No.734　ブロックチェーン　ー概要、展望、国内外事例

2016 年 8 月 6 日

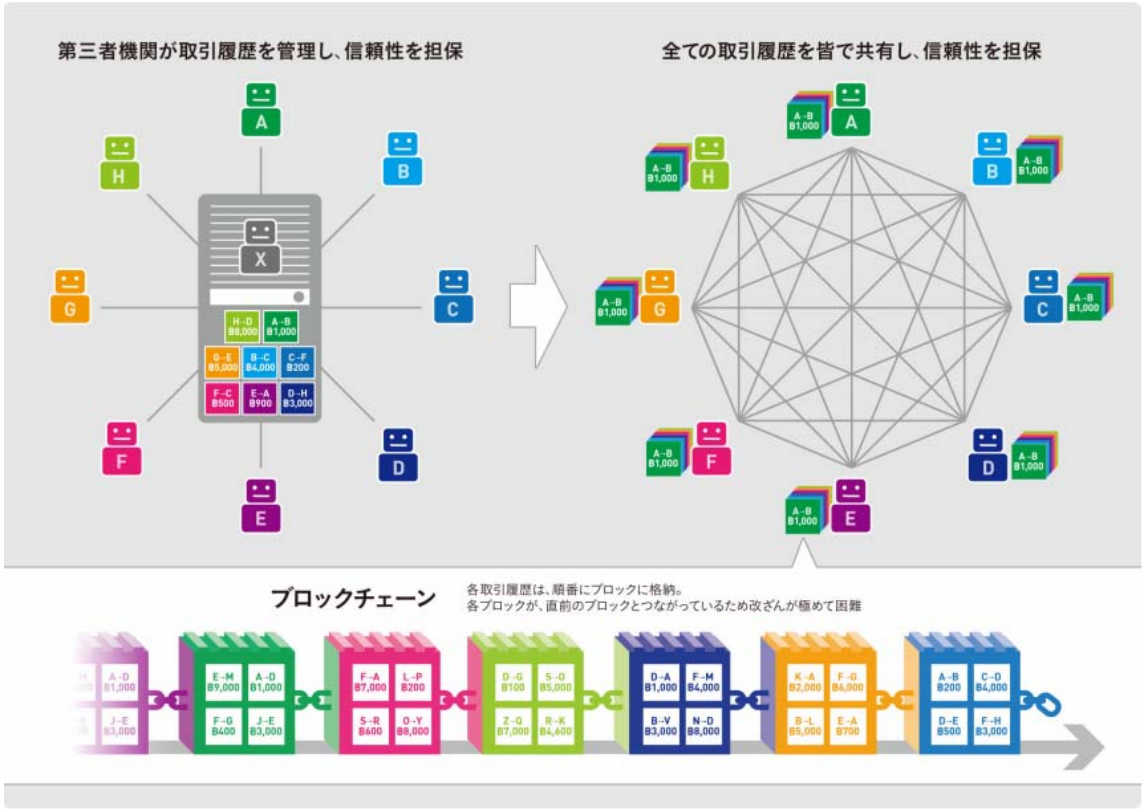
株式会社ユニバーサルエネルギー研究所

【概要】

近年、「ブロックチェーン」と呼ばれる技術が注目されている。これは「ビットコイン」と呼ばれる電子通貨の発明・発達とともに広まった技術であり、従来の金融機関のような集中管理型のデータベースを必要としない、分散型価値記録技術である。

本稿では、ブロックチェーンとは何か、これまでと何が変わるのか、そして現在どのような使用例があるのかについてまとめる。

【ブロックチェーンとは何か】



図．ブロックチェーンによる取引履歴の共有概念図

（出典：経済産業省 H27 ブロックチェーン技術を利用したサービスに関する国内外動向調査）

まず簡単な理解のために、従来の金融取引とビットコインを例に考える。

従来の金融機関は、台帳に「誰から」「誰へ」「いくら」という取引履歴を管理していた。そして金融機関自身がその取引履歴の信頼性を担保することで、金融取引をおこなっていた。したが

って、ある金融機関 X が関係するすべての取引履歴は、X 自身が管理し、かつ信頼性を担保しなければならなかった。

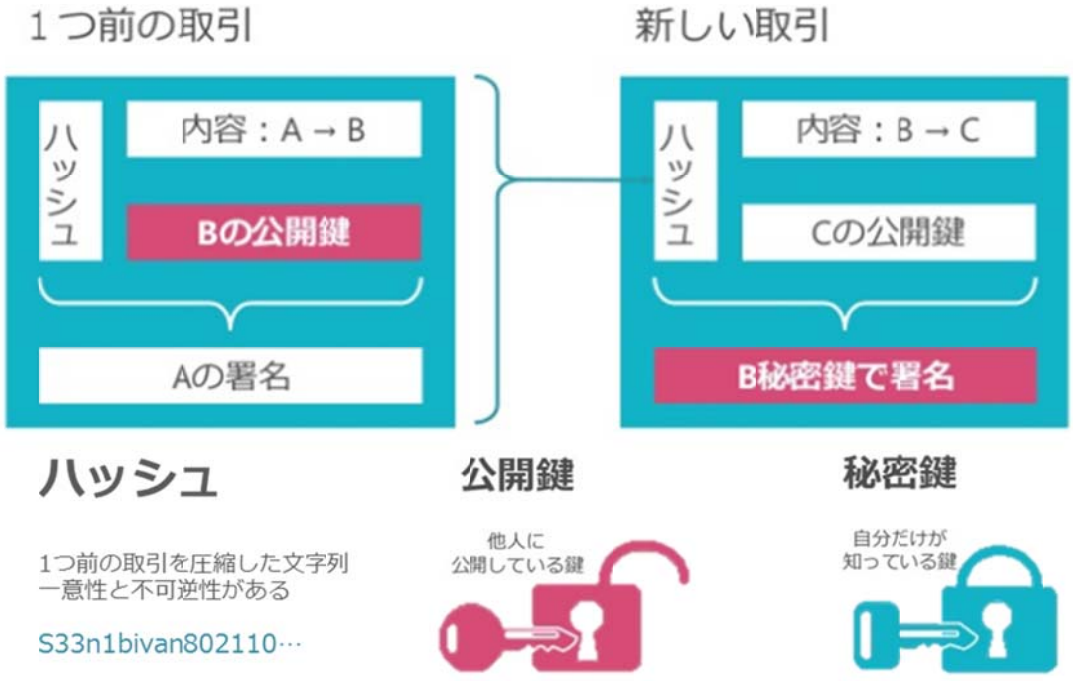
一方ビットコインは、ブロックチェーン技術を活用した、取引履歴を管理する主体が分散した、新しい金融取引手法による通貨である。特徴は、以下の４点。

（１）すべての取引履歴はすべてのビットコイン利用者によって管理され、障害に極めて強い。

（２）取引履歴は、「ブロック」単位で管理されている。

（３）各ブロックは１つ前のブロックの情報を持ち、「チェーン」のように繋がっていく。

（４）改ざんには非現実的な計算量が必要となるため、堅牢で信頼性が担保されている。



図．ブロックチェーンにおける各取引の保証原理図

（出典：各種資料より㈱ユニバーサルエネルギー研究所が作成）

例えば、ビットコインの取引（A さんから B さんへ送金）が発生したとする。この取引情報は、ひとつ前の取引のハッシュ、送金対象（B さん）の公開鍵、A さんの秘密鍵による電子署名と組み合わせて保存される。次の取引（B さんが C さんへ送金）が発生した場合、その取引情報は、ひとつ前の取引（A→B＋ハッシュ＋B の公開鍵＋A の電子署名）のハッシュ、送金対象（C さん）の公開鍵、B さんの秘密鍵による電子署名とともに保存される。

ハッシュには、ひとつ前のブロックの情報が入っており、そのブロックの中のハッシュにはさらに前のブロックの情報が入っており、これが無限に連鎖する。この連続性が「チェーン」と呼ばれる理由である。過去の 1 ブロックを改変した場合、以後のすべてのブロック内のハッシュ値が連鎖的に変更される必要が生じる。ブロックチェーンが大きくかつ継続的に成長する限り、膨大なブロックのハッシュを他の全利用者よりも早く再計算することは非現実的であるため、ブロックチェーンによる取引履歴の改竄は極めて困難であり、真正性の高い取引が実現されているといえる。

また、過去の取引履歴が（ハッシュ値としてではあるが）共有され、トレーサビリティが担保されるため、透明性の高い取引が実現されているとも言える。

従来の金融機関の台帳は、ともするとデータベースを 1 行書き換えるだけでも改竄が可能であること比較すると、システムとしての信頼性・透明性はブロックチェーン技術のほうが高いと言える。

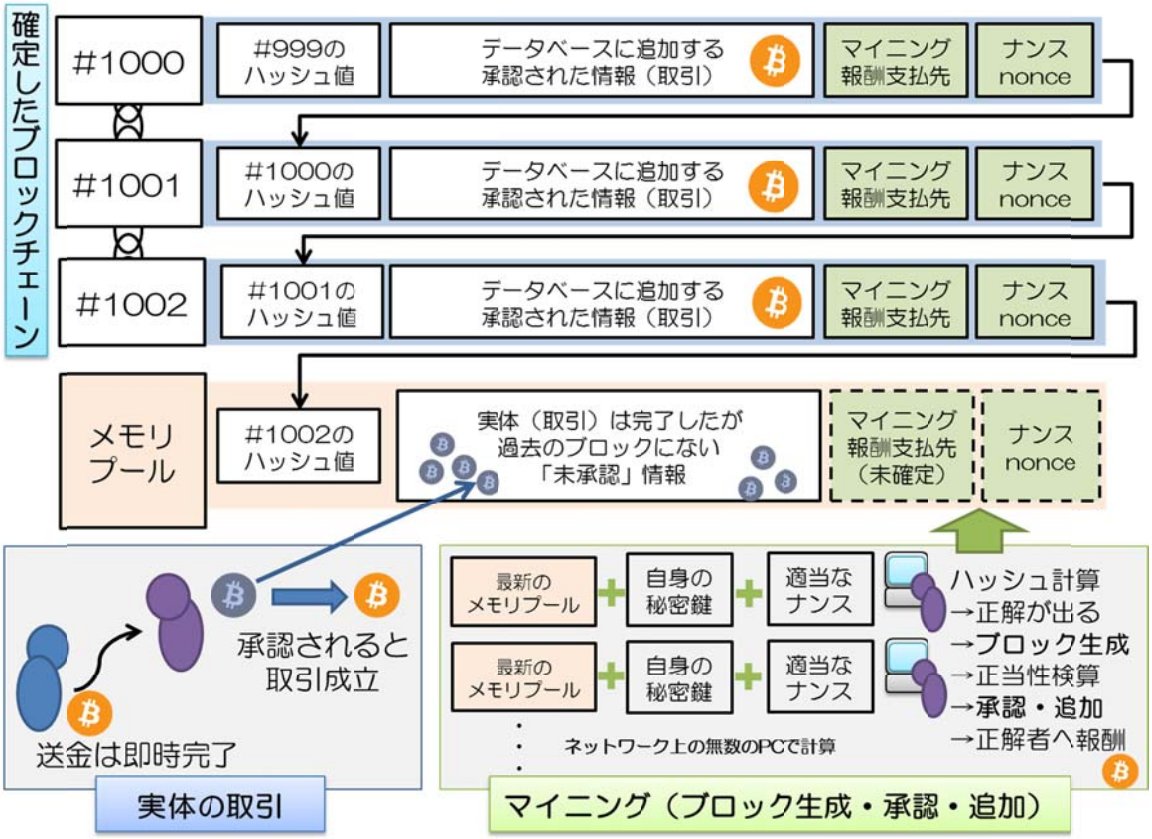
ここまでは金融を例に説明してきたが、台帳で管理する対象をより一般的な「価値取引」に置き換えると、さまざまなものをブロックチェーン技術により代替できる可能性があることがわかる。

すなわち、ブロックチェーンとは、「ネットワーク上において、価値取引情報を共有し、価値情報を相互承認することで、真正性・透明性を担保する手法」と言える。

【（詳細）ブロック生成・承認システム：ビットコインの例】

ブロックチェーンは、ブロック単位で管理されている。そして各ブロックは、ひとつ前のブロックのハッシュを包含することで連続性・唯一性を担保している。

さて、ここではそのチェーンにブロックを生成し、そのブロックが真正であることを確認し、既存のチェーンに追加するプロセスはどのようになっているかをまとめる。



図．ビットコインにおけるブロック生成・承認プロセスの詳細

（各種資料より㈱ユニバーサルエネルギー研究所が作成）

上図のように、各ブロックはひとつ前のハッシュ値を保有する（#1001 は#1000 のハッシュ値、#1002 は#1001 のハッシュ値）。上図では仮に#1002 ブロックまではチェーンが確定しているとした。この時、次のブロック#1003 が生成されるまでに何が起きるかを整理する。

まず、実体としてのビットコインの取引があったとする。このとき、ビットコインの送金行為・入金処理そのものは即時に成立するが、その取引そのものは「未承認」状態となり、メモリプールと呼ばれる一時保存領域に記録される。このメモリプールには、#1002 までのブロックチェーン内にはまだ記録されていない、実体として取引があった取引記録がストックされている。

このメモリプールから次のブロック（#1003）を生成するのが、ネットワークに接続している世界中の無数の PC（ノード）である。メモリプールおよび過去の取引情報のすべては、すべてのノードに逐次配信される。

各ノードでは、配信されたローカルのメモリプールから選んだ適当な量の取引情報と、#1002 のハッシュ値、自身の秘密鍵に加え、適当な自然数（ナンス（nonce）とよばれる）を加えて、これらをハッシュ関数でハッシュ値に変換する。この変換後のハッシュ値が、管理者の決めたルールに偶然合致した場合、このときの計算元データが、新ブロック#1003 となる。いわば、ハッシュ計算を用いた宝くじのようなものである。

この「あたり」ブロック#1003 は、即座に世界中に配信される。各ノードでは、受信した新#1003 の承認作業に入る。含まれる取引群によって残高不整合が起きないか、ハッシュ値は適当かが検証され、問題がなければ「ローカルで」チェーンにブロックが追加される。

各ノードは、#1003 を追加したのちに、各々で#1004 の計算に移行する。

ここで、#1003 の「あたり」が複数同時に配信されてしまう可能性、すなわちチェーンが分岐する場合（仮に#1003-A と#1003-B とする）が考えられる。

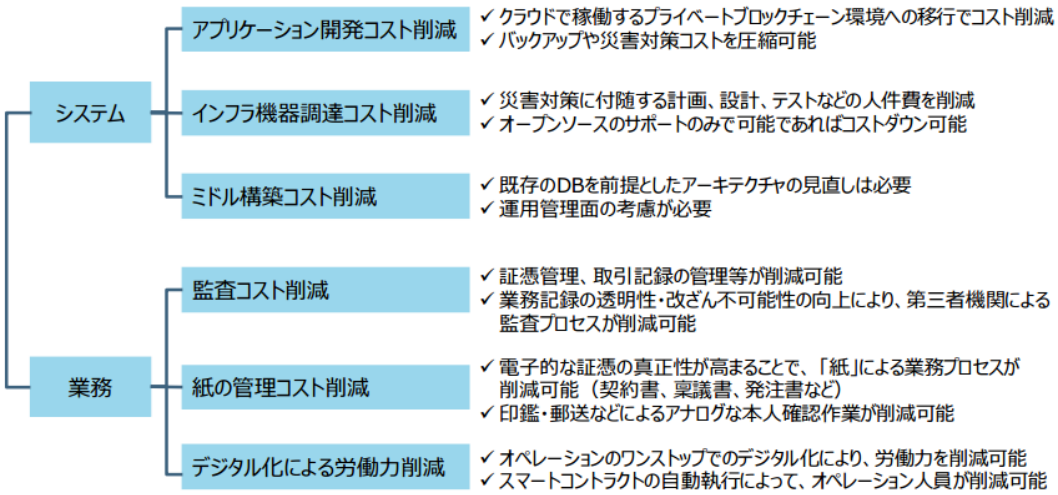
世界中のノードでは、それぞれ計算がおこなわれる。そのため#1003-A、#1003-B いずれの分岐に対しても次の#1004 が計算されてしまうが、各ノードは A、B いずれかのみに対して「あたり」を探す。そのうち、#1004 の「あたり」が発見される。この「あたり」が接続できるチェーンが選択され、#1004 が接続できないチェーンは破棄される。連続して、分岐が発生するのに十分同時的にブロックが生成される可能性は低いため、チェーンの分岐は長期的には続かないと考えられており、また実証されている。

また、#1003-A/B はいずれも内包している承認情報の内容は異なる（異なるノードで適当に選択したため）が、#1003 をもとに生成される#1004 は、#1003 と重複しない情報を含むため、いずれのチェーンが成長したとしても、取引情報が重複したり削除されることはない。

ただし、例えば悪意のあるノードが、非常に強力な計算機を使い、#1003-X を自作し、#1004-X、#1005-X、…と自分の都合の良い分岐を高速で成長させてしまい、正当な分岐が削除される可能性も考えられる。確率論的には、悪意のあるノードの計算量が、総ノードの計算量の 50%を上回らない限り、この種の攻撃は防ぐことができる（正当なチェーンの成長の方が速い）とされている。

【ブロックチェーンが社会へ与えるインパクトと課題】

ビットコインという仮想通貨に端を発したブロックチェーン技術は、様々な方向に拡張・展開されている。短期的に実現されるコスト削減効果について、および将来的に社会実装が進んだ場合に想定される応用分野について、下図に示す。



図．ブロックチェーンによりもたらされるコスト削減効果

（出典：経済産業省 H27 ブロックチェーン技術を利用したサービスに関する国内外動向調査）

図．ブロックチェーン技術による社会変革の可能性

（出典：経済産業省 H27 ブロックチェーン技術を利用したサービスに関する国内外動向調査）

ただし、ブロックチェーンは万能ではない上、社会実装は現在始まったばかりである。ブロックチェーンのもたらす利点が、実際の用途にもたらすメリットが十分にあるかを検討する必要がある。下図に想定される応用分野と、ブロックチェーンのどういった点が有益であるかを示す。

	地域通貨	土地の登記	サプライチェーン	シェアリングエコノミー	スマートコントラクト
➢スクリプトによりアプリケーションを実行可能			○		○
➢真正性の保証された取引が可能（二重支払の防止）	○	◎		○	○
➢データのトレーサビリティが可能で、透明性の高い取引が可能（改ざんが困難）	○	○	○	◎	○
➢サーバコスト（構築/運用）の低廉化	実証による検証が必要				
➢安定したシステムの構築・運用が可能（ゼロダウンシステム）	○				
➢中央管理者が不在でも、悪意を持つユーザがいてもエコシステムが安定維持される		○	○	○	○

図．ブロックチェーン技術の適用可能性の高いユースケース

（出典：経済産業省 H27 ブロックチェーン技術を利用したサービスに関する国内外動向調査）

上図において想定されている応用分野について、それぞれ以下で概要を述べる。

（１）地域通貨

自治体等が発行する地域通貨を、ブロックチェーン上で流通・管理する。一定の手続きを経て住民に地域通貨が付与され、それを地域内の商店や公共サービス等での支払に利用する。住民から住民へ譲渡をしたり、店舗が支払いで受け取った地域通貨を利用（地域内での原材料の調達に利用したり、地域内に在住する従業員への給与として支払ったりするなど）したり、当該通貨で納税した場合の税優遇といった使い方が考えられる。

（２）土地の登記

土地の物理的現況や権利関係の情報を、ブロックチェーン上で登録・公示・管理する。土地や建物、所有者に関する情報のほか、それらの移転や抵当権の設定なども記録、管理することも考えられ、関連する業務の効率化を図る。

（3）サプライチェーン

製品の原材料からの製造過程と流通・販売までを、ブロックチェーン上で追跡可能にする。

（4）シェアリングエコノミー

資産等の利用権移転情報、提供者や利用者の評価情報をブロックチェーン上に記録する。現在は Uber や AirBnB のような特定の企業が運営するプラットフォームにより提供されている、いわゆるシェアリングエコノミー型のサービスにおいて、利用権の管理および取引をブロックチェーン上で行うことを想定する。

（5）スマートコントラクト

契約条件、履行内容、将来発生するプロセス等をブロックチェーン上に記録することが可能であると考えられる。第三者を介在させずに契約の真正性担保などを実現できる。

ただし、ブロックチェーン技術は未成熟であり、十分な機能や信頼性があるとは言いがたい。以下に経済産業省がまとめたブロックチェーン技術の課題を示す。

ブロックチェーン技術の課題

（1）新ブロック生成に時間がかかる

ブロックチェーンの種類によるが、データ処理の確定に数秒～10 分程度かかるので、即時性が必要なアプリケーションには不向き。

（2）単位時間あたりのトランザクション件数が限られている

規定されているブロックに格納できるデータ量の上限と、新ブロック生成にかかる時間との関係から算出する、1 秒間に処理できるトランザクション件数が VISA 等の既存決済システムと比べて劣っている。

（3）実ビジネスでの運用方法等が確立されていない

実ビジネスへの適用例が少ないこともあり、ブロックチェーンに関わる各性能要件や仕様が明確ではなく、いわゆる SLA(Service Level Agreement)が整備されていない。

ブロックチェーン技術は、前述の課題を踏まえ、大きく 3 つの軸で技術開発・社会実装が進められている。

① ブロックチェーン上での記録・交換対象の拡張・汎用化

ビットコインのような価値情報だけでなく、様々な財の所有権やサービス（役務提供）を受ける権利（所有権、利用権など）の移転や証明にもブロックチェーンを応用する動き。

② コンセンサスアルゴリズムの改変・高性能化

ビットコインにおいて新ブロック生成に時間がかかるひとつの要因は、新ブロックを、分散したネットワーク内で相互に検証・承認するプロセスである PoW（Proof of Work）である。 この PoW に起因する課題に対応した、新たなコンセンサスアルゴリズムを採用する動き。

③ ネットワークへの参加を制限による参加者の信頼度の向上

不特定多数に参加を認めるのではなく、ある程度制限を掛けることで、コンセンサスの効率化とトランザクション処理の高速化を目指している。

【ブロックチェーンの活用事例】

図．ブロックチェーン技術の分野別活用事例

（出典：経済産業省 H27 ブロックチェーン技術を利用したサービスに関する国内外動向調査）

すでに国内外においてブロックチェーン技術を活用したサービスが数多く発表されている。ただし、ほとんどのサービスは実証が始まったばかりであり、世界的にブロックチェーン技術は黎明期にあると言える。我が国においては、社会的なインパクトの大きい分野において積極的な導入がなされているとかんがえられる。

図．ブロックチェーン技術の分野別活用動向

（出典：三菱総合研究所 2016 年 4 月 Monthly Report）

【海外の注目すべき動向】

●R3 CEV 社

世界各国の 42 社の金融機関が参加するコンソーシアムを主導しており、参加している企業群による Private Distributed Ledger を構築、複数の実証実験を実施中。我が国からは、三菱東京 UFJ、みずほ FG、SBI ホールディングスが参画中。使用されたブロックチェーンは「Ethereum（イーサリウム）」。

ちなみに「Ledger」は台帳の意。ブロックチェーンを利用する事業体・サービスによく現れる。

●NASDAQ

ブロックチェーン技術を活用した未公開株式取引システム「Nasdaq Linq」を発表。従来は株式未公開企業が同市場に参加するためのクラウドベースのシステムとして提供していた「Exact Equity」を補完するシステムとなる。当面、本システムは、Chain（ブロックチェーン関連企業）、ChangeTip（電子マネー関連スタートアップ）、PeerNova（暗号化台帳技術関連企業）、Synack（サイバーセキュリティ関連企業）、TangoMe（メッセージングアプリケーション関連企業）、Vera（企業向けメッセージングアプリ関連企業）の 6 社をと対象として使用される。

さらに 2016 年 5 月、NASDAQ Linq は太陽光エネルギー市場におけるブロックチェーン活用の事例を発表した。ネバダ州のスタートアップ「Filament」の技術により、太陽光パネルを IoT デバイス化する（ネットワーク接続し、管理・制御下におく）。このパネル情報をもとに、NASDAQ Linq の提供する API 上で電力証書をブロックチェーン上に証券化（トークン化）し売買する仕組み。

デモでは、西海岸で発電された太陽光エネルギーを即時的にニューヨークで購入するケースが披露された。トークン化された電力証書は発行者の匿名性が保たれる。

●Linux Foundation
ブロックチェーン技術を活用した共同開発プロジェクト「Open ledger」プロジェクトを発表。オープンソース分散型台帳（Distributed Ledger）フレームワークとその開発者の育成を狙うとしている。本プロジェクトへは 20 社以上が参加しており、我が国からは日立、NEC、NTT データが参加している。

●ISO
2016 年の ISO／TC68（金融サービス）年次総会において、”FinTech Services Technical Advisory Group”が設置された。またデジタル通貨に関する SG（Study Group）の提言にしたがい、fiat digital currency（不換デジタル通貨。金貨・銀貨のような本位貨幣との兌換が保証されない、日本銀行券のような法定通貨のデジタル版）について ISO4217 による付番が可能であることが確認された。ISO4217 による付番は、日本円であれば JPY、米国ドルであれば USD といったコードが割当てられることを意味する。
また現在、オーストラリアが主導してブロックチェーンおよび分散型元帳技術に関する TC の設置にかかる国際投票が実施されている（～2016 年 7 月 14 日）。この TC では、アプリケーションおよびシステム間でのインターオペラビリティやデータ交換をサポートするためのブロックチェーンおよび分散型元帳技術の標準化を目的としている。ISO では現在あらゆる産業分野に渡り約 250 の TC が活動している。

【本邦の注目すべき動向】
●ビットプロパティー
余剰電力などの各種エネルギーを個人間で売買できるプラットフォームの創出を謳う「ビットプロパティー」は、2016 年 6 月 17 日から「ブロックチェーンによるスマートコントラクトサービス　分散型 e-REIT『Bit property』」と銘打った Web サイトを公開した。不動産に対し、ビットコインにて REIT トークン（証券）の先行購入が可能な仕組みとした。

図．売買取引の対象とされた不動産：沖縄県石垣島太陽光発電施設
（出典；PR TIMES　ビットプロパティー社広報）

しかし、配分利益の原資になる不動産である石垣島の太陽光発電施設が未購入（株式会社日建はウジングより購入予定とされた）であること、ビットコインによる出資を呼びかけていること、ビットコインによる利益配分を謳っていること、それらの商取引が金融商品取引法におけるファンド規制や不動産特定共同事業法への抵触のおそれがあること、原資として公表していた 2 万 BTC（ビットコイン、取得時価額 14 億円相当）の実在が確認できないことなどを指摘されたことを受け、Web サイトの案内を中止した。

2016 年 6 月 22 日に適法性に関する見解を発表した後、7 月 8 日にコンプライアンス法務担当弁護士の委嘱を発表し、現在まで活動を休止している、

図．Bitproperty 社の分散型 e-REIT 案内（現在は削除）
（出典；PR TIMES　ビットプロパティー社広報）

●Orb（オーブ）社　「SmartCoin」

図．Orb 社のサービス「SmartCoin」を支える技術

（出典：Orb 社 HP）

Orb 社は国産ブロックチェーン技術「Orb」を活用したクラウドプラットフォームの提供、プラットフォーム上での仮想通貨ならびに関連サービスの開発をしているスタートアップ企業。現在、「SmartCoin」という仮想通貨サービスのベータ版を提供している。

ビットコインはグローバルに唯一のブロックチェーンを構築し、その単一チェーン上での取引単位として BTC を使用しているが、これに対し SmartCoin は Orb プラットフォーム上で企業や自治体がそれぞれのブロックチェーンを持つ仕組みとなっている。ブロックチェーンのオーナーは、仮想通貨を発行・管理でき、特定のユーザに任意のタイミング・額を付与したり、自然逓減率を導入したりすることができるため、ユーザのインセンティブを設計することができる。2016 年 5 月からは主に不動産取引の決済保全・信託（エスクロー）サービスを提供するエスクロー・エージェント・ジャパン社と調査研究・実証事業に関する基本合意を締結しており、同年 7 月 12 日には三井住友信託銀行、住信 SBI ネット銀行とともにエスクローサービス等における資金決済に関する事務負担の軽減を目的とした Orb 上での認証及び決済システムの調査研究及び実証実験を共同して行う基本合意書を締結している。

以上