Bech32

@DG Lab Nakagawa

Agenda

- Bech32
- Segwit address format（Bech32）
- Demo

Bech32

Bech32

新しい汎用的なアドレスフォーマット

- 「BIP 173」で定められている

Bech32

- 今までのアドレスフォーマット
  - Base58Check
    - QRコードに多くの領域が必要
    - モバイルキーボードで入力するのが大変
    - HASH256（2回のSHA256）は遅い
    - HASH256のチェックサムはエラー検出の保証がない

Bech32

- Bech32では
  - 大文字小文字を区別しない、簡単に読み書きが可能
  - 単純な変換（bignumを使わない）
  - Base58にくらべて、15%?17%?しか大きくならない
  - より良いチェックサム
  - コンパクトなQR

Bech32

- データ構造
  - human-readable part
    人が読める部分
  - separator
    「1」固定
  - data part
    データ＋チェックサム

Bech32

- human-readable part
  人が読める部分
  ASCIIコードの33-126が利用可能

```
! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A
B C D E F G H I J K L M N O P Q R S T U V W X Y Z [ \ ]
^ _ ` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
```

Bech32

・data part

	0	1	2	3	4	5	6	7
+0	q	p	z	r	y	9	x	8
+8	g	f	2	t	v	d	w	0
+16	s	3	j	n	5	4	k	h
+24	c	e	6	m	u	a	7	l

Base32
アルファベットと数字から、
「1」(いち)「b」(びー)「i」(あい)「o」(おー)
を除いた文字列を仕様
※:通常のBase32の文字列とは異なります

Bech32

・data part

チェックサム

・BCH符号

・最後の6文字（32bit×6=192bit）

Segwit address format（Bech32）

Segwit address format（Bech32）

・human-readable part
　メインネット「bc」、テストネット「tb」
・data part
　最初の値は、「witness version」（基本「0」）
　その後の値は、
　・P2WPKHでは、「PublicKey」のHASH160
　・P2WSHでは、「witnessScript」のSHA256

Segwit address format（Bech32）

- Segwit Address（例）

  bc1qw508d6qejxtdg4y5r3zarvary0c5xw7kv8f3t4

  * Human-readable part (any character)
  * Separator "1"
  * Data part (Base 32 character set encoded):
    * Witness version
    * Witness program
    * Checksum

Demo

Demo

・Segwit Address

https://bc-2.jp/tools/bech32demo/index.html

・Exsampleにある、PublicKeyからP2WPKH、P2WSH
のアドレスを作成してみよう作成できましたか？

・ヒント

・P2WPKHの「witness program」は、PublicKeyのHASH160

・P2WSHの「witness program」は、witnessScriptのSHA256

Demo

・Segwit Address Check
https://bc-2.jp/tools/bech32demo/index.html

・先程作成した、Segwit Addressをチェックしてみよう
・エラー検知
・二文字まで、「a」に置き換えてみよう

Demo

- QR Code
  https://bc-2.jp/tools/bech32demo/index.html

  - 「a」（小文字）を15文字いれてみよう
    「alphanumeric」「byte」でQRコードの大きさは？
  - スマートフォンなどでQRコードを読み取ってみよう
    「alphanumeric」は？

まとめ

- 汎用的なアドレスフォーマット
- 大文字小文字を区別しない
- QRコードがコンパクトに
- エラー検出が可能

参考資料

- BIP 173
  https://github.com/bitcoin/bips/blob/master/bip-0173.mediawiki
- Bech32: a base32 address format
  https://prezi.com/gwnjkqjqjjbz/bech32-a-base32-address-format/
- Pieter Wuille: New Address Type for SegWit Addresses
  https://www.youtube.com/watch?v=NqiN9VFE4CU

takatoshi@dglab.com