2020 年 11 月 30 日

取扱暗号資産概要説明書

この概要説明書は、一般社団法人日本暗号資産取引業協会が公表する「暗号資産概要説明書」を基に作成しています。
情報の正確性、信頼性、完全性を保証するものではありません。

暗号資産の日本語名称	ビットコイン
ティッカーコード	BTC、XBT
発行開始年月日	2009 年 1 月 3 日
発行者	なし
発行主体概要	不特定の保有・移転管理台帳記録者による発行プログラムの集団・共有管理
発行方法	分散型の価値保有・価値移転の台帳データ維持のための、暗号計算および価値記録を行う記録者への対価・代償として発行される暗号資産
発行可能上限額	約 2,100 万 BTC
保有・移転記録の秘匿性	ハッシュ関数（SHA－256、RIPEMD－160）、楕円曲線公開鍵暗号の暗号化処理を施しデータを記録
価値移転認証の仕組み	台帳形式 価値移転認証を求める暗号データを記録者が解読し、利用者および移転内容の真正性を確認して価値移転記録台帳の記録を確定する
価値移転記録の信頼性確保の仕組み	Proof of work コンセンサス・アルゴリズム（分散台帳内の不正取引を排除するために、記録者全員が合意する必要があるが、その合意形成方式）の 1 つであり、一定の計算量を実現したことが確認できた記録者を管理者と認めることで分散台帳内の新規取引を記録者全員が承認する方法
価値移転ネットワークの信頼性に関する説明	オープンソース・ネットワークの脆弱性に対し、暗号により連鎖する台帳群（ブロックチェーン）を用い、難易度の高い作業証明の蓄積されたチェーンが選択されることが Bitcoin のコンセンサス・アルゴリズムによって規定されており、データ改竄の動機を排除し、信頼性を確保している。
記録者の信用力に関する説明	記録者による多数の合意がなければ不正が成立せず、記録者が十分に多数であることによって、個々の記録者の信用力に頼らず、記録保持の仕組みそのものを信用の基礎としている

暗号資産の日本語名称	イーサリアム
ティッカーコード	ETH
発行開始年月日	2015 年 7 月 30 日
発行者	Ethereum Foundation
発行主体概要	不特定の保有・移転管理台帳記録者による発行プログラムの集団・共有管理
発行方法	初期発行と、分散型の価値保有・価値移転の台帳データ維持のための、暗号計算および価値記録を行う記録者への対価・代償としてプログラムにより自動発行
発行可能上限額	未定
保有・移転記録の秘匿性	公開鍵暗号の暗号化処理を施しデータを記録
価値移転認証の仕組み	台帳形式。価値移転認証を求める暗号データを記録者が解読し、利用者および移転内容の真正性を確認して価値移転記録台帳の記録を確定する。
価値移転記録の信頼性確保の仕組み	Proof of Work 現状は Bitcoin と同様の Proof of Work を用いているが、difficulty の累積和の意味で最長のチェーンを採択するのではなく、アンクルブロックの数も考慮して最も多くのブロックが累積したチェーンを採択する点で若干の差異がある。 また、Ethereum 2.0 において Proof of Stake に移行する予定であり、いわゆるマイニングの代わりとして、ETH をステークしている量に応じてブロック生成権が付与される形態となる。
価値移転ネットワークの信頼性に関する説明	オープンネットワークの脆弱性に対し、暗号により連鎖する台帳群（ブロックチェーン）および記録者による多数決をもって移転記録が認証される仕組みを用い、多数の記録者のネットワークへの参加を得ることによって、データ改竄の動機を排除し、信頼性を確保する。
記録者の信用力に関する説明	記録者による多数の合意がなければ不正が成立せず、記録者が十分に多数であることによって、個々の記録者の信用力に頼らず、記録保持の仕組みそのものを信用の基礎としている。

暗号資産の日本語名称	ビットコインキャッシュ
ティッカーコード	BCH（注）
発行開始年月日	2017 年 8 月 1 日
発行者	なし
発行主体概要	不特定の保有・移転管理台帳記録者による発行プログラムの集団・共有管理
発行方法	分散型の価値保有・価値移転の台帳データ維持のための、暗号計算および価値記録を行う記録者への対価・代償として発行される暗号資産
発行可能上限額	約 2,100 万 BCH
保有・移転記録の秘匿性	ハッシュ関数（SHA－256、RIPEMD－160）、楕円曲線公開鍵暗号の暗号化処理を施しデータを記録
価値移転認証の仕組み	台帳形式 価値移転認証を求める暗号データを記録者が解読し、利用者および移転内容の真正性を確認して価値移転記録台帳の記録を確定する
価値移転記録の信頼性確保の仕組み	Proof of work コンセンサス・アルゴリズム（分散台帳内の不正取引を排除するために、記録者全員が合意する必要があるが、その合意形成方式）の一つであり、一定の計算量を実現したことが確認できた記録者を管理者と認めることで分散台帳内の新規取引を記録者全員が承認する方法。
価値移転ネットワークの信頼性に関する説明	オープンネットワークの脆弱性に対し、暗号により連鎖する台帳群（ブロックチェーン）および記録者による多数決をもって移転記録が認証される仕組みを用い、多数の記録者のネットワークへの参加を得ることによって、データ改竄の動機を排除し、信頼性を確保する。
記録者の信用力に関する説明	記録者による多数の合意がなければ不正が成立せず、記録者が十分に多数であることによって、個々の記録者の信用力に頼らず、記録保持の仕組みそのものを信用の基礎としている

注：2020 年 11 月 15 日のハードフォークにより、BCHA と BCHN に分岐した。当社は BCHN が参照するチェーンを Bitcoin Cash (BCH)として表記する。

暗号資産の日本語名称	エックスアールピー（リップル）
ティッカーコード	XRP
発行開始年月日	2012 年 9 月
発行者	あり
発行主体概要	Ripple Labs Inc.
発行方法	2012 年のネットワーク発足時に全て発行済み
発行可能上限額	1,000 億 XRP
保有・移転記録の秘匿性	取引は ED25519 と SECP256K1 によって暗号署名が行われ、ハッシュには SHA512 half が使われる。Multi-sign 機能によって高度のセキュリティを可能としている
価値移転認証の仕組み	独自のコンセンサス・アルゴリズム 3～5 秒ごとにバリデーターが台帳における新たな取引について投票を行い、80％以上の合意を得た取引が承認されたとみなされ、パブリックな台帳に記録される。
価値移転記録の信頼性確保の仕組み	Ripple Consensus Ledger（RCL）はビザンチン将軍問題を解決する独自のコンセンサス・アルゴリズムを採用し、Proof-of-Work よりもより速くかつ効率的に取引を承認することができる。信頼される認証済み法人バリデーター（検証者）が取引についての投票を行い、80%以上の合意が得られた取引については承認を行う。RCL では決済が 3～5 秒ごとに実行され、1 秒につき 1,500 の取引まで対応できるスケーラビリティを有する。
価値移転ネットワークの信頼性に関する説明	信頼するバリデーターが意に反して結託した場合、台帳とデータは改ざんされる可能性がある。また、暗号資産の移転等を支えるコミュニティの崩壊等により、暗号資産の移転が不可能となる可能性及びその他の理由等に起因し、最悪の場合は、暗号資産の価値がゼロとなる可能性がある。
記録者の信用力に関する説明	パブリックな台帳ネットワークを保持する動機がある、確認・証明済みの法人がバリデーター（検証者）になっている。そのうち、トップのバリデーター運用のパフォーマンスを示した複数のバリデーターのみが Unique Node List （UNL）という推奨リストに追加され、ネットワークのノードによって参照されるため個々の記録者の信用は必要としない仕組みになっている。

暗号資産の日本語名称	ライトコイン
ティッカーコード	LTC
発行開始年月日	2011 年 10 月
発行者	なし
発行主体概要	不特定の保有・移転管理台帳記録者による発行プログラムの集団・共有管理
発行方法	分散型の価値保有・価値移転の台帳データ維持のための、暗号計算および価値記録を行う記録者への対価・代償として発行される暗号資産
発行可能上限額	8,400 万 LTC
保有・移転記録の秘匿性	Scrypt アルゴリズムを用いたプルーフオブワーク
価値移転認証の仕組み	台帳形式 価値移転認証を求める暗号データを記録者が解読し、利用者および移転内容の真正性を確認して価値移転記録台帳の記録を確定する
価値移転記録の信頼性確保の仕組み	Proof of work Scrypt アルゴリズムを用いたプルーフオブワークの仕組みにより、Litecoin ブロックチェーンの維持管理に参加する者が、ブロック生成に必要な、およそ 2 分 30 秒（150 秒）間隔で発見可能な難易度に調整され、かつ完全に確率的で計算コストの掛かる特定のナンス（nonce）を見つけ、Litecoin ネットワークに対し伝播することをもって、維持管理参加者が指定するアドレスに対してプロトコルから付与される。
価値移転ネットワークの信頼性に関する説明	オープンネットワークの脆弱性に対し、暗号により連鎖する台帳群（ブロックチェーン）および記録者による多数決をもって移転記録が認証される仕組みを用い、多数の記録者のネットワークへの参加を得ることによって、データ改竄の動機を排除し、信頼性を確保する。
記録者の信用力に関する説明	記録者が多数であることによって、個々の記録者の信用に頼らない仕組みを構築しているため、価値喪失の可能性はない