

Create a P2PKH Brainwallet



This is a TERRIBLE idea!

First, hash a memorable string

```
memorable = "Hackfest 2023 Village Bitcoin";  
h = Hash[memorable, "SHA256"]  
(*h = Nest[  
  Hash[#, "SHA256"] &  
    , memorable  
    , 100  
  ]*)
```

Out[249]=

```
69 546 454 228 202 271 489 193 945 445 697 119 936 932 839 335 510 282 048 680 182 503 051 133 5  
087 773
```

Out[250]=


```
86 881 367 315 791 155 155 031 903 649 539 957 183 234 639 397 751 225 950 039 008 399 443 862 5  
524 989
```

Next create an integer private key based on the hash

In[251]:=

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

Out[251]=

```
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[252]:=

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

Out[252]=

```
5KGt52j0LVh4Ua6znvASybhEH6ztLY7oAm1HBe2yavjUJSLCLgQ
```

Let's create a QR code for our WIF

In[253]:=

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

Out[253]=

