The Journal of Japanese Operations Management and Strategy, Vol. 12, No. 1, pp. 54-82, 2022

ブロックチェーンの再考：暗号化通貨からスマートコントラクトの応用へ

崔宇（追手門学院大学）

概要:
産業界やサプライチェーンの分野において，自律分散型のシステム・パラダイムの象徴であるブロックチェーンに対する関心と期待がますます高まっている．一方，新しい経営システム・アーキテクチャとして捉え，ブロックチェーンが如何に作動し，企業のビジネスプロセスや日々の業務運営にどのように変革をもたらすかについて具体的に説明する文献は少ない．本研究は，ブロックチェーン技術が誕生してから約10年が経った今，そのメカニズムと基幹技術について様々な領域の文献レビューを通して，ブロックチェーンの3つの発展段階におけるそれぞれの代表例を取り上げ，ビットコイン，イーサリアムとHyperledger Fabricの各々の作動原理を分析する．オペレーションズ・マネジメントの視点から，それらの特徴や現行のシステムにもたらしうる影響と変化について，図式化しながら詳細に説明する．また，ブロックチェーンのエッセンスとも言えるコンセンサスアルゴリズムについて，ブロックチェーンのメインフレームワークであるパブリックチェーン，プライベートチェーンとコンソーシアムチェーンにそれぞれ適合したアルゴリズムを紹介する．さらに，ビジネスプロセスやサプライチェーンにおける適用シナリオと実例について解説する．

キーワード:ブロックチェーン，スマートコントラクト，コンセンサスアルゴリズム

1. はじめに

近年のデジタル技術の進歩により，IoTやモバイルコンピューティングといった機械同士の相互作用による活動が活性化しており，暗号化通貨の誕生によって現実世界の個人間における価値交換も実現可能となった（Swan, 2015; Tapscott and Tapscott, 2017）．一方，産業界において，最先端なICTの利活用をベースにインダストリー4.0やインダストリアル・インターネット環境の推進と構築が着々と実施されると同時に，組織間の情報共有や信頼メカニズムの限界が改めて明らかになった（Hofmann and Rüsch, 2017; Xu et al., 2018）．つまり，今日の経営環境は不確実性が増し激変している中，今までの中央集権型，あるいはクライアント／サーバー（C/S）のシステム・アーキテクチャを中心に，実行してきたビジネスモデルは不発になり，新たな有効かつレジリエントなシステム・パラダイムへのシフトが求められている．そこで，ビットコインといった暗号化通貨の基盤技術として注目されるようになったブロックチェーン技術の登場により，自律分散型システム・アーキテクチャが構築され，透明性・安全性が高くトラストレス（Trustless）のビジネス環境が実現されるため，今日の企業経営やサプライチェーンのDX変革とレジリエンス強化が期待可能になった（Wang et al., 2019）．

しかしながら，今までのブロックチェーンの文献では，もっぱら暗号化通貨の仕組みについて説明したり，金融や農業といった特定分野におけるブロックチェーン技術の適用事例を分析したりするものが多く，ブロックチェーンのメカニズムを導入することにより，企業のビジネスプロセス全般にどのような変化をもたらすのかについて，システマティックに説明するものが少ない（Angrish et al., 2018）．とりわけ，ビットコインが代表とするブロックチェーン1.0の時代から，イーサリアムやスマートコントラクトの導入など新たなランドマークが示されたブロックチェーン2.0の時代を経て，今日のHyperledge FabricやEOSといった様々なブロックチェーンの応用を開発するためのプラットフォームが次々と登場するブロックチェーン3.0の時代に至るまで，具体

的にどのようなメカニズムのパラダイムシフトが行われているのか，それによって，企業のビジネスプロセスや業務運営にいかに変革をもたらしうるのかについて解説する文献は殆どなかった.

本論文では, 上述の背景を踏まえ, ブロックチェーン技術が誕生してから約10年が経ったいま，そのメカニズムと基幹技術について様々な領域の文献レビューを通して，前述したブロックチェーンの三つの発展段階におけるそれぞれの代表例を取り上げ，ビットコイン，イーサリアムとHyperledger Fabricの各々の作動原理を分析し，オペレーションズ・マネジメントの視点から，それらの特徴や現行のシステムにもたらしうる影響と変化について，図式化しながら詳細に説明する．また，ブロックチェーンのエッセンスとも言えるコンセンサスアルゴリズムについて，ブロックチェーンのメインフレームワークであるパブリックチェーン，プライベートチェーンとコンソーシアムチェーンにそれぞれ適合したものを紹介しながら，ビジネスプロセスやサプライチェーンにおける適用シナリオと実例について解説する．

以下では，まずブロックチェーンの発展軌跡を明確にするため，3つの発展段階に沿って，ブロックチェーンの約10年間の発展について簡潔に述べる．また，今日のブロックチェーン・メカニズムに至るまで，徐々に形成された3つのメインフレームワークを紹介し，ブロックチェーン発展の全体像について提示する．

1.1. ブロックチェーンの三つの発展段階

近年，ビットコインに代表される暗号化通貨の急速な発展に伴い，ビットコインの基盤であるブロックチェーン技術はますます注目を集めている（Chang et al., 2020）．ブロックチェーン技術の凄まじい進歩により，匿名の参加者は信頼できる第三者組織（Trust Third Party：TTP）に依存せずに価値を移転できるため，ブロックチェーンは次世代インターネットとも呼ばれ，その適用領域は暗号化通貨から金融，医療，IoT，サプライチェーンなど広く展開されている（Casino et al., 2019）.

ブロックチェーンは，分散型データストレージ，P2P通信，コンセンサスアルゴリズム，非対称暗号化技術，スマートコントラクトなどの既存技術を適用させ，自律分散型，マルチパーティメンテナンス，トレーサビリティ，改ざん困難性や透明性などの特性を持つ（Lo et al., 2021）．ビットコインの登場以来，ブロックチェーン技術は継続的に開発され，その発展プロセスは3つの段階に分けられる．

1.1.1. ブロックチェーン1.0

ビットコインに代表されるブロックチェーン1.0の段階は，現実世界での暗号化通貨の流通／決済を可能とし, 徐々にその存在を確立していった. ブロックチェーン技術を使用することにより，互いに信頼していない人同士であっても，TTPの介入なしに，ビットコインを使用して直接に支払いを行うことができるようになった（Nakamoto, 2008）．ビットコインとそれに続くライトコイン，ドージコインなどの暗号化通貨の登場により，個人間での海外送金や随時取引が可能となり，インターネット上で“価値”が流通するようになった.そのため暗号化通貨は従来の金融システムに大きな衝撃を与えた．一方，この時期は技術的な実験段階であり，ビジネスへの適用はまだ始まっていなかった.

1.1.2. ブロックチェーン2.0

ブロックチェーン技術に対する研究・開発が深まるにつれ，イーサリアムに代表されるブロックチェーン2.0の技術や実例が登場した（Buterin, 2014）．本段階では，暗号化通貨をベースに，スマートコントラクトを組み込むことによって，開発者が本来の手動操作を，ブロックチェーン上でプログラムを記述するというスマートコントラクトによる実行に置き換えることが可能となり, 情報処理の安全性, 公平性と透明性がより保たれることになった. スマートコントラクトは，イーサリアムのネットワーク上で実行可能なプログラムである．イーサリアムのユーザーは，設計済みのビジネスロジックをスマートコントラクトに書き込み，イーサリアムにデプロイし，イーサリアム仮想マシン（EVM）によって自動的に呼び出して実行する．イーサリアムでスマート

コントラクトを配置して呼び出すには，暗号化通貨で決済される料金を支払う必要がある．スマートコントラクトは，複雑なビジネスロジックを実現し，ブロックチェーンの適用範囲を拡大することにより，金融領域やデジタル資産の公証手続き（NFT）など，様々なビジネスシナリオにブロックチェーン技術を適用させることがするようになった（Raman and Raj, 2021）.

1.1.3. ブロックチェーン3.0

ブロックチェーン3.0の段階では，ブロックチェーン2.0のスマートコントラクトによるプログラム可能な特性を継続しながら，金融以外の幅広い分野に拡張するようになった．ヘルスケア，教育，ガバナンス，モノのインターネット，さらに，サプライチェーンの関連分野で広く応用されており，ブロックチェーンは“BaaS：Blockchain as a Service”という理念の下，様々なニーズある領域において，技術駆動型イノベーションを促進するようになった（Song et al., 2021）. 例えば，ブロックチェーンの匿名性を利用した匿名投票の分野，ブロックチェーンのトレーサビリティを活用したサプライチェーンの分野，モノのインターネット，スマート農業，スマートメディカル，スマートシティなど多くの分野が挙げられる（Khanna et al., 2021）．ただし，ブロックチェーンの時代の括り方は完全に分離されているわけではなく，並列カップリングの遷移になっていることを注目すべきであろう.

ブロックチェーンは，暗号化に基づく分散型台帳として，自律分散化，トラストレス（Trustless），P2Pネットワーク，改ざん困難などの特性により，当初から注目集まった（Klems et al., 2017）. また，コンセンサスアルゴリズムの採用は，ビザンチン将軍問題を解決するための新しいソリューションを提案し，互いに信頼性のないノード間でネットワークを介して安全に取引できるようになる．分散型アプローチによって実行または保存されるスマートコントラクトのスクリプトは，TTPがない場合でもプロトコルが正常に実行されることを保証し，ブロックチェーンシステムの自律分散化の実現を後押している.

ただし，多くのメリットが挙げられると同時に，あらゆるビジネスシナリオでブロックチェーン技術を導入する際，データスループットの限界や集中化と分散化のトレードオフなどが最大の障害になりつつある．これらの問題を解決するために，ブロックチェーンのシステム・アーキテクチャは徐々に下記の3つのメインフレームワークに形成されるようになった.

1.2. パブリックチェーン，プライベートチェーン，コンソーシアムチェーン

ブロックチェーンは，当初，システムのセキュリティを確保するためにSybil攻撃に抵抗するPoW（Proof of Work）のメカニズムで知られていた．しかし，莫大なコストやデータ処理速度を犠牲にするという前提のパブリックチェーンは，大量のデータ負荷がますます高まっている現在，実際のユーザビリティに支障を来すことが明らかになっている（Serdyuk, 2015）．それゆえ，ユーザビリティを担保しながらSybil攻撃に対抗するために継続的な改善を積み重ねた結果，プライベートチェーンとコンソーシアムチェーンのフレームワークが派生された.

パブリックチェーンでは，すべてのユーザーがネットワークアクセス，読み取り，書き込みのプロセスに参加し，すべてのノードが共にデータを保存し，システムのセキュリティを確保できる．ただし，分散化はトランザクションスループットを犠牲にして実現されるため，チェーンデータのアップロード速度とスマートコントラクトの呼び出し（Call）速度に大きな影響が及ぶ．コンセンサスアルゴリズムでは，作業量の証明（Proof of Work，PoW）や資産保有による証明（Proof of Stake，PoS）などがよく使用され，コンピューティングパワーのサポートには必然的にリソースの消費が伴うため，マイナー（Miner）に記帳作業を完了するように励ますことは必須である（Zheng et al., 2018）．代表的な実例には，ビットコイン，イーサリアムやEOS（Enterprise Operation System）など挙げられる.

パブリックチェーンとは異なり，プライベートチェーンのアプリケーションシナリオは主に組織内にあり，そのネットワークの読み取りおよび書き込みの権限とコンセンサスプロセスへの参加は大幅に制限されている（Bozic et al., 2016）．データのプライバシーを確保するために，参加している各ノードは厳格な審査を受ける必要がある．アイデンティティの可視性とシステムのプ

ライベート化により，ネットワークは悪意のあるノードの存在を考慮する必要がなくなる．したがって，ビザンチン障害耐性（Byzantine Fault-Toleran, BFT）アルゴリズムを使用して，ノードの悪意のある行動を検出したり，ノードのダウンタイムによる損失を回避したりできる（Vizier and Gramoli, 2020）．プライベートチェーンのアプリケーションシナリオの特性により，マイナーは追加の報酬なしでデータ記録作業を完了するための十分なモチベーションを持つことができる．パブリックチェーンと比較して，高速のデータスループットは，組織の実際のニーズをより適切に保証できる．代表的な実例はマルチチェーン（Multichain）などである（Oliveira et al., 2019）.

コンソーシアムチェーンの適用シナリオは，複数の組織で構成される企業の連合体である．ユーザーの対象範囲はパブリックチェーンとプライベートチェーンの間にあり，許可されたノードのみが読み取りと書き込みができるセミ分散型フレームワークである（Elisa et al., 2019）．プライベートチェーンと同様に，データの機密性は依然としてチェーンが主に考慮する要素の1つであるため，コンソーシアムチェーンのノードのアイデンティティを検証することも避けられない．コンソーシアムチェーン内において，一般ノードと記帳（マイニング）ノードは設置され，前者はデータ生成とダイレクトクエリ作業を担当し，後者はネットワークデータの検証とチェーンへのアップロードを担う．データのプライバシー，セキュリティ，監査などの要素を追加すると，コンソーシアムチェーンは実用的ビザンチン障害耐性（Practical BFT，PBFT）や委任型の関与の証明（Delegated Proof of Stake，DPoS）などのアルゴリズムを使用する傾向が強くなる（F. Wang et al., 2021; Saad and Radzi, 2020）．インセンティブメカニズムは，システムのビジネス特性に応じて追加または削除することができ，パブリックチェーンと比較すると，当該ネットワークのデータスループットは，実際の運用上のニーズにより一致している．代表的な実例には，Hyperledger Fabric，Enterprise Ethereum Alliance（EEA），R3 Blockchain Alliance（Corda）などがある（Zhong et al., 2020）.

本論文では，ブロックチェーンの発展3段階を代表する実例であるビットコイン，イーサリアムとHyperledger Fabricの特徴などを図式化することによって，それぞれの仕組みやビジネス適用領域などが明確になる．また，ブロックチェーンの主なパターンである，パブリックチェーン，コンソーシアムチェーンとプライベートチェーンのそれぞれの特性に適したPoW，PoS，PBFT，DPoSといったコンセンサスアルゴリズムを分析し，それらのビジネスプロセスや企業の業務運営における役割を明らかにする．ただし，プライベートチェーンは主にローカルのブロックチェーン構築やスマートコントラクトの発行前の動作試験などに使われるため，本稿では，コンセンサスアルゴリズムについて，主に上記のパブリックチェーンとコンソーシアムチェーンに適したもののみ詳述する．さらに，今日の企業経営およびビジネスプロセスの変革にいかにブロックチェーンのメカニズムを適用できるかについて，いくつかの応用研究の事例を説明する．

2. ビットコインの登場とブロックチェーンのジェネシス・メカニズム

ブロックチェーンの概念は，2008年にナカモトサトシという“人物”が投稿した論文“Bitcoin: A Peer-to-Peer Electronic Cash System”に端を発している（Nakamoto, 2008）．この論文では，改ざん困難な暗号化通貨であるビットコインについて説明しているが，ビットコインの発行と流通を支えているのがブロックチェーンである．

ビットコインのブロックチェーンは特別なチェーン構造になっており，TTPの承認が除かれても分散型の匿名決済を完了できるシステム・アーキテクチャであるため，後続の多くのブロックチェーン・プラットフォームの基盤となっている．また，ブロックチェーンのネットワーク基盤として分散型P2Pネットワーク（Peer-to-Peer Network）は機能している．従来のC／Sネットワーク（Client／Server Network）とは異なり，P2Pネットワークには中央サーバーがなく，ネットワークに参加しているすべてのノードが同時にクライアント（Client）とサーバー（Server）の両方として機能している（Ismailisufi et al., 2020）．つまり，すべてのノードがリクエストを送信できると同時に，他のノードから送信されたリクエストに応答することも可能である．ブロック

チェーンネットワークでは，ブロックはP2Pネットワークを介して送信される[1].

2.1. ブロックチェーンの運営メカニズム

ブロックチェーンの基本概念を下記のように簡潔に紹介する（Sabry et al., 2019).

トランザクション（Transaction)：ブロックチェーンシステムにおいて，実行されるたびにハッシュ値を生成するすべての操作を指し，これらのトランザクションのハッシュ値はブロックチェーンに格納される.

ブロック（Block)：各ブロックには，前のブロックで記録されなかった最新のデータセットの一部またはすべてが永続的に含まれる．これらのデータセットは，ブロックと呼ばれるファイルとして記録される.

チェーン（Chain)：暗号化技術を介して前後のトランザクションデータブロックを相互に接続することによって形成されるチェーンであり，増え続けるレコードのリストでも言える.

上記の概念に基づいて，ブロックチェーンは，ブロックを最小単位とし，時系列で一方向に接続されたチェーンデータ構造として定義できる．そして，コンセンサスアルゴリズムと暗号化技術を用いて，分散型ネットワーク内のノードが共有する情報の一致性と安全性を保つ（Puthal et al., 2018).

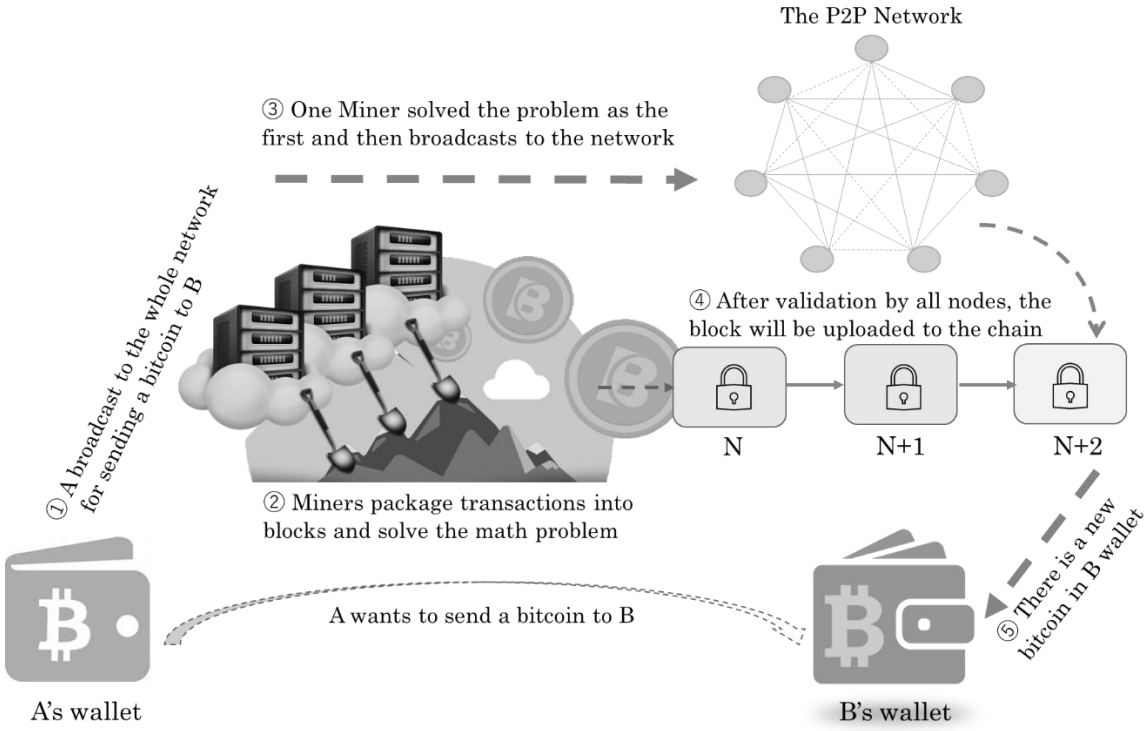

図 1 – 簡略化したブロックチェーンの運営メカニズム（著者作成）

上記の概念と定義によれば，ブロックチェーンの運営メカニズムは次のように要約できる（図1を参照）.

まず，ユーザーがP2Pネットワーク内のノードに新しいトランザクション（ユーザーAのウォレットから1ビットコインをユーザーBのウォレットに送金する）をブロードキャストし，ブロード

[1] 例えば，ビットコインでは，すべてのノードのステータスは同じであり，元帳の管理にはすべての参加者の共同作業が必要になっている．ノード間の通信を通して，すべてのトランザクションが確実にブロックチェーンのネットワークにブロードキャストされ，また，処理されることを確保する．すべてのノードによって保存された元帳データを一貫性のあるものにすることができるのは，「共有」と「同期」の考え方によるものである.

キャストされたコンテンツを受信するノード（マイナー）がトランザクションデータセットを検証する．検証に合格すると，トランザクション情報がブロックにパッケージ化される．次に，すべての受信ノード（マイナー）がこの新ブロックに対してコンセンサスアルゴリズムを実行し，合意に達した後，メインチェーンに正式にリンクし，保存される（崔，2022）．ノードは常に最長のブロックチェーンをメインチェーンと見なし，その後に生成されるブロックは最長のチェーンに基づいて拡張し続ける．

2.2. ハッシュ関数とマークルツリー

一方向の暗号化アルゴリズムとして，ハッシュ関数は平文をハッシュ値に処理できると同時に，このプロセスを逆にすることはできない．つまり，処理後に取得されたハッシュ値から元のデータを推定することは不可能である．

ハッシュ値は1つの元の平文にしか対応できず，ハッシュ値が複数の異なる平文に対応することはない（C, 2018）．元の平文がわずかに変化する限り，計算結果は完全に変化するのである．ハッシュ関数が上述の特殊な機能があるため，データ整合性検証，データ暗号化，およびその他のプロセスで広く使用されている．

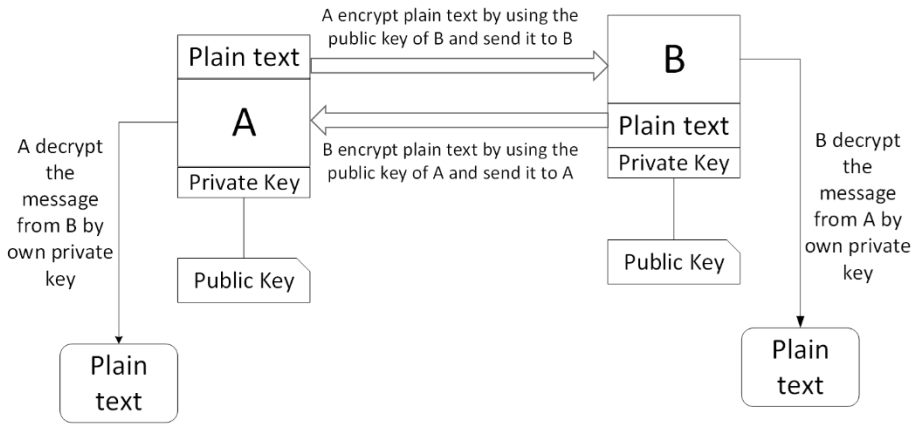

図 2 – 非対称暗号化の簡易プロセス（著者作成）

また，ブロックチェーンに適用されている非対称暗号化技術の最大の特徴は，鍵ペアの違いというところである．ユーザーの鍵ペアには，公開鍵と秘密鍵の2つの部分があり，図2に示すように，相互に暗号化と復号化ができる．公開鍵は署名に使用され，秘密鍵は検証に使用され，その逆も同様である．名前が示すように，秘密鍵はその人しか知らずに，公開鍵は完全に公開される．ブロックチェーンの暗号化コンポーネントでは，コンテンツは楕円曲線暗号化アルゴリズム（Elliptic Curve Cryptography：ECC）によって暗号化される．これは，楕円曲線の範囲内の代数的構造に基づいて作成されたアルゴリズムである（Safieh et al., 2020）．また，デジタル署名や偽造防止のランダムコード生成によく使用される．

マークルツリー（Merkle Tree）は，1979年にRalph C. Merkleによって提案されたが，一種のハッシュツリーでもあり，データのハッシュ値をバイナリツリーの形式で表すデータ構造である（Gamage et al., 2020）．マークルツリーの構造は図3に示しているように，最下層のトランザクションデータを除いて，すべてのノードはハッシュ関数処理の結果であり，ルートノードは32バイトのハッシュ値である．ビットコインは最も単純なバイナリのマークルツリーを使用している．各ブロックには独立したマークルツリーとなっており，ツリーのリーフノードはトランザクションのハッシュ値である[2]．

マークルツリーのルートノードは，リーフノードのハッシュ値を記録し，元データ（トランザ

[2] ビットコインはダブル SHA256 ハッシュを使用している．

クションデータ）を含まない．これによって，データの検証と識別の複雑さが軽減され，ブロックチェーンの運用効率を向上させる効果が期待できる．言い換えれば，マークルツリーでは，任意のブランチを検証できるため，すべてのブロックチェーンのノードを実行せずにデータを検証できる．即ち，簡易支払い検証（Simple Payment Verification: SPV）である（Dai et al., 2018）．ブロックヘッダー内の前のブロックのハッシュ値は，前のブロック内のすべてのトランザクション情報を伝達し，現在のブロックのハッシュ値は，ブロック生成の段階で検証されたすべてのトランザクション情報によって構成される[3].

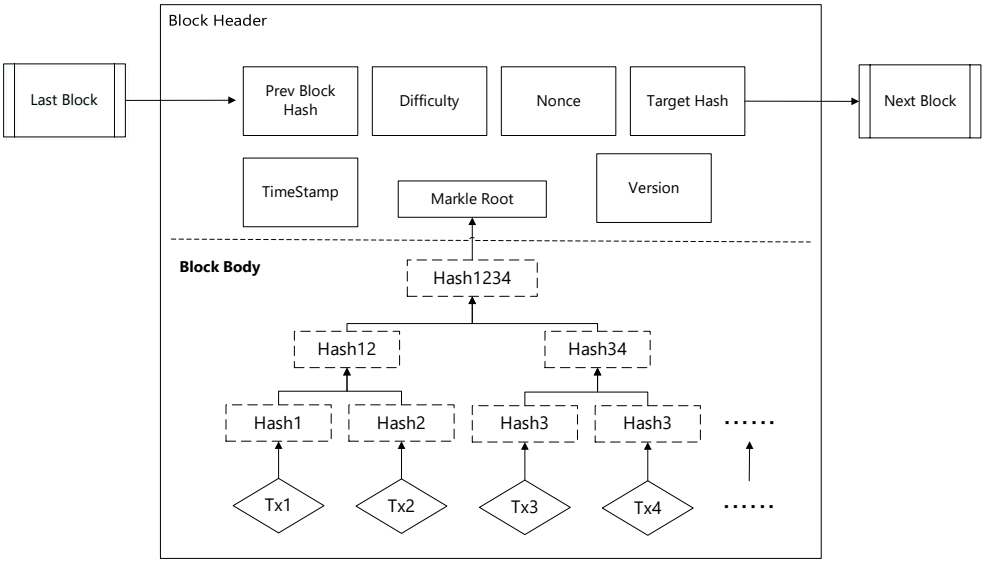

図 3 – ビットコインのブロック簡易図[4]（著者作成）

2.3. ビットコインのトランザクションの実行

ビットコインシステムでは，ユーザーIDとして，ビットコインアドレスは一連の一方向的なハッシュ関数を介してユーザーの公開鍵から取得され，1人のユーザーが複数のトランザクションアドレスを持つことができる．ビットコインシステムでは，トランザクション中心のモデルが採用されており，単一のトランザクションが複数のインプットとアウトプットを持つことができ，複数のアドレスに関連付けることができる（Belotti et al., 2019）．トランザクションのインプットは，未使用のトランザクションアウトプット（Unspent Transaction Output, UTXO）とセットで構成され，その合計金額はトランザクションの支払い金額を下回ってはならない．トランザクションのインプット側のユーザーは，お釣りを受け取るための新しいアドレスを指定できる．お釣りを受け取るために使用されるアドレスは，お釣り用アドレス（change address）とも呼ばれる．また，ビットコインには口座残高の概念がなく，ユーザーのウォレットのUTXO金額の合計でユーザーの残高を計算できる．

ブロックチェーンの独自のチェーン構造により，ジェネシスブロック（Genesis Block）から最新のブロックまでのすべての情報を完全に記録でき，暗号化技術の適用により，データが改ざん

[3] ブロックヘッダーには，現ブロックのバージョン番号（Version），前ブロックのハッシュ値（Prev-block Hash），現ブロックの作業量の証明（PoW）に使用されるターゲット難易度（Difficulty），および PoW に使用されるランダム数（Nonce）や現ブロックの生成タイムスタンプ（Timestamp）などある．最終的に，隣接するブロックは，端から端まで接続されてつなぎ合わせた緊密なチェーン・アーキテクチャを形成し，各ブロックはジェネシスブロック（Genesis Block）以降のすべての情報を網羅することになる．ブロック内の情報が変更されると，現ブロックのハッシュ値が変わるだけでなく，後続のすべてのブロックのハッシュ値も変わることになる．したがって，前ブロックからのフォークによる新しいブロックチェーンが構築されずに，ネットワーク全体による承認も得られない限り，ブロック内の情報が改ざんされることはないと言える（Aruna Sri and Bhaskari, 2018）．

[4] Tx は Transaction の略である．

困難であることが保証される．ブロックチェーンには，トレーサビリティや安全な情報開示などのメリットがあり，ブロックチェーンに保存されているすべてのデータをユーザーの端末で確認できる（Bigini et al., 2020）．一方，デジタル技術の発展とブロックチェーン技術の進化により，その適用領域は仮想通貨から金融，IoT，医療，その他の様々な分野に拡大した．スマートコントラクトなどの技術との融合により，ブロックチェーンはトランザクションレコードに限定されることなく，プリセットコマンドがアクティブ化されたときに自動スクリプトを介してインテリジェントにコントラクトを生成と保存することができる．次の章では，スマートコントラクトの概念とブロックチェーンとの融合により誕生した，“世界のコンピュータ”と称するイーサリアムが誕生と，その運営メカニズムおよびイーサリアムをベースに生成されるDAppsなどについて詳述する．

3. イーサリアムとスマートコントラクト

ビットコインは分散型仮想通貨の先例を創造した．ビットコインシステムは，マイニングというインセンティブメカニズムと通貨発行の関連付けを生かし，特殊な分散型ネットワークであるブロックチェーンに基づき，コンセンサスアルゴリズム（PoW）を使用してトランザクションの確認を行い，ネットワーク上でビットコインを安全に転送することでTTPのサポートなしに，お互いに信頼関係がない人々の間で通貨の交換を実現した．ブロックチェーン技術がビットコインで成功を収めた後，Vitalik Buterinは2014年12月にビットコインに基づいてイーサリアム（Ethereum）の概念を提案した（Buterin, 2014）．イーサリアムでは，ビットコインの仮想通貨機能を継承するだけでなく（イーサリアム上で流通する仮想通貨はイーサ（Ether）と呼ばれる），チューリング完全（Turing complete）プログラミング言語を提供することにより，スマートコントラクトをブロックチェーンシステムに適用させることができた（Hu et al., 2021）．

3.1. イーサリアムのブロック構造

ブロック生成の効率とノード内のアカウント状態データを検索する機能を向上させるために，イーサリアムでは，マークルルートを計算するときにマークルパトリシアツリー（Merkle Patricia Trie）を使用している（Qin et al., 2020）．イーサリアムとビットコインのブロックは同じトランザクションデータを持っているが，イーサリアムの状態データは頻繁に変化し，生成されるデータの量は比較的に多くなる．つまり，ビットコインの場合，新しいブロックの平均生成時間は10分であるため，フォークの確率は高くないが，イーサリアムの新しいブロックの平均生成時間は15秒である．また，ブロックチェーンのコンセンサスアルゴリズムとネットワーク運営メカニズムなどの制限により，15秒以内に，新しいブロックが他のノードによって検証および認可される前に，他のノードが同じブロック位置でさらに新しいブロックをマイニングし，それによって頻繁にフォークを生成する場合が考えられる．

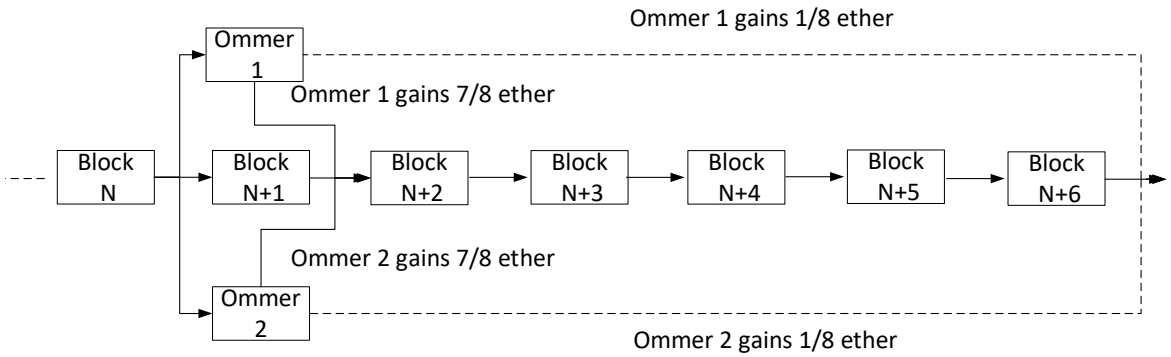

図 4 – GHOSTプロトコルの作動原理（著者作成）

イーサリアムのマイニングの公平性を反映し，イーサリアムネットワークの安定した運用を維持するために，イーサリアムでは，GHOST (Greedy Heaviest Observed Subtree) プロトコルを採用して，生成したフォークをできるだけ早く結合するようにした．GHOSTプロトコルはメインチェーン選択メカニズムであり，そのアイディアは“利益平準化 (profit equalization)”の原則に基づき，新しいブロックをマイニングしたすべてのノードが恩恵を受けるという (Ritz and Zugenmaier, 2018)．図4で示すように，ブロックN＋1が，ネットワークの場所，帯域幅，およびコンピューティングパワーといった点で絶対的な優位を持つマイニングプールであると想定する．当該ノードがメインチェーンの特定のブロック位置からマイニングを開始すると，ブロックを生成する可能性が高いため，ブロックの記帳権を獲得しやすく，そこから利益を得られる．ただし，ブロックチェーンネットワーク内の他のノードがマイニングに積極的に参加することを奨励するために，GHOSTプロトコルでは，ブロックN＋1が，参照によって同じ場所で新しいブロックをマイニングした他のマイナーに，相応する報酬を与えることを規定している．GHOSTプロトコルは，メインチェーンの唯一性を効果的に維持し，永続的なフォークを防ぎ，ブロックチェーンシステムの安定した運用を確保する．

フォークは，トランザクションの不確実性とシステム操作の不安定性をもたらす．具体的には，常に一部のブロックは少し遅れてマイニングされるため，メインチェーンの一部として使用できないようになっている．ビットコインの場合，このようなブロックを「孤立ブロック (orphan block)」と呼び，それらを完全に破棄する．一方，イーサリアムの場合，それらを“アンクルブロック (uncle／ommer block) と呼び，後続のブロックで参照できる．アンクルブロックが後続のブロックチェーンにおいて，アンクルブロックとして参照されている (referencing) 場合，各アンクルブロックはマイナーのブロック報酬の7/8を生成する．これはアンクルブロック報酬 (uncle block reward) と呼ぶ．

イーサリアムのブロック構造は，図5に示すように，ビットコインブロックに似ている．ブロックヘッダーには，番号 (number)，親ハッシュ値 (parentHash)，マイニング難易度 (difficulty)，ステートルート (stateRoot)，ナンス (nonce)，トランザクションルート (transactionRoot)，レシートルート (receiptRoot)，タイムスタンプ (timestamp) などが含まれる．各ブロックは親ハッシュ値フィールドを介して前ブロックを指し，徐々にチェーンを形成する必要があり，マイニングノードはメインチェーンにアップロードしたブロックにタイムスタンプする責任を負っている．ステートルートは，イーサリアムネットワーク内のすべてのトランザクションアカウントによって形成されるルートハッシュ値であり，トランザクションルートとレシートルートは，それぞれブロック本体のトランザクション情報とレシート情報によって形成されるルートハッシュ値である．3つのルートハッシュ値はすべて，マークルパトリシアツリーのメカニズムに従って演算される．

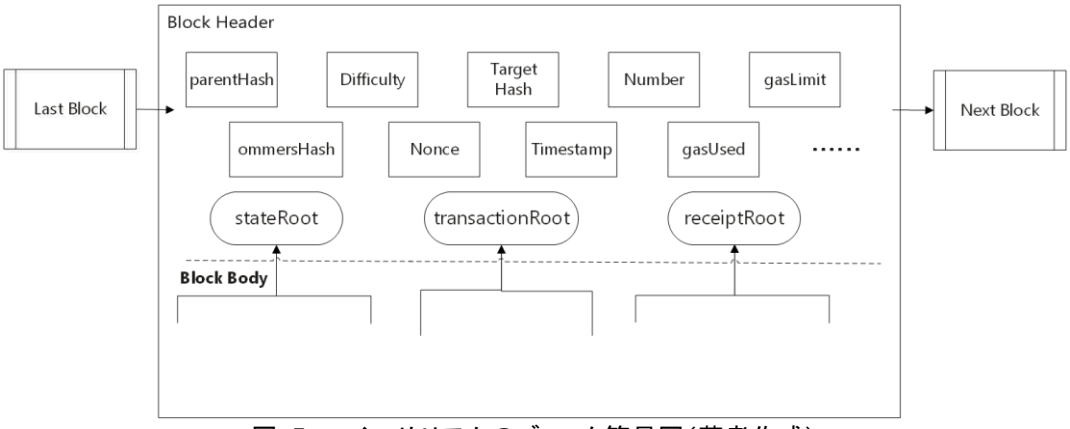

図 5 – イーサリアムのブロック簡易図（著者作成）

ビットコインのようなブロック構造では，安全性が高く確保できるが，新しいブロックの平均

生成時間は10分間であるため，実際のビジネス環境における業務運営の実態を考えると非現実的と言える．一方，イーサリアムの場合，ブロックの平均生成時間は15秒であるため，現実的なオペレーションの適用にかなり近づいている．効率的なブロック生成が確保できる一方，フォークの問題が頻繁に発生しうるが，GHOSTプロトコルやマークルパトリシアツリーなどの採用によって，本来のブロックチェーンの高い安全性と信頼性を保ちながら，現実のビジネス環境におけるオペレーションズ・マネジメントの効率性を確保することが可能になった．

3.2. スマートコントラクト

スマートコントラクトの概念を最初に提唱されたのは暗号学者のNick Szaboであったが，イーサリアムの創業者であるVitalik Buterinはブロックチェーン技術に加え，チューリング完全の機能性を付与したスマートコントラクトの設計環境を整備した．スマートコントラクトとブロックチェーンの融合により，ブロックチェーンはスマートコントラクトのプログラム可能性を利用して分散型ノード操作の複雑さを簡素化でき，他方では，スマートコントラクトがブロックチェーンの分散化メカニズムにより，トラストレスの環境下で効果的に実現できる．

イーサリアムはチューリング完全プログラミング言語[5]が組み込まれ，スマートコントラクトの概念が正式に導入された世界初のパブリックブロックチェーンとして，現在最も利活用されているスマートコントラクト開発プラットフォームである（Zinovyeva et al., 2021）．イーサリアムのスマートコントラクト開発プラットフォームとは，任意の複雑なアルゴリズムコーディングを実行できるイーサリアム仮想マシン（Ethereum Virtual Machine: EVM）のことである．イーサリアムにデプロイされたすべてのスマートコントラクトはEVMバイトコードにコンパイルされ，マイナーによってローカルで完全に分離されたEVMで実行される．ユーザーは，自分の希望に応じて，イーサリアムプラットフォーム上で暗号化通貨を含む様々なスマートコントラクトやスマートコントラクトに基づいて構築される自律分散型アプリケーション（Decentralized applications: DApps)[6]などを効率的かつ迅速に開発できる（Metcalfe, 2020）．DAppsは近年ますます注目を集めており，有名なゲームDAppsであるCryptoKittiesや非代替性トークン（Non-Fungible Token: NFT）などの発展が凄まじいものと言える（Serada et al., 2020）．イーサリアムの誕生は，ブロックチェーンとスマートコントラクトの適用環境を変え，もはや暗号化通貨に限定されず，よりマクロな金融システムを構築し，他の社会的分野に適用する機会が増えた．

スマートコントラクトの作動原理図を図6に示す．スマートコントラクトには通常，値とステータスの2つの属性があるが，コントラクトコード中に，If-ThenとWhat-Ifステートメントを使用して，契約条件と一致するトリガーシナリオとレスポンスルールが事前設定されるようになっている（Di Angelo and Salzer, 2019）．スマートコントラクトは，複数の当事者の相互合意後に，各当事者によって署名され，ユーザーが開始するトランザクションとともに送信される．また，スマートコントラクトはP2Pネットワークによって配布され，マイナーによって検証された後，ブロックチェーンの特定のブロックに保存される．ユーザーは返されたコントラクト・アドレスとコントラクト・インターフェース情報を取得した後，トランザクションを開始することでコントラ

[5] ビットコインのチューリング不完全なバイトコード言語 OP-Return に基づくビットコインスクリプトは，ブロックチェーンに適用される最も初期のスマートコントラクトと言える．OP-Return の計算能力は非常に限られているため，ループステートメントをサポートせず，基本的な計算，論理演算，検証および暗号化機能のみを実現できるため，初期のスマートコントラクトは通常，複雑なロジックを持つことはできない（Bistarelli et al., 2018）．

[6] イーサリアムのようなブロックチェーン開発プラットフォームの普及に伴い，DApps の数も急速に増加しており，ますます注目を集めている．DApps は，バックエンドを介して任意の言語で記述されたフロントエンドコードとユーザーインターフェイス（UI）を呼び出すことができる．バックエンドコードは，通常ブロックチェーンシステムにデプロイされるスマートコントラクトという．スマートコントラクトは，ロジック操作とデータストレージを取り扱っており，トランザクションを通じて DApps フロントエンドまたは複数のスマートコントラクトと相互作用する．DApps のプログラムロジックと機能が単純な場合，通常，スマートコントラクトは 1 つしか含まれない．通常，スマートコントラクトには長さの制限があるため，DApps は複数のスマートコントラクトを含めることでより複雑な機能を実現する．

クトを呼び出すことができる．

マイナーは，システムによって事前設定されたインセンティブメカニズムに動機付けられ，トランザクションを検証するために，自分のコンピューティングパワーを提供する．マイナーが契約の作成または呼び出しトランザクションを受け取った後，ローカルサンドボックス実行環境（EVMなど）でコントラクトを作成するか，コントラクトコードを実行する．コントラクトコードは，信頼できる外部データソース（Oracleと称する）とワールドステート（World State）[7]の検査情報に基づいて，現況がコントラクト・トリガー条件を満たしているかどうかを自動判断し，レスポンスルールを厳密に適用してワールドステートを更新する（Chen et al., 2020）．トランザクションが検証された後，新しいデータブロックにパッケージ化され，新しいブロックがコンセンサスアルゴリズムによって検証され，ブロックチェーンのメインチェーンにリンクされ，すべての更新が有効になる．

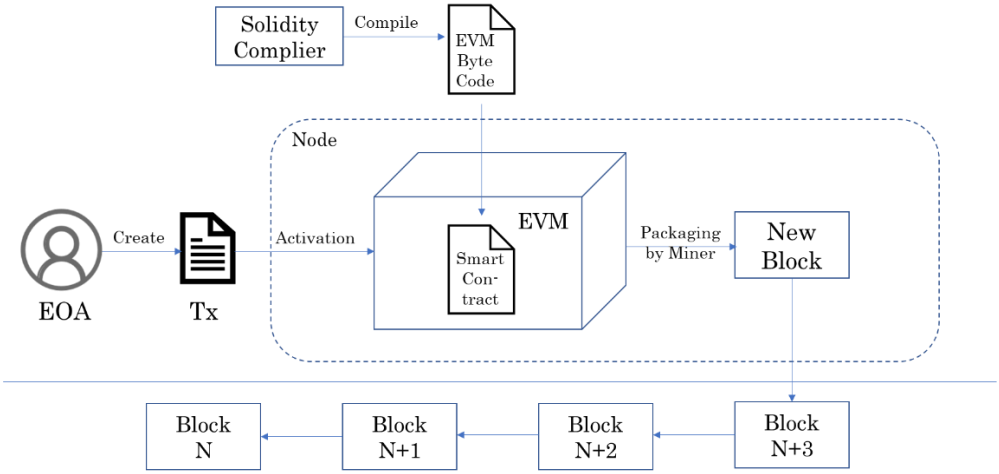

図 6 – スマートコントラクトの作動原理図[8]（著者作成）

3.3. トランザクションの実行

イーサリアムでは，グローバルにコンピューティングパワーの投入を奨励し，その使用権を合理的に割り当てるために，すべてのプログラムを実行するには，支払いが必要とされる．それはイーサリアムのトランザクションには帯域幅やストレージの消耗，コンピューティングパワーの消費などが伴うことを考慮し，悪意のあるプログラムによってシステムが制御不能になるのを防ぐためでもある．様々な運用コストがgas単位で計算され，どのプログラムフラグメントでも，ルールに従って消費されたgasの量が計算でき，完成されたトランザクションのプロポーザー（Proposer）は，すべての実行コストを支払う必要がある．トランザクションの実行中にガス切れ（Out of Gas, OOG），スタックオーバーフロー，無効な命令など異常終了が発生した場合，トランザクションは無効になり，消費されたgasは引き続きマイナーが貢献するコンピューティングリソースための報酬として使用するとされる（Liu et al., 2020）．

ビットコインのUTXOトランザクションアプローチとは異なり，イーサリアムではアカウントの概念が導入されている．イーサリアムのアカウントは，その機能と権限に応じて，外部アカウント（Externally Owned Account: EOA）とコントラクト・アカウント（Contract Account: CA）の2つに分類される（Farnaghi and Mansourian, 2020）．EOAは，ユーザーの公開鍵と秘密鍵のペアによって制御され，そのアドレスは公開鍵暗号化した後に取得される．CAは，アカウントに

[7] ワールドステートは，台帳（Ledger）の現在値を格納するデータベースである．ワールドステートを使用すると，現在値を計算するためにトランザクションログ全体にアクセスする代わりに，プログラムは台帳（Ledger）の現在値に直接アクセスできる．デフォルトでは，Ledger のステートはキー・バリューの組み合わせで表示される．

[8] EOA は外部アカウント（Externally Owned Account）の略である．Tx は Transaction の略である．

保存されているスマートコントラクトコードによって制御され，スマートコントラクトが展開されると，CAのアドレスが自動的に生成される．外部アカウントを作成するのにイーサ（Ether）を使う必要はなく，CAを作成するには，コントラクトのコンパイルを完了するために一定量のgasを支払う必要がある．EOAは秘密鍵を用いて，トークンの転送や計算の実行などのトランザクションを開始したり，トランザクション情報を他のEOAに送信したりできる．イーサリアムネットワークでは，EOAのみがトランザクションを開始可能である[9]．

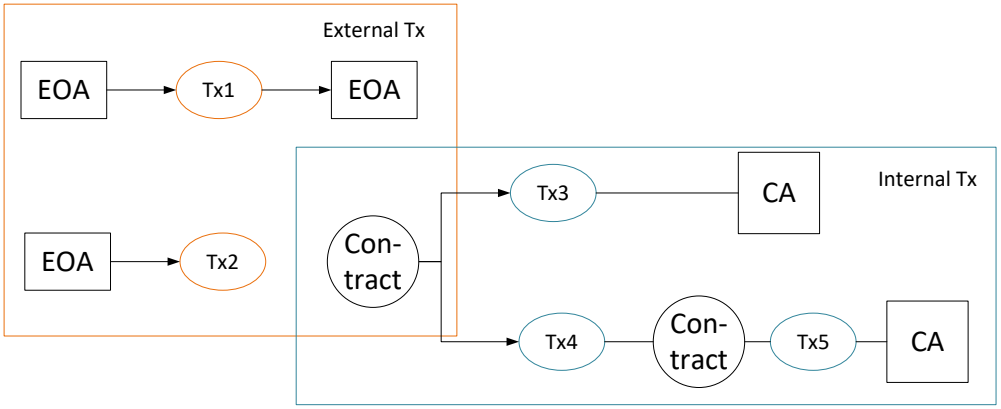

図 7 － 外部・内部トランザクションの関連性[10]（著者作成）

イーサはイーサリアムのネイティブ暗号化通貨であり，アカウント間でトランザクションまたは転送することができる．イーサリアムのユーザーは，トランザクションをプロポーザーすることでイーサを他のユーザーに転送する際，トランザクションの値フィールドは，転送されるイーサの量を示す．さらに，イーサリアムは，ブロックチェーンを些末なトランザクションや悪意のあるトランザクションから保護するために，ユーザーにトランザクション料金（gas）を支払うことを要求し，それによってリソースの浪費が回避される．トークン（Token）は，スマートコントラクトによって実現される一種の暗号化された通貨である（Grech et al., 2020）．トークンはトランザクションあるいは譲渡したり，イーサと両替したりすることもできる．

ビットコインのUTXOトランザクションアプローチでは，送金や仮想通貨の売買に限定され，一般的なビジネス環境におけるトランザクションやオペレーションの実行には，ほぼ不可能である．一方，イーサリアムの場合，アカウントという概念を取り入れているため，日常の業務や組織間のやり取りが実行可能になる．また，EOAとCAという2種類のアカウントを設けているため，例えば，サプライチェーンにおいて，まずEOAを用いて，参加するメンバーの確認や検証を行い，オペレーションやトランザクションの実行には，CAの中にあるスマートコントラクトを，一定の条件を満たせば，自動に作動させるという．それによって，オペレーションズ・マネジメントの効率性が高まり，ブロックチェーンのメカニズムを用いたため，チェーン全体の透明性と信頼性が確保できる．

---

9 トランザクションの異なるプロポーザーから，イーサリアムのトランザクションは，EOA によって開始される外部トランザクションと，コントラクトコールによってトリガーされる内部トランザクションに分けられる．図 7 は，イーサリアムの外部トランザクションと内部トランザクションの典型的な例を示している．トランザクション 1 と 2 はどちらも EOA によって開始されるトランザクションであるため，両方とも外部トランザクションである．それに対して，トランザクション 3，4 および 5 はスマートコントラクトによってトリガーされるため，3 つとも内部トランザクションである．外部トランザクションにより，多くの内部トランザクションの発生がもたらされる．例えば，トランザクション 2 では，EOA が CA を呼び出し，これにより，3 つの後続の内部トランザクションがトリガーされることになる．

10 Tx は Transaction の略である．

4. Hyperledger Fabric と EOS

スマートコントラクトは，デジタルメソッドを通してコントラクトをポットキャスト，検証および実行するコンピュータープロトコルであり，TTPなしで信頼できるトランザクションを可能にする．これらのトランザクションは追跡可能かつ逆算不可能であり，その目的は従来のコントラクトよりも優れたものを提供し，コントラクトに関連するその他のトランザクションコストが削減されることである．したがって，スマートコントラクトは，開発効率が高く，メンテナンスコストが低く，実行精度が高いため，ブロックチェーン技術と完全に適合しており，ブロックチェーン2.0の象徴としても過言ではない．

一方，スマートコントラクトをブロックチェーンと融合させることに成功したイーサリアムが継続的な発展を成し遂げると共に，企業のビジネスプロセスやサプライチェーンマネジメント(SCM) など産業型ブロックチェーンの進展がスマートコントラクトの新たな展開としてその重要性がますます増している．この章では，その代表的な事例として，ビジネスプロセスに特化したスマートコントラクト開発プラットフォームと言えるHyperledger fabricを紹介したい．また，同じく企業経営やサプライチェーンなどの分野に焦点を当て，独自のスマートコントラクト開発プラットフォームを構築しているEOS (Enterprise Operation System) について簡潔に説明する．

4.1. Hyperledger Fabric

ビットコインとイーサリアムネットワークでは，任意のノードがネットワークに参加することを許可するが，適用環境のコンピューティングパワーの規模に対して，非常に高い要件が課される．それはコンセンサスアルゴリズムの正常な運用を保証し，ブロックチェーンネットワークの完全性と安定性を維持するためである．しかし，伝統的な産業では，通常，強力なコンピューティングパワーはないが，ブロックチェーンのデータの逆算不可能や改ざん困難，分散型P2Pネットワーク特性などに依存する必要性がある．そのため，新世代のブロックチェーン技術であるHyperledger Fabric（以降，Fabricと略称）が登場した．Fabricは，ブロックチェーン3.0の代表例と見なされている．

Fabricは，最初にIBMによって主導され，ブロックチェーン技術のオープンソース仕様と標準の構築に特化したコンソーシアムチェーンとして開発された．2015年にオープンソースプロジェクトになり，Linux Foundationに引き渡され，維持されるようになった．ビットコインやイーサリアムなどのパブリックチェーンとは異なり，Fabricは，参加，共有，維持の許可を得た関連ビジネス組織のみが参加できる (Chacko et al., 2021)．これらのビジネス組織は相互に一定の信頼基盤を持っているため，Fabricは完全な自律分散型と言い難い．一方，Fabricは暗号化通貨を発行せず，モジュラー機能などを備えた分散型台帳プラットフォームと言える．

Fabricは，主に下記のコンポーネントによって構成されている (Iftekhar et al., 2021)．

クライアント (Client) ノード : ユーザーは，クライアントノードを介してアプリケーションとブロックチェーンネットワーク間の相互作用を実現し，クライアントノードは，トランザクションのプロポーザル，チャネルの確立，ピアの作成など，一連の操作コマンドをブロックチェーンネットワークにリクエストできる．

CA (Certificate Authority) ノード : Hyperledgerネットワークのすべてのメンバーの管理を担当する．Fabric CAとも呼ばれる．言い換えると，MSP (Member Service Provider)[11]の具現化である．また，MSPのコンポーネントとして，CA以外，PKI（Public Key Infrastructure：公開鍵基盤）[12]もMSPの実行に欠かせない．言い換えると，Fabricというコンソーシアムチェーンは許可された (Permissioned) ブロックチェーンネットワークであるため，ユーザーはネットワークにアクセスするためのIDを予め申請する必要がある．このIDは，公開鍵暗号とデジタル証明書

[11] MSP は Hyperledger Fabric においてメンバーシップを管理するために，システム抽象化を提供するコンポーネントである．

[12] PKI は, デジタル証明書, ペアキー (非対称鍵) アルゴリズム, 証明書発行・管理, 証明書失効リスト (Certificate Revocation List) の 4 つから構成され，ピア間通信の基盤となる．この設計メカニズムによってデータの安全な転送や記憶が保証される．

を使用するPKIに基づいており，一連のID証明書ファイルが含まれている．

チャネル（Channel）：完全なブロックチェーンネットワークは異なるプライベートサブネットに分割され，各チャネルには異なるピアがあり，データプライバシーを実現した．

ピア（Peer）：ピアの役割に応じて，エンドーサーピア（Endorser peer），コミッターピア（Committer peer），アンカーピア（Anchor peer），リーダーピア（Leader peer）に分けられる[13]．

オーダリングサービス（Ordering Service）：エンドーサーピアの署名を検証した後，トランザクションのオーダリングを行い，新しいブロックにパッケージ化し，コミッターピアに送信する．オーダリングサービスは，1つのオーダリングノード（Orderer Node）で構成されることも，複数のオーダリングノードで構成されることもある．

チェーンコード（Chaincode）：Hyperledgerで実行されているスマートコントラクトである．通常，スマートコントラクトはトランザクションの全ライフサイクルに関するビジネスロジックを定義し，ワールドステートを制御する．チェーンコードは，トランザクションのビジネスロジックをパッケージ化してブロックチェーンに配置し，論理的に首尾一貫した自動的なシステムを形成する．

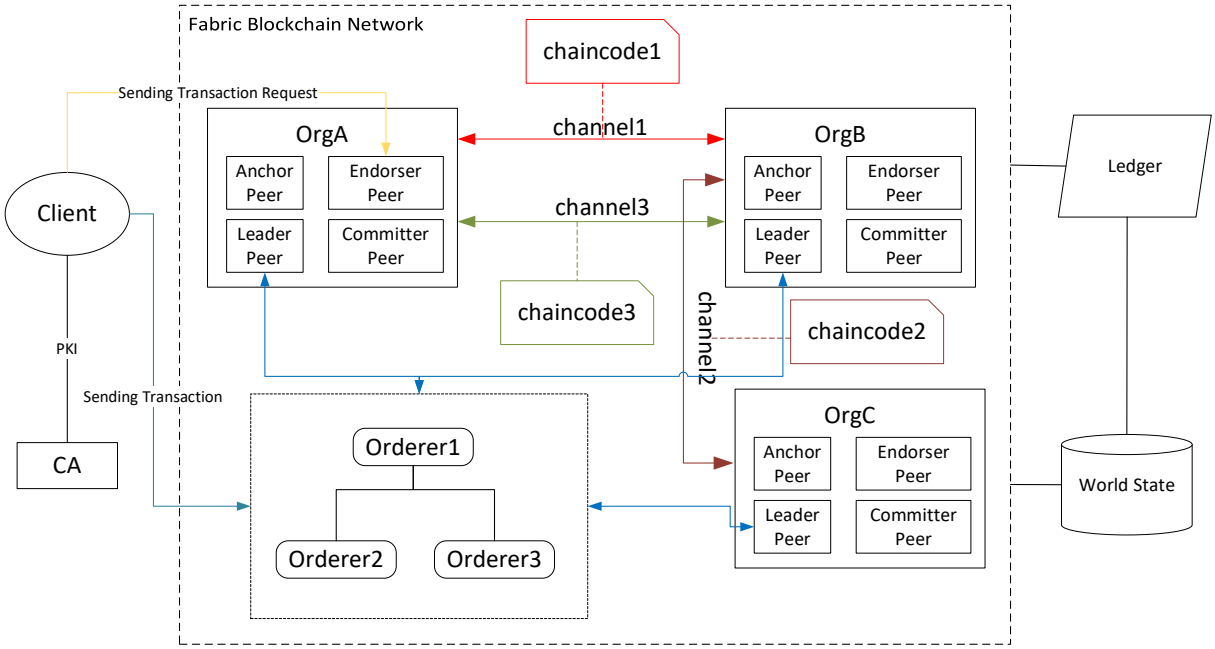

図 8 － Hyperledger Fabricの作動原理図[14]（著者作成）

図8が示すように，トランザクションが開始する時，クライアントノードはそれぞれトランザクション要求と承認されたトランザクションをエンドーサーピアとオーダリングノートに提出する必要があり，エンドーサーピアとオーダリングノードが後続のトランザクション処理作業を完成すると，トランザクションをブロックチェーンに書き込むことができる．また，ユーザーは，Fabricネットワークへのアクセスを取得する前に，クライアントノードを介してCAノードにID証明書の取得をリクエストする必要がある．さらに，オーダリングノードはFabricネットワーク中のチャ

[13] エンドーサーピアは，クライアントによって提出されたトランザクションの実行をシミュレートし，実行されたトランザクションに署名する役割を果たす．コミッターピアは配信された新しいブロックを検証し，検証に通れば，新しいブロックをブロックチェーンに追加する．アンカーピアはチャネル内のすべての Peer ノードを検出するために使用され，また，チャネル内の組織間の情報を同期化する．リーダーピアは主にオーダリングノードとの通信を行い，組織内のすべての Peer ノードに，オーダリングノードからの新しいブロック情報をブロードキャストする．

[14] ：Org は Organization の略である．

ネル内のトランザクションを管理し，それはネットワーク内のすべてのクライアントノードからのトランザクションを収集し，ある一定の時間内のトランザクションをオーダリングしてブロックを生成し，ブロックを各組織内のコミッターピアにブロードキャストする．

また，チェーンコードとピア間の関連性について図8に示されるように，仮に組織Aと組織Bが協力してプロジェクト１を立ち上げた場合，互いにChannel1を通して，情報伝達や意思決定などの作業に対して，事前にビジネスロジックを設定したChaincode1によって対処・実行されることになる．組織Cはこのブロックチェーンシステムに参加しているが，プロジェクト1に関して一切関与できない．同じく組織Bと組織Cが連携してプロジェクト2を立ち上げた場合，すべてのやり取りはChannel2の中で行えるので，組織Aが関与できない．つまり，プロジェクト間の情報プライバシーを実現するために，チャネル機能を生かし，自動的に情報の交差を防ぐ効果がもたらした．

さらに，Fabricが下記のいくつかのコアな機能を持っている：

プライバシー（Privacy）: Fabricは，ネットワーク内のすべてのコンピュータノードを識別できる必要があり，Fabricネットワーク内の許可されたメンバーは，いわゆる「許可された」メンバーシップであるMSPを介して参加やメンバーIDの識別ができなければならない[15]．

チャネル（Channel）: Fabricは，分類された元帳を「チャネル」の機能に分割する．この機能では，ネットワークのメンバーが，全ネットワークからは見えない独立したトランザクションセットを作成できる（Krstić and Krstić, 2020）．これにより，アクセスする必要のないノードからより機密性の高いデータを分離できる．

拡張性（Scalability）: 大企業向けのFabricのもう1つの魅力的な機能は，Fabricが非常に簡単にスケーラブルなネットワークを提供し，ネットワークに参加するノードの数をすばやく拡張できることである[16]．

モジュール式（Modularity）: Fabricのアーキテクチャは，個々のコンポーネントを異なる時間に追加および実行できるように設計されている．多くのコンポーネントはオプションであり，プラットフォームの機能に影響を与えることなく，完全に省略したり，必要に応じて後で導入したりできる[17]．

Fabricフレームワークは，Hyperledgerプロジェクト（BurrowやSawtoothなど）と互換性があり，スケーラブルなデータプラットフォームを提供できる．Hyperledgerフレームワークの下にある他のエコシステムプラットフォームメンバー（Composer，Quilt，Explorerなど）は，Fabricネットワークのデータを使用できる．

4.2. スマートコントラクト（チェーンコード）の実行

Docker[18]コンテナーは，広く使用されているオープンソースのサンドボックス環境であり，Fabricのスマートコントラクトチェーンコードは，軽量のDockerコンテナーで実行され，gRPCプロトコルを介して相応するPeerノード[19]と相互作用する（Zheng et al., 2019）．Dockerコンテナ

---

[15] データのプライバシーを維持することは多くの業界にとって重要であり，これだけでも Fabric は魅力的なアーキテクチャの選択肢になる．Fabric はブロックチェーンのすべての部分に対する許可を必要としないことに注意すべきである（Brandín and Abrishami, 2021）．許可の必要性は，ネットワークを設計する人によって決定される．

[16] ただし，プラットフォームは依然として少数のリソースセットを使用して大量のデータを処理でき，少数のノードを使用してブロックチェーンを構築し，必要に応じてスケーリングできる（Hyperledger Foundation, 2021）．

[17] この機能は，企業が実装するものと実装する必要のないものを個別に選択できるように設計されており，モジュール式と見なされる．一部のコンポーネントには，コンセンサスに達成するための方法，識別のためのメンバーサービスや特定のアクセス API などある（Blockchain Lab, 2021）．

[18] Docker は PaaS のプロバイダである dotCloud によってオープンソース化された LXC（Linux Containers）ベースのコンテナエンジンである．ソースコードは Github でホストされ，go 言語をベースとし，Apache2.0 プロトコルに準拠したオープンソースである．

[19] 台帳やチェーンコードなどの重要なデータを格納し，エンドーサーやチェーンコードなどの特定のプログラムを実行する物理ノードのこと．

ー[20]のセキュリティ分離機能に基づいて，ブロックチェーンホストプログラムがコンテナー内の悪意のあるコントラクトによって攻撃されるのを防ぎ，同時に，異なるコンテナーで実行されているコントラクト間の相互干渉を回避する．

チェーンコードの実行プロセスは以下の通りである（Hyperledger Fabric, 2021）：

パッケージ（Package）：パッケージの作成と署名を含め，チェーンコードをPeerノードにインストールする[21]．チェーンコードに複数の所有者を持たせる場合は，最初に署名付きチェーンコードパッケージ（SignedCDS Package）を作成してから，このパッケージに各所有者が順番に署名するようにする必要がある．

インストール（Install）：コントラクトを実行するPeerノードに，CDS規定のチェーンコードをインストールする．チェーンコードは，コントラクト所有者のエンドーサーピアにのみインストールされ，インストールの本質はコードのコンパイルプロセスである．

例示化（Instantiate）：ライフサイクルシステムチェーンコード（lifecycle system chaincode：LSCC）を呼び出し，チャネル[22]でDockerコンテナーを起動し，コントラクトとチャネル間のバインディングを実現する．

更新（Update）：更新は，例示化に似たトランザクションであり，即ち，新しいバージョンのチェーンコードをチャネルにバインドする[23]．

コントラクトがインストールされた各エンドーサーピアでのSignedCDSパッケージと，チェーンコードに対応するDockerコンテナーを削除する．開発中のバージョンでは，トランザクションのStopとStartコマンドを使用して，チェーンコードを直接削除せずに停止または再開できる．

Fabricのスマートコントラクトは，モジュール式でスケーラブルなアーキテクチャに基づいており，コンセンサスサービスをエンドーサーピアから分離して，独立した機能モジュールが形成される．それによって，強力なスケーラビリティと高いコンセンサス効率を備え，コンソーシアムチェーンアプリケーションとして，サプライチェーン，金融やIoTなどの産業に適用されている．

4.3. EOS (Enterprise Operation System)

イーサリアムとHyperledgerは，スマートコントラクトのレイヤーを追加することで複雑なビジネスシナリオでのブロックチェーン技術の適用を実現したが，イーサリアムのプラットフォームは，同時アクセスが制限された環境であり，比較的単一な操作機能を持つスマートコントラクトのみができ，Hyperledgerでも複雑なコントラクトの運用に制限される．

EOSは，ブロックチェーンのアプリケーション用に開発されたオペレーティングシステムである（Kim and Huh, 2020）．具体的には，コンピューターオペレーティングシステムと同等の機能レイヤーがコントラクトレイヤーの下に作成され，企業ユーザー向けのブロックチェーンベースのスマートコントラクトをさらに多く開発できるようにしている．それによって，複雑な分散型アプリケーション（DApps）は多く実現されるように，オペレーティングシステムレベルのサポートとサービスを提供できる[24]．EOSでは，マイニングに関連するノードリソースを使用して，DAppsをデプロイし，DPoSコンセンサスアルゴリズムを採用して，バリデーター（Validator）を

---

[20] Docker の主なコンポーネントは，Docker イメージと Docker コンテナである．Docker コンテナはパッケージ化されたイメージ（Image）によって作成される．

[21] 具体的には，開発言語（主に GO 言語を使用）で記述されたソースコードをチェーンコード展開仕様（Chaincode Deployment Spec：CDS）に従って再定義し，署名を通じてチェーンコードの所有者を検証・確認することを指す．

[22] トランザクションルールに基づいてブロックチェーンネットワークを分割することによって形成される論理ユニット．

[23] 更新後も，古いバージョンにバインドされている他のチャネルは，古いバージョンのチェーンコードを実行する．

[24] DApps はブロックチェーン技術に基づいており，すべてのプログラムコードと実行結果をブロックに保存して，プログラム操作の安全性とデータの信頼性を確保できるため，DApps はスマートコントラクトアプリケーション機能の拡張と見なされる．

通じて新しいブロックを生成する（Huang et al., 2020）．これにより，ネットワーク処理トランザクションの速度を大幅に向上させ，エネルギーの浪費を減らす効果が大いに期待できる．また，EOSはプライベートチェーンのフレームワークに適しているため，複雑なコントラクトの開発や実行が可能であり，企業自身の効率的なオペレーションズ・マネジメントの運営に適用である．

5. コンセンサスアルゴリズム

上述のブロックチェーンの象徴的なプラットフォームの特徴や着眼点から，ブロックチェーンのエッセンスとその発展プロセスについて，詳細に述べてきたが，如何にブロックチェーンの基本理念である自律分散型システム構造の維持やトラストレス環境の確保を実現するかについて，また，経済的な視点から効率性と安全性の均衡をどのように保つかなど現実的な問題を解決するための一連の方法論として代表的なコンセンサスアルゴリズムを紹介する．

コンセンサスメカニズムは，ブロックチェーンシステムの基本設計方針であり，主に，マイナーが所有するコンピューティングパワーまたは権利を使用して，ブロックチェーンの開発に影響を与える提案に“投票”し，分散型システム環境におけるコンセンサスを達成できるように特定のルール設計を実現することである．様々なブロックチェーン・プラットフォームでは，使用されるコンセンサスアルゴリズムも大きく異なっている．ただし，共通する目的は，一定期間内のトランザクションのシーケンスにルールを策定し，それらのルールによって，ネットワーク内のすべてのノードがトランザクションを検証できるということである．現在，主なコンセンサスアルゴリズムは，PoW（Proof of Work：作業量の証明），PoS（Proof of Stake：資産保有による証明），DPoS（Delegated Proof of Stake：委任型の関与の証明）やPBFT（Practical Byzantine Fault Tolerance：実用的ビザンチン障害耐性）など挙げられる（表1を参照）．

表 1 – コンセンサスアルゴリズムのパフォーマンス対照表（著者作成）

Consensus Algorism	PoW	PoS	DPoS	PBFT
Degree of Decentralization	high	high	low	low
Byzantine Fault Tolerance	$N \geqq 2f+1$	$N \geqq 2f+1$	$N \geqq 2f+1$	$N \geqq 3f+1$
Throughput (tx/s)	≦10	<1000	>100	≦3000
Block Generation Time (s)	>500	<100	－	<10

5.1. PoW（Proof of Work：作業量の証明）

1997年に，Adam BackのDoS攻撃に関する論文の中でPoWが初めて提唱された．その後，2008年，ナカモトサトシはビットコインのホワイトペーパーの中で，ノードの記帳権を決定するために，PoWアルゴリズムを使用してコンセンサスを達成することを提案した（Nakamoto, 2008）．ビットコインでは，2016枚のビットコインが生成されるたびにマイニングの難易度を制御するようにターゲット難易度[25]が調整されるため，ブロックの生成時間は約10分に維持される．

ビットコインのプロトコルにより，ビットコインの発行量は4年ごとに半減されていく．最初回に，50枚のビットコインが発行されたが，4年間に約210,000回が発行されるため，発行額が 1 サ

[25] ビットコインでのマイニングの難易度は，主に 2 回の SHA256 のハッシュ関数による演算でターゲット難易度値よりも小さいナンス値を見つけることである．つまり，ノードは最初にブロックヘッダーのナンス値を 0 に設定し，次にブロックヘッダーのナンス値とその他のデータを入力し，ダブル SHA256 のハッシュ関数演算を行う（C, 2018）．演算結果がターゲット難易度値よりも小さい場合は認定され，それ以外の場合はナンス値が 1 ずつ増やして演算が継続される．適切なナンス値が見つかるまで，または他のノードが見つかったことが分かったら，当該ブロックの競合を放棄して，次のブロックに進む．ターゲット難易度値は通常，連続するいくつかの 0 を持つ 16 進整数であり，連続する 0 が多いほど，マイニングが難しくなる．ブロックチェーンのブロック生成速度を約 10 分に維持できるようにするため，2,016 個のブロックが生成されるたびにマイニングのターゲット難易度が調整される（約 14 日）．SHA256 ハッシュ関数の強力な衝突防止性により，マイナーは大量の計算を通じて記帳権を争うよりほかない．

トシ[26]より小さい場合，ビットコインの発行が終了することになる．したがって，ビットコインの総発行量の上限は2,100万枚と予測できる．下記の式はビットコイン総発行量の計算式である．

$$50 \times 210{,}000 \times (1 + 1/2 + (1/2)^2 + (1/2)^3 + \cdots) = 21{,}000{,}000 \quad (1)$$

PoWアルゴリズムの特徴は，各参加ノードがコンセンサスに達成するプロセスの中で，経済的インセンティブメカニズムを導入することである．これにより，経済的利益を追求して，より多くのノードがマイニングの作業に積極的に参加する．PoWが適用されている環境下で，悪意あるノードの攻撃やブロックチェーンの一時的分岐が発生した場合，ネットワーク全体の51%以上のコンピューティングパワーを確保する必要がある．それは殆どのノードにとって実現不可能なため，ブロックチェーンの改ざんと分岐を防ぎ，システムの一貫性が確保できる．PoWアルゴリズムを採用している暗号化通貨として，ビットコイン以外，ドージコイン（Degecoin）やライトコイン（Litecoin）など挙げられる（Gervais et al., 2016）.

PoWアルゴリズムのメリットは，ビットコイン特有な価値属性を使ってノードにマイニングへの参加を促し，コンセンサス達成のプロセスの中でブロックの記帳権の競合を通じてビットコインの通貨発行とトランザクションの履行を実現して，採用された検証と競合メカニズムによりシステムの安全性と分散化が確保されることである．しかし，PoWコンセンサスの達成プロセスは，各ノードのコンピューティングパワーに完全に依存しているため，リソースの浪費が多く，今日のグリーン開発の概念と相反する．また，最大10分のブロック生成時間により，PoWアルゴリズムは，金額が小さく，トランザクション量が多いビジネスの応用には不適切であり，そのスケーラビリティは制限される．

5.2. PoS（Proof of Stake：資産保有による証明）

PoSアルゴリズムはPoWの代替手段であり，PoWで批判されてきたリソースの浪費を解決し，安全性に対するより高い要件を満たすために提案された．PoSによって設定される記帳権獲得ルールはPoWアルゴリズムと類似している．即ち，すべてのマイナーがコンピューティングパワーに基づいて特定の条件を満たすハッシュ値を求めて競合し，最初に問題解決することに成功したマイナーが記帳権を獲得するという．PoSによる合意結成の達成は投票によって行われ，システムがランダムに次のブロックの記帳を担うノードを選択する（Kaur et al., 2021）．しかし，該当ノードの選択は完全にランダムに行われるわけではなく，事前にネットワーク上に自身の保有する仮想通貨（例：イーサ）を預入する者からブロック生成ノードを選択するのである．PoSの場合，預入したイーサの保有量（Coin Number）と保有期間（Coin Time）の積（コインエイジ：Coin Age）によって記帳権の付与が決まるのは最大な特徴である（下式を参照）．PoSはシステムの構築にハードルが高く，複雑なシステム設計となっているため，以前のマイニング競争や専用なマイニングマシンの使用などを防ぎ，ブロックチェーンの安全性と合意形成の効率性が高まった．

$$Coin_{Age} = Coin_{Number} \times Coin_{Time} \quad (2)[27]$$

$$Hash(Block_{Header}) = Target \times Coin_{Age} \quad (3)[28]$$

PoWと比較すると，PoSアルゴリズムには，純粋なコンピューティングパワーの競合を放棄してエネルギーを節約したり，コンピューティングパワーの過度な集中化問題を解決するためにコインエイジのリセット対策を採用したり，オンラインユーザーのみ利益を得るように制限するなど，複数の利点が明らかである（Al Ahmad et al., 2018）．しかし，PoSメカニズムでは，フォークが発生しやすく，安全性と耐障害性が比較的低く，資産保有しているノードの中に，記帳権の

[26] ビットコインの最小単位であり，１ビットコイン＝100,000,000 サトシ（１億サトシ）である．

[27] 式 (2) の中に，$Coin_{Age}$はコインエイジ，$Coin_{Number}$は保有量，$Coin_{Time}$は保有期間を表す．

[28] 式 (3) の中に，$Block_{Header}$はブロックのヘッダー，$Target$は事前設定されたターゲット値を表す．

競合に消極的なものもある[29].

5.3. DPoS（Delegated Proof of Stake：委任型の関与の証明）

DPoSアルゴリズムはBitshares社の創業者であるDaniel LarimerがPoWとPoSの問題点をさらに改善するために，2014年4月に提唱したものである（Yang et al., 2019）．DPoSはシステムのスループットを高めるため，記帳権をネットワークの全ノードから一部分（100名）の株主（該当トークンを所有する）グループに限定することに変え，そのグループのメンバーを代理人（delegate）と名付ける．ネットワーク上に，株主は常に投票して代理人に新しいブロックの発行を促す．DPoSのネットワーク・スループットが高いため，代理人が常にオンライン状態（100%に近い）を保つ必要があり，そうしなければ，すぐに投票が撤回され，グループから除名される．EOS（トークン名：イオス）の場合，3秒間で１ブロックを生成し，PoWの平均10分間と比べると画期的な飛躍と言える（Wagner et al., 2019）．

該当グループは通常，一定期間後に更新され，新しいグループは新しい投票によって形成される．DPoSアルゴリズムの出現により，コンピューティングパワーや電力などのリソースの浪費が回避され，ノードの利益を保護するために民主的な投票が採用され，ブロック生成速度の加速により，トランザクション実行速度とスループットが向上した．しかし，グループの結成は必然的にある程度の中央集権化をもたらし，最も裕福な株主はブロックチェーンの安全を脅かす可能性がある（Li et al., 2020）．

5.4. PBFT（Practical Byzantine Fault Tolerance：実用的ビザンチン障害耐性）

PoW，PoS，DPoSとは異なり，BFT（Byzantine Fault Tolerance：ビザンチン障害耐性）アルゴリズムでは，記帳権を決定するために競合が必要としない．代わりに，システム内のノードが投票によって新しいブロックを生成し，システム内のコンセンサスの達成を実現でき，フォーク現象も発生しない．分散型システムのCAP理論によれば，どのシステムでも，C（consistency：整合性），A（availability：可用性），およびP（Partition-tolerance：分断耐性）の最大2つを同時に達成できる．これにより，BFTは，整合性と可用性を満たすことを前提として，分断耐性を弱めることしかできない．BFTアルゴリズムの整合性が高いため（これはコンセンサスアルゴリズムの前提でも言える），様々なBFTベースの派生アルゴリズムがブロックチェーンネットワークで広く活用されている（De Angelis et al., 2017）．HyperledgerやAntsharesなど多くのブロックチェーンシステムは，PBFTアルゴリズムを採用している．

PBFTは，アルゴリズムを最適化することにより，計算の複雑さを指数レベルから多項式レベルに軽減したため，BFTの運用効率が低いという問題が解決された．PBFTアルゴリズムには，主にコンセンサスプロトコル（Consensus protocol），チェックポイントプロトコル（Checkpoints protocol），およびビュー変更プロトコル（View change protocol）といった3段階が含まれる（Rahli et al., 2018）．

分散型（P2P）ネットワークでは，すべてのノード数がNで，悪意のあるノードの数がfであると仮定すると，PBFTアルゴリズムは，悪意のあるノードの数がネットワークノード全体の1/3未満の場合，即ち，$N \geqq 3f+1$が満たされたら，全ネットワークにおいて，コンセンサスが達成される．PBFTアルゴリズムには，プライマリーノードと他のレプリカノードが含まれる．プライマリ

[29] 2012年に，ピアコイン（Peercoin）が発行され，最初にPoSアルゴリズムを採用した暗号化通貨として，脚光を浴びていた（Lepore et al., 2020）．PoSメカニズムでは，通常，初期段階でPoWメカニズムを介して稼働開始用通貨として一定数のトークンが発行される．その後，PoSメカニズムでは，マイナーはマイニング時に自分のコインエイジを投入する必要がある．投入するコインエイジが多ければ多いほど，マイニングの難易度は低くなり，ブロックが正常に生成された後，公平性を保つために投入されたコインエイジはリセット（消去）される．PoSネットワークのメインチェーンに対して攻撃を仕掛ける場合，攻撃者は大量のトークンを保持する必要がある．しかし，実際，このような能力を持つユーザーによる悪意ある行動からの利益は，正直なノードとして受ける利益よりはるかに少ないことが証明されている．したがって，PoSアルゴリズムは，ユーザーの重要な利益を拘束することにより，トランザクションの安全性を保証することになる．

ーノードが正常に機能している場合，メッセージは，要求（request），事前準備（pre-prepare），準備（prepare），コミット（commit），および応答（reply）の5つのステップを経る必要がある．プライマリーノードでエラーが発生した場合，またはデータを時間内に処理できない場合は，ビューー変更プロトコルを開始し，レプリカノードから新しいプライマリーノードを選択し，作業を続行する[30].

PBFTアルゴリズムに基づいて，多くの研究者はその改良版を提案した．Gueta et al.（2019）は通信の複雑さを軽減するために，PBFTアルゴリズムに基づくしきい閾値署名技術を導入した．Aublin et al.（2013）は，システムの堅牢性を向上させるために，事前準備の段階で伝播（propagate）プロセスを追加した．PBFTとその改良されたアルゴリズムのアプリケーションシナリオは，主にFabricに代表されるコンソーシアムチェーンに適用される．コンソーシアムチェーンでは，インセンティブメカニズムが取り除かれたため，PBFTアルゴリズムを使用する場合，大量のコンピューティングパワーと電力リソースの浪費が解消される．

6. オペレーションズ・マネジメントにおける研究との関連性

ブロックチェーン技術が登場した当初は，その応用事例の殆どが暗号化通貨の分野に留まった．スマートコントラクトの導入と，イーサリアムやHyperledger Fabricなど様々なブロックチェーン開発プラットフォームが整備され，ブロックチェーン技術を適用できるビジネスシナリオは広範になり，オペレーションズ・マネジメントにおけるブロックチェーン技術適用についての研究が始まっている．本節では，その初期の文献を紹介し，自動車産業でのサプライチェーンをコンテキストとして，第４節で解説した，Hyperledger Fabricをはじめとするコンソーシアムチェーンの適用について解説する．

6.1. オペレーションズ・マネジメント分野におけるブロックチェーンの研究

Tapscott and Tapscott（2016）は，信頼できる経済社会のアーキテクチャを再設計するために，ネットワーク整合性（Networked Integrity），分散性（Distributed Power），インセンティブ価値（Value as Incentive），セキュリティ，プライバシー，権利保持（Rights preserved），包括性（Inclusion）というブロックチェーン革新の7原則を挙げている．一方，サプライチェーンでは管理コスト，オペレーション効率，製品価格，メンバーの激励，監督，関連サービスなど，すべての要素が信頼性と深く関わっている（Malik et al., 2019）．サプライチェーンの有効なソリューションとして，ブロックチェーンは強制的で拘束力のあるツールではなく，補助的で率先性のあるインフラストラクチャである．その導入はサプライチェーン設計に直結する要素を解決するのみならず，サプライチェーンのエコシステム全体の健全性と完備性を考慮する必要があり，目的は健全な自己循環システムと順方向フィードバック・メカニズムを構築することである．

ブロックチェーンの導入は，ビジネスプロセスの透明性を高め，取引コストを削減し，信頼を構築し，サプライチェーンの持続可能性を促進するのに有効である（Xu and Choi，2021）．そのためブロックチェーン・メカニズムの適用環境における，サプライチェーン企業間競争に関する

---

[30] PBFTアルゴリズムのコンセンサスプロセスは次の通りである：

1) クライアントはプライマリーノードにリクエストを送信する；
2) リクエストの受信後，プライマリーノードは事前準備メッセージを生成し，それをネットワーク全体のレプリカノードに送信する；
3) レプリカノードは，事前準備メッセージを受信した後，まず，検証する．検証に合格すると，準備メッセージが生成され，ネットワークのノード全体に送信すると同時に，ネットワーク内の他のノードからの準備メッセージが監視する；
4) ノードが，N≧2f + 1のノードの準備メッセージを受信した後，コミットメッセージを生成し，同時にネットワーク内の他のノードからのコミットメッセージを監視する；
5) ノードが，N≧2f + 1のノードのコミットメッセージを受信すると，ノードはメッセージへのコミットメントを完了し，自身のログを更新し，同時にコミットメント情報をクライアントにフィードバックする．クライアントが，N>fのノードのコミットメント情報を受信すると，ほとんどのノードでリクエストが確認されたことになる．

ゲーム理論の研究がオペレーションズ・マネジメントの新しい研究の焦点となっている．Nakasumi (2017) はダブル・マージナリゼーション (double marginalization) 問題に対してブロックチェーンに基づくサプライチェーン解決策を提案し，その解決策の有効性を検証した．Ghode et al. (2022) は情報共有の視点から企業間の情報の非対称によって引き起こされる“Bullwhip Effect”問題に対して，ブロックチェーンの適用により，その問題が解消され，サプライチェーン企業による平等なパートナシップ構築が可能であることを論証した．また，Zheng et al. (2021) は同じく情報共有の視点から，宇宙船のサプライチェーンにおける部品発注量決定とリスク対処策に関して，ブロックチェーンを適用したサプライヤ，メーカー，流通業者の3者間での情報共有のパターンをカテゴリー化し，シュタッケルベルグゲーム均衡について論じた．Choi and Luo (2019) はブロックチェーンによるデータ品質改善の視点からファッションサプライチェーンの発注決定問題を分析し，ブロックチェーンの適用は社会福祉 (social welfare) を高める一方，ファッションサプライチェーンの収益力を弱めることを例証した．

以上の文献はブロックチェーン技術をベースとしたサプライチェーン企業間関係についてのゲーム理論的考察である．これらの文献においては，ブロックチェーンの適用コストがサプライチェーン企業によるブロックチェーンの導入を妨げる要因になっているにもかかわらず，その要因の意思決定に与える影響を考慮に入れていなかった．De Giovanni (2020) は，取引コストの削減，メーカーの納品リスクと製品のアフターサービスリスクの排除という観点から，サプライチェーンのメンバーがブロックチェーン・プラットフォームの構築と運営に参加する条件について検討した．Fan et al. (2022) は，消費者のトレーサビリティ意識やブロックチェーン導入のコスト分担を考慮した上で，メーカーがブロックチェーンを適用する条件を検証した．Y.-Y. Wang et al. (2021) は，消費者の信念とブロックチェーンの適用コストが競合するプラットフォームの情報開示戦略に与える影響について検討した．Li et al. (2021) の研究によると，高級品eコマースプラットフォームでは，ブロックチェーン技術による認証コストと手動による認証コストの差が小さい場合のみ，認証手続きにブロックチェーン技術が選択されるということを示した．

一方，IoT設備の発達により，食品や農産物のサプライチェーンにおけるトレーサビリティの実現にブロックチェーン技術の適用は有効であると認識され，該当する研究・開発が行われている．Perboli et al. (2018) は，ブロックチェーンによるソリューションの開発と検証，サプライチェーンへの適合設計，ユースケースを配置するための標準的なアプローチを作成した．また，生鮮食品配送の実例を組み合わせて，ブロックチェーンがどのように物流コストの削減，オペレーションの最適化，適合設計の実現に直面する課題の解決に資するかについて議論した．Caro et al. (2018) はブロックチェーンに基づく農産物サプライチェーンのトレーサビリティに関するソリューションを提案し，サプライチェーンに沿ってデジタルデータを取り扱うIoT設備をシームレスに統合し，EthereumとHyperledger Sawtoothを使ってテストケースを配備し，それらの性能と優劣点について分析した．Kshetri (2018) は，コスト，品質，スピード，信頼性，リスク，持続可能性，柔軟性といった面において，ブロックチェーンがSCMに与える影響について，詳細に分析した．とりわけ，ブロックチェーンを適用したソリューションにおけるIoT統合の重要性について強調されている．

6.2. 自動車産業におけるブロックチェーン・メカニズムの適用に関する解説概念モデル

自動車のサプライチェーンを例にとると，通常，食品のサプライチェーンよりも多くの利害関係者が含まれる．関連する契約には，複雑な複数関係者のダイナミックな調整が関わり，可視性が低く，関係者同士のデータの非互換性があり，製品追跡コストが高く，盲点（死角）も存在する．Reimers et al. (2019) は，自動車サプライチェーンのブロックチェーンフレームワークとしてFabricを採用した．コンポーザー固有のアクセス制御言語によって，アクセス制御ルール (Access Control Lists，ACL) を作成し，情報ごとにアクセス権限を設定した．具体的な配置において，開発者は各部品にRFIDタグを付けると同時に，RFIDリーダーと関連センサーを各コントローラーに埋め込み，Fabricネットワークやコンポーザーはクラウドサーバーに統合されているため，インターネット接続が正常な場所であればどこでもIoTデバイスを利用できる．

上述の自動車サプライチェーンをベースに，本節では，図9の自動車産業におけるブロックチェーン・メカニズムの適用に関する概念モデルをもとに，4.1節で紹介したHyperledger Fabricの特徴や作動原理を解説する．

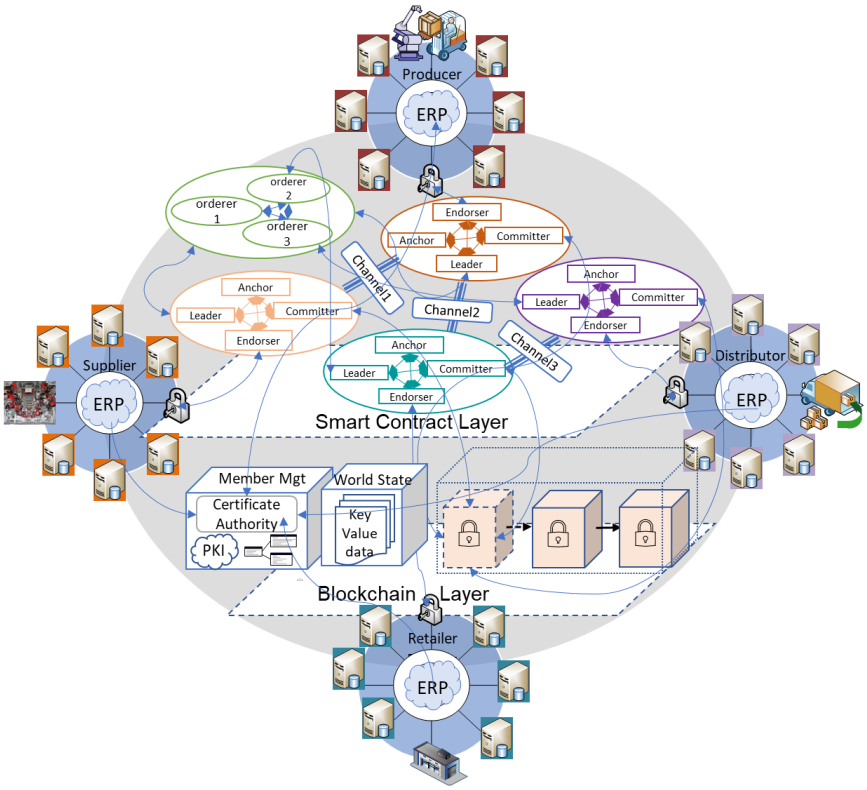

図 9 － 自動車サプライチェーンに適用したブロックチェーン・メカニズムの概念モデル（著者作成）

図9のモデルは，自動車サプライチェーンの基本メンバーであるサプライヤー（Supplier），メーカー（Producer），物流業者（Distributor）とリテーラー（Retailer）によって構成されている．また，本モデルの核心部分であるブロックチェーンネットワークは，スマートコントラクトレイヤーとブロックチェーンレイヤーに分けられる．

スマートコントラクト（Fabricシステムでは，チェーンコードと呼ばれる）レイヤーでは，様々なPeerノードが配置されている．Peerノードは役割的にエンドーサーピア，コミッターピア，アンカーピアとリーダーピアの4種類に分けられる．とりわけ，エンドーサーピアはトランザクションリクエストの承認処理（Endorsement）を担当し，コミッターピアはトランザクションの最終的な有効性の確認と新しいブロックの計上を担当する．また，Fabricは自律分散型ブロックチェーンネットワークであり，すべてのpeerノードは参加するチャネルの台帳のコピー（チャネル内のすべてのトランザクションの正確な履歴）を保持する．新しいブロックが作成されたら，ネットワークを介して，すべてのノード間で台帳のコピーを同期させる必要がある．即ち，(1) 新しいトランザクションは，エンドーサーピアにリクエストを提出し，エンドーサーピアが処理してデジタル署名をした後に応答を返し，合意形成のためオーダリングサービスに提出する．(2) 合意形成後，オーダリングが終了しトランザクションを含む新しいブロックが生成される．(3) オーダリングサービスは新たに生成されたブロックを各チャネル内のすべてのPeerノードにブロードキャストする．

一方，オーダリングノードは一定数のトランザクションをブロックにパッケージ化し，Peerノードに送信する．Peerノードが正当性を検証した後，ブロックチェーンの台帳に改ざん不可能な形で書き込む．すべてのトランザクションは暗号アルゴリズムで暗号化され，取引の安全性と信

頼性を保証する．さらに，このネットワークには複数のチャネルが含まれ，各チャネルには独立した台帳が維持され，各企業ノードは自社の業務ニーズに応じて異なるチャネルに参加することを選択できる．チャネルによるトランザクションの隔離を利用し，企業自身の機密データを保護する．それにより，Fabricのコンソーシアムチェーンにおけるプライバシー保護が確保される．

ブロックチェーンレイヤーでは，自動車サプライチェーンのビジネスプロセスとシステム全体のアーキテクチャを総合的に考慮し，システム機能をメンバーシップ管理（MSP）モジュールとワールドステート・モジュールの2つに分ける．Fabricを用いて構築されたブロックチェーンネットワークはコンソーシアムチェーンに属しており，システムに参加しようとする企業はネットワーク内のCAノードに特別なデジタルID証明書（PKIに基づく）の発行を申請し，許可を得た後，ブロックチェーンデータへのアクセスが可能になる．メンバーシップ管理モジュールは，システム全体の信頼の基盤であり，ID証明書の発行，ID識別，メンバーシップ，証明書の失効などの機能を提供する．ワールドステート・モジュールでは，システム中の各種の情報，例えば，企業情報，メンバー情報，生産情報，販売情報，検証記録と取引記録などKey Value形式で保存され，検索時に直接にアクセスできる．ブロックチェーンレイヤーの主な役割は，自動車サプライチェーンにおけるトランザクションデータを保存し，データのセキュリティとプライバシーを確保することである．

1台の車は何万もの部品で構成されており，それぞれに固有の認証ラベルが付いている．これらの関連情報はサプライチェーンのメンバーのそれぞれのエンタープライズ・システム（ERPシステム）に記録され，ブロックチェーンネットワークに送られる．情報が送られる前に，メンバーはPKIに基づき，部品などのデジタル署名を行い，そのデータを認証ラベルにも書き込む．また，上述の情報がブロックチェーンネットワークに送られてきたら，デジタル署名技術を用いて認証ラベルと照合しながら，情報の真偽が確認される．

ブロックチェーンネットワーク内のトランザクション情報はすべて1つのブロックチェーンに格納され，ネットワークの参加ノードは共同でこれらの情報を保持し，自社の関連情報をネットワークにアップロードする．これは，ブロックチェーンにアップロードされた情報がすべての参加ノードに公開されることを意味する．実際の自動車サプライチェーンのシナリオでは，競合関係にある企業は，同じ部品を製造しており，競合企業にすべての情報を公開することを望んでいるわけではない．部品の販売戦略に関する情報は，部品の受注を獲得できるかどうかに直結している．このような情報の機密性の問題が解決されないと，アップロードする参加企業の意欲が損なわれる．そこで，先述のように，本モデルではマルチチャネルによるトランザクションの履行が行われる．このモデルでは，オーダリングサービスを担当するオーダリングノードが，ネットワーク内のすべての取引をオーダリングする役割を担う．複数の企業ノードが共通チャネルに参加し，各ノードはルールに従って指定された情報をブロックチェーン台帳に書き込み，サプライチェーンのレイヤー関係に基づいて取引を完成させていく．

さらに，近年，ブロックチェーンの適用例は中古車市場にも及んでいる（Jiang and Sun, 2021）．従来の中古車市場では，自動車の使用過程における保守，メンテナンス，事故，危険発生，欠陥回収などの情報に関する信頼できる記録方式が少なく，中古車情報の不透明，検索しにくいなどの問題があった．つまり，「レモン市場」のような状態陥りやすく，中古車情報の真実性，有効性を保障することが困難である．そこで，ブロックチェーン技術を中古車市場に適用させ，Tokenをシステム全体に流通する．車の所有者がデータをアップロードし，真実の情報を共有させることによって，相応のTokenの奨励を得ることができる仕組みが考えられる．例えば，DAppを通じて，OBD上のデータを読み取り，オーナーが実際に有効な運転距離を報告するようにTokenの奨励を与える「Driving as Mining」を実現できる．

現在，トヨタ，Benz，Hyundai，BMW，ホンダやFordなど多くの自動車メーカーはブロックチェーンを用いた様々なプロジェクトを立ち上げ，自動車サプライチェーンのビジネスプロセスにおける付加価値を追及している．

7. まとめと課題

暗号化通貨のパイオニアであるビットコインが登場してから，10年以上経過した．当初，主に暗号化通貨のキャリアとして知られたブロックチェーンの一連の関連技術とそのメカニズムは進化を遂げ，とりわけ，スマートコントラクトとの融合に基づき，現在，様々な分野で活躍を見せている．暗号化通貨は，2021年12月末時点で総時価総額が約1兆3千億ドルに達しており，ビットコインだけでも9千億ドルを超えている．ただ12年間で1円にも値しないところから，今日の時価総額になるまで凄まじい成長を成し遂げたと言えよう．一方，この成長ぶりを裏で支えてきたブロックチェーンとそのコア技術群は本文に述べた通り，主に三つの段階を経て今日の発展に至っている．

本研究は，ブロックチェーンのメカニズムと基幹技術について様々な領域の文献レビューを通して，前述したブロックチェーンの三つの発展段階におけるそれぞれの代表例を取り上げ，ビットコイン，イーサリアムとHyperledger Fabricの各々の作動原理を分析し，オペレーションズ・マネジメントの視点から，それらの特性や現行のシステムにもたらしうる影響と変化について，図式化しながら詳細に説明した．また，ブロックチェーンのエッセンスとも言えるコンセンサスアルゴリズムについて，ブロックチェーンのメインフレームワークであるパブリックチェーン，プライベートチェーンとコンソーシアムチェーンにそれぞれ適合したものを紹介し，ビジネスプロセスやサプライチェーンにおけるブロックチェーン・メカニズムの適用性について解説した．

ブロックチェーン技術が産業界，とりわけ，サプライチェーンの分野で更に活用できるために，オペレーションズ・マネジメントの視点から，今後解決すべき5つの課題について，提示する．

スループットの増強：改ざん困難性は，データの透明性や製品のトレーサビリティといった特性の存在価値を保証し，サプライチェーンメンバーがブロックチェーン技術を採用する重要な要因である．しかし，この特性はスループットを犠牲にしていると考えられる．IoTデバイスの導入により，データ量は前例のない増加を告げるものになる．各ブロックに多数のトランザクションが設定される場合，マークルツリーのハッシュ演算は全体的な処理速度を低下させることをもたらす（Meng and Qian, 2018）．今後，システムスループットやその他のパフォーマンスを改善させることは，ブロックチェーン技術が直面する課題の1つである．

コストの低減：ブロックチェーンの導入と新しい解決策の提案はサプライチェーンのイノベーション促進につながるが，システムの正常な運用を保証するために，初期段階の大量資金の導入が必然的と言える．例えば，システムの開発，保守，コンピューティングパワーなどのハードウェア機器への投資，電力などのリソースの消費が挙げられる．さらに，データの収集を確保するために，膨大な数のRFIDおよび他のIoTデバイスが必要になると考えられる．設備のコストは，現在，ブロックチェーン採用時の最大な阻害要因と言える．無論，この課題は，サプライチェーンメンバーが大量データの統合と最適化を図る機会をも提供している．

安全性の強化：ブロックチェーン技術をサプライチェーンに適用させる際の安全性について，多くの研究は耐障害性の確保に焦点を当てるが，サプライチェーンの各段階におけるデータの取得は，主にIoTデバイスに依存しているため，コンピューティングパワーとストレージの限界から，悪意のある攻撃に対して脆弱である（Nour et al., 2020）．データの安全な入力を確実にする方法は，急務な課題と言える．また，ユーザーはアカウントの安全性を維持するために秘密鍵を保存することが多い．現在のブロックチェーンシステムには秘密鍵を変更するメカニズムがないため，秘密鍵を紛失した場合に，いかに情報の安全性を確保するかについては研究・解決すべき重要な課題である．

プライバシー保護の改善：ブロックチェーンシステムでは，ペアキーを識別する方法を使用してトランザクションを実行する．ユーザーは元帳の情報を読み取って実際のアイデンティティを直接に識別することはできないが，匿名性は追跡不可能という意味ではない．言い換えると，複数の固定トランザクションモードを使用してユーザーの実際のアイデンティティを推測することは可能である．現在，一部の解決案では現状を緩和させるために登録と認証を使用しているが，これらの解決案の効果には限界があり，分散化を犠牲にして達成されると言える．

スケーラビリティの向上：参加者（ノード）は，システムが改ざんされないように，独立した

元帳を維持する必要があるが，市場の取引規模が拡大し続けると，データの冗長性とデータベースの過負荷が必然的に発生すると考えられる．したがって，ブロックチェーンのスケーラビリティの問題を解決するために，更なる革新的な構想と実践を推進し続けることが重要である．

参考文献

Al Ahmad, M. A., Al-Saleh, A. and Al Masoud, F. A. (2018), "Comparison between PoW and PoS systems of cryptocurrency," *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 10, No. 3, pp. 1251-1256.

Angrish, A., Craver, B., Hasan, M. and Starly, B. (2018), "A case study for blockchain in manufacturing: "FabRec": A prototype for peer-to-peer network of manufacturing nodes," *Procedia Manufacturing*, Vol. 26, pp. 1180-1192.

Aruna Sri, P. S. G. and Bhaskari, D. L. (2018), "A study on blockchain technology," *International Journal of Engineering & Technology*, Vol. 7, No. 2.7, pp. 418-421.

Aublin, P.-L., Mokhtar, S. B. and Quéma, V. (2013), "RBFT: Redundant byzantine fault tolerance," *2013 IEEE 33rd International Conference on Distributed Computing Systems*, pp. 297-306.

Belotti, M., Božić, N., Pujolle, G. and Secci, S. (2019), "A vademecum on blockchain technologies: When, which and how," *IEEE Communications Surveys and Tutorials*, Vol. 21, No. 4, pp. 3796-3838.

Bigini, G., Freschi, V. and Lattanzi, E. (2020), "A review on blockchain for the Internet of Medical Things: Definitions, challenges, applications, and vision," *Future Internet*, Vol. 12, No. 12, 208, pp. 1-16.

Bistarelli, S., Mercanti, I. and Santini, F. (2018), "An analysis of non-standard bitcoin transactions," *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 93-96.

Blockchain Lab (2021), "Hyperledger whitepaper," https://blockchainlab.com/pdf/Hyperledger%20Whitepaper.pdf, Accessed 19 Dec 2021.

Bozic, N., Pujolle, G. and Secci, S. (2016), "A tutorial on blockchain and applications to secure network control-planes," *2016 3rd Smart Cloud Networks & Systems (SCNS)*, pp. 1-8.

Brandín, R. and Abrishami, S. (2021), "Information traceability platforms for asset data lifecycle: blockchain-based technologies," *Smart and Sustainable Built Environment*, Vol. 10, No. 3, pp. 364-386.

Buterin, V. (2014), "Ethereum: A next-generation smart contract and decentralized application platform," https://ethereum.org/en/whitepaper, Accessed 15 Nov 2021.

C, Karthik. (2018), "An overview of blockchain technology," *International Research Journal of Electronics and Computer Engineering*, Vo. 4, No. 4, pp. 1-4.

Caro, M. P., Ali, M. S., Vecchio, M. and Giaffreda, R. (2018), "Blockchain-based traceability in Agri-Food supply chain management: A practical implementation," *2018 IoT Vertical and Topical Summit on Agriculture - Tuscany (IOT Tuscany)*, pp. 1-4.

Casino, F., Dasaklis, T. and Patsakis, C. (2019), "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, Vol. 36, pp. 55-81.

Chacko, J. A., Mayer, R. and Jacobsen, H.-A. (2021), "Why do my blockchain transactions fail?: A study of Hyperledger Fabric," *SIGMOD/PODS '21: International Conference on Management of Data*, pp. 221-234.

Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J. and Arami, M. (2020), "How Blockchain can impact financial services: The overview, challenges and recommendations from expert interviewees," *Technological Forecasting and Social Change*, Vol. 158, 120166, pp. 1-12.

Chen, Y.-J., Wu, J.-L., Hsieh, Y.-C. and Hsueh, C.-W. (2020), "An Oracle-based on-chain privacy," *Computers*, Vol. 9, No. 3, 69, pp. 1-15.

Choi, T. M. and Luo, S. (2019), "Data quality challenges for sustainable fashion supply chain operations in emerging markets: Roles of blockchain, government sponsors and environment taxes," *Transportation Research Part E: Logistics and Transportation Review*, Vol. 131, pp. 139-152.

Dai, W., Deng, J., Wang, Q., Cui, C., Zou, D. and Jin, H. (2018), "SBLWT: A secure blockchain lightweight wallet based on Trustzone," *IEEE Access*, Vol. 6, pp. 40638-40648.

De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A. and Sassone, V. (2017), "PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain," *Italian Conference on Cyber Security*, pp. 1-11.

De Giovanni, P. (2020), "Blockchain and smart contracts in supply chain management: A game theoretic model," *International Journal of Production Economics*, Vol. 228, 107855, pp. 1-18.

Di Angelo, M. and Salzer, G. (2019), "A survey of tools for analyzing Ethereum smart contracts," *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*, pp. 69-78.

Elisa, N., Yang, L., Li, H., Chao, F. and Naik, N. (2019), "Consortium blockchain for security and privacy-

preserving in e-government systems," *Proceedings of the 19th International Conference on Electronic Business*, pp. 99-107.
Fan, Z.-P., Wu, X.-Y. and Cao, B.-B. (2022), "Considering the traceability awareness of consumers: Should the supply chain adopt the blockchain technology?" *Annals of Operations Research*, Vol. 309, No. 2, pp. 837-860.
Farnaghi, M. and Mansourian, A. (2020), "Blockchain, an enabling technology for transparent and accountable decentralized public participatory GIS," *Cities*, Vol. 105, 102850, pp. 1-12.
Gamage, H. T. M., Weerasinghe, H. D. and Dias, N. G. J. (2020), "A survey on blockchain technology concepts, applications, and issues," *SN Computer Science*, Vol. 1, No. 2, 114, pp. 1-15.
Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H. and Čapkun, S. (2016), "On the security and performance of proof of work blockchains," *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, pp. 3-16.
Ghode, D. J., Yadav, V., Jain, R. and Soni, G. (2022), "Lassoing the bullwhip effect by applying blockchain to supply chains," *Journal of Global Operations and Strategic Sourcing*, Vol. 15, No. 1, pp. 96-114.
Grech, N., Kong, M., Jurisevic, A., Brent, L., Scholz, B. and Smaragdakis, Y. (2020), "MadMax: Analyzing the out-of-gas world of smart contracts," *Communications of the ACM*, Vol. 63, No. 10, pp. 87-95.
Gueta, G. G., Abraham, I., Grossman, S., Malkhi, D., Pinkas, B., Reiter, M., Seredinschi, D.-A., Tamir, O. and Tomescu, A. (2019), "SBFT: A scalable and decentralized trust infrastructure," *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 568-580.
Hofmann, E. and Rüsch, M. (2017), "Industry 4.0 and the current status as well as future prospects on logistics," *Computers in Industry*, Vol. 89, pp. 23-34.
Hu, B., Zhang, Z., Liu, J., Liu, Y., Yin, J., Lu, R. and Lin, X. (2021), "A comprehensive survey on smart contract construction and execution: Paradigms, tools, and systems," *Patterns*, Vol. 2, No. 2, 100179, pp. 1-51.
Huang, Y., Wang, H., Wu, L., Tyson, G., Luo, X., Zhang, R., Liu, X., Huang, G. and Jiang, X. (2020), "Understanding (mis)behavior on the EOSIO blockchain," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, Vol. 4, No. 2, 37, pp. 1-28.
Hyperledger Fabric (2021), "A blockchain platform for the enterprise," https://hyperledger-fabric.readthedocs.io/en/release-1.4/index.html, Accessed 30 Nov 2021.
Hyperledger Foundation (2021), "An Introduction to Hyperledger," https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf, Accessed 19 Dec 2021.
Iftekhar, A., Cui, X., Tao, Q. and Zheng, C. (2021), "Hyperledger Fabric access control system for Internet of Things layer in blockchain-based applications," *Entropy*, Vol. 23, No. 8, 1054, pp. 1-19.
Ismailisufi, A., Popović, T., Gligorić, N., Radonjić, S. and Šandi, S. (2020), "A private blockchain implementation using multichain open source platform," *2020 24th International Conference on Information Technology (IT)*, pp. 1-4.
Jiang, Y.-T. and Sun, H.-M. (2021), "A blockchain-based vehicle condition recording system for second-hand vehicle market," *Wireless Communications and Mobile Computing*, 6623251, pp.1-10.
Kaur, M., Khan, M. Z., Gupta, S., Noorwali, A., Chakraborty, C. and Pani, S. K. (2021), "MBCP: Performance analysis of large scale mainstream blockchain consensus protocols," *IEEE Access*, Vol. 9, pp. 80931-80944.
Khanna, A., Sah, A., Bolshev, V., Jasiński, M., Vinogradov, A., Leonowicz, Z. and Jasiński, M. (2021), "Blockchain: Future of e-governance in smart cities," *Sustainability*, Vol. 13, No. 21, 11840, pp. 1-21.
Kim, S.-K. and Huh, J.-H. (2020), "Autochain platform: Expert automatic algorithm Blockchain technology for house rental dApp image application model," *EURASIP Journal on Image and Video Processing*, 47, pp. 1-23.
Klems, M., Eberhardt, J., Tai, S., Härtlein, S., Buchholz, S. and Tidjani, A. (2017), "Trustless intermediation in blockchain-based decentralized service marketplaces," in Maximilien, M., Vallecillo, A., Wang, J., Oriol, M. (Eds.), *Service-Oriented Computing: 15th International Conference, ICSOC 2017 Malaga, Spain, November 13–16, 2017 Proceedings*, Springer, Cham, pp. 731-739.
Krstić, M. S. and Krstić, L. J. (2020), "Hyperledger frameworks with a special focus on Hyperledger Fabric," *Vojnotehnički Glasnik*,Vol.68, No.3, pp. 639-663.
Kshetri, N. (2018), "Blockchain's roles in meeting key supply chain objectives," *International Journal of Information Management*, Vol. 39, pp. 80-89.
Lepore, C., Ceria, M., Visconti, A., Rao, U. P., Shah, K. A. and Zanolini, L. (2020), "A survey on blockchain consensus with a performance comparison of PoW, PoS and pure PoS," *Mathematics*, Vol. 8, No. 10, 1782, pp. 1-26.
Li, A., Wei, X. and He, Z. (2020), "Robust proof of stake: A new consensus protocol for sustainable blockchain systems," *Sustainability*, Vol. 12, No. 7, 2824, pp. 1-15.
Li, G., Fan, Z.-P. and Wu, X.-Y. (2021), "The choice strategy of authentication technology for luxury e-commerce platforms in the blockchain era," *IEEE Transactions on Engineering Management*, Early Access, pp. 1-14.

Liu, C., Gao, J., Li, Y., Wang, H. and Chen, Z. (2020), "Studying gas exceptions in blockchain-based cloud applications," *Journal of Cloud Computing*, Vol. 9, 35, pp. 1-25.

Lo, S. K., Staples, M. and Xu, X. (2021), "Modelling schemes for multi-party blockchain-based systems to support integrity analysis," *Blockchain: Research and Applications*, Vol. 2, No. 2, 100024, pp. 1-9.

Malik,S., Dedeoglu,V., Kanhere, S. S. and Jurdak, R. (2019), "TrustChain: Trust management in blockchain and IoT supported supply chains," *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 184-193.

Meng, M. H. and Qian, Y. (2018), "The blockchain application in supply chain management: Opportunities, challenges and outlook," *The 3rd Symposium on Distributed Ledger Technology (SDLT 2018)*, pp. 1-5.

Metcalfe, W. (2020), "Ethereum, smart contracts, DApps," in Yano, M, Dai, C., Masuda, K., Kishimoto, Y. (Eds.), *Blockchain and Crypt Currency: Building a High Quality Marketplace for Crypto Data*, Springer, Singapore, pp. 77-93.

Nakamoto, S. (2008), "Bitcoin: A peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf, Accessed 31 Oct 2021.

Nakasumi, M. (2017), "Information sharing for supply chain management based on block chain technology," *2017 IEEE 19th Conference on Business Informatics (CBI)*, pp. 140-149.

Nour, B., Sharif, K., Li, F. and Wang, Y. (2020), "Security and privacy challenges in information-centric wireless Internet of Things networks," *IEEE Security & Privacy*, Vol. 18, No. 2, pp. 35-45.

Oliveira, M. T., Carrara, G. R., Fernandes, N. C., Albuquerque, C. V. N., Carrano, R. C., Medeiros, D. S. V. and Mattos, D. M. F. (2019), "Towards a performance evaluation of private blockchain frameworks using a realistic workload," *2019 22nd Conference on Innovation in Clouds, Internet and Networks (ICIN)*, pp. 180-187.

Perboli, G., Musso, S. and Rosano, M. (2018), "Blockchain in logistics and supply chain: A lean approach for designing real-world use cases," *IEEE Access*, Vol. 6, pp. 62018-62028.

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E. and Das, G. (2018), "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consumer Electronics Magazine*, Vol. 7, No. 4, pp. 6-14.

Qin, B., Huang, J., Wang, Q., Luo, X., Liang, B. and Shi, W. (2020), "Cecoin: A decentralized PKI mitigating MitM attacks," *Future Generation Computer Systems*, Vol. 107, pp. 805-815.

Rahli, V., Vukotic, I., Völp, M. and Esteves-Veríssimo, P. (2018), "Velisarios: Byzantine fault-tolerant protocols powered by Coq," in Ahmed, A. (Ed.), *Programming Languages and Systems: 27th European Symposium on Programming, ESOP 2018 Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2018 Thessaloniki, Greece, April 14–20, 2018 Proceedings*, Springer, Cham, pp. 619-650.

Raman, R. and Raj, B. E. (2021), "The world of NFTs (Non-Fungible Tokens): The future of blockchain and asset ownership," in Mnaouer, A. B. and Foutati, L. C. (Eds.), *Enabling Blockchain Technology for Secure Networking and Communications*, IGI Global, Hershey, PA, pp. 89-108.

Reimers, T., Leber, F. and Lechner, U. (2019), "Integration of blockchain and Internet of Things in a car supply chain," *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*, pp. 146-151.

Ritz, F. and Zugenmaier, A. (2018), "The impact of uncle rewards on selfish mining in Ethereum," *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 50-57.

Saad, S. M. S. and Radzi, R. Z. R. M. (2020), "Comparative review of the blockchain consensus algorithm between Proof of Stake (POS) and Delegated Proof of Stake (DPOS)," *International Journal of Innovative Computing*, Vol. 10, No. 2, pp. 27-32.

Sabry, S. S., Kaittan, N. M. and Ali, I. M. (2019), "The road to the blockchain technology: Concept and types," *Periodicals of Engineering and Natural Sciences*, Vol. 7, No. 4, pp. 1821-1832.

Safieh, M., Thiers, J.-P. and Freudenberger, J. (2020), "A compact coprocessor for the elliptic curve point multiplication over Gaussian integers," *Electronics*, Vol. 9, No. 12, 2050, pp. 1-21.

Serada, A., Sihvonen, T. and Harviainen, J. T. (2020), "CryptoKitties and the new ludic economy: How blockchain introduces value, ownership, and scarcity in digital gaming," *Games and Culture*, Vol. 16, No. 4, pp. 457-480.

Serdyuk, O. S. (2015), "Public-private consortium as economic-organizing mechanism of coal enterprises liquidation," *Economy of Industry*, Vol. 70, pp. 88-96.

Song, J., Zhang, P., Alkubati, M., Bao, Y. and Yu, G. (2021), "Research advances on blockchain-as-a-service: Architectures, applications and challenges," *Digital Communications and Networks*, In Press, pp. 1-11.

Swan, M. (2015), *Blockchain: Blueprint for a New Economy (1st ed.)*, O'Reilly Media, Sebastopol, CA.

Tapscott, D. and Tapscott, A. (2016), *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, Portfolio/Penguin, New York, NY.

Tapscott, D. and Tapscott, A. (2017), "How blockchain will change organizations," *MIT Sloan Management Review*, Vol. 58, No. 2, pp. 10-13.

Vizier, G. and Gramoli, V. (2020), "ComChain: A blockchain with Byzantine fault-tolerant reconfiguration," *Concurrency and Computation: Practice and Experience*, Vol. 32, No. 12, e5494, pp. 1-19.

Wagner, K., Keller, T. and Seiler, R. (2019), "A comparative analysis of cryptocurrency consensus algorithms," *Proceedings of 16th International Conference Applied Computing*, pp. 217-225.

Wang, F., Ji, Y., Liu, M., Li, Y., Li, X., Zhang, X. and Shi, X. (2021), "An optimization strategy for PBFT consensus mechanism based on consortium blockchain," *Proceedings of the 3rd ACM International Symposium on Blockchain and Secure Critical Inflastructure*, pp. 71-76.

Wang, Y., Han, J. H. and Beynon-Davies, P. (2019), "Understanding blockchain technology for future supply chains: A systematic literature review and research agenda," *Supply Chain Management: An International Journal*, Vol. 24, No. 1, pp. 62-84.

Wang, Y.-Y., Tao, F. and Wang, J. (2021), "Information disclosure and blockchain technology adoption strategy for competing platforms," *Information & Management*, In Press, 103506, pp. 1-11.

Xu, L. D., Xu, E. L. and Li, L. (2018), "Industry 4.0: State of the art and future trends," *International Journal of Production Research*, Vol. 56, No. 8, pp. 2941-2962.

Xu, X. and Choi, T.-M. (2021), "Supply chain operations with online platforms under the cap-and-trade regulation: Impacts of using blockchain technology," *Transportation Research Part E: Logistics and Transportation Review*, Vol. 155, 102491, pp. 1-21.

Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N. N. and Zhou, M. (2019), "Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism," *IEEE Access*, Vol. 7, pp. 118541-118555.

Zheng, K., Zhang, Z. (J.), Chen, Y. and Wu, J. (2021), "Blockchain adoption for information sharing: Risk decision-making in spacecraft supply chain," *Enterprise Information Systems*, Vol.15, No. 8, pp. 1070-1091.

Zheng, W., Zheng, Z., Chen, X., Dai, K., Li, P. and Chen, R. (2019), "NutBaaS: A blockchain-as-a-service platform," *IEEE Access*, Vol. 7, pp. 134422-134433.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X. and Wang, H. (2018), "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, Vol. 14, No. 4, pp. 352-375.

Zhong, B., Wu, H., Ding, L., Luo, H., Luo, Y. and Pan, X. (2020), "Hyperledger fabric-based consortium blockchain for construction quality information management," *Frontiers of Engineering Management*, Vol. 7, No. 4, pp. 512-527.

Zinovyeva, E., Reule, R. C. G. and Härdle, W. K. (2021), "Understanding smart contracts: Hype or hope?" *SSRN Electronic Journal*, 15 Mar 2021, pp. 1-75.

崔宇 (2022),「ブロックチェーン：ビットコイン」，伊藤宗彦・松尾博文・富田純一編著，『1 からのデジタル経営』碩学舎，pp. 61-76.

RETHINKING BLOCKCHAIN AND ITS MECHANISM: FROM CRYPTOCURRENCIES TO SMART CONTRACT APPLICATIONS

Yu Cui
Otemon Gakuin University

ABSTRACT
In the field of industrial and supply chain management, blockchain symbolizes a paradigm of autonomous decentralized system. In spite of increasing interests in it, there are few literatures which concretely explain how the blockchain works and how it brings about the change in business process and daily management of the enterprise as a new management system architecture. In about 10 years after the birth of blockchain, this paper highlights and explains representative examples in each of three development stages of blockchain. Through the review of literatures in various fields, the operating principle of Bitcoin, Ethereum and Hyperledger Fabric are analyzed. From the viewpoint of operations management, their features and effects on the current system are explained in detail and schematically. Moreover, on the consensus algorithms which are called the essence of blockchain, this paper introduces the one which is respectively suitable for public chain, private chain and consortium chain, which are the main frameworks of blockchain. It also explains application scenarios and examples in the context of business process and supply chain.

Keywords: blockchain, smart contract, consensus algorithm