**Key Fields for Analysis**

Based on the sample log, here are the most useful fields:

* **Transaction Hash (hash)**: Unique identifier for each transaction.
* **Timestamp (time)**: Unix timestamp of the transaction, useful for time-series analysis.
* **Input Address (inputs[0].prev\_out.addr)**: Address from which Bitcoin is being sent.
* **Output Address (out[0].addr)**: Address receiving the Bitcoin.
* **Input Value (inputs[0].prev\_out.value)**: Amount of Bitcoin in the input, in satoshis (smallest Bitcoin unit, 1 BTC = 100 million satoshis).
* **Output Value (out[0].value)**: Amount of Bitcoin in the output, in satoshis.
* **Transaction Size (size)**: Size of the transaction in bytes; larger transactions usually indicate multiple inputs/outputs or higher complexity.
* **Relayed By (relayed\_by)**: IP address of the node that broadcasted the transaction, helpful for geographical analysis.

**Dashboard Ideas and Report Examples**

Here are ideas for three Splunk dashboards and specific reports to include in each.

**Dashboard 1: Transaction Volume Analysis**

This dashboard focuses on visualizing the volume, frequency, and value of Bitcoin transactions over time.

**Reports:**

1. **Total Transaction Volume Over Time**:
   * Use the time and out[0].value fields.
   * Create a time chart that sums the out[0].value field over time to show transaction volume trends.
2. **Average Transaction Value Over Time**:
   * Use the time and out[0].value fields.
   * Display the average out[0].value per transaction to understand value trends, especially useful for identifying high-value transaction periods.
3. **Number of Transactions Per Hour**:
   * Use the time field.
   * Create a time-based histogram showing the count of transactions per hour or per day to understand transaction frequency.
4. **Top 10 Addresses by Received Value**:
   * Use the out[0].addr and out[0].value fields.
   * Aggregate the out[0].value by out[0].addr to find the top addresses receiving the most Bitcoin.
5. **Distribution of Transaction Sizes**:
   * Use the size field.
   * Plot the distribution of transaction sizes to understand common transaction sizes. Larger sizes might indicate higher complexity or multiple inputs/outputs.

**Dashboard 2: Transaction Activity by Address**

This dashboard focuses on analyzing the activities of specific addresses to identify major participants and track their activity over time.

**Reports:**

1. **Top 10 Most Active Sending Addresses**:
   * Use the inputs[0].prev\_out.addr field.
   * Count transactions by inputs[0].prev\_out.addr to show the most active addresses in terms of sending Bitcoin.
2. **Top 10 Most Active Receiving Addresses**:
   * Use the out[0].addr field.
   * Count transactions by out[0].addr to show the most active addresses in terms of receiving Bitcoin.
3. **Total Bitcoin Sent by Address**:
   * Use the inputs[0].prev\_out.addr and inputs[0].prev\_out.value fields.
   * Sum inputs[0].prev\_out.value by inputs[0].prev\_out.addr to show how much Bitcoin each address has sent in total.
4. **Total Bitcoin Received by Address**:
   * Use the out[0].addr and out[0].value fields.
   * Sum out[0].value by out[0].addr to show how much Bitcoin each address has received in total.
5. **Address Activity Over Time**:
   * Use time, inputs[0].prev\_out.addr, and out[0].addr fields.
   * Create a time-based chart showing the number of transactions over time for a specific address (e.g., selected from a dropdown), useful for tracking address activity.

**Summary of Key Dashboard Ideas**

1. **Transaction Volume Analysis**: Focuses on trends in transaction values, volume, and frequency.
2. **Transaction Activity by Address**: Identifies top sending and receiving addresses and tracks their Bitcoin activities.

These dashboards and reports would provide a comprehensive view of transaction data, helping you track Bitcoin movement trends, address-level activity, and global network dynamics in Splunk.