BITFURY

# Crystal Blockchain Analytics: Investigation of the Zaif Exchange Hack

October 22, 2018

In this report, Bitfury shares analysis completed by its Crystal Blockchain Analytics engineering team on the movement of bitcoin from the Zaif exchange after its hack in September 2018.

**Key Takeaways:**

30% of stolen bitcoin are still located at addresses related to the hacker.
24% of stolen bitcoin were sent to Binance for exchange/withdrawal. Remaining bitcoin (46%) were split into small amounts and sent to various addresses. The addresses with unknown owners are still under surveillance using Crystal Blockchain.

**Summary:**

On September 17, 2018, the Zaif exchange suspended deposits and withdrawals in BTC, BCH and MONA. On September 18, the exchange reported to the police that it had been hacked and funds had been stolen. In their announcement, they shared the following information:

Someone gained unauthorized access to the exchange on September 14, 2018 between 5PM and 7 PM local time (8 AM and 10AM UTC). They successfully transferred away 5,966 bitcoin (BTC) and unknown amounts of BCH and MONA. Zaif was alerted to this unauthorized access when a server malfunction was detected on September 17.

# Crystal Analytics Research

Bitfury's Crystal Blockchain Analytics engineering team investigated the hack, focusing specifically on the movement of stolen bitcoin. A summary of our investigation can be found below.

## Step 1: Identify the hacker addresses

Because Zaif shared the exact time of unauthorized access, we were able to pinpoint which transactions belong to the hacker. We researched the largest transactions that happened between 7am and 11 am UTC. We shortly discovered a suspicious transaction. The transaction ID is c3b9a4a0831a65523c81e6a04f6ddf5a7a89f344d990e8a13e5278efe57f4280.

This transaction has 131 inputs. Using Crystal's identification software, we were able to determine all of the input addresses were Zaif addresses. The output address is 1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w. All bitcoin were sent to this address.

## Step 2: Track the stolen funds

After identifying the bitcoin address the stolen bitcoin were sent to, we began monitoring that address. Our goal was to find addresses or known entities that received stolen bitcoin from this address. We did this by using Crystal's Tracking tool.

Address 1FmwHh6pgkf4meCMoqo8fHH3GNRF571f9w had 9 outgoing transactions and we tracked each one. After monitoring these transactions, we discovered that 5,109 addresses had received a portion of stolen funds.

Next, we sorted tracking results by the amount settled and found addresses in control of the most significant portion of funds. In some cases, we were able to attribute those addresses to real entities.

## Results (as of October 22, 2018)

The tracking results indicated that significant part of the funds (30% of total amount) had settled on two bitcoin addresses:

1. 3MyE8PRRitpLxy54chtf9pdpjf5NZgTfbZ – 1,007.6 BTC settled on the address.
2. 3EGDAa9rRNhxnhRzpyRmawYtcYg1jP8qb7 – 754.5 BTC settled on the address.

These addresses received bitcoin within a very short chain of transactions (average length was 3 transactions). They had not appeared on the blockchain before, so the owner is unknown. It is probable that these addresses belong to the hacker, so we will monitor their activity going forward.

A significant portion of bitcoin (1,451.7 BTC or 24%) was sent to Binance within a set of small transactions, to Binance address 1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s. Binance

confirmed that they own this address in their official Twitter account. Binance allows users to withdraw up to 2 BTC without going through a strict KYC/AML process, so the average sum sent to each Binance deposit address was 1.99-2 BTC.

Fractions of bitcoin were also sent to ChipMixer.com. The mixing service was reached within a rather short chain of transactions. Approximately 60 BTC have been sent to ChipMixer.com. You may see a transaction to ChipMixer.com on the figure below.

The remaining bitcoin were split into relatively small amounts. Nearly 13 BTC have been sent to various Huobi addresses. Some of bitcoin reached exchanges such as BTCBox.com, Bitstamp, and Livecoin. Some portions of bitcoin were sent to mixing/gambling services such as CoinGaming.io and Bitcoin Fog. However, these entities were reached within a rather long chain of transactions.

The rest of the funds have settled on addresses with unknown owners, and we will keep monitoring them in the future.

## Images Appendix

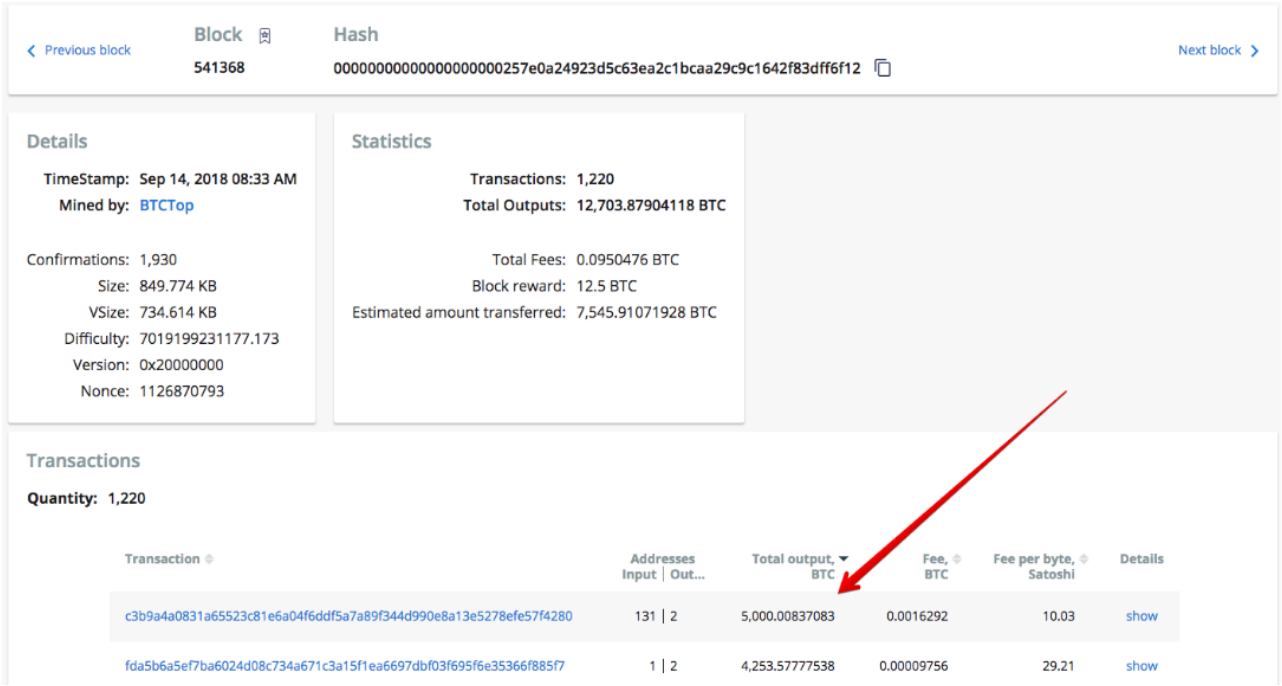


Figure 1: Identification of the suspicious transaction from Zaif to the hacker.

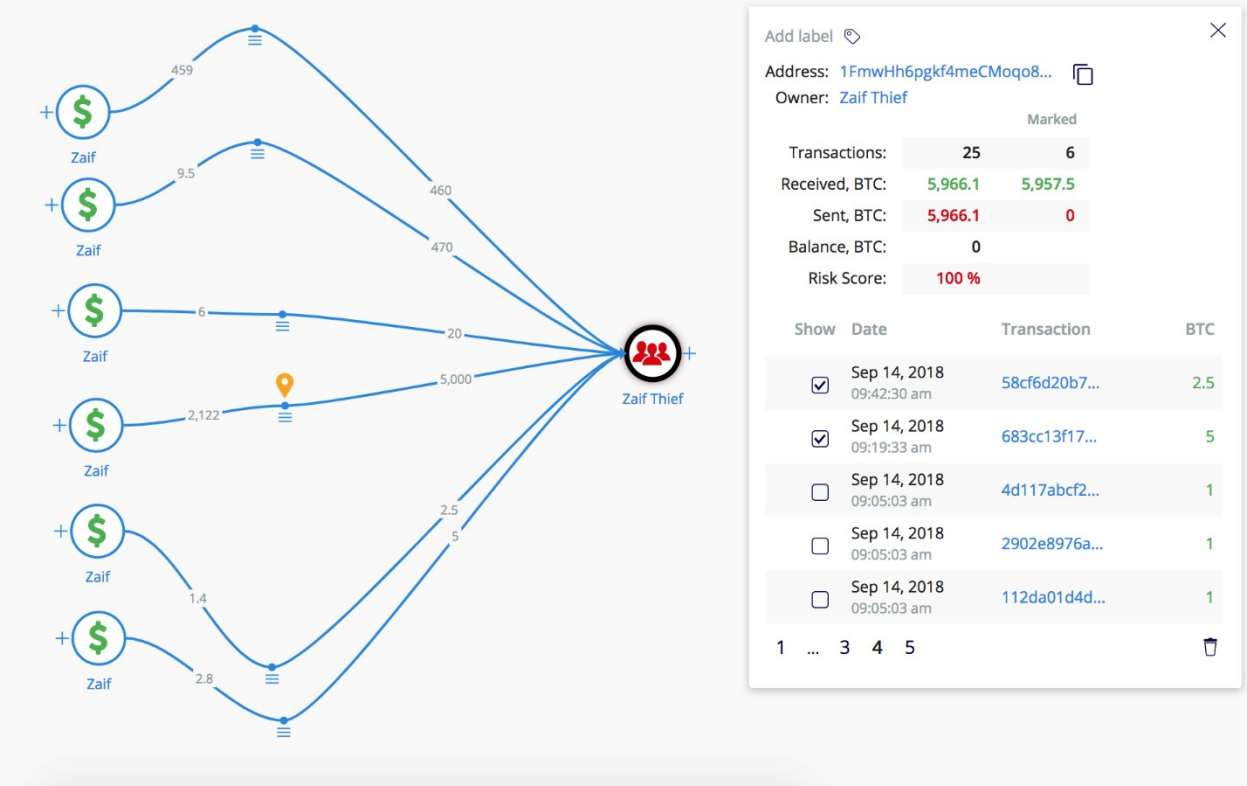


Figure 2: Transfer of funds from Zaif wallets to the hacker

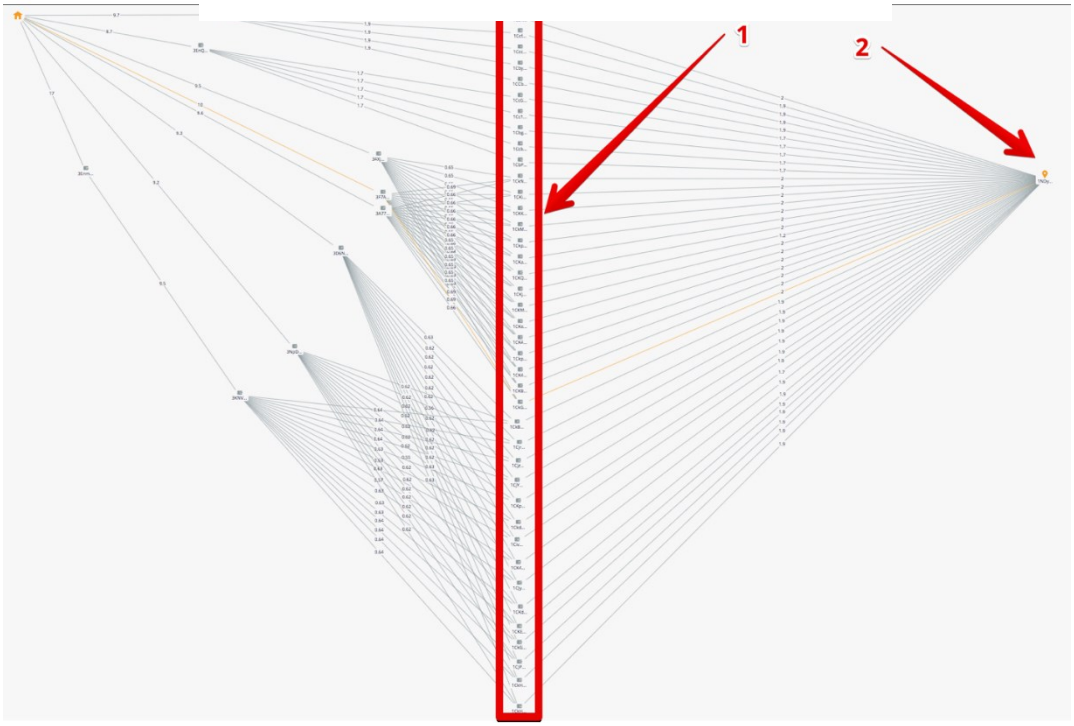


Figure 3: Pattern of Binance deposits

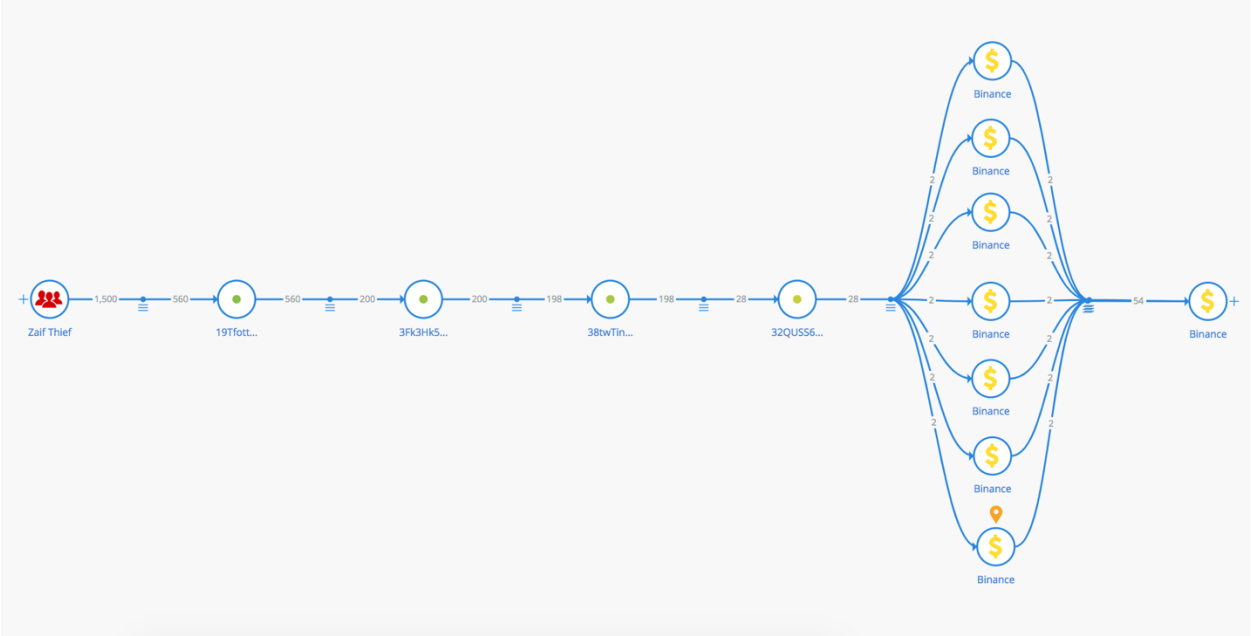


Figure 4: Visualization of money flow to a Binance address

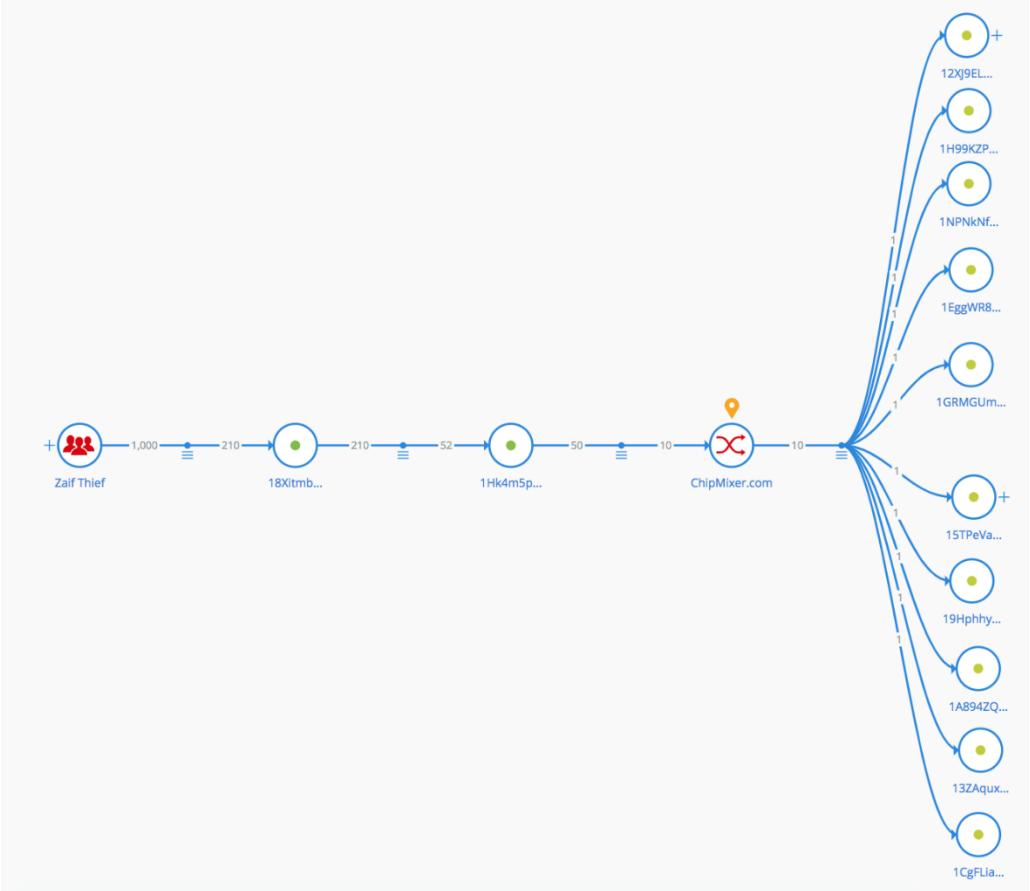


Figure 5: Visualization of money flow to ChipMixer.com