日本酒コイン

目次

第 I 部
概要

日本酒コインはブロックチェーンを利用した仮想通貨の一つです. 日本酒コインは B to C におけるサービスを目的しており,

第 II 部
アカウント

アカウントには以下の 4 種類が存在する.

1. 個人アカウント
2. 企業アカウント
3. 事業者アカウント
4. 管理アカウント

それぞれのアカウントには情報が紐づけされている.
また、アカウントごとに可能なトランザクションが異なる.

0.1　個人アカウント

個人アカウントには以下の情報が紐づけられる.

- 残高
- 生成したブロック数
- 有効期限内の自身に付けたタグ
- 企業アカウントから受け取ったメッセージ
- 最初に参照されたトランザクションが含まれるブロック高
- 最後のブロックから 20160 ブロック以内に BtoC 送金を送った総額

個人アカウントはトランザクションに以下のように関係する.

- 他のアカウントへの、他アカウントからの**通常送金**
- 企業アカウント、事業者アカウントへの **BtoC 送金**
- 自分自身のアカウントへの**タグ付け**
- 企業アカウント送信された**メッセージ**の受け取り

0.2　企業アカウント

企業アカウントには以下の情報が紐づけられる.

- 残高
- 生成したブロック数
- 最初に参照されたトランザクションが含まれるブロック高
- 個人アカウントに送信したメッセージ
- 最後のブロックから 10080 ブロック以内に自分自身及び自身が作成した事業者ア

カウントが BtoC 送金をもらった総額
- 自身が作成した事業者アカウント

企業アカウントはトランザクションに以下のように関係する.

- 他のアカウントへの、他のアカウントからの**通常送金**
- 個人アカウントからの **BtoC 送金**の受け取り
- 自分自身のアカウントへの**タグ付け**
- 個人アカウントへの**メッセージ**の送信
- 自身が企業アカウントとして作成される**アカウント作成**

0.3 事業者アカウント

事業者アカウントには以下の情報が紐づけられる.

- 残高
- 生成したブロック数
- 最初に参照されたトランザクションが含まれるブロック高
- 最後のブロックから 10080 ブロックいないに受け取った BtoC 送金の総額
- 自身のが作成されるトランザクションを作成した企業アカウント

事業者アカウントはトランザクションに以下のように関係する.

- 他のアカウントへの、他のアカウントからの**通常送金**
- 個人アカウントからの **BtoC 送金**の受け取り
- 自身が事業者アカウントとして作成される**アカウント作成**

0.4 管理アカウント

管理アカウントには以下の情報が紐づけられる.

- 残高
- 最初に参照されたトランザクションが含まれるブロック高
- 自身が作成した企業アカウント

管理アカウントはトランザクションに以下のように関係する.

- 他のアカウントへの、他のアカウントからの**通常送金**
- **タグ付け**のための新しいタグの作成
- 企業アカウントを作成するための**アカウント作成**

第 III 部
トランザクション

トランザクションには以下の 4 種類が存在する.

1. 通常送金
2. BtoC 送金
3. タグ付け
4. メッセージ
5. アカウント作成

0.5　通常送金

通常送金は他のアカウントに送金するために使われる.

0.6　BtoC 送金

BtoC 送金は以下の条件に従って利用される.

- 個人アカウントは企業アカウント、事業者アカウントにしか、企業アカウントは個人アカウントにしか BtoC 送金を送ることができない
- 企業アカウントがトランザクションに短文の記載が可能
- トランザクションには差出人と受取人の二人の署名が必要

0.7　タグ付け

タグ付けは以下の条件に従って利用される

- 新しいタグの作成は企業アカウントのみが作成できる
- 個人アカウントは既に作成されたタグを自身に付けることができる
- 個人アカウントにつけられたタグは 20160 ブロックの間効力を持つ

0.8　メッセージ

企業アカウントが自身の生産している商品などの情報を以下の条件に一致する個人アカウント全てに自社の URL や PR などを短文で送信することができる.

- 送信されたメッセージにつけられたタグと同一のタグをつけている
- 通常送金、BtoC 送金、タグ付けのトランザクションで最後のブロックから 40320 以内のブロックに含まれる
- 同一の企業アカウントからのメッセージを最後のブロックから 1440 以内のブロックで受け取っていない

0.9　アカウント作成

管理アカウントが地元の会社を企業アカウントにしたい場合に使われる.

第 IV 部
ブロックとブロックチェーン

0.10　ブロックの情報

ブロックチェーンの各ブロックが以下の情報からなる.

- ブロックのバージョン
- ブロックのタイムスタンプ
- ブロック作成者の公開鍵
- ブロックに対する署名
- ひとつ前のブロックのハッシュ値
- このブロックのハッシュ値
- ブロック高
- トランザクションのリスト

0.11　ブロックの作成

ブロックの作成では新しいブロックのブロック数が 60 以下ならば、個人アカウントと企業アカウントの双方がブロックを作成でき、ブロック数が 60 より大きい場合、新規に作成するブロックのブロック数が奇数なら個人アカウントが、偶数なら企業アカウントが作成する.
偶数番目のブロック作成時企業アカウントが存在しない場合個人アカウントがブロックを作成することができる

0.12　タイムスタンプ

タイムスタンプは UNIX 時間を使う.

0.13　ブロック作成難易度

ブロックが 60 個以下ならば作成難易度は一定である.
ブロックが 60 個より多いならば以下のようにして作成難易度が求められる.
奇数番目のブロックと偶数番目のブロックの作成難易度は異なる.
難易度の調整には以下の変数が使われる.

- $d_n \equiv n$ 番目のブロックの作成難易度
- $t_n \equiv n-1$ 番目のブロックと n 番目のブロックのタイムスタンプの時間差

奇数番目のブロックの作成難易度は新しいブロックのブロック高を $2n+1$ とすると以下のように求められる.

- $d = \sum_{i=n-30}^{n-1} d_{2i+1}$　合計作成難易度
- $t = \sum_{i=n-30}^{n-1} t_{2i+1}$　合計経過時間
- $d_{2n+1} = \frac{60d}{t}$　新しいブロックの作成難易度

偶数番目のブロックの作成難易度は新しいブロックのブロック高を $2n$ とすると以下のように求められる.

- $d = \sum_{i=n-30}^{n-1} d_{2i}$　合計作成難易度
- $t = \sum_{i=n-30}^{n-1} t_{2i}$　合計経過時間
- $d_{2n} = \frac{60d}{t}$　新しいブロックの作成難易度

0.14　ブロックの分岐

ブロックの分岐時には分岐から先に 60 ブロック目を作成したチェーンを採用する.

0.15　Part of Token Economy

日本酒コインは Part of Token Economy というコンセンサスアルゴリズムを使う.
PoA は以下のような変数と数式を満たすことによってブロックの生成ができる.

- $b \equiv$ 残高
- $a \equiv$ アカウントのアドレス
- $p \equiv$ 前ブロックのハッシュ値
- $m \equiv$ マークルルート
- $d \equiv$ ブロック作成難易度
- $tt \equiv$ アカウントごとの一定期間内の BtoC 送金の総額
- $ts \equiv$ タイムスタンプ

$\frac{b}{d} \times (-\frac{250000}{tt+500} + 501) \geq sha256(a + p + m + ts)$