

【発行状況】	発行可能数の変更可否	可	不可
	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	18,528,231 BTC	113,160,000 ETH
	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6.25BTC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。 ・2020年10月28日18:00時点でのブロック数=654,536個 (データ取得元) https://btc.com/ およそ10分に1ブロックを更新しており、日本時間2020年5月12日に半減期を迎え1ブロック更新当たり新規発行数が12.5BTCから6.25BTCとなっている。	・現行は平均13.3秒につき1ブロックを生成、1ブロックあたりの報酬2ETH+トランザクション手数料 ・Ethereum 2.0に移行完了後は、PoWによるマイニングは廃止(ただし、並行して新旧2つのチェーンが当面稼働の予定) ・代わって、PoSによるステーキング報酬へと移行し、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	保有・移転管理台帳の管理者に対し、以下の数量を発行 2017年1月1日～2017年12月31日 694,625 BTC 2018年1月1日～2018年12月31日 676,250 BTC 2019年1月1日～2019年12月31日 677,513 BTC (データ取得元) https://www.blockchain.com/ja/charts/total-bitcoins?timespan=all	・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 ・2020年1月時点では発行済量が105,867,881あり、2020年10月26日時点では113,160,038へ増えた
	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	2014年7月～8月 クラウドセールによる発行 2015年7月30日以降 プログラムによる自動発行
	過去3年間の償却状況	なし	なし
	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	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	あり
	ブロックチェーンの形式	パブリック型	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。	・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	公開
	保有者個人データの秘匿性の有無	あり	あり
	秘匿化の方法	公開鍵と秘密鍵による暗号化	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。	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	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		主に中国	不特定
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	不特定、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。	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	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	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。	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	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。	なし
	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。	—
【暗号資産に内在するリスク】	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。	ブロックチェーン上にデPLOY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	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	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。

スク	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	2016年7月 The DAO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)
	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/coins/	出所: Cryptocurrency Market Capitalizations URL: https://coinmarketcap.com/currencies/ethereum/
	1取引単位当たり計算単価 (ドル基準、例: \$ 1,000,000)	\$13,735.02	\$409.24
	1取引単位当たり計算単価 (円基準、例: ¥100,000,000)	¥1,428,442.08	¥42,917
	ドル/円計算レート	1ドル/約104円 (2020年10月28日基準)	1ドル/約105円 (2020年1月17日基準)
備考	—	注1 旧来のイーサリアムをハードフォークすることにより、2016年6月の自律分散型投資ファンド「The DAO」への攻撃によって盗難されたDAOを救出した。このHFを支持しなかったマイナーによって存続することとなった旧仕様のイーサリアムはEthereum Classicに改称され、HF側がイーサリアムの名称を引き継いだ。スマートコントラクトの実行プラットフォームとして開発された現在のETCの性格を引き継いでいる。	