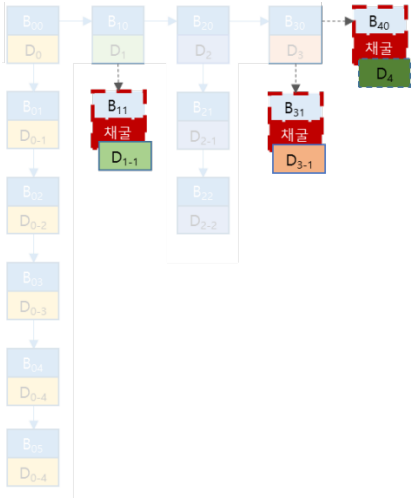

Figura 7. Transaction Processing – X.Blockchain

Sin embargo, en la cadena X.Blockchain de la estructura multidimensional, la explotación de los bloques B_{11} y B_{31} no necesita ser esperado sobre las modificaciones de los documentos D_1 y D_3 hasta que se complete la explotación del bloque B_{40} de creación del documento D_4, como se muestra en la figura anterior. En el ejemplo presentado, la explotación para todos los bloques nuevos B_{40}, B_{11}, B_{31} se puede llevar a cabo de forma independiente y simultánea.

Efectividad

Este documento explica cómo la aplicación de X.Blockchain difiere de la aplicación de las cadenas de bloques existentes, asumiendo una situación en la que el resumen de registro cívil se documenta electrónicamente y se gestiona mediante la aplicación de la tecnología de cadena de bloques.
Se supone que hay un resumen por 1 población constituyente y que constituye nuevamente 1 bloque, y que la renovación del registro cívil ocurre tanto como la población de migración cada año y que ésto también se registra como un bloque.

[Unidad: 1 mil de personas, %, 1 mil de casos], Fuente: Oficina de Estadística 「Estadística de Migración Interna」

		2016
Migración Total	**No. de población migrada**	7,378
	Tasa de población migrada(%)	14.4
	No. de declaración de población entrada	4,636
	Tasa de Sexo de Población Migrada(Mujer=100)	103.9
No. bruto de población migrada por cada zona	**Área Metropolitana**	-1
	Área Central	41
	Área de Honam	-16
	Área de Youngnam	-40

La población total de Corea es de 51,525,338 a finales de 2015 según el portal nacional de estadística(http://kosis.kr). 1 resumen de registro civil debe haber por cada población, y renovarse cada vez que se mueva en el area de residencia. De acuerdo con los datos de la tabla anterior, se puede observer que un total de 7,378,000 renovaciones de resumen ocurrieron durante el año 2016.

Si se trata de una cadena de bloque lineal, entonces la cadena de bloque inicial consta de tantos bloques como la población total, y se deben agregar los bloques como el número de personas que viven en cada año. Si se aplica desde 2016, la cantidad de bloques en la cadena de bloques a partir de finales de 2016 es la siguiente.

51,525,338 (No. de bloques iniciales) + 7,378,000 (No. de bloques modificados en 2016) = 58,903,338

Y suponiendo un promedio de 7,000,000 migraciones al año, se agregan 7 millónes de bloques anualmente. Aquí, el tamaño total de la cadena de bloques, que es el tamaño de 80bytes por bloque y se acumula durante 10 años, se calcula de la siguiente manera.

$$\textit{Tamaño de la cadena de bloque} = (51{,}525{,}338 + 7{,}000{,}000 * 10) * 80 / 1024^3 = 9.1\ G$$

---

[7] Según los datos publicados por el Portal Nacional de Estadística, el número exacto de migrantes en 2016 es de 7,378,383.
[8] El tamaño del encabezado de bloque del Bitcoin es de 81 bytes.

En el caso de una cadena de bloque lineal, el tamaño de la cadena de bloque acumulativa de 9.1G durante 10 años y el aumento incremental de 0.52G para cada año se aumentan linealmente.

Si aplica las mismas condiciones a X.Blockchain, el número y el tamaño de todos los bloques serán los mismos, pero el número de bloques modificados que se agregarán cada año consistirá en las subcadenas en lugar de estar linealmente conectadas a la cadena principal. Es decir, 70,000,000 de bloques sobre los modificados durante 10 años estarán compuestos de las subcadenas de la cadena principal que constarán de 51,525,338 bloques. La aplicación de un promedio aritmético simple de los bloques modificados en la subcadena de la cadena principal tiene una subcadena por 1 bloque en cada cadena principal y 1,35 bloques por subcadena. El tamaño de la cadena de bloques por 1 población basado en ésto es el siguiente.

*Tamaño promedial de subcadena = (7,000,000 * 10 / 51,525,338) * 80 = 108.68 B*

*Tamaño de la cadena principal = 51,525,338 * 80 / 1024^3 = 3.83 G*

A diferencia de las cadenas de bloques lineales, X.Blockchain permite una gestión selectiva de los datos requeridos. Si por alguna razón es posible proporcionar los servicios tales como la gestión del resumen del registro cívil para 1 millón de población específica. En este caso, la capacidad total de almacenamiento requerida para verificar el historial de modificación del resumen del registro cívil de 1 millón de población durante 10 años es la siguiente.

$$3.83 + 108.68 * 1{,}000{,}000 / 1024^3 = 3.93\ G$$

En el futuro, el tamaño de la cadena de bloque se aumenta solo por el tamaño del bloque de modificación promedia para 1 millón de personas cada año.
[3]Las suposiciones en este capítulo no tomaron en cuenta el aumento en la cadena principal con el nacimiento, y el aumento de subcadena[3] según la muerte, el matrimonio y el divorcio. Entonces se necesitará un tamaño de todo el bloque más grande. Además, los criterios de clasificación de la cadena principal no son necesariamente 1 población, ni un bloque contiene un documento(transacción). Por lo tanto, el valor anteriormente calculado tiene el significado no práctico, sino solo como un valor relativo para comparar la cadena de bloques de la estructura lineal y X.Blockchain de la estructura multidimensional.

Sin embargo, el ejemplo anterior se aplica solo a un documento 1 llamado el resumen del registro civil, pero varios documentos públicos se pueden aplicar al mismo tiempo. Cuantos más documentos se agreguen, mayor será la eficiencia relativa de la cadena de bloque multidimensional frente a la cadena de bloque lineal. Suponiendo que el ejemplo anterior agregue 1 documento de prueba de otra institución pública y que la transacción, como el historial de modificación, ocurra a una tasa similar al resumen del registro cívil, en caso de la cadena de bloque lineal y al agregar 1 documento más, se necesitará la doble cantidad de bloque. Si se agrega otro documento, el mismo bloque también se incrementará.

Sin embargo, en el caso de X.Blockchain, no hay modificaciones en el tamaño de la cadena principal, y dado que la adición de bloques por el tipo de documento agregado se realiza solo en la subcadena, mayor será la eficiencia relativa de X.Blockchain de la estructura multidimensional.

---

[9] Corresponde al número promedio de migrantes durante 10 años por población.
[10.] Cuanto mayor es el incremento de la subcadena, mayor es la eficiencia de X.Blockchain de la estructura multidimensional.

Conclusión

Como se mencionó anteriormente, no se cambia el tamaño de toda la cadena de bloque. La diferencialidad principal de X.Blockchain en la estructura multidimensional es que permite la gestión selective de datos(bloques) de acuerdo con los criterios específicos. Además, el cliente usuario almacena y gestiona selectivo y directamente una cadena de bloques dentro de un rango requerido, de modo que el problema de confianza en el documento puede resolverse por sí mismo sin la intervención de la tercera institución fiduciaria dentro del rango.