Create a P2PKH Brainwallet

This is a TERRIBLE idea!

First, hash a memorable string

In[174]:=

```
h = Hash["Hackfest 2023 Village Bitcoin", "SHA256"]
```

Out[174]=

```
69 546 454 228 202 271 489 193 945 445 697 119 936 932 839 335 510 282 048 680 182 503 051 133 \
  087 773
```

Next create an integer private key based on the hash

In[175]:=

```
pk = PrivateKey[
   <|
    "Type" → "EllipticCurve",
    "CurveName" → "secp256k1",
    "PrivateMultiplier" → h
    |>
  ]
```

Out[175]=

```
PrivateKey[ ⊞  Type: Elliptic curve   (secp256k1 )
               Private key size:   256 b
               Public key size:   512 b ]
```

Create a Wallet Import Format (WIF) code

See https://en.bitcoinwiki.org/wiki/Wallet_import_format

In[176]:=

```
wif = BlockchainKeyEncode[
  pk,
  "WIF",
  BlockchainBase → "Bitcoin"
 ]
```

Out[176]=

```
5Jz17EauP7bzgngMkZkvxsr49zXESUgdeYNMe2Spq9ebkTxEurC
```

Let’s create a QR code for our WIF

In[177]:=

```
BarcodeImage[wif, "QR"]
```

Out[177]=