Deep-Learning Based

Case Investigation Report

Case ID: MT 20240230 XXXXX

Client: Frank C

Inspector: Ling CHENG

January 23, 2024

1 Basic Information

Attribute	Value
Hash	bc1q9svj9wp68zftgejjgk6f96ukuyx8c5urkqsv69
Type	witness-pubkeyhash
Birth Height	575013
Birth TX	e8b406091959700dbffc**********5fe23c5a554ab05ea
Birth Time	2019-05-07 17:17:18
Balance	0
Latest Height	575142
Latest Time	2019-05-08 14:52:26
Times As Output	2
Times As Input	1
In/Out Ratio	0.5
Total Spend Amt	19399903803
Max Spend Amt	19399900000
Min Spend Amt	3803
Mean Spend Amt	9699951901.5
Std Spend Amt	9699948098.5
Total Receive Amt	19399903803
Max Receive Amt	19399900000
Min Receive Amt	3803
Mean Receive Amt	9699951901.5
Std Receive Amt	9699948098.5
Sibling Number	12

Table 1: Details of the Bitcoin Address

Table 1 provides a comprehensive overview of a Bitcoin address. This address is of the type witness-pubkeyhash and was first active in block 575013 on May 7, 2019. It had a brief active period, with the latest activity recorded on May 8, 2019. The balance of the address is 0, indicating that all funds have been transferred out. It has been used more as an output (2 times) compared to its use as an input (1 time), giving an In/Out Ratio of 0.5. The address has handled a significant total amount of 19,399,903,803 units, both in terms of spending and receiving. The maximum transaction amounts for both spending and receiving are notably high, at 19,399,900,000 units, indicating involvement in large transactions. The standard deviations for both spend and receive amounts are very high, suggesting major differences in the sizes of transactions it has been involved in. The address has been associated with 12 sibling accounts, indicating a network of related addresses. The repeated appearance of certain addresses in the sibling account list points to frequent interactions with these accounts. The short active period and the large transaction amounts could suggest that this address was used for specific, high-value transactions and then discontinued. This pattern might be typical for certain types of activities, such as large one-time transfers or transactions related to specific events or purposes. The sibling address list is as follow:

Index	Sibling Address Hash String
1	bc1qywpjgfzgakcqsvqa0slax9pd2mpweptujysf46
2	bc1q3ldtrr6xtpx8jam5gw68aaexz2wtluj0qullvr
3	bc1qfdfgtnlfl2zsnc3hl2h3fk3c9k4h4adtq0s7nc
4	bc1qvstwzsrfml43jrclsp68220l4lx5lw3kwf7dp0
5	bc1qywpjgfzgakcqsvqa0slax9pd2mpweptujysf46
6	bc1q9svj9wp68zftgejjgk6f96ukuyx8c5urkqsv69
7	bc1qywpjgfzgakcqsvqa0slax9pd2mpweptujysf46
8	bc1q3ldtrr6xtpx8jam5gw68aaexz2wtluj0qullvr
9	bc1qvstwzsrfml43jrclsp68220l4lx5lw3kwf7dp0
10	bc1q9svj9wp68zftgejjgk6f96ukuyx8c5urkqsv69
11	bc1qfdfgtnlfl2zsnc3hl2h3fk3c9k4h4adtq0s7nc
12	bc1q4rxsql29tkqn2v2s8vpjltww72kuyajkc05p9u

Table 2: Sibling address list

2 Asset Transfer Path Analysis

This report presents a comprehensive analysis of the Long-Term (LT) and Short-Term (ST) asset transfer paths associated with a specific Bitcoin address. The goal is to understand the transaction behavior linked to this address by examining both forward and backward paths. The analysis reveals distinct differences between LT and ST paths. LT paths, both forward and backward, tend to have shorter and less complex transaction chains. In contrast, ST paths exhibit greater complexity and longer lengths, particularly in backward paths. This suggests a more intricate and frequent transaction history in the short term. Notably, the ST backward paths stand out with a significantly higher average and maximum path length, indicating a complex web of transactions in the recent past. The contrast between LT and ST paths suggests different patterns of asset accumulation and distribution over varying time spans, which could be indicative of the address's changing transaction behaviors or strategies. The examination of both LT and ST asset transfer paths provides insights into the transaction behavior of the address. Understanding these patterns can be crucial for identifying regular or potentially suspicious activities within the Bitcoin network, assisting in efforts to monitor and analyze cryptocurrency transactions. The following table summarizes the key attributes of the LT and ST asset transfer paths:

Type	Direct	Total Tx	Max Len	Min Len	Avg Len	Median Len
LT	Forward	1	-	-	-	-
LT	Backward	2	18	18	18.0	18.0
ST	Forward	1	-	-	-	-
ST	Backward	2	18	2	4.34	4.0

Table 3: Summary of LT and ST Asset Transfer Paths

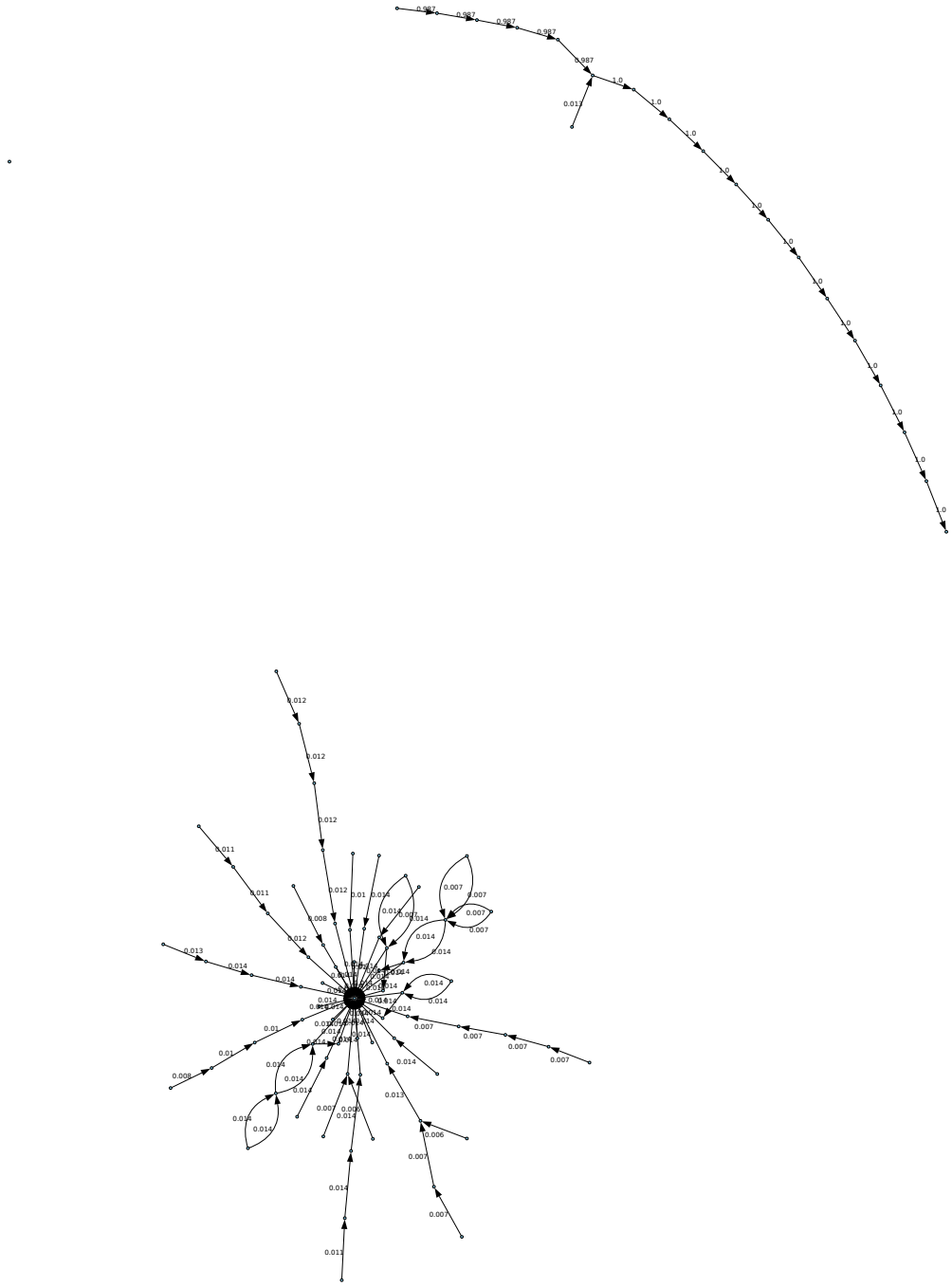

Figure 1: Short-Term (ST) asset transfer paths

3 State Analysis

The state sequence for this address is ”2, 25, 25, 25, 25, 25, 25.” Since state ”25” appears repeatedly and is the only unique state other than ”2,” I’ll first show the path in the decision tree leading to state ”25” and then explain the semantic meaning of states ”2” and ”25.”

3.1 Path in the Decision Tree to State ”25”:

a) `ST_bk_path_hop_len_p_100 <= 0.16`

b) `ST_fr_path_height_len_p_std <= -0.03`

c) `ST_bk_min_input_amt_p_mean <= -0.09`

d) `Act_Ratio <= 0.57`

e) `ST_fr_max_output_num_p_std > -0.80`

Following this path, the address is classified into state ”25” when it meets these criteria.

Figure 2: Decision Tree State

3.2 Semantic Meaning of States:

- **State ”2”**: This state is characterized by addresses that have a relatively moderate or high activity ratio (`Act_Ratio > 0.57`) and are engaged in short-term forward paths (`ST_fr_path_num`) with certain characteristics. This could imply that the address is active over its lifetime with a balanced approach to asset transfers, possibly indicating routine or periodic transactions.
- **State ”25”**: Addresses in this state have a low percentile 100 in short-term backward path hop length (`ST_bk_path_hop_len_p_100 <= 0.16`), indicating short chain lengths in recent transactions. Coupled with the low standard deviation in short-term forward path height length (`ST_fr_path_height_len_p_std <= -0.03`) and low mean percentile in minimum input amount for short-term backward paths as we can see (`ST_bk_min_input_amt_p_mean <= -0.09`). This state might suggest a pattern of small, frequent, and less varied transactions. The fact that the action ratio is relatively low (`Act_Ratio <= 0.57`) and the standard deviation of the maximum output number in short-term forward paths is not very low (`ST_fr_max_output_num_p_std > -0.80`) could imply a somewhat passive but steady transaction behavior.

3.3 Possible Reasons for the Change:

The change from state ”2” to ”25” suggests a shift in transaction patterns. Initially, the address had more balanced and possibly more diverse activities (state ”2”), but later, it

moved to a state characterized by smaller, less varied, and potentially more routine transactions (state "25"). This shift could be due to changes in the behavior or strategy of the entity controlling the address. For instance, the address might have moved from engaging in larger, less frequent transactions to smaller, more regular ones. The reasons could range from strategic decisions based on transaction purposes to responses to market conditions or operational changes.

Without further context, it's challenging to precisely determine why the address's behavior changed, but the decision tree analysis provides valuable insights into the evolving nature of its transactions.

4 Action Analysis

The action sequence for this address is ”24, 2, 2, 2, 2, 2, 2.” As the sequence transitions from action ”24” to ”2,” let’s explore the paths in the decision tree leading to these unique actions and their semantic meanings.

4.1 Path in the Decision Tree to Action ”24”:

a) `ST_bk_path_hop_len_p_100 <= 0.05`

b) `ST_fr_path_height_len_p_std <= 1.49`

c) `ST_bk_min_input_amt_p_mean <= -0.24`

d) `Act_Ratio > 0.89`

e) `LT_bk_path_height_len_p_std <= 0.35`

Figure 3: Decision Tree Action

This path suggests that action ”24” is associated with addresses having a very short maximum hop length in short-term backward paths, a lower standard deviation in short-term forward path height lengths, a lower mean percentile in minimum input amount for short-term backward paths, a very high activity ratio, and a lower standard deviation in long-term backward path height lengths.

4.2 Path in the Decision Tree to Action ”2”:

a) `ST_bk_path_hop_len_p_100 <= 0.05`

b) `ST_fr_path_height_len_p_std <= 1.49`

c) `ST_bk_min_input_amt_p_mean <= -0.24`

d) `Act_Ratio <= 0.89`

e) `ST_fr_max_output_num_p_std > -1.08`

The transition to action ”2” occurs under similar conditions as action ”24,” with the difference being in the activity ratio (now lower) and the standard deviation of the maximum output number in short-term forward paths not being very low.

4.3 Semantic Meaning of Actions:

- **Action "24"**: This action could represent a state of heightened activity and engagement in asset transfers, as indicated by a high activity ratio. The address's transactions are characterized by shorter backward paths and a tendency towards uniformity in transaction amounts and path lengths, suggesting a possible focus on specific types of transactions or consistent behavior over time.

- **Action "2"**: This action might indicate a shift to more routine or less active transaction behavior, as evidenced by the lower activity ratio. While still maintaining similar characteristics in terms of transaction amounts and path lengths, the address may be engaging in less varied or smaller transactions, possibly indicating a more passive or steady state of operation.

4.4 Possible Reasons for the Change:

The transition from action "24" to "2" implies a significant shift in the address's transaction behavior. Initially, the address may have been actively engaged in diverse or significant transactions (action "24"), possibly indicating a period of high intensity or focused transactional activity. The shift to action "2" could suggest a move towards more regular, less varied transactions, possibly indicating a change in strategy, a response to external factors, or a shift in the operational focus of the entity controlling the address.

This change could be driven by various factors, such as a strategic decision to alter transaction patterns, a response to market conditions, operational changes, or even a shift in the underlying purpose of the address. The decision tree analysis provides a nuanced view of these changes, offering insights into the evolving transactional behavior of the address.

5 Behavioral Analysis of Predicted Malicious Activity

To analyze why the two XGB models predicted the given address as malicious (label 1) for both state and action across all hours, let's consider the state and action sequences and their behavioral implications:

5.1 Analysis of State Sequence:

- The state sequence predominantly features state "25," which, based on our earlier analysis, indicates a pattern of small, frequent, and less varied transactions. This kind of behavior can sometimes be associated with malicious activities, particularly when an address consistently engages in transactions that are small enough to potentially evade detection but frequent enough to accumulate significant amounts over time.
- The consistency in this state, without variation, can signal a systematic approach, which is often a characteristic of addresses involved in illicit activities like money laundering or fraud.

5.2 Analysis of Action Sequence:

- The action sequence transitioned from "24" to "2", which we analyzed as a shift from a state of heightened activity and diverse transactions to more routine or less active behavior.
- Malicious addresses might initially engage in varied and significant transactions to build trust or test the waters (action "24") and then shift to more regular, smaller transactions (action "2") as part of their deceptive practices. This transition could be interpreted by the model as indicative of a strategy commonly employed in fraudulent schemes.

5.3 Combined State and Action Behavior Analysis:

- When combining the insights from the state and action sequences, a picture emerges of an address that may initially have been testing its operations or capabilities and then settled into a pattern of behavior that is consistent with certain types of malicious activities.
- The lack of variability in the state and the specific type of actions observed might suggest to the model that this address is engaging in systematic, potentially malicious activities, rather than exhibiting the more varied and less predictable behavior often seen in benign addresses.

5.4 Conclusion:

The XGB models' predictions of the address as malicious for both state and action across all hours likely stem from the combination of consistent, small-scale transaction behavior (state "25") and the transition from a period of testing or diverse activities to a more

steady state of operation (action “24” to “2”). These patterns, particularly when observed consistently over time, can be indicative of strategic behavior associated with malicious activities in the cryptocurrency domain. It’s important to note that while these models provide insights based on patterns, the actual intent can only be definitively determined through a thorough investigation that includes more contextual information.

6 Analysis of Model Predictions and Weights

Based on the provided information, the two XGB models (Status-XGB and Action-XGB) for predicting the label of a given BTC address at various time steps are dynamically weighted by the Intention-Attention module. This approach accounts for the changing contributions of state and action sequences to the final prediction. Let's analyze the observed weights and predictions from the perspective of State and Action Sequence and behavior Analysis.

6.1 Analysis of State and Action Sequence Weights:

a) **Early Hours (0-4)**: Initially, the action sequence has a higher weight compared to the state sequence. This suggests that the model places greater emphasis on the actions of the address, possibly due to the initial action sequence indicating a shift from diverse transaction behavior to more routine transactions. This shift is often a red flag in behavioral analysis, as it may suggest a strategy commonly employed in fraudulent activities.

b) **Middle Hours (16-24)**: We observe a significant fluctuation in weights, where the state sequence weight increases notably, indicating that the state of the address becomes more critical in determining its behavior. This could be due to the state sequence settling into a consistent pattern, which might be indicative of systematic, potentially malicious activities.

c) **Later Hours (25-199)**: As time progresses, there is a trend where the weights stabilize, with the action sequence generally maintaining a higher weight than the state sequence. This stability could indicate that the address's actions over time provide more consistent clues to its potential maliciousness than the state sequence, which might have fewer variations at this stage.

6.2 Behavior Analysis and Predictions:

- The consistent prediction of '1' (malicious) across all time steps by the Intention Monitor, combined with the Intention-Based Survival Analysis, suggests that the address exhibits patterns commonly associated with malicious behavior.
- The survival probability, which remains relatively stable and does not drop significantly, reinforces the consistency of the prediction. This implies that the address's behavior does not deviate significantly from patterns that the model associates with malicious intent.
- The model seems to be effectively filtering out noise and focusing on significant behavioral patterns that persist over time, leading to a consistent malicious prediction.

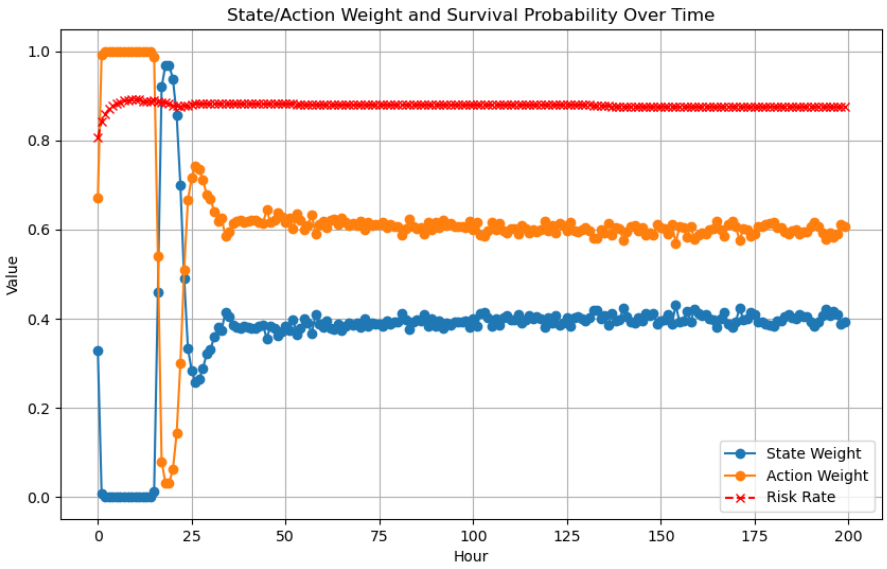

Figure 4: State/Action Weight and Survival Probability Over Time

7 Mixing Transaction Analysis

With a threshold of 80, we found 0/1 possible In/Output mixing transactions. **Output Tx**: e8b406091959700dbffcff30a60b190133721e5c39e89bb5fe23c5a554ab05ea. **Input Tx**: 71 / **Output Tx**: 44. Corresponding value mapping for each suspicious transaction:

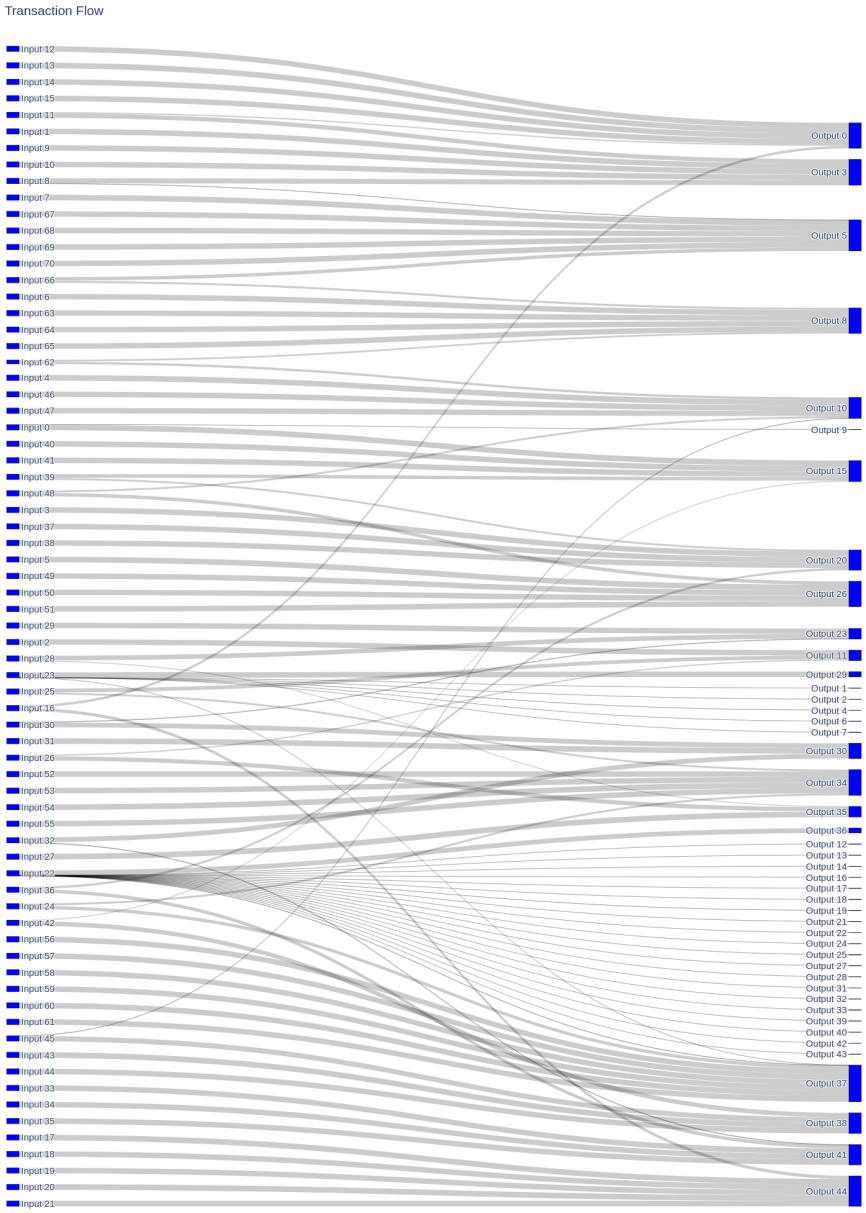

Figure 5: Possible Token Flow Among High Risk Transaction.

Input Index	Output Index	Value
0	9	19950000.0
0	15	9980050000.0
1	3	10000000000.0
2	11	10000000000.0
3	20	10000000000.0
4	10	10000000000.0
5	26	10000000000.0
6	8	10000000000.0
7	5	10000000000.0
8	3	9399200000.0
8	5	600800000.0
9	3	10000000000.0
10	3	10000000000.0
11	0	1999450000.0
11	3	8000550000.0
12	0	10000000000.0
13	0	10000000000.0
14	0	10000000000.0
15	0	10000000000.0
16	44	5599700000.0
16	0	4400300000.0
17	44	10000000000.0
18	44	10000000000.0
19	44	10000000000.0
20	44	10000000000.0
21	44	10000000000.0
22	12	22950000.0
22	13	700984.0
22	14	1915703.0
22	16	225422.0
22	17	1467074.0
22	18	1909324.0
22	19	129968020.0
22	21	150000.0
22	22	2090000.0
22	24	658533.0
22	25	560366.0

Table 4: Details of the Bitcoin Address (Part 1)

Input Index	Output Index	Value
22	27	1303291.0
22	28	74111256.0
22	31	579781.0
22	32	999820.0
22	33	3010804.0
22	36	8999950000.0
22	37	725905510.0
22	39	3076946.0
22	40	25150000.0
22	42	2129172.0
22	43	1188000.0
23	1	260000.0
23	2	7465350.0
23	4	17787495.0
23	6	1944165.0
23	7	1493527.0
23	29	9799950000.0
23	37	171099460.0
24	34	3797355000.0
24	37	6202645000.0
25	11	6797605000.0
25	34	3202395000.0
26	11	2202295000.0
26	35	7797705000.0
27	35	10000000000.0
28	23	8397805000.0
28	35	1602195000.0
29	23	10000000000.0
30	23	1002095000.0
30	30	8997905000.0
31	30	10000000000.0
32	30	9001945000.0
32	41	998054970.0
33	41	10000000000.0
34	41	10000000000.0
35	41	10000000000.0
36	20	3898255000.0
36	41	6101745000.0
37	20	10000000000.0
38	20	10000000000.0
39	15	6698455000.0
39	20	3301545000.0
40	15	10000000000.0
41	15	10000000000.0
42	15	1721295000.0
42	38	8278705000.0
43	38	10000000000.0
44	38	10000000000.0

Table 5: Details of the Bitcoin Address (Part 2)

Input Index	Output Index	Value
45	10	478904970.0
45	38	9521095000.0
46	10	10000000000.0
47	10	10000000000.0
48	10	3600250000.0
48	26	6399750000.0
49	26	10000000000.0
50	26	10000000000.0
51	26	10000000000.0
52	34	10000000000.0
53	34	10000000000.0
54	34	10000000000.0
55	34	10000000000.0
56	37	10000000000.0
57	37	10000000000.0
58	37	10000000000.0
59	37	10000000000.0
60	37	10000000000.0
61	37	10000000000.0
62	8	3098650000.0
62	10	4320645000.0
63	8	10000000000.0
64	8	10000000000.0
65	8	10000000000.0
66	5	6198900000.0
66	8	3801100000.0
67	5	10000000000.0
68	5	10000000000.0
69	5	10000000000.0
70	5	10000000000.0

Table 6: Details of the Bitcoin Address (Part 3)