



## KRYPTON RECOVERS FROM A NEW TYPE OF 51% NETWORK ATTACK

Published on August 26, 2016



**Stephanie Kent** | [Follow](#)  
Krypton, KR | Founder



13



3



4

[Krypton](#), an Ethereum based blockchain, recovered from a novel version of a 51% attack which appears to be the first of its kind.

The exploit includes a two pronged attack: first prong was, overpowering the network with at least 51% of the hashing power to roll back transactions and spend the same coins twice, and the second prong was DDoS-ing nodes to multiply network power. This exploit should be understood by all smaller coins to prevent copycat attacks.

The attackers managed to steal around 21,465 KR from Bittrex by double spending on the network. The attackers did this by sending KR to Bittrex, sold them for bitcoin and then rolled back the blockchain to reverse the transaction. Supernova mining pool and Krypton stats servers were also DDoS attacked to give the malicious miners an edge over the network.

The miners rented extra hashing power from Nicehash and used 4miners pool to conduct the attack. KR deposits and withdrawals are frozen on Bittrex and Yobit, pending confirmation that all work arounds have been successfully implemented.

### LOW HASHING ETHEREUM BASED COINS AT RISK

This attack may be a “dry run” intended as proof of concept before targeting other

Ethereum based blockchains. Shift, another Ethereum type coin, was also targeted by a similar 51% attack last week.

Ethereum based blockchains are being targeted predominantly because they're easy to fork and manipulate offline, while being used in conjunction with DDoS attacks.

It is suspected that the attackers may be using these lower cap coins as a testnet before [targeting Ethereum Classic](#). This attack may be more difficult to scale up because of ETC's larger aggregated hashing power.

## SOLUTIONS

The Krypton and Shift core development teams have been working to resolve the problem. Krypton has resolved the issue of lost funds due to the attack and suggested to Bittrex to increase KR withdrawal times to 1000 confirmations, to mitigate the risk of rolling back the network for another double spend. Deposits and withdrawals are expected to be re-enabled upon implementation of the above noted workarounds.

The Krypton community also stepped in to purchase additional hashing power and spread it across multiple pools. Bittrex also upgraded their Krypton client code to fix a caching bug with the new KR block explorer.


Potentially affected blockchains may consider merging POS with POW, because doing so may require the attackers to own coins prior to mounting their attack, thus increasing the barriers to a 51% attack. Node operators should be mindful of behaviour suggesting a DDoS as a signal that a 51% attack may be attempted.

HomeProfileMy NetworkJobsInterestsBusiness ServicesTry Premium for fre

Search for people, jobs, companies, and more...Advanced

LikeCommentShare


Tagged in: [hacking](#), [fintech](#), [bitcoin](#)Report this



**Stephanie Kent**  
Krypton, KR | Founder  
[10 posts](#)

Follow

3 commentsRecommended



Leave your thoughts here...

**Stephanie Kent**  
Krypton, KR | Founder

... 3h



I'd like to thank Team Krypton for the professional manner in which this attack was handled. Everyone from devs to miners worked in concert to quickly identify and mitigate this novel attack vector. You have my deepest admiration. It is my pleasure to work with you. - [Stephanie Kent](#)

Like Reply | 1



**Prof. Nick Colosimo** CEng MIET

... 1h

Strategy & Planning Executive, Global Engineering Fellow, Technologist (Disruptive Capabilities)

It's a huge challenge Stephanie. Glad you got it sorted. I've often wondered about the distribution of mining resource and whether there is a way to improve resilience to these kinds of attacks (DDoS to valid nodes and 51 percent attack via malignant nodes). I'm thinking about pool size and number of pools albeit this may require some rethinking of the underpinning blockchain tech.

Like Reply | 1



**Frank Ramirez**

... 15h

IQ2, PowerMyData Founder

grr - pains of growing up and dealing with global inequities in ethics and accountability. The challenge is not many govt. are progressive enough, most view crypto as a threat, and none have the domain strength to have a substantive impact. Still they should try. Tech may just be the force the globe to finally get its act together.

Like Reply

## Don't miss more posts by Stephanie Kent



### Krypton Corp Names Advisors

Stephanie Kent on LinkedIn



### Stephanie Kent (covertress) LIVE on Core Radio

Stephanie Kent on LinkedIn



### COVERTRESS LIVE IN TORONTO 18-AUG ANONYMOUS NO MORE!

Stephanie Kent on LinkedIn

Looking for more of the latest headlines on LinkedIn?

[Discover more stories](#)

[Help Center](#) | [About](#) | [Careers](#) | [Advertising](#) | [Talent Solutions](#) | [Sales Solutions](#) | [Small Business](#) | [Mobile](#) | [Language](#) | [Upgrade Your Account](#)

LinkedIn Corporation © 2016 | [User Agreement](#) | [Privacy Policy](#) | [Ad Choices](#) | [Community Guidelines](#) | [Cookie Policy](#) | [Copyright Policy](#) | [Send Feedback](#)