washingtonpost.com

The long, perplexing search for the creator of Bitcoin just took another weird turn

https://www.facebook.com/sarah.kaplan.31

Play Video1:29

One step closer to unmasking Bitcoin's creator?

Who is the man behind bitcoin? It's a question that's puzzled the cybersphere ever since the virtual currency was created in 2009. But tech magazine Wired now claims to have solved the riddle, naming its creator as Australian entrepreneur and academic Craig Steven Wright. (Reuters)

On Tuesday afternoon, separately and within two hours of each other, two well-known tech websites suggested that they'd solved a mystery that had eluded the online world for more than half a decade.

They'd found "Satoshi Nakamoto," the pseudonymous creator of Bitcoin.

He was an Australian named Craig Steven Wright, a 44-year-old former academic "nobody," as Wired put it. Wright had never before appeared on the public lists of any Nakamoto-hunters and yet troves of leaked (or perhaps hacked) documents published by both Wired and the tech blog Gizmodo seemed to point to him.

Within hours of the two stories' publication, Wright's online presence had all but vanished, Gizmodo reported, and Australian authorities were raiding Wright's suburban Sydney home.

In a statement to the Associated Press, Australian Federal Police said the searches were related to a tax investigation, not the recent articles linking Wright to Bitcoin

But the media reports and subsequent raid have thrown the virtual currency and its inscrutable founder back in the spotlight. And if the events of the past two days seem oddly timed, they're hardly more bizarre than any that have occurred in the lengthy hunt for "Nakamoto" since Bitcoin launched seven years ago.

The open source software for Bitcoin, which allows users to make online transactions anonymously and without going through banks or other financial institutions, was released in 2009. It started out more resembling monopoly money than real currency — people would trade the "coins" (really just lines of code) for favors or even give them away. But as the exotic system gained popularity, it gained value.

Now anyone — tech nerds, central bank-averse Libertarians, criminals — can use bitcoins for anything from ordering pizza to trafficking drugs. Their value fluctuates wildly, but at the moment one is worth about $415, according to the AP.

But as the currency became a financial force unto itself, its creator — a person or group of people calling themselves "Satoshi Nakamoto," though there are no known coders who go by that name — remained enigmatic.

"Back then, it was not clear that creating Bitcoin might be a legal thing to do," Bitcoin's chief scientist, Gavin Andresen, told Newsweek last year. "[Nakamoto] went to great lengths to protect his anonymity."

Then, in 2011, with a message to a developer that read simply, "I've moved on to other things," Nakamoto disappeared, leaving fans of the currency and nosy tech journalists with few clues as to his, her or their true identity.

 A bitcoin logo is displayed at the Inside Bitcoins conference and trade show, Monday, April 7, 2014 in New York. (AP Photo/Mark Lennihan)

Here's what we do know:

In his initial writings about Bitcoin, Nakamoto claimed to be a 36-year-old from Japan who had been driven by anger about the 2008 financial crisis to try and invent an alternative. But many Nakamoto-hunters believe their man (or woman) is a native English speaker: the person who blogged about Bitcoin extensively before signing off in 2011 wrote in flawless English and tended to use British spellings — "colour," "grey" — once described something as "bloody hard" and embedded a reference to the Times of London into the "genesis" lines of code that got the currency started, according to the New Yorker.

In 2011 Stefan Thomas, a Swiss coder and active member of the Bitcoin community, graphed the time stamps for each of Nakamoto's 500-plus bitcoin forum posts. He found, according to Wired, that Nakamoto was rarely writing between 5 a.m. and 11 a.m. Greenwich Mean Time (midnight to 6 a.m. Eastern Standard Times), even on Saturdays and Sundays. Perhaps the elusive currency creator was an East Coaster who slept during those hours?

But those hints are largely circumstantial. The potentially biggest clue is a million-coin trove stored behind an encrypted signature known as a PGP key. The stash is plainly visible in public record of all bitcoin transactions called the "block chain" and is widely thought to belong to Nakamoto, according to Wired.

Someone moving coins from that trove would offer the best confirmation that they were the real Nakamoto. But the release of $400 million worth of bitcoins would also likely destabilize the currency and throw the online financial world into chaos.

So far, the stash remains untouched.

It is with this scant evidence that Nakamoto hunters go seeking their elusive target — so far, with little luck. Writing in the New Yorker in 2011, Joshua Davis floated the idea that Irish cryptography student Michael Clear might be responsible for Bitcoin; he emphatically denied it.

"I'm not Satoshi," Clear told Davis. "But even if I was I wouldn't tell you."

Later that year, Fast Company ran its own investigation, searching the web for key phrases pulled from Nakamoto's initial Bitcoin paper, based on the logic that writers tend to repeat favorite phrases. That brought up a patent for an encrypted communication system. But when the reporter contacted the three men who filed the patent, they too denied any involvement. One said he had to look "Bitcoin" up on Wikipedia to figure out what it was.

Other suspects include: Andresen, a prominent developer for Bitcoin and the chief scientist of the Bitcoin Foundation, "the closest thing to a central authority in the world of Bitcoin," in the words of

the MIT Tech Review; Shinichi Mochizuki, a brilliant Japanese American mathematician who once solved one of the world's hardest math problems, quietly posted his solution on the Internet, and walked away; Jed McCaleb, who started the world's largest bitcoin exchange; and Nick Szabo, a cryptographer and legal scholar who had been working on digital currency for more than a decade before Bitcoin was launched.

Then there's Hal Finney, the first person to actually use Bitcoin — aside, of course, from Nakamoto himself. A reporter for Forbes had a language analysis firm compare Finney's writing to the creator's fluid blog posts, and found a surprising degree of similarity. What's more, Finney had talked about the idea of a digital currency on email lists as far back as the early '90s, and he helped develop PGP — the encryption program that protects, among millions of other files, Nakamoto's million-bitcoin stash.

But Finney responded to Forbes' questions the way they all did.

"I'm flattered but I deny categorically these allegations," he wrote in an email. "I don't know what more I can say."

The splashiest — and most disastrous — declaration of Nakamoto's true identity came last year, when Newsweek ran a cover story titled "The Face Behind Bitcoin."

The true identity of Satoshi Nakamoto, reporter Leah McGrath

Goodman [wrote](), was a 64-year-old Californian named Satoshi Nakamoto, though he now went by Dorian. He was trained as a physicist and a veteran of a long career in engineering and military related projects, plus he had the libertarian bent that characterizes so many Bitcoin admirers. In a confrontation with Goodman in front of his home and two Temple City, Calif. police officers (who confirmed the quote), he seemed to tacitly acknowledge his involvement.

"I am no longer involved in that and I cannot discuss it," he said "It's been turned over to other people. They are in charge of it now. I no longer have any connection."

But after Newsweek's story ran and reporters began [clamoring for interviews]() — resulting in a car chase through the streets of Los Angeles — he quickly reached back out to the magazine with a [statement]() via his lawyer: Dorian Nakamoto had nothing to do with Bitcoin, he thought that Goodman was referring to his military projects, he wanted all this attention to go away.

Just after that, [a statement appeared]() from the "real" Satoshi Nakamoto's in an Bitcoin forum: "I am not Dorian Nakamoto."

There was a bit of a lull in purported Nakamoto-outings after the dust settled from the Newsweek debacle. If anything, the incident seemed to illustrate just how perilous any claims to have found the elusive creator can be — after all, it really did seem like Dorian

Nakamoto had admitted to being involved.

But Wired and Gizmodo seem to believe the evidence that Wright and his friend American computer forensics analyst David Kleiman, who died in 2013, are behind Bitcoin was worth taking a risk for.

Their assertion relies mostly on documents leaked by people close to Wright, including a transcript from a conversation between Wright, his attorney and the Australian Taxation Office in which Wright says, "I did my best to try and hide the fact that I've been running bitcoin since 2009. By the end of this I think half the world is going to bloody know."

It's not clear whether the same person leaked the documents to both Wired and Gizmodo — some details of their reports differ. Wired also uncovered a liquidation report on a company Wright owned that showed he'd invested several millions of dollars in bitcoins in the company — "a strangely large stash for an unknown player in the bitcoin world," Wired said.

Wright did not respond to requests for comment from either site.

Both reports acknowledge that the leaked documents could be a hoax, particularly Wired.

"But this much is clear," Wired reported. "If Wright is seeking to fake his Nakamoto connection, his hoax would be practically as

ambitious as bitcoin itself."

Other tech sites have already thrown some cold water on Wired and Gizmodo's reveals (Motherboard, for example, wrote a lengthy analysis of disparities in PGP codes, about 20 percent of which is intelligible to the lay Bitcoin observer).

But the fact remains that people desperately want to know who Nakamoto is. Bitcoin is currently dealing with a dispute about how currency is created, and some would like Nakamoto re-emerge to intervene, according to the AP. There's also the matter of the PGP-protected stash of $400 million in bitcoin that could totally alter the market.

And then there's the fact that so many Bitcoin users are computer scientists and cryptographers, people who have built worlds online and delight in deconstructing others'.

Nakamoto is yet another cipher. Just begging to be solved.