COINFIRM

# Investigation report of the bitcoin address: 1X[redacted]

(this is a censored report and real addresses were changed or sanitized)

## Date of the report: 31st July 2016

https://coinfirm.io

# Contents

# 1. Scope

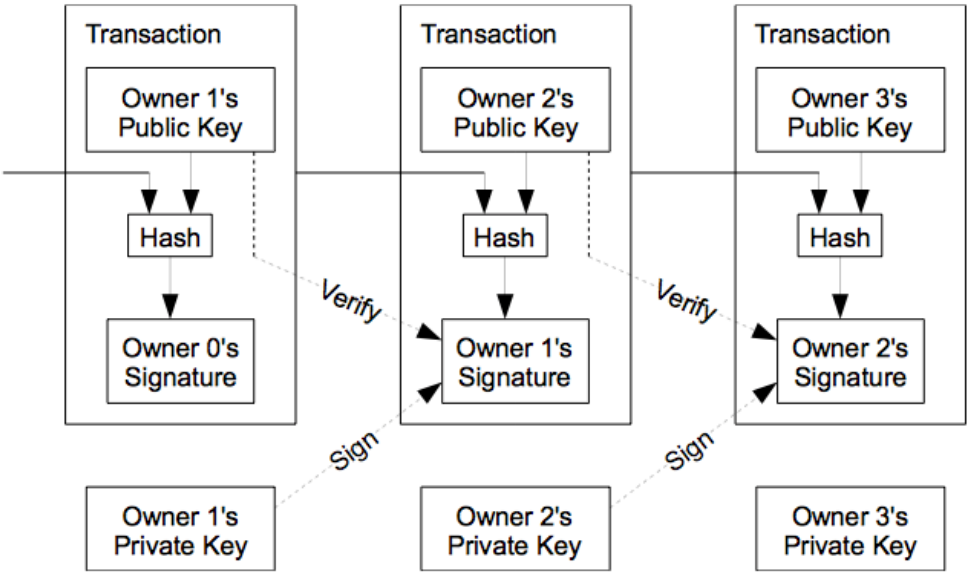
On July 22nd 2016 we were requested by a Client to investigate the potential irregularities related to bitcoin transactions made by a user with the bitcoin address 1X[redacted]. The Client indicated that transactions made by the user of this address may be associated with ransomware extorting bitcoin payments from the owners of infected devices. The Client also pointed out that the user address could be associated with hacker attacks on financial institutions in Poland.

# 2. Introduction

Bitcoin - a digital currency introduced in 2009 by a person (or a group of) under the pseudonym Satoshi Nakamoto. Bitcoins can be stored on a personal computer in the form of a wallet file or kept by an external third party service involved in the storage of such portfolios. In each of these cases bitcoins can be transferred to another person over the Internet to any holder of a bitcoin address. Each bitcoin is divided into 100 000 000 smaller units called Satoshi.

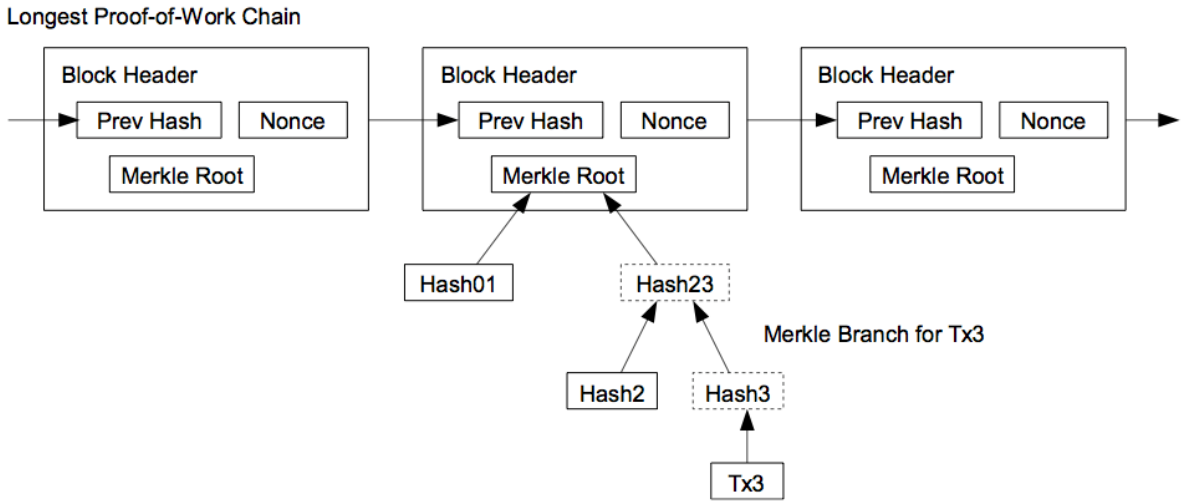
The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.




Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the

other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof- of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.




The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.

## 3. Restrictions

Coinfirm, its partners and other individuals working on this report and its annexes are not in any way connected with the Client and therefore have full ability to provide independent advisory services.

Coinfirm is not liable for any changes in assumptions and updates to this document in the case of new facts or circumstances occurring after the date of the report.

Coinfirm has conducted this investigation on the basis of documents, data and information provided by the Client. The credibility of the information obtained is not subject to verification by Coinfirm.

The addressee of this report is only the Client. Coinfirm does not assume any liability to any other party except for the Client, which would be in possession of the report.

This report should be read in full because any separate analysis of each of its parts can lead to erroneous conclusions.

Employees of Coinfirm involved in preparation of this report are available to clarify any aspects contained therein. We assume that if there are any questions – readers of this report will turn to Coinfirm to receive adequate explanations.

Analysis of the data takes into account the transactions up to block height 404k.

# 4. Summary

1. We have identified 14 addresses belonging to the exchange XYZ1 and 25 addresses belonging to the exchange XYZ2 on which the funds, sourcing from the address 1X[redacted], were sent.
2. We identified 3086 addresses belonging to the same user as the user of the address 1X[redacted], on which the user has accumulated 988.66 BTC (approx. 650k USD according to the exchange rate on the date of the report).

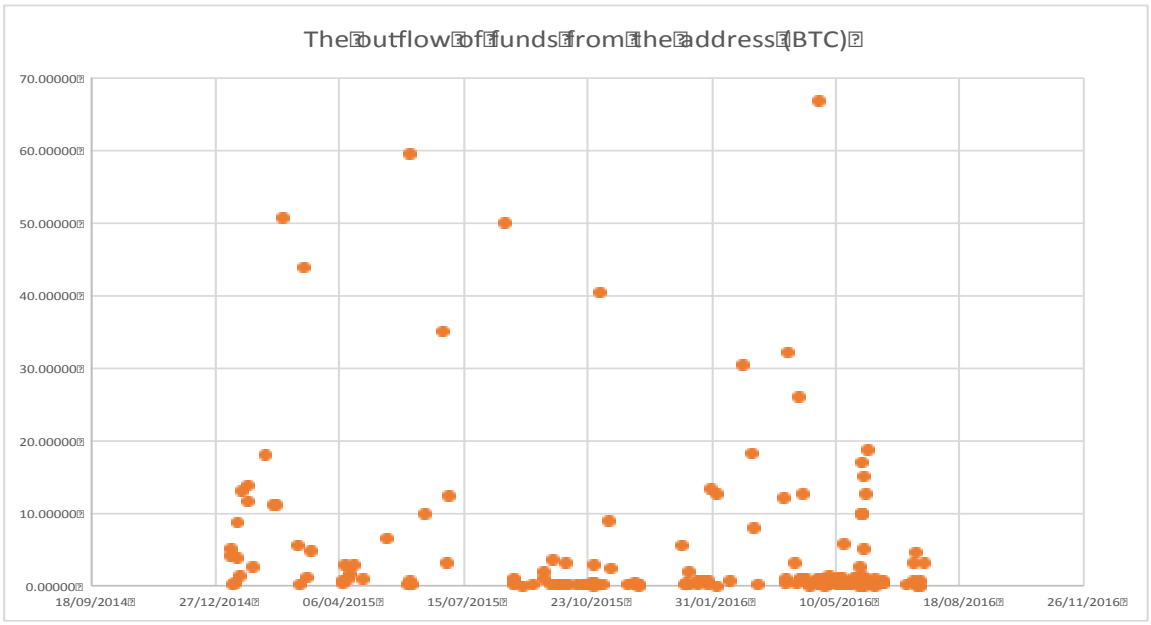
   The greatest activity was observed at the bitcoin address 1Y[redacted], where the user has made 1,523 transactions for a total of 1988.31 BTC (1.3 million USD according to the exchange rate on the date of the report).

   We found 257 addresses belonging to 5 different exchanges to which the funds from the addresses belonging to the user of the address 1X[redacted] were sent.
3. The exchanges XYZ1 and XYZ3 are partnering exchanges of Coinfirm and they declared to disclose the identity of the account owners upon the request of law enforcement authorities. The accounts of the suspected owners have been frozen and their total balance amounted to 494,32 BTC (approx. 375k USD according to the exchange rate on the date of the report).

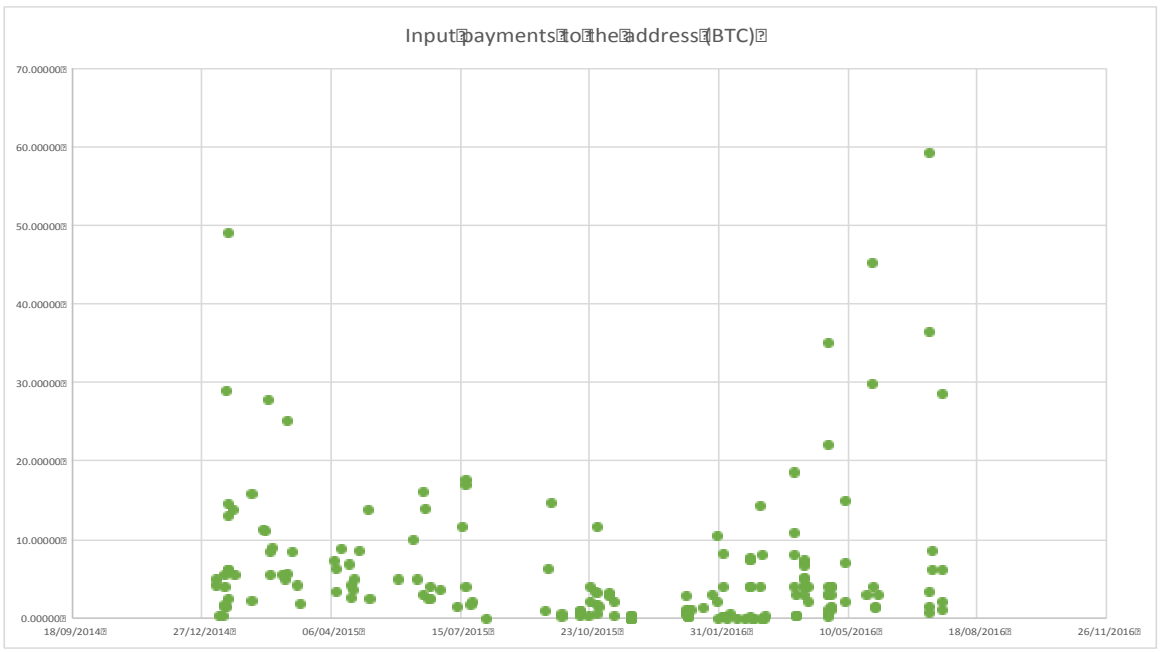
# 5. Detailed Report

## 5.1. Activity on the examined address

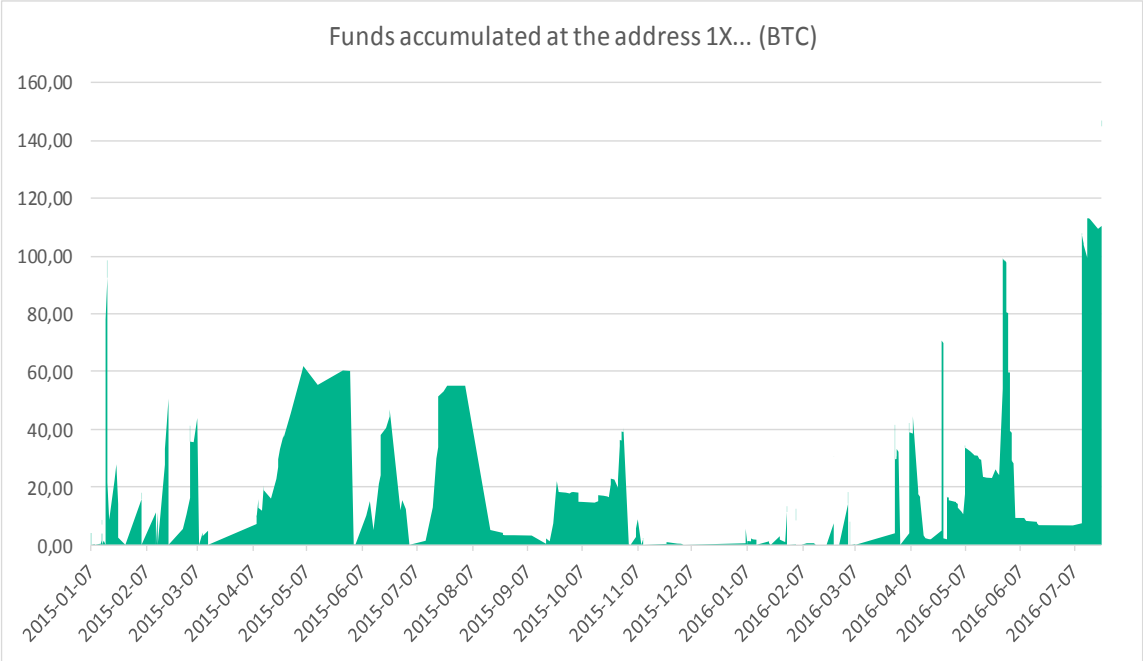
1. Statistics of activity:
   a. Date and time of the first transaction: 2015-01-07 5:33:50 p.m. UTC
   b. Date and time of the last observed transactions: 2016-07-22 11:13:13 p.m. UTC
   c. The largest transaction:
      a1z[redacted]
      (transfer of funds from the analyzed address on 2016-04-25 1:18:45 p.m.:
      - 66.66 BTC were sent from the address 1X[redacted],
      - 310.37 BTC was the total value of this transaction);
   d. Average transaction value: 4.01484042 BTC
   e. Number of direct transactions with the analyzed address: 367
   f. Number of transactions in the proximity of 2 transactions from the analyzed address: 5683
   g. Number of transactions in the proximity of 3 transactions from the analyzed address 10932
   h. Total funds received at the analyzed address: 1104.49 BTC (719k USD):




i. Total sent from the address: BTC 957.57 (623k USD):




j. The sum of the funds collected on the address on the day of the report amounted to 146.91 BTC (96k USD):




For the full list of transactions and history of funds on the address please refer to the Appendixes 1a and 1b.

## 5.2. Activity on the other addresses belonging to the same user

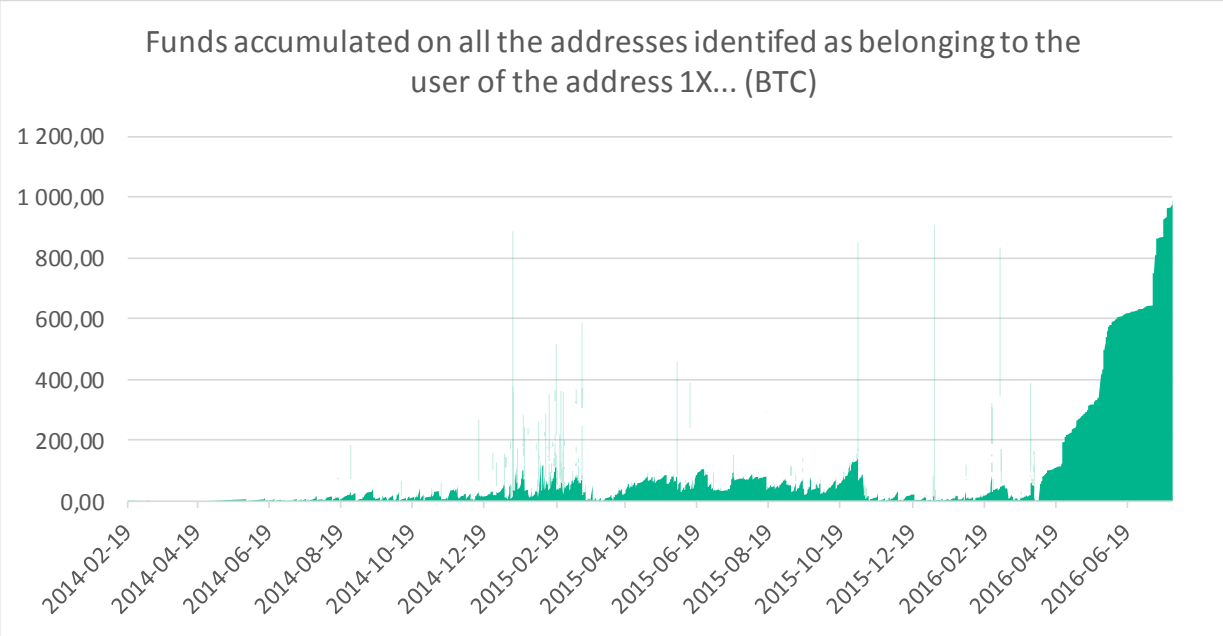
1. We have identified 3086 other addresses belonging to the same user as the owner of the address 1X[redacted]. Their full list with relevant statistics is presented in Appendixes 2a and 2b):

| ID | Address | Number of transactions to the address | Number of transactions from the address | Total number of transactions where the address appears at least once | Value of the transactions to the address (BTC) | Value of the transactions from the address (BTC) | Value of the transaction to the address (in USD w; USD/BTC from the transacton timestamp | [...] | The address is the address of the source (destination) in transactions to (from) address 1X... |
|---|---|---|---|---|---|---|---|---|---|
| | Totals -> | 5 946 | 4 385 | 9 921 | 22 509 | 21 544 | 6 110 664 | [...] | |
| 1 | 1YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY | 1 422 | 318 | 1 508 | 2 290,71590988 | 2 121,58972981 | 624 194,97 | | No |
| 2 | 1XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX | 332 | 103 | 372 | 1 648,36458376 | 871,73123160 | 210 601,43 | | No |
| 3 | 19vXAizZKJnwXhJHdVCsP1fEi6EFgLEYwA | 83 | 51 | 134 | 698,65804263 | 698,65804263 | 161 888,08 | | No |
| 4 | 16VaRtm9zFAyK6ez2S6zdX4Q3b4qgHU4rA | 124 | 51 | 173 | 466,75223483 | 447,34880000 | 110 325,59 | | No |
| 5 | 17FmnDKQZXNLqB33tx9nXQbs66cP8wjEWr | 31 | 18 | 49 | 287,50010000 | 287,50010000 | 72 708,25 | | No |
| 6 | 1FXk7Wsy2aaSEwDVJsoZCSxJVBWKnCcwb9 | 26 | 22 | 48 | 227,48120000 | 227,48120000 | 71 137,14 | | No |
| 7 | 1EJUszCfWujyL8PnPfkc9Q3q2GXXaEHeBB | 23 | 19 | 42 | 167,11819799 | 167,11819799 | 63 221,92 | | No |
| 8 | 1H98rdaNg1tGXFqxguP8ZkqkqbdLWjESnz | 2 | 2 | 3 | 72,34505330 | 72,34505330 | 36 743,04 | | No |
| 9 | 1NpuuRGeJeQ4fTPtj6FoEAX7V4SVwGwe5v | 2 | 2 | 3 | 87,74591540 | 87,74591540 | 24 898,52 | | No |
| 10 | 12S72Gzz8m4fgYDFDX4uULWfd8zjHXGh23 | 1 | 1 | 2 | 49,58838500 | 49,58838500 | 22 619,39 | | No |

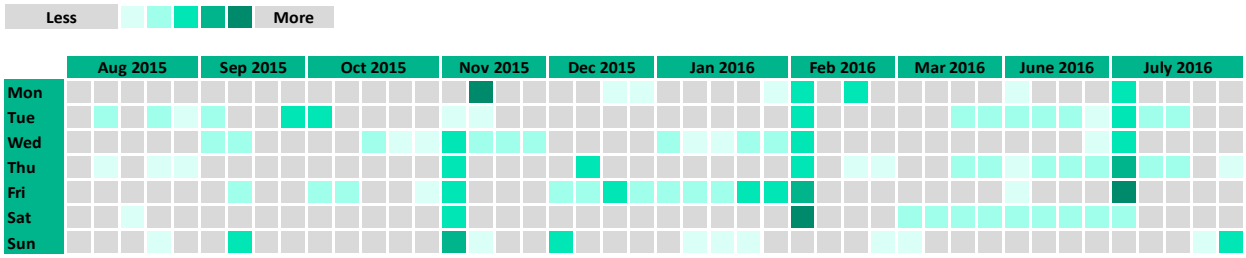
2. The highest activity was recorded on the address 1Y[redacted], where the user made 1523 transactions for a total of 1988.31 BTC ($ 1.3 million at the exchange rate on the day of the report). The current value of the funds collected at this address is 2.21 BTC (1400 USD at the exchange rate of the report).

3. The total value of transactions for the 3086 identified addresses amounted to 22509 BTC (6.1 million USD at the exchange rates corresponding to the times of the transaction). The total value of the

funds in the 3086 addresses on the day of the report totalled 988.66 BTC (about 650k USD according to the exchange rate on the date of the report):




4. The frequency of the transactions occurring on the addresses belonging to the user of the address 1X[redacted] is outlined in the diagram below:




The analysis reveals that the user executed most of the transactions during the first week of the selected months.

5. The table below presents the 2341 addresses from which the largest amount of funds were sent to the identified 3086 addresses belonging to the user of the address 1X[redacted] (directly or indirectly through other addresses, including anonimizers - mixers and tumblers). Complete address list is presented in the Appendix 3a.

| ID | Address | % of funds | Number of transactions | Owner of the address | The address belongs to the same user as the owner of the address 1X... |
|---|---|---|---|---|---|
| 1 | 16QrnX3SjzjsSzwNjDQfudXbnibuFRWLQA | 8,146140916% | 40 | No data | No |
| 2 | 1LygTHjQtprX5wjjVjNZVCkD9J5ySqxgD9 | 3,854262863% | 24 | No data | No |
| 3 | 1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP | 1,203330310% | 21 | No data | No |
| 4 | 19govWMzsRXqLUsUrHQKQ3DzekRxhsqwWH | 0,549286413% | 4 | No data | No |
| 5 | 1BgPFdurz9fgzPGS5idtuJWT3DGndUmndY | 0,480412429% | 10 | No data | No |
| 6 | 1NaRMgB35pGH3hpoYYCUm4cKatA36pxtxs | 0,401656427% | 33 | No data | No |
| 7 | 1Bnx7YbsgduRBXfeW3vnQvvJt2ueA4WWRq | 0,281154821% | 1 | No data | No |
| 8 | 3AgxodEvv9FZtm6LMgPxCSmBwhNSBdFsSk | 0,281115432% | 1 | No data | No |
| 9 | 13chcm1gihAC4J4nerbEjsw6tYomG6Ru7a | 0,268021874% | 46 | No data | No |
| 10 | 1ETAKWN3NuoC9HiPm2vmV5gNFT6yH9yqZP | 0,263434097% | 1 | No data | No |

None of these addresses have been recognized as addresses belonging to known exchanges, wallets or other known endpoints. It may mean that funds on the user's addresses mostly come from ransomware attacks.

6. The table below presents the identified 1326 addresses to which the largest amount of funds were sent from the 3086 addresses belonging to the user of the address 1X[redacted] (directly or indirectly through other addresses, including anonimizers - mixers and tumblers). Complete address list is presented in the Appendix 3b.

| ID | Address | % of funds | Number of transactions | Owner of the address | The address belongs to the same user as the owner of the address 1X... |
|---|---|---|---|---|---|
| 1 | 1Kz1eU5GajMRXzWgcGsprWTNgeWPHpuLUz | 0,7717507444% | 2 | No data | No |
| 2 | 1BQv78xuwokjFwfe87JyUwUJLKpPBuyTwD | 0,7011986999% | 2 | No data | No |
| 3 | 1FG4wjHggRoLaiNdV3oYuSFH3gaBUcCisa | 0,6838275008% | 2 | No data | No |
| 4 | 1Bs4wTXa3wK82DozHi3VSHLhRMU7Xk7ZKe | 0,5840758448% | 2 | No data | No |
| 5 | 1NmemWVrC8t2P8ACzMYmR3TWbmykXxbQtB | 0,3634228188% | 4 | XYZ1 | No |
| 6 | 13c7hgPoxAMMfFPjS7wqNYS9pffNbd3Sn8 | 0,3462939788% | 2 | No data | No |
| 7 | 1CkYQnGPVreWTaJHUz1YyrQkCUL4AfcaV3 | 0,3360673968% | 2 | No data | No |
| 8 | 1JCvnbeTAFyw2Ad4J6EsMpM8iCpDi1ZaGz | 0,3224947238% | 2 | No data | No |
| 9 | 1PthtLWkgZ8bpVV1MXTVBVGEbHo718JLJx | 0,2499876318% | 2 | No data | No |
| 10 | 18dfcnDfeCEpxJLBipBaW5PYLMgSuh7mYx | 0,1587182038% | 2 | No data | No |
| 11 | 1Mx14s8GSCSp3hbXx5KsjWxZ3enxvdhqxU | 0,1141551858% | 6 | No data | No |
| 12 | 3FMXBbSMEztoVFQex78Y8oVUqSVhMC3mKx | 0,0848442988% | 2 | No data | No |
| 13 | 15aYiMMCVZjaixrJJE35TxdEJWhdg1NQR7 | 0,0825570508% | 6 | No data | No |
| 14 | 363nxYLA3ceoBaaZY1yQXorbA6FVHZmsFF | 0,0734358658% | 2 | No data | No |
| 15 | 1G7SsoYxvTCfMAWjSbYRrGa4FXpXLEy4T3 | 0,0696338378% | 2 | No data | No |
| 16 | 1A9gxC3Nfu3yryD3kZ5ufUQhqYHcE2nK8t | 0,0674909808% | 14 | Agora Market | No |
| 17 | 38VZTRqFEn3v6eAiRVLCfvpTqutFazzvWb | 0,0658616488% | 2 | No data | No |
| 18 | 1PJ5iWxuXEGLU8d7uorvczggjV6mT4yoQD | 0,0655645978% | 2 | XYZ1 | No |
| 19 | 1NyKq2EwYeYUX3cpiCG2TKtSwbNgDoY8Mr | 0,0644051498% | 2 | No data | No |
| 20 | 3HqAnTMRBdZLGf75F8FayHjPw8fczkaU9W | 0,0608877268% | 2 | No data | No |

The analysis revealed 14 addresses belonging to the exchange XYZ1 and 25 addresses belonging to the exchange XYZ2 on which the funds from the address 1X[redacted] were sent.

In total we found 257 addresses belonging to 5 different exchanges to which the funds from the addresses belonging the user of the addresses 1X[redacted] were sent. Further 19 addresses belonging to the user of the address 1X[redacted] are black market addresses related to drugs trade.

## 6. Recommendations and next steps

1. Consider the engagement of law enforcement authorities to contact the exchanges in order to obtain information from them about the users of the accounts related to the 257 identified beneficiary addresses.
2. Consider recovery of funds frozen on the accounts of our partnering exchanges.

## 7. List of attachments*

* All annexes and attachments to the report have been included in MS Excel format

**Appendix No. 1a** - list of transactions on the address 1X[redacted]

**Appendix No. 1b** - history of funds on the address 1X[redacted]

**Appendix No. 2a** - list of addresses belonging to the same user as the user of the address 1X[redacted]

**Appendix No. 2b** - the history of funds on the addresses belonging to the same user as the owner of 1X[redacted]

**Appendix No. 3a -** list of addresses sourcing the funds to the addressed belonging to the user of the address, 1X[redacted]

**Appendix No. 3b** - list of addresses that were the ultimate beneficiaries of the funds sourced from addresses belonging to the user of the address 1X[redacted]

The report was prepared by:

### Paweł Aleksander

One of the more recognizable fraud prevention experts in Central Europe. Former Head of Fraud Investigations in ArcelorMittal, and former AML/KYC Project Manager in the Royal Bank of Scotland and fraud investigator and auditor in Ernst & Young and Deloitte. He holds the titles of Certified Fraud Examiner and Certified Internal Auditor.

### Jakub Fijołek

An innovative IT and security specialist, Jakub has been analyzing and developing around blockchain and its applications since 2010. He is the former head of multi-algorithm cryptocurrency mining farms with vast experience in attacking, testing and creating the security systems around Blockchain.