JPYCoin (JPYC)WhitePaper ~自家型前払式支払手段 ERC20 トークン~

岡部典孝 原沢陽水

日本暗号資産市場株式会社

概要

本プロジェクトペーパーでは、前払式支払手段扱いの日本円連動ステーブルコインの提案をします。ビットコインやイーサリアムなどブロックチェーンを活用した暗号資産による決済手段が 2010 年前後から台頭してきましたが、価格変動が大きく物との売買に用いるには困難を極めました。そういった問題意識から、近年になってブロックチェーンを活用し法定通貨や暗号資産を担保にした USD 連動ステーブルコインが複数発行されました。これらUSD 連動ステーブルコインの台頭はあるものの、いずれも日本円連動ステーブルコイン実用化は遠いものでした。 JPYCoin(以下 JPYC) では、事業者用自家型前払式支払手段であった ICB からご利用いただけるユーザーを拡大し、一般向けの前払式支払手段扱いの日本円連動ステーブルコインとして、暗号資産と物との売買を円滑にします。

1 イントロダクション

1.1 暗号資産が抱える問題

2008 年にビットコインが誕生して以来、ブロックチェーンを活用した決済手段は世界中で議論、実験されています。しかし、大きな価格変動リスクを抱えていることが原因で一般的な決済手段として普及することは未だ難しいとされています。ドル建ての日本円価値は 2020 年初から 2021 年初の 1 年間で約 5 %ほどの変動率ですが、ドル建てのビットコイン価値の変動率は同期間で約 400 %になります。1 日で数十%変動することもあるため、一般的な決済手段として用いるには非常に大きな壁があります。

1.2 現行の安定した価格を実現するように設計されたステーブルコイン

事業者が決済を円滑にすることを目的としてブロックチェーンを活用した決済手段を導入するためには、ビットコインなどの価格が安定しない暗号資産では難しいことが早々に周知のこととなりました。その中で当社は、前払式支払手段扱いの日本円連動ステーブルコインを発明し発行しました。

ブロックチェーン上で、安定した価格を実現するように設計されたステーブルコインはおおむね3種類あり、(i) 法定通貨を担保にした法定通貨担保型ステーブルコイン、(ii) ETH などの暗号資産を担保にした暗号資産担保型ステーブルコイン、及び(iii) 無担保型ステーブルコインです。

1.3 現行の安定した価格を実現するように設計されたステーブルコインが抱える問題

法定通貨担保型ステーブルコインと暗号資産担保型ステーブルコインは、市場に出回りつつありますが、いくつかの問題を抱えています。法定通貨担保型ステーブルコインの代表例として、米国の Tether 社が発行している USDT が挙げられますが、担保となる資産(ドルなど)を発行体である企業が不正使用してしまうリスクがあります。また、暗号資産担保型ステーブルコインの代表例としては MakerDAO が発行する DAI が挙げられますが、DAI は主に ETH の過剰担保によって成り立っているため、資本効率に課題があります。

また、現行の安定した価格を実現するように設計されたステーブルコインは、USD 連動型が基本であり、日本円での決済ができないことから日本国内での利便性の低さを課題としています。2021 年 1 月時点では、日本国内における前払式支払手段扱いの日本円連動ステーブルコイン(ERC20)は、当社の発行する事業者用前払式支払手段である ICB のみとなっております。

1.4 既に暗号資産を保有しているユーザーが抱える問題

暗号資産を保有しているユーザーが、物や体験に変えたいと思った時にいくつかの課題があります。

まず、暗号資産のサービスにアクセスするには交換業社を通さなければならず、日本円に変換するために高額の手数料を支払う必要があります。さらに、暗号資産を日本円に変換してから、口座への入金が完了し、物やサービスを購入するまでの一連の流れには時間を必要とします。このことも決済手段として用いるには非常に大きな壁となっています。

1.5 これから暗号資産を保有するユーザーが抱える問題

日本国内でこれから暗号資産を保有しようとするとき、いくつかの方法がありますが、それぞれ問題を抱えています。代表的な方法としてマイニングが挙げられますが、現在は企業が莫大なコストを設備投資にかけて採掘をしています。そのため、2021年1月時点で個人での採掘が困難な状態です。また、暗号資産交換業の販売所や取引所にて購入する方法も、いくつかの問題を抱えており、例えば、KYC手続きのため実際の売買まで待たされることがあります。また、システムのメンテナンスが高頻度で実施されることから、24時間開かれている市場での取引に最適とは評価できません。さらに、いくつかの取引所では手数料が高く設定されているためユーザーへの負担が高いことが課題となっています。

1.6 ICB が抱える問題とその対応

ICB は事業者向けであったたため、事業者しか購入ができませんでした。そのため、複数の個人の方から ICB を購入できないのかとお問い合わせいただくことがありました。しかし、これからはどなたでも JPYC を手に入れることが可能です。

また、ICB は資金決済法の適用除外による取扱いであった為、同法に基づく供託義務がありませんでした。 JPYC は資金決済法に従って供託を行うことで、ICB と比較して利用者保護をより重視した設計になっております。

2 JPYC の具体的内容

2.1 価格維持メカニズムについて

JPYC は前払式支払手段であり、当社でユーザーが使用する際には基本的に 1 JPYC =1 円となります。JPYC の価格維持メカニズムにより、ユーザーは従来の価格変動リスクを抱えたブロックチェーンを活用した決済手段から解放され、前払式支払手段扱いの日本円ステーブルコインである JPYC を用いて、物品調達等の決済手段としての使用が可能になります。ユーザーの健全な経済活動を支えるための JPYC 価格維持メカニズムは以下のとおりです。

2.1.1 1JPYC < 1 円の時(1円を下回る時)

Uniswap などの非中央集権分散型取引所にて、1JPYC の価格が長期間平均して1円を下回るとき、発行体は資金決済法に定められた供託金(基準日未使用残高の50%)以上の供託金を法務局に供託し、あるいは資金決済法に定められた金融機関保証を受けることにより二次流通価格の上昇を試みます。当面は資金決済法に定められ

た供託金の 200 % + 1000 万円を法務局に供託いたします。供託金額が増加した場合は供託後に当社 Web ページ 等にて告知します。

これにより万一当社が倒産等した場合でも国により倒産隔離されていることから JPYC の利用者の権利は保護されると考えておりますが、当社は元本保証するものではありません。

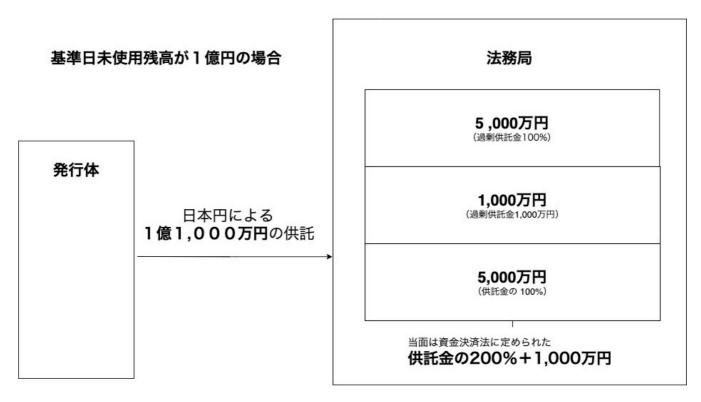


図 1 1JPYC < 1 円の時(1 円を下回る時)のイメージ図

2.1.2 1JPYC > 1 円の時 (1 円を上回る時)

二次流通の 1JPYC の価格が 1 円を上回る際には当社が公式サイトにて 1JPYC=1 円で売却を続けることで、二次流通の JPYC の価格も 1 円に近づき安定すると考えています。

また、上記にかかわらず長期間二次流通の平均価格が1円を上回っている場合、かつ、当社が資金決済法で要求される供託額を超える供託金(以下、過剰供託金といい、金融機関保証を含みます)を供託している場合には過剰供託による資金効率低下を防止する目的で、事前に当社 Web ページ等で告知の上、過剰供託金の一部(30%以下の範囲で平均二次流通価格が1円を下回らないと当社が判断した金額)を取り崩すことがあります。

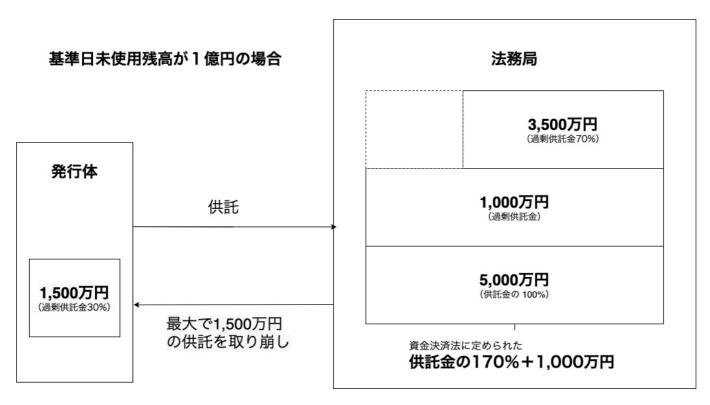


図 2 1JPYC > 1 円の時 (1 円を上回る時) のイメージ図

2.1.3 初回発行の JPYC の大部分が市中に流通したとき

初回は 1 億 JPYC を発行しますが、JPYC 需要の拡大により 1 億 JPYC では市場のニーズを満たせなくなるおそれがあります。あらかじめ決定された割合まで市場に JPYC が供給された段階で次のフェーズに移行し、JPYC を追加発行することで需要に応じた適切な発行量を保ちます。詳細は 2.4 にて後述します。

2.1.4 発行者が発行の業務を廃止したとき

資金決済法では、発行者が発行業務を廃止した際に払戻しを義務づけています。1JPYC=1 円で当社から払戻しを受けることができます。

2.1.5 発行者が破産したとき

発行者が破産すると JPYC は使えなくなりますが、利用者の保有残高は Ethereum ブロックチェーン上に記録され続けています。未使用分がある場合は、破産手続き上で、利用者に金銭を弁済する手続きが取られることになっています。

発行保証金の供託

資金決済法では、所定の基準日における未使用残高が 1,000 万円を超える自家型発行者は、その未使用残高の 2分の 1以上に相当する額の発行保証金を法務局に供託し保全することが義務づけられています。

還付手続

発行者が破産すると、この発行保証金を元に利用者にお金を返還する手続きが取られることになっており、これを還付手続といいます。利用者は還付手続に基づき発行保証金から優先的に弁済(配当)を受けることができます。

2.2 JPYC の法的性質

JPYC は日本法に基づき設立された株式会社により発行される自家型前払式支払手段です。通貨建資産であるため、法的には暗号資産ではありません。昨今、DeFi(分散型金融)の市場が急激に拡大しており、中でも Uniswap(運営者のいない非中央集権分散型取引所)は最も有名な DEX(分散型取引所)です。当社は Uniswap 等の分散型取引所を運営しておりませんが、JPYC 利用者の方は一利用者として Uniswap 等の分散型取引所を自己運用の為に利用することができます。

JPYC を用いて代理購入できないもの

JPYC は、日本法に基づく自家型前払式支払手段です。販売許可や資格・免許が必要になる商品は、代理購入をすることができない場合があります。

例:一部食品・酒類・医薬品・ペット・その他法令で転売が制限されているもの

2.3 ユーティリティ

2.3.1 日本暗号資産市場から Amazon 等の EC サイトの代理購入で1 JPYC = 1円で物を購入できます

BTC・ETH・JPY で購入いただいた JPYC は、日本暗号資産市場を通じて Amazon 等の EC サイトの代理 購入が可能です。二次流通の価格と関係なく 1JPYC=1 円で購入可能です。

2.3.2 Ethereum 上の各種 DeFi を利用できます

JPYC は ERC20 トークンであるため、Ethereum 上の各種 DeFi を利用可能です。一例として、非中央集権 貸出プラットフォーム Compound などを通じて JPYC を貸し出すことが考えられます。

なお、各種 DeFi の利用自体は、各利用者の権限と責任において行っていただくものとし、当社は DeFi の利用による損害等に関して一切の責任を負いません。あらかじめご了承ください。

2.4 JPYC の発行量

当社は、JPYC の発行量を順次増やしていく予定です。

- JPYC 1 発行上限 1 億 JPYC
- JPYC 2 発行上限 10 億 JPYC
- JPYC 3 発行上限 100 億 JPYC
- JPYC 4 発行上限 1000 億 JPYC
- JPYC 5 発行上限 1 兆 JPYC
- JPYC 6 発行上限 10 兆 JPYC
- JPYC 7 発行上限 100 兆 JPYC

JPYC の発行及び流通のメカニズムとしては、JPYC の 9 割 (9000 万 JPYC) 以上が外部に流通されると JPYC2 が発行され、その後 JPYC2 の 9 割 (9 億 JPYC) 以上が外部に流通されると次いで JPYC3 が発行されるという具合に、発行上限の 9 割以上が外部に流通した段階で、順次、JPYC を発行することを予定しています。

JPYC は追加発行可能(mintable)な ERC20 トークンなので、追加発行に伴うコントラクトアドレスの変更はありません。

2.5 JPYC インセンティブ提供プログラム(JIP)について

JPYC インセンティブ提供プログラム (本項では、JIP*1という) は、JPYC を Uniswap 等の分散型取引所 (本項では、DEX*2という) に流動性提供いただいた方に対して、提供量と提供期間に応じて報酬をお受けとりいただけるプログラムです。報酬はステーブルコインである USDC でお受け取りいただけます。JIP は指定した期間継続して 50,000JPYC 以上を DEX に流動性提供していただく必要があります。また、JIP は流動性提供いただいたタイミングにより以下のとおりフェーズ*3が決定します。

- フェーズ 1:DEX の JPYC 総額が 5,000 万円まで
- フェーズ 2:フェーズ 1 終了から DEX の JPYC 総額が 2 億 5,000 万円まで
- フェーズ 3:フェーズ 2 終了から DEX の JPYC 総額が 5 億円まで
- フェーズ 4:フェーズ 3 終了から DEX の JPYC 総額が 25 億円まで
- フェーズ 5:フェーズ 4 終了から DEX の JPYC 総額が 50 億円まで

各フェーズ毎のインセンティブ報酬は、流動性提供いただいた際の JPYC 提供量に対する割合で、表 1 のとおり 1 年毎に報酬をお受けとりいただけます。

	1 年間継続	2 年間継続	3 年間継続	4 年間継続	5 年間継続
フェーズ 1	10%	8%	6%	4%	2%
フェーズ 2	8%	6%	4%	2%	-
フェーズ 3	6%	4%	2%	-	-
フェーズ 4	4%	2%	-	-	-
フェーズ 5	2%	-	-	-	-

表1 各フェーズ毎のインセンティブ報酬

インセンティブプログラムの詳細は「JPYC インセンティブ提供プログラムとは*4」を参照ください。

3 ユースケース

3.1 ユースケース 1 「暗号資産の保有者による物の決済利用」

暗号資産を保有しているユーザーが、物の購入に暗号資産を用いたいときに、日本暗号資産市場へ Amazon 等の EC サイトでの代理購入を依頼することで 1 JPYC = 1 円で物を購入できます。

JPYC の購入方法については、「6.JPYC の購入方法」をご確認ください。

3.2 ユースケース 2「これから暗号資産を保有するユーザー」

JPYC の利用者は、ご自身の権限と責任において自己運用として非中央集権分散型取引所である Uniswap において ETH や JPYC とともに流動性供給されている ERC20 トークンと交換することができます。

 $^{^{*1}}$ JPYC Incentive Program

 $^{^{*2}}$ Decentralized Exchange

 $^{^{*3}}$ 各フェーズは DEX の JPYC 総額により自動的に移行します。移行した際には別途アナウンスいたします。

 $^{^{*4}}$ https://jpyc.jp/jip.pdf

3.3 ユースケース 3「非中央集権分散型取引所の利用」

JPYC の利用者は、ご自身の権限と責任において、自己運用として非中央集権分散型取引所である Uniswap において流動性を供給することができます。

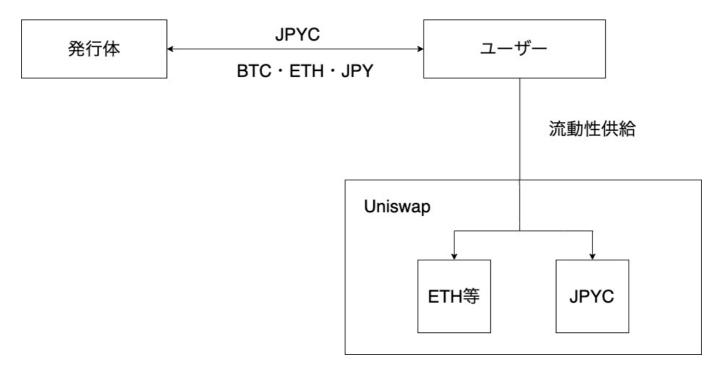


図3 発行体からの JPYC 取得、及び流動性提供のイメージ図

JPYC が流動性供給されると、発行体の承認が無くとも、Uniswap 上において取引可能な全ての ERC20 トークン及び ETH と交換(Swap)できるようになります。流動性供給者は Uniswap 上で JPYC が Swap に利用されればされるほど、より多くの流動性供給報酬を JPYC、ETH またはその他の ERC20 トークンとして得ていただくことが可能です。

3.4 ユースケース 4「非中央集権分散型貸出プラットフォームの利用」

JPYC は ERC20トークンですので技術的には全ての ERC20トークンを扱う DeFi を利用することができます。例えば、ご自身の権限と責任において自己運用として非中央集権分散型貸出プラットフォームの Compound など を通じて JPYC を貸し出すような利用方法が考えられます。現時点では JPYC は Compound での取り扱いはありませんが、Compound コミュニティにより JPYC の取り扱いが承認されると、JPYC を貸し出して金利収入を 得たり、金利を支払うことで JPYC を借り受けるといった利用が可能となります。Compound コミュニティの承認内容次第ですが、これらの貸借により Compound に貢献した報酬として、Compound のガバナンストークンである COMP を得られる場合もございます。

3.5 ユースケース 5 「DeFi ユーザーの裁定取引」

JPYC は ERC20 トークンですので技術的には全ての ERC20 トークンを扱う DeFi を利用することができます。 DeFi は、成長途中の市場のため、同一の価値を持つ商品の一時的な価格差が生じやすい傾向にあります。その際に、ご自身の権限と責任において、自己運用として、割高なほうを売り、割安なほうを買い、その後、両者の価格差が縮小した時点でそれぞれの反対売買を行うことで利益を獲得する裁定取引における利用方法が考えられます。

3.6 ユースケース 6「クリプトアーティストなどの物品購入」

JPYC は技術的には全ての ERC20 トークンと同様に利用することができます。NFT(Non Fungible Token)を発行し、販売を行うことで暗号資産を手に入れているアーティストは、手に入れた暗号資産を Uniswap などで JPYC に替えることで物品購入が可能です。

4 JPYC のガバナンス

JPYC の発行及び流通に関する重要事項は、発行体の役員、正社員及びアドバイザーボードの専門家らの協議に基づいて決定されます。アドバイザーボードには、弁護士・ベンチャーキャピタリスト・国際税理士・上場企業元 CFO・ブロックチェーン企業経営者・コンサルタント等が就任しており、専門的な知見をチーム全体に共有しています。

5 発行体について

5.1 チーム

- 岡部 CEO
- 原沢 COO
- 小野 エンジニア
- 伊藤 エンジニア

5.2 アドバイザー

- 村口 和孝 ベンチャーキャピタリスト
- 森 和孝 国際弁護士
- 水井 大 弁護士
- 柳澤 賢仁 国際税理士
- 佐々木 義孝 上場企業元 CFO
- 井堂 裕功 公認会計士・税理士

5.3 会社情報

- 設立日:2019年11月
- 本社:東京都港区芝公園 4-8-12 猫来坊 2 階
- 資本金: 2653 万円
- 事業内容:古物営業法に基づく古物商および古物市場の運営/前払式支払手段の発行
- 許認可:
 - 古物市場主許可 東京都公安委員会 第 304372004710 号
 - 古物商許可 東京都公安委員会 第 304372004277 号

6 JPYC の購入方法

6.1 推奨する購入方法

発行体が推奨する購入方法は、現在、以下の3通りです。

- 発行体 Web サイトから日本円で購入
- 発行体 Web サイトから ETH で購入
- 発行体 Web サイトから BTC で購入

発行体の Web サイトを通じて、以上のいずれかの方法で支払いを行うことで、1JPYC=1 円で購入することが可能です。但し、Uniswap において 1JPYC=1 円を大きく上回る、または下回る価格で継続的に取引されている場合には、原因が特定されるまでの間、一時的に販売を休止することがあります。

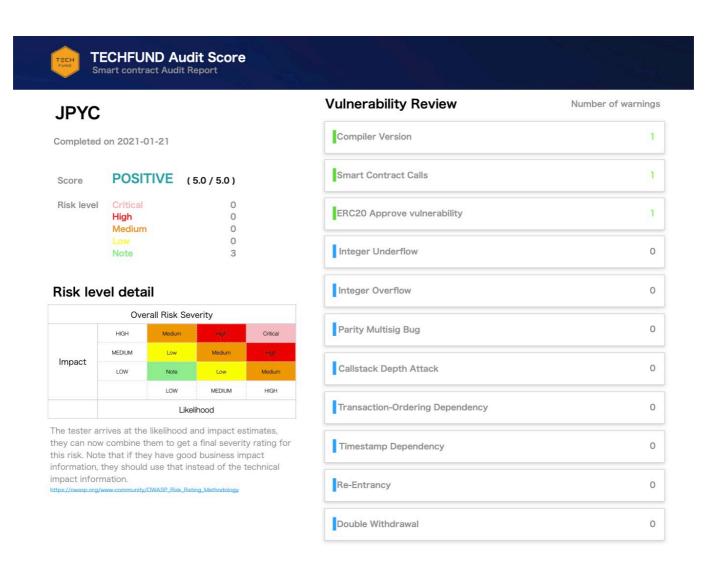
6.2 他の購入方法

非中央集権分散型取引所を通じて他の ERC20 トークンをもって JPYC を購入していただくことは可能です。一例として、Uniswap での購入が可能です。しかし、価格は需給により刻一刻と変わること、さらにこれらの取引所は発行体とは資本関係その他なんらの関係もありませんので、ご利用にあたっては、利用者ご自身の権限と責任において、自己運用として行ってください。

6.3 将来的にありうる購入方法

発行体が将来的に用意する予定の購入方法として、日本暗号資産市場取扱予定通貨をもって、JPYC を購入できるようにする予定です。

7 発行コントラクトの監査結果 TECHFUND





Compiler

It is suggested to use particular version as there might be changes in future versions of a compiler which cannot be checked for now and might lead to breaking changes in deployed smart contract.

Smart Contract

function isContract(address account) internal view returns (bool) {
 // This method relies in extcodesize, which returns 0 for contracts in
 // construction, since the code is only stored at the end of the
 // constructor execution.

uint256 size;
// solhint-disable-next-line no-inline-assembly
assembly { size := extcodesize(account) }
return size > 0;
}

Generally do not use the EXTCODESIZE check to prevent smart contracts from calling a function. This is not foolproof, it can be subverted by a constructor call, due to the fact that while the constructor is running, EXTCODESIZE for that address returns 0.

ERC20 Approve vulnerability

Someone already approved can acquire extra allowance when a token holder changes the allowance for him/her. Here is possible attack scenario:

- 1) Alice allows Bob to transfer N of Alice's tokens (N>0) by calling approve method on Token smart contract passing Bob's address and N as method argumentsAfter some time,
- 2) Alice decides to change from N to M (M>0) the number of Alice's tokens Bob is allowed to transfer, so she calls approve method again, this time passing Bob's address and M as method arguments
- 3) Bob notices Alice's second transaction before it was mined and quickly sends another transaction that calls **transferFrom** method to transfer N Alice's tokens somewhere
- 4) If Bob's transaction will be executed before Alice's transaction, then Bob will successfully transfer N Alice's tokens and will gain an ability to transfer another M tokens

 5) Refers Alice poticed that compating worth wrong Rob calls.
- 5) Before Alice noticed that something went wrong, Bob calls **transferFrom** method again, this time to transfer M Alice's tokens.

So, Alice's attempt to change Bob's allowance from N to M (N>0 and M>0) made it possible for Bob to transfer N+M of Alice's tokens, while Alice never wanted to allow so many of her tokens to be transferred by Bob.

8 免責事項

JPYC を保有しご利用いただくにあたっては、あらかじめ、以下のリスクを正確に認識しご了承いただくようお願いいたします。また、当社は、以下の各リスクに起因して利用者に生じる損害につき、責任を負わないものとします。

8.1 JPYC の財産的価値そのものに関するリスク

JPYC は金融商品取引上の有価証券・金融商品その他いかなる投資商品として発行されたものではなく、資金決済法上の暗号資産でもなく、あくまで自家型前払式支払手段として発行されたものです。そのため、当社所定の使途以外に使用できることが保証されているものではなく利用者相互間の決済には利用できません。

また、JPYC は、ERC20 規格に従って発行されているため、ERC20 規格を受け入れている各種外部サービスにおいて JPYC を処分等することができますが、当社はこれを推奨しまたは保証するものではありません。ご利用いただくにあたっては、JPYC 利用者において、自らの責任と権限のもと、自己運用として外部サービスをご利用いただくようお願いいたします。

8.2 秘密鍵の喪失により JPYC を失うリスク

秘密鍵自体または秘密鍵の組合せは、利用者自らの JPYC の処分等のため必要となり、その秘密鍵の管理は、利用者自らの権限と責任において管理いただくものとします。利用者の JPYC が保管されたウォレットに関連づけられた秘密鍵の喪失は JPYC そのものの喪失と同じです。利用者に対するフィッシング攻撃や、利用端末に対する JPYC はマルウェア攻撃、DoS 攻撃、合意ベースの攻撃その他の様々な形での攻撃により、JPYC 喪失等の被害を受ける可能性があります。

8.3 イーサリアムプロトコルに関連するリスク

JPYC はイーサリアムプロトコルである ERC20 に基づくため、あらゆるイーサリアムプロトコルの誤作動、故障または不具合によって JPYC に対し重大な悪影響を及ぼす場合があり、JPYC が一時的に使用できなくなる可能性があります。また、JPYC を使用するためにはイーサリアムネットワーク上での送金時において送金手数料(GAS代)を要するところ、イーサリアムネットワークの混雑等、当社とは関係のない原因によって送金手数料(GAS代)が高騰する可能性があります。

8.4 マイニング攻撃のリスク

JPYC は、他のパブリックチェーンプロトコルに基づく分散型暗号トークンと同様に、ブロックチェーン上でのトークントランザクションの検証中にマイニングによる攻撃の影響を受ける可能性があります。これらの攻撃を受けた場合には、JPYC に関するトランザクションの記録等に対してリスクをもたらす場合があります。

8.5 法令等の変更及び課税リスク

JPYC に関連する法律、政令、法令、規制、命令、通達、条例、ガイドラインその他の規制もしくは税制の将来の変更がなされる可能性があります。また、利用者は自己の権限と責任において JPYC に関する税務申告の要否その他の課税に関する判断をしなければならないものとします。

8.6 利用者による入力誤りその他の要因によるリスク等

利用者の入力誤りその他のいかなる行為、利用者、第三者の通信・システム機器等の故障、障害もしくは稼働状況、天災地変またはサイバー攻撃その他のいかなる原因により意図しない取引結果となるリスクが存在する可能性があります。

8.7 利用者相互間の関係

当社ウェブサイトに関連して利用者と他の利用者または第三者との間において生じた取引、連絡、紛争等については、利用者の責任において処理および解決するものとし、当社はかかる事項について責任を負いません。

8.8 JPYC の発行ないし流通の停止等によるリスク

JPYC の発行ないし流通の停止、終了、または変更、利用者のメッセージまたは情報の削除または消失、利用者の登録の取消し、本サービスの利用によるデータの消失または機器の故障もしくは損傷、その他の事項に関連して利用者が被った損害につき当社は責任を負いません。

8.9 附則

1. 本ホワイトペーパーは 2021 年 1 月 27 日に作成し公表する。