

## Is Craig Wright the multimillionaire genius behind bitcoin?

- 



Is this man the multimillionaire genius behind bitcoin: the digital currency now worth over £8bn and threatening to do for banks what Uber did to cab offices? Or does he just really want people to believe he is?



Photography by **Nick Wilson**

Just f\*\*\* off! Either validate or f\*\*\* off right now!"

The computer scientist, [Craig Wright](#), had stood up and was displaying the universal sign to tell someone to f\*\*\* off (the V), while also backing this up by repeatedly shouting it. A broad 45-year-old Australian man with TV hair, he wore a boxy, dark-grey business suit, wide gold tie and red socks that

now matched the colour of his face. He claimed to be the inventor of bitcoin, the first genuinely successful virtual currency in the world. In total, it is now worth over \$10 billion (£8bn), and he personally possessed a fortune of more than \$672 million of them - assuming his identity wasn't also virtual. This is what we were here to confirm. It was not going well.

"F\*\*\* off!"

Until this point, the creator of bitcoin was known only under the pseudonym of Satoshi Nakamoto, ostensibly a 37-year-old male living in Japan. Perhaps due to that, or perhaps due to his blog posts, which were precise, calm and erudite, Nakamoto was imagined to be a gentle, even shy, individual. This was not proving to be the case.

The object of Wright's ire was Dr Nicolas T Courtois, a French-Polish expert in cryptology, code-breaking, virtual currencies and specifically bitcoin, who was sitting to my right. He was here as GQ's expert witness, having made the short walk from his office at University College London, where he lectures, to the offices on the fourth floor of a narrow building on Tottenham Court Road. A big man who spoke in halting English, he wore a smart shirt and boasted trousers so blue they looked like they were part of a costume. The other people in the room were economist and Bitcoin Foundation founding director Jon Matonis, who was the expert witness for the PR agency brokering the interview, and its two representatives, who were attempting not to look too panicked.

We were barely eight minutes in when Wright took issue with Dr Courtois' suggestion that his evidence was not conclusive.

"You've got this one thing," said Wright. "If you don't like it, then f\*\*\* off."

There was an audible groan from the PR side of the room.

"No more bullshit. F\*\*\* off!" he shouted a few moments later, when it was suggested the evidence he was presenting could have been compromised or stolen.

"It's absolutely possible," countered Courtois.

"F\*\*\* off. F\*\*\* off."

"I have over 100 papers in cryptography..."

"Over. F\*\*\* off."

It was at this point he walked out.

GQ had first been approached over a month before about the interview. The deal was this: the fabled inventor of bitcoin would unveil himself to be Craig Wright. The BBC and the Economist would do news stories; we would do the profile piece.

The search for Nakamoto, I knew, had become the digital age's hunt for the white whale. Imagine if the inventor of Facebook was still unknown and you get the idea.

Every so often a publication would dispatch another willing Captain Ahab, and each would return having spotted him, just rarely the same one. Everyone from the New Yorker (which named a student) to Vice (which named the US government) had been on the hunt. The New York Times put an author of a book about bitcoin's creation (Digital Gold's Nathaniel Popper) on the case, who named cryptographer Nick Szabo, and cornered him in a kitchen at a tech gathering, putting it to him that he was both Satoshi ("I'm not Satoshi") and a college professor ("And I'm not a college professor"). Forbes tracked early bitcoin coder Hal Finney down to his home, only to find him incapacitated - Finney had to spend the best part of a day writing an email using the movement of his eyeball just to deny it ("I must be brief..."). Newsweek got particularly excited last year after thinking it had finally cracked it when it found someone actually called Satoshi Nakamoto (hooray!) and ran it as a cover story. It turned out, however, his name was pretty much the only evidence, and the story was so widely discredited Newsweek yanked it from its website.

Wright had been the latest name in the frame, identified by two parallel stories in Wired and Gizmodo in December last year, after a hacker claimed to have retrieved data from Wright's computer that proved he was Satoshi and leaked it to them.

The documents - including a series of leaked emails, minutes of meetings and legal documents - all clearly pointed to Wright as the creator of bitcoin.

The Wired story ran with the bet-hedging headline: "Bitcoin's Creator Satoshi Nakamoto Is Probably This Unknown Australian Genius". Yet only days later they both got cold feet: evidence emerged that some of the material might have been doctored, more still that some may be false; even some of his degrees were called into question. The Australian tax authorities raided his house.

Soon, a remarkably strange alternative emerged: either Craig Wright was the mysterious creator of bitcoin - or he was the perpetrator of an incredibly detailed and elaborate hoax, all desperately aimed at making people think he was.

Yet I was assured Wright would provide irrefutable cryptographic proof. So far, this was not it.

The door swung open again. Wright came back in the room, sat back down, took a glug from his water bottle and slammed it down on the table like he was trying to hammer a nail. He was breathing heavily. Dr Courtois attempted to calm the mood.

"I'm not saying your evidence is invalid, but it's just one thing, I'm saying there are other sorts of evidence that people could ask from you, because it's just one thing... "

But it wasn't long until Wright was screaming again. Their argument was easy to understand but impossible to follow.

Sentences like "Bloody regenerate things on a single... show me where" and "There are f\*\*\*ing thousands of transactions on bitcoin every f\*\*\*ing day signed with pissy f\*\*\*ing bloody number generators" and "If I hear one more bullshit comment about how I can do it with unknown nodes, you show me proof or you f\*\*\* off out" were common.

Occasionally, it looked dangerously close to spilling over into physical violence. I dreaded having to explain it for the police report.

But the gist was clear: in his expert opinion, Dr Courtois didn't feel Wright's evidence was conclusive. Wright, in turn, was not pleased about this.

"The other interviews were easy," he exclaimed at one point. "This is bullshit!"

It was suggested we move on.

"You can validate," added Wright. "Or you can f\*\*\* off."

"You have to understand," interjected Jon Matonis, acting as peacemaker. "It's taken us a long, long time for Craig to get to this point, you know."

The proof session ended without conclusion. After that, I had an hour alone with Wright. He calmed. He spoke expansively about bitcoin's creation and the personal cost of it. The wife who left him, the friend's death that made him quit it in 2011.

If all this was a show, he was a convincing con man. I left thinking that, despite everything, yes, this could be Satoshi Nakamoto. It was a few days later that I got the email from Dr Courtois, who had examined the evidence we had been shown.

"Stuart," he wrote. "Craig has cheated us. It is a hoax. I have proof."

To explain what bitcoin is, it's perhaps easier to start with what bitcoin isn't. It is not, strictly speaking, a currency. Whereas the value of a currency rises and falls at the mercy of interest rates, inflation, trade, global downturns, whims of government and, at the most extreme, simply how much of it there is in circulation (print too much, as Zimbabwe found at the turn of the century, and it becomes worthless), bitcoin is designed to be a finite resource, and is therefore classified by the American government as a commodity.

New bitcoins are created each day, but the rate they're produced at will continue to halve until, by around 2140, 21 million have been created, at which point there will be no more. In this way, it's more like gold.

It is not the first "virtual" currency, but it is the first successful one. There have been the likes of digicash, which used "cyberbucks" (launched 1990, bankrupt 1998), beenz, which used a points system (launched 1998, defunct 2001), and e-gold, which used a digital currency redeemable for gold

(launched 1996, everyone involved arrested by the American government in 2007).

All failed for different reasons, but the crucial one is trust. Digicash and beenz failed because not enough people used them. This is rarely a problem with pounds. E-gold failed because hackers stealing money became widespread, plus it's actually illegal to create your own currency in most countries, not least the US. (This is something Hawaii resident Bernard von NotHaus also found to his cost in 2009, after he was arrested by the FBI and charged with conspiracy against the United States for creating and distributing his distinctly old-school "liberty dollars" - he had minted his own coins and printed his own notes.)

As with all currencies, bitcoin is only valuable because people think it is. This is something bitcoin developers I spoke to call a "collective hallucination". The idea being: if everyone has the same hallucination, it is, to all intents and purposes, real.

We can be reasonably sure the pound today is still a pound tomorrow or next year. A bank may be robbed, but no one is going to rob all the banks. The worry with a digital currency is that a single hacker could crack the sourcecode and take the lot (though even here there's an irony: steal it all and it becomes worthless. Imagine stealing all the money in the world and you start to appreciate the irony).

On all these fronts, bitcoin has proved remarkably resilient. Launched in 2009, it works using a "distributed database" known as the blockchain - essentially, this is a constantly updated record of every bitcoin transaction, shared across every computer on the bitcoin network. There's no central hub, and so no office to raid (music and film piracy works in a similar way and is similarly tricky to squish). In a stroke, it solved a key problem of electronic money - the "double-spend" dilemma. With bits and bytes, what's to stop you copying money several times over, rather than actually moving it? Banks solve this by acting as trusted middlemen who maintain an electronic ledger. Now, everyone held the ledger and everyone's computers did the hard work (the reward for leaving your computer on is a chance of winning the newly created bitcoins - the process is called "mining").

Put another way: the internet is an exchange of information, some of it true, some of it not. Satoshi's code harnessed it by ensuring an exchange of facts.

The central code, also, has also shown itself to be uncrackable. This is where Satoshi's reputation is born.

Dan Kaminsky, an internet security expert who is notorious for once discovering a flaw in the internet that would have allowed a skilled hacker to shut it down, famously tried, but failed. He came to a simple conclusion: either Satoshi was actually a team of people or he was a genius.

That was 2011 and it remains as bulletproof as ever.

The first ever real-world bitcoin transaction took place on 22 May 2010, when Florida programmer Laszlo Hanyecz made an offer on an internet forum: he would pay 10,000 bitcoins for someone to buy him two pizzas. He was taken up on the offer by a man in England who paid with his credit card: two

Papa John's pizzas duly arrived and Hanyecz sent the bitcoins over.

At the time, the 10,000 were worth around \$20 (£15). Today, they would be worth \$6.6m (£5m). Ever since, it's been celebrated annually as "bitcoin pizza day", where people raise a slice to the most expensive takeaway in history.

For quite some time, bitcoin effectively had no value: two events were to drastically change that. On 1 June 2011, Gawker published a story about the Silk Road - an underground dark web marketplace where everything from drugs to firearms were sold. The story mentioned these items were being purchased using bitcoin, a digital currency they called "untraceable". This was not entirely accurate: the blockchain ledger is entirely transparent. The problem was, it didn't link back to a person unless they were to convert their bitcoins back into regular currency, at which point, it did.

Regardless, the story put bitcoin on the map, and the value of a single bitcoin soared to \$22 within days. Ironically, it was the arrest of the person behind the Silk Road - Ross Ulbricht, a 32-year-old from Austin, Texas who had gone under the pseudonym Dread Pirate Roberts - that caused it to skyrocket. The FBI seized over 144,000 bitcoins - worth \$28m (£21m) at the time and \$96m today - and subsequently told a US Senate committee hearing in November 2013 it was a "legitimate financial service". Briefly, the price soared to \$1,242 for a single bitcoin, before levelling out in the low hundreds.

Still, there have been problems. As bitcoins are essentially just data stored on your computer rather than in a bank, they're remarkably easy to lose. Horror stories abound. Memory sticks worth thousands overwritten, computers worth fortunes junked. Notably, a Welsh IT worker called James Howells lost 7,500 bitcoins in 2013 when he accidentally threw out an old hard disk. It is currently somewhere in a Welsh landfill and worth over \$5m.

Regardless, over 100,000 companies now accept direct payment in bitcoin. You can book a holiday (Expedia), sign up for dating (OkCupid), buy everything from a computer (Dell) to lingerie (Victoria's Secret). You can even travel into space (Sir Richard Branson has said they will accept bitcoin payment for Virgin Galactic). Japan have even declared it a legal currency.

It could just be the start. Cameron Winklevoss - one of the twins involved in the disputed foundation of Facebook and the subject of the 2010 film The Social Network - has, along with his twin, invested most of his fortune in bitcoin, and the brothers are currently estimated to own one per cent of all bitcoin in circulation. He has suggested that, eventually, a single bitcoin could rise in value to over \$40,000, putting the cost of that 2010 pizza at just under half a billion dollars (at which point you'd hope Hanyecz got his preferred toppings).

In the month and a half since Wright claimed to be Satoshi - a period that took in Donald Trump securing the Republican nomination for the White House and the lead-up to the Brexit vote, events that weakened the dollar, pound and euro - bitcoin's value soared once more, rising from \$445 to \$731.

Bitcoin was created by Nakamoto in the aftermath of the 2008 global financial crisis to be free of such outside influences - and it was proving to be the case. Uber threatens to eliminate cab offices, but bitcoin is threatening to eliminate banks. It had, seemingly, become the most trusted form of money in the world.

The screenshot shows the Silk Road anonymous market website. At the top, it says "Silk Road anonymous market" with a camel logo. Navigation links include "messages 0", "orders 0", and "account \$0.00". A search bar is present. Below the navigation is a "Shop by Category" sidebar listing various items with their counts:

- Drugs 6,625
  - Cannabis 1,080
  - Dissociatives 190
  - Ecstasy 829
  - Opioids 382
  - Other 450
  - Precursors 59
  - Prescription 1,429
  - Psychedelics 828
  - Stimulants 1,079
- Apparel 310
- Art 114
- Biotic materials 1
- Books 858
- Collectibles 1
- Computer equipment 43
- Custom Orders 60
- Digital goods 590
- Drug paraphernalia 247

The main content area displays a grid of drug listings with images and prices:

- Generic XANAX (Alprazolam 1mg): 400 pills Grade A+ \$1.52
- Pure Oxycodone HCL Powder (OC, Roxy)- 1/4 \$0.53
- TESTOSTERONE CYPIONATE 250mg/ml x 10 \$0.89
- 100 GR - MDMA 84%
- Pack of Five (5) Suboxone (Buprenorphine) 8mg/2mg
- SALE SALE!!!!!! 250 grams METHYLONE!

Bitcoin value skyrocketed after being mentioned in a Gawker news story about the Silk Road website.

Craig Wright is a computer scientist, serial entrepreneur (of many failing companies, at least one of which, Hotwire, went into administration) and serial collector of various degrees (even if, yes, he admits he may have exaggerated some on his LinkedIn profile: "It was all piss taken at myself," he says, suggesting a curious sense of humour).

He apparently has qualifications in subjects ranging from theology to statistics, engineering to law. He is also being investigated by the Australian tax authorities (late last year, they raided his house over tax rebates his companies have claimed, of which Wright said, "We've been in negotiation with them for years! It's not a criminal investigation!").

When I visit Dr Courtois' fourth floor office at UCL before the interview - London skyline in the background, NSA coffee mug on the shelf - he says yes, Wright could be Satoshi.

"He has the skills, he has been at the crypto conferences."



But he warns two things. One: "It's quite possible it was a collective creation." And two: "You would be a fool to claim you are Satoshi. Not for a criminal connection, but a criminal responsibility connection. He could be prosecuted."

The test was cryptographic, which is to say, the claim could easily be verified to be true or false. There should be no shades of grey.

The real Satoshi didn't just create the code of bitcoin. He owns - according to a widely cited internet study by bitcoin security consultant Sergio Demian Lerner - around one million himself. At today's value, they're worth just over half a billion pounds. Think of every bitcoin in existence as a Tetris stack: the earliest sit at the bottom.

To prove he was Satoshi, Craig Wright had to spend, and therefore move, one of those earliest bitcoins in existence. Instead, however, he chose to "sign" one - essentially showing the note, rather than handing it over for inspection.

Before the meeting, the evidence was evenly balanced, if confusing and contradictory.

Here's what I knew about Satoshi: he was a native English speaker, as his writing was remarkably fluent in his many blog posts (tick). He used terms like "bloody hard" and "flat" rather than "apartment", suggesting an English, or at least a Commonwealth, origin (tick). He embedded one of the very first, unspendable, coins - known as the genesis block - with a Times headline from January 2009 about a second Gordon Brown bailout, suggesting a libertarian nature (Wright is a former subscriber to the Cypherpunks mailing list) and a British press reader (entirely possible). He wrote in a particular code (C++) and used a particular notation that several experts told me was popular in the late Eighties and early Nineties, likely placing him in his forties (tick).

And finally, I knew he left. At 6.22pm GMT on 12 December 2010, seven days after a plea not to use bitcoin to donate to Wikileaks ("the heat it would bring would likely destroy us at this stage"), Satoshi Nakamoto posted his final message and disappeared.

Why come out now after six years away?

"I don't want to come out," he says. "But people in my organisation keep going, 'We've got to do this'."

When Dr Courtois was in the room, he had said it was due to his family - "so they don't get painted with this shit". This was new.

What organisation? There's a pause. "I have a nice big organisation. We have offices in different locations, including London. No one knows who the f\*\*\* we are, and I like that."

I'd heard he was building a supercomputer in Iceland. "Yes... I don't want to talk about where it is... it's not in Australia."

But is it in Iceland?

"If I answer that question I get in big trouble," he says. Why? "People are going to go, 'Craig, you're not supposed to talk about those things.'" He looks over at the PRs. "At the end of the day, there is a company, people working for me. There are about 30 people here in London. They don't want to be known. Not because they don't want to be seen with me, but... because..." Because? "Because this is what they do." He won't say exactly what that was.

Far from coming clean, every reply only opens up further questions - ones he then refuses to answer. He is curt in a half-smiling way that suggests he wants to let me know he knows more than I do. In some ways, he is almost childlike. He often leans back and straightens his tie, like a bank manager conducting an appraisal. Every so often he brings up Dr Courtois, unprompted, to bristle at how unfairly he'd been treated, despite him having been the aggressor.

He didn't need to move (ie, spend) any bitcoins to prove who he is, he says, because simply signing one showed he had access, and so, "It would be like I've stolen the Mona Lisa, put it on my wall, took a couple of pictures, then put it back." It barely needs pointing out that a polaroid of the Mona Lisa would not confirm one owned it.

I ask him about the claim by early bitcoin developer Gregory Maxwell that the documents leaked to Wired had been edited to make it look like he was Satoshi.

"Bullshit from Maxwell that we had to get disproven: the codes are f\*\*\*ing out there."

The person behind the leak, he says, was a former employee attempting to extort him. "I have my suspicions [who it was], but I don't have proof so I can't say."

Curiously, it is only when we speak about his private life, about how much bitcoin's creation had cost him, that he relaxes and calms; he strokes his tie once more, and finally the words begin to flow. This is how bitcoin started - at least, as far as he tells it.

He'd been working on bitcoin, on and off, he says, for a decade. Tinkering here and there. He'd initially got into computers through his grandfather, who let him use his terminal in the basement. His father, he says, openly disliked him. "We didn't get on. I haven't spoken to my father in a long time. He never liked what I did, never liked my life."

He collected degrees for fun, and soon developed a reputation as the go-to guy for a range of computing consultancy roles at start-ups. It was only when he was let go, he says, from his role at accountancy firm BDO on 3 January 2008, when the financial crisis started to hit, that he fully devoted himself to it.

"They gave me this whack of money, enough not to work, not forever, but from then I could dedicate my time." He hunkered down at his house in a remote farm in Port Macquarie, surrounded by screens, and set to work. He had help, he says, notably from a friend called Dave Kleiman. As a former army officer and Palm Beach County Sheriff, Kleiman was not your usual computer geek. After suffering a motorcycle accident in 1995, which left him wheelchair-bound, he became a computer autodidact. He was regularly called on by CNN and ABC to dish out advice on security and passwords. He had so many three-letter qualifications after his name his nickname was Dave Mississippi.

"He helped a lot," says Wright. "He knew who I was."

The leaked documents - if accurate - reflect this. An email sent from Wright to Kleiman on 12 March brings it up abruptly: "I need your help editing a paper..."

By October 2008, the now-famous white paper was published: "Bitcoin: A Peer-To-Peer Electronic Cash System". By January, the software was released for free online.

He says it consumed him. He didn't look for a job. Soon, his marriage started failing.

"It wasn't the best way to maintain a marriage," he says. His wife would ask, "Craig, what the f\*\*\* are you going to do to pay the rent?" He would simply reply, "We're fine!" Except, he wasn't fine. The value of bitcoin was still on the floor. He remortgaged his house just to keep going.



By 2011, he says, everything fell apart. His wife decided to leave him ("Some of that was bitcoin's cause"). Kleiman had fallen in the shower in late 2010, and was subsequently in and out of hospital ("Dave was my best friend. He kept me sane... That was hard").

The burden of being Satoshi, he says, became too great. He left it all behind.

The search for Satoshi has been difficult precisely because of his brilliance. He would have to be an expert in many fields: a deep understanding of coding, of economics, of financial markets and advanced cryptology. Hardly anyone fits the bill. A team - or a genius.

"I know people want me to be something else," he says. "People want me to be an academic. I'm not. I'm an applied scientist and an applied engineer. I take different ideas and stick them together. Edison didn't invent new theory. And Ben Franklin didn't invent new theory. Tesla didn't. Steve Jobs didn't."

The most telling story, I felt, was this: once, while studying advanced economics for one of his many qualifications, he came across a famous essay, "I, Pencil", written in 1958 by Leonard Read. It contains a proposition - the pencil may seem like a simple object, yet "not a single person on the face of this earth knows how to make me".

From the wood to the tools to chop the wood, to the tools to make those tools, to the graphite, the rubber and the metal, a single pencil is a co-operation of thousands of experts in dozens of skills, stretching back in time, from across the world. But Wright took this as a challenge. He wanted to make a pencil.

"And I couldn't cheat. You can't go out and buy a chisel. You have to build the tools. And you can't start by building iron tools. To make them you need copper tools. And for copper tools you need stone tools." He spent years on it, even building his own kiln to make the graphite. In the end, he made five pencils that cost him over \$1,200 each. "That's probably another reason I got divorced."

It was that story, perhaps, that saw me leaving the room that day thinking, yes, this could well be Satoshi. Despite him not moving early bitcoins. Despite the unconvincing answers about his reasons for coming out (what was this company?). Despite the unauthored paper I was given to disprove Maxwell's claims about the leaked documents having actually been written by himself ("It doesn't say 'By Craig Wright' on the piece as such," says the PR firm when I contact them after a tip-off, "but as the whole pack is called Craig Wright and relates to him, it seems clear it's his piece"). Despite, also, a source of mine, who asked not to be named, seemingly confirming a company had forced Wright to say he's Satoshi: "They are big players, but they want him to come out as Satoshi Nakamoto in order to basically get more gravitas."

Also, for a man supposedly worth near half a billion ("I'm not spending them," he said of his bitcoin stash. "They're going nowhere"), he was weirdly boastful about what car he drove ("I own an i8, a BMW, a nice fast car. I get speeding tickets but I pay them") or the restaurants he ate at ("I've been to three of Gordon Ramsay's so far"). Because didn't that pencil story just sum him up? The genius who would have to master so many skills; the man who would have to put them all together. Wasn't it such a great story?

But this story was about to get stranger still.

When the judgement came, it was swift and unforgiving. This happens on the internet: damnation goes viral. Reddit forums light up. He lied.

When the news embargo was lifted a few days after our interview, it took the world no more than a few hours to realise what Dr Courtois had already discovered: the cryptographic proof he had presented was fake. Or rather, he used an early bitcoin transaction that had already been signed by Satoshi years ago. Anyone could have done it. To use Wright's own Mona Lisa metaphor: he didn't present a polaroid of the painting on his wall. He presented someone else's old polaroid.

Stories around the world that first reported his outing as straight news - from the BBC to the New York Times to the Guardian - were swiftly followed up by claims of a hoax.

Wright countered: he would now provide "extraordinary proof" to match his "extraordinary claim". It never came. Days later, he released a statement on his website: "I know now that I am not strong enough for this. I'm sorry."

I speak to various experts working on bitcoin-related projects. "If he is who he claims to be, there's an easy way to prove it," says Pavel Matveev, of bitcoin start-up Wirex, which is working on a bitcoin debit card. "It seems like he's Satoshi Nakamoto," says Frank Schuil, of bitcoin spending platform start-up Safello, "but he has one hell of a reason not to reveal it."

"It's a strange play either way," says Dr James Smith of Elliptic, a bitcoin company that identifies illicit activity for financial institutions and law enforcement agencies. "I think he'd be nuts if it isn't him, but I think he'd be nuts if it is as well."

Something else came to light too - there was another journalist, unknown to GQ, who had been chronicling Wright's story from the inside. The novelist Andrew O'Hagan had been contacted some months before by the mysterious company who were now in business with Wright - the one only mentioned under duress to GQ, and not mentioned at all to the BBC and the Economist. In O'Hagan's subsequent profile in the London Review Of Books, published just before GQ went to press, it would be named as nCrypt. Its offer to O'Hagan was to write the life story of the real Satoshi Nakamoto.

The people behind nCrypt, it turned out, had rescued Wright. His businesses were failing, he was in trouble with the Australian tax authorities; he owed his lawyers millions. They offered an out: they would buy up his companies and settle his debts. In return, he would work on patents linked to the underlying blockchain technology behind bitcoin. And he would publicly out himself as Satoshi. The package, they felt, was worth billions. They planned to sell to Google.

Coincidence or not, just weeks after O'Hagan had accepted to write the story, the documents linking Wright to Satoshi were leaked to Wired and Gizmodo. It would contain a neat explanation of why a man worth nearly half a billion should need such help: most of his bitcoins were held in a trust, a document suggested. Wright could not sell them until 2020. It would be one of many "facts" that didn't quite add up.

The patent story was true enough. A search on the patents pending by nCrypt uncovered nothing, but a search at Companies House showed the company director as a Mr Robert MacGregor. He, in turn, is linked - in documents seen by GQ - to an umbrella company called EITC Holdings Limited. Between 23 February and 29 April this year, they filed 51 patents, all linked to blockchain technology. They were, in essence, trying to corner the market in the new internet of fact exchange. Though experts GQ spoke to expressed scepticism that the patents would be successful. They were really selling Satoshi. The documents show plans to use the technology for everything from voting to payroll, from money lending to music and film software that could eradicate piracy.

But many other claims by Wright in the story don't stand up to scrutiny.

Take his story about his friend Dave Kleiman. That story is a tragic one.

After the fall in the shower that December day - which saw Wright, so he says, leave the mantle of Satoshi behind him - Kleiman's condition worsened. He developed sores which became infected with MRSA; he was in and out of hospital and had multiple operations. Yet every time, say people familiar with the matter, he would get right back to his computer, holding up for days at a time, rarely going out. After dismissing himself from hospital for a final time, he was to be found dead in his wheelchair on 27 April 2013. According to the Palm Beach County Medical Examiner Office, his body was decomposing; there was blood and faecal matter; an empty bottle of alcohol and a loaded handgun next to him. He died apparently penniless; his Palm

Beach home was in foreclosure. It had been suggested, however, that as one of the founders of bitcoin, he actually passed away with some 350,000 bitcoins sitting on an encrypted USB drive he kept on him at all times.

"Yes, that's accurate based on the information that I have," says Jon Matonis when I contact him by email.

The question remains: why didn't he cash out to get private health care?

Speaking to O'Hagan, Wright confirms Kleiman did indeed have 350,000 bitcoins. Yet in explaining why he didn't sell, Wright says, "It wasn't worth much then. Dave died a week before the value went up by 25 times."

O'Hagan then adds, "He emphasised something he said the commentators never understood: for a long time, bitcoin wasn't worth anything and they constantly needed money."

This goes unquestioned, but it's not remotely true. At the time of Dave Kleiman's death, on 26 April, 2013, bitcoin's value was at \$136.90, making his 350,000 stash worth just under \$50m. The next week, meanwhile, rather than having gone up in value 25 times as Wright claims, it had gone down, to \$98.10. In fact, it wasn't until just under six months later that it had even reached the same level.

It was baffling: why lie? What was being hidden here?

One of the few solid things that we know came from the real Satoshi are his blog posts, now archived at [satoshi.nakamotoinstitute.org](http://satoshi.nakamotoinstitute.org). He writes about the task at hand; personal details are virtually nonexistent. Yet the most telling thing isn't what the posts are about, but when they were posted. In more than 500 posts, Satoshi almost never published between the hours of 5am and 11am GMT, suggesting that's when he slept.

When Wright spoke with me, he simply said: "I was up at all times always doing stuff, as people have seen I was around the clock... "

Yet in Sydney, where Wright lived at the time, those hours would suggest a truly bizarre sleeping pattern of 3pm-9pm. Transpose those same timings to Florida, however, where Kleiman lived, and it becomes 1am-7am.

Kleiman is rumoured to have died without giving anyone, not least his family, the drive's encryption keys, meaning no one can access them. At today's prices, the bitcoin on it would be worth some \$235m. If Kleiman - and not Wright - was the real Satoshi, it would explain why Wright didn't move them. Maybe no one could. It would also mean he stepped away from being Satoshi after first being admitted to hospital, as his health began to fail.

When I call Kleiman's former colleague at Computer Forensics LLC, Patrick Paige, and let him know I'm working on a story about Craig Wright, the first thing he says to me is: "Is he on suicide watch yet?" His tone does not suggest concern.

Perhaps most bizarrely from the London Review Of Books story is the reason Wright finally gives for not wanting to move the early bitcoins and thereby proving beyond all doubt he's Satoshi. He sends O'Hagan a link to an article with the headline: "UK Law Enforcement Sources Hint At Impending Craig Wright Arrest". He sobs about this. He says, "The Brits have got their own version of Guantánamo Bay." He says he's damned if he does, he's damned if he doesn't. He'll be seen as a fraud, or he'll go to jail.

Yet it turns out this isn't true either. The story appeared on specialist bitcoin website bitcoinist.net. Yet go to that link now and it starts with an editor's note: "The SiliconAngle piece cited in this article was produced by an impostor site posing as the real SiliconAngle."



Photography by **Getty Images**

Someone had gone to the effort of creating a fake website to create that story, the only difference being an extra "l" in the name.

When I contact the senior editor at Bitcoinist, Evan Faggart, I ask how long the Wright story was on their website before the editor's note was added.

"No more than 24 hours."

Twenty-four hours. Is it feasible that Wright clicked on this link once then never again? A man sobbing at the prospect of being locked up in whatever he assumes the British Guantánamo Bay to be? Would he not check back?



One thing the editors at both sites agree on - the fake site, which has since been taken down, was an uncanny replica of the real thing. It would have taken substantial computer skills, and no little effort. "I've never seen anything like it," says Faggart.

One line in the London Review Of Books piece, therefore, felt particular pertinent: when the act seems to slip; when Wright seems to admit he was actually Satoshi's sidekick.

Wright makes the point that he wrote all the new patents himself and "not just Dave".

In May of this year, after Wright's claims had begun to unravel, I travelled to New York and sat in on a United Nations conference called ID2020. It is the brainchild of John Edge, a former investment banker who on 4 May 2013, was set up on a blind date with a girl who asked him, "All this money stuff, fine, but what are you doing to make a difference?" He didn't have an answer, but he did have an idea. He knew how money flowed through computer systems. Specifically, how the FIX (Financial Information eXchange) protocol radically changed trading when it was introduced in 1992, all but eliminating human errors. "What it did was turn a telecommunications network into a transactions network." He realised Satoshi Nakamoto, with the shared ledger that underpinned bitcoin, had done the same for the internet. But how to use it? He'd had meetings with BT, with major banks, but the reaction was always the same: don't be stupid. Isn't bitcoin that thing for drug dealers?

Only now, he had his lightbulb moment. What if there was an altruistic use for it? The bitcoin technology, the shared ledger, was incorruptible. It sat with no single government. He knew 1.5 billion people around the world didn't have identities on paper - and without birth certificates, they could have no bank account, and were at greater risk of kidnap and trafficking and abuse.

Edge is a likeable, plain-speaking northerner. He is also not a shy man. On his second date, he said to the girl, "I think this system can get a billion people a bank account."

In the UN conference hall, there are over 400 people, and along with various NGOs and seemingly every major tech company, there are representatives from virtually every bank in the world. When I ask why, I get the same answer: because a billion micro-payments add up.

SEARCH NEWS SCIENCE SECURITY

GIZMODO

## NEW CLUES SUGGEST CRAIG WRIGHT, SUSPECTED BITCOIN CREATOR, MAY BE A HOAXER



Australian Federal Police officers walk down the driveway after searching the home of Craig Steven Wright in Sydney's north shore (December 9, 2015). © DAVID BRAYFLANSHY

WHEN WIRED NAMED Craig Wright Tuesday as the most likely suspect to be Satoshi Nakamoto, the mysterious creator of bitcoin, we laid out two possibilities that outweighed any

### This Australian Says He and His Dead Friend Invented Bitcoin

Sam Biddle and Andy Green  
Illustration: Marco Altieri



ARE THESE MEN SATOSHI NAKAMOTO?

This story was originally published on December 8, 2015. Shortly thereafter, Craig Wright scrubbed much of his digital presence and disappeared for months—until May 2, 2016, when he publicly announced that he is the creator of Bitcoin.

A monthlong Gizmodo investigation has uncovered compelling and perplexing new evidence in the search for Satoshi Nakamoto, the pseudonymous creator of Bitcoin. According to a cache of documents provided to Gizmodo which were corroborated in interviews, Craig Steven

As the keynote speakers stand and talk, a running theme becomes clear: the technology is spoken about as being a second internet. The internet of fact and record. Or, as Microsoft's John Paul Farmer, puts it, "I look at it akin to where the web was in the early Nineties." It's a sentiment repeated throughout the day. Bitcoin may change banking, but it's the underlying technology that may truly end up changing the world. Some weeks before, I sat in the back of a lecture theatre at University College London, and watched students specialising in the tech, pitch to start-ups who were specialising, too. There was no shortage of positions.

The tens of thousands of jobs that have already been created are likely just the start.

In one of the few breaks during the day, I catch up with Edge. Has it hindered you, I ask, that no one had convincingly come forward as Satoshi? Quite the opposite, he says - it would have meant you would have had to ask permission. "Satoshi might be the most genius sales strategy of all time."

And even here, of course, there's a final irony. That a man who sat in his house and invented the future but never wanted his own identity known - perhaps Kleiman, who died alone, and whose real identity perhaps we'll never know - may end up providing identities for billions.

When Satoshi first went missing, a popular tagline among bitcoin's early adopters suggested they knew it was for the best; that perhaps one man would be too small for it, the invention was too big. It's a line repeated to me again and again at the United Nations.

"We are all Satoshi now."

Originally published in the September 2016 issue of *British GQ*

## Bitcoin from the start

From the creation of the first bitcoin in 2009, Satoshi Nakamoto's cryptocurrency has been used to buy everything from pizza to drugs, and could potentially change the face of modern banking. Here, a timeline...

### 9 January 2009

The first version of the bitcoin software goes online, claiming to allow money to be paid "without going through a financial institution".

### 22 May 2010

The first real-world bitcoin transaction takes place - programmer Laszlo Hanyecz buys two pizzas for 10,000 bitcoin. It becomes known as "bitcoin pizza day".

### 9 February 2011

Bitcoin reaches dollar parity.

Value of one bitcoin: \$1

### 1 June 2011

Bitcoin value skyrockets after being mentioned in a Gawker story about the Silk Road website.

### 8 July 2011

Top of the first "bubble".

Value of one bitcoin: \$31

## **27 February 2012**

*Bitcoin Magazine* launches. Seven months later the Bitcoin Foundation is formed.

## **28 March 2013**

Total value of all bitcoin passes \$1bn.

Value of one bitcoin: \$86

## **29 November 2013...**

Bitcoin reaches all-time peak price of \$1,242 after the FBI tells a US Senate committee hearing it is a legitimate financial service.

## **Value of gold: \$1,240 per oz**

...and on the same day

Bitcoin value surpasses that of gold for the first time in the US.

## **14 March 2014**

Newsweek cover story mistakenly identifying the creator of bitcoin hits shelves.

## **29 August 2015**

Barclays announces it will be the first UK high street bank to accept bitcoin.

## **October 2015**

Bitcoin value reaches its peak for 2015.

Value of one bitcoin: \$504

## **8 December 2015**

Wired and Gizmodo publish rival stories suggesting the Australian Craig Wright invented bitcoin after being leaked personal documents.

## **May-June 2016**

Large spike in value occurs for the currency.

Value of one bitcoin: \$750

## **13 June 2016**

The value of bitcoin doubles in a month in the run-up to Brexit. Following the result, a surge of investors flock to bitcoin as the value of sterling slumps to a 32-year low.