

Forum:[Hack Forums](#)

Thread: [\[CYBERSEC SERIES #8\] Blockchain OSINT: Investigating Cryptocurrency Wallet Activity](#)

Mastercarder - June 4, 2026, 12:33 pm

? INTRODUCTION ?

Hello everyone,

Welcome back to Cyber Series #8.

Today we're looking at cryptocurrency wallet investigations and how blockchain explorers can be used to understand the movement of funds using publicly available information.

Blockchain transactions are transparent by design. While wallet owners are not automatically identified, transaction history can still reveal useful patterns, relationships and movement between addresses.

? WHAT YOU'LL NEED ?

- Internet connection
- Blockchain explorer
- Public wallet address
- Basic understanding of cryptocurrency

Popular explorers:

- Etherscan
- Blockchain Explorer
- Solscan

? STEP 1 - FIND A PUBLIC WALLET ADDRESS ?

Start with a wallet address that is already public, such as a donation address, exchange wallet or address referenced in a public article.

Never assume a wallet belongs to a specific individual without evidence.

? STEP 2 - SEARCH THE ADDRESS ?

Paste the address into a blockchain explorer.

You will typically see:

- Current balance
- Transaction history
- Assets held
- Wallet activity
- Timestamps

This provides a quick overview of the wallet's behaviour.

? STEP 3 - REVIEW TRANSACTION HISTORY ?

Look for patterns:

- Are funds mostly entering or leaving?
- How frequently is the wallet active?
- Are there unusually large transfers?
- Does activity occur around specific dates?

Patterns often reveal more than individual transactions.

? STEP 4 - FOLLOW THE FLOW OF FUNDS ?

Every blockchain transaction has a sender and receiver.

By opening connected wallets and following transfers, investigators can build a picture of how assets move through a network.

The diagram above shows a simple example of how funds may move from a source wallet, through intermediate wallets, and eventually to an exchange or service.

The goal is not to identify people.

The goal is to understand relationships, movement patterns and transaction behaviour.

? STEP 5 - IDENTIFY INTERESTING EVENTS ?

Things worth noting:

- Large deposits

- Large withdrawals
- Long periods of inactivity
- Sudden spikes in activity
- Repeated transfers between the same wallets

Document everything.

Good investigators build timelines rather than relying on memory.

? STEP 6 - BUILD A TIMELINE ?

Example:

March 3 – Wallet created

March 5 – First incoming transaction

March 12 – Large deposit received

March 14 – Funds moved to another address

March 20 – Wallet became inactive

Creating a timeline helps reveal patterns that might otherwise be missed.

? STEP 7 - UNDERSTAND THE LIMITATIONS ?

Important points:

- Wallets can be anonymous
- One person may control multiple wallets
- Organisations may control thousands of addresses
- Public activity does not automatically reveal identity

Avoid making assumptions without supporting evidence.

? WHY THIS MATTERS ?

Blockchain investigations are used by:

- Security researchers
- Fraud investigators

- Journalists
- Compliance teams
- Financial analysts

Because blockchain data is public, it provides a unique source of intelligence that traditional financial systems do not.

? CONCLUSION ?

Understanding wallet activity is one of the most valuable OSINT skills in the cryptocurrency space.

The objective is not to identify individuals, but to understand patterns, relationships and the movement of funds using publicly available blockchain data.

While blockchain transactions are transparent, interpreting them correctly requires patience, critical thinking and attention to detail.

I hope this tutorial provided a useful introduction to cryptocurrency wallet investigations and blockchain intelligence.

Thank you for reading.

MasterCard @ HF

Cyber Series #8

Stay safe. Stay curious. Keep learning.

Omniscient - June 4, 2026, 12:37 pm

Or just get an AML Risk Check account and run a transaction id or address.

Mastercarder - June 4, 2026, 12:39 pm

(Jun 4, 2026 12:37 PM)Omniscient Wrote: [\[CITE\]](#) Or just get an AML Risk Check account and run a transaction id or address.

Good point. AML tools can definitely provide a lot more context and risk intelligence than what you'll get from a standard blockchain explorer alone. I wanted to keep this tutorial focused on free and publicly accessible methods, but that's a great option for anyone looking to go a bit deeper into wallet investigations. Appreciate the addition Omni!

Boobarina - June 4, 2026, 1:52 pm

That's a jam packed thread full of info nice stuff