取扱暗号資産の概要説明書

		ビットコイン	イーサリアム	ビットコインキャッシュ	XRP
概要書更新年月日		2020年3月30日	2020年3月30日	2020年10月26日	2020年11月4日
【基礎情報】	日本語の名称	ビットコイン	イーサリアム	ビットコインキャッシュ	エックスアールピー（リップル）
	現地語の名称	Bitcoin	Ethereum	Bitcoin Cash	XRP（Ripple）
	呼称（日本語の名称と同じ場合は－表記）	－	－	－	－
	ティッカーコード（シンボル）	BTC、XBT	ETH	BCH、BCC	XRP
	発行開始（年、月、日）	2009年1月3日	2015年7月30日	2017年8月1日	2012年9月（Ripple Consensus Ledgerの開始日）
	時価総額（ドル基準、例：＄1.000.000）	$254,485,541,126	$46,309,598,400	$4,379,000,000	$10,518,586,978
	時価総額（円基準、例：￥100.000.000）	¥26,466,496,277,104	¥4,856,487,584,208	¥459,300,000,000	¥1,101,084,875,752
	主な利用目的	送金、決済、投資	送金、決済、スマートコントラクト	送金、決済、投資	送付（送金）、決済、投資
	利用制限の有無	－	なし	－	－
	海外流通の有無	あり	あり	あり	あり
	国内流通の有無	あり	あり	あり	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	－	なし	－	－
	利用制限の内容	－	なし	－	－

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。	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。	・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。 ・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1,500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。
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	第1号	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）	－	なし	－	－
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	－	なし	－	－
発行者に対して保有者が負う義務	－	なし	－	－
価値の決定	保有者間の自由売買による	保有者間の自由売買による	保有者間の自由売買による	保有者間の自由売買による
交換（売買）の制限	－	なし	－	－
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	パブリック型ブロックチェーン	パブリック型ブロックチェーン	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	公開	公開	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	公開鍵暗号の暗号化処理を施しデータを記録	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	・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
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	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。	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	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	現状はBitcoinと同様のPoW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PoS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。	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。	・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（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
	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）	－	なし	BTC	－
【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	finned=0.001ETH szabo=0.000001ETH wei=0.000000000000000001ETH	1 BCH= 1,000m BCH m：ミリ 1 m BCH=1,000μ BCH μ：ミクロン 1 μ BCH=1bits bits：ビッツ 1 bits=100satoshi	1 XRP = 1,000,000 drop
	保有・移転記録の最低単位	1 satoshi（＝0.00000001 BTC）	1wei（=0.000000000000000001 ETH）	1 satoshi （＝0.00000001 BCH）	1 drop （＝0.000001 XRP）
	交換可能な通貨又は暗号資産	全て可	全て可	全て可	全て可
	交換制限	－	なし	－	－
	制限内容	－	－	－	－
	交換市場の有無	あり	あり	あり	あり
【連動	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	－	－	－	－

する資産の	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	－	金融機関の国際送金において流動性確保するためのブリッジ通貨として使われる。Ripple Labs Inc.とR3 LLCが共同で行い、12の金融機関が参加した実証試験ではXRPを使用することで送金コストが60%低減できることが実証された。
	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	－	・上記の通り、2016年に金融機関による実証試験が行われた ・マネーグラム社がXRPを利用し米国とメキシコ間でODLを利用した国際送金を初めて行っている ・FlashFXはフィリピンへの支払いで正式にODLを導入した（AUD/PHP）
【発行状況】	発行者	－	あり	－	あり
	発行主体の名称	プログラムによる自動発行	Ethereum Foundation	プログラムによる自動発行	Ripple Labs Inc.
	発行主体の所在地	－	スイス連邦ツーク州	－	San Francisco, California, U.S.
	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	－	ソフトウェア開発
	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	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	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	Ripple Labs Inc.（https://ripple.com/）

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	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	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	XRPはオープンなネットワーク上で固有のコンセンサスアルゴリズムによって取引が承認され、暗号化技術による堅牢なセキュリティ構造を有する。取引が承認されるためには80%以上の認証済み法人バリデータが合意をする必要があり、承認された取引はグローバルに共有されたパブリックな台帳に記録され、改ざん不可能となる。 XRPは国際送金の法人向けユースケースをサポートする機能を有したデジタルアセットであり、銀行によって直接保管され使用される実証試験が行われた唯一の独立型暗号資産である。 XRPはネットワーク開始以降2900万回台帳が更新されており、2016年には一度もダウンタイムは発生しておらず、強固なネットワークにより支えられている。
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	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	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	2012年のネットワーク発足時に全て発行済み
発行可能数	20,999,999.9769 BTC	未定	20,999,999.9769 BCH	100,000,000,000 XRP
発行可能数の変更可否	可	不可	可	不可（全量発行済みのため追加発行無し）

変更方法	発行プログラムの変更	−	発行プログラムの変更	Ripple Consensus LedgerのP2Pサーバ向けソフトウェアであるrippledのプログラム変更（現時点では発行するプログラム自体が存在しないので、新規に作成する必要がある）
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	−	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	・80％以上のバリデータが合意しなければならない ・合意後に、プログラムの修正を実施する必要がある
発行済み数量	18,528,231 BTC	113,160,000 ETH	18,274,075 BCH	100,000,000,000 XRP
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/	・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	−	・2012年に全て発行されており、今後の発行予定は無い ・発行済のXRPの約62%（2017年9月時点）をRipple Labs Inc.が保有し、市場に分配している。約37%はすでに市場に流通している

	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 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	－	－（2012年に全て発行済）
	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	－	2018年5月28日の99,992,075,649から2020年11月4日までに1,216,776が消滅され、99,990,858,873となった。
	過去３年間の償却理由	－	－	－	ネットワークを攻撃者から守るためのメカニズムとして手数料を課し、その手数料分のXRPを消滅させセール
	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	－	－	－	－
【特徴】	ブロックチェーン技術の利用の有無	あり	あり	あり	あり

【価値移転記録台帳に係る技術】

ブロックチェーンの形式	パブリック型	パブリック型	パブリック型	パブリック型台帳（「ブロック」の代わりにその時点での全ての情報を含む「台帳」（スナップショット）が公開される）
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。	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すのが難しくなる仕組みである。	・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
価値記録公開/非公開の別	公開	公開	公開	公開
保有者個人データの秘匿性の有無	あり	あり	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	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。	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。	・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によって取引が承認される仕組みを有している ・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

【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	79団体 https://investoon.com/mining_pools/eth	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	89のバリデータ（検証者）ノード（2020年11月時点） 注：他のパブリックブロックチェーンにも言えるように、ノードは情報の共有を拒否することも可能であるため、上記の数字はRipple Labs Inc.が把握している部分の数字のみを示している
	記録者の分布状況	主に中国	不特定	主に中国	世界中に分散
	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。	誰でも自由に記録者になることができる	誰でも自由に記録者になることができるが、信頼されているバリデータの投票だけが投票プロセスにおいて考慮される
	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。	記録者が合意し、各記録者が保管する台帳の修正を自ら行う	・取引が一旦記録されると、取引は変更することができない ・承認された送金はキャンセールすることができないので、その送金を無効とするためには反対の取引を別途行う必要がある

	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	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。	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	・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（検証者）になっている。 ・そのうち、トップのバリデータ運用のパフォーマンスを示した複数のバリデータのみが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。
	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	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。	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	・信頼するバリデータ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。
	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。	－	・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。 ・Ripple Consensus Ledgerは「Multisign」という機能を有しており、取引を承認する際に複数の秘密鍵を使用することによって、１つの秘密鍵が盗まれても損失を被らないような堅牢なセキュリティ構造を提供している。

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	−	ブロック生成が遅れることによって記録遅延が生じる。	信頼されるバリデータの大多数のネットワーク接続が失われた場合、接続が復活するまで価値移転の記録が遅延する可能性がある。 また、信頼されるバリデータが互換性のないソフトウェアのバージョンを使用した場合、大多数のバリデータが互換性のあるソフトウェアに移行するまで、または、非互換のソフトウェアを使うバリデータを投票プロセスから除外するという設定をするまでは価値移転の記録が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	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。	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。	・どのようなソフトウェアにも言えることだが、ソフトウェアの不具合が問題を引き起こす可能性は否定できないが、Ripple Labs Inc.では新しいバージョンがアップデートされる前に入念なQAを行っており不具合の可能性を最小化している。 ・Ripple Consensus Ledgerはこれまで2,900万回、一度もフォークなどの大きな問題は経験することなく台帳を更新している。

	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。	2019年5月15日ハードフォーク後バグ発生 https://cc.minkabu.jp/news/2557	－
	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）	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	－
	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：CryptoCurrency Market Capitalizations URL:https://coinmarketcap.com/currencies/ethereum/	出所：CoinMarketCap URL： https://coinmarketcap.com/coins/	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）	$13,735.02	$409.24	$235.92	$0.23
	1取引単位当たり計算単価（円基準、例：￥100.000.000）	¥1,428,442.08	42,917.00	¥24,744	¥24.57
	ドル/円計算レート	1ドル/約104円（2020年10月28日基準）	104.87円/ドル	1ドル/約104円	1ドル/約105円
	四半期取引数量（協会加盟会員合計、現物、単位は百万円）	1,869,929	50,398 百万円	28,775 (2020/4~6)	143,784
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Ether 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。	－

取扱暗号資産の概要説明書

		ライトコイン	オントロジー	クアンタム	ダイ
概要書更新年月日		2020年10月31日	2021年7月5日	2021年9月8日	2023年1月27日
【基礎情報】	日本語の名称	ライトコイン	オントロジー	クアンタム	ダイ
	現地語の名称	Litecoin	Ontology	Qtum	Dai
	呼称（日本語の名称と同じ場合は－表記）	－	－	－	－
	ティッカーコード（シンボル）	LTC	ONT	QTUM	DAI
	発行開始（年、月、日）	2011年10月	2018年6月30日	2017年9月13日	2019年11月18日
	時価総額（ドル基準、例：＄1.000.000）	$3,656,741,432	$620,145,350	$1,143,834,153	$5,145,378,434.55
	時価総額（円基準、例：￥100.000.000）	¥383,069,262,192	¥68,215,988,500	¥126,029,362,719	¥668,358,931,755
	主な利用目的	送金、決済、投資	送金、決済、投資	送金、決済、投資	送金、決済
	利用制限の有無	－	－	なし	なし
	海外流通の有無	あり	あり	あり	あり
	国内流通の有無	あり	なし	なし	あり
	店舗等の利用制限の有無	－	－	なし	なし
	利用制限を行う者の属性	－	－	なし	－
	利用制限の内容	－	－	なし	－

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	分散型のアイデンティティおよびデータ管理に特化した高性能パブリックブロックチェーンプロジェクトで、ONTは同ブロックチェーン上のガバナンストークンである	Bitcoinで用いられている安全性の高い残高確認方式を採用しつつ、Ethereumと互換性のあるスマートコントラクトを実装できるため、BitcoinとEthereumの長所を掛け合わせた暗号資産と言われる。 またProof of Stake Version 3の採用により、ブロック生成者選出の公平性を保ちつつ、BitcoinやEthereumのPoWを用いたシステムよりも少ない消費電力でトランザクション処理が可能。	Ethereumのブロックチェーン上で発行されたトークン
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	第1号	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	なし	なし
発行者に対する保有者の支払請求権（買取請求権）	－	なし	なし	なし
支払請求（買取請求）による受渡資産	－	なし	－	なし

発行者が保有者に付与するその他の権利	－	なし	なし	なし
発行者に対して保有者が負う義務	－	なし	なし	なし
価値の決定	保有者間の自由売買による	保有者間の自由売買による	保有者間の自由売買による	スマートコントラクト等の仕組みにより擬似的におよそ1米ドルの価値を保つように制御されているが、市場における需要と供給によって決定する
交換（売買）の制限	－	なし	なし	なし
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	パブリック型ブロックチェーン	パブリック型ブロックチェーン	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	公開	公開	公開
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	なし	公開鍵暗号の暗号化処理を施しデータを記録	Ethereumに準じるため公開鍵暗号の暗号化処理を施しデータを記録する。
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	取引所を通じて取引される場合は取引所がKYCを行っている	ECDSA(secp256k1曲線)を用いて秘密鍵と公開鍵を発行し、利用者本人が発信した移転データと特定し、記帳する	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 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。	Ontologyで採用されているVBFTアルゴリズムは、Verifiable Random Function（VRF）によって導入されたランダム性により、代替提案ノード/検証ノード/確認ノードが異なる仕組みとなっており、どのノードが参加するか予測は困難である。このためコンセンサスアルゴリズムへの攻撃に対する耐性が大幅に向上する。	Proof Of Stake Versoin 3を元に独自に改良を加えた価値移転記録ロジックを使用しており、ステーキングの量に応じてブロック生成者を選出し分散台帳に書き込みを行う方法	ERC－20トークンであるため、Ethereumのブロックチェーンで使用されているPoS (Proof of Stake)の枠組みに則って記録が管理されている
	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	－	なし	ETH
【取引単位・交換制限】	取引単位の呼称	1 LTC = 1,000m LTC m：ミリ 1 m LTC = 1,000μ LTC μ：ミクロン 1 μ LTC = 1 bits bits：ビッツ 1 bits = 100 satoshi	1ONT	QTUM	DAI
	保有・移転記録の最低単位	1 satoshi （＝0.00000001 LTC）	1ONT	0.00000001 QTUM	小数点以下18桁（decimals－18）
	交換可能な通貨又は暗号資産	全て可	全て可	全て可	全て可
	交換制限	－	－	なし	なし
	制限内容	－	－	－	なし
	交換市場の有無	あり	あり	あり	あり
【連動	価値が連動する資産等の有無	－	－	なし	なし
	価値連動する資産等の名称	－	－	－	－

する資産の	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	あり	なし
	付加価値（サービス）の内容	－	ONTをステークすることでコンセンサスアルゴリズムへ参加し、報酬を得ることが可能である	Ethereumネットワーク上で動作しているスマートコントラクトと互換性のあるスマートコントラクトが動作可能	－
	過去3年間の付加価値（サービス）の提供状況	－	ステーキングサービスが提供されている	問題なく付加価値を提供している	－
【発行状況】	発行者	－	プログラムによる自動発行	あり	不特定多数の利用者が担保資産をもとに発行
	発行主体の名称	プログラムによる自動発行	Ontology Foundation	Qtum Chain Foundation Ltd.	－
	発行主体の所在地	－	2 VENTURE DRIVE #11－31 VISION EXCHANGE SINGAPORE 608526	シンガポール（SG 079027 Singapore Singapore 100 TRAS STREET #16－01 100 AM）	－
	発行主体の属性等	－	－	非営利団体	－
	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	Ontology FoundationはONT利用者及びエコシステムを拡大し、ネットワークの価値を高めることを目的とする団体である。	2016年に設立されたシンガポールに本社を置く非営利団体であり、元アリババのエンジニアだったPatrick Dai がCEOを務める	－

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	Ontologyのネットワークが正常に稼働していることやアプリケーションが構築されていることが信用力につながる。	ECDSA(secp256k1曲線)を用いた暗号化技術により秘匿性を保ちつつ、POSV3による合意形成で管理台帳への記録更新を行っている	DAIは、イーサリアムのプラットフォームを利用して作られたERC－20トークンであるため、技術的な安定性に問題はない。また、実際にも、プログラム通りに運営されており、記録者による記録が継続され、市場で取引されているという実績がある
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	全部で10億ONTがジェネシスブロック(1番最初のブロック)生成の時点で発行済み	2017年3月16日のICO時に全量である1億枚が既に発行されており、毎年1%ずつ上限が増えていく仕組みとなっている	Vaultと呼ばれるスマートコントラクトを通じて不特定多数の利用者が暗号資産を担保にDAIを発行
発行可能数	84,000,000 LTC	1,000,000,000 ONT	上限は107,822,406 QTUM 参照： https://coinmarketcap.com/currencies/qtum/	－
発行可能数の変更可否	可	可	可	－

変更方法	発行プログラムの変更	プロトコルの変更	発行プログラムの変更	−
変更の制約条件	−	保有者達にとって追加発行は既に保有している分の価値が薄まることを意味するため、保有者であり記録者であるプレーヤーを納得させる十分な理由が必要となる	プロポーザルの提出、プログラム修正、Adminらによるガバナンス投票の実施	−
発行済み数量	65,799,340 LTC	1,000,000,000	103,713,908 QTUM（2021/9/8時点） 参照： https://coinmarketcap.com/currencies/qtum/	5,145,378,434.55 DAI
今後の発行予定または発行条件	・採掘者は1ブロック発掘するごとに12.5 LTCが与えられる ・この数は約4年ごとに半減する（840,000ブロックごと） １回目: 2015年8月26日、２回目: 2019年8月5日 ・Litecoinネットワークでは、Bitcoinのおおよそ4倍の量の暗号資産、約840,000,000枚のLitecoinが生成される事になる	なし	年毎のインフレーションレートは1% 2021年9月現在、1ブロックを発行するごとに1QTUM発行 4年毎に半減期を迎える（次回は2021年12月）	なし

	過去３年間の発行状況	－	1,000,000,000	2017年3月、ICO時に1億QTUMが発行され、それ以降ブロック高5,001から844,999までは1ブロックごとに4QTUM、ブロック高845,000（2021年4月30日）以降は1ブロックごとに1QTUMの報酬が発行されている。	発行済数量に等しい
	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	不特定多数の利用者の需要による
	過去３年間の償却状況	－	－	－	不明
	過去３年間の償却理由	－	－	－	不特定多数の利用者の需要による
	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	－	－	－	－
【	ブロックチェーン技術の利用の有無	あり	あり	あり	あり

【価値移転記録台帳に係る技術】

ブロックチェーンの形式	パブリック型	パブリック型 VBFT形式のPoSの独自コンセンサスアルゴリズムを採用	パブリック型	パブリック型ブロックチェーン
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	ブロックチェーンが60000ブロック進むごとに、記録者候補の中から提案、検証、承認のフェーズごとにランダムに複数の記録者が選ばれ、選ばれた記録者はトランザクションの整合性を確認し合意形成を行いブロックを生成する	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	EthereumのPoSに則って価値の移転が認証されている（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	公開	公開
保有者個人データの秘匿性の有無	あり	あり	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	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	ネットワークの記録者になるには、最低1万ONTをステークする必要があるうえ、candidate nodeになるにはステーク量が上位343位に、register nodeとなるためには上位15位に入る必要がある。この為記録者にとっては保有通貨の価値が下がることは行わない動機が働く。	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。	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	マイニングプールの数は約20だが、誰でも自由に記録者になることができるため、総数については特定できない。 また、ハッシュレートが1%以上のマイニングプールは11である。 参考 https://chainz.cryptoid.info/ltc/#!extraction	14（コンセンサスノードの数）	https://qtum.org/en/product/nodemap	https://beaconscan.com/validators
	記録者の分布状況	世界中に分布	世界中に分布	主にアメリカ合衆国、韓国	不特定
	記録者の主な属性	マイニングプールが主流	ONTをステーキングしている人たちが記録者	不特定、誰でも自由に記録者になることができる	ERC－20トークンであるためEthereumのマイナー（記録者）と同一（Ethereumの記録者に必要な設備さえあれば、誰でも自由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	ブロックに記録された後は修正・変更は行われない

	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	60000ブロック進むごと提案、検証、承認のフェーズごとに複数の記録者がランダムに変更されるため、悪意をもった記録者が結託することは難しい仕組みとなっている	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	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	－	あり	なし	なし
	統括者の名称	－	Ontology Foundation	－	－
	統括者の所在地	－	2 VENTURE DRIVE #11－31 VISION EXCHANGE SINGAPORE 608526	－	－
	統括者の属性	－	－	－	－
	統括者の概要	－	Ontology Foundationはシンガポールに本部を置き、ONT利用者及びエコシステムを拡大し、ネットワークの価値を高めることを目的とする団体。	－	－

【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	VBFTコンセンサスアルゴリズムでは、承認作業に参加するノードをランダムに選択することによって、ネットワーク攻撃への耐性を向上さセール。また、ネットワーク分離が発生しチェーンが分岐するリスクに対しても、検証可能なランダム関数(VRF)コンセンサスエンジンにより、悪意のあるフォークを維持し続けることは非常に困難または不可能となり、すぐに消滅する。	メインネットワーク上で多数の記録者が結託することで記録台帳を改竄することができる	記録者が結託する、もしくは単独でその時点における計算能力の半分を上回る計算能力を得ることができたら、記録の変更が可能である（51%攻撃など）
	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	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。	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	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	−	なし	なし	発行者が破たんした場合は、資産の利用価値が著しく低下する恐れもあるが、自発的に参加する開発者によってプロジェクトが継続され、価値喪失にまでは至らない可能性もある。

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	－	－	－	ERC－20トークンであるため、記録者はEthereumと同一である。記録者の大多数が破たんした場合は正しい記録が行われないリスクや価値移転が記録されないリスクに直面し、価値が喪失する可能性はあるものの、ごく一部の記録者の破たんではネットワークに問題はないものと思われる。この点、Ethereumの記録者は十分に分散しているため、一度に破綻するような事態は想定しにくい

移転の記録が遅延する可能性に関する特記事項	・一旦、分岐したブロックの一方が否決された場合、否決されたブロックに収録された取引は再び認証を得なければ、次の送金が行なえなくなる ・記録者の目に留まらず、未承認データのまま放置される恐れあり	なし		ERC－20トークンであるため、処理能力はEthereumに依存する。Ethereumの処理能力を上回る取引がブロックチェーン上で行われた場合、もしくは、記録者の数や処理能力が極端に低下した場合には、遅延が生じる可能性がある
プログラムの不具合によるリスク等 に関する特記事項	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Litecoinの異なる者との取引、複数の所有者が同一のLitecoin 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。	現在発見されていない脆弱性を悪意のある攻撃者に突かれた場合、他の仮想通貨と同程度の一定のリスクは存在する。	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	他の暗号資産と同様に、現時点でまだ発見されていない脆弱性を悪意のある攻撃者に突かれる一定のリスクは存在するものの、現状は正常に稼働している

	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	・2016年、Cryptsy交換所（倒産）がハッキングを受け、100,000,000円相当のLTC（300,000 LTC）が盗難に遭った事例がある ・BTCとは異なり、すべてのLTCがホットウォレットで管理されていたとされる	－	－	なし
	非互換性のアップデート(ハードフォーク）の状況	－	－	－	ETHとETCに分かれるハードフォークが起きている
	今後の非互換性アップデート予定	－	－	－	なし
	正常な稼働に影響を与えたサイバー攻撃の履歴	－	－	－	The DAO事件が起こっている（2016年6月）

【流通状況】	価格データの出所	出所：CoinMarketCap URL： https://coinmarketcap.com/coins/	出所：CoinMarketCap URL： https://coinmarketcap.com/coins/	出所：CoinMarketCap URL： https://coinmarketcap.com/coins/	出所：CoinMarketCap https://coinmarketcap.com/coins/
	1取引単位当たり計算単価（ドル基準、例：$1.000.000）	$55.59	$0.71	$11.59	$1.00
	1取引単位当たり計算単価（円基準、例：￥100.000.000）	¥5,823.00	¥78.40	¥1,277.64	¥138.50
	ドル/円計算レート	1ドル/104.757円（2020年10月31日基準）	1ドル/110円（2021年7月5日基準）	1ドル/約110円（2021年9月8日基準）	138.5円/ドル（2023年1月27日基準）
	四半期取引数量（協会加盟会員合計、現物、単位は百万円）	9,355	－	442,753	非公開
備考			Ontology Foundationが一部当社マーケティング費用を負担する	Qtum Chain Foundationが一部当社マーケティング費用を負担する	出所：CoinMarketCap

取扱暗号資産の概要説明書

		フレア
概要書更新年月日		3月10日
【基礎情報】	日本語の名称	フレア
	現地語の名称	Flare
	呼称（日本語の名称と同じ場合は－表記）	－
	ティッカーコード（シンボル）	FLR
	発行開始（年、月、日）	2022年7月14日（メインネットローンチ）
	時価総額（ドル基準、例：＄1.000.000）	$386,730,770
	時価総額（円基準、例：￥100.000.000）	51,938,830,106円
	主な利用目的	FXRP（Flare Networks上のXRP）発行時の担保、Flare Time Series Oracle(FTSO)データ提供者へのデリゲート報酬、ガバナンス参加
	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	Flare（旧Spark）はAvalancheプロトコルをベースに開発されたFlare Network上で、ガバナンス投票、取引手数料の支払い、ステーキング、に利用可能なネイティブトークンである。
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）	なし
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	2023年1月に配布予定の15%のAirDropが行われ、残りの85%をWrapしたトークン保有者に対して36カ月に渡って配布する予定。https://flare.network/fip01/
発行者に対して保有者が負う義務	なし
価値の決定	保有者間の自由売買による
交換（売買）の制限	なし
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	保有・移転の記録は公開されているが、移転記録上のトランザクションやアドレスから個人を特定をすることはできない。
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	Avalanche Consensus
	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）	AVAX
【取引単位・交換制限】	取引単位の呼称	FLR
	保有・移転記録の最低単位	0.000000000000000001 FLR
	交換可能な通貨又は暗号資産	全て可
	交換制限	なし
	制限内容	－
	交換市場の有無	なし
【連動	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	－

する資産の	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	FLRは、他ネットワークのトークンをトラストレスにFlareネットワーク上で発行するための担保として使用できる。
	過去3年間の付加価値（サービス）の提供状況	ー
【発行状況】	発行者	あり
	発行主体の名称	Flare Foundation
	発行主体の所在地	Netherlands, Keizersgracht 391A, 1016 EJ Amsterdam
	発行主体の属性等	非営利団体
	発行主体概要	Flare Foundationは、Flareエコシステムの成長と分散化の推進に対して責任を負う非営利団体。

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
発行方法	Flare Networkでは、メインネットローンチ時に1,000億FLRが発行された。
発行可能数	上限なし
発行可能数の変更可否	可能

変更方法	ガバナンス投票
変更の制約条件	ガバナンス投票は議題によってSimple Majority、Super Majority、Super Super Majorityの3つの段階に分類される。また、段階に応じて定足数と可決に必要な投票率が定められている。FLRの追加発行はSuper Super Majorityに分類され、80%の定足数と投票率70%が可決の条件となっている。
発行済み数量	100,559,787,198 FLR 参照： https://coinmarketcap.com/ja/currencies/flare/
今後の発行予定または発行条件	ガバナンスによって決定されたインフレ率に基づいてオラクル情報提供者に対して付与される。

	過去３年間の発行状況	100,559,787,198 FLR 参照： https://coinmarketcap.com/ja/currencies/flare/
	過去３年間の発行理由	初期発行、オラクル情報提供者への報酬
	過去３年間の償却状況	現在の焼却状況は不明だが、トランザクション手数料は焼却される設計となっている。
	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	-
【その他】	ブロックチェーン技術の利用の有無	あり

【価値移転記録台帳に係る技術】

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	Flareネットワークは、ノードとして誰でも簡単に参加することができ、完全に独立した意思決定者として価値移転認証を行うことができる

【価値移転の記録者】	記録者の数	5団体 https://twitter.com/FlareNetworks/status/1586004361578221568
	記録者の分布状況	5団体 https://validators.towolabs.com/
	記録者の主な属性	Flare Networkの記録者はFlare Time Series Oracle（FTSO）と呼ばれるオラクルにデータ提供を行う者である。 一定の要件を満たすことでノードとして誰でも参加することができる。
	記録の修正方法	取引が一旦記録されると、取引は変更することができない。承認された送金はキャンセルすることができないので、その送金を無効とするためには反対の取引を別途行う必要がある。それらの履歴は全てブロックチェーン上に記録される。

記録者の信用力に関する説明	記録者は一定の要件を満たすことで誰でも参加することができる。また、記録者は個別に信頼できるノードを選択できるため、ビザンチン耐性が高いと言える。
価値移転の管理状況に対する監査の有無	あり
監査を実施する者の氏名又は名称	Trail of Bits
直近時点で行われた監査年月日	44743
その監査結果	ー
（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	価値移転ネットワークの仕組み対して、ノードのFLRの保有数や担保数は直接的に関係していないため、51%攻撃やシビル攻撃耐性を有する。また、各ノードは事前に信頼できないノードを決定することによって、万一ノードにネットワーク障害が発生した場合であっても価値移転ネットワークを問題なく行うことができる。
	保有情報暗号化技術の脆弱性に関する特記事項	暗号資産の保有情報にあたる公開鍵や秘密鍵は暗号化されるため、個人を特定することはできないものの、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。防止策として秘密鍵の管理者は自己の責任で厳重に管理する必要がある。

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	発行者であるFlare Foundationが破たんした場合、開発遅延を含む混乱が生じることから短期的な価格への影響が考えられる。しかし、基本的にはFlare FoundationはFLR保有者によるガバナンスの決定に基づいて開発を主導するのみに留まるため、FLRの価値と開発者の存在に相関関係はなく、価値喪失にまでは至らない可能が考えられる。

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	記録者の大多数が破たんした場合、正しい記録が行われないリスクや価値移転が記録されないリスクに直面し、価値が喪失する可能性がある。しかし、記録者には一定の要件を満たすことで誰でもなることができるため、記録者が一度に破たんするような可能性は低いと考えられる。また、一部の記録者のみの破たんではネットワークに問題は生じない。 具体的なブロック承認や記録を行う仕組みとして、The Flare Consensus Protocol（FCP）が採用されている。FCPでは、ネットワーク上のノードは完全に独立した意思決定者としてランダムにトランザクションを引き受け、そのトランザクションの承認または非承認を決定する。その後、ネットワークの他のノードがこの決定に同意するかどうかの投票を行い、クォーラム（必要な最低限の投票数）に達すると価値移転認証が行われる。

移転の記録が遅延する可能性に関する特記事項	Avalanche Consensus TOSは4500以上とされている。また、一般的なPoSではバリデーターの数が増加すると検証回数も増加するため遅延が発生する場合があるが、Avalanche Consensusではトランザクションの並列処理が行われるため、バリデーターの増加による遅延は発生しない。
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、資金の意図しないロックや紛失等のリスクが発生する可能性がある。また、プログラムの不具合をついた攻撃によるリスクがある。

	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	ー
	非互換性のアップデート(ハードフォーク）の状況	ー
	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	ー

【流通状況】	価格データの出所	出所：CryptoCurrency Market Capitalizations https://coinmarketcap.com/ja/currencies/spark-flare/
	1取引単位当たり計算単価（ドル基準、例：$1.000.000）	$0.03
	1取引単位当たり計算単価（円基準、例：￥100.000.000）	¥4.28
	ドル/円計算レート	1ドル/134.84円（2023年3月10日基準）
	四半期取引数量（協会加盟会員合計、現物、単位は百万円）	
備考		