TaoTao 株式会社
2019 年 3 月 4 日

取り扱い仮想通貨　概要書

仮想通貨の名称	ビットコイン	取引所内取扱最小単位	（現物）0.001BTC　　（レバレッジ）0.01BTC
仮想通貨ティカーコード	BTC,　XBT	取引所内最小刻み幅	1 円
当該仮想通貨の仕組み	【総発行数量】17,569,400 BTC（2019 年 3 月 4 日現在） 【発行上限数量】20,999,999.9769 BTC（2019 年 3 月 4 日現在） 【時価総額】67,916,329,606 米ドル（7,583,848,448,257 円）（2019 年 3 月 4 日現在） 【発行方法】 SHA-256 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、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される。 【認証方法】 SHA-256 アルゴリズムを用いたプルーフオブワーク(PoW) 【当該仮想通貨固有の特徴】 仮想通貨の起源であり、認知が進んでおり、取引の流動性も高い。PoW の負荷が高い為、認証に要する時間が長い。又、コミュニティの規模が大きいので、意見の相違から、分岐のリスクが相対的に高い。		
リスク等の記載	【価格変動リスク】 2018 年のビットコイン(BTC/USD)のヒストリカル・ボラティリティは 81.8%であり、価格変動リスクは相応に高い。 【サイバー攻撃リスク】 ブロックチェーンセキュリティ会社の CipherTrace 社が 2018 年 10 月に公表した「Cryptocurrency Anti-Money Laundering 2018 Q3」によると、2018 年 9 月までに全世界で 9 億 2,700 万ドル（約 1,000 億円）相当の仮想通貨がハッカーにより盗まれたとされている。		

	【流動性リスク】 従来の金融市場と比較すると、時価総額も低く、参加者が相対的に少ないため、需給の均衡価格＝適正価格との判断が難しい。 【決済完了性がないリスク】 仮想通貨プロトコル及び仮想通貨取扱事業者の仮想通貨管理方法により、仮想通貨ネットワーク（ブロックチェーン）が51%攻撃を受けた場合、またハードフォークによってそのアルゴリズム等によるバグが発生した場合において、仮想通貨取扱事業者であれば、認証回数（ブロックに追加されてからどの時点で仮想通貨の入庫を決定するのか）によって、当該事象発生区間におけるトランザクション（仮想通貨の入出庫）が遡って無効化されるリスクがある。 【ハードフォーク等による分岐リスク】 2018 年 11 月のビットコインキャシュの分岐（ABC 系と SV 系による分岐*）に代表されるように、適切な手段とプロセスによって実施されるハードフォークにおいては、リプレイプロテクションが双方実施されずに、送付元がどのクライアント（モジュール）を採用しているかによって、ネットワークが分断されたユーザー同士でトランザクションを送受信出来ないリスクが存在する。 また、ハードフォーク後に予期せぬバグが顕在化した場合においても、ブロックチェーンが無制限に分岐する、プロトコルが異常な挙動を示すなど、仮想通貨プロトコルとしての機能が失われるリスクがある。 *ABC 系と SV 系のハードフォークの際には、思想的な論争に発展したことからリプレイプロテクションが施されない問題（のちに SV 系においてリプレイプロテクションが実施）もあり、分岐直後の仮想通貨の送付等には、細心の注意が必要になることが顕著に現れた。 【51%攻撃等によるリスク】 現状、ビットコインのマイニング・プールは寡占状態にあり、理論上は、51%攻撃が可能（51% 攻撃とは悪意のあるグループまたは個人により、ネットワーク全体の採掘速度の 51%（50% 以上）を支配し、不正な取引を行うこと。 1 ノードが全体の計算能力の過半数を支配すると、①不正な取引の正当化、②正当な取引の拒否、③採掘の独占、を行うことが理

	論上可能となる。）な状態にある。51%攻撃に対する有効な対策は無いと言われているが、仮想通貨の時価総額とハッシュレートの関係（時価総額が上がると一般的にはハッシュレートが上がり、採掘が困難になる）から、通常の仮想通貨においては、攻撃者は期待値以上の利益を生めないため、攻撃を仕掛ける合理性が無いと言われている。 【リプレイ攻撃リスク】 ハードフォークの前後でトランザクションを明示的に識別しない、突発的または敵対的ハードフォークが発生した場合において、次のようなことが考えられる。ブロックチェーンに書き込まれるトランザクションには、送金者の秘密鍵によって電子署名が付与される。分岐したブロックチェーンに署名つきのトランザクションのコピーが存在する場合において、これも正規のトランザクションとみなされる。悪意を持った者がこのトランザクションを実行することで、もともとのトランザクションと同額の分岐後の仮想通貨を引き出すことが可能となる。 【ビザンチン障害リスク】 ビザンチン障害（相互に通信し合う P2P ネットワーク上で、通信そのものや個々のノードが故障、または故意に偽の情報を伝達する可能性がある場合に、全体として正しい合意が形成できるかを問う問題）に対して、プルーフオブワークにおいては、プロトコルにより、生成済みブロックの数が多いブロックチェーンが正しいとルールが定められているため、ビザンチン障害が発生したとしても、プロトコル上のリスクはない。 【エクリプス攻撃のリスク】 P2P ネットワークにおいて、すべてのブロックの情報が伝達されるまでにはラグが存在する可能性が十分にあり、地理的に分散した P2P ネットワーク・ノードのうち、一つのネットワークを形成するために地理的・ネットワーク的に重要な地点にあるノード郡が重点的に攻撃されることによって、P2P ネットワークが分断されるリスクがある（エクリプス攻撃）。この分断した状況を用いて、異なるトランザクションを流し、ブロックチェーンの分岐を意図的に起こし、ハードフォークされた状況と同様の状態を起こし、分断されたネットワーク間でのトランザクションの送受信が不可能となるリスクがある。

	そして、エクリプス攻撃から復旧し、ネットワークが再接続された際、ブロックチェーンは再び一つに統合されるため、分断から復旧までに発生し承認された２つのネットワークのトランザクションのうち、片方のトランザクションが無効になるリスクがある。

仮想通貨の名称	イーサリアム	取引所内取扱最小単位	0.01ETH
仮想通貨ティカーコード	ETH	取引所内最小刻み幅	1 円
当該仮想通貨の仕組み	【総発行数量】105,110,130 ETH（2019 年 3 月 4 日現在） 【発行上限数量】未定 【時価総額】13,860,348,536 米ドル（1,552,686,876,093 円）（2019 年 3 月 4 日現在） 【発行方法】 Ethash 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、Ethreum 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 15 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、Ethereum 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。 【認証方法】 Ethash アルゴリズムを用いたプルーフオブワーク（PoW） (Casper アルゴリズムを用いたプルーフオブステイク（PoS）に移行される予定。) 【当該仮想通貨固有の特徴】 スマートコントラクト実行用のプラットフォームとしての性格を有する。		
リスク等の記載	【価格変動リスク】 2018 年のイーサリアム(ETH/USD)のヒストリカル・ボラティリティは 107.8%であり、価格変動リスクは相応に高い。 又、今後、現行の Ethash アルゴリズムから Casper アルゴリズムに変更することが予定されており、基幹コンセンサス・アルゴリズムの変更の影響、また発行可能上限への影響から、大きな価格変動が発生するリスクがある。 【サイバー攻撃リスク】		

	サイバー攻撃によるハッキングによる仮想通貨建て資産の盗難：ブロックチェーンセキュリティ会社の CipherTrace 社が 2018 年 10 月に公表した「Cryptocurrency Anti-Money Laundering 2018 Q3」によると、2018 年 9 月までに全世界で 9 億 2,700 万ドル（約 1,000 億円）相当の仮想通貨がハッカーにより盗まれたとされている。 【決済完了性がないリスク】 仮想通貨プロトコル及び仮想通貨取扱事業者の仮想通貨管理方法により、仮想通貨ネットワーク（ブロックチェーン）が 51%攻撃を受けた場合、またハードフォークによってそのアルゴリズム等によるバグが発生した場合において、仮想通貨取扱事業者であれば、認証回数（ブロックに追加されてからどの時点で仮想通貨の入庫を決定するのか）によって、当該事象発生区間におけるトランザクション（仮想通貨の入出庫）が遡って無効化されるリスクがある可能性がある。 【流動性リスク】 従来の金融市場と比較すると、時価総額が低く、参加者が依然少ないため、適正価格で売買が成立しないリスクがある。 【ハードフォーク等による分岐リスク】 2018 年 11 月のビットコインキャシュの分岐（ABC 系と SV 系による分岐*）に代表されるように、適切な手段とプロセスによって実施されるハードフォークにおいて、リプレイプロテクションが双方実施されずに、送付元がどのクライアント（モジュール）を採用しているかによって、ネットワークが分断されたユーザー同士でトランザクションを送受信出来ないリスクが存在する。 また、ハードフォーク後に予期せぬバグが顕在化した場合においても、ブロックチェーンが無制限に分岐する、プロトコルが異常な挙動を示すなど、仮想通貨プロトコルとしての機能が失われるリスクがある。 *ABC 系と SV 系のハードフォークの際には、思想的な論争に発展したことからリプレイプロテクションが施されないなどの問題（のちに SV 系においてリプレイプロテクションが実施）もあり、分岐直後の仮想通貨の送付等には、細心の注意が必要になることが顕著に現れた。 【51%攻撃等によるリスク】

	イーサリアムのブロックチェーンも非中央集権化されており概ねセキュアであるが、ビットコイン同様に 51%攻撃を受けるリスクがある。 ただし、経済的合理性がなく本攻撃が確認されたことは無いが、ビットコインに比べると攻撃に必要なコストは低い(1/4 程度)という試算は行われている。 【リプレイ攻撃リスク】 ハードフォークの前後でトランザクションを明示的に識別しない、突発的または敵対的ハードフォークが発生した場合において、次のようなことが考えられる。ブロックチェーンに書き込まれるトランザクションには、送金者の秘密鍵によって電子署名が付与される。分岐したブロックチェーンに署名つきのトランザクションのコピーが存在する場合において、これも正規のトランザクションとみなされます。悪意を持った者がこのトランザクションを実行することで、もともとのトランザクションと同額の分岐後の仮想通貨を引き出すことが可能となる。 【ビザンチン故障リスク】 プルーフオブワークにおいては、プロトコルにより、生成済みブロックの数が多いブロックチェーンが正しいとルールが定められているため、ビザンチン故障が発生したとしても、プロトコル上のリスクはない。 【エクリプス攻撃のリスク】 P2P ネットワークにおいて、すべてのブロックの情報が伝達されるまでにはラグが存在する可能性が十分にあり、地理的に分散した P2P ネットワーク・ノードのうち、一つのネットワークを形成するために地理的・ネットワーク的に重要な地点にあるノード郡が重点的に攻撃されることによって、P2P ネットワークが分断されるリスクがある。このような攻撃をエクリプス攻撃と呼ぶ。この分断した状況を用いて、異なるトランザクションを流し、ブロックチェーンの分岐を意図的に起こし、ハードフォークされた状況と同様の状態を起こし、分断されたネットワーク間でのトランザクションの送受信が不可能となるリスクがある。

	そして、エクリプス攻撃から復旧し、ネットワークが再接続された際、ブロックチェーンは再び一つに統合されるため、分断から復旧までに発生し承認された２つのネットワークのトランザクションのうち、片方のトランザクションが無効になるリスクがある。 【PoS への移行後のリスク】 PoS は PoW の弱点となる部分を解決するために考案されたコンセンサスアルゴリズムであるが、いくつかの問題点が存在する。 ＜Nothing at Stake 問題＞ block を生成することにコストがあまりかからなくなることから、悪意のあるホルダーによって、PoW のようにマイニングマシンへの投資や計算コストをかけることなく不正ブロックの生成が可能になってしまう恐れがある。アルゴリズムによって分岐した複数のブロックへの投票については、アルゴリズムにおいて投票の価値を計算することから、故意での分岐したブロックへのブロック追加は、難しいものとなる仕様である。 その一方で大規模保有者による、不正ブロックの生成した場合にはこの限りではなくなるため、一定のリスクがある。 （大規模保有者が自らの保有通貨の価値を著しく低下させるような行為をとることは考えにくいが、複数の保有者が結託することでのリスクは避けられない。Ethereum はこれまでを PoW でのコンセンサスアルゴリズムでの実装を行い、広くその保有者も世界各地に広がっていることから考えると現実化する可能性は低い。）

仮想通貨の名称	ライトコイン	仮想通貨の最小単位	1000LTC
仮想通貨ティカーコード	LTC	取引所内最小刻み幅	0.1 円
当該仮想通貨の仕組み	【総発行数量】60,720,736 LTC（2019 年 3 月 4 日現在） 【発行上限数量】83,999,999.9076 LTC（2019 年 3 月 4 日現在） 【時価総額】2,943,226,269 米ドル（329,200,849,291 円）（2019 年 3 月 4 日現在） 【発行方法】 Scrypt アルゴリズムを用いたプルーフオブワーク（PoW）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 【認証方法】 Scrypt アルゴリズムを用いたプルーフオブワーク(PoW) 【当該仮想通貨特有の特徴】 決済利用を前提に認証の容易性を打ち出した仮想通貨。又、アトミックスワップとの親和性も高い。		
リスク等の記載	【価格変動リスク】 2018 年のライトコイン(LTC/USD)のヒストリカル・ボラティリティは 95.21%であり、価格変動リスクは相応に高い。 【サイバー攻撃リスク】 サイバー攻撃によるハッキングによる仮想通貨建て資産の盗難：ブロックチェーンセキュリティ会社の CipherTrace 社が 2018 年 10 月に公表した「Cryptocurrency Anti-Money Laundering 2018 Q3」によると、2018 年 9 月までに全世界で 9 億 2,700 万ドル（約 1,000 億円）相当の仮想通貨がハッカーにより盗まれたとされている。 【流動性リスク】 従来の金融市場と比較すると、時価総額が低く、参加者が依然少ないため、適正価格で売買が成立しないリスクがある。		

	【決済完了性がないリスク】 仮想通貨プロトコル及び仮想通貨取扱事業者の仮想通貨管理方法により、仮想通貨ネットワーク（ブロックチェーン）が51%攻撃を受けた場合、またハードフォークによってそのアルゴリズム等によるバグが発生した場合において、仮想通貨取扱事業者であれば、認証回数（ブロックに追加されてからどの時点で仮想通貨の入庫を決定するのか）によって、当該事象発生区間におけるトランザクション（仮想通貨の入出庫）が遡って無効化されるリスクがある可能性がある。 【ハードフォーク等による分岐リスク】 2018 年 11 月のビットコインキャシュの分岐（ABC 系と SV 系による分岐*）に代表されるように、適切な手段とプロセスによって実施されるハードフォークにおいて、リプレイプロテクションが双方実施されずに、送付元がどのクライアント（モジュール）を採用しているかによって、ネットワークが分断されたユーザー同士でトランザクションを送受信出来ないリスクが存在する。 また、ハードフォーク後に予期せぬバグが顕在化した場合においても、ブロックチェーンが無制限に分岐する、プロトコルが異常な挙動を示すなど、仮想通貨プロトコルとしての機能が失われるリスクがある。 *ABC 系と SV 系のハードフォークの際には、思想的な論争に発展したことからリプレイプロテクションが施されないなどの問題（のちに SV 系においてリプレイプロテクションが実施）もあり、分岐直後の仮想通貨の送付等には、細心の注意が必要になることが顕著に現れた。 【51%攻撃等によるリスク】 一部のマイナーの共謀、またはマイニングプールの寡占により、ネットワーク全体の計算力のうち、過半数以上を占めた場合、最新のブロックとは別に、異なるハッシュ値を持つブロックを採掘しブロックチェーンを上書き、上書かれた一部のトランザクションを無効化する 51%攻撃が可能になるリスクがある。51%攻撃を成功させるには、66%超の計算力が必要になるとされている。 【リプレイ攻撃リスク】

	ハードフォークの前後でトランザクションを明示的に識別しない、突発的または敵対的ハードフォークが発生した場合において、次のようなことが考えられる。ブロックチェーンに書き込まれるトランザクションには、送金者の秘密鍵によって電子署名が付与される。分岐したブロックチェーンに署名つきのトランザクションのコピーが存在する場合において、これも正規のトランザクションとみなされます。悪意を持った者がこのトランザクションを実行することで、もともとのトランザクションと同額の分岐後の仮想通貨を引き出すことが可能となる。 【ビザンチン故障リスク】 プルーフオブワークにおいては、プロトコルにより、生成済みブロックの数が多いブロックチェーンが正しいとルールが定められているため、ビザンチン故障が発生したとしても、プロトコル上のリスクはない。 【エクリプス攻撃のリスク】 P2P ネットワークにおいて、すべてのブロックの情報が伝達されるまでにはラグが存在する可能性が十分にあり、地理的に分散した P2P ネットワーク・ノードのうち、一つのネットワークを形成するために地理的・ネットワーク的に重要な地点にあるノード郡が重点的に攻撃されることによって、P2P ネットワークが分断されるリスクがある。このような攻撃をエクリプス攻撃と呼ぶ。この分断した状況を用いて、異なるトランザクションを流し、ブロックチェーンの分岐を意図的に起こし、ハードフォークされた状況と同様の状態を起こし、分断されたネットワーク間でのトランザクションの送受信が不可能となるリスクがある。 そして、エクリプス攻撃から復旧し、ネットワークが再接続された際、ブロックチェーンは再び一つに統合されるため、分断から復旧までに発生し承認された 2 つのネットワークのトランザクションのうち、片方のトランザクションが無効になるリスクがある。

仮想通貨の名称	リップル	取引所内取扱最小単位	100drop
仮想通貨ティカーコード	XRP	取引所内呼値	0.001 円
当該仮想通貨の仕組み	【総発行数量】41,432,141,931 XRP （2019 年 3 月 4 日現在） 【発行上限数量】100,000,000,000XRP（2019 年 3 月 4 日現在） 【時価総額】12,949,720,688 米ドル（1,449,970,232,009 円）（2019 年 3 月 4 日現在） 【発行方法】 Ripple, Inc.が一元的に発行・管理する。 2012 年のネットワーク発足時に全て発行済み 【認証方法】 Proof of Consensus Ripple, Inc. の独自アルゴリズム – Consensus 登録されているバリデータの 80%以上が合意を行うことにより、そこで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る。 【当該仮想通貨固有の特徴】 送金利用を前提とした仮想通貨であり、ED25519 and SECP256K1 による暗号署名、SHA512 half によるハッシュに化、Multi-sign 機能を実装。不特定、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（Ripple 社に選出されたもの）の投票だけが投票プロセスにおいて考慮される。バリデータの 80%の合意が取れたことを移転の完了とすることから、完全なファイナリティが得られる。		
リスク等の記載	【価格変動リスク】 2018 年のリップル(XRP/USD)のヒストリカル・ボラティリティは 129.1%であり、価格変動リスクは相応に高い。 【サイバー攻撃リスク】		

	サイバー攻撃によるハッキングによる仮想通貨建て資産の盗難：ブロックチェーンセキュリティ会社の CipherTrace 社が 2018 年 10 月に公表した「Cryptocurrency Anti-Money Laundering 2018 Q3」によると、2018 年 9 月までに全世界で 9 億 2,700 万ドル（約 1,000 億円）相当の仮想通貨がハッカーにより盗まれたとされている。 【流動性リスク】 従来の金融市場と比較すると、時価総額が低く、参加者が依然少ないため、適正価格で売買が成立しないリスクがある。 【決済完了性がないリスク】 Ripple, Inc.がバリデーター・ノードを一元的に管理しているため、実質的に決済完了性が担保されるため、決済完了性がないリスクはない。 【ハードフォーク等による分岐リスク】 2018 年 11 月のビットコインキャシュの分岐（ABC 系と SV 系による分岐*）に代表されるように、適切な手段とプロセスによって実施されるハードフォークにおいて、リプレイプロテクションが双方実施されずに、送付元がどのクライアント（モジュール）を採用しているかによって、ネットワークが分断されたユーザー同士でトランザクションを送受信出来ないリスクが存在する。 また、ハードフォーク後に予期せぬバグが顕在化した場合においても、ブロックチェーンが無制限に分岐する、プロトコルが異常な挙動を示すなど、仮想通貨プロトコルとしての機能が失われるリスクがある。 *ABC 系と SV 系のハードフォークの際には、思想的な論争に発展したことからリプレイプロテクションが施されないなどの問題（のちに SV 系においてリプレイプロテクションが実施）もあり、分岐直後の仮想通貨の送付等には、細心の注意が必要になることが顕著に現れた。 【リプレイ攻撃リスク】 ハードフォークの前後でトランザクションを明示的に識別しない、突発的または敵対的ハードフォークが発生した場合において、次のようなことが考えられる。ブロックチェーンに書き込まれるトランザクションには、送金者の秘密鍵によって電子署名が付与される。分岐したブロックチェーンに署名つきのトランザクションのコピーが存在する場合において、

	これも正規のトランザクションとみなされます。悪意を持った者がこのトランザクションを実行することで、もともとのトランザクションと同額の分岐後の仮想通貨を引き出すことが可能となる。 【51%攻撃等によるリスク】 Ripple,Inc.が適正に一元的に発行・管理される限り、リスクはない。 【ビザンチン故障リスク】 Ripple, Inc.が指定するバリデーター・ノードが何らかの攻撃を受け停止する、または虚偽の情報を発信する場合、Ripple コンセンサス・レジャーの追記が不可能になるリスクがある。 【エクリプス攻撃のリスク】 P2P ネットワークにおいて、すべてのブロックの情報が伝達されるまでにはラグが存在する可能性が十分にあり、地理的に分散した P2P ネットワーク・ノードのうち、一つのネットワークを形成するために地理的・ネットワーク的に重要な地点にあるノード郡が重点的に攻撃されることによって、P2P ネットワークが分断されるリスクがある。このような攻撃をエクリプス攻撃と呼ぶ。この分断した状況を用いて、異なるトランザクションを流し、ブロックチェーンの分岐を意図的に起こし、ハードフォークされた状況と同様の状態を起こし、分断されたネットワーク間でのトランザクションの送受信が不可能となるリスクがある。 そして、エクリプス攻撃から復旧し、ネットワークが再接続された際、ブロックチェーンは再び一つに統合されるため、分断から復旧までに発生し承認された 2 つのネットワークのトランザクションのうち、片方のトランザクションが無効になるリスクがある。

仮想通貨の名称	ビットコインキャシュ	販売所内最小取扱単位	0.1BCH
仮想通貨ティカーコード	BCH, BCC	取引所内呼値	1 円
当該仮想通貨の仕組み	【総発行数量】17,652,838 BCH（2019 年 3 月 4 日現在） 【発行上限数量】20,999,999.9769 BCH（2019 年 3 月 4 日現在） 【時価総額】2,325,678,103 米ドル（260,202,720,802 円）（2019 年 3 月 4 日現在） 【発行方法】 SHA-256 アルゴリズムを用いたプルーフオブワーク（PoW）の仕組みにより、Bitcoin Cash 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 10 分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、Bitcoin Cash 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。 【認証方法】 SHA-256 アルゴリズム及び Median Time Past (MTP)を用いたブロック時間を基準に、直近 6 ブロックが 12 時間以内に採掘されていない場合、最大 20%ずつ採掘難易度が調整される難易度調整アルゴリズムを用いたプルーフオブワーク 【当該仮想通貨固有の特徴】 ビットコインからマイナー主導で分岐し誕生した仮想通貨であるため、マイナーの寡占状態が続いている。又、ブロックサイズは８MB、Segwit を実装していない。		
リスク等の記載	【価格変動リスク】 2018 年のビットコインキャシュ(BCH/USD)のヒストリカル・ボラティリティは 143.7%であり、価格変動リスクは相応に高い。 【サイバー攻撃リスク】		

	サイバー攻撃によるハッキングによる仮想通貨建て資産の盗難：ブロックチェーンセキュリティ会社の CipherTrace 社が 2018 年 10 月に公表した「Cryptocurrency Anti-Money Laundering 2018 Q3」によると、2018 年 9 月までに全世界で 9 億 2,700 万ドル（約 1,000 億円）相当の仮想通貨がハッカーにより盗まれたとされている。 【流動性リスク】 従来の金融市場と比較すると、時価総額が低く、参加者が依然少ないため、適正価格で売買が成立しないリスクがある。 【決済完了性がないリスク】 仮想通貨プロトコル及び仮想通貨取扱事業者の仮想通貨管理方法により、仮想通貨ネットワーク（ブロックチェーン）が 51%攻撃を受けた場合、またハードフォークによってそのアルゴリズム等によるバグが発生した場合において、仮想通貨取扱事業者であれば、認証回数（ブロックに追加されてからどの時点で仮想通貨の入庫を決定するのか）によって、当該事象発生区間におけるトランザクション（仮想通貨の入出庫）が遡って無効化されるリスクがある可能性がある。 【ハードフォーク等による分岐リスク】 2018 年 11 月のビットコインキャシュの分岐（ABC 系と SV 系による分岐*）に代表されるように、適切な手段とプロセスによって実施されるハードフォークにおいて、リプレイプロテクションが双方実施されずに、送付元がどのクライアント（モジュール）を採用しているかによって、ネットワークが分断されたユーザー同士でトランザクションを送受信出来ないリスクが存在する。 また、ハードフォーク後に予期せぬバグが顕在化した場合においても、ブロックチェーンが無制限に分岐する、プロトコルが異常な挙動を示すなど、仮想通貨プロトコルとしての機能が失われるリスクがある。 *ABC 系と SV 系のハードフォークの際には、思想的な論争に発展したことからリプレイプロテクションが施されないなどの問題（のちに SV 系においてリプレイプロテクションが実施）もあり、分岐直後の仮想通貨の送付等には、細心の注意が必要になることが顕著に現れた。 【51%攻撃等によるリスク】

	2019 年 1 月 3 日、一時的に中国を拠点とするマイナーである BTC.TOP のハッシュパワーが 679PH/s となり、他のプールをはるかに上回り、51%攻撃が可能な状態が生じた（ViaBTC：215 PH / s、BTC.com：257 PH / s、Bitcoin.com：187 PH / s、AntPool：125 PH / s） 【リプレイ攻撃リスク】 ハードフォークの前後でトランザクションを明示的に識別しない、突発的または敵対的ハードフォークが発生した場合において、次のようなことが考えられる。ブロックチェーンに書き込まれるトランザクションには、送金者の秘密鍵によって電子署名が付与される。分岐したブロックチェーンに署名つきのトランザクションのコピーが存在する場合において、これも正規のトランザクションとみなされます。悪意を持った者がこのトランザクションを実行することで、もともとのトランザクションと同額の分岐後の仮想通貨を引き出すことが可能となる。 【ビザンチン故障リスク】 プルーフオブワークにおいては、プロトコルにより、生成済みブロックの数が多いブロックチェーンが正しいとルールが定められているため、ビザンチン故障が発生したとしても、プロトコル上のリスクはない。 【エクリプス攻撃のリスク】 P2P ネットワークにおいて、すべてのブロックの情報が伝達されるまでにはラグが存在する可能性が十分にあり、地理的に分散した P2P ネットワーク・ノードのうち、一つのネットワークを形成するために地理的・ネットワーク的に重要な地点にあるノード郡が重点的に攻撃されることによって、P2P ネットワークが分断されるリスクがある。このような攻撃をエクリプス攻撃と呼ぶ。この分断した状況を用いて、異なるトランザクションを流し、ブロックチェーンの分岐を意図的に起こし、ハードフォークされた状況と同様の状態を起こし、分断されたネットワーク間でのトランザクションの送受信が不可能となるリスクがある。 そして、エクリプス攻撃から復旧し、ネットワークが再接続された際、ブロックチェーンは再び一つに統合されるため、分断から復旧までに発生し承認された 2 つのネットワークのトランザクションのうち、片方のトランザクションが無効になるリスクがある。