X.Blockchain

Yongseok Kwon

2017-05-23 Rev 1.

Abstract

Bitcoinの登場とこれを利用した取引の急増は、ブロックチェーン技術が取引元帳として信頼できるほど充分に安全であることを証明した。
ブロックチェーン技術が注目されるようになった主な理由は、既存の方式とは違って信頼性の確保の問題において第三の信頼機関（Trusted Third Party、TTP）を排除したことと、全ての取引内容がネットワークに参加する全ての参加者に分散保存されることで取引内容の造作を事実上不可能にしたことにある。
ブロックチェーン技術において最も重要な核心的概念は「Decentralization（脱中心化）」と「Distributed Ledger（分散元帳）」の概念である。従来の方式では全ての取引が1つの集中化した中央サーバーに記録され、その取引の信頼はこの中央サーバー（第三の信頼機関）によって「保証される」方式であった。しかし、ブロックチェーン上で発生した取引はネットワークに参加する全ての参加者に伝達され、「検証」、「合意」され、「ブロック」単位で束ねられて順次的（線形的）に繋がる。

全ての取引内容が記録されるブロックチェーンのサイズは、累積取引件数が増えるほど、すなわち時間が経つほど段々増大するしかなく、これはネットワークの全ての参加者が全体ブロックチェーンを保存管理するということは事実上不可能になる時期がいつか到来するということを意味する。すなわち、ブロックチェーン全体を保存管理できるほどの性能を備えたシステム（ノード）は徐々にその数が減っていき、相対的に少数のノード集団を形成する可能性が高い。そして、これはまた別の形態の中央集中化という結果を引き起こすことになるだろう。相対的に少数のノード集団が全体ブロックチェーンを管理する状況では、取引の信頼性はこの少数のノード集団に依存することになってしまう。すなわち、ブロックチェーンの根本概念である「脱中心化」が酷く棄損されてしまうことを示唆する。

本文書は、特に電子文書を保護するためのブロックチェーン技術の応用において、ブロックチェーンの連結構造を既存の線形的な構造から多次元構造へと変形したX.Blockchainを提案することにより、全体ブロックチェーンサイズの問題とこれに伴うノード集中化の問題に対する解決策を模索することを目的とする。

Problems

ブロックチェーンのサイズは時間が経つほど取引の累積件数に比例して増加し続ける。ブロックチェーンネットワークに参加する全てのノードに元帳が分散保存管理され、これによって第三の信頼機関がなくても取引に対する信頼確保が可能となるというブロックチェーンの根本概念に充実しようとしたとき、増え続けるブロックチェーンサイズの問題はノードの参加において限界状況を引き起こすことになる。すなわち、巨大化したブロックチェーンを保存管理する完全ノード[1]として参加するためには、保存空間の確保といった一定水準以上の性能が要求される。この性能水準はブロックチェーンのサイズに比例して上向きになるだろうから、参加ノードの数的減少は避けられなくなり、これはさらにまた別の形態の「中央集中化」を生み出すことになると考えられる[2]。2017年5月現在、Bitcoinの取引データを含めた全体ブロックチェーンのサイズは既に115G[3]を超えており、イーサリアムのブロックチェーンもやはり最近20Gを超えた。

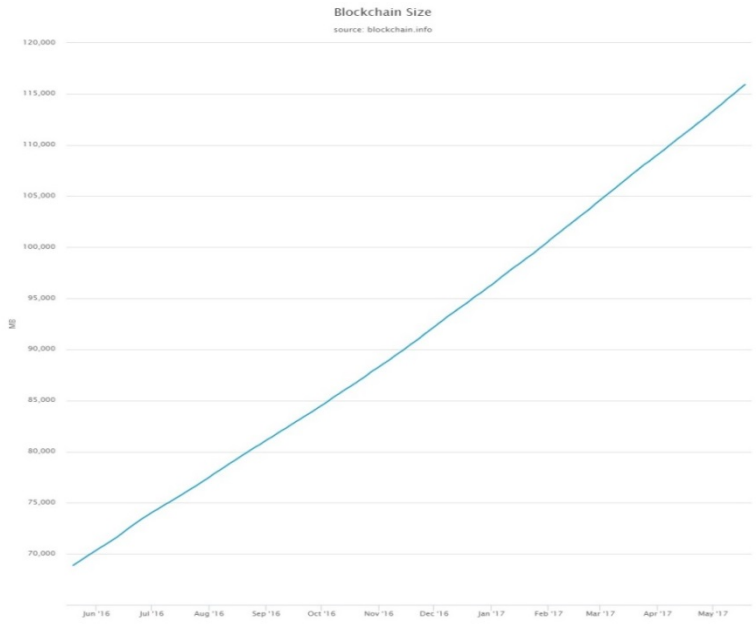

Figure 1. Bitcoin's full blockchain size

また、Bitcoin基準で現在世界的に存在する完全ノードの数は約5,000～7,000個ほどと集計されている。

---

[1] 完全ノードは全体ブロックチェーンを細ンし、新しいブロックの採掘作業を行うノードを意味する。

[2] この問題に対する解決策として、Bitcoin では SPV を提案している。トランザクションデータを除くブロックヘッダー情報だけで取引の証明を行うことにより、これに必要なリソースを最小限に抑える方法であり、電子文書のためのブロックチェーン応用においてこれは必須的に適用される。暗号通貨によってトランザクションを構成するのが取引内容だとすれば、電子文書応用においては電子文書データがトランザクションの主要な部分となる。ここで、文書のサイズは暗号通貨の取引内容とは比べものにならないほど大きいため、ブロックチェーンに文書データそのものが含まれることはない。
本文書で別の記載がない限り、「ブロックチェーンのサイズ」とは「ブロックチェーンのヘッダーのサイズ」を意味する。

[3] 取引を記述するすべてのトランザクションデータとブロックヘッダー情報を含む全体ブロックチェーンのサイズ。

一方、一定水準に達していない数多くのユーザークライアント（モバイルデバイスを含む）は完全ノードとしての参加を制限されることになる。これにより、取引に対する信頼の有無をユーザークライアントが自ら（第三の信頼機関なしに）判断することができず、相対的に少数であるこのノード集団に「依頼」せざるを得ず、その結果を一方的に「受け入れる」しかなくなる。ここで、少数の完全ノード集団は「第三の信頼機関」のように作動する。

このような「完全ノードの集中化」の問題の背景には、前述したとおり、巨大化した全体ブロックチェーンの保存及びブロックの生成（採掘）時に要求される高いコンピューティングパワーが原因となっている。ここで、再び全体ブロックチェーンの保存が要求される理由は、ブロックチェーンの構造が線形的な連結構造となっているため、実際に必要なブロックだけを切り離すことは意味がないからである。連結が途切れたブロックの集合はいかなる信頼も確認してくれることができず、何らの価値を持たない。

このような問題は暗号通貨などの「取引」においては一面避けられない側面がある。どのくらいの通貨が、どこの口座からどこの口座に移動したかを記録するにおいて、ある制限や分類が不可能である。通貨の「量」または通貨の移動に利用される「口座」を基準にして取引を分類することができない。全ての取引は同様の意義を持っており、同様の意義を持つ全ての取引はどんな基準でも分類することができないため、このような性格の記録を扱ううえで線形的な構造から脱皮するということは事実上不可能に見える。

しかしその一方で、「電子文書」の場合、暗号通貨のそれとは違って文書に関する様々な記録は全て該当する「文書」を中心に行われる。文書に対する生成、修正、転送、閲覧、廃棄など全ての記録は該当する「文書」が対象となる。
これは、文書そのものとそれに関連した記録がその「文書」を基準にして分類できるということを意味し、またこれはブロックチェーン上のチェーンが1つの線形的な構造ではなく多数のチェーンに分類できるということを意味する。

N-Dimensional Blockchain – X.Blockchain

X.Blockchain は、前述した電子文書の特性を反映し、文書に関するすべての記録（Transaction）を 1 つの線形的構造で連結するのではなく、「文書」またはそれに準ずるある「基準」によって分類する。そしてこの基準に従って複数のチェーンを構成することにより、多次元形態のブロックチェーンを提案する。
例えば、「文書」を基準とした場合、各文書の「最初生成」は既存のブロックチェーンと同様の線形的な構造のブロックチェーン（main-chain）に記録される。しかし、既にmain-chainに記録された特定の文書に対して発生した変更などの追加記録（Transaction）については、main-chainではなくmain-chain上の該当

するブロックをgenesis block[4]とするまた別のブロックチェーンであるsub-chain上に記録される。

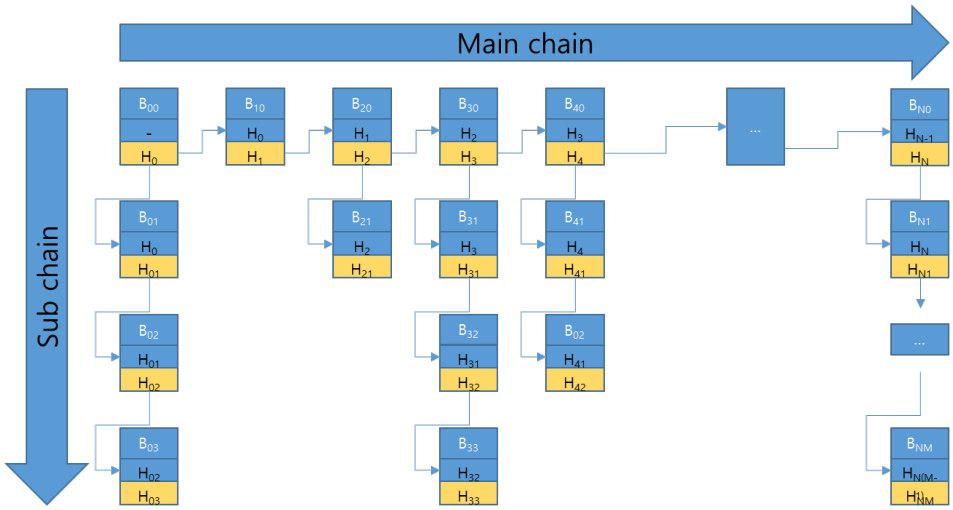

Figure 2. X.Blockchain

上図は2次元構造で構成されたX.Blockchainを表している。前述の「文書」をmain-chainの基準とした場合、main-chainを構成する個々のブロック（B_{00}～B_{n0}）には全て新規文書の生成記録が含まれており、同時に各sub-chainのgenesis blockになれる。例えば、B_{20}に生成が記録された電子文書E_{20}に対する最初の修正が発生した場合、これはmain-chain上の次のブロックであるB_{30}ではなく、B_{20}をgenesis blockとするsub-chain上のB_{21}に記録される。

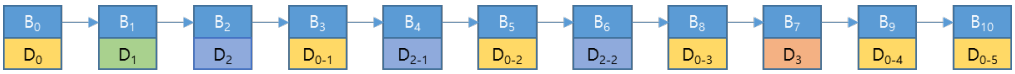

Figure 3. 線形的なブロックチェーン

線形的なブロックチェーン構造では、同じ文書であっても該当する文書の変更などの追加記録はブロックチェーンの追加ブロックを必要とする。

上図は文書D_0～D_3がブロックチェーンに追加された状況を線形的に構成した例である。この例において、文書D_nは生成、D_{n-m}は文書D_nに発生した変更や転送などの追加記録を意味する。文書D_0の場合、生成を含めて全6件の記録（～D_{0-5}）が発生しており、文書D_2の場合、全3回の記録（～D_{2-2}）が発生している。

上記のような線形的なブロックチェーンにおいては、全てのクライアントは特定の文書の信頼を自ら検証す

[4] ブロックチェーンの最初のブロック.

るには全体ブロックを全て確保して保存しなければならない。すなわち、文書D_2だけを必要とするクライアントであっても、事実上不要なD_0、D_1、D_3に対するブロックとD_0の追加記録が入っているブロックD_{0-1}～D_{0-5}までの全11個のブロックが必要となる。

しかし、同じ状況をX.Blockchainで構成すると、下図のようになる。

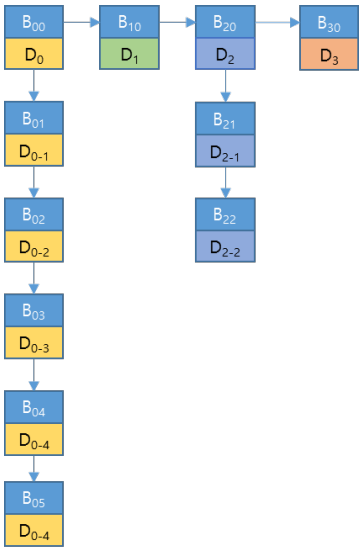

Figure 4. X.Blockchain

上図においてB_{00}～B_{30}はmain-chainを構成し、B_{00}とB_{20}をgenesis blockとするそれぞれのsub-chainが構成されている。このような多次元構造のブロックチェーンでは、全てのクライアントが全体ブロックチェーンを持つ必要がない。上記の例のとおり、文書D_2だけを必要とする場合は、全体ブロックチェーンではなくD_2をgenesis blockとするsub-chainとその上位のmain-chainだけを保有すれば、文書D_2に対する信頼性を自ら判断できる。すなわち、main-chainのブロックB_{00}～B_{30}とsub-chainのブロックB_{21}～B_{22}で構成された全6個のブロック情報を保有するだけで十分なのである。

ここで、Main-chainに適用された「分類基準」が必ずしも「文書」になる必要はない。サービスの構成に応じて「部署」単位が基準として適用されることもでき、または関連性のある文書の集合が分類基準として適用されることもできる。
また、状況によってはsub-chainはまた別のsub-chainのmain-chainになるように構成することもできる。土地台帳の場合、大きな範囲である「地域」をmain-chainの基準とし、それより小さい単位である市町村単位を第1のsub-chainとし、さらに土地の区分単位を第2のsub-chainに分類すれば、上図で示された2次元構造ではなく、下図のような3次元構造の構成が可能となる。

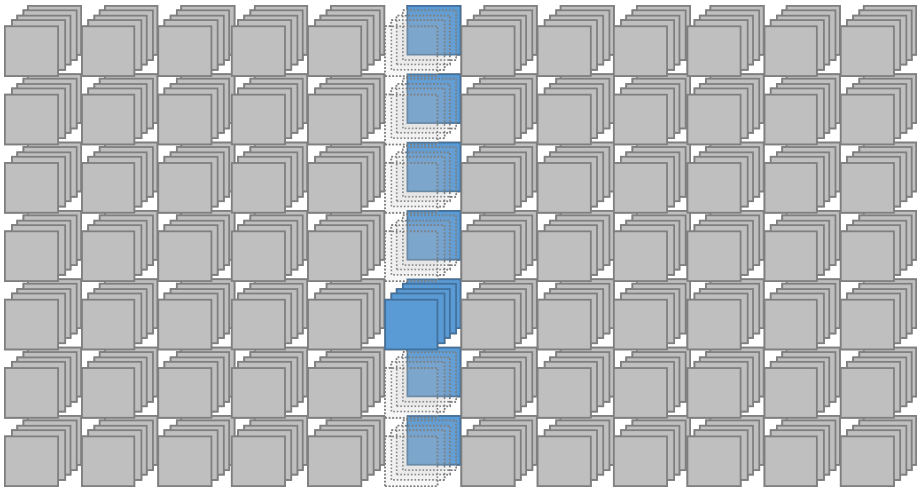

Figure 5. 3 次元構造の X.Blockchain

X.Blockchain上で新しいブロックの採掘を担当する完全ノードは依然として全てのブロックに関する情報を必要とする。しかし、採掘ではない、文書に対する信頼の有無を判断するにおいてクライアント（ユーザー機器）では全体ブロックの情報を必要としない。それぞれのユーザーは検証する必要のある文書が含まれたsub-chainとすぐ上位レベルのmain-chainを確保するだけで十分対象文書に対する信頼を「第三の信頼機関」抜きで検証できる。ここで完全ノードは信頼の有無を確認してくれる第三の信頼機関ではなく、「採掘」を行う役割を果たすだけである。

Parallel Transaction Processing

線形的なブロックチェーン構造では、1つのブロックが生成される間に発生した全ての取引（Transaction）は次のブロックの採掘が開始されるまで待機状態になる。さらに、1つのブロックのサイズ[5]が無限に大きくなることが許されていないため、場合によっては、次のブロックではなくその次のブロックが採掘される時まで待機されることも十分あり得る。ブロックチェーンネットワークに配布されたトランザクションがブロックに含まれて確定されるまでの待機時間は「1秒当たりのトランザクション処理数」－TPS[6]を低下させることになり、その分トランザクションの処理は遅延される。

しかし、X.Blockchain上では、sub-chainごとにブロックの採掘作業を同時に進めることができる。例えば、main-chain上のブロックB_{n0}の採掘作業とsub-chain上のブロックB_{2m}の採掘作業を同時に行うことができる。

[5] Bitcoin ではブロックサイズを 1MB に制限している。ブロックサイズの制限はブロックに含まれる取引の数を制限することになり、単位時間当たりに処理される取引の数（Transaction Per Seconds – TPS）を低下させる。現在、Bitcoin のブロックサイズを拡張しようとする議論がなされており、Bitcoin Classic のような一部の実装では、2MB のブロックサイズを使用していることもあるが、採掘者らからの支持は得られていない。

[6] 現在、Bitcoin の TPS は約 7 TPS 程度を記録している。

B_{n0}とB_{2m}は互いに分離されたブロックチェーンに属しているため、相互連結の関係がないからである。

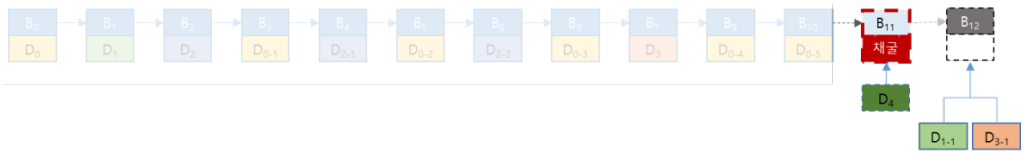

Figure 6. Transaction Processing - 線形構造ブロックチェーン

上図は、前述した例の状況において、D_4が新規生成され、続いて文書D_1とD_3に対する変更記録が発生した場合を仮定したものである。線形的なブロックチェーンでは、D_1とD_3の変更記録は進行中のD_4の新規生成に対する採掘作業が行われる間、待機状態になる。D_4の生成ブロックB_{11}の採掘作業が完了した後、次のブロックB_{12}に対する採掘が開始されるときに、D_1とD_3に対する変更事項はブロックB_{12}に含まれ、採掘作業が完了し最終的にブロックチェーンに連結されるときにはじめてブロックチェーンへの記録が完了する。

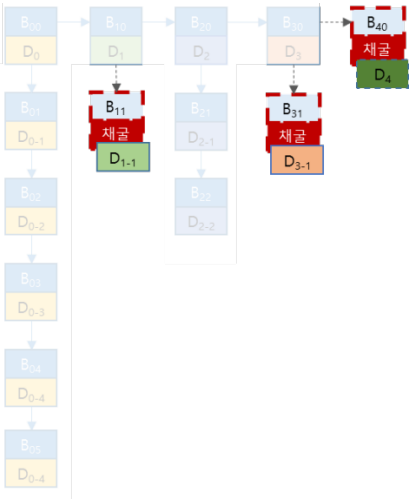

Figure 7. Transaction Processing – X.Blockchain

しかし、多次元構造のX.Blockchainでは、上図のとおり、文書D_4の生成ブロックB_{40}の採掘が完了するまで文書D_1、D_3の変更事項に対するブロックB_{11}、B_{31}の採掘作業を待たせる必要がない。提示された例において、全ての新規ブロックB_{40}、B_{11}、B_{31}に対する採掘作業はそれぞれ独立して同時に進行できる。

Effectiveness

住民登録抄本を電子文書化のうえでブロックチェーン技術を適用して管理すると仮定した場合、X.Blockchainの適用と既存のブロックチェーンの適用でどのような違いがあるかについて説明する。

構成人口1人当たりに1つの抄本が存在し、これが1つのブロックを構成すると仮定し、移動人口数の分だけ住民登録抄本の更新が発生するが、これもやはり1つのブロックに記録されると仮定した。

[単位：千人、%、千件]、出所：統計庁「韓国国内人口移動統計」

		2016
総移動	**移動者数**	7,378
	移動率（%）	14.4
	転入届件数	4,636
	移動者の男女比（女性=100）	103.9
圏域別の純移動者数	**首都圏**	-1
	中部圏	41
	湖南圏	-16
	嶺南圏	-40

国家統計ポータル（http://kosis.kr）の発表によると、2015年末現在の韓国の総人口は51,525,338人である。人口1人当たりに住民登録抄本1部が存在し、居住地域を移動する度に抄本は更新される。上表のデータによると、2016年の一年間に全7,378,000回[7]の抄本更新が発生したことが分かる。

これを線形的なブロックチェーンで構成すると、最初のブロックチェーンは全体人口数分だけのブロックで構成され、毎年移動人口数分だけのブロックが追加されなければならない。2016年から適用したとすれば、2016年末現在のブロックチェーンのブロック数は以下のとおりとなる。

51,525,338（初期ブロック数） ＋ *7,378,000*（*2016*年の変更ブロック数） ＝ *58,903,338*個

そして、1年で平均7,000,000人の人が移動すると仮定した場合、毎年7百万個のブロックが追加される。これに、1つのブロックサイズを80byte[8]として10年間の記録が累積された全体ブロックチェーンのサイズを算出すると、以下のとおりとなる。

ブロックチェーンのサイズ ＝ （*51,525,338* ＋ *7,000,000* × *10*） × *80* ÷ 1024^3 ＝ *9.1 G*

[7] 国家統計ポータルの発表資料によると、2016 年の移動人口の数は正確には 7,378,383 人である。

[8] Bitcoin のブロックヘッダーのサイズは 81byte である。

すなわち、線形構造のブロックチェーンでは、10年間の累積ブロックチェーンのサイズ9.1Gと今後の毎年の変更による増加分0.52Gが線形的に増加する。

同じ条件をX.Blockchainに適用した場合は、全体ブロックの数とサイズは同一であるが、毎年追加される変更ブロックの数がmain-chainに線形的に連結されるのではなく、sub-chainとして構成される。すなわち、10年間の変更分に対する70,000,000個のブロックは51,525,338個のブロックで構成されたmain-chainのsub-chainに分散されて構成される。変更分のブロックがmain-chainのsub-chainに分散される程度を単純な算術平均で求めると、main-chainのブロック1個当たりに1個のsub-chainを持ち、sub-chain1個当たりに1.35個[9]のブロックを持つことになる。これに基づいて人口1人当たりのブロックチェーンのサイズを求めると、以下のとおりとなる。

$$\textit{sub-chain}\text{の平均サイズ} = (7{,}000{,}000 \times 10 \div 51{,}525{,}338) \times 80 = 108.68\ B$$
$$\textit{main-chain}\text{のサイズ} = 51{,}525{,}338 \times 80 \div 1024^3 = 3.83\ G$$

線形構造のブロックチェーンとは違ってX.Blockchainの場合は、必要なデータに対する選別的管理が可能である。ある理由で特定の人口1百万人に対する住民登録抄本を管理するなどのサービスが必要になってもそれが可能であるということである。この場合、人口1百万人の10年間の住民登録抄本の変更履歴を検証するために必要な総保存容量は、以下のとおりとなる。

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

以後、ブロックチェーンのサイズは、毎年1百万人に対する1年間の平均変更分のブロックサイズの分だけ増加することになる。
この章の仮定では、出生によるmain-chainの増加と、死亡・結婚や離婚によるsub-chainの増加[10]を考慮に入れていない。そのため、実際に必要となる全体ブロックのサイズはもっと大きくなるはずである。また、main-chainの分類基準が必ずしも人口1人に限定されるのではなく、1つのブロックに1つの文書（Transaction）だけが含まれるものでもない。だから、上記の算出値は実際的な意味ではなく、線形構造のブロックチェーンと多次元構造のX.Blockchainとを比較するための相対的な値としてのみ意味を持つ。

ただし、上記の例では住民登録抄本という1種の文書に対してのみ適用しているが、実際には多様な公共文書が同時に適用されることがあると思われる。追加される文書が多いほど、線形的ブロックチェーンに対する多次元ブロックチェーンの相対的効率性は格段にアップする。もし、上記の例に他の公共機関の諸証明文書1種が追加され、かつ変更履歴などのトランザクションが住民登録抄本と同等の比率で発生すると仮定すると、

[9] 人口 1 人当たりの 10 年間の平均移動数に該当する。

[10] sub-chain の増加分が大きいほど多次元構造 X.Blockchain の効率性は高まる。

線形的なブロックチェーンの場合は文書1種が追加されるとさらに約2倍のブロックが必要となる。そして、また別の文書が追加されるとまた同様にブロックの増加が発生する。
一方で、X.Blockchainの場合はmain-chainのサイズには変化がなく、文書種類の追加によるブロック追加は全てsub-chain上で行われるため、多次元構造のX.Blockchainの相対的効率性はその分高くなる。

Conclusion

上述のとおり、全体ブロックチェーンのサイズには変わりがない。多次元構造のX.Blockchainの主な差別性は特定の基準によるデータ（ブロック）の選択的管理が可能であるということになる。また、ユーザークライアントが必要な範囲のブロックチェーンを選択的に自ら保存管理するため、少なくとも該当する範囲内では文書の信頼の問題について第三の信頼機関の介入を必要とせず、自らが解決できるようにすることにその目的がある。