製薬協

ブロックチェーンって，なに？

日本製薬工業協会
データサイエンス部会
2019 年度 タスクフォース 1
2020 年 6 月

Executive Summary

近年，様々な分野で「ブロックチェーン」と呼ばれる技術が注目を集めている。医療分野でも活用検討が進められており，パーソナル・ヘルス・レコード（Personal Health Record: PHR）（2.1 章），臨床試験（2.2 章），医薬品流通（2.3 章）などで検討が始まっている。

ブロックチェーンは「分散型台帳技術」（distributed ledger technology: DLT）と呼ばれる技術の一種である。「台帳」といえば，住民基本台帳や備品管理台帳など，ヒト・モノ・カネの出入りを記録・管理する帳簿であるが，なぜ台帳技術であるブロックチェーンが注目を集めているのであろうか。

ブロックチェーンで管理される「台帳」は追記専用（修正不可）に設計されており，デジタル署名（1.2.2.2 章），暗号学的ハッシュ関数（1.2.1 章），合意形成アルゴリズム（1.4 章）等の技術の組み合わせによって改竄が非常に困難となっている（1.6.4 章）。加えて，中央のサーバでその台帳を管理するのではなく，参加者が利用するコンピュータの間で行われる P2P 通信（1.2.3 章）を介して各参加者のコンピュータ内にある台帳を同期することで，参加者の皆で台帳を保持する仕組みを持つ（「分散型」と呼ばれる所以である）。ここから以下のような特徴が生まれる（1.6 章）。

- サーバダウンによるシステム停止が起こらない（耐障害性）
- 全てのデータは参加者が持つため，誰でも内容を確認・検証できる（透明性）
- データを書き換えたり，書き込みを妨げたりできる特別な権限を持つ者がいない（非中央集権性）

これらの特徴一つ一つは従来技術でも達成可能であるが，ブロックチェーンは上記の要素技術を組み合わせたことで「その内容も，その存在も，誰にも否定できないように記録を保存・維持でき，その確かさを誰でも確認できる」ことを可能にするとされている [1]（1.5.1 章）。このような性質により，ビットコイン[1]等の暗号資産（いわゆる仮想通貨）のように改竄の誘惑が働きやすく，悪意ある者を排除できない状況下でも，信頼できる台帳データが管理者なしで維持される。この仕組みがビットコインに留まらず，様々な電子データの「信頼」に革命的変化を起こしうると期待されている。

ブロックチェーンには，大きく分けて自由参加型（Permissionless 型）（1.5.1 章）と許可型（Permissioned 型）（1.5.2 章）があり，それぞれ前提，アプローチ，メリット，限界等が全く異なる。ブロックチェーンをビジネスに利用する際には，両者の違いをよく理解する必要がある。

ブロックチェーンの応用技術として「スマートコントラクト」（1.8.1 章）が挙げられる。これを使えばブロックチェーン上のデータが特定の条件を満たしたときにプログラムを自動実行させることができる。例えば，ブロックチェーンを医療データベースへのアクセス履歴の記録に利用している場合，研究者が

[1] ブロックチェーンはビットコインの中核技術として使用されている。

患者データにアクセスした履歴が書き込まれるたびに，対象患者に当該研究者から自動的に謝礼が支払われるプログラムを載せることなどができる。このような性質から，スマートコントラクトはオートメーションや IoT（Internet of Things）と非常に相性がよい。

他にも「ゼロ知識証明」（1.8.2 章）と呼ばれる技術を使えば，データを秘匿したまま，当該データが特定の条件を満たすか否かを示すことができる。例えば，パスワード自体を開示することなく，正当なパスワードを保有していることを証明したり，暗号化された医療データを復号することなく，ある患者が 18 歳以上であることを証明したりできる。これを用いればブロックチェーンの「透明性」が問題となるような，データの機密性が求められる用途にもブロックチェーンを活用する道が開ける。

さらに，ブロックチェーン上で自分の ID を作成・管理する「非中央集権型識別子」（decentralized Identifier: DID）（1.8.5 章）と呼ばれる応用例もある。Facebook，Google，Amazon といった企業（又は EDC ベンダーなど）が中央集権的に発行する ID ではなく，ブロックチェーンに書き込んだ ID を自己管理し，様々なプラットフォームで利用する。これを「検証可能な資格情報（Verifiable Credentials: VC)」や「ゼロ知識証明」（1.8.2 章）と組み合わせると，「18 歳以上である」「●●社の社員ではない」というふうに，そのつど必要とされる最小限の範囲で，その ID に紐づく個人情報を自由に開示・利用することもできる。

本報告書では，ブロックチェーンの基本的技術を解説するとともに，この技術の課題点や医療業界での活用検討事例について紹介する。

目次

報告書内の用語

用語	説明
P2P	中央のサーバを必要とせず，端末同士が直接通信を行う通信方法。 「1.2.3 P2P（Peer to Peer）通信」を参照。
イーサリアム	代表的なブロックチェーンプラットフォームの１つ。 スマートコントラクトを利用可能。
合意形成アルゴリズム	別々のブロックの同時発生を抑制したり，追加するブロックを投票で決めたりすることで，各ノードが保有するブロックチェーンデータが同一となるように収束させる手法。 「1.4 合意形成アルゴリズム」を参照。
スケーラビリティ	サービスの利用者増大に伴ってシステム規模を拡大できる余地があること。 規模への拡張性。
スマートコントラクト	ブロックチェーン上にプログラムを組み込むことにより，プログラムの条件に基づいた取引を自動で行う仕組み。「1.8.1 スマートコントラクト」を参照。
トランザクション	取引のデータなど，既存のデータの状態を別の状態に変更するためのアクションをまとめた，最小のデータ単位。
ナンス（nonce）	暗号通信で用いられる使い捨てのランダムな値 [2]。“Number Used Once” に由来する。 ブロックチェーンでは，ブロックのハッシュ値が条件に合うようにするために，マイナーがブロックヘッダに追加する任意の数字。値自体に意味はない。 「1.3.3 ブロックの作成（マイニング）」を参照。
ノード	コンピュータネットワークにおける，データの中継装置又は端末装置のこと。 ブロックチェーンでは，参加者ひとりひとりがノードとなる。 「1.2.3 P2P（Peer to Peer）通信」を参照。
ハッシュ値	あるデータから一定のアルゴリズムによって導出されるデータの固有値。 「1.2.1 暗号学的ハッシュ関数」を参照。
ファイナリティ	行われた決済が後から絶対に取り消されないこと。 「1.7.1 即時性」を参照。
マイナー	マイニングを行う検証ノード。「1.3.3 ブロックの作成（マイニング）」を参照。
マイニング	ブロックチェーンにブロックを追加する権利を得るために検証ノードが行う作業。「1.3.3 ブロックの作成（マイニング）」を参照。

はじめに

「ブロックチェーンはコンピューター科学の歴史を変えるほどの大発明である。」

マーク・アンドリーセン（Netscape 開発者，Facebook 取締役）[3]

「インターネットが情報革命を起こしたように，ブロックチェーンは信頼に革命を起こすだろう。これはあらゆることを変える可能性を秘めた技術だ。」

伊藤 穰一（MIT メディアラボ所長 (当時)）[3]

「ブロックチェーンの話を聞いて，これこそが次世代の医療情報基盤として活用できるのではないかと思った。初めてインターネットを導入して触れたときのようなわくわく感がみなぎってきた。」

水島 洋（国立保健医療科学院 研究情報支援研究センター センター長）[4]

ブロックチェーンは，データをブロックと呼ばれる単位にまとめ，時系列順に鎖のように繋げて保存する技術である。ブロックチェーンに記録されるデータは，ブロックチェーンネットワークを構成する多数の参加者から検証を受けながらネットワーク全体に伝搬され，参加者皆が保持し合うことで維持されており，中央のサーバや管理者を必要としない。また，様々な暗号技術や経済的インセンティブを組み合わせることで，ブロック内に記録されたデータを遡及的に改竄することを困難にしている。

ブロックチェーンは暗号資産であるビットコインの中核技術として知られる[1]が，近年，暗号資産以外への応用が盛んに検討されている。医療の分野でも，FDA や各製薬企業がブロックチェーンの活用検討を進めているのに加え，PaaS (Platform as a Service) としてブロックチェーンプラットフォームを提供するサービスプロバイダーも医療分野での活用を積極的に模索している。加えて 2018 年 3 月にはピア・レビュー誌である “Blockchain in Healthcare Today[2]” が創刊され，2019 年 11 月には医療ブロックチェーンに関する網羅的な書籍の和訳版 [4]が発刊され，2019 年 DIA 日本年会でもブロックチェーンに関するセッションが組まれるなど，我々もブロックチェーンについて耳にする機会が増えてきた。

その一方，改竄不可能な夢のツールというイメージや期待が先行し過ぎたためか， Gartner 社の 2019 年の調査によれば，ブロックチェーンは期待に見合う成果を伴わずに過度にもてはやされる「過度な期待のピーク期」を過ぎ，熱狂が冷めて期待が一気に幻滅した「幻滅期」の谷底に向かっているとされている [5]。しかし今後，テクノロジが進化し，ブロックチェーンの特徴を生かした実用的なユースケー

[1] 一般的には「ブロックチェーンはビットコインから生まれた」と説明されるが，ブロックチェーンをどう定義するかによっては Stuart Haber らが考案者であるとする立場（参考文献 [15]など）などもあるため，本報告書では「ブロックチェーンはビットコインの中核技術である」との記載に留めた。

[2] https://blockchainhealthcaretoday.com/

スの展開が広がることによって，2021 年までに幻滅期から脱し始めるとも予測している [5]。

ブロックチェーンは医療分野の様々な課題を解決しうる可能性を持つツールではあるが，これを適切に活用するためには，ブロックチェーンの持つ特徴や限界を正しく理解する必要がある。

本報告書ではブロックチェーンの基本的技術を解説するとともに，この技術の課題点及び医療分野における活用検討事例について紹介する。本報告書が製薬業界におけるブロックチェーンの適切な理解・活用を促進するための一助となれば幸いである。

本書の構成

本書は大きく 2 部構成とした。

第 1 章ではブロックチェーン及びその要素技術を広く浅く解説している。第 1 章は特に読者の事前知識を前提とせず，ブロックチェーンの初学者でも理解できる内容とするよう心掛けた。第 2 章が第 1 章の知識を前提としていることもあり，まずは第 1 章を通読していただくことを推奨する。
ただし初学者のかたは下記の項に関しては必ずしも最初から全て理解いただく必要はない。

- 「1.1 ブロックチェーンの定義」,「1.4 合意形成アルゴリズム」
  ・・・いずれもやや専門的な内容であるため。

- 「1.7 ブロックチェーンの課題」
  ・・・できるだけ網羅的になるよう記載したため。

第 2 章ではブロックチェーンの医療分野での活用事例を紹介している。医療分野での活用に関しては，コンセプトの提唱に留まっているもの，プルーフ・オブ・コンセプト（Proof of Concept: PoC） の段階で止まっているもの，実用化に進んでいるもの，状況が全く不明のものなど，様々なものが混在している。それらの中から，代表的かつ日本の読者諸氏に関心を持っていただけそうなユースケースに絞り，できるだけ具体性のあるものを選んで紹介するよう努めた。

技術的な基礎よりも，ブロックチェーンがどのような分野で，どのような目的で，どのような方法で利用されているのかを知りたいかたは，まず第 2 章から読み始め，詳しく知りたい部分のみ第 1 章に戻ってお読みいただいてもよい。

1　ブロックチェーンとは

1.1　ブロックチェーンの定義

現時点（2020 年 3 月時点）で，国内外で広く合意された定義は存在しない[3]。
ただし，現在 ISO（International Organization for Standardization）に設置された専門委員会[4] で用語の検討が進められており，ここでの定義が最終化されれば，それが国際標準の定義となることが見込まれる。2020 年 3 月 1 日現在におけるドラフト版[5] の定義は下記の通り[6] である [6]。

3.6 ブロックチェーン
暗号技術によるリンクを用いた，追加しかできず逐次的である鎖の中に編成された承認済ブロックからなる分散型台帳。
項目への注記 1：ブロックチェーンは耐改竄性であるように，並びに，最終的，決定的及び不変的台帳記録を創り出すように，デザインされている。

3.22 分散型台帳
DLT ノード全体で共有され，合意形成メカニズムを用いて DLT ノード間で同期される台帳。
項目への注記 1： 分散型台帳は耐改竄性，追記専用，及び不変であるようデザインされており，承認済みかつ検証済みトランザクションを含む。

（原文）
3.6 blockchain
distributed ledger (3.22) with confirmed blocks (3.9) organized in an append-only, sequential chain using cryptographic links (3.16)
Note 1 to entry: Blockchains are designed to be tamper resistant and to create final, definitive and immutable (3.41) ledger records (3.45).

3.22 distributed ledger
Ledger (3.44) that is shared across a set of DLT nodes (3.27) and synchronized between the DLT nodes (3.27) using a consensus mechanism (3.12)
Note 1 to entry: a distributed ledger is designed to be tamper resistant, append-only and immutable (3.41) containing confirmed (3.8) and validated (3.81) transactions (3.77).

---

[3] 日本では，日本ブロックチェーン協会の定義 [100]が言及されることが多い。
[4] TC307 Blockchain and electronic distributed ledger technologies
[5] ISO/DIS 22739
[6] 和訳は本タスクフォースによるものであり，英文が原文である。解釈については原文が優先する。

すなわち，「合意形成メカニズム」（「1.4 合意形成アルゴリズム」参照）によって参加者間で中身が同期される追記専用の台帳を「分散型台帳」と呼び，その中でも，ブロック単位にまとめたデータを時系列順に鎖のように繋ぐものを「ブロックチェーン」と呼ぶ[7]。

[7] 上記定義から明らかなように，ブロックチェーンと分散型台帳の目的に違いはない。“改良版” ブロックチェーンとして近年開発が進められているものの中には，ブロック構造を持たず，厳密には「分散型台帳」と呼ぶべきものもあるが，本報告書では特に区別が必要な場合を除き，便宜的に両者をまとめて「ブロックチェーン」と呼ぶ。

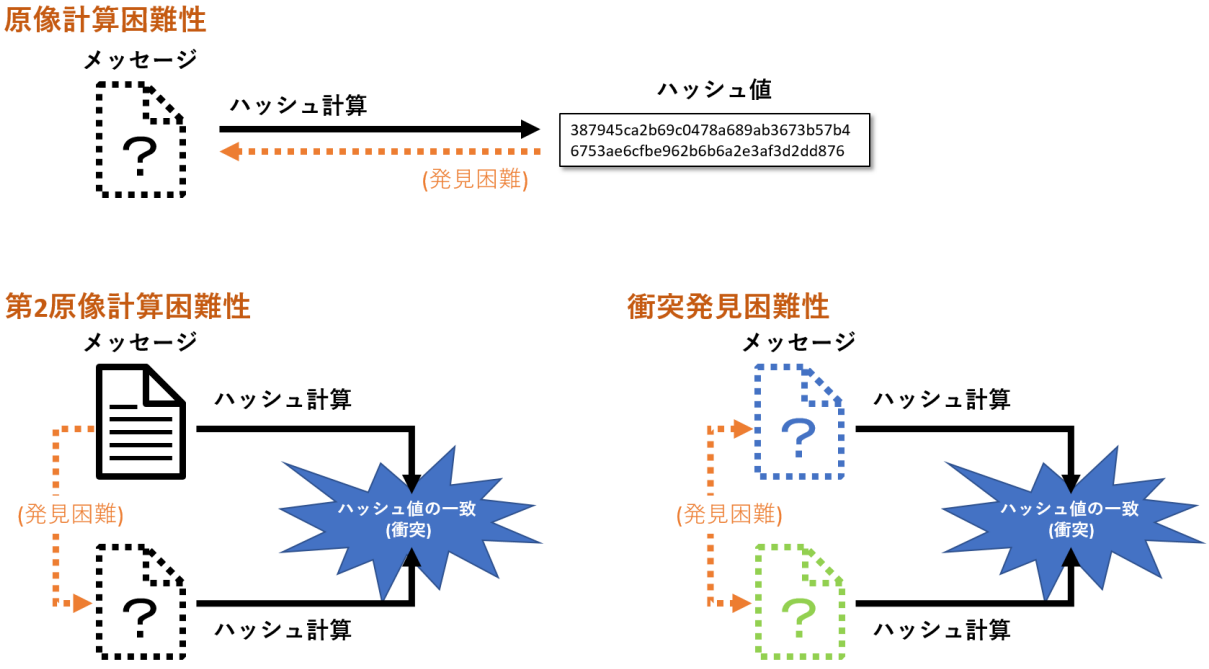
1.2　ブロックチェーンの要素技術

ブロックチェーンを構成する要素技術として，暗号学的ハッシュ関数，鍵暗号技術及び P2P 通信が使用されている。本項では，これらの技術について紹介する。

1.2.1　暗号学的ハッシュ関数

ハッシュ関数とは，メッセージ（入力データ）に対して規則性のないハッシュ値[8]（出力データ）を計算する関数であり，メッセージが 1 文字でも異なれば全く異なるハッシュ値が出力される性質を有する。ブロックチェーンでは，ハッシュ関数の中でも暗号学的ハッシュ関数と呼ばれるハッシュ関数が使用されている。暗号学的ハッシュ関数に求められる安全性として，次の 3 つが挙げられている [7]。

- 原像計算困難性（Preimage Resistance）：
  既知のハッシュ値から，元のメッセージ，又は同一のハッシュ値である別のメッセージを見つけることが困難であること
- 第 2 原像計算困難性（Second Preimage Resistance）：
  既知のメッセージから，同一のハッシュ値である別のメッセージを見つけることが困難であること
- 衝突発見困難性（Collision Resistance）：
  あらゆるメッセージの中から，同一のハッシュ値となるメッセージを 2 つ以上見つけることが困難であること



暗号学的ハッシュ関数には MD5，SHA-1，SHA-2，SHA-3 などの種類がある。しかしながら，MD5 と SHA-1 は衝突発見に成功しており，安全ではないことが知られている [8] [9]。2013 年 3 月に策定さ

[8] 暗号学的ハッシュ関数により生成されるハッシュ値は特に「メッセージダイジェスト」や「セキュアハッシュ」と呼ばれるが，本報告書では「ハッシュ値」と表記する。

れた「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）［10］」では，SHA-2 ハッシュ関数である SHA-256，SHA-384，SHA-512 を使用することが推奨されている。

Windows PC であれば，コマンドプロンプトから certitutil -hashfile <ファイルパス> <ハッシュ関数アルゴリズム>でハッシュ値を求めることができる[9]。

1.2.2　鍵暗号技術

暗号化とは，第三者に通信を傍受されても，その内容を知られないようにする方法である。暗号化する前のメッセージは平文（ひらぶん），暗号化されたメッセージは暗号文と呼ばれ，暗号文を元の平文に復元することを復号という。このときに暗号化と復号に使われる情報を鍵と呼ぶ [2]。本項では，この鍵暗号技術と，それを用いたデジタル署名について紹介する。

1.2.2.1　暗号と鍵

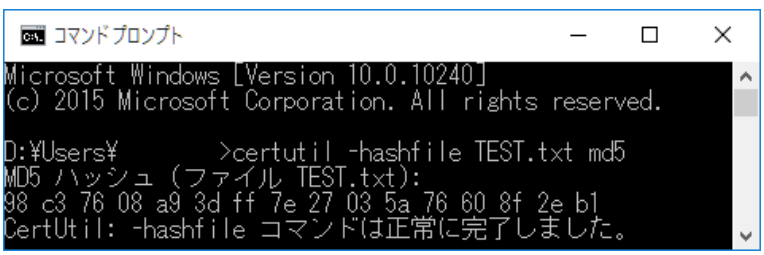
歴史上実際に使われてきた有名な暗号として，シーザー暗号やエニグマがある。シーザー暗号は全てのアルファベットを特定の文字数だけ「ずらす」ことで暗号化を行い，平文に対して「何文字ずらしたか」が鍵となる。エニグマは第 2 次大戦においてドイツ軍が使用した暗号機で，ここから生み出される暗号は 1 文字ごとに変わるアルゴリズムによって文字を置き換えることで暗号化を行うが，このアルゴリズムの設定が鍵となる。

暗号文は鍵を使って暗号化されているため，受信者は鍵を知らなければ復号できない。しかし，鍵の送信時に盗聴されてしまうと，暗号文も第三者に復号されてしまう。このように暗号化と復号に同一の鍵を使う共通鍵暗号では，「鍵配送問題」と呼ばれる課題が生じていた。そこで考え出されたのが，暗号化する鍵と復号する鍵を分ける公開鍵暗号である [2]。

「鍵」と言われて最もイメージしやすいのは家や車の鍵だと思うが，ここでは輸送可能な金庫とその鍵を思い浮かべてほしい。今，秘匿したい情報を金庫に格納して送りたいが，その鍵は金庫を開けてほしい人にしか渡したくない。開閉できる鍵を使っていた場合，この鍵を直接会って渡すか，信頼できる誰かに託すことが主な手法であった。この鍵配送問題を解決するために考え出されたのが，「金庫を閉めることしかできない鍵（鍵 A)」と「鍵 A で閉めた金庫しか開けられない鍵（鍵 B)」に分ける公開鍵暗号である。閉めることしかできない鍵 A を不特定多数に渡したとしても，鍵 B を誰にも渡さなければ中

---

[9] “HASH TEST” という文字を保存したテキストファイルから，md5 でハッシュ値を求めた例：



身を覗き見られることはない。秘匿情報の受け渡しは，公開している鍵 A で金庫を閉めて送ってもらい，自分しか持っていない鍵 B で開けることで安全に達成される。このように，鍵の 1 つを公にすることから公開鍵暗号と呼ばれ，閉めることしかできない鍵 A は公開されていることから「公開鍵」，開けることしかできない鍵 B は自分しか持たないことから「秘密鍵」と呼ばれる。
情報の暗号化において，これらの鍵は 2 本で一対となっており，公開鍵で暗号化された暗号文は，その公開鍵とペアになっている秘密鍵でしか復号できない [2]。

現実の世界においては，「開けることしかできない鍵」や「閉めることしかできない鍵」はイメージが付きにくいと思うが，デジタルな世界では，RSA 暗号や楕円曲線暗号などの現実的な時間で解くことが難しい[10]とされている数学的問題を利用することで，このような鍵が作られている。

1.2.2.2 デジタル署名

デジタル署名は紙媒体における手書きの署名に相当するものであり，本人であることの証明や責任を明らかにするために用いられる。デジタル署名は公開鍵暗号における「秘密鍵を使って作られた暗号文は，秘密鍵を知らない人には作ることができない」という特徴を利用して実現されており，公開鍵暗号を利用しているものの，情報の秘匿を目的とはしていない。
送信者は署名したいメッセージに対して秘密鍵を用いて署名データを作成し，受信者は公開鍵を用いて署名の検証を行う。つまり，デジタル署名において送信者が作成した暗号文は，公開鍵を用いて誰でも復号できる状況となっている[11]。

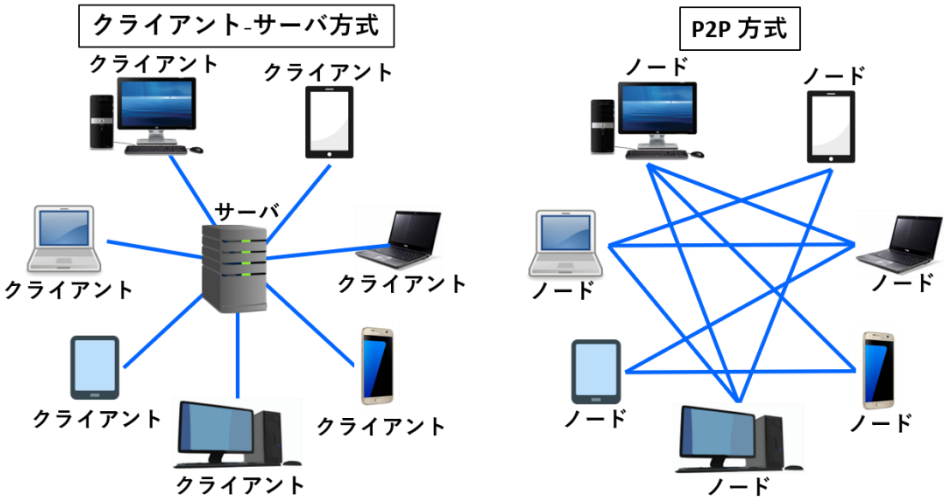
デジタル署名の方法には，メッセージに直接署名する方法と，メッセージのハッシュ値に署名する方法が考えられるが，一般的にはメッセージのハッシュ値に署名する方法が使用[12]されている [2]。ブロックチェーンにおいては，あるアカウントの所有者が特定のトランザクション（1.3 参照）に対してデジタル署名を行うことで，そのトランザクションの内容に同意したことを表明する [11]。

---

[10]量子コンピュータの実現により，現実的な時間で解くことが可能とされている。課題（1.7.8 量子コンピュータ耐性）を参照。
[11]デジタル署名では情報の秘匿を目的としないため，「暗号化」や「復号」という用語が適切ではないとの指摘もあるが，ここでは理解のしやすさを優先して「暗号化」や「復号」という用語を使用した。
[12]メッセージに直接署名する方法では，メッセージ全てに対して秘密鍵や公開鍵による計算を行うため，データ量に比例して署名や検証に時間がかかる。そのため，メッセージから暗号学的ハッシュ関数で算出した，データ量の少ないハッシュ値にデジタル署名を行うことで計算の時間を短縮している。

1.2.3　P2P（Peer to Peer）通信

ブロックチェーン内のデータ通信には P2P 通信が用いられる。P2P は複数の端末（ノード）が対等（Peer）の立場で直接通信することを特徴とする通信方式である。使用例として 2000 年代前半に流行した Winny 等のいわゆる「ファイル共有ソフト」が挙げられるほか，現在では一部の IP 電話などで端末同士が中央のサーバを介さずに直接音声データ等をやり取りするのに利用されている。



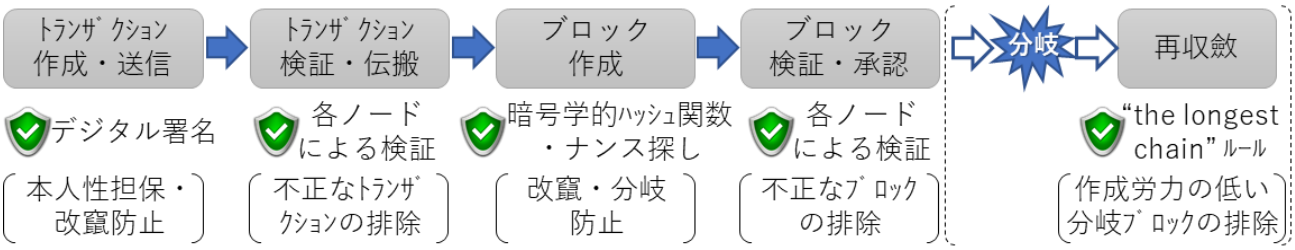
クライアント-サーバ方式ではサーバがダウンするとシステムが止まってしまうのに対し，P2P 方式ではいずれかのノードに障害が発生しても，接続可能なノードがある限りデータ送受信を継続できる。

ブロックチェーンの持つ耐障害性や非中央集権性は，上記のような P2P 方式の特徴に由来する。

1.3　ブロックチェーンの動作メカニズム

本項では最も古典的なブロックチェーンの 1 つであるビットコインを題材として，ブロックチェーンの動作メカニズムの概要を説明する。より詳しくは参考文献 [12] [13]などを参照されたい。

全体の流れ，及び，各 step で用いられる主な技術・手法は下記の通り。



1.3.1　トランザクションの作成・送信

ブロックチェーン上に保存する個々のデータを「トランザクション」と呼ぶ。ビットコインであれば，

- ビットコインをどのアドレスからどのアドレスにどれだけ移すか
- マイナー（1.3.3 参照）に支払う手数料
- トランザクション作成者のデジタル署名（1.2.2.2 参照）及び公開鍵[13]

などが各トランザクションに記録される。

作成されたトランザクションは順次ブロックチェーンネットワークに送信（broadcast）され，P2P 通信（1.2.3 参照）を介して隣接ノードに到達する。

1.3.2　トランザクションの検証・伝搬

トランザクションを受け取ったノードは，受け取ったトランザクションのデータフォーマットが正しいか，既存のトランザクションと重複していないか，支払元のビットコインが使用済みのものではないか等の一連の検証（validation）を行い，有効なトランザクションのみ，自ノードの「メモリプール[14]」と呼ばれるローカルメモリ領域に保存するとともに，隣接ノードにも転送する。一方，無効と判定したトランザクションは保存も転送もせずに廃棄する。この仕組みにより，有効なトランザクションのみがブロックチェーンネットワーク全体に伝搬（flooding）してゆく。

---

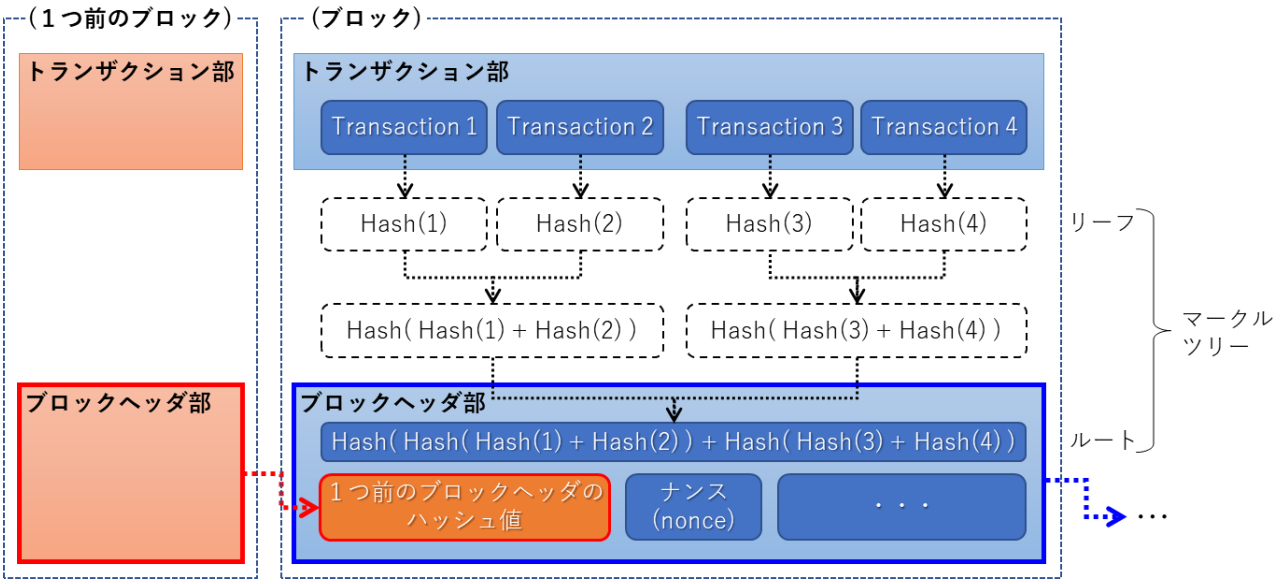
[13] ビットコインでは，公開鍵に暗号学的ハッシュ関数（SHA-256，RIPEMD-160）を適用して得られた値（を，さらに一定のルールに従って加工したもの）をビットコインアドレス（ビットコインの口座番号）として利用している。そのため，トランザクションに含まれている公開鍵に上記の計算を行えば，そのデジタル署名がそのビットコインアドレスの所有者本人のものであるか否かを誰でも検証できる。

[14] 「トランザクションプール」とも呼ばれる。

1.3.3　ブロックの作成（マイニング）

次に，トランザクションをブロックにまとめる作業が行われる。

ブロック作成を行うノードはそれぞれ，自ノードのメモリプールから 1 ブロック分[15]のトランザクションを選び，そのそれぞれを暗号学的ハッシュ関数（1.2.1 参照）にかけてハッシュ値を算出する。そうして得られたハッシュ値を 2 個ずつ連結して再びハッシュ値を算出する。これを繰り返すと，1 ブロック分のトランザクションから樹形図のような形（「マークルツリー」という）で最終的に 1 個のハッシュ値（「マークルツリーのルートハッシュ」又は「マークルルート」）が求められる。



マークルルートは，いわば当該ブロックの全トランザクションの要約値であり，トランザクションのどれかが 1 文字でも異なると，算出されるマークルルートは全く別の値となる。

次に，算出した「マークルルート」に，

- 1 つ前のブロックヘッダのハッシュ値
- タイムスタンプ
- ナンス（nonce）と呼ばれる任意の数字（「報告書内の用語」参照）

などを合わせた「ブロックヘッダ」を作り，そのハッシュ値を計算する。算出されたハッシュ値が，ある決められた数値（ターゲット）よりも小さければそのブロックは完成となり，ブロック作成に成功した者に報酬が与えられる[16]。ハッシュ値がターゲットよりも大きい場合は，ナンスの数値を変更して再度ブロックヘッダのハッシュ値を計算する。ハッシュ値は元のデータから推測できないため，ハッシュ

[15] ビットコインの場合，1 ブロックに含まれるトランザクション数は 2,000~2,500 前後である [99]。

[16] ビットコインで 1 ブロックの生成に成功すると，報酬として 12.5 ビットコイン（日本円で約 1160 万円相当）と，自分がそのブロックに詰め込んだ全トランザクションの手数料の総額を獲得することができる（報酬ビットコイン数・円換算レートとも 2020 年 3 月 1 日時点）。

値をターゲットよりも小さい値にするためには「ナンスを変更してハッシュ値を再計算」を手当たり次第に繰り返さなければならない[17]。これはターゲットの値が小さければ小さいほど困難になるが，ビットコインのターゲットは「平均 10 分間に 1 回，世界で誰か 1 人がようやくブロック作成に成功する」という難易度になるよう，定期的に調整（retargeting）されている[18]。このようにブロック生成ペースをコントロールすることにより，多数のノードがブロック作成を競っていても，無秩序にブロックが作成されることなく，１本のブロックチェーンを連続的に延ばすことが可能となっている。

このような，膨大な計算を行った者がブロックを作成できる方式をプルーフ・オブ・ワーク（Proof of Work: PoW，1.4.1.1 参照)と呼ぶ。また，このように報酬獲得を目指してブロック作成を行うことを，貴金属の採掘になぞらえて「マイニング」と呼び，マイニングを行うノードを「マイナー」と呼ぶ。

また，トランザクションとブロックヘッダ，及び，ブロックとブロックは全てハッシュ値で繋がっているため，どこか 1 箇所改竄すると，連鎖的にそれ以降のブロックも全て改竄しなければ辻褄が合わなくなる。

1.3.4　ブロックの検証・承認

ブロックを完成させたノードは，そのブロックを P2P ネットワーク（1.2.3 参照）に送信（broadcast）する。
ブロックを受け取ったノードはブロック作成作業を休止し，受け取ったブロックの検証[19]を行う。
検証の結果，問題がなければ，そのブロックを自ノードのブロックチェーンに追加する（これを承認（confirmation）という）とともに隣接ノードにも送信する。
加えて，承認した新ブロックに含まれているトランザクションと同じものが自ノードのメモリプールにあれば全て削除し，残った未承認トランザクションを使って次のブロックの作成作業を開始する。

---

[17] 2020 年 3 月 1 日現在，ターゲットは下記の値（16 進数）である [98]。
00000000000000000122cbc00000000000000000000000000000000000000000
すなわち，偶然頭に 18 桁（16 進数で）以上ゼロが続くハッシュ値を生むブロックヘッダになるまで，ナンスを変更しながらハッシュ計算を繰り返さなければならない。

[18]具体的には，ブロックが 2016 個作成されるたびに以下の計算が行われ，ターゲット値が変更される。

$$新しいターゲット値 = 現在のターゲット値 \times \frac{2016\ ブロックの作成に要した時間（min）}{2016 \times 10\ \mathrm{min}}$$

平均 10 分間隔で 2016 ブロックを作成するのに要する時間は計 20,160 分間（＝2 週間）である。これよりも短期間で 2016 ブロックが作成された場合はターゲット値を下げて難易度を上げ，これよりも長期間かかった場合はターゲット値を上げて難易度を下げる。このようにして約 2 週間毎に難易度が自動調整される。

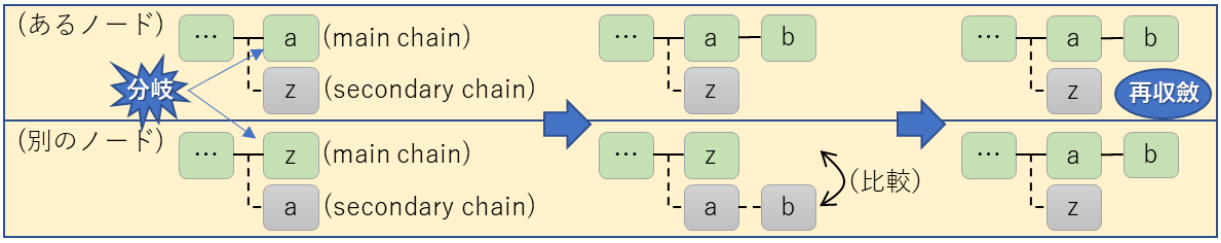
[19] データ構造は正しいか，ブロックヘッダのハッシュ値がターゲット以下か，含まれる各トランザクションがトランザクション検証時の検証項目を満たすか，等。詳細は [13]などを参照。

1.3.5　ブロックチェーンの分岐・再収斂

ブロックチェーンは原則，親ブロック 1 つに子ブロック 1 つが繋がって直線的に延びてゆくが，複数のマイナー（1.3.3 参照）がほぼ同時にブロック作成を成功させたときなど，1 つの親ブロックに対して複数種類の子ブロックが生じることがある。これを分岐（fork）という。ビットコインの場合，分岐が発生したときは最も長い[20]鎖を正当な記録とみなすルールがある。

具体的には，ノード A がブロック a を，ノード Z がブロック z を同時に生成した場合，

1. A・Z 以外の各ノードは，それぞれ先に届いたブロックを検証の上，自ノードのチェーンに追加（承認）する。その結果，ブロックチェーンネットワーク内には最新ブロックが a であるノードと，z であるノードとが一時的に混在する状態になる（分岐）。なお，遅れて届いたもう一方のブロックは，後でそちらが正式なブロックとなる可能性もあるため，「セカンダリーチェーン」（secondary chain）と呼ばれる扱いで各ノードが保持しておく。
2. 次に，誰かがブロック a の後続ブロックである b を新たに作成・送信したとする。b のブロックヘッダには直前のブロックである a のハッシュ値が明記されており（1.3.3 参照），a の後ろにしか繋ぐことが許されない。
3. 最新ブロックが a であるノードが b を受け取った場合，b を a の後ろに繋げる。
4. 最新ブロックが z であるノードが b を受け取った場合，セカンダリーチェーンとして保持されている a の後ろに b を繋げた上で a+b と z の「長さ」を比較し，最も長い a+b を承認し，承認済みであったブロック z をセカンダリーチェーンに変更する。このように一旦行った承認を取り下げて分岐を解消することをブロックチェーンの再収斂（reconvergence）と呼ぶ。



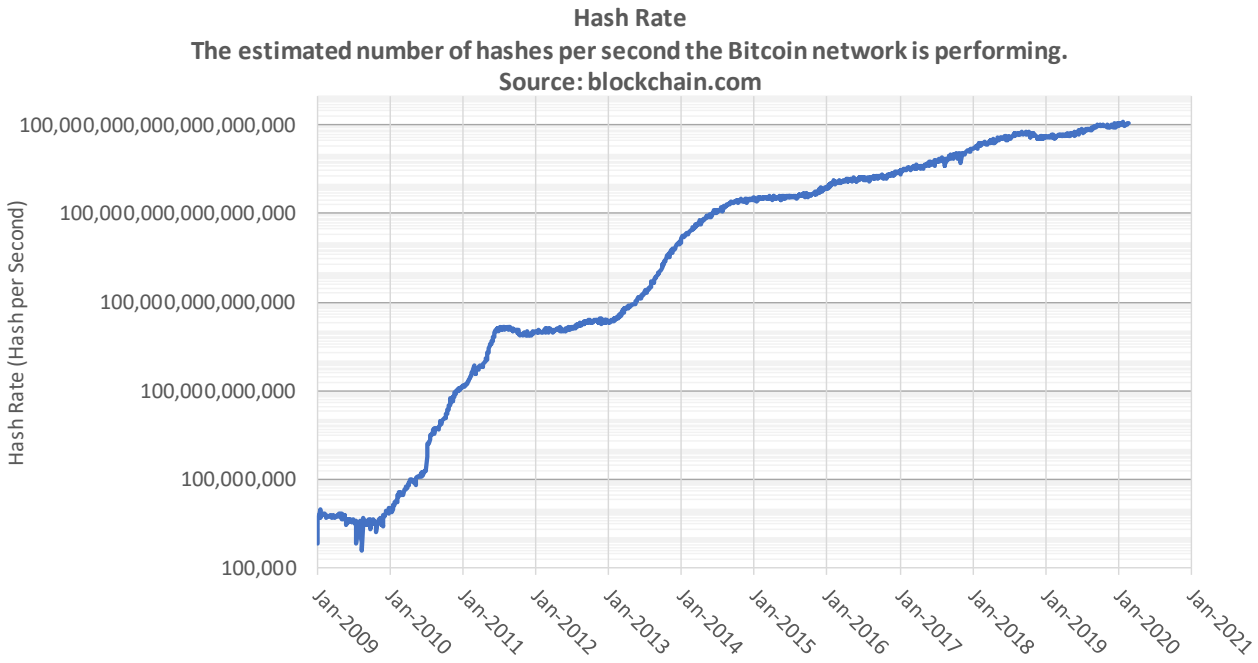
分岐が生じるタイプのブロックチェーンでは，このように一旦行われた承認が後から取り下げられることがあるため，すぐにはデータが確定しないという課題がある（1.7.1 参照）。また，圧倒的な計算力を持つノードが現れ，メインチェーンが伸びる速度よりも速くセカンダリーチェーンを伸ばし続けた場合，後から記録を引っ繰り返すことが可能となる。これは「51%攻撃」（1.7.6 参照）と呼ばれる。

[20] 厳密には「最も累積難易度（cumulative difficulty）が大きい」である。難易度（difficulty）はナンスを発見する難しさを意味し，ターゲット値が低いほど高くなる。各ブロックを生成するのに，それぞれどれだけの計算量がつぎ込まれたかを示す指標となる。

Column 1: ブロックチェーンの耐改竄性を支えているもの

「ブロックチェーンはハッシュの連鎖構造になっているので改竄困難である」という説明を見かけることがある。しかし，単にハッシュ値の入れ子になっているだけならば，マイニングに用いるようなコンピュータ（個人で購入可能な価格帯のモデルでもテラハッシュ毎秒の計算速度である）を使えばブロックチェーン全体のハッシュ再計算など一瞬で終わってしまう。ビットコインをはじめとする自由参加型ブロックチェーン（1.5.1 参照）が持つ絶対的ともいえる耐改竄性は，単にハッシュ値の入れ子構造をしているからではなく，ナンス探しというハードルが設けられていて，全世界のマイナー（1.3.3 参照）が血眼になってマイニングしていることではじめて実現している。

例えばビットコインにおいて全世界のマイナーが行っているハッシュ計算数の総計は毎秒 1 垓回（10^{20} 回）を超えるが [94]，これだけの計算量を投入しても，ナンス探しは平均 10 分間に 1 回，世界で誰か 1 人がようやく成功する難易度に常に調整され続けている。



（参照文献 [94]のデータを基に本タスクフォースにて描画）

改竄を行う場合，改竄ブロックから最新のブロックまでのナンスを全て独力で計算し直さなければならない（1.3.3 参照）。しかも，チェーンは今この瞬間も全世界のマイナーが延ばし続けており，これに追いつき追い越さねばならない。そのため，マイニングが活発に行われている限りにおいて，そのブロックチェーンは改竄が困難となる。加えて，攻撃者がそれだけの計算力を有しているならば，それをマイニングに使ってビットコインを獲得する方が合理的な判断となる。

もしビットコインの価格が下落して人気が落ち，マイナーが減り，ハッシュレートが下がれば，ナンス探しの難易度も自動的に引き下げられ，51%攻撃（1.7.6 参照）の標的となる可能性がある。現に，ビットコイン以外のマイニングハッシュレートが低い暗号資産では 51%攻撃が起きている。ブロックチェーンはけっして改竄「不可能」ではない。

1.4　合意形成アルゴリズム

中央集権型のシステムにおいては，決定権は全て管理者にゆだねられている。一方で，分散型のシステムの決定権は参加ノードの結論にゆだねられており，全ノードが一つの結論に収束することが必要となる。ネットワークにおいて情報伝達のタイムラグや未到達といった事態を避けられない中，全ノードが 1 つの結論に収束していく仕組みを合意形成アルゴリズムと呼ぶ [14]。

Nguyen ら [15]は，合意形成アルゴリズムを「証明に基づく合意形成アルゴリズム」と「投票に基づく合意形成アルゴリズム」に分類しており，本報告書でもこの分類を採用した。
「証明に基づく合意形成アルゴリズム」は，他のノードよりも自分が「適格」であることを証明してブロックをチェーンに追加する形式であり，多数のノードを有するネットワークのアルゴリズムに適しているとされる。また，「投票に基づく合意形成アルゴリズム」は，投票による多数決でブロックをチェーンに追加する形式であり，ノード数が限定される少数のネットワークのアルゴリズムに適しているとされる。ブロックチェーンで採用可能なアルゴリズムは，ブロックチェーンの分類（「1.5 ブロックチェーンの分類」を参照）に影響されず，「証明に基づく合意形成アルゴリズム」は自由参加型（Permissionless 型）のみならず許可型（Permissioned 型）のブロックチェーンでも採用が可能であり，その逆に「投票に基づく合意形成アルゴリズム」も自由参加型（Permissionless 型）で採用することが可能である。

また，Wang ら [16]によると，PBFT などの「投票に基づく合意形成アルゴリズム」はネットワークに参加するノードの数を犠牲にして即時的なファイナリティと高いトランザクション処理能力を提供するとされ，PoW などの「証明に基づく合意形成アルゴリズム」はネットワークのノード数を制限しない代わりに確率的なファイナリティしか得られないと述べている。

1.4.1　証明に基づく合意形成アルゴリズム

証明に基づく合意形成アルゴリズムの基本概念は，ネットワークに参加する多くのノードの中で，十分な証明を提示したノードがチェーンに新しいブロックを追加する権利と，報酬を受け取る権利を得るものである [15]。

1.4.1.1　プルーフ・オブ・ワーク（Proof of Work: PoW）

PoW は，設定された課題に対して各ノードが取り組み，最初に正しい解を得たノードが新しいブロックを既存のチェーンに追加できる仕組みである。
ビットコインで採用されている PoW を例にとると，マークルルートやタイムスタンプ，1 つ前のブロックのブロックヘッダのハッシュ値と共に，ナンスと呼ばれる数字がブロックの作成に必要となる。
ナンスを加えて作成されたブロックヘッダのハッシュ値が決められたターゲットの値以下であれば，ブロックを追加する権利とビットコインの報酬が得られる仕組みとなっている（「1.3.3 ブロックの作成（マイニング）」を参照）。
「1.2.1 暗号学的ハッシュ関数」で述べたように，暗号学的ハッシュ関数を用いて導出されたハッシュ値から元のメッセージを推測することは困難であり，そのためにナンスを入れ替えて繰返しハッシュ値

を計算する。このように，正しい解を得るために繰返し計算作業を行うため，PoW と呼ばれている [15]。

1.4.1.2 プルーフ・オブ・ステーク（Proof of Stake: PoS）

PoS は，そのブロックチェーンに対する利害関係に応じてブロックを追加する権利が得やすくなる仕組みであり，ブロックチェーンで保証される資産が多ければ多いほど，そのブロックチェーンの信頼度を下げる行動はとらないであろうという考えに基づいている。PoW と組み合わせて使用されることもあり，ターゲットの難易度が全ノードで同一な PoW に対して，PoS ではノードの資産に応じた難易度を設定することが可能であり，これによって無駄な電力消費も抑えることが可能となる。
また，PoS において後述の 51%攻撃（「1.7.6 51%攻撃」を参照）を仕掛けるには全体の 51%の資産を所有する必要があり，攻撃によって保有する資産価値が低下するため，PoW よりも 51%攻撃を受けにくいとされる [15]。

PoS は一部の資産保有者がブロックを作成しやすい状況となるため，PoW よりも中央集権的だとの指摘もあるが，PoS を採用している NXT コインによれば，上位 5 つの資産保有者で全体の 42%のブロックが作成される程度であり，権限の集中度合いは高くないとしている [17]。

このほかにも類似するアルゴリズムとして，自身の保有する利害関係の量を他の誰かに委任するデリゲーティド・プルーフ・オブ・ステーク（Delegated Proof of Stake: DPoS）[18]や，資産だけではなく，他のノードとの取引量を勘案したアルゴリズムでノードの重要性を評価し，その重要度に応じてブロックの作成権利が得やすくなる仕組みであるプルーフ・オブ・インポータンス（Proof of Importance: PoI）[19]と呼ばれるアルゴリズムが使用されているブロックチェーンがある。

1.4.2 投票に基づく合意形成アルゴリズム

投票に基づく合意形成アルゴリズムでは，ブロックチェーンネットワーク内でブロックを作成・検証するノードを限定し，それらのノード内で投票を行うことでトランザクションやブロックを承認するか否かを決定する。このとき，事前に決められた閾値を超えるノードが採用と判断することで，ネットワークとしてトランザクションやブロックが承認される。
この閾値は，分散型台帳にどのような耐障害性を持たせるかで異なり，代表的な耐障害性としてクラッシュ・フォールト・トレランス（Crash Fault Tolerance: CFT）とビザンチン・フォールト・トレランス（Byzantine Fault Tolerance: BFT）[21] がある [15]。一般的に，フォールト・トレランスとはシステムの一部に障害が発生した場合でも全体として正常にシステム運用できる機能や状態のことを指し，ブロックチェーンにおいては一部のノードが正常に機能しない状態でもブロックチェーンのネットワークを正常に運用可能な仕組みが，その一つである。

---

[21] 「1.4.1 証明に基づく合意形成アルゴリズム」で紹介した PoW や PoS も，応答しないノードや悪意のあるノードの中で合意形成を行える仕組みであり，BFT アルゴリズムと考えることができる。

ブロックチェーンにおいてブロックを作成・検証するノードを限定する場合，誰をどのように選出するかという課題が残るが，その解決策として，プラットフォーム上での自分の身元を，公的文書などで明示し，合意形成に一貫して貢献可能な能力を示すプルーフ・オブ・オーソリティ（Proof of Authority: PoA）[20]や，自身の保有する利害関係の量を委任する DPoS を応用して選出する方法 [21]などが実際に運用されている。このような手法に基づいて選出されたノードが複数存在する場合，選出されたノード内でどのような合意形成手法を採用するかはブロックチェーンの設計次第であり，1.4 章の冒頭で述べたように証明に基づく合意も投票に基づく合意も採用可能である。一般的に，検証ノードを選出する理由はブロックチェーンの処理能力を高めることを目的に行われることが多いため，即時的なファイナリティを得られる投票に基づく合意が採用されることが多い。

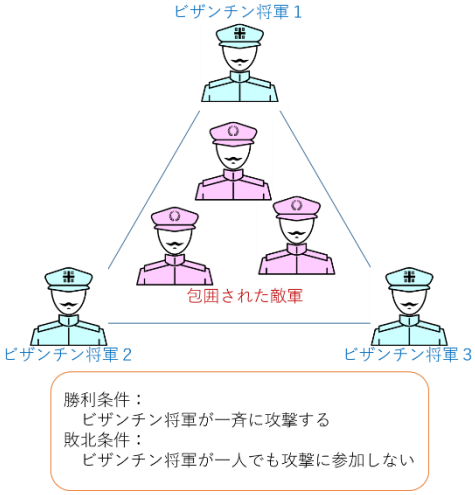
1.4.2.1 クラッシュ・フォールト・トレランス（Crash Fault Tolerance: CFT）

CFT は，一部のノードが応答しない状況下でもネットワークが正常な処理を続行可能な耐障害性である。全体のノード数を 2f+1 とするとき，障害ノード数は f まで許容可能であり，f+1 のノードから応答が得られた場合にネットワーク内で合意されたとみなされる。ただし，応答するノードは全て正しく応答をしていることが前提とされているため，ノードが誤った応答を返す可能性を考慮する必要がある場合は，BFT を採用する必要がある [15]。

1.4.2.2 ビザンチン・フォールト・トレランス（Byzantine Fault Tolerance: BFT）

BFT は，一部のノードが応答しない，又は故意や過失を問わずに誤った応答が発生する状況下でも，ネットワークが正常な処理を続行可能な耐障害性である。BFT では全体のノード数を 3f+1 とするとき，障害ノード数は f まで許容可能であり，2f+1 のノードから同一の応答が得られた場合にネットワーク内で合意されたとみなされる [15]。特に有名なのはプラクティカル・ビザンチン・フォールト・トレランス（Practical Byzantine Fault Tolerance: PBFT）というアルゴリズムで，IBM 社の Hyperledger Fabric（v0.6）で使用されていた [15]。

Column 2: ビザンチン将軍問題

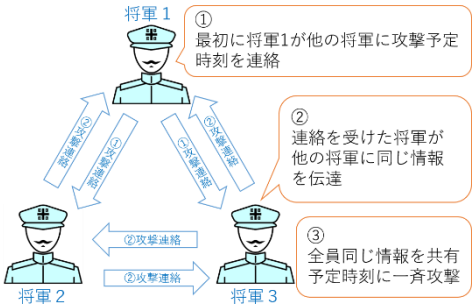


いま，ビザンチン帝国の将軍達は，敵軍を包囲した状態にある。全軍で一斉に攻撃すれば勝つことができるが，誤った情報が伝わって全軍の合意形成に失敗して一部の将軍だけ攻撃すると敗北してしまう。将軍たちの間で伝令を飛ばすことができるが，帝国に反逆する将軍がいて，一部の伝令は正しく伝わらない可能性がある。このような状況の中で，全軍の合意形成ができる手法や条件とは何か，という問題である。

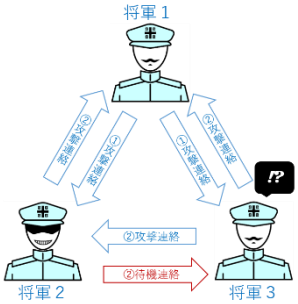
将軍が 3 人のとき：

全ての伝令が正しく伝われば問題なく合意形成が行われる[A]が，いずれか 1 人の将軍が裏切り，誤った情報を伝えると合意形成が失敗してしまう[B]，[C]。

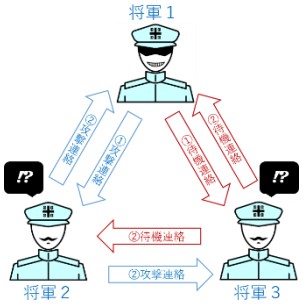
[A] 全員が正しい情報を伝達



[B] 将軍 2 から将軍 3 に誤情報を伝達



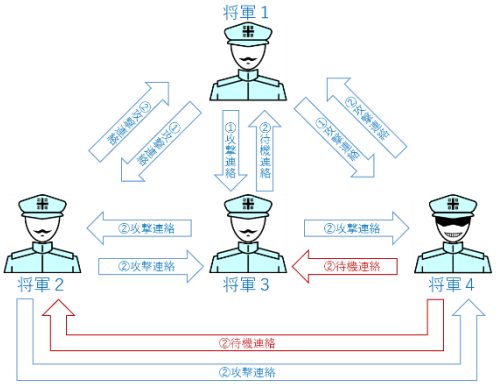
[C] 将軍 1 が異なる情報を伝達



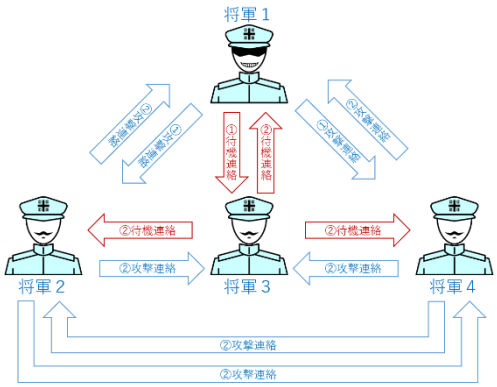
将軍が 4 人のとき：

一部で誤った情報が伝達されても，不正な情報を伝えている将軍が一人だけである限り，正しい情報が不正な情報よりも多く到達し，正しい合意が達成される。

[D] 将軍 4 が将軍 2 と将軍 3 へ誤った情報を伝達



[E] 将軍 1 が異なる情報を伝達



このように，「分散システム上で誤った情報が伝達される可能性がある場合，システム全体として正しく合意を形成することが可能か」という問題について，情報を伝達するノードをビザンチン帝国の将軍に置き換えて紹介されたのがビザンチン将軍問題であり，不正なふるまいを起こすノード数を N としたとき，正しく稼働するノードが 2N+1 以上存在する場合に正しい合意が達成可能となる [22]。

1.5　ブロックチェーンの分類

ブロックチェーンには様々な種類があり，それぞれ前提，アプローチ，メリット，限界等が全く異なる。ブロックチェーンをビジネスに利用する際には，それぞれの違いを正しく理解するとともに，自分が必要としているのはブロックチェーンのどのような側面なのかを明確にしておく必要がある。以下，最も一般的な分類方法であるアクセス権に基づく分類について延べる。

インターネットにアクセスできる者ならば誰でも自由にトランザクションを閲覧・作成できるタイプを公開（Public）型，それらを制限しているものを非公開（Private）型と呼ぶ [11] [23] [24]。非公開型の中でも複数の企業がコンソーシアムを形成し，加入者だけが使えるものは特にコンソーシアム（Consortium）型と呼ばれる。
また，権限を持つ者のみがトランザクションの承認（≒ブロック作成）を行えるものは許可（Permissioned）型，誰でも承認者になれるものは自由参加（Permissionless）型[22] と呼ばれる [23] 。

これらの分類を表にまとめると，概ね以下のようになる[23]。あわせて各タイプの例を挙げる。

<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="3">トランザクション承認</th></tr>
<tr><th>誰でも可能（自由参加型）</th><th colspan="2">権限が必要（許可型）</th></tr>
<tr><td rowspan="2">トランザクション閲覧・作成</td><td>誰でも可能</td><td><u>公開型</u>
• ビットコイン
• イーサリアム</td><td colspan="2"><u>公開-許可型</u>
• Sovrin (Hyperledger Indy)</td></tr>
<tr><td>制限</td><td></td><td><u>非公開型</u>
• mijin
• miyabi</td><td><u>コンソーシアム型</u>
• Hyperledger Fabric
• Hyperledger Iroha
• Corda
• Quorum</td></tr>
</table>

以下，各タイプの特徴を述べる。

1.5.1　自由参加型（Permissionless 型）

1.5.1.1　公開型（Public 型）

公開型は，誰でも中身を閲覧でき，誰でもトランザクションの承認者となれるタイプである。非中央集権性，透明性，耐改竄性など，一般にブロックチェーンの特徴として知られる性質が最も顕著に表れるタイプである。

公開型は以下のような特徴をもつ。

---

[22] “Unpermissioned 型” と呼ばれることもある。

[23] Public/Private/Permissionless/Permissioned の定義及びその和訳は，人によって異なる場合がある。

1. 非中央集権性
   公開型は完全非中央集権型であり，いかなる者も，団体も，国家も，その運営を止めたり，特定のノードの参加を制限したり，ルール（プロトコル）を強制的に変更する権限を持たない。

2. 透明性
   公開型ブロックチェーンに記録されたデータは，インターネットに接続できさえすれば，いつでも誰でも確認することができる[24]。

3. インセンティブが必要
   公開型は参加ノードが自主的にトランザクションの承認を行うため，インセンティブがなければ誰もトランザクションを承認せず，ブロックチェーンが機能しない。そこで承認者への報酬として暗号資産（ビットコイン，イーサなど）を用いている。

4. 耐改竄性が極めて高い
   特にビットコインのようなメジャーな公開型ブロックチェーンでは，上記インセンティブに惹かれた多数の者が膨大な計算力を持ち込んでブロック作成を競い合っている。このような状況下では，過去のトランザクションの改竄はほぼ不可能となる。公開型の耐改竄性は，このインセンティブによって支えられている側面がある（Column 1 参照）。

これらをまとめると，（少なくとも，メジャーな）公開型ブロックチェーンは以下の特徴を持つ。

- 一旦確定（1.7.1 参照）した記録を後から誰かが（単独で）改竄・消去することはほぼ不可能。
- ブロックチェーン上に記録されたデータはいつでも誰でも確認・検証できる。管理者不在で自律的に動き続けるため，運営主体の消滅等に伴って将来的に閲覧できなくなるリスクもない。

言い換えると「その内容も，その存在も，誰にも否定できないように記録を保存・維持でき，その確かさを誰でも確認できる」[1]。これは従来のシステムでは得られなかった特徴である。

その反面，公開型の「管理者がいない」「悪意あるノードが承認者になる可能性がある」等の前提は「システム変更が困難」「ファイナリティがない」「トランザクション処理速度が低い」「膨大な電力消費」「全てが利用者の自己責任」等の課題にも繋がっている（「1.7. ブロックチェーンの課題」参照）。

---

[24] 例えばビットコインの中身は chainFlyer（https://chainflyer.bitflyer.jp/）等のサイトで確認できる。“0” を検索すると最初のブロック（ジェネシスブロック）を検索でき，そこに含まれるトランザクションを開くと “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”（2009/1/3 Times 紙 “財務大臣，2 度目の銀行救済の瀬戸際” ）という Satoshi Nakamoto が刻んだ有名なメッセージをいつでも誰でも読むことができる。

1.5.2　許可型（Permissioned 型）

1.5.2.1　非公開型（Private 型）

企業が業務にブロックチェーンを導入しようとするとき，前項の最後に述べた公開型の課題が足枷となるケースが出てくる。加えて，記録したいデータに社外秘の情報が含まれる場合，公開型は利用しにくい。そのような場合に使われるのが非公開型である。

非公開型には以下の特徴がある。

1. 中央集権性
   非公開型には管理者がおり，ルールの変更や，ノードに与える権限の制御が公開型よりも容易である。そのため，より柔軟な運用が可能となり，よりビジネスで利用しやすい。
   また，素性の明らかな者のみがトランザクションを承認するため，公開型のように「悪意ある承認者が行った不正な承認を検知・是正する」という仕組みを置く必要がない。よって，PoW（1.4.1.1 参照）のような膨大な計算量を要求する合意形成アルゴリズムを使わなくともよいため公開型よりも承認の確定（1.7.1 参照）が早く，単位時間あたりのトランザクション処理数を高くすることができる。その反面，承認ノードがダウンするとトランザクションの承認が止まるなど，システムの可用性は公開型ほど高くない。加えて，管理者の判断でブロックチェーンの運用を打ち切ることもできるため，公開型のような記録の永続性[25]は期待できない。

2. 機密性
   非公開型は第三者のアクセスを遮断できるので社外秘の情報もブロックチェーンに載せることができる。その反面，公開型のような「いつでも誰でも記録の内容や存在を確認・検証できる」という透明性はない。

3. インセンティブ不要
   非公開型ではトランザクションの承認を組織内の人物が行うことができるため，承認者へのインセンティブ（トランザクション手数料等）なしでもブロックチェーンを運用できる。

4. 耐改竄性
   非公開型では素性の明らかなノードがトランザクションを承認するため，51%攻撃（1.7.6 参照）等，悪意あるノードから記録を書き換えるような攻撃を受ける可能性は低い。また，非公開型もトランザクションがハッシュ値で結ばれた連鎖構造をしており，データ構造上，改竄の検出は容易である。しかし，公開型のような絶対的な耐改竄性とは異なり，当該企業が組織ぐるみで意図的に行う改竄まで防げるわけではない。

[25] ただし公開型も暗号技術の危殆化など，永続性に対するリスクはゼロではない。

1.5.2.2 コンソーシアム型（Consortium 型）

複数の企業・団体がコンソーシアムを形成し，その加入者が利用するタイプがコンソーシアム型である。特徴は非公開型とほぼ同じであるが，一部，コンソーシアム型に特有の特徴もある。

- 非公開型は管理者やトランザクション承認者が 1 つの企業・団体内に限定されるのに対して，コンソーシアム型ではこれらが複数の企業・団体にまたがるため，非公開型よりも相互監視が働きやすく，より不正が困難となることが期待できる。

- 複数の企業で運営することから，「インフラ・ガバナンスの共有」（1.7.13 参照）という，コンソーシアム型に特有の課題が生ずる。

1.5.2.3 公開-許可型（Public-Permissioned 型）

公開-許可型は，トランザクションの閲覧・作成は誰でもできるが，承認は権限を与えられた者しか実施できないタイプである [11] [25] [26]。基本的な特徴は非公開型やコンソーシアム型と共通であるが，ブロックチェーンに記録されたデータをいつでも誰でも利用できる点に特色がある。

例えば DID（1.8.5 参照）を提示された相手がその ID の真正性を検証するケースのように，ブロックチェーンのデータをいつでも誰でも閲覧できることが重要だが，トランザクション承認は身元の明らかな信頼できる者に行わせたいという用途に適しており，DID に利用される Sovrin (Hyperledger Indy) などで採用されている [25]。

1.6　ブロックチェーンのメリット

ブロックチェーンの種類によってメリットは多少異なるが，この項ではブロックチェーンの一般的なメリットを紹介する。

1.6.1　分散管理

従来の一般的なシステムは中央管理型であり，信頼できる中央管理のシステムや組織が必要である。一方，ブロックチェーンではネットワーク上の合意に基づきデータの検証が行われるため，そのような信頼できる中央管理が不要となる。このため，中央管理が不在の下，運用が可能となる。例えば，ビットコインをはじめとする暗号資産の取引の場合，銀行のような第三者機関が存在しなくとも通貨として機能が成り立っている。

また，スマートコントラクト（1.8.1 参照）の機能との組み合わせにより，様々な分野での取引をブロックチェーンで自動運用することができ，仲介者や管理組織が不在の下，取引が可能となることが期待され，仲介手数料削減によるコストカットも期待できる。

1.6.2　耐障害性

耐障害性の事例として先に挙げたフォールト・トレランスとゼロ・ダウンタイム（Zero Downtime）などが知られている。ゼロ・ダウンタイムとは，常時使用できることが期待される機器やシステム，回線，サービスなどが停止・中断している時間がなくストレスなく利用できる状態を意味する。ブロックチェーン上で管理されているデータは複数のノードで共有されており，この複数のノードのうち 1 部のノードがダウンした場合でも，他のノードが機能していればブロックチェーンの仕組みは動き続ける。この為，従来の仕組みと比べて，ブロックチェーンはシステムダウンが起きにくい仕組みであるといえる [27]。

1.6.3　記録の透明性

ブロックチェーン上の記録は全て各ノードで共有され，ネットワーク参加者であれば誰でも確認，トレースすることができる。この特性を利用してサプライチェーンの管理等に応用が期待できる。

1.6.4　耐改竄性

ブロックチェーンのブロックは，連鎖するデータ構造となっており，一つ前のブロックの情報を要約しながら繋がり共有される。そのため，過去の記録を改竄しようとすると，それ以降連なっている全ての連鎖するブロックの内容の書き換えと合意形成の処理（例えば PoW の場合はナンスを見つける処理）を行わなければならないため，データの改竄が非常に困難といえる。また，従来の仕組みでは管理者がシステムに変更を加えることができるが，ブロックチェーンでは管理者不在の分散管理で成り立っている仕組みなので，特定のユーザが変更を加えることができない仕組みとなっている。

さらに，耐改竄性の応用として，文書等のデータからハッシュ値を計算してブロックチェーンに記録しておき，後でハッシュ値を再度計算して比較することで，元のデータに変更が加えられたかどうかを確認できる仕組も可能となる [28]。

1.6.5 効率化

特定の場面でブロックチェーンを導入したときに，プロセスの効率化が期待できる場合がある。以下，効率化が期待できる例を紹介する。

- システム運用コスト削減
  例えば銀行などの金融機関は，取引や顧客に関する膨大なデータを維持する必要がある。そのために大規模な集中管理センターを保有して，セキュリティやバックアップに巨額の費用をかけている。これに対してブロックチェーンネットワークを利用して管理することにより運用コストが削減される可能性がある [29]。

- スマートコントラクト（1.8.1 参照）による効率化
  事前にプログラム化した前提条件に基づく取引が可能となるので，これまで書面等で事前合意必要だったやり取りが省略化され，自動取引が可能となる。

- 取引管理の効率化
  複数のプラットフォームが存在し，それらの取引を管理する場合，既存のシステムを用いて構築するよりも，ブロックチェーンで管理した方が効率的である可能性がある。例えば，複数のプラットフォームにまたがって情報が保存されている場合，ブロックチェーンを利用すれば，プラットフォーム間の直接のやり取りがブロックチェーン上で管理され，既存のシステムで管理するよりも効率的であることが期待される。この特性を利用した製薬業界での取り組みとして，後の「2.2.2 臨床試験データの二次利用のプロセス管理」で事例を紹介している。

1.7　ブロックチェーンの課題

ブロックチェーンには従来の中央集権的システムではあまり見られないような特徴的な課題が幾つかある。ブロックチェーンの分類（1.5 参照）や，使用する合意形成アルゴリズム（1.4 参照）によっても課題は異なるが，代表的なものをまとめると概ね以下のようになる。

	自由参加型	許可型	
	公開型	コンソーシアム型	非公開型
即時性	✔		
システム変更の難しさ	✔		
スケーラビリティ問題	✔		
トランザクション処理速度	✔		
電力消費	✔（PoW）		
51%攻撃	✔（PoW）		
責任の所在	✔		
量子コンピュータ耐性	✔	✔	
秘密鍵の管理	✔	✔	✔
相互運用性	✔	✔	✔
オラクル問題	✔	✔	✔
個人情報保護	✔	✔	✔
機密データの運用	✔	✔	
競合会社間でのインフラ・ガバナンス共有		✔	

ブロックチェーンをビジネスで利用する際に課題を検討する場合は，自分が使おうとしているブロックチェーンがどのような種類なのかを念頭に置く必要がある。以下，各課題の内容を紹介する。

1.7.1　即時性

PoW など，チェーンの分岐（フォーク）が発生しうるタイプの合意形成アルゴリズムは，取引内容が覆る可能性を完全にゼロにすることができない（「ファイナリティが確保できない」という）[30]。そのため，トランザクションの確定にはチェーンがフォークしている可能性を考慮して，一般的に 6 段階の承認を待つことが安全だといわれている。承認とはトランザクションがブロックに取り込まれることを言い，トランザクションがブロックに取り込まれると 1 段階の承認，そのブロックの後ろにブロックが追加されると 2 段階の承認となる。6 段階の承認は，全体の 10%の計算力を持った攻撃者が，不正なブロックを追加してチェーンを覆す確率が 0.1%未満となる指標とされる [31]。

ビットコインにおいては，ブロックの追加速度が平均 10 分間隔となるように計算の難度が調整されており，承認を待っていると迅速な取引が実現できないことが課題とされている [32]。

即時性が求められる場合は，トランザクションの送信（「1.3 ブロックチェーンの動作メカニズム」参照）時点でトランザクションが確定したとみなす「ゼロ・コンファメーション」と呼ばれる運用を取ることがある。この場合，後で当該トランザクションが無効となって損害を被るリスクを排除できないが，そのリスクを取引の手数料等に反映させたり，損害が出た時のために保険に加入するなどの方法で対処することが可能である [14]。

1.7.2　システム変更の難しさ

ブロックチェーンはシステムの変更が難しいという課題がある。特に，管理者が不在である自由参加型のブロックチェーンでは，全てのノードが新ルールに切り替えてくれる保証が得られない状態で，システムの変更に挑むこととなる。

システムを変更するには，ソフトフォークとハードフォークの 2 つの手法がある。ソフトフォークは，旧ルールから徐々に新ルールに移行させ，ルールが混在した状態から最終的に新ルールへの収斂を目指す手法であるが，新ルールに合意するノードが少なければ最終的に旧ルールに収斂し，システムの変更は失敗となる。ハードフォークは，新ルールに合意したノードから別のネットワークに移行し，独立したネットワークで新ルールの運用を目指す手法であり，少数であっても新ルールに合意したメンバーのみでネットワークの運用が可能な手法である [32]。ただし，ハードフォークでは新ルールと旧ルールに互換性を持たせることが出来ないため，システム変更を行う方法は慎重に検討する必要がある。

1.7.3　スケーラビリティ問題

ビットコインでは 1 MB のブロックが平均 10 分間おきに作成される。しかしながらユーザの増加に伴って取引が増え，10 分間に 1 MB を超えるトランザクションデータが発生し，ブロックに含まれなかったトランザクションに承認の遅延が発生した。この課題は一般にスケーラビリティ問題と呼ばれており，ビットコインのブロックサイズを 8 MB に拡張することで課題の解決を目指したブロックチェーンが，ビットコインからハードフォークしたビットコインキャッシュである。

1.7.4　トランザクションの処理速度

「1.5 ブロックチェーンの分類」で述べたように許可型のブロックチェーンではトランザクションの承認も非常に早く行うことができるが，自由参加型のブロックチェーンでは正当なトランザクションに対する合意形成に時間がかかる。一般に広く認知されている暗号資産のほとんどは自由参加型であり，ビットコインを例にとると，ブロックサイズが 1 MB に制限されているため，1 秒間に最大 7 つのトランザクションしか処理できない [33]。そのため，トランザクションの発生速度がこれを超えると，処理しきれないトランザクションが発生してくる。対照的に，ブロックチェーンを使用しない例として，世界的な決済手段であるクレジットカードの VISA は，1 秒間に 65,000 件のトランザクションまで処理できるといわれている [34]。

1.7.5　電力消費

ビットコインをはじめとする PoW を採用しているブロックチェーンでは，マイナー（1.3.3 参照）がブロック追加の報酬を得るべく計算競争を繰り広げている。しかしながら，マイニングのための計算は今のところ何の役にも立たず，チェーンにブロックを追加する権利とその報酬のために，無意味な計算によって過剰に電力が消費されていることが課題である [32]。

ケンブリッジ大学によれば，全世界の消費電力のおよそ 0.4%がビットコインのマイニングに使用されており，ベルギーやフィンランドの年間電力消費量を上回ると予測している [35]（2020 年 4 月時点）。

1.7.6　51%攻撃

PoW では，システム全体の計算リソースの過半数が不正をしないノードによって所有されている限り，不正をしないノードによってブロックが追加され，他の競合しているチェーンよりも早いペースで成長し，正当なチェーンとしてネットワークに伝播されるはずである（1.3.5 参照）。しかし，攻撃者が所有する計算能力が，不正をしないノードの所有する計算能力を超えたとき，攻撃者が伸ばした不正なトランザクションを含むチェーンを伸ばしていき，正当なチェーンとしてネットワーク全体に伝播する可能性が高まる。マイニング（1.3.3 参照）には運の要素も絡むため，過半数の計算能力を確保すれば必ず不正がまかり通るわけではないが，どのようなブロックチェーンでも正しく運用するために最低限必要な不正をしないノードの数を定義し，攻撃者に対抗できるようにする必要がある [11] [32]。
2018 年には，ビットコインゴールド，Verge，モナコインなどが実際に 51%攻撃を受け，不正送金の被害を被っている [36]。

1.7.7　責任の所在

中央で取引の仲介をしていたヒトや組織がブロックチェーンに置き換わって居なくなり，ネットワーク上に存在する端末同士が直接取引を行う世界になった場合，そこで発生した損害は誰に責任があり，誰が補償するのか不明確である。これは，ブロックチェーンが非中央集権の為，従来中央が担っていた問題解決機能等を担う先が不明であることにより生じてしまう。
許可型であれば管理主体が明確であるが，自由参加型のブロックチェーン上で提供されるサービスは，発行や販売に対する責任の所在が曖昧である場合が多い。利用者に損害が発生しても，管理主体がいないため泣き寝入りするしかない等という「責任の所在が不明確である」という課題がある。
参加者間の責任分界や問題解決方法のルール化といった面について，それぞれの関連法令に基づいて検討が必要である。

1.7.8　量子コンピュータ耐性

ブロックチェーンの要素技術として暗号化技術を用いたデジタル署名（1.2.2.2 参照）が使用されている。現在広く使われている暗号化技術である RSA 暗号や楕円曲線暗号は，それぞれ素因数分解問題と楕円曲線離散対数問題と呼ばれる現実的な時間で解くことが難しいとされる数学的問題を利用しているが，量子コンピュータの実現により，これらの問題が現実的な時間内で容易に解けるようになるといわれている。そのため，量子コンピュータを用いた攻撃手法に対しても安全な公開鍵暗号（耐量子計算機暗号）への移行が対策として検討されている [37]。

1.7.9　秘密鍵の管理

ブロックチェーンに対する攻撃の一つに，秘密鍵（「1.2.2 鍵暗号技術」を参照）を盗み取ることが挙げられる。ブロックチェーン上の特定の記録が確かに自分のものであると証明する手段は「自分が秘密鍵を持っている」というただ 1 点以外になく，ビットコインを使用（他のビットコインアドレスに移転）するときも，DID（1.8.5 参照）の所有者が自分だと証明するときも，秘密鍵が必要になる。そのため，秘密鍵を他人が知ってしまうと本人になりすまして不正を行うことが可能になり，秘密鍵を紛失してしまうとブロックチェーン上の記録が自分のものであると証明できる人がいなくなる。

実際に，暗号資産の流出事件のほとんどは秘密鍵を管理する「取引所」からハッキングによって流出した秘密鍵が第三者に不正利用されることで起きたとされている[26]。また，秘密鍵の紛失によって数十億円～数百億円規模の暗号資産が誰にも動かせなくなってしまった事件も度々報道されている[27]。
秘密鍵の管理もブロックチェーンを利用する際に考慮すべき点となる。

1.7.10 相互運用性（インターオペラビリティ）

ビットコインやイーサリアムなど，ブロックチェーンには複数の種類があり，それぞれ互換性がない状態となっている。例えば，ビットコイン（BTC）はイーサリアムのブロックチェーン上では扱えず，反対にイーサリアム（ETH）はビットコインのブロックチェーン上では扱うことができない。これでは不都合が大きいため，異なるブロックチェーン同士を繋ぐことができるようにする仕組みが開発されている（「1.8.4 クロスチェーン」参照）。

1.7.11 オラクル問題

ブロックチェーンにおける「オラクル」とは，ブロックチェーンにブロックチェーン外のデータを取り込む仕組みを指す [38]。スマートコントラクト（1.8.1 参照）をビジネスで利用する場合，ブロックチェーン外のデータに基づいてプログラムを実行[28]させたいケースが多いため，不可欠な機能になる。
オラクルには大きく分けて 2 種類ある。

	単一型オラクル（Single oracle 又は Centralized oracle）	**分散型オラクル（Decentralized oracle）**
データ取得方法	信頼できる第三者機関（TTP: Trusted Third Party）を単一の情報源としてデータを取得	複数の情報源からデータを取得し，情報の妥当性について合意形成を行う
特徴	非常にシンプルな作りであり，運用の利便性が高い	TTP が存在しない分野でも利用できる
課題	TTP が存在しない分野では利用できない	• 取得したデータの検証・合意形成に手間がかかる • 検証が正しく行われるためのインセンティブ設計が非常に難しい
実装・利用状況	オラクルの実装例のほとんどが単一型	事例はまだごく少数

（参考文献 [38]などに基づき作成）

[26] CoinCheck 社 NEM 流出事件，MtGox 事件等。

[27] QuadrigaCX 事件，アイルランド麻薬密売人事件等。

[28] 例えば，保険会社である AXA 社がかつて試験的に提供していた保険「fizzy」では，飛行機が 2 時間以上遅延した場合に自動的に保険金が支払われるスマートコントラクトを組んでいた [101]。この場合，飛行機の運行情報データをブロックチェーン外から取り込む必要がある。

単一型オラクルでは，そのオラクルがブロックチェーンに持ち込むデータが正しいことを信頼しなければならない。一方，分散型オラクルでは複数のデータソースを使うので，どれが正しいかを決めるために「合意形成」が必要となり，検証のためには人間の判断が必要になり，相当な手間がかかる（ブロックチェーン本体の合意形成のように，オンチェーンの情報だけで検証でき，マイニングマシンのプログラムを走らせておけば良いのではないため，相当な手間がかかる）。
第三者の信用へのコストを最小化するスマートコントラクトの執行を単一のオラクルに依存すると，結局，データが正確であるとのオラクルの信頼が必要になるが，本当に信頼できるソースかどうかの判断はとても難しい。ブロックチェーンのデータは改竄されず，スマートコントラクトによって契約が信頼できるものとなる一方で，オラクルによって取得される現実世界のデータの信頼性が大きな問題となってくる。また，単一のオラクルによってスマートコントラクトを実行させる場合，スマートコントラクトが長期にわたり実行されるものの場合，途中でデータの提供元が消滅してしまう可能性がある。トランザクションの作成から完了までに消滅する可能性は，スマートコントラクトが長期になればなるほど高まる。これが単一型オラクルを信用したときに生じるオラクル問題である。
単一のオラクルでは誤った情報取得やオラクル自体の消滅リスクがあるため，多くの情報源を用意することで解決しようとしており，どの解決策でもコストがかかってしまう信頼性とコストのトレードオフの関係になる。

1.7.12 個人情報や機密データの運用

個人情報は本人の求めに応じて削除する義務が日本の個人情報保護法や EU の GDPR（General Data Protection Regulations）に定められているが，ブロックチェーンに個人情報などを記録すると二度と削除できなくなってしまうだけでなく，たとえトランザクションを暗号化したとしてもネットワーク上の全てのノードに行き渡ってしまう。そのため，個人情報や機密データを取り扱う際には，ブロックチェーン単体ではなく，外部のデータベース等と組み合わせて使う（オフチェーン）等の工夫をする必要がある（「1.8.3.1 オフチェーン」参照）。

1.7.13 競合会社間でのインフラ・ガバナンス共有

複数の会社でブロックチェーンのプラットフォームを活用する場合，暗号化（「1.2.2.1 暗号と鍵」を参照）やゼロ知識証明（「1.8.2 ゼロ知識証明」を参照）の活用によって，ブロックチェーン上に秘匿したいデータを書き込みながらも，特定の相手に必要最低限の情報のみ公開する仕組みが構築可能とされる[39]。しかしながら，複数の会社間でデータを共有する仕組みを構築する場合，「どのようなメンバーでどのような商業モデルを組むか，インフラやシステムは誰が管理構築するのか」というインフラやガバナンスを共有し，管理・運用していくための合意を得ることは，Brexit や NAFTA（北米自由貿易協定）の交渉と同じくらい困難であるとの意見もある[40]。

1.8　ブロックチェーンに関連した技術

1.8.1　スマートコントラクト

ブロックチェーンにおけるスマートコントラクトとは，ブロックチェーン上にプログラムを組み込むことにより，プログラムの条件に基づいた取引を自動で行う機能を指す。イーサリアムと呼ばれるブロックチェーンで初めて実装された機能であり，現在ではビットコインのブロックチェーンにおいてもサイドチェーン（「1.8.3.2 サイドチェーン」を参照）を用いることにより実装可能である。他にもこの機能を有するブロックチェーンが多数存在しており，ブロックチェーンの代表的な応用技術の一つである。スマートコントラクト機能を有するブロックチェーンでは，通常のトランザクションと同様にプログラムも改竄されない形で記録することができ，ブロックチェーン上での取引について事前条件を取り決めることが可能となる。ブロックチェーン上の取引の際，プログラムで取り決めておいた条件を満たすと，自動的にプログラムが実行され，その結果が検証ノードによって検証された後にブロックチェーン上に記録される。ブロックチェーンでは管理者不在の下で取引の記録が可能であり，スマートコントラクトの機能を活用することにより，様々な取引の自動実行及びその結果の記録が可能となる。ビジネス工程におけるブロックチェーン導入案ではこの機能を活用するものが多い（「2 ブロックチェーンの医療分野での活用事例」を参照）。

1.8.1.1　スマートコントラクトのメリット

スマートコントラクトのメリットとして，複雑なやり取りもスマートコントラクト化できれば，管理者不在の下，取引を自動化させられることが挙げられる。

非ブロックチェーンのシステムでの自動取引の場合は，システムを管理している運営会社が存在し，不具合なく取引が行われることの保証はその運営会社に委ねられており，それが信頼できなければ利用することができない。また，そのシステムを利用する際のシステム利用料や仲介手数料が発生する。一方スマートコントラクトの場合はプログラムが改竄されない状態で公開されており，その条件に基づいて必ず取引が行われる。また，仲介者やシステム管理者が不要となり，取引手数料の削減が期待できる[41]。

1.8.1.2　スマートコントラクトのデメリット

一度ブロックチェーン上に記録されたスマートコントラクトのプログラムは後から変更することができない。前項で記載した通りこれはメリットでもあるが，プログラムに不備がある場合はデメリットとなり得る。プログラムの不備に気づかず，予期しない取引が行われる可能性があり，そのプログラムの不備を修正することができない。また，管理者が不在の下動く仕組みであるため，間に入ってトラブルを解決する仲介者が存在しない（「1.7.7 責任の所在」を参照）。また，曖昧な取引，免責事項が発生するようなフレキシブルな対応が必要な取引はスマートコントラクトで行うことが難しい。

1.8.2　ゼロ知識証明

公開型のブロックチェーンでは「誰から誰」に「何」の所有権が譲渡されたのか，トランザクションがブロックチェーン上に公開情報として記録されるが，この開放性に対するプライバシー保護のアプローチの一つとしてゼロ知識証明が活用されている。ゼロ知識証明は，証明したいデータに完全にアクセス

できなくても，そのデータの内容が正確であることを証明できる手法である [11]。
匿名暗号資産の一つとして知られている Zcash は，zk-SNARKs と呼ばれるゼロ知識証明の一種を使用し，トランザクションの内容ではなくトランザクションのハッシュ値による検証を可能とした。つまり送信者，受信者，送金額を全て秘匿したままの状態で取引の正当性を保証可能としている [42] [43]。
ゼロ知識証明では楕円曲線暗号などの数学的問題が利用されることがあるが，「1.7.8 量子コンピュータ耐性」で述べたように RSA 暗号や楕円曲線暗号は量子コンピュータ耐性を持たないことが知られている。量子コンピュータ耐性を持たない zk-SNARKs に量子コンピュータ耐性を持たせた zk-STARKs と呼ばれるゼロ知識証明も発表されており，ポスト量子コンピュータ時代に向けて期待されている [44]。

1.8.3　セカンドレイヤー

例えばビットコインの場合，個々のコインがいつ発生し，どのアドレスを渡って現在どのアドレスにあるかといった情報はブロックチェーン上に逐一記録されている。しかし，データプライバシーの問題，ブロック生成スピードの問題，トランザクション手数料（マイクロペイメント）の問題[29]又は取り扱えるデータサイズの制限など様々な理由から，全てのデータを直接ブロックチェーン上に記録するのではなく，一部のデータをブロックチェーン外で管理したり，他のブロックチェーンと組み合わせたりする手法が開発されてきた。このように，あるブロックチェーンをベース（レイヤー 1）として利用しつつ，それとは別の階層で動くものを「レイヤー 2」「セカンドレイヤー」などと呼ぶ。

1.8.3.1　オフチェーン

ブロックチェーン上で行われる処理や，ブロックチェーン上に直接記録されるデータ等を「オンチェーン」と表現するのに対し，ブロックチェーンの外側で行われる処理や，ブロックチェーンの外側で管理されるデータ等を「オフチェーン」と表現する。

使用例として，ビットコインの授受（A さんから B さんに 0.1 ビットコインを 10 回送金）をブロックチェーン外で行い，その間の変化（A さんから B さんに 1 ビットコインを送金）のみをブロックチェーンに書き込むことでブロックチェーンのスケーラビリティ問題（1.7.3 参照）を回避する「ライトニングネットワーク」 [45]と呼ばれる手法などがある。

また，ブロックチェーンのメリットの 1 つに透明性（1.6.3 参照）があるが，それは裏を返せば機密性が求められるデータを扱うのにあまり適していないことを意味する。そのため，個人情報や機密性の高いデータはブロックチェーンに直接書き込まず別のデータベースで管理し（オフチェーン），ブロックチェーンにはハッシュだけ書き込むケースが多い。特に医療データのようなセンシティブなデータは（少なくとも現時点では）オフチェーンで管理するのが定石とされている。

---

[29] 少額の取引の場合，トランザクション毎にマイナー（1.3.3 参照）に支払う手数料が，取引額に比して割高になってしまう問題。

ただし，オフチェーンにした部分は，そのままではブロックチェーン（レイヤー１）のメリット（透明性，耐障害性，耐改竄性等）を享受できないため，追加の手当てが必要ではないか，ブロックチェーンを使う意義が失われていないか，よく検討する必要がある。

1.8.3.2　サイドチェーン

公開型ブロックチェーンは機能の追加・変更が容易でないという機能拡張性の課題がある（「1.7.2 システム変更の難しさ」参照）。サイドチェーンはセカンドレイヤー技術の１つであり，主にこの機能拡張性の課題を解決するために開発された [46]。

具体的には，まずスマートコントラクト（1.8.1 参照）等，親チェーン（レイヤー1）では利用できない機能[30]を搭載したブロックチェーン（サイドチェーン）を構築する。そしてサイドチェーンのトランザクション情報を親チェーンのトランザクションにも書き込む仕組みとする。そうすることで，親チェーンが持つセキュリティの高さを享受しつつ，親チェーンにはない機能を利用することができる。

代表例として Liquid，Plasma，Rootstock などが挙げられる。

1.8.4　クロスチェーン

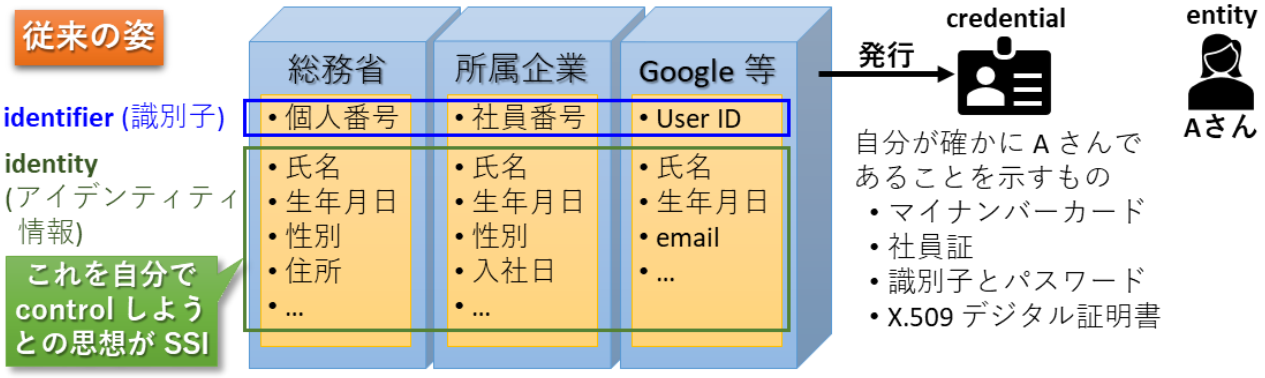
ブロックチェーンの課題の１つに相互運用性（1.7.10 参照）があり，複数のブロックチェーンシステム間で情報を直接（オフチェーンのステップを挟まずに）共有することは困難なのが現状である。
クロスチェーンは複数のブロックチェーン同士を繋ぎ，ブロックチェーン間の情報の自由な交換を可能にする技術である。「ブロックチェーンのインターネット」などとも呼ばれ，ブロックチェーンが真に次世代のインフラとなるために不可欠な技術として注目を集めている。

代表例として Cosmos や Polkadot などが挙げられる。

[30] 例えば，オリジナルのビットコインブロックチェーンはスマートコントラクトに対応していない。

1.8.5　非中央集権型識別子

ブロックチェーンの応用例の 1 つに非中央集権型識別子（Decentralized Identifier: DID）が挙げられる。DID は「自分のアイデンティティ情報（identity）[31] は自分で所有・コントロールすべき」という「自己主権型アイデンティティ」（Self-sovereign identity: SSI）の思想を実現する技術として期待されている。



（参照文献 [47]などを基に作成）

従来，個人のアイデンティティ情報は，Google，Amazon，Facebook，Apple 等，様々な企業や団体がそれぞれ保持しており，時に本人が意図しない形で利用されたり，ハッキング・流出の問題が起きたりしている。アイデンティティ情報を自分で管理し，開示範囲を本人がコントロールできるようにすべきという思想が SSI であり，これを実現するために W3C（World Wide Web Consortium）が開発したのが DID [48] 及び検証可能な資格情報（Verifiable Credentials: VC） [49]である[32]。

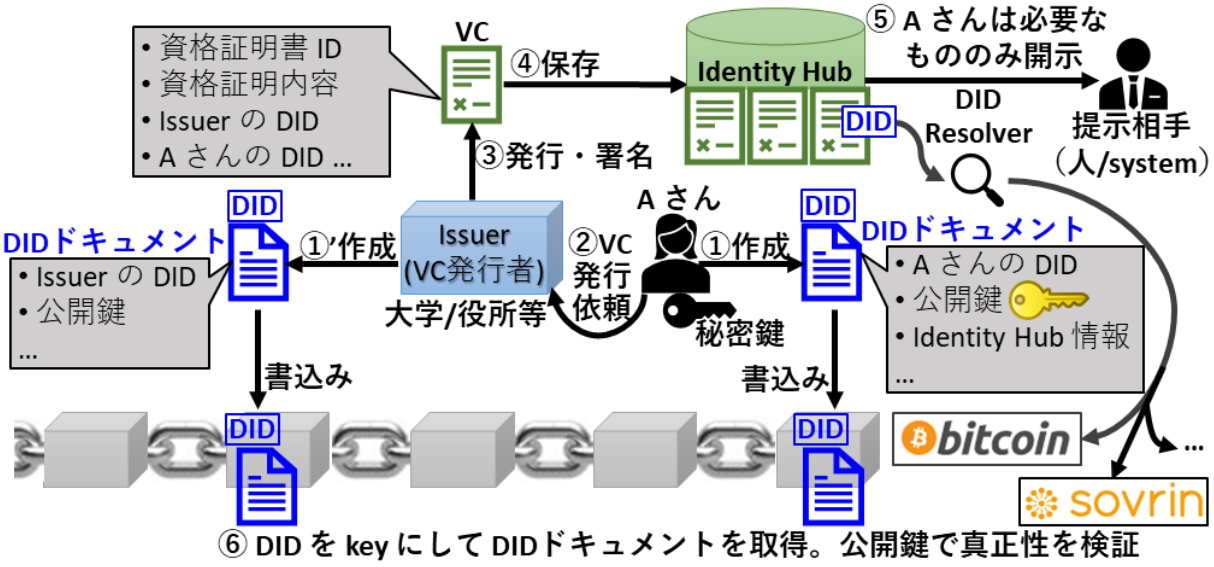
利用者は DID と呼ばれる識別子（ID）及び DID ドキュメント[33] を作成し，ブロックチェーンに書き込む。アイデンティティ情報は DID ドキュメントには含まれず，VC という形式で別途発行者（issuer：卒業証明データならば学校，戸籍データならば国や行政機関など）に発行してもらう。取得した資格情報（credential）はアイデンティティハブ（Identity Hub）に保管し，必要に応じて自分が開示したい分だけ相手に開示する。

---

[31] ここでいう identity（アイデンティティ情報）は，生年月日や性別など「ヒトやモノに紐づく様々な属性情報」を指す（図の緑枠部分）。identifier（識別子。図の青枠）と混同しないよう注意。

[32] ドラフト文書ではあるが W3C が “A Primer for Decentralized Identifiers”（DID 入門）と題した文書 [95] を公開しており，DID の概念をわかりやすく解説している。

[33] DID は DID ドキュメントと key-value database の関係になっており，DID を key として DID ドキュメントを取り出すことができる [95]。



DID/ VC には以下の特徴がある。

- 特定の企業・団体等に紐づかない ID であり，ID 発行者の都合で利用停止されることがない
- その ID が自分のものであることを秘密鍵でいつでも証明できる
- 自分のアイデンティティ情報の何をどこまで開示するか自分でコントロールできる
- 開示されたアイデンティティ情報の発行者をブロックチェーンでいつでも検証できる
- たとえ発行者が消滅（大学の閉校，国家クーデター等）しても当該ブロックチェーンが残っている限り DID ドキュメントは残り，VC の真正性検証が可能であり続ける

多くの企業がこの技術に取り組んでいるが，特に Microsoft が積極的に取り組んでおり，Identity Overlay Network（ION）というシステムを構築し，テスト版を公開している [50]。

2　ブロックチェーンの医療分野での活用事例

ブロックチェーン技術は世界各国で様々な分野に応用されているが，これを医療にも適用し，医療における様々な課題を解決しようとの試みがなされている。
例えば DID/VC（1.8.5 参照）のように，自分のデータを誰に開示するかを中央の管理者ではなく個人個人が自ら制御するという考え方は，ブロックチェーンの持つ非中央集権性と相性がよいため，ブロックチェーンをパーソナル・ヘルス・レコード（Personal Health Record: PHR）に応用しようとの試みが国内外で多数みられる。また，あらかじめ設定した条件を満たしたときにプログラムを自動実行するスマートコントラクト（1.8.1 参照）を臨床試験に適用し，臨床試験の様々なプロセスを自動化することで，プロトコル不遵守を減らし，関係者の負担，ひいては費用を低減する試みが検討されている [4]。
さらに，ブロックチェーンの代表的なユースケースとして挙げられるサプライチェーン管理[34]の仕組みは，そのまま医薬品サプライチェーンに適用できる。
本章では，ブロックチェーンの医療分野での活用について，事例を挙げて説明する。

2.1　パーソナル・ヘルス・レコード（Personal Health Record: PHR），エレクトロニック・ヘルス・レコード（Electronic Health Record: EHR）

近年，個人の健康情報を電子記録として本人や家族が正確に把握するための仕組みである PHR の考え方が世界的に広まっている。日本においても成長戦略フォローアップ（令和元年 6 月 21 日閣議決定）に PHR の推進が謳われるなど，環境整備に向けた検討が進められている [51]。

現時点で PHR の定まった定義はないが，一例として American Health Information Management Association（AHIMA）の定義は以下の通りである [52]。

PHR は，健康に関する決定を下すために個人が必要とする健康情報の，電子的で生涯にわたる情報源である。医療提供者及び本人が収集した情報を，個人が各々の PHR 内に所有及び管理する。 PHR は安全かつ非公開の環境で維持され，アクセス権はその個人が決める。 PHR は，いかなる医療提供者の法的記録も置き換えるものではない。

（原文）[35]
The personal health record (PHR) is an electronic, lifelong resource of health information needed by individuals to make health decisions. Individuals own and manage the information in the PHR, which

---

[34] 一般に，材料が製品になり消費者に届くまでに数多くの企業が関与するため，各社バラバラの方法（場合によっては紙伝票等）でデータを管理していると，需給の調整や，製品に問題が発見されたときのトレースに多大な時間と労力を要する。ブロックチェーンという透明性・耐改竄性の高いプラットフォームに，サプライチェーン管理に必要なデータを各社が載せ合って共有することでこれらの課題解決を目指している。
[35] 和訳は本タスクフォースによるものであり，英文が原文である。解釈については原文が優先する。

comes from healthcare providers and the individual. The PHR is maintained in a secure and private environment, with the individual determining rights of access. The PHR does not replace the legal record of any provider.

ユーザ本人が自己のデータの所有者となり，そこへのアクセス権を，管理者によらずスマートコントラクト（1.8.1 参照）などを活用して自らコントロールすることはブロックチェーンのユースケースの 1 つであり，ブロックチェーンを PHR に活用しようという試みが国内外で進められている。以下にその事例をいくつか紹介するが，上記 PHR の定義の通り，PHR 自体は安全かつ非公開の環境で維持する必要があり，いずれの事例においても医療情報はオフチェーン（1.8.3.1 参照）で管理されている。ブロックチェーンで管理しているのはアクセス権管理等の限定された用途のみである。

2.1.1　日本医師会による糖尿病データベース研究事業「J-DOME」

ブロックチェーンを使用する目的	データベースへのアクセス履歴の保存
ブロックチェーン上に保存されるデータ	データベースへの書き込み・修正等の履歴
ブロックチェーン基盤	独自プラットフォーム
ブロックチェーンの分類（1.5 参照）	非公開型

J-DOME は，かかりつけ医に通院する糖尿病患者の診療データを収集し，糖尿病診療の実態把握や治療の有効性の検証などを行うことで糖尿病患者の治療アウトカム向上を目指す研究事業である [53]。かかりつけ医で得られた検査結果をレジストリデータベースに入力しているが，その監査証跡の記録にブロックチェーンが利用されている [54] [55]。
なお，この仕組みを開発した医療福祉クラウド協会（MeWCA）では，今後の取り組みとして，データレイクに存在する医療データを「誰が」「いつ」「どこで」参照したのか，アクセス履歴を可視化する取り組みをブロックチェーンで行うとしている [56]。

2.1.2　英国の Medicalchain 社の活動

ブロックチェーンを使用する目的	医療データ閲覧権限の付与・削除をスマートコントラクト（1.8.1 参照）で実行するため	医療データを使用したサービスを受けることを目的として，参加者の意思で保険会社や研究機関にデータを提供する等の仕組みを実現するため
ブロックチェーン上に保存されるデータ	対象の医療データの閲覧権限 ※医療データ自体はブロックチェーン外のデータストアに保存	各種サービスのトランザクション記録
ブロックチェーン基盤	Hyperledger Fabric	独自プラットフォーム（イーサリアムベース）
ブロックチェーンの分	非公開型	

類（1.5 参照）	

英国の Medicalchain 社は，ブロックチェーン技術を使用して患者の医療情報を一元管理することを目指す医療データのプラットフォーム「Medicalchain」を構築している。2 つのブロックチェーン基盤を使用しており，Hyperledger Fabric で医療情報へのアクセス権管理を行い，イーサリアムベースのプラットフォームを使用してアプリケーションやサービスの基盤を構築している。医療情報のアクセス権管理では，「誰に」「どの情報を」「どのような権限で」「どれだけの期間」のアクセスを許可するか，情報の閲覧・更新権限の制御を患者自身が行える仕組みとしている [57]。2019 年末より，25 万人以上の患者を抱える 30 の英国の診療所でパイロット的に運用しているとされる。主な目的は，医師に医療記録のアクセスを許可することで誤診を防ぐこと，また，患者が処方薬を乱用することを防ぐこととしている [58]。また，米国のメイヨ・クリニック（Mayo Clinic）とも提携して，ブロックチェーンの医療適用に取り組んでいる [59]。

2.1.3 FDA トランスレーショナル・サイエンス局（office of translational sciences）のパイロットプラットフォーム

ブロックチェーンを使用する目的	医療データ閲覧権限の付与・削除をスマートコントラクト（1.8.1 参照）で実行するため
ブロックチェーン上に保存されるデータ	対象の医療データの閲覧権限 ※医療データ自体はブロックチェーン外のデータストアに保存
ブロックチェーン基盤	独自プラットフォーム（イーサリアムベース）
ブロックチェーンの分類（1.5 参照）	非公開型

FDA のトランスレーショナル・サイエンス局が Booz Allen Hamilton 社と共に病院間のデータシェアを行うパイロット試験を行っている。

病院内にデータシェアのプラットフォームをオフチェーン（1.8.3.1 参照）で構築して暗号化した医療データを格納し，そのデータの閲覧権限をブロックチェーンで管理する。すなわち，データのオーナーが閲覧を許可すると，イーサリアムベースのプラットフォームからスマートコントラクト（1.8.1 参照）によって復号可能な情報が提供される仕組みとなっている [60] [61]。

2.1.4 メドレック・プロジェクト（MedRec project）

ブロックチェーンを使用する目的	医療データ閲覧権限の付与・削除をスマートコントラクト（1.8.1 参照）で実行するため
ブロックチェーン上に保存されるデータ	対象の医療データの閲覧権限 ※医療データ自体はブロックチェーン外のデータストアに保存
ブロックチェーン基盤	独自プラットフォーム（イーサリアムベース）
ブロックチェーンの分類（1.5 参照）	非公開型

マサチューセッツ工科大学メディアラボ（MIT Media Lab）とボストンのベス・イスラエル・ディーコネス医療センター（Beth Israel Deaconess Medical Center：BIDMC）が「MedRec」プロジェクトを共

同で開発し実証実験を進めている。イーサリアムベースのブロックチェーン（スマートコントラクト）技術を基盤とする MedRec のシステムでは，プライベートブロックチェーン上に患者の医療データは実際に保存されず，様々な医療機関及び医師の既存データベースに保存されている患者の医療データにアクセスするためのインターフェースとして機能する。同システムでは医療データの閲覧及び変更権限を誰に付与するかを患者自身が決定できるようになっており，ブロックチェーン上には医療機関の関係者や患者及びその家族など，許可された人物のデータ閲覧又はデータ変更の履歴が記録される仕組みである。

合意形成アルゴリズム（1.4 参照）として，プルーフ・オブ・オーソリティ（Proof of Authority: PoA）が用いられている。中央集権的な側面を残す一方で，PoA により身分が保証された患者や医者だけがネットワークに参加できる仕組みになっている [62]。

2.1.5　米国の Nebula Genomics 社の活動

ブロックチェーンを使用する目的	ゲノムデータのアクセス権限の付与・削除，及びゲノムデータ所有者への謝礼をスマートコントラクト（1.8.1 参照）で実行するため
ブロックチェーン上に保存されるデータ	ゲノムデータのハッシュ値，データへのアクセス権，データ利用者の名前や所属機関など
ブロックチェーン基盤	Exonum
ブロックチェーンの分類（1.5 参照）	公開-許可型

米国の Nebula Genomics 社では，ゲノム配列を解析して本人に健康情報などを提供すると共に，ゲノム情報を企業や研究者に提供するサービスを検討している。ゲノム情報の仲介者を排除して，ゲノム情報を所有する本人から利用者へゲノム情報を提供し，その見返りにゲノム情報を所有者が利益を得られるプラットフォームを目指している [63]。なお，ゲノム情報の提供者は匿名で使用できるが，データの利用者については名前や所属機関などの開示が求められている [64]。

ゲノム情報は暗号化されたデータベースに格納され，ゲノム情報の所有者がアクセスを許可すると，利用者には復号キーが与えられ，所有者にはネブラ・プラットフォーム（Nebula Platform）の暗号資産が譲渡される [63]。復号キーの管理は単一の組織で行うのではなく，複数の独立した組織が所有するキーを組み合わせて復号キーとすることで，流出や悪用に対する保護を強化するとしている [64]。

また，唾液サンプル提出時や遺伝子検査費用支払い時にも以下の手法で匿名性を保つことができるとしている [65]。

① ビットコインなどの暗号資産やプリペイドクレジットカードを使用して費用の支払いを行う
② 個人情報に紐づかないメールアドレスを使用
③ VPN を使用してポータルサイトにアクセスする
④ 私書箱を利用して唾液サンプルの提出を行う

2.1.6　AI（人工知能）ホスピタルによる高度診断・治療システム

内閣府による戦略的イノベーション創造プログラムの一つとして「AI ホスピタルによる高度診断･治療システム」の開発が進められている。AI，IoT，ビッグデータ技術を用いた「AI ホスピタルシステム」を開発・構築・社会実装することにより，高度で先進的な医療サービスを提供するとともに，医療機関における効率化を図り，医師や看護師などの医療従事者の抜本的な負担の軽減を実現することを目標としているプロジェクトである。医療データの情報トレーサビリティ確保と情報アクセス権等の管理にブロックチェーン及びスマートコントラクト（1.8.1 参照）を活用し，患者情報のセキュリティ確保及び活用促進につなげるための概念仕様の構築と技術仕様の確立を行うとしており，2023 年以降に民間企業への情報提供が期待されている [66] [67]。

2.1.7　エストニアの X-Road

IT 先進国として取り上げられるエストニアのシステムに X-Road という仕組みがある。国内の様々な公共機関，民間機関の情報システムを連携しており，医療情報も連携されている。ID を発行された人がオンラインポータルから医療情報にアクセスできるシステムであり，自分の記録だけでなく，未成年の子供など，アクセスが許可された人の記録にもアクセス可能である。また，医師の診察結果や処方内容が確認でき，どの医師がデータにアクセスしたかを確認することも可能なシステムとなっている [68] [69]。

北欧相互運用性ソリューション研究所(Nordic Institute for Interoperability Solutions :NIIS)[36]の記事によれば，X-Road では KSI ブロックチェーンという技術がログの管理に使用されており，各ログはひとつ前のブロックと共に暗号学的ハッシュ関数（1.2.1 参照）によってリンクされている。しかしながら，X-Road 上の他のシステムからセキュリティサーバーのログファイルにアクセスすることはできず，単一のセキュリティサーバー内で独自にチェーンを形成する方式となっているため，ブロックチェーン技術は使用していないとしている [70]。イーエストニア（e-estonia）も NIIS の記事を引用し，暗号学的ハッシュ関数を使用している点では共通しているが，X-Road はブロックチェーン技術に基づいたものではないと述べている [71]。

[36] X-Road や電子政府の構成を，国境を越えて戦略的に開発・管理をすることを目的としてエストニアとフィンランドが共同で設立した組織。2018 年にはアイスランドがパートナーとなっている [93]。

2.2　臨床試験

2.2.1　臨床試験へのブロックチェーン適応検討状況

国内外において，臨床試験の各工程に対してブロックチェーンの導入の検討が進められている。

事例①：サスメド社

サスメド社は「ブロックチェーン技術を用いた臨床研究モニタリングの実証」に関する新技術等実証計画（規制のサンドボックス制度）について厚生労働大臣，経済産業大臣の認定を受け，検証を進めている。臨床試験に参加した被験者が自身の状態に関するアンケート結果を専用アプリで入力し，データのハッシュ値がブロックチェーンに記録されることで改竄が困難となり，データの信頼性を高める試みである。臨床試験ではデータの信頼性を担保する為に，モニターによる入力データと原資料との照合が必要であるが，この費用を削減することを目的としている。公表された論文ではブロックチェーンによる耐改竄性の高いデータの格納が可能であることが示された [72]。論文中では，既存の仕組みである患者報告アウトカム（ePRO）システムや EDC システム等との比較は示されていないが，今後ブロックチェーン導入の利点の明確化が期待される。

事例②：カリフォルニア大学

カリフォルニア大学にて，臨床試験の以下の各工程のやり取りをブロックチェーン上でトレース可能とするシステムのプロトタイプを作成し，その内容を 2019 年 2 月に論文で公表した [73]。

・症例登録のプロセス
・臨床試験開始時のプロトコル承認プロセス
・盲検化試験に於ける，盲検キーオープンのやり取り
・当局への有害事象報告
・CRO とスポンサー間の CRF データの授受
・スポンサーと当局間のデータ授受

ブロックチェーンにデータを記録し，耐改竄性が保証できることが示されたが，その前段階で不正やエラーがあった場合については信頼性が保証出来ない為，この部分が課題となっている。

事例③：クィーンズ大学

クィーンズ大学にて，イーサリアムのプラットフォームを用いてスマートコントラクト（1.8.1 参照）により臨床試験の工程を管理するシステムのプロトタイプを作成し，その内容を 2018 年 12 月に論文で公表した [74]。スマートコントラクトにより，以下のプロセスを事前に定義し，定義通りに臨床試験実施が保証されることを実証した。

被験者関連のスマートコントラクト

・被験者の試験への登録とアクセス権限の管理
・被験者のアクセス権限の変更
・試験に登録された被験者の抽出

臨床試験実施側

・クエリー追加

・クエリー結果追加
・クエリー受領
・未回答クエリーのカウント
今後，さらに他のステークホルダーのロールについてもブロックチェーンでの管理を適応することにより，臨床試験の信頼性を高められる可能性があると結論付けている。

ここで紹介したもの以外にも，臨床試験のプロセスにおいてブロックチェーン適応が検討されている事例が幾つか存在する。現状，実際の臨床試験へ導入された事例は少ないが，ブロックチェーンの特性を利用したプロセスの信頼性向上が今後期待される。

2.2.2　臨床試験データの二次利用のプロセス管理

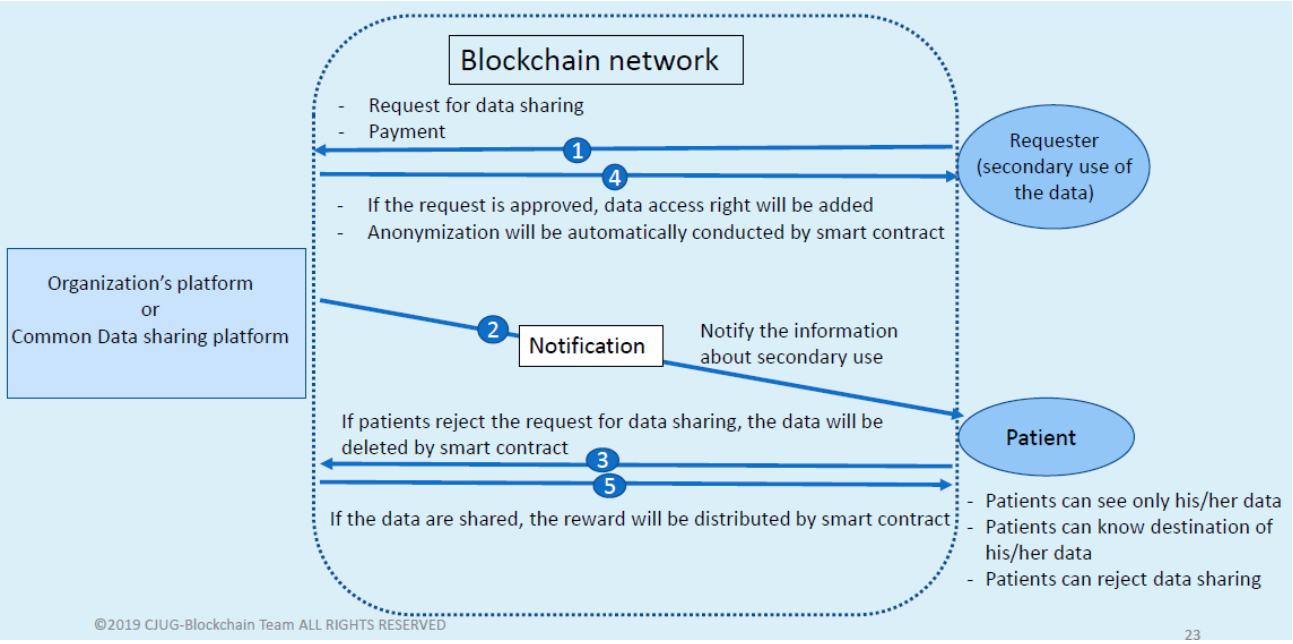
臨床試験データを二次利用する際，個人情報保護の観点から，被験者が特定されないよう非特定化処理を行った後にデータ共有が行われている。このプロセスには課題があり，非特定化の処理を行った場合でも個人が特定されるリスクを完全に取り除くことが難しく，被験者は自身のデータがどこで使用されているのか把握することができない。CJUG-SDTM ブロックチェーン・サブ・チームはこの課題に着目し，ブロックチェーンでの課題解決を提案している。大まかに以下の流れである。

1. 臨床試験開始時に被験者よりデータ二次利用に対する同意を取得
2. ブロックチェーンで管理するための変数を付与
3. データ共有の流れをブロックチェーンで管理

また，スマートコントラクト（1.8.1 参照）の機能やブロックチェーンに紐づいた IT システムの組み合わせにより，以下の仕組みが可能となる。

- 被験者がデータの行き先を見ることができる
- 被験者が二次利用を拒否した場合，そのデータが削除された状態でデータ共有が行われる
- スマートコントラクトによるデータ共有に関するメール通知
- データ共有で発生する支払いの管理と被験者への報酬分配

下図がデータ共有時の想定フローとなる。



[75] CJUG SDTM ブロックチェーン・サブ・チームに掲載許諾をいただいている

既存の技術でこの仕組みを構築するのに比べ，ブロックチェーンを用いることにより，各プロセスの標準化，複数のプラットフォーム間の取引履歴の一元管理等の効率化が期待される。
この案は公開時点（2019 年 10 月 24 日 PharmaSUG SDE Tokyo で公開）では計画段階であるが，今後システム開発及び検証が行われる予定である。

2.2.3　医療機関による医療データの二次利用管理

ブロックチェーンを使用する目的	医療データ閲覧権限の付与・削除や選択除外基準の検証をスマートコントラクト（1.8.1 参照）で実行するため
ブロックチェーン上に保存されるデータ	各種同意情報，個人が特定可能な保健医療情報（PHI）のメタデータ
ブロックチェーン基盤	Hyperledger Fabric
ブロックチェーンの分類（1.5 参照）	非公開型

2.2.2 では，臨床試験を行った企業が，収集した医療データを二次利用するためのプロセス管理にブロックチェーンの活用を検討していることに対し，IBM 社は医療機関における医療データの二次利用管理にブロックチェーンの活用を提案している。IBM 社の提案によると，PHI を参照したスマートコントラクトの使用による適格性の判定や，様々な同意情報をリアルタイムに変更可能なダイナミック・コンセント（Dynamic Consent）[37]のプラットフォームとして活用でき，適切なデータの権限管理が可能にな

[37] 従来の，研究参加当初の同意内容がずっと継続し，その同意内容に同意し続けるか同意撤回するかの二種類しか選択肢がない，という状況（静的：static)に対し，活発な双方向のコミュニケーションを行うことか

るとしている [76]。

IBM 社が提案した運用手順

① 参加者が試験への参加に同意する。
② アクセスに同意した情報と PHI のメタデータを台帳に記録する。
③ 試験中に被験者から収集したデータをデータベースに保存する。
④ 二次利用者がデータのアクセスをリクエストする。
⑤ リクエストを受けたサーバは，対象のデータのアクセス許諾を確認し，有効な場合はデータベースから取り出したデータを二次利用者へ提供する。

ら”動的(dynamic)”という [96]。

2.3　医薬品の流通

2017 年に本邦で判明した C 型肝炎治療薬の偽造医薬品流通問題は記憶に新しい方も多いと思うが，偽造医薬品の流通対策は世界的にも課題とされている [77]。本章では，米国の政策である医薬品サプライチェーンセキュリティ法（Drug Supply Chain Security Act: DSCSA）の中で実施されている，ブロックチェーンを使用した流通管理のパイロット試験を紹介する。

また，本邦においては調剤薬局におけるデッドストック医薬品の存在も課題の一つと考えられており，薬局間での医薬品の授受が日常的に行われている。C 型肝炎治療薬の偽造医薬品流通問題では現金問屋と呼ばれる仲介業者から持ち込まれたとされており [78]，そのような仲介業者を介することなく，互いに認識のない個人経営の薬局間でも医薬品取引が行えるプラットフォームの実証実験も紹介する。

2.3.1　DSCSA 対応

米国の医薬品サプライチェーンセキュリティ法（Drug Supply Chain Security Act: DSCSA）では，製品をパッケージ単位で追跡可能な，相互運用性のある電子的なシステムを 2023 年までに導入することを規定している[38] [79] [80]。この電子的なシステムの構築においてブロックチェーン技術の可用性を評価するため，2017 年に Chronicled 社と The Linklab 社によって合弁会社メディレッジャー・プロジェクト（MediLedger Project）が設立され，Genentech 社，Pfizer 社などの製薬企業や AmerisourceBergen 社，McKesson 社などの卸業者を含むワーキンググループによって実証実験が行われてきた [81] [82] [83]。

実証実験において構築されたプロトタイプシステムは，イーサリアムを基盤としたブロックチェーンシステムであり，ゼロ知識証明技術（zk-SNARKs）（1.8.2 参照）を使用することでトランザクションの内容を開示せず，ハッシュ化したトランザクション情報を証明としてブロックチェーン上に記録する手法であった。

2020 年 1 月に発行された最終報告では，ブロックチェーンが医薬品サプライチェーンの管理に使用可能な，相互運用性を持つシステムとしての基礎となる技術を持つことを示せた一方で，他のシステムと連携するための標準規格が存在していないことを，相互運用性を持つための明確な課題として挙げている [84]。

なお，メディレッジャー・プロジェクトの他に少なくとも 5 つ（IBM 社/KPMG 社/Merck 社/Walmart 社，IDLogiq 社，Rymedi 社，TraceLink 社，UCLA Health）の組織が，2019 年 8 月より FDA が開始している DSCSA 対応のパイロット試験に，ブロックチェーンを用いて参加している [85]。（2020 年 3 月末時点）

また，本邦においては，日本通運がアクセンチュアやインテル日本法人と組み，偽造医薬品の混入防止に向けたサプライチェーン管理にブロックチェーンを活用することが発表された。3 社は 2021 年を目

[38] 日本国内においても，平成 30 年 12 月に発出された「医薬品の適正流通（ＧＤＰ）ガイドライン」において，「製品回収を迅速に行うために受領及び輸送される製品のトレーサビリティを保証するための文書と手順書を整備すること」を定めている [97]。

標に医薬品分野のシステム構築を目標としている [86]。

2.3.2　医薬品のデッドストック販売プラットフォーム

ブロックチェーンを使用する目的	個人経営の薬局間において，仲介者不在でデッドストックを売買するプラットフォームを提供するため
ブロックチェーン上に保存されるデータ	医薬品の売買情報
ブロックチェーン基盤	Hyperledger Fabric
ブロックチェーンの分類（1.5 参照）	非公開型

厚生労働省の調査によると，2017 年度の全国の薬局数は約 59,000 店舗と，その数は同年度の全国のコンビニエンスストア店舗数（約 55,000 店舗）よりも多い状況となっている [87] [88]。また，後発品の普及により常備する在庫品が増加しているため，デッドストック医薬品が在庫を圧迫しており，調剤薬局間でデッドストックの解消を図りたいというニーズが存在している。一方で，個人経営が多いといわれる薬局では，見ず知らずの事業者間でのデッドストック医薬品の取引に不安を感じている可能性が高いことから，取引を行う際の信頼性を担保するための基盤としてブロックチェーンが注目されている。これまで実証実験を進めてきた INDETAIL 社によれば，同時アクセス 100 トランザクションが実行されるシステムであれば実運用が可能であると結論付けている [89] [90]。

2.4　ファーマレッジャー・プロジェクト（PharmaLedger project）

DSCSA 対応のために米国で設立されたメディレッジャー・プロジェクトに対し，欧州では 2020 年 1 月にファーマレッジャー・プロジェクトが設立された [91]。サプライチェーン，臨床試験，ヘルスケアデータのイノベーションを実現するために設立されたコンソーシアムで，革新的医薬品イニシアティブ（Innovative Medicines Initiative: IMI）と欧州製薬団体連合会(European Federation of Pharmaceutical Industries and Associations: EFPIA)が支援する 3 年間のプロジェクトである。本報告書の執筆時点では設立から間がなく，具体的な活動内容が明らかになっていないが，今後の展開が期待される。

ファーマレッジャー・プロジェクトとメディレッジャー・プロジェクトに参加している製薬企業を以下の表にまとめた。ファーマレッジャー・プロジェクトは全 29 組織中 12 社が製薬企業であり，メディレッジャー・プロジェクトは全 23 組織中，10 社が製薬企業である[39]。

参加企業[40]（アルファベット順）	PharmaLedger	MediLedger
AbbVie 社	○	
Amgen 社		○
AstraZeneca 社	○	
Bayer 社	○	
Boehringer Ingelheim 社	○	
Dermira 社		○
Eli Lilly 社		○
F. Hoffmann-La Roche 社	○	
Gilead Sciences 社		○
GlaxoSmithKline 社	○	○
Genentech 社		○
Janssen 社	○	
Novartis 社	○	○
Novo Nordisk 社	○	○
Pfizer 社	○	○
Sanofi 社		○
UCB 社	○	

[39] メディレッジャー・プロジェクトは DSCSA パイロット試験ファイナルレポート時点の参加企業，ファーマレッジャー・プロジェクトは設立時点の参加企業を一覧化した。

[40] ファーマレッジャー・プロジェクトでは，欧州各国で設立されている傘下企業の参加が表明されているが，ここでは比較のため母体となる企業名を表記した。

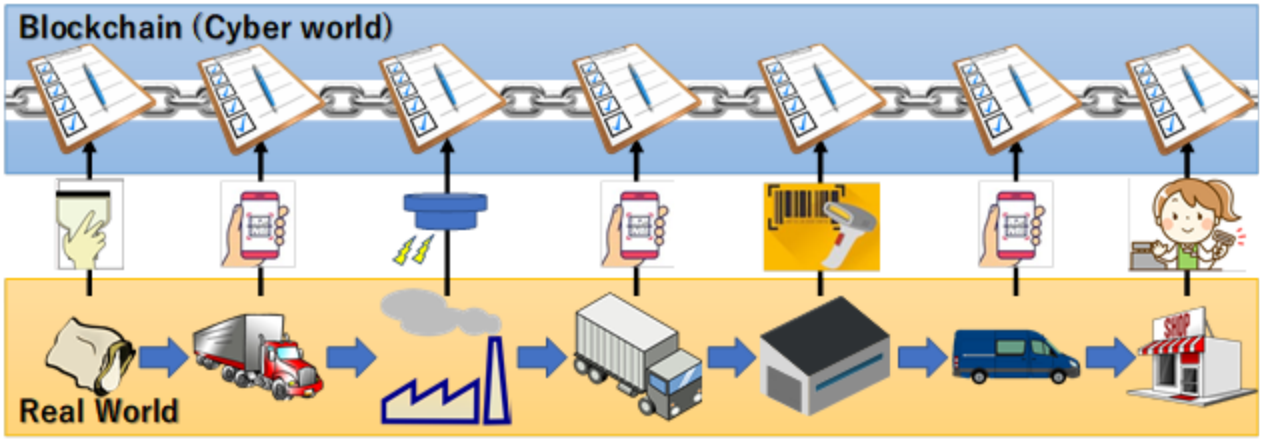
Column 3: トレーサビリティにまつわる過剰な期待

サプライチェーンのトレーサビリティ管理はブロックチェーンの代表的なユースケースであり，医薬品だけでなく，食品からダイヤモンド，ルイ・ヴィトンのバッグに至るまで，様々な分野で実用化されている。

「サプライチェーンが透明化される」「真贋判定も可能になる」という宣伝文句と，「ブロックチェーンは改竄が困難」というイメージとが相まって，あたかも「ブロックチェーンで管理しさえすれば偽物や不正を排除できる」と誤解されることがあるが，果たしてそうであろうか。

ビットコインのように，ブロックチェーンの台帳上にしか存在しない仮想的な資産*ならば，台帳を改竄しない限り「偽札」が入り込む余地はない。しかし，現実世界の資産をブロックチェーンで管理する場合は話が変わってくる。「台帳」は改竄できなくとも，その台帳で管理する資産は（ものにもよるが）すり替え等が可能だからである。そのため，たとえブロックチェーンを使用したとしても，資産と台帳とが確実に結びつく（偽造品と台帳とがけっして結びつかない）手段を別途講じない限り，偽造品を排除することはできない。

例えば偽造困難なマイクロチップ等を製品に埋め込み，「ブロックチェーンに記録されているこの製品は，マイクロチップの ID が一致するこの製品に間違いない」などと証明する仕組みができれば，偽造品の判定は容易になる。しかしその場合も，もし生産者自身が工程の途中で原材料・製品のすり替え等の不正を行った場合，それをブロックチェーンで検知できるわけではない。



「ブロックチェーンとは何か？」を正しく理解することで，ブロックチェーンで何ができて何ができないのかが自明となる。我々皆がブロックチェーン技術を正確に理解することで，過剰な期待を排し，この有望な技術を正しく活用できるようになることを願ってやまない。

---

*「ビットコインは交換所で換金できるので『仮想的な資産』ではない」と思われるかもしれないが，それは取引を行う当事者同士が実体のない「ビットコイン」というものに金銭的価値があると信じているから成立しているに過ぎない。

おわりに

連日ニュースを賑わせたビットコインの急騰・急落から 2 年以上が経過した。この数年でブロックチェーンの暗号資産以外への活用検討が進み，「ブロックチェーン＝暗号資産」と理解する人も少なくなっているように感じる。しかし，ブロックチェーンについてウェブサイトなどで手に入る情報の多くは，本来全く異なる許可型と自由参加型が混同されていたり，専門的過ぎたりと，ある程度の知識（リテラシー）を持たなければ正しく読み解くことが難しい状況にある。本報告書は，ブロックチェーンはどういう技術なのか，何に適用できるのか，なぜ世間の暗号資産ブームが去っても注目されているのか，課題や限界はないのかといった疑問に答え，我々がブロックチェーン技術を用いたサービス等を「目利き」して業務に適切に活用できる手掛かりになるよう作成したつもりである。

本報告書を執筆するにあたり，技術的な詳細をどこまで報告書に盛り込むべきかタスクフォース内で議論となったが，許可型と自由参加型との本質的な違いや，ブロックチェーンの「耐改竄性」の正体など，ブロックチェーンの本質を正しく理解し活用できるようになるためには技術的な理解も欠かせないと考え，1 章ではブロックチェーン技術及びその要素技術の解説に多くの紙面を割いた。ただし読了のハードルを上げないよう極力簡潔な記載とし，上記目的にとって必須でないと判断した事項（例えば UTXO，トランザクションスクリプト等）は思い切って削った。十分に納得のいく解説ができていない項目があるかもしれないが，参照文献を手掛かりに理解を補っていただければ幸いである。

続く 2 章では医療分野における活用事例の紹介を行った。現在は医療分野に限らず，各社がブロックチェーンに取り組み始めた黎明期であり，今後はより多くの事例が出てくることが期待される。医療情報というセンシティブデータを扱う我々にとって，ブロックチェーンは改竄困難な良いこと尽くしの万能ツールではなく，扱い方を間違えると重大なコンプライアンス違反を犯しうる諸刃の剣である。一方で PHR の管理や医療データの二次利用に関する同意取得など，我々の直面する様々な課題を解決できる可能性を秘めたツールでもあり，今後の展開に期待したい。また，今回の報告書では適切な実例が見つからず紹介できなかったバリューベースドペイメント（Value-based Payment）への応用 [92]など，医療分野では他にも様々な用途への応用が検討されている。興味を持たれたかたは是非参考文献 [4]や最近の論文などを参照いただきたい。

ブロックチェーンはまだ発展途上の技術であり，様々な用語の定義もまだ十分に統一されていない状況である。ブロックチェーンそれ自体の定義さえ，本報告書の執筆中に新たに ISO がドラフト版定義を公表するなど，日々状況が変わっている。情報技術の発展が目まぐるしい今日では，本報告書の内容もすぐに陳腐化してしまうかもしれない。しかしながら，今，ブロックチェーンに興味を持つ読者諸氏にまとまった基礎知識を提供し，我々の業界におけるブロックチェーンの適切な活用に一役買わせていただけたなら幸いである。

参照文献

[1] 斉藤賢爾, 信用の新世紀 ブロックチェーン後の未来, インプレス R&D, 2017.

[2] 結城浩, 暗号技術入門 第 3 版, SB クリエイティブ, 2015.

[3] ドン・タプスコット , アレックス・タプスコット, ブロックチェーン・レボリューション ビットコインを支える技術はどのようにビジネスと経済、そして世界を変えるのか, ダイヤモンド社, 2016.

[4] デイビッド・メトカーフ, ジョン・バース, マックス・フーパー, アレックス・カハナ , ヴィクラム・ディロン, 海外の最新事例に学ぶ 医療×ブロックチェーン~ブロックチェーン技術は医療・ヘルスケア業界に変革をもたらすか~, 日経 BP, 2019.

[5] ガートナー ジャパン株式会社, “ガートナー、「日本におけるテクノロジのハイプ・サイクル：2019年」を発表 - デジタル・ビジネスを推進する上で特に注目すべきテクノロジと そのトレンドを明らかに,” 31 Oct 2019. [オンライン]. Available: https://www.gartner.com/jp/newsroom/press-releases/pr-20191031. [アクセス日: 28 Mar 2020].

[6] ISO, “ISO/DIS 22739 Blockchain and distributed ledger technologies — Terminology,” [オンライン]. Available: https://www.iso.org/standard/73771.html. [アクセス日: 1 Mar 2020].

[7] 篤. 山岸, “暗号アルゴリズム移行問題 - 暗号研究者の立場から -,” 3 July 2008. [オンライン]. Available: https://www.jnsa.org/seminar/2008/0703/data/09_panel03.pdf. [アクセス日: 22 May 2020].

[8] 独立行政法人 情報処理推進機構, “MD5 の安全性の限界に関する調査研究報告書,” Jul 2008. [オンライン]. Available: https://www.ipa.go.jp/files/000013897.pdf. [アクセス日: 28 Mar 2020].

[9] M. Stevens, E. Bursztein, P. Karpman, A. Albertini , Y. Markov, “The First Collision for Full SHA-1,” Springer, Cham, 2017.

[10] 総務省 経済産業省, “電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト),” Mar 2013. [オンライン]. Available: https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r4.pdf. [アクセス日: 28 Mar 2020].

[11] D. Drescher, 徹底理解ブロックチェーン ゼロから着実にわかる次世代技術の原則, インプレス, 2018.

[12] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Bitcoin.org, 2008.

[13] アンドレアス・M・アントノプロス, ビットコインとブロックチェーン：暗号通貨を支える技術, NTT 出版, 2016.

[14] 杉井靖典, いちばんやさしいブロックチェーンの教本　人気講師が教えるビットコインを支える仕組み, インプレス, 2017.

[15] G.-T. Nguyen , K. Kim, “A Survey about Consensus Algorithms Used in Blockchain,” *Journal of Information Processing Systems,* 第 巻 14, 第 1, pp. 101-128, 2018.

[16] W. WANG, D. T. HOANG, P. HU, Z. XIONG, D. NIYATO, P. WANG, Y. WEN , I. D. KIM , “A

Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access,* 第 巻 7, pp. 22328-22370, 2019.

[17] Nxt, "Nxt Whitepaper," [オンライン]. Available: https://nxtdocs.jelurida.com/Nxt_Whitepaper#Proof_of_Stake. [アクセス日: 28 Mar 2020].

[18] bitshares, "Delegated Proof-of-Stake Consensus," [オンライン]. Available: https://bitshares.org/technology/delegated-proof-of-stake-consensus/. [アクセス日: 28 Mar 2020].

[19] nem, "What is POI," [オンライン]. Available: https://docs.nem.io/en/gen-info/what-is-poi. [アクセス日: 28 Mar 2020].

[20] POA, "POA Network Whitepaper," 28 Sep 2018. [オンライン]. Available: https://github.com/poanetwork/wiki/wiki/POA-Network-Whitepaper. [アクセス日: 28 Mar 2020].

[21] NEO, "Consensus Mechanism," [オンライン]. Available: https://docs.neo.org/developerguide/en/articles/consensus/readme.html. [アクセス日: 28 Mar 2020].

[22] L. Lamport, R. Shostak , M. Pease, "The Byzantine Generals Problem," ACM Transactions on Programming Languages and Systems, 1982.

[23] BitFury Group, ""Public versus Private Blockchains Part 1: Permissioned Blockchains" White Paper," 20 Oct 2015. [オンライン]. Available: https://bitfury.com/content/downloads/public-vs-private-pt1-1.pdf. [アクセス日: 28 Mar 2020].

[24] BitFury Group, ""Public versus Private Blockchains Part 2: Permissionless Blockchains" White Paper," 20 Oct 2015. [オンライン]. Available: https://bitfury.com/content/downloads/public-vs-private-pt2-1.pdf. [アクセス日: 28 Mar 2020].

[25] Sovrin Foundation, "Is Sovrin 'Permissioned'?," 8 Dec 2018. [オンライン]. Available: https://sovrin.org/faq/is-sovrin-permissioned/. [アクセス日: 28 Mar 2020].

[26] J. Ruiz, "Public-Permissioned blockchains as Common-Pool Resources," 14 Feb 2020. [オンライン]. Available: https://www.linkedin.com/pulse/public-permissioned-blockchains-common-pool-resources-jesus-ruiz/. [アクセス日: 28 Mar 2020].

[27] 翁百合, 柳川範之 , 岩下直行, "すぐわかるブロックチェーンの種類とメリット," [オンライン]. Available: https://bizgate.nikkei.co.jp/article/DGXMZO28437700220320180000000?channel=DF260320183674&page=2. [アクセス日: 28 Mar 2020].

[28] インフォテリア株式会社, "プレスリリース: ブロックチェーン技術による 文書改ざん検知ソリューション を提供開始," 21 Jun 2018. [オンライン]. Available: https://www.asteria.com/jp/news/press/2018/06/21_01.php. [アクセス日: 3 Apr 2020].

[29] Accenture, "BANKING ON BLOCKCHAIN," 2017. [オンライン]. Available: https://www.accenture.com/us-en/_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/consulting/accenture-banking-on-blockchain.pdf. [アクセス

日: 3 Apr 2020].

[30] 翁百合, 柳川範之 , 岩下直行, 共同編集, ブロックチェーンの未来 金融・産業・社会はどう変わるのか, 日本経済新聞出版社, 2017.

[31] M. Rosenfeld, “Analysis of hashrate-based double-spending,” 11 Dec 2012. [オンライン]. Available: https://bitcoil.co.il/Doublespend.pdf. [アクセス日: 28 Mar 2019].

[32] 岡嶋裕史, ブロックチェーン 相互不信が実現する新しいセキュリティ, 講談社, 2019.

[33] Bitcoin community, “Scalability,” [オンライン]. Available: https://en.bitcoin.it/wiki/Scalability. [アクセス日: 28 Mar 2020].

[34] VISA, “VISA Fact Sheet,” [オンライン]. Available: https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf. [アクセス日: 28 Mar 2020].

[35] University of Cambridge, “Cambridge Bitcoin Electricity Consumption Index,” [オンライン]. Available: https://www.cbeci.org/comparisons/. [アクセス日: 14 Apr 2020].

[36] 玄忠雄, “仮想通貨に新たな脅威、51%攻撃でオルトコインに被害続出,” 日経 xTECH／日経コンピュータ, 11 Jun 2018. [オンライン]. Available: https://tech.nikkeibp.co.jp/atcl/nxt/column/18/00001/00591/. [アクセス日: 28 Mar 2020].

[37] 清藤武暢 , 四方順司, “量子コンピュータが共通鍵暗号の安全性に与える影響,” Jan 2019. [オンライン]. Available: https://www.imes.boj.or.jp/research/papers/japanese/kk38-1-4.pdf. [アクセス日: 28 Mar 2020].

[38] 伊東謙介, “分散型オラクルの合意形成に対する ピア予測法の潜在的有用性（A Potential Utility of Peer Prediction Method to Consensus Building on DecentralizedOracle Systems）,” 東京大学大学院情報学環紀要　情報学研究　No95, 2018.

[39] pwc, “What it takes to build your blockchain,” [オンライン]. Available: https://www.pwc.com/gx/en/issues/blockchain/blockchain-in-business/build-an-ecosystem.html. [アクセス日: 28 Mar 2020].

[40] コインテレグラフ日本版, “製薬大手ファイザー幹部、「ブロックチェーンを成長させるには十分な力ある」,” 15 May 2019. [オンライン]. Available: https://jp.cointelegraph.com/news/pfizer-executive-technology-is-basically-good-enough-to-ramp-up-production-blockchains. [アクセス日: 28 Mar 2020].

[41] IPA 独立行政法人情報処理推進機構, “ブロックチェーンの特性から理解する社会実装の展望,” [オンライン]. Available: https://www.ipa.go.jp/ikc/reports/blockchain_01-03.html. [アクセス日: 3 Apr 2020].

[42] Zcash, “What are zk-SNARKs?,” [オンライン]. Available: https://z.cash/technology/zksnarks/. [アクセス日: 28 Mar 2020].

[43] P. Peterson, “Anatomy of A Zcash Transaction,” 23 Nov 2016. [オンライン]. Available: https://electriccoin.co/blog/anatomy-of-zcash/. [アクセス日: 28 Mar 2020].

[44] E. Ben-Sasson, I. Bentov, Y. Horesh , M. Riabzev, “Scalable, transparent, and post-quantum secure computational integrity,” 6 Mar 2016. [オンライン]. Available: https://eprint.iacr.org/2018/046.pdf. [アクセス日: 28 Mar 2020].

[45] J. Poon , T. Dryja, “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments,” 2016.

[46] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón , P. Wuille, “Enabling Blockchain Innovations with Pegged Sidechains,” 2014.

[47] 独立行政法人 情報処理推進機構 セキュリティセンター, “アイデンティティ管理技術解説 -ドラフト-,” Jan 2013. [オンライン]. Available: https://www.ipa.go.jp/files/000014270.pdf. [アクセス日: 1 Mar 2020].

[48] World Wide Web Consortium (W3C), “Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations,” 23 Feb 2020. [オンライン]. Available: https://www.w3.org/TR/did-core/. [アクセス日: 28 Mar 2020].

[49] World Wide Web Consortium, “Verifiable Credentials Data Model 1.0,” [オンライン]. Available: https://www.w3.org/TR/vc-data-model/. [アクセス日: 28 Mar 2020].

[50] Microsoft, “分散型 ID - デジタル ID を自分で所有,” [オンライン]. Available: https://www.microsoft.com/ja-jp/security/business/identity/own-your-identity. [アクセス日: 1 Mar 2020].

[51] 厚生労働省健康局健康課, “第 1 回国民の健康づくりに向けたＰＨＲの推進に関する検討会の開催について,” 6 Sep 2019. [オンライン]. Available: https://www.mhlw.go.jp/stf/newpage_06643.html. [アクセス日: 28 Mar 2020].

[52] AHIMA e-HIM Personal Health Record Work Group, “Defining the Personal Health Record.,” Journal of AHIMA 76, no.6.

[53] 日本医師会, “日本医師会 かかりつけ医 糖尿病データベース研究事業 （J-DOME）,” [オンライン]. Available: https://www.jdome.jp/index.html. [アクセス日: 28 Mar 2020].

[54] 日経デジタルヘルス, “国内でもブロックチェーンの医療応用が始まった,” 31 Oct 2018. [オンライン]. Available: https://xtech.nikkei.com/dm/atcl/event/15/101000173/103000041/. [アクセス日: 28 Mar 2020].

[55] 長瀬嘉秀, “日本医師会におけるブロックチェーンを利用した医療情報システム,” 4 Mar 2019. [オンライン]. Available: https://www.mewca.jp/wp-content/uploads/2019/03/190304-2.pdf. [アクセス日: 28 Mar 2020].

[56] 特定非営利活動法人医療福祉クラウド協会, “MeWCA クラウドブロックチェーンの実装例,” 4 Mar 2019. [オンライン]. Available: https://www.mewca.jp/wp-content/uploads/2019/03/190304-3.pdf. [アクセス日: 28 Mar 2020].

[57] Medicalchain, “Medicalchain Whitepaper 2.1,” 2018. [オンライン]. Available: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf. [アクセス日: 28 Mar 2020].

[58] FINANCIAL TIMES, “Businesses turn to blockchain for answers,” 23 Oct 2019. [オンライン].

Available: https://www.ft.com/content/4e6df6d2-e90a-11e9-85f4-d00e5018f061. [アクセス日: 28 Mar 2020].

[59] Medicalchain, “Medicalchain Announces Joint Working Agreement with Mayo Clinic,” 18 Jun 2018. [オンライン]. Available: https://medium.com/medicalchain/medicalchain-announces-joint-working-agreement-with-mayo-clinic-9cfb474dcf0f. [アクセス日: 28 Mar 2020].

[60] S. FRIEDMAN, “FDA builds blockchain-based health data sharing platform,” 22 Jun 2018. [オンライン]. Available: https://gcn.com/articles/2018/06/22/fda-blockchain-ehr-sharing.aspx. [アクセス日: 28 Mar 2020].

[61] M. A. Cyran, “Blockchain as a Foundation for Sharing Healthcare Data,” 23 Mar 2018. [オンライン]. Available: https://blockchainhealthcaretoday.com/index.php/journal/article/view/13. [アクセス日: 28 Mar 2020].

[62] 中沢潔, “米国におけるブロックチェーンの現状,” [オンライン]. Available: https://www.ipa.go.jp/files/000067088.pdf. [アクセス日: 7 Apr 2020].

[63] D. Grishin, K. Obbad, P. Estep, K. Quinn, S. W. Zaranek, A. W. Zaranek, W. Vandewege, T. Clegg, N. César, M. Cifric , G. Church, “Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation,” 17 Dec 2018. [オンライン]. Available: https://blockchainhealthcaretoday.com/index.php/journal/article/view/34. [アクセス日: 28 Mar 2020].

[64] R. Kain, S. Kahn, D. Thompson, D. Lewis, D. Barker, C. Bustamante, C. Cabou, A. Casdin, F. Garcia, J. Paragas, A. Patrinos, A. Rajagopal, S. Terry, A. V. Zeeland, E. Yu, Y. Erlich , D. Barry, “Database shares that transform research subjects into partners,” Nature Biotechnology, 2019.

[65] NEBULA GENOMICS, “Anonymous Sequencing Now Available,” 19 Sep 2019. [オンライン]. Available: https://blog.nebula.org/anonymous-sequencing/. [アクセス日: 7 Apr 2020].

[66] 内閣府, “AI（人工知能）ホスピタルによる高度診断・治療システム 研究開発計画,” 19 Jul 2018. [オンライン]. Available: https://www.nibiohn.go.jp/nibio/part/promote/files/SIP-plan.pdf. [アクセス日: 28 Mar 2020].

[67] 内閣府, “AI（人工知能）ホスピタルによる高度診療・治療システム 工程表,” [オンライン]. Available: https://www8.cao.go.jp/cstp/gaiyo/sip/keikaku2/aihospital_kotei.pdf. [アクセス日: 28 Mar 2020].

[68] e-estonia, “x-road,” [オンライン]. Available: https://e-estonia.com/solutions/interoperability-services/x-road/. [アクセス日: 28 Mar 2020].

[69] e-estonia, “e-health records,” [オンライン]. Available: https://e-estonia.com/solutions/healthcare/e-health-record/. [アクセス日: 28 Mar 2020].

[70] P. Kivimäki, “There is no blockchain technology in X-Road,” 26 Apr 2018. [オンライン]. Available: https://www.niis.org/blog/2018/4/26/there-is-no-blockchain-technology-in-the-x-road. [アクセス日: 28 Mar 2020].

[71] e-estonia, “Weekly press review | X-Road not to be confused with blockchain,” May 2018. [オンライン]. Available: https://e-estonia.com/why-x-road-is-not-blockchain/. [アクセス日: 28 Mar 2020].

[72] D. Ichikawa, M. Kashiyama , T. Ueno, “Tamper-Resistant Mobile Health Using Blockchain Technology,” JMIR Mhealth Uhealth, 2017.

[73] D. R. Wong , S. Bhattacharya , A. J. Butte , “Prototype of running clinical trials in an untrustworthy environment using blockchain,” Nature Communications, 2019.

[74] D. M. Maslove, J. Klein, K. Brohman , P. Martin, “Using Blockchain Technology to Manage Clinical Trials Data: A Proof-of-Concept Study,” 2018.

[75] CJUG SDTM Blockchain sub-team, “PHUSE Single Day Event Shanghai,” [オンライン]. Available: https://www.pharmasug.org/proceedings/tokyo2019/presentations/PharmaSUG-Tokyo-2019-07.pdf. [アクセス日: 28 Mar 2020].

[76] O. Choudhury, H. Sarker, N. Rudolph, M. Foreman, N. Fay, M. Dhuliawala, I. Sylla, N. Fairoza , A. K. Das, “Enforcing Human Subject Regulations using Blockchain and Smart Contracts,” *Blockchain in Healthcare Today,* 第 巻 1, 23 3 2018.

[77] 木村和子, “世界の偽造医薬品対策,” 29 Mar 2017. [オンライン]. Available: https://www.mhlw.go.jp/file/05-Shingikai-11121000-Iyakushokuhinkyoku-Soumuka/siryou6.pdf. [アクセス日: 28 Mar 2020].

[78] 厚生労働省医薬・生活衛生局, “「ハーボニー配合錠」偽造品流通事案と国の偽造医薬品対策について,” *医薬品・医療機器等安全性情報,* 第 巻 350, p. 3, 2018.

[79] FDA, “Drug Supply Chain Security Act (DSCSA),” 22 May 2019. [オンライン]. Available: https://www.fda.gov/drugs/drug-supply-chain-integrity/drug-supply-chain-security-act-dscsa. [アクセス日: 28 Mar 2020].

[80] FDA, “Drug Supply Chain Security Act Resources for State Officials,” 3 Sep 2019. [オンライン]. Available: https://www.fda.gov/drugs/drug-supply-chain-security-act-dscsa/drug-supply-chain-security-act-resources-state-officials. [アクセス日: 28 Mar 2020].

[81] Chronicled, “Chronicled and The LinkLab Announce The MediLedger Project, a Revolutionary Blockchain-backed System to Safeguard the Pharmaceutical Industry,” 21 Sep 2017. [オンライン]. Available: https://www.prnewswire.com/news-releases/chronicled-and-the-linklab-announce-the-mediledger-project-a-revolutionary-blockchain-backed-system-to-safeguard-the-pharmaceutical-industry-300522426.html. [アクセス日: 28 Mar 2020].

[82] MediLedger Project, “The MediLedger Project 2017 Progress Report,” Feb 2018. [オンライン]. Available: https://assets.chronicled.com/2017-MediLedger-Progress-Report.pdf. [アクセス日: 28 Mar 2020].

[83] MediLedger Project, “MediLedger 2018 Progress Report,” [オンライン]. Available: https://assets.chronicled.com/2018-MediLedger-Progress-Report.pdf. [アクセス日: 28 Mar 2020].

[84] MediLedger, “FDA DSCSA Pilot Project,” [オンライン]. Available:

https://www.mediledger.com/fda-pilot-project. [アクセス日: 28 Mar 2020].

[85] FDA, “DSCSA Pilot Project Program,” 22 May 2019. [オンライン]. Available: https://www.fda.gov/drugs/drug-supply-chain-security-act-dscsa/dscsa-pilot-project-program. [アクセス日: 28 Mar 2020].

[86] 日本経済新聞　電子版, “日通、ブロックチェーンで偽造品排除　物流に 1000 億円,” 9 Mar 2020. [オンライン]. Available: https://www.nikkei.com/article/DGXMZO56545270Y0A300C2MM8000/. [アクセス日: 22 May 2020].

[87] 厚生労働省, “厚生統計要覧（平成 30 年度）,” [オンライン]. Available: https://www.mhlw.go.jp/toukei/youran/index-kousei.html. [アクセス日: 28 Mar 2020].

[88] 一般社団法人 日本フランチャイズチェーン協会, “ＪＦＡコンビニエンスストア統計調査月報 ２０１８年３月度,” 20 Apr 2018. [オンライン]. Available: https://www.jfa-fc.or.jp/particle/70.html. [アクセス日: 28 Mar 2020].

[89] ブロックチェーン北海道イノベーションプロ グラム, “ブロックチェーンを活用した医薬品の デッドストック販売プラットフォーム PoC [Phase 1] 報告書,” 12 Oct 2017. [オンライン]. Available: https://blockchain-jp.com/wp-content/uploads/2017/11/drugPoC_Report_F1.1.3_BHIP.pdf. [アクセス日: 28 Mar 2020].

[90] 一般社団法人ブロックチェーン北海道イノベーションプログラム（BHIP）, “ブロックチェーンを活用した医薬品の デッドストック販売プラットフォーム PoC [Phase 2]報告書,” 10 Oct 2018. [オンライン]. Available: https://blockchain-jp.com/wp-content/uploads/2018/10/drugPoC_Report_F2.0.1_BHIP.pdf. [アクセス日: 28 Mar 2020].

[91] PharmaLedger: Blockchain Enabled Healthcare, “PharmaLedger: Blockchain Enabled Healthcare,” [オンライン]. Available: https://pharmaledger.eu/. [アクセス日: 22 May 2020].

[92] 水島洋, “ブロックチェーンによる健康医療統合プラットフォームをめざして,” *JAPIC NEWS,* 第 巻 424, p. 2, 8 2019.

[93] Nordic Institute for Interoperability Solutions, “YEARBOOK 2018,” 2019.

[94] BLOCKCHAIN.COM, “Hash Rate,” [オンライン]. Available: https://www.blockchain.com/ja/charts/hash-rate?timespan=all&scale=1. [アクセス日: 28 Mar 2020].

[95] World Wide Web Consortium, “A Primer for Decentralized Identifiers - An introduction to self-administered identifiers for curious people,” 19 Jan 2019. [オンライン]. Available: https://w3c-ccg.github.io/did-primer/. [アクセス日: 28 Mar 2020].

[96] 末松誠, “ダイナミックコンセントについて,” 28 Jun 2019. [オンライン]. Available: https://www.kantei.go.jp/jp/singi/kenkouiryou/genome/dai14/siryou4.pdf. [アクセス日: 28 Mar 2020].

[97] 木村和子, “医薬品の適正流通（ＧＤＰ）ガイドライン,” Dec 2018. [オンライン]. Available:

https://www.mhlw.go.jp/content/11120000/000466215.pdf. [アクセス日: 28 Mar 2020].

[98] G. Walker, “learn me a bitcoin,” [オンライン]. Available: https://learnmeabitcoin.com/guide/target. [アクセス日: 1 Mar 2020].

[99] BLOCKCHAIN.COM, “Average Number Of Transactions Per Block,” [オンライン]. Available: https://www.blockchain.com/ja/charts/n-transactions-per-block?timespan=all. [アクセス日: 28 Mar 2020].

[100] 一般社団法人 日本ブロックチェーン協会, “「ブロックチェーンの定義」を公開しました,” 3 Oct 2016. [オンライン]. Available: https://jba-web.jp/news/642. [アクセス日: 27 Apr 2020].

[101] AXA, “AXA goes blockchain with fizzy,” 13 Sep 2017. [オンライン]. Available: https://www.axa.com/en/newsroom/news/axa-goes-blockchain-with-fizzy. [アクセス日: 1 Mar 2020].

日本製薬工業協会 医薬品評価委員会 データサイエンス部会
2019 年度タスクフォース 1 「新しい技術や概念の解説」サブチーム 4 「ブロックチェーン」

執筆者・タスクフォースメンバー

氏名	所属会社	執筆箇所
新井 賢太郎	ノバルティスファーマ株式会社	1.6, 1.8.1, 2.2.1-2
伊藤 圭輔	ファイザーR&D 合同会社	1.1, 1.3, 1.5, 1.7.9, 1.8.3-5, Column 1, 3
奥 玲子*	帝人ファーマ株式会社	1.7.7, 1.7.10-12, 2.1.4-5
田中 拓海	エーザイ株式会社	1.2, 1.4, 1.7.1-6, 1.7.8, 1.7.13, 1.8.2, 2.1.1-3, 2.1.5-7, 2.2.3, 2.3, 2.4, Column 2

*：2020 年 3 月まで

担当副部会長

グラクソ・スミスクライン株式会社　内海 啓介
大日本住友製薬株式会社　土屋 悟

レビュアー

サノフィ株式会社　加藤 智子
エーザイ株式会社　酒井 弘憲
ファイザー株式会社　土綿 慎一
塩野義製薬株式会社　藤原 正和
中外製薬株式会社　山本 英晴
執筆者所属各社 御協力者のみなさま