

取扱暗号資産の概要説明書

概要書更新年月日		2021年10月27日
【基礎情報】	日本語の名称	ビットコインキャッシュ
	現地語の名称	Bitcoin Cash
	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)	BCH、BCC
	発行開始(年、月、日)	2017年8月1日
	時価総額(ドル基準、例: \$ 1,000,000)	\$11,557,532
	時価総額(円基準、例: ¥ 100,000,000)	¥1,318,179,444
	主な利用目的	送金、決済、投資
	利用制限の有無	—
	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	—
	利用制限を行う者の属性	—
	利用制限の内容	—
	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	—
	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 work コンセンサス・アルゴリズム(分散台帳内の二重取引を排除するための合意形成方式)の一つであり、そのときのナンスのターゲット以下のブロックハッシュであるブロックを各自のノードが任意に取り込み、最も計算量の多いチェーンを正当と見なす。	
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)	BTC	
【取引単位・交換制限】	取引単位の呼称	1 BCH= 1,000m BCH m: ミリ 1 m BCH=1,000 μ BCH μ: ミクロン 1 μ BCH=1bits bits: ビッツ 1 bits=100satoshi
	保有・移転記録の最低単位	1 satoshi (= 0.00000001 BCH)
	交換可能な通貨又は暗号資産	全て可
	交換制限	—
	制限内容	—
【連動する資産の有無等】	交換市場の有無	あり
	価値が連動する資産等の有無	—
	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	—
【付加価値】	価値連動する資産との交換条件	—
	その他の付加価値(サービス)の有無	—
	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	最も計算量の多いチェーンを正当とみなす作業証明により信用を担保している分散型の価値保有・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
	発行方法	—
	発行可能数	20,999,999.9769 BCH
	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	18,883,156BCH
	今後の発行予定または発行条件	—
	過去3年間の発行状況	—
	過去3年間の発行理由	—
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	—	
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	トランザクションの形式と多重支払いをしていないかのチェック、ブロックの形式と最も大きな作業証明(Proof of Work)を持つチェーンを確認している。後続のブロックが連なるに従って、チェーンが覆る確率が低くなっていき覆るのが難しくなる仕組みである。
	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	不定のため直近24時間・48時間・4日に機能した記録者数として以下を参照 https://bch.btc.com/stats/pool?pool_mode=year
	記録者の分布状況	主に中国
	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	作業証明(Proof of Work)が最も多いチェーンが正しいという合意によって信用が維持されている
	価値移転の管理状況に対する監査の有無	—
	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	—
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、記録台帳の改竄およびブロックチェーンデータの改変が可能になる
	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	—
	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	ブロック生成が遅れることによって記録遅延が生じる。 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 Cashの異なる者との取引、複数の所有者が同一のBitcoin Cash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。
	プログラムの不具合によるリスク等に関する特記事項	2019年5月15日ハードフォーク後バグ発生 https://cc.minkabu.jp/news/2557
	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11月16日 ABC系とSV系の分裂 2020年11月15日 ABC系とBitcoin Cash Node(BCHN)の分裂
	非互換性のアップデート(ハードフォーク)の状況	—
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/
	1取引単位当たり計算単価(ドル基準、例: \$ 1,000,000)	\$611.00
	1取引単位当たり計算単価(円基準、例: ¥ 100,000,000)	¥69,770
	ドル/円計算レート 2021年10月27日基準	1ドル/約114円
	四半期取引数量(協会加盟会員合計、現物、単位は百万円)	248,282(4-6月期)
備考	2017年8月Bitcoinのハードフォークにより組成された暗号資産。	