



ColossusXT Forensic Statement on CoinsMarkets Exchange Fraud



Overview:

In this presentation we wish to document and share our evidence and findings with regards to the CoinsMarkets exchange scam.

We encourage other cryptocurrencies that have been defrauded by CoinsMarkets to come forward with their findings as well, and are committed to open collaboration with all involved in this issue and full cooperation with any involved law enforcement personnel.



Timeline:

- The CoinsMarkets exchange went offline on January 4th, 2018. After several days of being unreachable, the site returned in a limited capacity, with trading and withdrawal suspended, and displayed a message indicating that they are working to recover from database issues
- This situation remained for approximately 7 weeks, with occasional changes to the status message.
- In late February, CoinsMarkets began releasing some cryptocurrencies for withdrawal. COLX was not among them.
- The COLX team attempted to contact CoinsMarkets a multitude of times, including the March 1st legal letter demanding immediate release of COLX. There was no reply or acknowledgement.



Timeline:

- The COLX team had been monitoring the CoinsMarkets wallet, which contained approximately 350M COLX, and had seen no movement of assets. It was hoped that although CM was handling the situation extremely poorly, they were acting in good faith and would eventually release COLX for withdrawal.
- On March 19th, the Crypto-Bridge exchange began to be flooded by extremely large sell-offs from a single address containing 500M COLX. These sales were at extremely high volumes, at and *below* current market value, driving the COLX price down significantly.
- Though suspicious and frankly idiotic from an investing standpoint, there was nothing yet to directly tie these transactions to CoinsMarkets, and they were assumed to be the result of a "whale" investor selling off assets as quickly as possible.



Timeline:

- On March 24th, COLX trading was enabled on Cryptopia. Shortly thereafter, large sell-offs began to occur on that exchange as well.
- On March 31st, the 500M COLX "whale" address reached a balance of zero.
- Hours later on March 31st, the CoinsMarkets wallet that had sat motionless since CoinsMarkets went offline on January 4th began to be liquidated, eventually being entirely emptied. The details of these transactions revealed that the selloff of the CoinsMarkets wallet and the 500M address were in fact perpetrated by the same fraudulent actor.
- Over the course of the next 12 days, all CoinsMarkets wallet assets were liquidated entirely, reaching a zero balance on April 11th.



Evidence & Conclusions

Based on the evidence that will follow, we draw the following conclusions:

- 1) The CoinsMarkets wallet containing 350M COLX and the additional address containing 500M COLX were in fact controlled and fraudulently sold off by the same individual or group; all 850M were likely Coinsmarkets user assets.
- 2) Those 850M COLX have been fully liquidated on Crypto-Bridge, Cryptopia, and possibly other exchanges as well.
- 3) The Crypto-Bridge selloff of stolen assets was perpetrated in part by Crypto-Bridge user "allanosti1".
- 4) Crypto-Bridge user allanosti1 has withdrawn the BTC resulting from the COLX sell-off from the Crypto-Bridge exchange.
- 5) Crypto-Bridge User allanosti1 appears to have been involved in similar fraudulent activity for ECA, POLIS, and ALQO currencies, all of which were primarily traded on the CoinsMarkets exchange.



The 500M Address

A series of massive sell-offs began on the Crypto-Bridge exchange on March 19th. These selloffs appeared to correspond to withdrawals from a single COLX address containing 500M COLX:

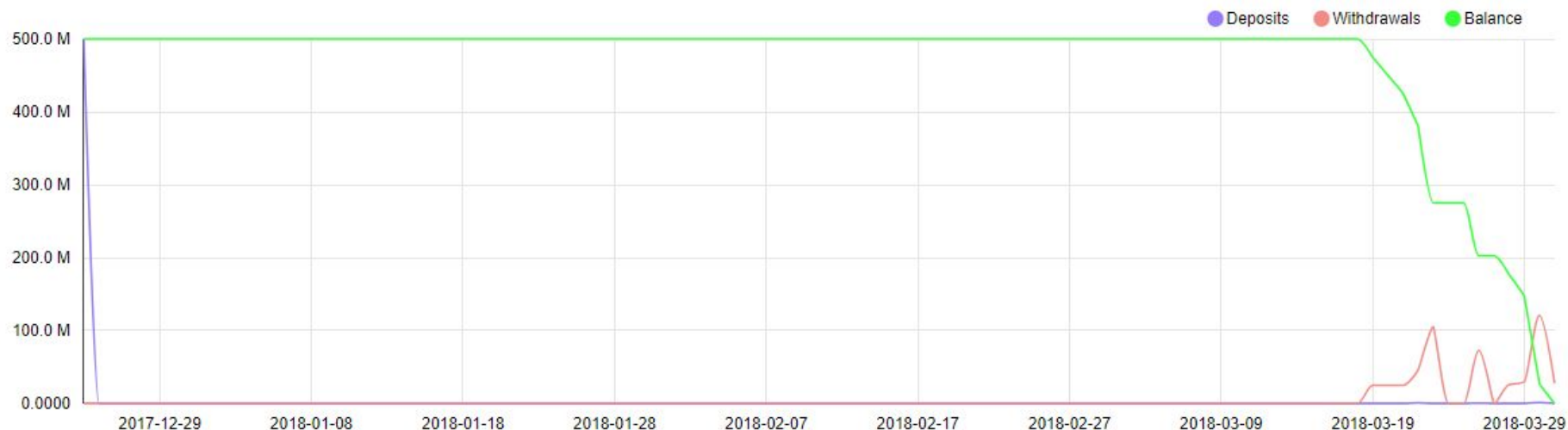
<https://chainz.cryptoid.info/colx/address.dws?DQzEEey3v1v83r9nAVGuvDCPporWvECCJY.htm>



The 500M Address

A review of the transaction history of this address shows a steady withdrawal of all COLX assets from this address from March 19th to March 31st:

Guesstimated Balance History





The 500M Address

Study of the Crypto-Bridge blockchain revealed that some of these transactions indicate a connection with Crypto-Bridge user "allanosti1". There are many such examples of this:

Here is a transaction where 20M COLX is sent from the 500M address (DQz...) to a Crypto-Bridge address:

<https://chainz.cryptoid.info/colx/block.dws?260039.htm>

And here is that same asset being issued to allanosti on Crypto-Bridge a few minutes later:

<https://wallet.crypto-bridge.org/block/25720672>



The 500M Address

Here is another example correlating allanosti1 to the 500M address.

First the withdrawal from the DQz... 500M address:

<https://chainz.cryptoid.info/colx/tx.dws?535489.htm>

Followed immediately by the issuance of an identical asset to allanosti on Crypto-Bridge:

<https://wallet.crypto-bridge.org/block/25496144>



The CoinsMarkets Wallet

This is the wallet known to be the primary CoinsMarkets COLX store:

<https://chainz.cryptoid.info/colx/wallet.dws?4048.htm>

We can positively verify that this is in fact the CoinsMarkets wallet by confirming that it contains deposit addresses used by COLX users to deposit COLX onto the CoinsMarkets exchange. One such address, provided to us by a COLX user, is the following: (see screenshot on next page)

DAfDrX9rA7aoJmHus97qqS4NDyrwmeXf46

This address is contained within the CoinsMarkets wallet as expected:

<https://chainz.cryptoid.info/colx/wallet.dws?4048.htm>

(Click “show latest 1000 addresses...” and search for the address)







The CoinsMarkets Wallet

This is a screenshot from the CoinsMarkets site showing a user's CoinsMarkets deposit address:

Balance

Search: [Hide Empty Balance](#)

General Balance	On Hold	Wallet Management
 Bitcoin Balance: 0.13574851 BTC Total: 0.30743351 BTC	On orders: 0.17168499 BTC	<div>Deposit Withdraw</div>
 ColossusCoinXT Balance: 300189.08333847 COLX Total: 350189.08333847 COLX	On orders: 50000.0000	<div>Deposit Withdraw</div> <div>DAfDrX9rA7aoJmHus97qqS4NDyrwmeXf46 ?</div>
 CraftRToken Balance: 10.95089774 CRFT Total: 10.95089774 CRFT	On orders: 0.00000000 CRFT	<div>Deposit Withdraw</div> <div>Click here to Create an Address</div>
 GanjaCoin Balance: 0.00000000 MRJA Total: 0.00000000 MRJA	On orders: 0.00000000 MRJA	<div>Deposit Withdraw</div> <div>?</div>

* Transaction fees: Fees will be deduced from the amount being sent

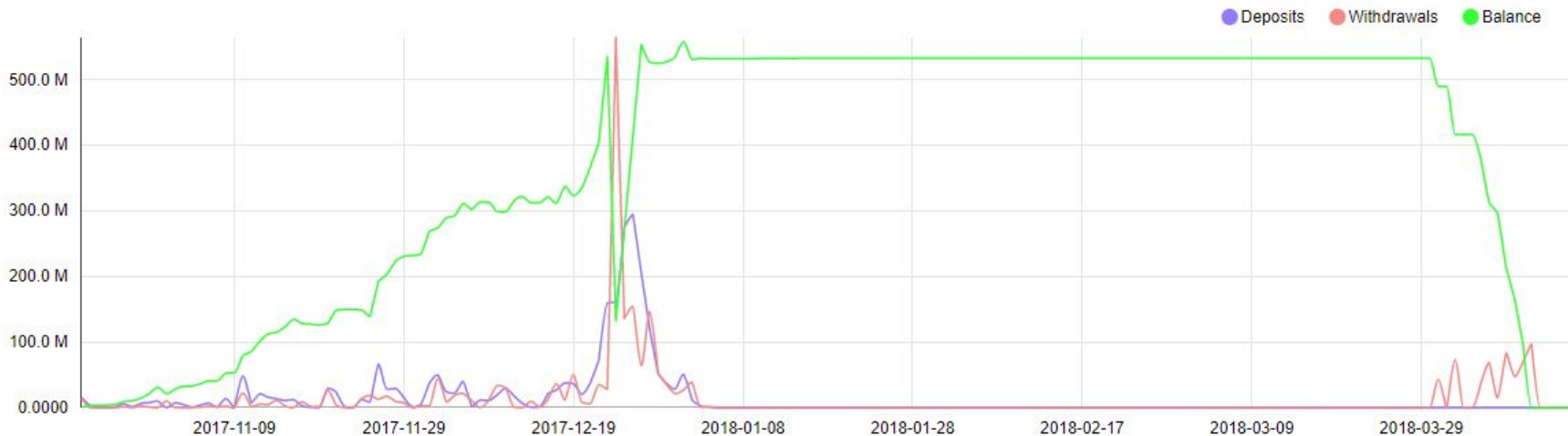




The CoinsMarkets Wallet

The CoinsMarkets wallet sat idle with a 350M balance, starting with the CoinsMarkets downtime on January 4th. Beginning on March 31st (hours after the 500M address reached zero), assets began to be removed from this address, reaching a zero balance on April 11th:

Guesstimated Balance History





CM Wallet & 500M Address Deposit To Same Address

Further study of the blockchain reveals that the CoinsMarkets address and the 500M address eventually deposited COLX to the same address:

Here is the 500M address (DQz...) depositing to an unknown address (DLSKh...):

<https://chainz.cryptoid.info/colx/tx.dws?562822.htm>

And here is an address contained in the aforementioned CoinsMarkets wallet, also depositing to that SAME address (DLSKh...):

<https://chainz.cryptoid.info/colx/tx.dws?595319.htm>

Again, this is one example of many available.

Based on this correlation, we can conclude that the liquidations of the CoinsMarkets wallet and the 500M address were carried out by the same individual or group as part of the same fraudulent action, and that it is likely that all 850M COLX were stolen CoinsMarkets assets.



Cryptopia

In the process of our investigation, we observed that withdrawals from the 500M address and the CoinsMarkets wallet to the address below were followed quickly by large sell-offs on the Cryptopia exchange:

<https://chainz.cryptoid.info/colx/address.dws?DLSKh5XMGoxYohTqNzHaqQ7HaiQoHivgdc.htm>

We contacted Cryptopia and they were able to positively confirm that this address is a deposit address on their exchange.

PLEASE NOTE: the balance currently contained in the above address does not indicate that there are still COLX in that account! Once assets are deposited onto an exchange, the deposit address is no longer a valid measure of that account's balance. Exchanges track account balances on their own internal ledgers and manage actual asset addresses and balances as they see fit.



BTC Withdrawal

Crypto-Bridge user allanosti1 has withdrawn BTC from that exchange several times.

Here is one such example:

<https://wallet.crypto-bridge.org/block/26028223>

And here is the corresponding resultant transaction on the BTC blockchain:

<https://blockchain.info/tx/9585369338b9c104ddadf226b8d392b986f371f88e401d7197da937e630b3f27>

The address to which these BTC were withdrawn currently contains over 170 BTC.

<https://blockchain.info/address/1HFEZLPJJaquTFPAnvkyjD6vHukhfm7mEk>



Other Cryptocurrencies

COLX was just one of many cryptocurrencies that were defrauded by CoinsMarkets.

We have heard of similar experiences from POLIS, ALQO, SHIELD, and many others.

A small portion of these transactions are viewable on Crypto-Bridge user allanosti1's account ledger:

<http://bitshares-explorer.io/#/accounts/allanosti1>

To review assets deposited onto Crypto-Bridge by this user, use the export tool:

<http://open-explorer.io/bitshares-account-exporter/>

Search for user 1.2.831419, March 1 - present, and filter for the action "Asset Issued". Column M displays the assets (by asset code) and amounts.



Other Cryptocurrencies

Also note that the Crypto-Bridge exchange is only a small part of the fraudulent sell-off.

Considering that we know COLX was sold on Cryptopia as well as Crypto-Bridge, we should assume the same is the case for other cryptocurrencies stolen from CoinsMarkets users.



Guesstimator Note

Cryptoid's COLX blockchain explorer "guesstimator" service was used to identify and correlate addresses in the CoinsMarkets wallet.

This feature analyzes transactions to identify addresses that are contained within the same wallet. For example, if two addresses containing 50K each are used as inputs in a single transaction sending 100K, we can conclude that those two addresses are contained within the same wallet. Over time, this service can correlate large sets of addresses, which are likely exchanges, in this case, the CoinsMarkets exchange

While this service warns that this feature is not 100% accurate, it's important to note that any possible inaccuracy lies not in false correlations, but in missing addresses. It's safe to conclude that addresses listed in this wallet are in fact on the CoinsMarkets exchange. However, it is possible that some addresses are missing from the list, meaning that the now-stolen balance of 350M COLX shown in this wallet is lower than the actual total of CoinsMarkets wallet assets.



Further Information

If you have any questions or are able to provide any additional information regarding the CoinsMarkets fraud, please contact a ColossusXT team member on our Discord:

<https://discord.gg/FzRcsFY>

#coinsmarkets-questions