取扱暗号資産概要説明書

		ビットコイン
概要説明書更新年月日		2024年4月24日
基礎情報	日本語の名称	ビットコイン
	現地語の名称	Bitcoin
	呼称（日本語の名称と同じ場合は一表記）	ー
	ティッカーコード（シンボル）	BTC、XBT
	発行開始（年、月、日）	2009年1月3日
	時価総額（ドル基準、例：＄1.000.000）	$1,314,171,072,095
	時価総額（円基準、例：￥100.000.000）	¥203,565,099,067,516
	主な利用目的	送金、決済、投資
	利用制限の有無	なし
	海外流通の有無	あり
	国内流通の有無	あり
	店舗等の利用制限の有無	なし
	利用制限を行う者の属性	ー
	利用制限の内容	ー
	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
	法的性格（資金決済法第2条第5項第１号、第２号の別　例：第1号）	第1号
	2号の場合：相互に交換可能な1号暗号資産の名称	–
	発行暗号資産に対する資産（支払準備資産）の有無および名称	なし
	発行者に対する保有者の支払請求権（買取請求権）	–
	支払請求（買取請求）による受渡資産	–
	発行者が保有者に付与するその他の権利	–
	発行者に対して保有者が負う義務	–
	価値の決定	保有者間の自由売買による
	交換（売買）の制限	–
	価値移転、保有情報を記録する電子情報処理組織の形態	パブリック型ブロックチェーン
	保有・移転記録台帳の公開、非公開の別	公開
	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、シュノア署名等による暗号化処理を施しデータを記録
	利用者の真正性の確認	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 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
	誕生時に技術的なベースとなったコインの有無とその名称（アルトコインのみ）	–
取引単位・交換制限	取引単位の呼称	1 BTC = 1,000 m BTC　　m：ミリ 1 m BTC=1,000 μ BTC　　μ：ミクロン 1 μ BTC=1 bits　　bits：ビッツ 1 bits=100 satoshi
	保有・移転記録の最低単位	1 satoshi (= 0.00000001 BTC)
	交換可能な通貨又は暗号資産	全て可
	交換制限	–
	制限内容	–

	交換市場の有無	あり
連動する資産の有無等	価値が連動する資産等の有無	なし
	価値連動する資産等の名称	－
	価値連動する資産等の内容	－
	価値連動する資産との交換の可否	－
	価値連動する資産との交換比率	－
	価値連動する資産との交換条件	－
付加価値	その他の付加価値（サービス）の有無	なし
	付加価値（サービス）の内容	－
	過去3年間の付加価値（サービス）の提供状況	－
発行状況	発行者	－
	発行主体の名称	プログラムによる自動発行
	発行主体の所在地	－
	発行主体の属性等	－
	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
	発行暗号資産の信用力に関する説明	多数の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 ブロックチェーンによる保有・移転管理台帳による記録管理と重層化した暗号化技術による記録の保全能力 保有・移転管理台帳の公開 暗号化技術による保有者個人情報の秘匿性
	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
	発行可能数	20,999,999.9769 BTC
	発行可能数の変更可否	可
	変更方法	発行プログラムの変更
	変更の制約条件	分散型保有・移転管理台帳の記録者の95%以上の同意及び記録者によるプログラム修正の実施
	発行済み数量	19,689,431 BTC
	今後の発行予定または発行条件	・1ブロックを更新するごとに3.125 BTCを新規発行している ・210,000ブロックの更新を終えるごとに1ブロック更新による新規発行数が半減する仕組みとなっている ・2024年4月24日15:52時点でのブロック数:840,617個 （データ取得元）https://www.blockchain.com/explorer およそ10分に1ブロックを更新しており、日本時間2024年4月20日に半減期を迎え1ブロック更新当たり新規発行数が6.25BTCから3.125BTCとなっている。
	過去３年間の発行状況	保有・移転管理台帳の管理者に対し、以下の数量を発行 2019年1月1日～2019年12月31日　677,888 BTC 2020年1月1日～2020年12月31日　453,631 BTC 2021年1月1日～2021年12月31日　329,325 BTC 2022年1月1日～2022年12月31日　332,000 BTC 2023年1月1日～2023年12月31日　336,875 BTC （データ取得元）https://www.blockchain.com/explorer/charts/total-bitcoins
	過去３年間の発行理由	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
	過去３年間の償却状況	－
	過去３年間の償却理由	－
	発行者の行う発行業務に対する監査の有無	なし
	監査を実施する者の氏名又は名称	－
	直近時点で行われた監査年月日	－
	直近時点における監査結果	－
価値移転記録台帳に係る技術	ブロックチェーン技術の利用の有無	あり
	ブロックチェーンの形式	パブリック型
	ブロックチェーン技術を利用しない場合には、その名称	－
	利用するブロックチェーン技術以外の技術の内容	－
	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
	価値記録公開/非公開の別	公開

	保有者個人データの秘匿性の有無	あり
	秘匿化の方法	公開鍵と秘密鍵による暗号化
	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。
価値移転の記録者	記録者の数	不定だが主なPoolとそのシェアに関しては以下を参照 https://www.blockchain.com/charts/pools
	記録者の分布状況	2024年4月現在のHashrate上位3カ国は、米国約35%、カザフスタン約18%、ロシア約11% https://worldpopulationreview.com/country-rankings/bitcoin-mining-by-country
	記録者の主な属性	誰でも自由に記録者になることができる
	記録の修正方法	記録者が合意し、各記録者が保管する台帳の修正を自ら行う
	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。
	価値移転の管理状況に対する監査の有無	なし
	監査を実施する者の氏名又は名称	–
	直近時点で行われた監査年月日	–
	その監査結果	–
	（統括者に関する情報）	
	記録者の統括者の有無	なし
	統括者の名称	–
	統括者の所在地	–
	統括者の属性	–
	統括者の概要	–
暗号資産に内在するリスク	価値移転ネットワークの脆弱性に関する特記事項	多数の記録者が結託し、あるいは既存の記録者が有する処理能力合計よりも強力な能力を用いることによって、記録台帳を改竄することができる脆弱性があり、51%攻撃とも呼ばれる
	保有情報暗号化技術の脆弱性に関する特記事項	–
	発行者の破たんによる価値喪失の可能性に関する特記事項	BTC価格の下落（対法定通貨）等に起因したマイナー撤退により、ハッシュパワーが低下し、セキュリティ低下を招く可能性がある
	価値移転記録者の破たんによる価値喪失の可能性に関する特記事項	–
	移転の記録が遅延する可能性に関する特記事項	マイニングに参加するマイナーが少ないもしくは全くいなくなった場合、移転の記録が遅延もしくは進行しない恐れがある
	プログラムの不具合によるリスク等 に関する特記事項	現時点ではプログラムが適正に機能し、所有データの改竄、同一のBitcoinの異なる者との取引、複数の所有者が同一のBitcoin を同時に保有する状況などの不適切な状態に陥ることを排除しているが、未検出のプログラムの脆弱性やプログラム更新などにより新たに生じた脆弱性を利用し、データが改竄され、価値移転の記録が異常な状態に陥る可能性がある。
	過去に発生したプログラムの不具合の発生状況に関する特記事項	2018年9月に無限増殖バグ等が発見され、Bitcoinが無限に発行できる危険性があったが、既に解消されている https://coinpost.jp/?p=47597
	非互換性のアップデート(ハードフォーク）の状況	Bitcoinのハードフォークは以下の通り 2017年8月1日 ビットコインキャッシュ（BCH） 2017年10月24日　ビットコインゴールド（BTG） 2017年11月24日　ビットコインダイヤモンド（BCD） 2017年12月12日　スーパービットコイン（SBTC） 2017年12月18日　ライトニングビットコイン（LBTC） 2017年12月27日　ビットコインゴッド（GOD） （取得元）https://coinpedia.cc/bitcoin-hard-fork
	今後の非互換性アップデート予定	–
	正常な稼働に影響を与えたサイバー攻撃の履歴	–
流通状況	価格データの出所	出所：CoinMarketCap URL：https://coinmarketcap.com/ja/currencies/bitcoin/
	1取引単位当たり計算単価（ドル基準、例：＄1.000.000）	$66,745
	1取引単位当たり計算単価（円基準、例：￥100.000.000）	¥10,338,801
	ドル/円計算レート（基準日付）	1ドル/154.9円
	四半期取引数量（現物、単位は百万円）	3,699,745 百万円

		イーサリアム
概要説明書更新年月日		2024年4月24日
基礎情報	日本語の名称	イーサリアム
	現地語の名称	Ethereum
	呼称（日本語の名称と同じ場合は一表記）	–
	ティッカーコード（シンボル）	ETH
	発行開始（年、月、日）	2015年7月30日
	時価総額（ドル基準、例：＄1.000.000）	$388,598,157,440
	時価総額（円基準、例：￥100.000.000）	¥60,193,854,587,456
	主な利用目的	送金、決済、スマートコントラクト
	利用制限の有無	なし
	海外流通の有無	あり
	国内流通の有無	あり
	店舗等の利用制限の有無	なし
	利用制限を行う者の属性	ー
	利用制限の内容	ー
	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 ・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
	法的性格（資金決済法第2条第5項第１号、第２号の別　例：第1号）	第1号
	2号の場合：相互に交換可能な1号暗号資産の名称	–
	発行暗号資産に対する資産（支払準備資産）の有無および名称	なし
	発行者に対する保有者の支払請求権（買取請求権）	ー
	支払請求（買取請求）による受渡資産	–
	発行者が保有者に付与するその他の権利	ー
	発行者に対して保有者が負う義務	ー
	価値の決定	保有者間の自由売買による
	交換（売買）の制限	ー
	価値移転、保有情報を記録する電子情報処理組織の形態	パブリック型ブロックチェーン
	保有・移転記録台帳の公開、非公開の別	公開
	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
	利用者の真正性の確認	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 Stake 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が多いほどブロック生成（承認）の成功確率が上昇する承認方式。
	誕生時に技術的なベースとなったコインの有無とその名称（アルトコインのみ）	ー
取引単位・交換制限	取引単位の呼称	finney=0.001ETH szabo=0.000001ETH wei=0.000000000000000001ETH
	保有・移転記録の最低単位	1wei (=0.000000000000000001 ETH)
	交換可能な通貨又は暗号資産	全て可
	交換制限	ー
	制限内容	–

	交換市場の有無	あり
連動する資産の有無等	価値が連動する資産等の有無	なし
	価値連動する資産等の名称	–
	価値連動する資産等の内容	–
	価値連動する資産との交換の可否	–
	価値連動する資産との交換比率	–
	価値連動する資産との交換条件	–
付加価値	その他の付加価値（サービス）の有無	あり
	付加価値（サービス）の内容	Ethereumネットワーク上でのスマートコントラクトの記録と実行
	過去3年間の付加価値（サービス）の提供状況	安定してサービスが続いている
発行状況	発行者	あり
	発行主体の名称	Ethereum Foundation
	発行主体の所在地	スイス連邦ツーク州
	発行主体の属性等	次世代の分散型アプリケーションの開発
	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
	発行暗号資産の信用力に関する説明	多数の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。 ブロックチェーンによる保有・移転管理台帳による記録管理と重層化した暗号化技術による記録の保全能力 保有・移転管理台帳の公開 暗号化技術による保有者個人情報の秘匿性
	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
	発行可能数	未定
	発行可能数の変更可否	不可
	変更方法	–
	変更の制約条件	–
	発行済み数量	122,047,160 ETH
	今後の発行予定または発行条件	PoSによるステーキング報酬として、およそ年率0.5%程度のインフレ率で発行される
	過去３年間の発行状況	・約15秒に一回のマイニング報酬としてETHが支払われる ・2015年7月の稼働時は5ETHであったが、2017年10月のハードフォークで3ETHに減少し、2019年1月のハードフォークで2ETHへと減少した ・2024年4月24日時点では発行済量が122,047,160となる。
	過去３年間の発行理由	・約15秒に一回のマイニング報酬としてETHが支払われる ・2015年7月の稼働時は5ETHであったが、2017年10月のハードフォークで3ETHに減少し、2019年1月のハードフォークで2ETHへと減少した ・2024年4月24日時点では発行済量が122,047,160となる。
	過去３年間の償却状況	–
	過去３年間の償却理由	–
	発行者の行う発行業務に対する監査の有無	なし
	監査を実施する者の氏名又は名称	–
	直近時点で行われた監査年月日	–
	直近時点における監査結果	–
価値移転記録台帳に係る技術	ブロックチェーン技術の利用の有無	あり
	ブロックチェーンの形式	パブリック型
	ブロックチェーン技術を利用しない場合には、その名称	–
	利用するブロックチェーン技術以外の技術の内容	–
	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。
	価値記録公開/非公開の別	公開

	保有者個人データの秘匿性の有無	あり
	秘匿化の方法	公開鍵と秘密鍵による暗号化
	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。
価値移転の記録者	記録者の数	6,575 (2024年4月24日時点のノード数) https://etherscan.io/nodetracker
	記録者の分布状況	米国、韓国、ドイツ、英国など
	記録者の主な属性	不特定。 記録者は最低32ETHの保有が必要となる。
	記録の修正方法	記録者が合意し、各記録者が保管する台帳の修正を自ら行う。
	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。
	価値移転の管理状況に対する監査の有無	なし
	監査を実施する者の氏名又は名称	-
	直近時点で行われた監査年月日	-
	その監査結果	-
	（統括者に関する情報）	
	記録者の統括者の有無	なし
	統括者の名称	-
	統括者の所在地	-
	統括者の属性	-
	統括者の概要	-
暗号資産に内在するリスク	価値移転ネットワークの脆弱性に関する特記事項	多数の記録者が結託し、あるいは既存の記録者が有する処理能力合計よりも強力な能力を用いることによって、記録台帳を改竄すること発行プログラムを改変することができる。
	保有情報暗号化技術の脆弱性に関する特記事項	第三者に秘密鍵を知られた場合には、利用者になりすまして送付指示を行うことができる。
	発行者の破たんによる価値喪失の可能性に関する特記事項	ー
	価値移転記録者の破たんによる価値喪失の可能性に関する特記事項	-
	移転の記録が遅延する可能性に関する特記事項	処理可能なトランザクションを上回る量の取引がブロックチェーン上で発生した場合に遅延する可能性がある。
	プログラムの不具合によるリスク等 に関する特記事項	ブロックチェーン上にデプロイされたコントラクトコードに脆弱性があった場合に不正に資産が盗み取られるリスクがある。
	過去に発生したプログラムの不具合の発生状況に関する特記事項	Ethereum上のアプリケーション「The DAO」のプログラム（スマートコントラクト）のバグ（脆弱性）を攻撃されて、集まったファンド資金３分の１以上を盗み取られた事例がある。
	非互換性のアップデート(ハードフォーク）の状況	2016年7月 The DAOへの攻撃によって盗まれたDAOを取り戻すEthereum Classicハードフォーク（注1） 2017年7月に発生した盗難案件をきっかけに、2018年1月に再び分裂しEthereum Zeroが誕生 2022年9月一部のETHマイニング団体がEthereum Proof of Workモデルをサポートし続けるため、再び分裂しEthereum PoWが誕生予定
	今後の非互換性アップデート予定	ー
	正常な稼働に影響を与えたサイバー攻撃の履歴	-
流通状況	価格データの出所	出所：Etherscan URL：https://etherscan.io/stat/supply
	１取引単位当たり計算単価（ドル基準、例：＄1.000.000）	$3,184
	１取引単位当たり計算単価（円基準、例：￥100.000.000）	¥493,202
	ドル/円計算レート（基準日付）	1ドル/154.9円
	四半期取引数量（現物、単位は百万円）	654,431 百万円