### Locks funds using Pay-to-Public-Key-Hash (P2PKH) script

#### 1. Kết Quả

Khóa quỹ thành công sử dụng script Pay-to-Public-Key-Hash (P2PKH).

#### 2. Cách Thức Hoạt Động Chi Tiết

**Bước 1: Tạo Địa Chỉ Bitcoin Testnet**

1. Tạo địa chỉ Bitcoin testnet để nhận và chi tiêu coin.
2. Sử dụng một chuỗi bí mật 32 byte cố định để đảm bảo tạo ra cùng một địa chỉ mỗi lúc.

Ví dụ chuỗi bí mật là ‘**feed nephew grain suggest law faint female coin emerge neck traffic midnight easily female atom**’ tạo ra địa chỉ như sau:

Private Key: cTX1aa9CenXgkfqgsj4W8o4oE5prbWaobBAp4UP1PfSLKR5DpHwM

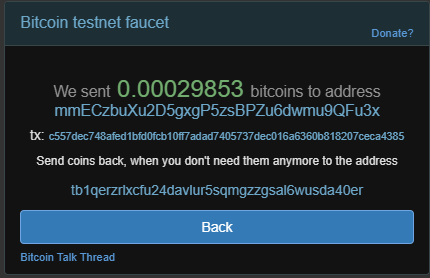
Public Key: 037ee565181e737c3bbcb6131e2c122818187ebe50018c396f035b6a77a0b15d68

Bitcoin Address: **mmECzbuXu2D5gxgP5zsBPZu6dwmu9QFu3x**

**Bước 2: Yêu Cầu Nhận Coin Cho Địa Chỉ Vừa Tạo**

1. Truy cập một faucet Bitcoin testnet, như [Bitcoin Faucet](https://coinfaucet.eu/en/btc-testnet/), để yêu cầu nhận coin testnet cho địa chỉ vừa tạo.
2. Chờ giao dịch được xác nhận. Thời gian có thể kéo dài vài giờ, tùy vào mức độ bận rộn và tương tác của mạng

Kết quả như sau:



**Bước 3: Chi Tiêu UTXO** (Unspend Transaction Ouput)

Thực hiện các bước sau để chi tiêu UTXO

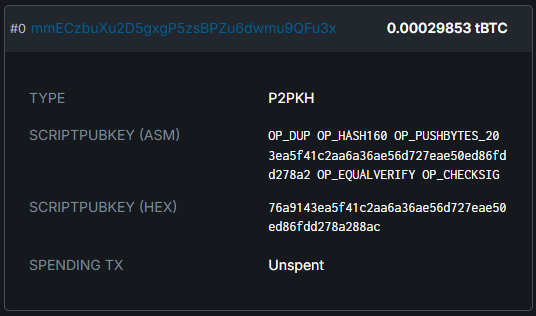
**Tạo đầu vào giao dịch (Transaction Input )**

1. Xác định mã giao dịch (txid) và chỉ số đầu ra (output index) của UTXO muốn chi tiêu.

##### Mã giao dịch là: [c557dec748afed1bfd0fcb10ff7adad7405737dec016a6360b818207ceca4385](https://blockstream.info/testnet/tx/c557dec748afed1bfd0fcb10ff7adad7405737dec016a6360b818207ceca4385)

Chỉ số đầu ra là: 0 (xem hình bên dưới)

Chứa một ouput được khóa (lock) cho địa chỉ của bạn như sau:



Vậy sau khi giao dịch nhận coin này được xác nhận (confirmed) bạn có thể chi tiêu output này, tới 0.00029853 BTC hay **29853 satoshis**

1. **Tạo đầu vào giao dịch (Transaction Input)**

Một đầu vào giao địch được tạo từ txid và output index. Lưu ý cần cung cấp scriptSig P2PKH hợp lệ (chứa khoá công khai và chữ ký trên giao dịch đang xây dựng) để chi tiêu UTXO (được thực hiện ở bước **Ký giao dịch**)

**Xác Định Số Lượng Cần Chi Tiêu**

* Chỉ định lượng Bitcoin testnet muốn chi tiêu tính bằng satoshi (1 Bitcoin = 100.000.000 satoshi).
* Đảm bảo lượng tiền lớn hơn ngưỡng "dust" (khoảng 540 satoshi) và nhỏ hơn lượng coin sẵn có của UTXO muốn chi tiêu. Cũng cần phải tính toán phí giao dịch (fee):
  + Phí (fee) là phần còn lại của UTXO sau khi trừ số tiền chi tiêu và số tiền trả lại (change) cho địa chỉ của bạn.
  + Phí cao sẽ được ưu tiên xử lý trong mạng lưới Bitcoin.

Cụ thể, chúng ta sẽ gửi đi 10000 satoshis với chi phí fee là 5000 satoshis và gửi lại 14853 satoshis

1. **Tạo Đầu Ra Giao Dịch (Transaction Output)**

Giao dịch thông thường có hai đầu ra (outputs):

* Gửi coin cho người nhận dự kiến.
* Trả lại phần còn lại (change) cho địa chỉ người gửi.

Cần cung cấp scriptPubKey để khóa các outputs. Cụ thể đối với script P2PKH, cấu trúc như sau:

[**OP\_DUP, OP\_HASH160**, **<Hash160 của địa chỉ nén của người nhận>**, **OP\_EQUALVERIFY, OP\_CHECKSIG**]

Lúc này, giao dịch mới đã được tạo với một đầu vào input và hai đầu ra outputs (người nhận và change).

1. **Tạo Và Ký Giao Dịch**

Ký giao dịch bằng **khoá bí mật của bạn** để chứng minh quyền sở hữu (các) đầu vào.

Mặc định, Cờ SIGHASH\_ALL được sử dụng, nghĩa là chữ ký được ký trên tất cả đầu vào và đầu ra, đảm bảo giao dịch không bị thay đổi sau khi ký.

1. **Phát Giao Dịch (Broadcast)**

Sử dụng API của Blockstream.info (một dịch vụ RPC Bitcoin Testnet công khai) để phát giao dịch lên mạng lưới Bitcoin testnet.

Chờ giao dịch được xác nhận và ghi vào blockchain.

Giao dịch đã được phát đi thành công, có mã định danh là:

#### [97d20ad02b735444712ffd9d0cca170a7a2d95e5358aed3b2c6ade71fc7d9d8a](https://blockstream.info/testnet/tx/97d20ad02b735444712ffd9d0cca170a7a2d95e5358aed3b2c6ade71fc7d9d8a)

#### 3. Tài Liệu Tham Khảo

* [Tài liệu python-bitcoinlib](https://python-bitcoinlib.readthedocs.io/en/latest/)
* [Hiểu Cách Hoạt Động Hệ Thống Bitcoin](https://learnmeabitcoin.com/technical/)