2020 年 8 月 6 日

# 取扱仮想通貨概要説明書

一般社団法人日本仮想通貨交換業協会 ( JVCEA ) が公表する「仮想通貨概要説明書」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。

| | |
|---|---|
| 仮想通貨の名称 | ビットコイン |
| ティッカーコード | BTC、XBT |
| 仮想通貨の単位 | 0.00000001 BTC |
| 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仮想通貨 |
| 発行可能上限額 | 約 2,100 万 BTC |
| 一般的な性格 | 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仮想通貨 |
| 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 |
| 価値移転記録の信頼性確保の仕組み | Proof of work<br>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。 |

| | |
|---|---|
| 仮想通貨の名称 | イーサ（イーサリアム） |
| ティッカーコード | ETH |
| 仮想通貨の単位 | 0.00000001 ETH |
| 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 | 未確定 |
| 一般的な性格 | 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仮想通貨。<br>分散型アプリケーションが動作する実行環境の役割を果たす特徴を持つ。 |
| 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 |
| 価値移転記録の信頼性確保の仕組み | Proof of Stake<br>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、保有している基軸仮想通貨の量が多いほど採掘の成功確率が上昇するブロックの承認方式。 |
| 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。 |

| | |
|---|---|
| 仮想通貨の名称 | イーサ（イーサリアムクラシック） |
| ティッカーコード | ETC |
| 仮想通貨の単位 | 0.00000001 ETC |
| 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 | 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 | 未確定 |
| 一般的な性格 | 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仮想通貨。<br>分散型アプリケーションが動作する実行環境の役割を果たす特徴を持つ。 |
| 保有・移転記録の秘匿性 | 秘密鍵と公開鍵を用いた暗号化技術により、利用者本人が発信した移転データと特定し、記帳する。 |
| 価値移転記録の信頼性確保の仕組み | Proof of work<br>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。 |

| | |
|---|---|
| 仮想通貨の名称 | ライトコイン |
| ティッカーコード | LTC |
| 仮想通貨の単位 | 0.00000001 LTC |
| 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仮想通貨 |
| 発行可能上限額 | 8,400 万 LTC |
| 一般的な性格 | 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仮想通貨 |
| 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 |
| 価値移転記録の信頼性確保の仕組み | Proof of work<br>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 90 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。 |

| | |
|---|---|
| 仮想通貨の名称 | ビットコインキャッシュ |
| ティッカーコード | BCH |
| 仮想通貨の単位 | 0.00000001 BCH |
| 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仮想通貨 |
| 発行可能上限額 | 2,100 万 BCH |
| 一般的な性格 | 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仮想通貨 |
| 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 |
| 価値移転記録の信頼性確保の仕組み | Proof of work<br>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。 |

| | |
|---|---|
| 仮想通貨の名称 | モナコイン |
| ティッカーコード | MONA |
| 仮想通貨の単位 | 0.00000001 MONA |
| 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 | 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・代償として発行される仮想通貨 |
| 発行可能上限額 | 10,512 万 MONA |
| 一般的な性格 | 日本および世界で有名なアスキーアート「モナー」をモチーフにした日本初の暗号通貨になり、非中央集権によるクライアントプログラムによって維持される完全分散型決済システムを基盤とした暗号通貨。 |
| 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 |
| 価値移転記録の信頼性確保の仕組み | Proof of work<br>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。 |

| | |
|---|---|
| 仮想通貨の名称 | リスク |
| ティッカーコード | LSK |
| 仮想通貨の単位 | 0.00000001 LSK |
| 発行者 | Lisk Foundation |
| 発行主体概要 | Lisk のソースコードの開発とメンテナンスを行っている |
| 発行方法 | プログラムによる自動発行 |
| 発行可能上限額 | 無制限 |
| 一般的な性格 | 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仮想通貨 |
| 保有・移転記録の秘匿性 | 公開鍵暗号における公開鍵のハッシュを使って残高を記録 |
| 価値移転記録の信頼性確保の仕組み | Delegated Proof of Stake<br>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、投票により委任された承認者が取引履歴を管理し、ブロックを承認する仕組み。 |
| 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）および当該ネットワークの暗号通貨を多量に保有する人に傾斜的に付与された投票権を使用して選出された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。 |

| | |
|---|---|
| 仮想通貨の名称 | リップル（XRP） |
| ティッカーコード | XRP |
| 仮想通貨の単位 | 0.000001 XRP |
| 発行者 | Ripple Labs Inc. |
| 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 |
| 一般的な性格 | リップル（XRP）は金融機関の送金において法定通貨間のブリッジ通貨としてオンデマンドの流動性を提供する役割を有している。これによって金融機関は従来よりも格段に流動性コストを下げつつも送金先のリーチをグローバルに広げることができる。また、XRP は Ripple Consensus Ledger 上での取引における取引料としての性格も有している。ネットワークへの攻撃が起こった時には手数料が自動的に釣り上げられるため、攻撃が未然に防げる仕組みとなっている。XRP は 3〜5 秒ごとにファイナリティをもって決済を行うことができ、1 秒につき 1000 の取引を決済できるスケーラビリティを有する構造となっている。 |
| 保有・移転記録の秘匿性 | 取引は ED25519 and 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。さらに、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 1000 の取引まで対応できるスケーラビリティを有する。 |
| 価値移転認証の仕組み | 独自のコンセンサスアルゴリズムに基づく。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。 |
| 価値移転ネットワークの信頼性に関する説明 | 健全なネットワークを保全する動機を有する認証済法人バリデーターによって取引が承認される仕組みを有している。またネットワークの攻撃に対して自動的に取引手数料が釣り上がる仕組みを有しており、攻撃を未然に防ぐことができる。 |
| 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。その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。 |

| | |
|---|---|
| 仮想通貨の名称 | ベーシックアテンショントークン |
| ティッカーコード | BAT |
| 仮想通貨の単位 | 0.00000001 BAT |
| 発行者 | Brave Software, Inc. |
| 発行主体概要 | ベーシックアテンショントークンを利用したウェブブラウザ Brave を運営、開発している。 |
| 発行方法 | 初期発行のみ |
| 発行可能上限額 | 15 億 BAT |
| 一般的な性格 | 2017 年に ICO で初めて発行された。ベーシックアテンショントークンは分散型広告システムで利用されるトークンであり、それによって従来のシステムの仲介者を排除してユーザーの利便性を高めることができる。 |
| 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 |
| 価値移転記録の信頼性確保の仕組み | Ethereum ブロックチェーン上のスマートコントラクトとして実行され、コントラクトの実行結果がブロックチェーンに記録される。 |
| 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。 |

| | |
|---|---|
| 仮想通貨の名称 | ステラルーメン |
| ティッカーコード | XLM |
| 仮想通貨の単位 | 0.0000001XLM |
| 発行者 | ステラ開発財団 |
| 発行主体概要 | ステラ開発財団 |
| 発行方法 | ICO、プログラムによる自動発行、プロジェクトへのエアドロップ |
| 発行可能上限額 | 500 億 XLM |
| 一般的な性格 | 一般人、中小企業、中小金融機関の間で直接的に資金を移動可能なプラットフォームを利用するための仮想通貨。 |
| 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 |
| 価値移転記録の信頼性確保の仕組み | Stellar Consensus Protocol |
| 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。 |
| 価値移転ネットワークの信頼性に関する説明 | バリデーター（検証者）が取引についての投票を行い、合意が得られた取引については承認を行う事により信頼性を確保する |
| 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。 |

| | |
|---|---|
| 仮想通貨の名称 | ネム |
| ティッカーコード | XEM |
| 仮想通貨の単位 | 0.000001 XEM |
| 発行者 | なし |
| 発行主体概要 | なし |
| 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 | 8,999,999,999 XEM |
| 一般的な性格 | 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 |
| 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 |
| 価値移転記録の信頼性確保の仕組み | Proof of Importance<br>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、保有している基軸暗号資産の量および取引量に応じて採掘の成功確率が上昇するブロックの承認方式。 |
| 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 Eigentrust ++ によるノードの過去動作を監視した評価軸とノードの計算作業量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 | ネットワーク内における参加ノード間でトランザクションが共有・検証され、不正なトランザクションは除外され、また不正なトランザクションを送信するノードの評価を下げることで、ネットワーク内の健全性と信用を保つことを基礎としている。 |