

タイトル：医薬品エンジニア向けのブロックチェーン

著者：James Canterbury, Steven Thompson, Arthur D. Perez, PhD.

(Pharmaceutical Engineering, 2019, Vol. 3, No. 1, 60-65)

翻訳：京都大学大学院医学研究科薬剤疫学分野 大学院生 木戸 愛 (Ai KIDO)

本稿では、ブロックチェーン技術によって、規制対象のプロセスでデータを収集および管理する方法がどのように崩壊する可能性があるかについて議論する。最初のセクションでは、ブロックチェーンの概要やブロックチェーンに当てはまらないものなど、ブロックチェーンの機能について技術用語を使わないで要約している。次のセクションでは、それを踏まえて、ライフサイエンス系の企業が現在試験運用しているブロックチェーンのユースケースをいくつか議論する。最後のセクションでは、人々や組織がブロックチェーン技術をどのように活用できるかを説明する。

もしこれまでにブロックチェーンという用語を聞いたことがない人でも、おそらく直に耳にするようになるだろう。暗号通貨が流行した背景にあるこの技術は、2016年初頭から勢いを増しており、減速の兆しは見られない。現在、様々な経営の領域にまたがって、ライフサイエンス系企業が、ブロックチェーンを取り入れ始めている。PE magazine (National Society of Professional Engineers; 全米プロフェッショナルエンジニア協会が発行している雑誌) は、2018年7月・8月号に特集記事「ブロックチェーン：臨床試験における次世代の創造的破壊者」を掲載した[1]。これは確かに素晴らしいユースケースだが、業界内で追求されている多くの事例の一つに過ぎない。ライフサイエンスにおけるブロックチェーンの応用に目を向ける前に、まずはその概要から話をはじめよう。

ブロックチェーン

ブロックチェーンとは何か？

多くの人にとって、ブロックチェーンと暗号通貨（最初に広まり、最もよく知られているのはビットコインだろう）は同義語である。しかし、前者は基盤となる技術であり、後者はその技術の応用である。この二つは関連しているが、暗号通貨市場が乱高下しているからといってブロックチェーン技術が不安定だというわけではないことを理解することが重要である。それは未だに進化を続けており、多くの新技術と同様に、世界を変える方法について多くの誇大宣伝や憶測が飛び交っている。この初期の興奮と憶測は、技術が成熟するにつれて薄れていくものである。しかし、ブロックチェーンは、情報を共有および信頼する上で本質的に新しい方法であり、コンピュータシステム間でデータを交換するための

新しい情報の共有や信頼のプロトコルである。もし成功すれば、TCP/IP（伝送制御プロトコルとインターネットプロトコル）が1980年代に導入されたときと同じように、多くの技術の基盤となり、現在至るところで使われているインターネットの発展につながるだろう[2]。

医薬品エンジニアは、ブロックチェーンについて何を知るべきだろうか？それは多くの要因に左右されるのだが、ブロックチェーンプロトコルの進化に携わっているコミュニティがその要因を探求している。しかし、ここで定着していく可能性が高い基本的な概念がいくつか存在し、こういった概念が今のプロセスを再定義してこの技術を活用する方法を決定するだろう。これを医薬品製造業者の文脈の中で捉えるために、図1に示す単純な流通モデルを考えてみたい。

この事例では、完成品の輸送をブロックチェーン上のトランザクションとして捉えることができる。これらの動きを管理および追跡するために、以下の基本的なブロックチェーン要素を使用することにする。

トランザクション：ブロックチェーンネットワークは、peer-to-peer のトランザクションシステムである。つまり、これらは交換の媒体としてネットワークを使用する当事者間の交換を追跡している。とりわけ、これによって、ネットワークプロトコルに基づいて（個人の管理外で）トランザクションにタイムスタンプを付けることができる。ブロックチェーンはデータベースと見なされ、各トランザクションに追加情報を一部含めることができるが、これらは大規模なデータストアではなく、行と列を備えた典型的なリレーショナルテーブル（関係表）にまとめられているわけでもない。

分散型台帳技術：すべてのブロックチェーンは分散型台帳技術（DLT）の一種だが、すべてのDLTがブロックチェーンだというわけではない。

- DLTの「台帳」とは、クレジットカードの明細書とは違い、単に順序付けられたトランザクションのリストである。後で詳しく説明するように、これらの台帳は「追加」しかできない。新しい記録は台帳の最後にしか追加できず、一度追加した記録は二度と変更することができない。
- 「分散型」とは、一つのソースにトランザクションのリストを管理させるのではなく（例：クレジットカード会社）、多くのソースがリストを管理することを意味する。
- 「技術」とは、分散型台帳を同期する方法を定義するプロトコルのことである。これは「コンセンサス（合意）」と呼ばれるメカニズムを通じて行われる。DLTの種類によって、合意に達する方法も異なる。

DLTは、トランザクションリストの完全性を維持する上で中央権力を必要としない、冗長性と回復力の高いネットワークを生み出す。もちろんこれは、この情報がどの程度公開され

ているのか、誰が何を参照できるのかという懸念をもたらすことにもなる。例えば、人々は自分のクレジットカードの明細書を公開することを習慣にはしないだろう。そこで暗号化技術の登場である。

暗号化技術はブロックチェーンの機能性の根底に位置する。これは、私たちが（公開鍵と秘密鍵を使って）トランザクションを保護する方法であり、権限保持者だけがトランザクションに関する特定の情報を閲覧できる状態にする方法の一部でもある。

暗号化技術で最も利用されているツールの一つは、アルゴリズム（コンピュータコードの一部）がほぼすべてのデジタルに対して一意の識別子を生成するハッシュ化である。SHA-256 のアルゴリズムを使用した文字「ISPE」のハッシュは、以下のようになる。

```
E7AE003CF0974DEC21E4BB1000EB3ECD1B-C389471C8CDA83798AA825C51C04B9
```

ハッシュは一方暗号化である。このハッシュしか持っていない場合、それが何を意味するのかを把握する方法は存在しない。しかし、「ISPE」という文字が与えられ、使用したアルゴリズムを知っていれば、同じハッシュを再現することができる。大半のハッシュは非常に影響を受けやすい。元の入力を少し変更しただけで、まったく異なるハッシュが生成される。例えば、同じ SHA-256 のアルゴリズムを使用した「ISPe」のハッシュは、以下のようになる。

```
481A9F91046AEF67E2D2407C05C3E6EE-052894108794324A2B2A1DBFOCB880
```

現在、ブロックチェーンにおけるプライバシーに関して多くの開発が行われており、これは近い将来に大きな進歩をもたらすと期待されている分野である。

ハッシュのハッシュ化：ブロックチェーンが従来の分散型コンピューティングシステムと異なる点の一つは、イミュータブル（不変）なチェーンを作るための「ハッシュのハッシュ化」の概念である。ブロックチェーンは、トランザクションが書き込まれた時期に基づいてトランザクションを「データブロック」にグループ化する。検証後、データが変更されていないことを証明するために、各トランザクションのハッシュが生成される。次に、ブロックチェーンプロトコルは、各トランザクションハッシュをツリー構造に結合し（これによって、ブロックチェーンをより早く検索できるようになる）、その構造に含まれるすべてのトランザクションハッシュのハッシュを作成する。次のトランザクションのブロックが作成されると、前のブロックのハッシュが全体のブロックハッシュに組み込まれ、ブロックを事実上「連鎖」させる。ソースデータを変更するとまったく新しいハッシュが生成されるため、過去のトランザクションを変更するとそのブロックのハッシュが無効になり、それ以降に発生したすべてのブロックのハッシュが無効になる。これは「改ざん不可

能」として知られており、次のブロックチェーン要素（イミュータビリティ（不変性））を導き出す。

イミュータビリティ（不変性）：トランザクション（とそれに関連するデータ）がブロックチェーンに格納されると、（台帳が配布されるため）誰にも知られずに変更することはできなくなる。記録はブロックチェーンの最後にしか追加できないため、どのような変更を加えてもすぐにわかってしまう。履歴を書き換えるには、すべての台帳を同時に変更するための大規模な調整作業が必要になる。これは、誤って書き込まれたトランザクションを修正できないという意味ではない。誤って書き込んでしまった場合、後続のトランザクションによって取り消すものとし、その取り消しの記録は常に残る。ブロックチェーンにルールやコントロールを実装することで、こういった間違いを防ぐことをお勧めする。そこで登場するのがスマートコントラクトである。

スマートコントラクトは、ブロックチェーンに展開できるロジックの一部（ビジネスルール）である。これらは、（コントラクトロジックによって定義された）特定の条件が満たされたときにトランザクションを送信できる「アカウント」として機能する。これらは、通常別のトランザクションである「イベント」を生成することができる。スマートコントラクトをサポートするブロックチェーンの大半は、トランザクションの書き込みと同様の方法でスマートコントラクトを展開する。つまり、コントラクトコードが書き込まれてブロックチェーンに転記されると、それを変更することはできない。ライフサイエンス系企業では、私たちのシステムに存在する多くの統制がスマートコントラクトに組み込まれる可能性がある。これによって、非連結のシステム間でルールを適用することができる。例えば、スマートコントラクトによって、使用期限が過ぎた在庫の移動を防ぐことができるかもしれない。使用期限を設定するのは製造業者だが、在庫を管理するのは卸売業者または調剤者である。現在の世界でこれを実現するためには、一連のインタフェースまたは電子データの交換が必要になる。

トークナイゼーション（トークン化）：ブロックチェーン内のトランザクションは、多くの場合、2つのアカウント間における価値の交換である。その価値を追跡するために、ブロックチェーンはトークンを使用する。暗号通貨やモバイル決済アプリケーションで使用される「代替可能な」トークンは、ユーティリティを表すこともあれば、単なる価値の保管場所になることもある。これらは一意ではなく交換可能である。一方、ライフサイエンス系企業にとって特に興味深いのは、「代替不可能な」トークン（NFT）である。これらは薬のシリアル化されたユニットや一意に識別される医療デバイスといった一意の資産を表している。NFTは、作成、転送、相互の関連付け、および消費（破棄）が可能である。NFTの移動や変更を追跡することで、製品の来歴をブロックチェーンで捉えることができる。「ト

クン化」プロセスは、トークンをブロックチェーン上に作成して維持する。会社が資産の交換媒体としてブロックチェーンを使用し始めるようになると、大規模な取り組みが行われることになるだろう。これがどのように機能するのかを見たい場合は、図 2 にあるブロックチェーン上の資産の追跡を確認してほしい。

ブロックチェーンでないものは何か？

ブロックチェーンの概要がわかったところで、ブロックチェーンに該当しないものについてもいくつか説明したい。

ブロックチェーンは、困難を一発で解決できる方法ではないし、独自のスタンドアロンソリューションでもない。 ブロックチェーンはシステムやビジネスパートナーをつなぐ屋台骨になる可能性が高いが、既存のシステムも依然として役割を果たすだろう。また、イベントを引き起こしたり重要な情報を記録したりするには、既存のシステムをブロックチェーンに統合する必要がある。ブロックチェーンを利用すると、オフチェーンデータを格納および保護するために追加のデータ共有要件が導入される可能性がある。

ブロックチェーンはビットコインではない。 ビットコインは、長期にわたるブロックチェーンの実験であり、アカウント間で価値を受け渡すためにブロックチェーンネットワークを使用している暗号通貨である。ライフサイエンスにおけるブロックチェーンの最初の本格的な使用が、ビットコインやその他の暗号通貨に関連する可能性は低い。

ブロックチェーンはアプリケーションではない。 ブロックチェーンの上に新しい種類の分散型アプリケーションを構築することは可能だが、ブロックチェーン自体はアプリケーションではなく、プロトコルベースのネットワークである。イーサリアム（オープンブロックチェーンプラットフォーム）といった多くのブロックチェーンネットワークプロトコルでは、ネットワーク自体の中でスマートコントラクトを実行することができる。ネットワークはロジックを実行できるため、仮想世界のコンピュータと見なすことができるが、それでもやはりアプリケーションではない。

ブロックチェーンはすべてのデータを格納するわけではない。 ブロックチェーンのユースケースを考慮すると、このことを強調しておく必要がある。ブロックチェーンは分散型データベースだが、従来の意味でのデータベースではない。それは、トランザクションの台帳（または順序）を格納するように設計されている。各トランザクションは、わずか数バイトの情報である。大半のブロックチェーンは、トランザクションをできるだけ小さくするようにユーザーにインセンティブを与えている。トランザクションが大きくなりすぎる場合、または多くのトランザクションがある場合、ブロックチェーンにレイテンシ（遅延

時間)が発生する(機能が低下する)。技術が進歩するにつれて、現在のスケーラビリティ(拡張性)の問題は解決されるだろうが、依然としてスモールデータの基本原則は適用されるだろう。つまり、ブロックチェーンが統合されても、現在ライフサイエンス会社が利用しているような電子データインタフェースのような見た目にはならない。

可能性のある用途

ブロックチェーンをライフサイエンスの分野でどのように適用できるかについては、多くの魅力的な予測があるが(「医薬品向けブロックチェーン」とインターネットで検索すると、数日間は困らないくらい多くの読み物がある)、おそらくこの技術の最初の本格的な使用を推進するのは以下の特徴だろう。

反検閲とデータの完全性：これは、まさにブロックチェーンの存在理由である。ブロックチェーンは、記録を操作または抑制できないようにしたいというニーズによって作られた。

加工・流通過程の管理、資産追跡、不変の監査証跡：これはシリアル化を意味する可能性があるが、それは当事者間の資産の交換を追跡することができるネットワークの単なる副産物である可能性が高い。その追跡の信頼性と透明性は、(2~3例を挙げると)資産価値の会計処理、法的所有権/監護権の決定、税務管轄区域間の移動による税金の計算といったやり方を変えるだろう。

存在証明：タイムスタンプは、ブロックチェーン上のイベントを発生順に証明する。資産が100ブロック前に書き込まれた場合、その時点でその資産は存在していたことがわかる。

すべて統合しなくても**モノのインターネット (IoT) を接続する**。ブロックチェーンはネットワークでもあるし、データベースでもある。つまり、ブロックチェーンは、従来の意味でIoTセンサーや既存のシステムといった多くのソースを「接続」することなく、これらのソースからのデータを保存および共有するために使用することができる。上記で指摘したように、ブロックチェーンはビッグデータを格納することを意図していないため、設計によってキャプチャや書き込みができる内容を指定しなければならない。

データ機密性と認証：ブロックチェーンは二要素認証(ユーザー名/パスワード)の範囲を超えて、合意を保存したり、アクセスを許可/取り消したりするための優れたメカニズムを提供する。ソリューションで興味深いのは、人々がブロックチェーンによって自身の個人データの管理方法を改善できるということである。また、これらのソリューションは、組織が個人データをどのように管理しているかを追跡するための信頼性の高い方法を提供する。これは、データ機密性規制に対するコンプライアンスをサポートするのに役立つ。

ユースケース

マッキンゼー・アンド・カンパニー社が公開した最近の記事[3]によって、業界別のブロックチェーンの戦略的重要性が明らかになった。記事に掲載されたいくつかのヘルスケア分野におけるユースケースは、GAMPの実践コミュニティ (CoP) フォーラムで最近議論されているトピックでもある。

ヘルスケア研究：医療情報が個々の患者や治療に関連するトランザクションの形式でブロックチェーンに格納されるようになると、信頼できるデータセットが豊富に出現し、新薬や予防的ケアに対するインセンティブの研究方法を変えるかもしれない。また、履歴を記録するこの新しい方法は、データ管理に関する多くの既存ポリシーに疑問を投げかける可能性がある。

現在、ブロックチェーンは諸刃の剣である。既知の機能は取引相手にとっても問題がある。例えば、不変性は有益だが、データ所有者が記録を削除する権利を持つという会社のデータ保持ポリシーに反する場合もある。可視性は重要だが、プライバシーも重要である。必要性和可能性のバランスを探る上で、業界の利害関係者（ステークホルダー）とブロックチェーンプラットフォーム開発者との対話は極めて重要になるだろう。

ー サプライチェーン研究センター (Center for Supply Chain Studies) 創設者、Bob Celeste

アイデンティティとデータセキュリティ：ブロックチェーンで医療記録を管理する可能性はあるが、これにはデータ機密性とセキュリティに関連するリスクがある。現在進行中のいくつかのイニシアチブは、情報交換を管理し、デジタルアイデンティティを検証し、個人データの使用に対するアクセスを許可する（または取り消す）ための手段としてブロックチェーンを探究している。これは、情報の所有権（および統制）を個人の手に戻し、私たちのエコシステムを安全な方法で結びつける上で重要な役割を果たす可能性がある。

ブロックチェーンは、信頼を構築する方法や、ビジネスパートナー間でデータを共有する方法を変えるだろう。

ブロックチェーンはネットワークでもあるし、データベースでもある。

ブロックチェーンはデータシステムやデータセキュリティの相互運用性といった現在の課題に対処する可能性があるため、ヘルスケア業界は大きな期待を寄せている[4]。

－ ノバルティス社 CEO、Vas Narasimhan

薬サプライチェーン：医薬品業界におけるシリアル化と一意のデバイス識別といった主要な要因により、特定の分散型台帳ソリューションは、薬サプライチェーンの来歴を証明する上で多大な利益をもたらしている。また、これらの多くは、輸送中や保管中の薬の安定性に影響を与え得る環境要因を記録するために、IoT デバイスを組み込んでいる。

私たちは、処方薬のセキュリティ機能を段階的に向上させる、医薬品業界向けに承認された分散型ネットワークを構築するために、ブロックチェーン技術の独自の機能を使用することを検討している。私たちは、薬の持ち主が変わるにつれて、秘匿性の高い所有権の連鎖を作り出すことで、流用や偽造を抑える能力を実現できると信じている。この技術で何が実現できるのかを積極的に実験している業界リーダーと協力できるのは刺激的だ。

－ Chronicled 社 医薬品ソリューション責任者、Susanne Somerville

治験：患者レジストリを管理することから治験プロトコルと結果を不変な方法で保護することに至るまで、治験分野におけるブロックチェーンのユースケースは多数存在する。ブロックチェーンは、開発業務受託機関、スポンサー組織、規制当局間のコミュニケーション、信頼、プライバシーのギャップを埋めることができる。

ブロックチェーンは、ERP（統合基幹業務システム）が個々の組織に対して機能しているのと同様に、会社のネットワークにも貢献する。ライフサイエンス分野では、これは研究開発や薬サプライチェーン内で流動性とトレーサビリティの両方を生み出すことを意味する。これは、新薬の承認をより効率的にしなが、患者の安全を保つのに役立つだろう。

－ EY Global ブロックチェーンリーダー、Paul Brody

ブロックチェーンを活用するユースケースの開発には多くの可能性が残されているが、業界の解決困難な問題に対するソリューションが登場するのはまだ数年先だろう。技術は未だに進化し続けているため、現在のユースケースを把握することが重要である。これによって、要件を洗練させ、未来のブロックチェーントランザクションを形成するオープンソース規格に組み込むことができる。このような規格の一つが、Ethereum Request for Comment (ERC) -721 であり [5]、Ethereum ブロックチェーン上で NFT（例：シリアル化された薬およびデバイス）を送信するための規格を定義している。これは、ブロックチェーンがライフサイエンス会社にもたらすもう一つの興味深い変化（業界全体の問題を解決するためのオープンソース開発のアプリケーション）にも関わることである。

オープンソース開発は多くの人が力を結集しており、連続する各アプリケーションはコミュニティ内の他者から得られた教訓を用いて構築されている。これによって、よくある同じ間違いをしなくて済み、品質を向上させながら迅速に進むことができる。そのトレードオフは、会社が自分たちのコードを快く共有し、幅広いコミュニティの設計を積極的に取り入れる必要があるということである。

— ブロックチェーン開発者、Will Entriken

ブロックチェーンの扉を開く

では、ブロックチェーンによってライフサイエンス業界はどこに向かうのだろうか。ブロックチェーンは、信頼を構築する方法や、ビジネスパートナー間でデータを共有する方法を変えるだろう。これによって、意思決定時にそのデータの完全性を保証する方法が変わる。規制の観点から見ると、会社はそのことが何を意味するのかを理解し、それを規制当局に説明できるようにする必要がある。スマートコントラクトを介してブロックチェーンに組み込まれるコントロールポイント（管理点）の数が増えるにつれて、外部の上流サブライヤが設定し、社内システムによって執行される「ビジネスルール」が生まれるかもしれない。（例えば、卸売業者から見た使用期限の事例を考えてみてほしい。）こういった変更を理解および活用するには、初期の段階でブロックチェーンを試して「実際にやってみる」ことが重要である。開発者のコミュニティは、ブロックチェーンのユースケースや実用的なアプリケーションに飢えており、ライフサイエンス分野にはそのようなユースケースがあふれている。

ブロックチェーンを始める方法

1. **コツを覚えよう。** あなたの組織やあなたのビジネスパートナーのいずれかが、既にブロックチェーンの試験運用を行っている可能性が高い。プロトコル自体は一般的に無料でダウンロードすることができ、多くの人が段階的なチュートリアルを備えた簡単にインストールできる試験環境を構築している。ブロックチェーンコミュニティは、協働的なものが多いため、手を伸ばせばすぐにアクセスできるだろう。
2. **勉強しよう。** 素晴らしいオンライン DIY チュートリアルがたくさん存在しており、それを体験すればすぐに技術的な側面を理解できるだろう。ユースケースの特定や設計を支援するために、ブロックチェーンの教育セッションやスポンサーワークショップを提供するサービス組織が増えている。
3. **アプリケーションを構築しよう。** これは誰もが得意なことではないかもしれないが、

その技術で実現できることについて学ぶためには、手を動かすことが一番有用である。組織内で概念実証を開始する場合でも、既存の概念実証に参加する場合でも、単に自分で試してみる場合でも、ブロックチェーンの基本を理解すると将来的に役立つだろう。

4. **GAMP ブロックチェーン SIG (Special Interest Group : 特定の興味ある事柄について、その道の専門家の考えを聞いたり、メンバー同士が互いに知識や情報を交換する場)に参加しよう！**本稿の執筆者の多くは、最新の傾向や開発について話し合い、業界のスピーカーから彼らの刺激的なプロジェクトについて聞くために、毎月集まっている。また、私たちは、当社の CoP ウェブサイトを通じて、ライフサイエンス分野における優れた参考記事やケーススタディの一覧表を構築している。

本文以上

<図表の説明>

図 1. 完成品の単純な流通

図 2. トークン化された紙幣で追跡された完成品の流通