

ANDY GREENBERG AND GWERN BRANWEN SECURITY 12.08.15 4:25 PM

# BITCOIN'S CREATOR SATOSHI NAKAMOTO IS PROBABLY THIS UNKNOWN AUSTRALIAN GENIUS



Adam Voorhes | Gail Anderson + Joe Newton

**EVEN AS HIS** face towered 10 feet above the crowd at the Bitcoin Investor's Conference in Las Vegas, Craig Steven Wright was, to most of the audience of crypto and finance geeks, a nobody.

The 44-year-old Australian, Skyping into the D Hotel ballroom's screen, wore the bitcoin enthusiast's equivalent of camouflage: a black blazer

and a tieless, rumpled shirt, his brown hair neatly parted. His name hadn't made the conference's list of "featured speakers." Even the panel's moderator, a bitcoin blogger named Michele Seven, seemed concerned the audience wouldn't know why he was there. Wright had hardly begun to introduce himself as a "former academic who does research that no one ever hears about," when she interrupted him.

"Hold on a second, who are you?" Seven cut in, laughing. "Are you a computer scientist?"

"I'm a bit of everything," Wright responded. "I have a master's in law...a master's in statistics, a couple doctorates..."

"How did you first learn about bitcoin?" Seven interrupted again, as if still trying to clarify Wright's significance.

Wright paused for three full seconds. "Um. I've been involved with all this for a long time," he stuttered. "I—try and stay—I keep my head down. Um..." He seemed to suppress a smile. The panel's moderator moved on. And for what must have been the thousandth time in his last seven years of obscurity, Wright did not say the words WIRED's study of Wright over the past weeks suggests he may be dying to say out loud.

"I am Satoshi Nakamoto, the creator of bitcoin."

Since that pseudonymous figure first released bitcoin's code on January 9th, 2009, Nakamoto's ingenious digital currency has grown from a nerd novelty to a kind of economic miracle. As it's been adopted for everything from international money transfers to online narco-trafficking, the total value of all bitcoins has grown to nearly \$5 billion. Nakamoto himself, whoever he is, appears to control a stash of bitcoins easily worth a nine-figure fortune (it rose to more than a billion at the cryptocurrency's peak exchange rate in 2014). But the true identity of bitcoin's creator remains a cipher. Media outlets from the *New Yorker* to *Fast Company* to *Newsweek* have launched investigations into unmasking Nakamoto that were either inconclusive or, in *Newsweek's* case, pointed to a man who subsequently denied having anything to do with cryptography, not to mention

cryptocurrency. Altogether, the world's Satoshi-seekers have hardly put a dent in one of the most stubborn mysteries of the 21st century, one whose answer could resonate beyond a small sphere of crypto geeks and have real economic effects.

In the last weeks, WIRED has obtained the strongest evidence yet of Satoshi Nakamoto's true identity. The signs point to Craig Steven Wright, a man who never even made it onto any Nakamoto hunters' public list of candidates, yet fits the cryptocurrency creator's profile in nearly every detail. And despite a massive trove of evidence, we still can't say with absolute certainty that the mystery is solved. But two possibilities outweigh all others: Either Wright invented bitcoin, or he's a brilliant hoaxer who very badly wants us to believe he did.



## The Evidence

The first evidence pointing to Wright appeared in mid-November, when an anonymous source close to Wright began leaking documents to Gwern Branwen, a pseudonymous, independent security researcher and dark web analyst. Branwen provided those documents to WIRED, and

they immediately led to several direct, publicly visible connections between Nakamoto and Wright:

- An August 2008 post on Wright's blog, months before the November 2008 introduction of the bitcoin whitepaper on a cryptography mailing list. It mentions his intention to release a "cryptocurrency paper," and references "triple entry accounting," the title of a 2005 paper by financial cryptographer Ian Grigg that outlines several bitcoin-like ideas.
- A post on the same blog from November, 2008. It includes a request that readers who want to get in touch encrypt their messages to him using a PGP public key apparently linked to Satoshi Nakamoto. A PGP key is a unique string of characters that allows a user of that encryption software to receive encrypted messages. This one, when checked against the database of the MIT server where it was stored, is associated with the email address `satoshin@vistomail.com`, an email address very similar to the `satoshi@vistomail.com` address Nakamoto used to send the whitepaper introducing bitcoin to a cryptography mailing list.
- An archived copy of a now-deleted blog post from Wright dated January 10, 2009, which reads: "The Beta of Bitcoin is live tomorrow. This is decentralized... We try until it works." (The post was dated January 10, 2009, a day *after* Bitcoin's official launch on January 9th of that year. But if Wright, living in Eastern Australia, posted it after midnight his time on the night of the 9th, that would have still been before bitcoin's launch at 3pm EST on the 9th.) That post was later replaced with the rather cryptic text "Bitcoin - AKA bloody nosey you be...It does always surprise me how at times the best place to hide [is] right in the open." Sometime after October of this year, it was deleted entirely.



## Cracked, inSecure and Generally Broken

*The ravings of a SANS/GIAC GSE (Compliance & Malware) For more information on my role as a presenter and commentator on IT Security, Digital Forensics Statistics and Data Mining; E-mail me:*

Dr. Craig S Wright  
GSE

Craig Wright

facebook



Name:  
Craig S Wright

Email:

Status:  
None

Create Your Badge

SATURDAY, 10 JANUARY 2009


### Bitcoin

Well.. e-gold is down the toilet. Good idea, but again centralised authority.

The Beta of Bitcoin is live tomorrow. This is decentralized... We try until it works.

Some good coders on this. The paper rocks. <http://www.bitcoin.org/bitcoin.pdf>

Posted by Craig Wright at [Saturday, January 10, 2009](#) [0 comments](#)

A screenshot from Craig Wright's blog showing his apparent plan to launch Bitcoin. The post has since been removed.  WIRED

In addition to those three blog posts, we received a cache of leaked emails, transcripts, and accounting forms that corroborate the link. There's a leaked message from Wright to his lawyer date June 2008 in which Wright imagines "a P2P distributed ledger"—an apparent reference to bitcoin's public record of transactions known as the blockchain, long before it was publicly released. The email goes on to reference a paper called "Electronic Cash Without a Trusted Third Party" that Wright expects to release in 2009.

Another leaked email from Wright to computer forensics analyst David Kleiman, a close friend and confidant, just before bitcoin's January 2009 launch discusses a paper they'd been working on together. Wright talks about taking a buyout from his job and investing in hundreds of computer processors to "get [his] idea going." There's also a PDF authored by Kleiman, who died in April of 2013, in which he agrees to

take control of a trust fund, codenamed the “Tulip Trust,” containing 1.1 million bitcoins. The PDF is signed with Kleiman’s PGP signature, a cryptographic technique that ensures it couldn’t have been altered post-signature.

That million-coin trove—The Tulip Trust—is the same size as a mysterious bitcoin fortune that’s long been visible on bitcoin’s blockchain and widely attributed to Satoshi Nakamoto. No one but Nakamoto is known to have assembled such a massive hoard of the cryptocurrency, and only Nakamoto could have generated so many bitcoins so early in its evolution, when a bitcoin could be “mined” with relatively small amounts of processing power. Only one such bitcoin megapile exists, and the closely-watched coins haven’t moved in bitcoin’s entire history.

---

## MORE BITCOIN:

---

Bitcoin Survival Guide: Everything You  
Need to Know About the Future of Money

---

The Rise and Fall of Bitcoin

---

Everyone Says Bitcoin Is Back. But It  
Never Really Left

---

Another clue as to Wright’s bitcoin fortune wasn’t leaked to WIRED but instead remains hosted on the website of the corporate advisory firm McGrathNicol: a [liquidation report](#) on one of several companies Wright founded known as Hotwire, an attempt to create a bitcoin-based bank. It shows that the startup was backed in June 2013 by \$23 million in bitcoins owned by Wright. That sum would be worth more than \$60 million today. At the time of the company’s incorporation, Wright’s investment in that one firm alone represented more than 1.5 percent of all existing bitcoins, a strangely large stash for an unknown player in

the bitcoin world.

The giveaways go on: There's a leaked email from Wright to an associate in January 2014 about a tax dispute with the Australian government. In it, he seems to consider using Nakamoto's name to wield influence with New South Wales Senator Arthur Sinodinos "Would our Japanese friend have weight coming out of retirement?" Wright asks. It includes a draft email to the senator signed "Satoshi Nakamoto." And a leaked transcript of Wright's meeting with attorneys and tax officials in February 2014 quotes him in a moment of exasperation: "I did my best to try and hide the fact that I've been running bitcoin since 2009," Wright says. "By the end of this I think half the world is going to bloody know."

## Making Contact

On December 1st, WIRED sent an encrypted email to Wright suggesting that we knew his secret and asking for a meeting. A few hours later, we received a wary response from the address Tessier-Ashpool@AnonymousSpeech.com, a cyberpunk reference to a rich and powerful corporate dynasty in William Gibson's *Sprawl* trilogy. Wright had referenced the same fictional family in the bio of his private twitter profile. The email's IP showed that it came from an IP address in Panama controlled by Vistomail, the same service that Satoshi Nakamoto had used to send his emails introducing bitcoin and to run Bitcoin.org. "This is a throw away account. There are ways even with [the anonymity software] Tor, but the people in Panama are extremely [sic] good and do not violate people's desired privacy," the email read. "You are digging, the question is how deep are you?" The message ended, "Regards, the Director of Tessier-Ashpool"

A few hours later, we received another, even more perplexing message from the same account. "The nature of this moniker is selected for a purpose. I now have resources. This makes me a we now. I am still within that early phase of learning just what my capabilities happen to

be. So, even now with resources I remain vulnerable,” it read. “You seem to know a few things. More than you should.”

When we responded by describing the three blog posts that showed Wright’s clear connection to bitcoin’s creation and asking again for a meeting, he gave a revealing answer. “Although we all desire some level of credit, I have moved past many of these things,” read his response from the same Tessier-Ashpool account. “Too many already know secrets, the world does not need to know. There are other means to lead change than to be a dictator.”

After our second followup message asking for a chance to talk, Wright responded that he would consider our request. Then he stopped responding altogether.

## Dropping Breadcrumbs?

Despite that overwhelming collection of clues, none of it fully proves that Wright is Nakamoto. All of it could be an elaborate hoax—perhaps orchestrated by Wright himself. The unverified leaked documents could be faked in whole or in part. And most inexplicably of all, comparisons of different archived versions of the three smoking gun posts from Wright’s blog show that he did edit all three—to *insert* evidence of his bitcoin history. The PGP key associated with Nakamoto’s email address and references to an upcoming “cryptocurrency paper” and “triple entry accounting” were added sometime after 2013. Even the post noting bitcoin’s beta launch is questionable. While it was ostensibly posted in January 2009, it later seems to have been deleted and then undeleted—or possibly even written for the first time—sometime between October 2013 and June of 2014.

Why those breadcrumbs were dropped remains a mystery. Is Wright trying to falsely steal Nakamoto’s glory (or money)? Is he quietly revealing himself as bitcoin’s creator?

But this much is clear: If Wright is seeking to fake his Nakamoto



connection, his hoax would be practically as ambitious as bitcoin itself. Some of the clues added to his blog were made more than 20 months ago—a very patient deception if it were one. His references to Grigg’s “triple entry accounting” paper would represent an uncannily inventive lie, representing a new and obscure possible inspiration for bitcoin. And there’s little doubt Wright is a certified bitcoin mogul. Even the \$60 million portion of his cryptocurrency stash that’s verifiable in McGrathNicol’s public audit record is suspiciously large.

More circumstantially, Wright’s blog, his public records, and his verified writings on mail lists and Twitter sketch a man who matches with Satoshi Nakamoto’s known characteristics well enough to place him leagues above other candidates. He’s a former subscriber to the 1990s “cypherpunks” mailing list devoted to anti-authoritarianism and encryption, an advocate of gold as a financial tool, an accomplished C++ coder, a security professional plausibly capable of writing a tough-to-hack protocol like bitcoin, a libertarian who battled with tax authorities, and a fan of Japanese culture.

He is also—parallels to Nakamoto aside—a strange and remarkable person: an almost obsessive autodidact and double-PhD who once boasted of obtaining new graduate degrees at a rate of about one a year. He’s a climate-change denier, a serial entrepreneur who started companies ranging from security consultancies to a bitcoin bank, and an eccentric who wrote on his blog that he once accepted a challenge to create a pencil from scratch and spent years on the problem, going so far as to make his own bricks to build his own kiln in which to mix the pencil’s graphite.



Wright's blogging and leaked emails describe a man so committed to an unproven cryptocurrency idea that he mortgaged three properties and invested more than \$1 million in computers, power, and connectivity—even going so far as to lay fiberoptic cables to his remote rural home in eastern Australia to mine the first bitcoins. His company, Tulip Trading, built two supercomputers that have officially ranked among the top 500 in the world, both seemingly related to his cryptocurrency projects. (Wright seems to enjoy tulip references, a likely taunt at those who have compared bitcoin to the Netherlands' 17th century “tulip bubble.”) The first of those supercomputers he named Sukurinuto Okane—Japanese for “script money.” Another, named Co1n, holds the title of the world's most powerful privately owned supercomputer. As Wright told the Bitcoin Investor's conference, he's applying that second machine towards the mysterious task of “modeling Bitcoin's scalability,” and meanwhile building an even more powerful supercomputing cluster in Iceland because of its cheap geothermal power.

Bitcoin watchers have long wondered why the giant cache of coins they attribute to Satoshi Nakamoto never moved on the bitcoin's publicly visible blockchain. Wright's “Tulip” trust fund of 1.1 million bitcoins may hold the key to that mystery. The trust fund PDF signed by Wright's late friend David Kleiman keeps those coins locked in place until 2020, yet gives Wright the freedom to borrow them for applications including

“research into peer-to-peer systems” and “commercial activities that enhance the value and position of bitcoin.”

Despite those exceptions to the trust’s rules, the million-coin hoard has yet to budge, even after Kleiman’s death in 2013. That may be because Wright could be keeping the coins in place as an investment. He could be leveraging the trust in less visible ways, like legally transferring ownership of money to fund his companies while still leaving it at the same bitcoin address. Or he might still be waiting for January 1st, 2020, a countdown to a date that could take the lid off the biggest cryptocurrency fortune in history.

## Coming Clean

In spite of all the clues as to Wright’s possible secret life—some that he apparently placed himself—Wright has demonstrated such a talent for obfuscation and a love of privacy that he’s never even raised the suspicions of most Nakamoto-worshipping bitcoiners. “If we don’t want to go out there and say ‘I’m a billionaire,’ or ‘I’m running XYZ,’ or ‘this is my life,’ I shouldn’t have to tell people that,” Wright told the Las Vegas crowd in October when an audience member asked his thoughts about what bitcoin means for property rights. “We should be able to choose how we live.”

In the leaked emails, Wright seems to bristle at the few times anyone has attempted to out bitcoin’s creator. “I am not from the bloody USA! Nor am I called Dorian [sic],” reads a message from Wright to a colleague dated March 6, 2014. That’s the same day as *Newsweek*’s largely discredited story claimed the inventor of bitcoin to be the American Dorian Satoshi Nakamoto.

Wright seemed to take personal offense at the *Newsweek* story. “I do not want to be your posterboy. I am not found and I do not want to be,” he writes in another message the same day. The email, addressed to a colleague and titled “please leak,” may have been an early draft of the Nakamoto’s posted denial of *Newsweek*’s story. That public denial, a

rare message from Nakamoto posted from his account on the P2P Foundation forum, simply read “I am not Dorian Nakamoto.” But Wright’s private response was far angrier. “Stop looking... Do you know what privacy means? A gift freely given is just that and no more!”

At times, however, Wright has seemed practically envious of Nakamoto. “People love my secret identity and hate me,” he complained to Kleiman in a leaked email from 2011. “I have hundreds of papers. Satoshi has one. Nothing, just one bloody paper and I [can’t] associate myself with ME!”

If Wright is bitcoin’s creator, the revelation of his work carries more importance than merely sating the curiosity of a few million geeks. The bitcoin economy would need to consider that if his million-bitcoin trust unlocks in 2020, Wright and those to whom he may have assigned hundreds of thousands of bitcoins would be free to sell them on the open market, potentially tanking the cryptocurrency’s price; debates within the bitcoin community like the current fracas over bitcoin’s “block size” may look to long-lost Nakamoto for guidance; the world would have to grapple with the full scope of Wright’s vision when he unleashes the result of his companies’ post-bitcoin research. The other suspected Satoshis may finally get a reprieve from nosey reporters like us. And the intellectual history of cryptocurrencies would be forever rewritten.

Wright himself, despite his hostile response to Satoshi-seekers, has lately seemed to be dropping clues of a double life. In the last two years he’s started to write more frequently about bitcoin on his blog; he’s even peppered Twitter with hints (Though he also deleted many of those earlier this month and made his tweets private.)

**WIRED**

SUBSCRIBE

they do not  
als,” he

wrote in one tweet in October.

When a UCLA professor nominated Satoshi Nakamoto for a Nobel Prize earlier this month—and he was declared ineligible due to the mystery of his identity—Wright lashed out. “If Satoshi-chan was made for an ACM turing price [sic] or an Alfred Nobel in Economics he would let you bloody know that,” he wrote on twitter, using the Japanese “chan” suffix that indicates familiarity or a nickname.

“I never desired to be a leader but the choice is not mine,” reads a third recent tweet from Wright. “We are a product of the things we create. They change us.”

In one cryptic and meandering blog post in September in which Wright takes stock of his long career, he even seems to concede that no one can build and wield the wealth that Satoshi Nakamoto has amassed and remain hidden indefinitely. “There is a certain power and mystery in secrets,” Wright mused.

“Am slowly coming to the realisation and acceptance,” he added, “No secret remains forever.”

---

#BITCOIN #DIGITAL CURRENCY #SATOSHI NAKAMOTO

---



VIEW COMMENTS

## SPONSORED STORIES



### HOW TO SPEND IT

A second-hand marketplace for chic collectibles



**MANSION GLOBAL**

Inside the Ritz-Carlton Residences, Miami Beach

**WEBIOT**

13 Little Known Free Programs Any LifeHacker Must Try

**MANSION GLOBAL**

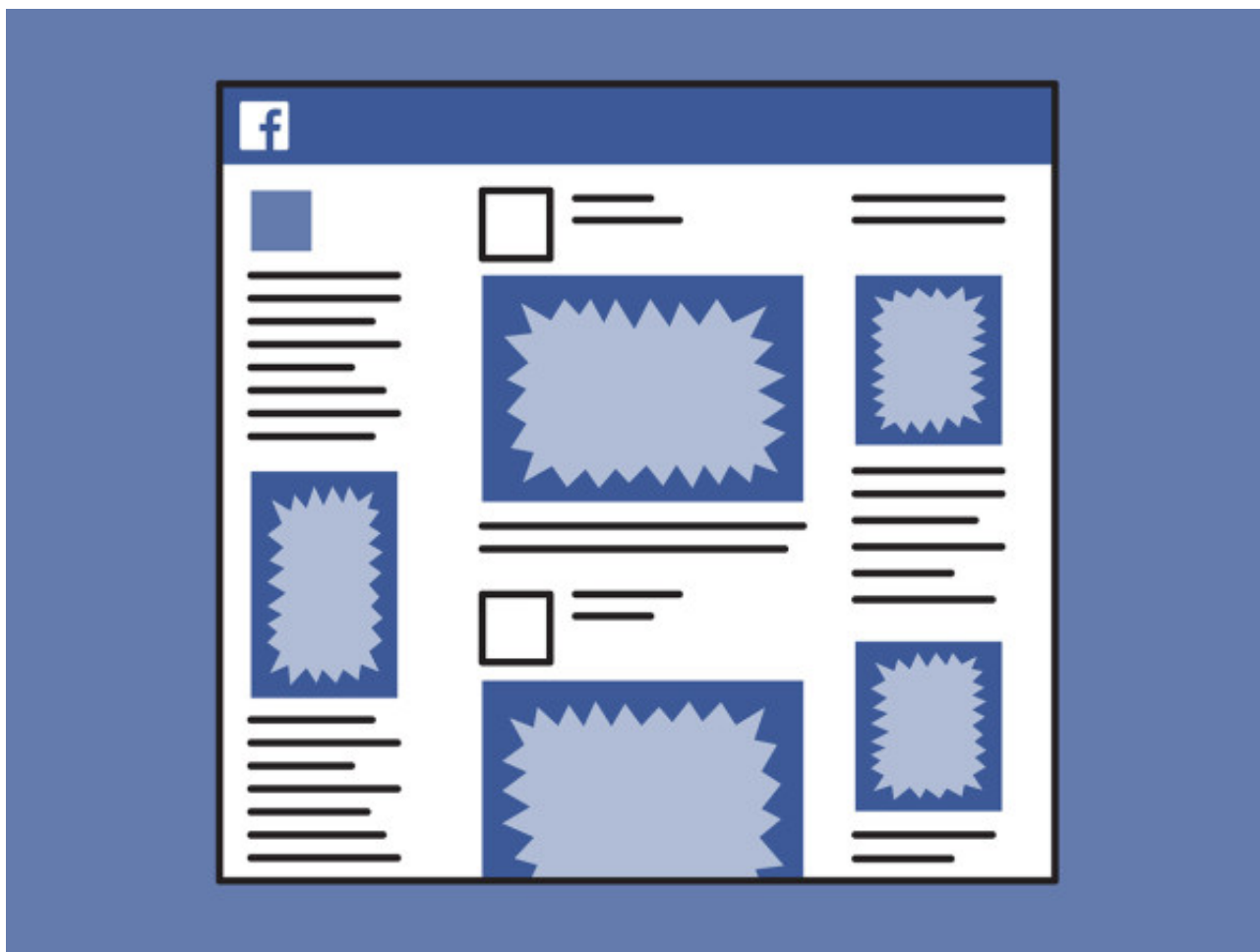
China's Losses Could Be London's Gain

**TALKMARKETS**

How I Used The Force To Save My Business

POWERED BY OUTBRAIN

## MORE SECURITY



## SECURITY THIS WEEK

**Security News This Week: Facebooking at Work Can No Longer Be Charged as 'Hacking'**

12.05.15



## SECURITY

**Variety Jones, Alleged Silk Road Mentor, Arrested in Thailand**

12.04.15

---



EXPLAINED

## Answers to Your Burning Questions on the Ashley Madison Hack

08.21.15

---



HACKS

## Anonymous Leaks Paris Climate Summit Officials' Private Data

12.03.15

---





## SECURITY

**Hacker Leaks Customer Data After a United Arab Emirates Bank Fails to Pay Ransom**

12.03.15

## WE RECOMMEND



CADE METZ

Google's Quantum Computer Just Got a Big Upgrade



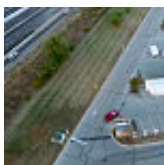
CADE METZ

The Porn Business Isn't Anything Like You Think It Is



BRIAN BARRETT

The OnePlus X Is a Steal—And That's Why It's So Hard to Buy

**ALEX DAVIES**

Obviously Drivers Are Already Abusing Tesla's Autopilot

**MANSION GLOBAL**

Michael Jackson's 'Neverland' Estate Courts Chinese Buyers

POWERED BY OUTBRAIN

## FOLLOW US ON FACEBOOK

Don't miss our latest news, features and videos.



FOLLOW

**WIRED**

SUBSCRIBE



ADVERTISE	SITE MAP
PRESS CENTER	FAQ
CUSTOMER CARE	CONTACT US
NEWSLETTER	WIRED STAFF
JOBS	RSS

Use of this site constitutes acceptance of our [user agreement](#) (effective 3/21/12) and [privacy policy](#) (effective 3/21/12). [Affiliate link policy](#). [Your California privacy rights](#). The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written [permission of Condé Nast](#).

---