ポスター
# ポスター12
# 病院情報システム４・電子カルテ
2018年11月24日(土) 10:00 〜 11:00 K会場(ポスター、HyperDemo) (2F 多目的ホール)

[3-K-2-4] ブロックチェーン技術を用いた単一医療機関向け診療記録システムの検討

○百崎 仁祐[1], 高橋 遼[2], 五味 悠一郎[3] （1.日本大学理工学部応用情報工学科, 2.日本大学大学院理工学研究科情報科学専攻, 3.日本大学理工学部）

診療録等の法的に保存義務のある記録を電子保存する場合,電子保存の三原則である真正性と見読性及び保存性の確保が義務づけられている.ブロックチェーン技術では,電子署名による文書作成者の証明とマイニングによる記録の非可逆性から真正性を確保しており,P2P型システムを用いることで見読性と保存性も確保している. そのため,ブロックチェーン技術の医療分野への応用が注目されている.ブロックチェーン技術を用いた診療記録システムは幾つか提案されているが,複数医療機関で利用する方式では,医療機関同士で事前に合意形成を行う必要があるため,導入が難しい.そこで,単一医療機関でも導入できる方式として,単一医療機関内で完結する分散型システムを提案する.この方式では,医療機関内で管理する診療情報が改ざん不可能になるだけでなく,各医療機関の鍵が正当であることを証明する外部機関が不要となる.本研究では, 診療情報量とブロックサイズ及びハッシュチェーンサイズの関係性を明らかにするため,ブロックチェーン技術を用いた単一医療機関向け診療情報システムを構築した. 診療情報量は,医療機関で使用するパソコン台数と入力可能文字数を仮定し,一定時間内に記録される文章量として導出した.実験では,記入と修正及び削除機能を有するブログシステムを構築し,ブログシステムを複数のパソコン上で稼働させ,ブロックサイズとハッシュチェーンサイズを変更した場合の処理時間を計測した.実験結果より,ブログシステムをモデルとした場合の診療情報量とブロックサイズ及びハッシュチェーンサイズの関係性が明らかとなり,単一医療機関向け診療記録システムにブロックチェーン技術を適用できる可能性を示せた.

ブロックチェーン技術を用いた単一医療機関向け診療記録システムの検討

百崎 仁祐[*1]、高橋 遼[*2]、五味 悠一郎[*3]
*1 日本大学理工学部応用情報工学科、*2 日本大学大学院理工学研究科、*3 日本大学理工学部

Examination of medical record system for single medical institution using block chain system

Miyu Momosaki[*1] ,Ryo Takahashi[*2], Yuichiro Gomi [*3]
*1 Department of Computer Engineering, College of Science and Technology, Nihon University ,
*2Graduate School of Science and Technology , Nihon University
*3 College of Science and Technology, Nihon University

Block chain technology is a technology that ensures authenticity because the recording is irreversible. In addition, readability and preservability are secured by P2P type system. This research is an evaluation of medical records system for single medical institution using this technology. First, prepare a blog system using block chain technology. By changing the block size and hash chain size against the amount of information to be handled, we clarify the relationship between them. These experiments show the practicality of the medical record system using block chain technology.

Keywords: block chain, medical records system, single medical institution

1. 緒論

診療録等の法的に保存義務のある記録を電子保存する場合、電子保存の三原則である真正性と見読性及び保存性の確保が義務付けられている [1)]。

ブロックチェーン技術では,電子署名による文書作成者の証明とマイニングを利用した記録の非可逆性から真正性が確保されており、P2P 型システムを用いることで,見読性と保存性も確保されている [2)]。

ブロックチェーンとは、2009 年に Satoshi Nakamoto 氏の論文で提唱された仮想通貨であるビットコインの根幹技術として生まれた分散型台帳システムを指し、記録の改ざん困難性等の特徴が注目され、現在はブロックチェーン 2.0 と呼ばれる仮想通貨以外の用途での活用が進められており、医療分野への活用もその一つである [3)]。ブロックチェーン技術を用いた診療記録システムはいくつか提案されている [4)5)]。 複数医療機関で利用する方式では、医療機関同士で事前に合意形成を行う必要があるため、利用する対象を全国と設定すると導入が難しい。ただし、地域や関連医療機関といった形で対象の範囲を狭めると、導入も簡単になる。

2. 目的

単一医療機関向け診療記録システムにブロックチェーン技術を適用できる可能性を示すために、一定時間に block へ記録できる情報量が、一定時間に記録される診療情報量よりも多いことを明らかにする。加えて、ブロックに診療情報量と transaction のサイズ(ブロックサイズ)及びマイニングの条件(ハッシュチェーンサイズ)の関係性を明らかにする。

3. システム概要

PHP を用いてブロックチェーンを構築した。ただし、1block あたりに取り込まれる情報である transaction のサイズと、新しく block を作成する条件であるマイニングの条件は可変とする。

3. 1 システムプログラム

システムのアルゴリズムを図 1 に示す。

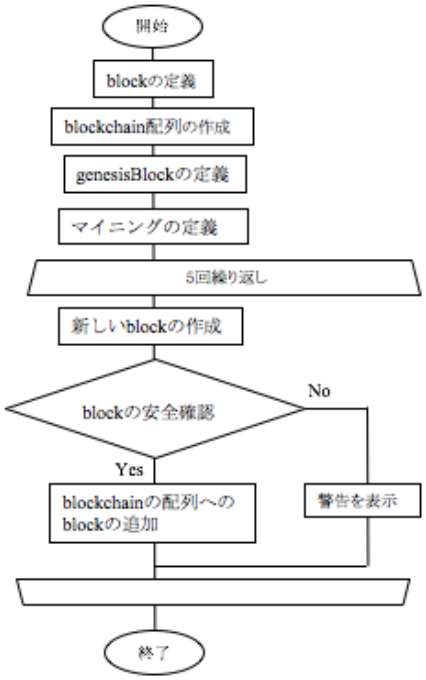

図 1 システムのアルゴリズム

3. 2 システム要素技術

図 1 に示したシステムの処理内容を 1)~7)で説明する。

1) block の定義

図 2 に示すように、block を info と info の hash から構成する。なお info は index、previousHash、timestamp、transaction、proof から構成しており、index は block の通し番号、previousHash は一つ前の block の hash の値である。更に timestamp はタイムスタンプ、transaction は 1block あたりに取り込まれる情報であり、proof はマイニング条件で利用する値である。

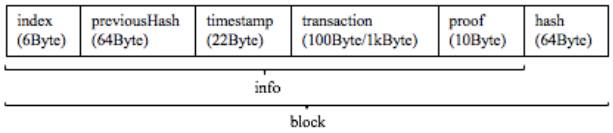

図 2 block の構成

2） blockchain 配列の作成

新しく作成した block が格納されていく blockchain の配列を作成する。作成した配列は、このシステムに参加しているノードで共有される。ただしノードとは、マイニングを行うために、もしくは block に情報を書き込むためにシステムに参加しているコンピュータのことである。

3） genesisBlock の定義

定義した block を使い、genesisBlock を作成する。構成は図 3 に示す。ただし、genesisBlock とは blockchain における最初の block であり、transaction 部分の空きスペースは詰めずに 0 で埋める。

0	"0"	1465154705	"my genesis block!!"	0	"716534932c2b7154836da6afc367695e6337db8a921823784c14378abed4f7d7"

図 3 genesisBlock の構成

4） マイニングの定義

本研究では、block 内の proof と previousHash を連結させて SHA256 のアルゴリズムで計算し、導出したハッシュ値を miningHash と呼ぶ。計算する時は、proof の値を 0 から順に増やしていき、計算したハッシュ値がマイニングの条件に当てはまらない場合は proof の値を 1 増やす。マイニングの条件とは、計算した miningHash を 16 進数とした場合に、下 Y 桁が 0 になる時である。この Y は変数であり、設定する必要がある。条件に当てはまる proof が見つかると proof の値は新しく作成した block に格納される。

5） 新しい block の作成

index には前に作成した block の index に 1 を足した値が入る。また、previousHash には前に作成した block の hash が入り、proof にはマイニングの条件に従った値が入る。更に、timestamp には microtime 関数で求めた結果が入り、transaction は 1block あたりに取り込まれる情報である。ただし、空きスペースには 0 が入るものとする。最後に hash には info を SHA256 のアルゴリズムで計算した結果が入る。

6） block の安全確認

新しい index の値が、1 つ前の block の index に 1 を足した値と等しいことを確認する。また、1 つ前の block の hash が現在の block の previousHash と等しいことを確認する。更に現在の block の hash が info から計算した hash と等しいことを確認する。この 3 つの確認のうち、いずれか 1 つでも等しくなかった場合は警告を表示する。警告が表示された場合は、blockchain の配列に block を追加せずに、新しい block の作成の処理まで戻る。ただし block の作成の処理を 5 回行った後には、警告を出した後、システムは終了する。

7） blockchain の配列への block の追加

安全性が確認された block を blockchain の配列の最後に追加する。追加後は新しい block の作成の処理まで戻る。ただし block の作成の処理を 5 回行った後には、blockchain 配列の最後に block を追加した後、システムは終了する。

3. 3 システム動作環境

システムの動作環境を示す。

・Tera Term
teraterm-4.99.exe
・Raspberry Pi
Raspberry Pi 3 Model B V1.2
・OS
Raspbian GNU/Linux9
・CPU
quad-core ARMv8 Cortex-A53
・メモリ
1GB
・PHP
PHP7.0
・Apache
Apache/2.4.25

4 システム評価

システム評価のための実験は、Tera Term 上で Raspberry Pi を用いて行った。

表 1 に今回の実験条件を示す。1block あたりの transaction のサイズは 100Byte と 1kByte の 2 種類を選べるようにした。マイニングの条件で設定する変数 Y は 3 と 4 及び 5 の 3 種類で行った。設定した桁数が増えるほどマイニングの難易度は上がり、1block が作成されるまでにかかる時間が長くなった。

	transactionのサイズ[Byte]	マイニングの条件[桁]
1)	100	3
2)	100	4
3)	100	5
4)	1k	3
5)	1k	4
6)	1k	5

表 1 実験条件

表 1 に示した 1)～6)の実験条件でシステムを動かした結果を表 2 に示す。ただし、1block の作成時間は 10 回の実験結果を平均したものである。この 10 回の実験結果は、平均値±2SD の範囲に 95%が含まれていたため、求めた平均値は信頼できる値とみなせる。

表 2 実験結果

	1Block作成時間[s]	1秒で作成されたblock数[個]	1秒間に格納できる情報量[Byte]
1)	0.0049600	201.61	20,161
2)	0.0049252	203.04	20,304
3)	0.014700	68.027	6,803
4)	0.0031750	314.96	314,961
5)	0.0038834	257.51	257,506
6)	0.018367	54.446	54,446

更に、診療情報量を表 3 に示す。この情報量は「医療機関が所持するパソコン台数×1 台に1秒で入力される文字数」で導出した。今回の実験では、パソコン台数は鹿児島市医師会病院の 600 台、広島赤十字・原爆病院の 2000 台を参考とした [6), 7)]。更に 1 台あたりの1秒間での入力文字数は、ビジネス

文書実務検定試験 1 級の合格入力文字数である 70 文字を参考とした。

表 3 比較条件

	パソコン台数[台]	1秒で格納する必要がある情報量[Byte]
鹿児島市医師会病院	600	1,400
広島赤十字・原爆病院	2,000	4,667

5 考察

表 1 の実験条件を踏まえて表 2 の結果を比較することにより、マイニングの条件が 1block を作成する時間に与える影響を明らかにすることができた。1)~3)の比較によって、マイニングの条件が 3 桁と 4 桁の場合は 1block を作成する時間は結果の桁数が同じという点で大きな違いは見られなかったものの、5 桁の場合は他の 2 種類の場合よりも結果の桁数が違うという点で大きな違いがあることが分かった。4)~6)を比較した場合も同様であり、5 桁の場合は他の 2 種類の条件よりも 1block を作成する時間に結果の桁数が違うという点で大きく影響を及ぼし、作成時間が他の 2 種類の条件よりもかかる結果となった。

また、1)~3)と 4)~6)を比較することによって、transaction のサイズが 1block を作成する時間に与える影響が分かった。transaction のサイズを増やしてみたところ、1block を作成する時間は結果の桁数が同じという点で大きな影響はなく、このことからマイニングの速さに transaction のサイズは関係がないことが分かった。そのため、1 秒あたりに block 格納できる情報量は transaction のサイズが大きくなるほど多くなる結果となった。

更に、表 2 に示した 1 秒間に格納できる情報量と表 3 に示した 1 秒間に格納する必要がある情報量を比較することによって、一定時間に block へ記録できる情報量が、一定時間に記録される診療情報量よりも多いことを明らかにすることができた。

加えて、これらの結果より診療情報量に対する transaction のサイズとマイニングの条件の関係性を示すことができた。

6 結論

今回の実験では、マイニングの条件が 3 桁と 4 桁の場合に比べて 5 桁の場合で 1block を作成する時間に違いが見られた点から、マイニングの条件が 1block を作成する時間に影響を与えるということが明らかとなった。また、transaction のサイズを増やしてみても 1block を作成する時間は同じという点から、transaction のサイズが 1block を作成する時間に影響を与えないということが明らかとなった。更に、1 秒間に block に格納できる情報量が診療情報量よりも多いことが明らかとなったことから、単一医療機関向け診療記録システムにブロックチェーン技術を適用できる可能性を示すことができた。

ただし、実験条件や比較条件がまだ少ないため、マイニングの条件や診療情報量の参考とする医療機関の数を増やして実験を行う必要がある。更にプログラムの点では、blockchain の配列をノード内で共有する処理を追加する必要がある。

7 文献

1) 医療情報システムの安全管理に関するガイドライン 第 4.2 版 2013. [http://www.mhlw.go.jp/file/05Shingikai12601000Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000026087.pdf(cited 2018-June-23)].
2) 加嵜長門,篠原航:ブロックチェーンアプリケーション開発の教科書,2018.
3) 荒牧裕一:ブロックチェーンアルゴリズムの分類と問題点 2017. [https://ci.nii.ac.jp/els/contents110010061066.pdf?id=ART0010630959 (cited 2018-April-14)].
4) 大下淳一:ブロックチェーンは医療にどう活用できるのか 2018. [http://tech.nikkeibp.co.jp/dm/atcl/feature/15/050200094/011900011/?ST=health&P=3(cited 2018-June-20)].
5) GMO ブロックチェーン オープンソース提供プロジェクト 2017. [https://www.gmo.jp/news/article/?id=5736(cited2018-June-18)].
6) 株式会社ディー・オー・エス導入事例「鹿児島市医師会病院様」 2018. [https://www.dos-osaka.co.jp/ss1_d_kagoshima_med.html (cited-2018-July-15)].
7) 株式会社ディー・オー・エス導入事例「広島赤十字・原爆病院様」 2018. [https://www.dos-osaka.co.jp/ss1_d_jrchiroshima.html(cited-2018-July-15)].
8) ブロックチェーンを PHP でやっていく 2018. [https://www.tomcky.net/entry/2018/01/10/000416 (cited-2018-Aufust-10)].