ĐẠI HỌC BÁCH KHOA TPHCM
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

Assignment 2

Mathematical models for UTXOs selection

GVHD: Huỳnh Tường Nguyên
Môn: Mô hình hóa toán học
Trình bày: Nhóm 5

Danh sách thành viên

Đỗ Đăng Khôi	1711807
Lê Văn Nam	1712237
Phạm Văn Anh Dũng	1710879
Dương Văn Hiếu	1711272
Hồ Công Sơn	1712964

Mã nguồn – Slide – Báo cáo

https://tinyurl.com/y4h7yffe

1.Mô hình 1: Giảm thiểu phí giao dịch

Biến quyết định : $x_i = \begin{cases} 1, & \text{nếu UTXO } u_i \text{ được chọn} \\ 0, & \text{ngược lại} \end{cases}$

Biến trung gian :

- z_v : giá trị của thay đổi đầu ra (giá trị tiền thối)
- z_s : kích thước của thay đổi đầu ra (kích thước tiền thối)

$$z_s = \begin{cases} 0, & 0 \leq z_v \leq \varepsilon \\ \beta, & z_v > \varepsilon \end{cases}$$

1.Mô hình 1: Giảm thiểu phí giao dịch

Các ràng buộc:

- Kích thước giao dịch không được vượt quá kích thước khối dữ liệu tối đa

$$y = \sum_{i|u_i \in U} s_i^u * x_i + \sum_{j|o_j \in O} s_j^o + z_s \leq M$$

- Một giao dịch phải có đủ giá trị để tiêu thụ

$$\sum_{i|u_i \in U} v_i^u * x_i = \sum_{j|o_j \in O} v_j^o + \alpha * y + z_v$$

1.Mô hình 1: Giảm thiểu phí giao dịch

Các ràng buộc:

- Mối quan hệ giữa giá trị đầu ra thay đổi z_v và kích thước z_s của nó như sau

$$z_S = \sigma \times \beta$$
$$z_V \geq \varepsilon + 0.001 - M(1-\sigma)$$
$$z_S \leq \varepsilon + M\sigma$$

- Sigma là biến nhị phân.

1.Mô hình 1: Giảm thiểu phí giao dịch

Các ràng buộc:

- Tất cả các đầu ra giao dịch phải cao hơn ngưỡng DUST để chắc chắn rằng giao dịch này được chuyển tiếp đến mạng và được xác nhận.

$$\forall v \in V^o, v \geq T$$

1.Mô hình 1: Giảm thiểu phí giao dịch

Hàm mục tiêu:

$$\mathrm{m}i\mathrm{n}i\mathrm{m}i\mathrm{z}e \;\; y$$

2.Mô hình 2: Giảm kích thước UTXOs ban đầu

Các biến: Tương tự trong **Mô hình 1**

Các ràng buộc: Bao gồm tất cả các ràng buộc trong **Mô hình 1** và thêm 1 ràng buộc

$$y \leq (1+\gamma) * Y$$

- Y : là min của kích thước giao dịch thu được từ **Mô hình 1**.

- γ : là hệ số ($0 \leq \gamma \leq 1$).Nếu γ tiến đến 0, chúng ta muốn giữ lại kích thước giao dịch nhỏ nhất thu được từ kết quả của **Mô hình 1**. Mặc khác, một giao dịch có kích thước phù hợp khi nó được tạo ra bởi một số lượng UTXO càng lớn càng tốt.

2.Mô hình 2: Giảm kích thước UTXOs ban đầu

Hàm mục tiêu

$$maximize \ \left(\sum_{i|u_i \in U} x_i - z_s/\beta \right)$$

Hiện thực mô hình: Ngôn ngữ Python và thư viện PuLP

Lý do sử dụng ngôn ngữ python và PuLP :

- Python là ngôn ngữ mạnh mẽ, linh hoạt, phổ biến. Thuận tiện để đọc file, vẽ đồ thị, tính toán.
- PuLP là công cụ mã nguồn mở, có cộng đồng sử dụng lớn. Dễ dàng để tìm hiểu và sử dụng.
- PuLP có thể gọi nhiều trình giải như CPLEX, GUROBI, GLPK, COIN CLP/CBC.

Đánh giá mô hình

Dữ liệu đầu vào*:*

123 file có kích thước < 100Kb của tập dữ liệu được cho.

Ví dụ: file 5ad4a25d4c372215dd13d685.txt

```
// parameters
// n \t m \t outValue \t M \t alpha \t T \t epsilon \t beta \t txsize \t iosize \t cout \t coutValue
3       1       2004420 1048576 8.1055900621118 4426    4426    34      1932    478     0       0

// vin
// id \t size \t value \t confirm \t vout \t choosen \t txid
1       148     512547  3249    24      1       08de1bea48d97596ccc20b738f4ab4f5124714533c0e8b4c6c64e
2       148     1106779 16367   45      1       93499781bcaadda684a4cfb82a1dc77de11a66e3bafd6f4e9c3f1
3       148     400754  16367   3       1       a5291ed636c90291e135a15186d6a869579f6615a44fb534407b2

// vout
// id \t size \t value
1       34      2004420
```

Đánh giá mô hình

Dữ liệu đầu ra:

Test file(.txt) được tạo ra bởi python script, lưu ở thư mục output :

+ Bao gồm các output của mô hình LVF và HVF, mô hình 1, mô hình 2 với gamma là 0,1 - 0,2 - 0,3 - 0,4 - 0,5 - 1

+ Ngoài ra còn có 1 file excel(.xlsx) chứa dữ liệu đầu ra của tất cả các mô hình, dùng để so sánh, vẽ đồ thị.

```
//fileName //status   //y //zs   //zv   //totalSelectedUTXO
5ad448a959678302d59e6f75.txt Optimal  216 34    66581864 1
5ad44bfdce94cf05c955f862.txt Optimal  364 34       1366 2
5ad44e0ece94cf05c955f864.txt Optimal  250 34    39454264 1
5ad44e1bce94cf05c955f865.txt Optimal  364 34       1365 2
5ad4503ece94cf05c955f868.txt Optimal  364 34    1037718 2
5ad4517cce94cf05c955f86a.txt Optimal  250 34   695247540 1
5ad4519cce94cf05c955f86b.txt Optimal  364 34      13393 2
5ad45307ce94cf05c955f86c.txt Optimal  364 34       1363 2
5ad45353ce94cf05c955f86d.txt Optimal  546 34      38497 3
5ad4537ece94cf05c955f86e.txt Optimal  398 34        545 2
```

Đánh giá mô hình

Các file cài đặt mô hình:

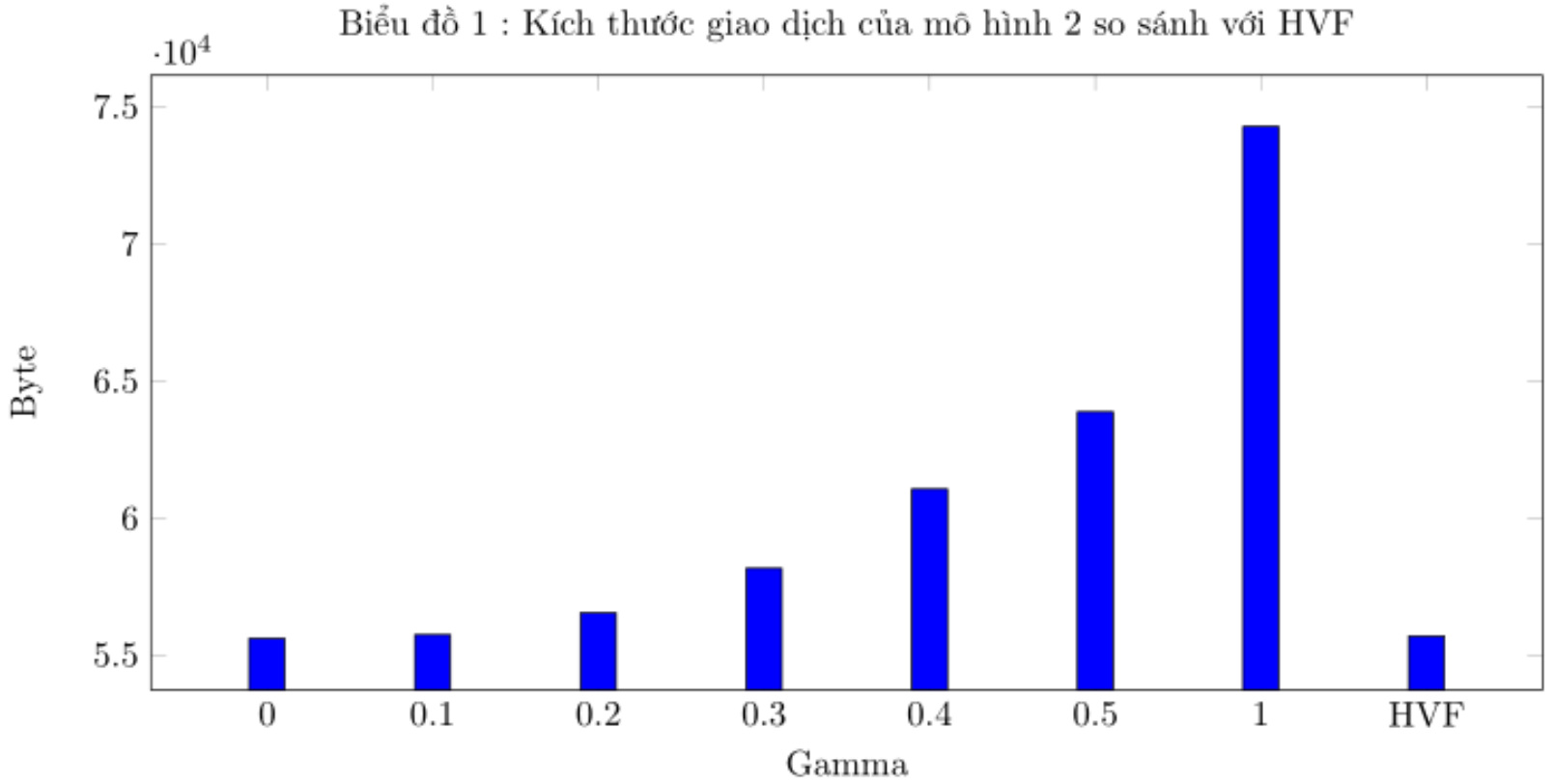
- Model1.py: File hiện thực mô hình 1
- Model2.py: File hiện thực mô hình 2
- LVF.py: File hiện thực giải thuật LVF
- HVF.py: File hiện thực giải thuật HVF

Đánh giá mô hình

4 Bước cài đặt mô hình:

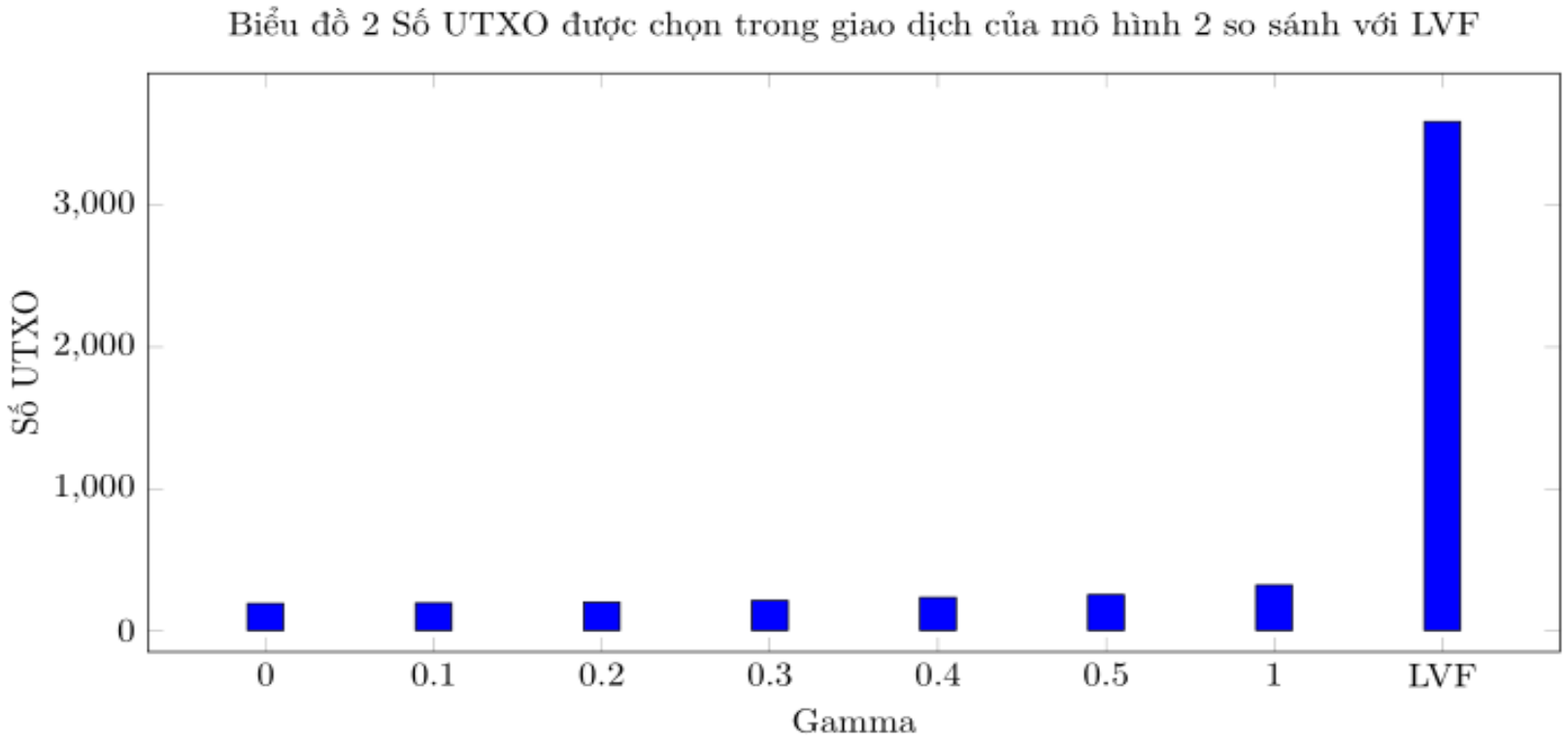
- Bước 1: Đọc file input để lấy tham số đầu vào
- Bước 2: Khai báo mô hình và các biến
- Bước 3: Khai báo các ràng buộc và hàm mục tiêu
- Bước 4: Chọn trình giải và in ra kết quả

So sánh các mô hình:



Gamma	LVF	HVF	0	0.1	0.2	0.3	0.4	0.5	1
Kích thước giao dịch	560268	55692	55600	55600	55735	56534	58162	61054	74276
Số UTXO được chọn	3593	182	189	192	199	210	232	251	319

So sánh các mô hình:



Gamma	LVF	HVF	0	0.1	0.2	0.3	0.4	0.5	1
Kích thước giao dịch	560268	55692	55600	55600	55735	56534	58162	61054	74276
Số UTXO được chọn	3593	182	189	192	199	210	232	251	319

Kết luận

Mô hình đầu tiên giảm thiểu kích thước giao dịch để nó có thể tạo ra một khoản phí nhỏ cho nhiệm vụ khai thác chịu trách nhiệm xác nhận giao dịch này trên mạng.

Cái thứ hai được chế tạo để kiềm chế sự bùng nổ của nhóm UTXO bằng cách chọn càng nhiều càng tốt số lượng UTXO trong khi duy trì kích thước giao dịch để giúp người dùng trả chi phí phải chăng và phù hợp