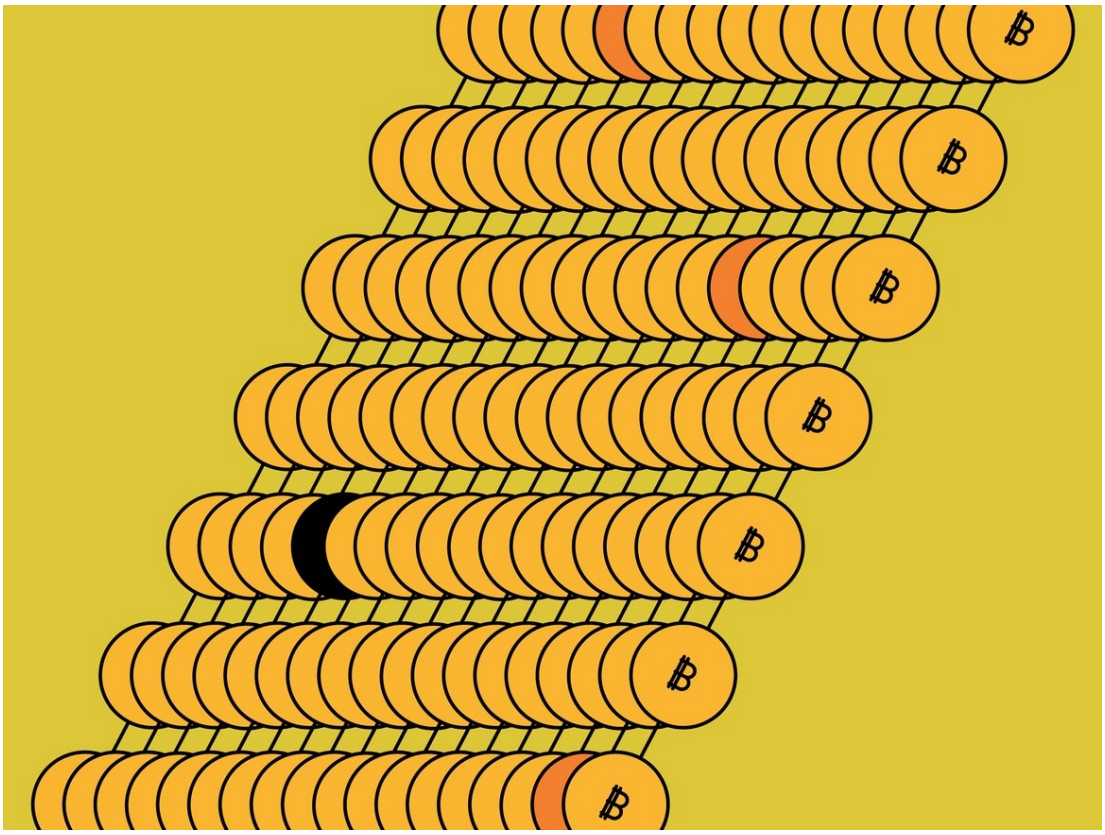
ANDY GREENBERG SECURITY 04.05.18 07:00 AM

A 200-YEAR-OLD IDEA OFFERS A NEW WAY TO TRACE STOLEN BITCOINS



Cambridge researchers point to an 1816 precedent that could fundamentally change how "dirty" Bitcoins are tracked.
HOTLITTLEPOTATO

thousands of computers, of every Bitcoin transaction that's ever taken place. Many of the transactions recorded on that distributed ledger are crimes: Billions of dollars in stolen funds, contraband deals, and paid ransoms sitting in plain sight, yet obscured by unidentifiable Bitcoin addresses and, in many cases, tangles of money laundering.

But a group of Cambridge cybersecurity researchers now argues that one can still distinguish those contraband coins from the legitimate ones that surround them, not with any new technical or forensic technique, but simply by looking at the blockchain differently—specifically, looking at it more like an early 19th century English judge.

In a paper published last week, the Cambridge team argues for a new way of tracing "tainted" coins in the blockchain, particularly ones that have been stolen or extorted from victims and then sent through a series of transactions to hide their ill-gotten origin. Rather than try to offer any new detective tricks to identify the source of a Bitcoin transaction hiding behind a pseudonymous address, their idea instead redefines what constitutes a dirty bitcoin. Based on a legal precedent from an 1816 British court decision, they posit that the first coin that leaves a Bitcoin address should be considered the same coin as the first one that went into it, carrying with it all of that coin's criminal history. And if that coin was once stolen from someone, he or she may be allowed to claim it back even after it has passed through multiple addresses.

'One unlucky person is going to end up holding the stolen bitcoin.'

—ROSS ANDERSON, CAMBRIDGE UNIVERSITY

The Cambridge researchers have gone so far as to code a proof-of-concept software tool, which they plan to release later this year, that can scan the blockchain and, starting from known instances of Bitcoin theft, theoretically identify the same tainted coins, even if they've hopped around the blockchain for years.

"The software we're going to publish will let you know whether your favorite bitcoin was ever owned by Ross Ulbricht or Mt. Gox," says Ross Anderson, the Cambridge computer science professor who leads the research group, referring to the convicted administrator of the Silk Road Bitcoin drug market and the first

MORE SECURITY

PRIVACY

Did Cambridge Analytica Access Your Facebook Data?

BRIAN BARRETT

SOCIAL MEDIA

Most Links to Popular Sites on Twitter Come From Bots

ISSIE LAPOWSKY

PRIVACY

Facebook Messenger's 'Unsend' Feature Feels Half-Baked

LOUISE MATSAKIS

SURVEILLANCE

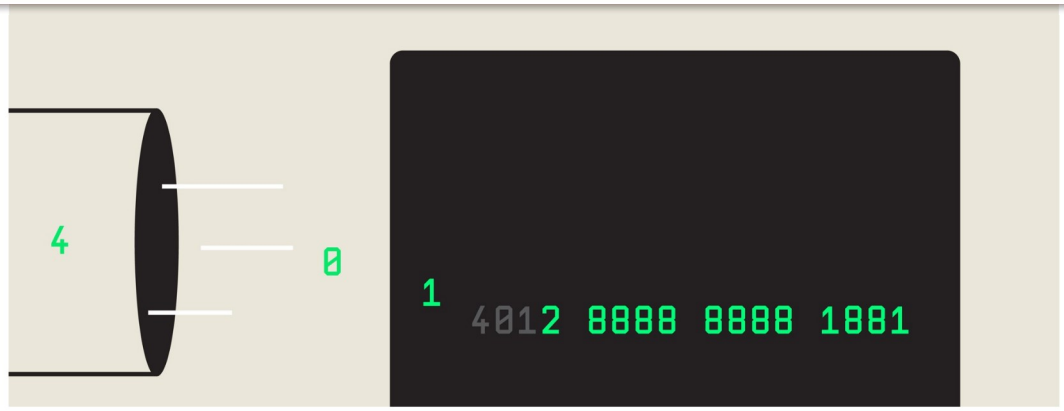
DC's Stingray Mess Won't Get Cleaned Up

LILY HAY NEWMAN

POLICIES

Cyberinsurance Tackles the Unpredictable World of Hacks

JOSEPHINE WOLFF



FIN7

LILY HAY NEWMAN