






We're using cookies to improve your experience. [Click Here to find out more.](#)

>

-
- [Mashable](#)
[Mashable Asia](#) [Mashable Australia](#) [Mashable France](#) [Mashable India](#) [Mashable UK](#)
- [Sign in](#)
- - Like
 -  Follow 10.1M followers
 -  Follow 844,059
 -  Mashable
 -  Mashable
 - [see more >](#)
- [Search](#)
- [Video](#)
- [Entertainment](#)
- [Culture](#)
- [Tech](#)
- [Science](#)
- [Business](#)
- [Social Good](#)
- [More](#)
 - - Channels
 - [Video](#)
 - [Entertainment](#)
 - [Culture](#)
 - [Tech](#)
 - [Science](#)
 - [Business](#)
 - [Social Good](#)
 - - Company
 - [About Us](#)
 - [Licensing & Reprints](#)
 - [Archive](#)
 - [Mashable Careers](#)
 - - Contact
 - [Contact Us](#)
 - [Submit News](#)
 - - Advertise
 - [Advertise](#)
 - - Legal
 - [Privacy Policy](#)
 - [Terms of Use](#)
 - [Cookie Policy](#)
 - - Resources
 - [Subscriptions](#)
 - - Sites
 - [Job Board](#)
 - [Social Good Summit](#)



Tech

Verge cryptocurrency hack shows, no, blockchain isn't invincible

Share on Facebook Share Tweet on Twitter [Share](#) [Share](#)



Another day, another cryptocurrency hack.

IMAGE: THOMAS TRUTSCHEL / CONTRIBUTOR / GETTYIMAGES

BY [STAN SCHROEDER](#)

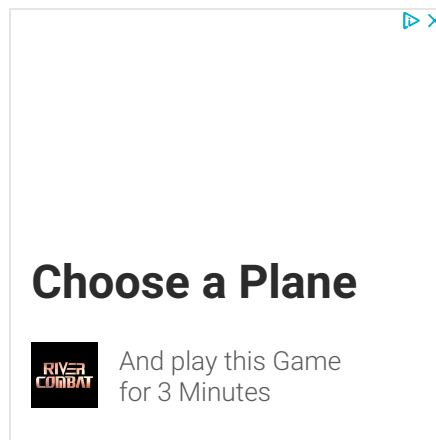
3 DAYS AGO

Privacy-oriented cryptocurrency Verge (symbol: XVG) was apparently hacked Wednesday, with the attacker making off with around 250,000 coins with a value of roughly \$15,000 (though some reports go as high as [\\$1 million](#)).

Compared to some recent crypto-related hacks, this attack was particularly nasty

as it compromised the integrity of Verge's blockchain.

SEE ALSO: [Cryptocurrency exchange puts \\$250,000 bounty on hackers](#)



The attack was discovered by ocminer, a poster on [Bitcointalk](#) forums (via [Bitcoin.com](#)), on Wednesday afternoon. According to him, a hacker used "several bugs" in Verge's code to mine an extraordinarily large number of new blocks in Verge's blockchain, thus rewarding himself with a lot of Verge coins.

Ocminer and several media outlets called this a "51% attack," which is frightening as this type of attack is theoretically possible on other blockchains which rely on a proof-of-work (PoW) validation mechanism, including Bitcoin and Ethereum.

But even though this attacker technically managed to capture the majority of mining power on Verge's network, this type of attack wouldn't work on Bitcoin.

In plain terms: In PoW-based cryptocurrency systems, miners are people who use computing power to validate the transactions on the network and are awarded in new coins. These systems are typically quite robust, but if any one miner (or mining pool) should capture the majority (hence the 51%) of the network's mining power, then they can do all sorts of bad things on the network, including spending coins that were already spent (this is called double spending).

In Verge's particular case, it's a little more nuanced. Verge uses five different cryptographic algorithms for mining, switching to a new one for every block, but the attacker figured out a way to fake timestamps of his blocks and mined them all with one algorithm. In this way, he was able to capture the majority of the network's mining power with far less computing power than he'd normally need.

Nevertheless, the attack is serious as it requires a [hard fork](#) (cryptocurrency lingo for a very big upgrade that leaves the old blockchain behind and requires all participants to switch to new software) to exclude the blocks the attacker had mined.

Verge's official Twitter account tried to downplay the severity of the attack by calling it a "small hash attack" that's been "cleared up now."



But [Reddit](#) and some experts seem to disagree.



And a poster on the Bitcointalk forums called IDCToken, who claims he's responsible for the attack, [said](#) there are two more exploits in the Verge's code that could be used to perform a similar hack.

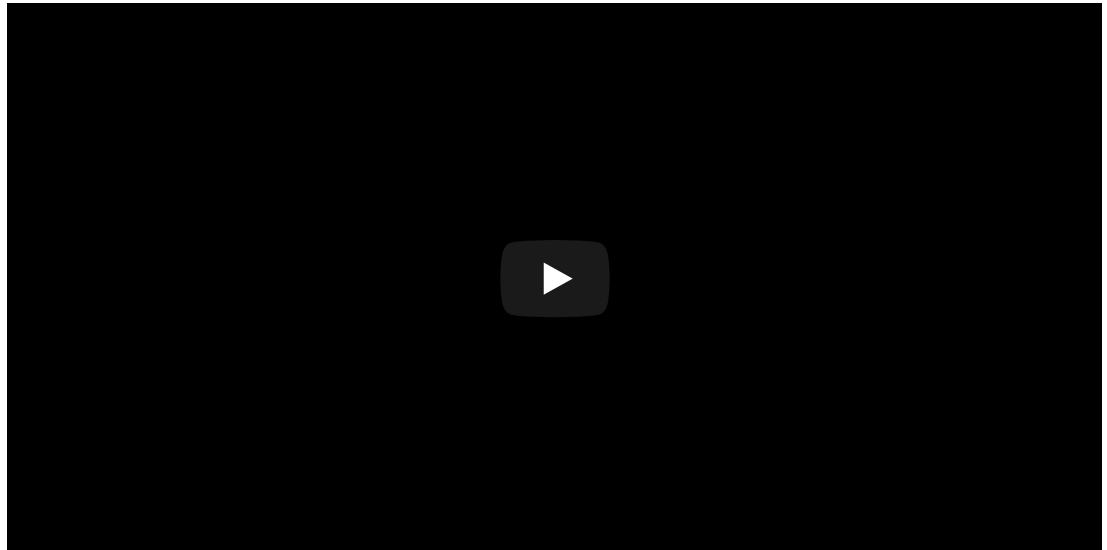
Verge's price fell 14.6% to \$0.0547 at the time of writing according to [CoinMarketCap](#).

The attack on Verge follows a reported [51% attack](#) on another cryptocurrency, Electroneum, though that one didn't appear to result in much damage.

These attacks are notable as they show that even a seemingly foolproof PoW system can be tricked. Ethereum has already had [one hack](#) of large magnitude in its history while Bitcoin has mostly stood the test of time in its nine years of existence, but it'd be imprudent to completely brush off the possibility of this happening to any cryptocurrency, even the most thoroughly tested one.

Disclosure: The author of this article owns, or has recently owned, a number of cryptocurrencies, including BTC and ETH.

WATCH: This bitcoin wallet claims to be hack-proof



TOPICS: [BITCOIN](#), [CRYPTOCURRENCY](#), [ELECTRONEUM](#), [HACK](#), [TECH](#), [VERGE](#)

You May Like

Powered by ZergNet



Can You Answer Elon Musk's Favorite Job Interview Question?

Curiosity.com



What Great Movies Look Like Without Special Effects

Looper.com



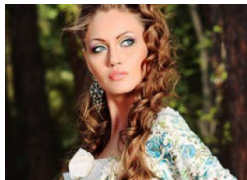
The Real Reason Why There Aren't Any Snakes in Ireland

Irishcentral.com



Why You Should Stop Charging Your Phone Overnight

TLC.com



Messed Up Things You Never Knew Happened in the Victorian Era

Grunge.com



Here's How Stephen Hawking Predicted the World Will End

Nypost.com



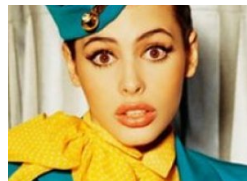
What Happens To Your Body When You Stop Making Love

TheList.com



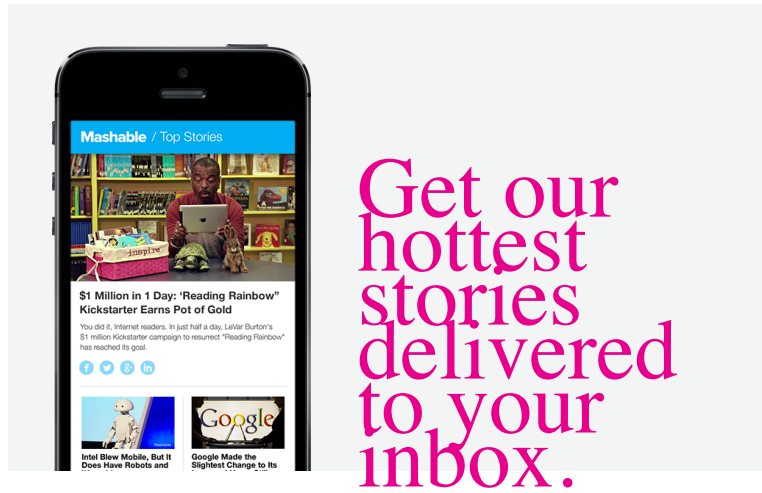
Viking Skeleton's DNA Proves Historians Wrong

Nypost.com

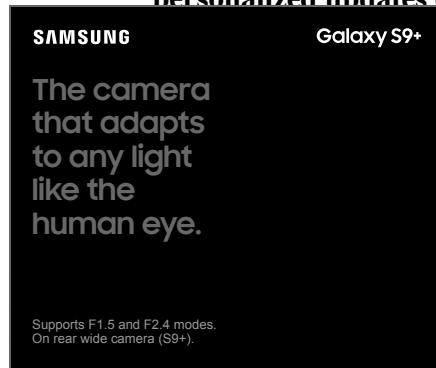


Things People Believed 50 Years Ago That Turned Out to Be Wrong

Grunge.com



Sign up for Mashable
Newsletters to get
personalized updates on top



[Science](#)

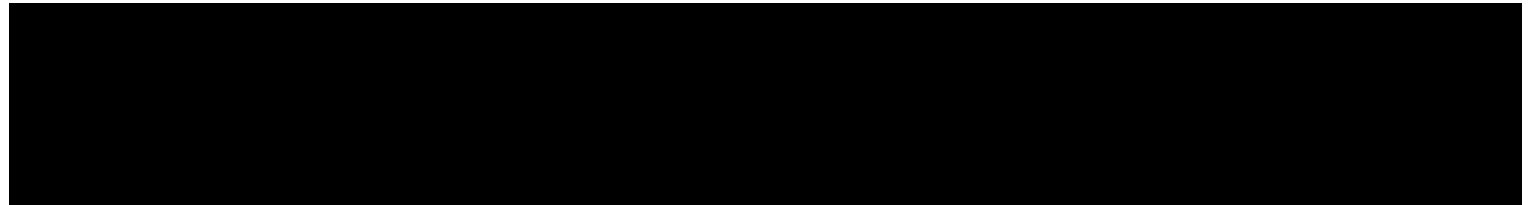
[Hey, how about we helicopter grizzly bears into this remote National Park?](#)

Mark Kaufman

"It ain't easy -- but it sure is possible."

1 day ago

[Share](#) [Tweet](#) [Share](#) [Share](#)





[Continue](#)

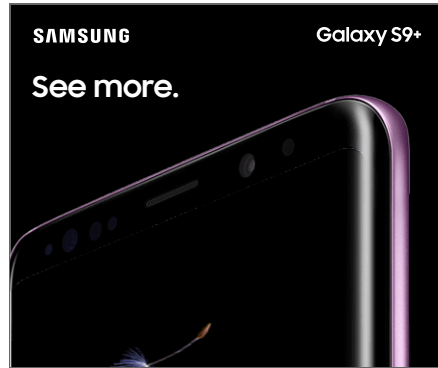
[15 times we screamed while watching Drake's celeb-heavy new video](#)

Laura Vitto

Jourdan Dunn on a horse! Tiffany Haddish smoking cigarettes! Olivia Wilde smashing dishes!

19 hours ago

[Share](#) [Tweet](#) [Share](#) [Share](#)



[Entertainment](#)

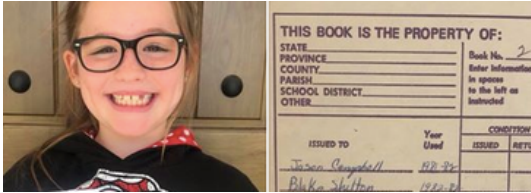
[Watch Kendall Jenner rave about 'Incredibles 2' fashion icon Edna Mode](#)

Laura Vitto

"She's a visionary, a giant – I mean, well, not literally. She comes up to my knees."

1 day ago

[Share](#) [Tweet](#) [Share](#) [Share](#)



[Culture](#)

[Oklahoma mom 'embarrassed' that her child's textbook once belonged to Blake Shelton](#)

Laura Vitto

Her viral post comes amid Oklahoma's multi-day teacher walkout in protest of lacking school funding.

22 hours ago

[Share](#) [Tweet](#) [Share](#) [Share](#)



[Culture](#)

[Prince gets a brand new tribute in the form of a flowering bush](#)

Laura Vitto

Though the mural itself attracted attention back in 2016, it found new online fame after Stein shared a photo of the surrounding the bush in bloom on Twitter.

1 day ago

[Share](#) [Tweet](#) [Share](#) [Share](#)



[Entertainment](#)

'Black Panther' sinks 'Titanic' in the most obvious box office headline ever

Adam Rosenberg

'Black Panther' is now Hollywood's third-biggest box office earner of all time in U.S. theaters.

1 day ago

[Share](#) [Tweet](#) [Share](#) [Share](#)

- [About Us](#)
- [Jobs](#)
- [Advertise](#)
- [Subscribe](#)
- [Privacy](#)
- [Terms](#)

-
-
-
-
-
-
-
-

[Mashable](#) is a global, multi-platform media and entertainment company. Powered by its own proprietary technology, Mashable is the go-to source for tech, digital culture and entertainment content for its dedicated and influential audience around the globe.

- ©2005-2018 Mashable, Inc.
- Mashable is among the federally registered trademarks of Ziff Davis, LLC and may not be used by third parties without explicit permission.
- Designed in collaboration with [Code & Theory](#)