Association of International Certified Professional Accountants™

AICPA® CIMA®

ブロックチェーン用語集

注：本用語集は、本協会のすべてのブロックチェーン及びデジタル資産関連コンテンツに関する参照資料として作成された。本文書に含まれる用語には、*AICPA のブロックチェーン CPE 各コース*、*Digital Assets Practice Aid（デジタル資産実務支援）*のほか、*Implications of the Use of Blockchain in SOC for Service Organization Examinations（受託会社に関する SOC 業務におけるブロックチェーンの使用がもたらす影響）*からの用語が含まれる。上記各文書の更新・改訂に伴い、本用語集も合わせて更新される。

Access control mechanism (access control) アクセス・コントロール・メカニズム（アクセス・コントロール）：承認された個人、組織又はノードのみに、特定のブロックチェーンネットワークに参加する、又はネットワーク上で取引を行うことを許可する統制。アクセス・コントロールは、パブリック型ブロックチェーンとプライベート型ブロックチェーンの主要な相違点の一つである。

Airdrop エアドロップ：1つ又は複数のブロックチェーンアドレスに対するデジタル資産の配分で、多くの場合、受け取る側のブロックチェーンアドレスを全く考慮せずに行われる。多くの場合、エンティティはデジタル資産に対する認識や関心を生み出す一方法としてエアドロップを採用し、エアドロップされたデジタル資産の受領又は獲得には一定の基準を課す場合がある。

Bad actor バッドアクター：違法又は不正な意図を持っている可能性のあるデジタル資産エコシステムの参加者。

Bitcoin ビットコイン：暗号資産の一例。（「暗号資産」を参照）

Block ブロック：ブロックチェーンに記録される、デジタル資産取引の 1 つのまとまり。

Blockchain technology. ブロックチェーン技術：暗号化技術を使用して結び付けられる記録（ブロックと呼ばれる）のリストを記録する技術。各ブロックには暗号化されたハッシュ、タイムスタンプ及び取引データが含まれる。

Block explorer ブロックエクスプローラー：取引の詳細、ブロック及びアドレスを検索・表示するための特殊なソフトウェア又はウェブベースブラウザ。

Consensus mechanism コンセンサス・メカニズム：一連のルール（プロトコル）やアルゴリズムを使用して、コンセンサス（ブロックチェーン内の複数の参加者によって記録された値についての合意等）に至る手順を定義する。（コンセンサス・アルゴリズム、又はコンセンサス・プロトコルとも呼ばれる。）

Crypto asset 暗号資産[1]：デジタル資産のうち、

- 交換の仲介として機能し、かつ
- 以下のすべての特徴を有する種類のもの。
  - 法域を有する統治機関（主権国家等）によって発行されたものではない。
  - 保有者と他の当事者との間での契約を生じさせない。
  - 米国の 1933 年証券法又は 1934 年証券取引所法における証券とはみなされない。

これらの特徴は包括的なものではなく、他の事実及び状況を考慮することが必要な場合がある。上記の特徴を満たす暗号資産の例として、ビットコイン、ビットコインキャッシュ、イーサが挙げられる。

[1] （訳註）
日本において一般的に用いられている「暗号資産」の定義の一つとして、資金決済に関する法律第２条第５項に定められている内容が挙げられる。

Cryptographic key (key) 暗号鍵(鍵):平文を暗号化されたメッセージに変換するために、暗号アルゴリズムにより使用されるビット文字列。ブロックチェーンネットワークで暗号化されたメッセージを符号化・復号するのに必要な暗号鍵のペアが、公開鍵と秘密鍵である。

- Private key 秘密鍵:個人的に保有され、暗号化されたメッセージを解読するために公開鍵と併せて使用する必要がある暗号鍵。
- Public key 公開鍵:特定の受け手を意図したメッセージを暗号化するため、誰もが使用できる暗号鍵。

Cryptography 暗号化技術:通信やデータをセキュアにするための技術。

Digital asset デジタル資産:分散型デジタル台帳(ブロックチェーンと呼ばれる)上に、検証及びセキュリティを目的とする暗号化技術を使用して作成されたデジタル記録。デジタル資産は、交換手段として、モノの提供やサービスへのアクセスを表すものとして、あるいは証券等の金融手段として等、さまざまな目的で使用できることを特徴とする。

Digital asset ecosystem デジタル資産エコシステム:デジタル資産に参加又は関与するすべてのエンティティ。これには、開発、維持管理、利用(購入、販売、投資、商取引、交換等)、カストディもしくはセキュリティ(ホットウォレットとコールドウォレットのプロバイダー、有資格のカストディアン、又は他のカストディサービス等)、又は検証等、エコシステムのさまざまな要素に関与しているエンティティが含まれる場合がある。

Digital signature デジタル署名:秘密鍵、公開鍵、メッセージ、及びハッシュ化の組み合わせにより、デジタル署名が生成される。デジタル署名はすべての取引に対して一意であり、メッセージの発信者が秘密鍵へのアクセスを有していることを証明する方法の 1 つである。

Distributed ledger technology (DLT) 分散型台帳技術(DLT):あらゆるブロックチェーン技術、及びブロック又はブロックチェーンを使用しないさまざまな技術の総称。ブロックチェーンはすべて DLT だが、あらゆる DLT がブロックチェーンというわけではない。

Encryption 暗号化:不正なアクセスを防止する方法でデータを符号化するプロセス。

Ethereum イーサリアム:他のアプリケーションをその上に構築できるブロックチェーンプラットフォームであり、スマートコントラクトプラットフォームである。イーサはイーサリアム上で通用する暗号資産である。(「暗号資産」と「ブロックチェーン技術」を参照)

Exchanges 取引所:暗号資産を含むデジタル資産の売買のためのプラットフォーム。(「デジタル資産取引所」とも呼ばれる。)

Fiat currency フィアット通貨:主権国家により発行される、一般に受け入れられている法定通貨(ドル、ポンド、ユーロ等)。

Fork フォーク:コンセンサス・プロトコルへの変更。

- Hard fork ハードフォーク:以前のバージョンのコンセンサス・プロトコルと遡及的に互換できないフォークで、レガシーのコンセンサス・プロトコルを使用しているコンピューターは、新しいコンセンサス・プロトコルの下で生成された取引を拒絶する。
- Soft fork ソフトフォーク:以前のバージョンのコンセンサス・プロトコルと遡及的に互換可能なフォークで、新しいコンセンサス・プロトコルを使用して生成された取引は、レガシーのコンセンサス・プロトコルを使用しているコンピューターに受け入れられる。

Hashing ハッシュ化:データを一連の数字と文字に変換するプロセス。

Hybrid blockchain ハイブリッド型ブロックチェーン:パブリック型とプライベート型の両方のブロックチェーンの特徴を合わせ持つネットワークで、実装で必要な一定のプライバシー、セキュリティ及び可監査性をブロックチェーンに組み込むことができる。(「パブリック型ブロックチェーン」と「プライベート型ブロックチェーン」を参照)

Immutability 不変性:変更ができない、又は変更を許さないという特徴。ブロックチェーンネットワークにおいては、ブロックチェーン技術の特定の機能が以前に検証された取引がその後に改変又は変更されることを防ぐという概念をいう。

Key generation or key ceremony 鍵生成又はキーセレモニー:公開鍵及び秘密鍵を生成するプロセス。(「暗号鍵」を参照)

Key management risk 鍵管理リスク:秘密鍵が適切にセキュア化又はバックアップされず、結果としてデータやデジタル資産が失われるリスク。

Node ノード:ブロックチェーンの完全な又は部分的なコピーをダウンロード及び維持し、ブロックを検証し、取引をリレーできる参加者。

Off-chain transactions オフチェーン取引:基礎となるブロックチェーンの外部で記録される取引(パブリック型ブロックチェーンに記録されない、第三者のウォレットサービスプロバイダーによるそのユーザー間での移転等)。

On-chain transactions オンチェーン取引:基礎となるブロックチェーンに記録される取引。

Peer-to-peer network P2P ネットワーク:参加者が平等な権限を持ち、他のネットワーク参加者が直接利用可能な特定のリソースを作成する分散型ネットワーク。

Privacy coins プライバシーコイン：ブロックチェーンの観察により取引を行う当事者の ID を特定することが限定されるブロックチェーンデジタル資産。

Private blockchain (permissioned) プライベート型ブロックチェーン（許可型）：特定のエンティティ又はグループが管理する、アクセスが制限されたネットワークで、従来の集中型ネットワークと類似している。

Pseudo-anonymous 仮名性：ブロックチェーン環境において、デジタル資産が複数のブロックチェーンアドレス間で交換され、それら取引当事者の具体的な名前と ID が当該アドレスによって明確に特定されないという状況を表すために使用される。

Public address (blockchain address) 公開アドレス（ブロックチェーンアドレス）パブリック型ブロックチェーンでのデジタル資産の受領を記録するために用いられる一意の識別子。ブロックチェーンアドレスは公開鍵の暗号化操作（すなわちハッシュ化）により生成され、メッセージを受領するため誰もが共有できる。

Public blockchain (permissionless) パブリック型ブロックチェーン（自由参加型）：参加者がデータを閲覧し、読み取り、書き込めるオープンネットワークで、どの参加者も管理者でないもの（ビットコイン、イーサリアム等）。

Sharding シャーディング：暗号化技術を使用したデータの分割。

Smart contracts スマートコントラクト：参加者が相互にやり取りをする上で合意する一連のルールを含むデジタルコード。事前に定義されたルールに合致すると、このコードにより自動的に合意が執行される。このスマートコントラクトコードは合意又は取引の実行を促進、承認及び執行し、その後、取引の結果がブロックチェーンに書き込まれる。

Stablecoins ステーブルコイン：フィアット通貨、コモディティ、デジタル資産又は資産バスケット等の他の資産の価値とその価値をリンク（「ペッグ」等）させることよって、価格変動を最低限に抑えるために設計された仕組みを含むデジタル資産。（「デジタル資産」を参照）

Validator バリデーター：ブロックチェーンネットワークの参加者で、取引の検証を担うコンセンサス・メカニズムの構成要素。プルーフ・オブ・ワーク（Proof of Work）を使用する特定のブロックチェーンに関しては、バリデーターはマイナーと呼ばれる。（「コンセンサス・メカニズム」を参照）

Wallet ウォレット：秘密鍵とそれに関連する公開鍵又はブロックチェーンアドレスを保管するために使用される媒体で、中には、参加者に P2P ネットワークへの取引の送信、及び他者からのデジタル資産の受領を許可するものもある。以下のような複数の種類のウォレットがある。

- Cold storage wallet コールド・ストレージ・ウォレット：インターネットに接続されていないウォレットで、オフラインウォレットとも呼ばれる。
- Hardware wallet ハードウェアウォレット：ソフトウェアの代わりに秘密鍵を生成するハードウェア（物理的）デバイス。
- Hot storage wallet ホット・ストレージ・ウォレット：インターネットにアクセス可能なウォレット。ウォレットの最も一般的な実装で、単にウォレットと呼ばれることもある。
- Mobile wallet モバイルウォレット：モバイルアプリを通じてアクセス可能なウォレット。
- Multisig (multisignature) wallet マルチシグ（マルチ署名）ウォレット：ウォレットアドレスからデジタル資産を移転するために 2 つ以上の署名を必要とするウォレット。
- Physical wallet フィジカルウォレット：鍵をオフラインで物理的形態により保管するために用いられる媒体（ペーパーウォレット等）。
- Software wallet ソフトウェアウォレット：ハードウェアウォレット又はフィジカルウォレット以外のウォレットをいう。
- Third-party hosted wallet service 第三者がホストするウォレットサービス：任意のエンティティのデジタル資産を保有する第三者サービスプロバイダーで、カストディウォレット（custodial wallet）とも呼ばれる。