The Craig Wright May 2016 Signing Sessions Debacle, In Full Context

There's a story that has never been told before in the Faketoshi saga...

MyLegacyKit

Photo credits: Mark Harrison, The Economist

> ***Written by Arthur van Pelt***
>
> ***ABOUT EDITS*** *to this article: as more material might become available after publication of this article, it will have edits and updates every now and then. In that sense, this article can be considered a work in progress, to become a reference piece for years to come.*

EDIT JULY 1, 2021

The highly reputable and respected WizSec Bitcoin Security Specialists

outlet, well known for their Mt Gox research and Kleiman v Wright lawsuit coverage, just released an article that can be found here. It is highly recommended to pick it up also, either first, or after reading "**The Craig Wright May 2016 Signing Sessions Debacle, In Full Context**".

This article is sort of a spiritual companion piece to MyLegacyKit's comprehensive write-up of the timeline of the Wright key signings. While independently written, they pair well together as a shot and chaser. If after reading through this post you have a thirst for more details, go check it out!

Intro

In Bitcoin, signing a message is a cryptographical way to prove control and ownership of a public bitcoin address (using the associated private key) via a feature in the Bitcoin wallet. The procedure of signing takes less than a minute to perform, and the output -a so called digital signature, a lengthy string of letters and numbers- can be used by others to verify said ownership and control.

For example, Craig Wright has been using the Bitcoin public address starting with 16cou, that once contained over 160,000 BTC, in numerous forgeries over the years since April 2013 when his Bitcoin fraud, quickly followed by a Satoshi Nakamoto cosplay, started. In these forgeries, Craig pretended to own and control the 16cou address.

2. On 11 October 2013, Mr Wright came into my office and showed me his HTC mobile phone (**Wright mobile**).

3. On the screen of the Wright mobile, I viewed and verified the following Bitcoin wallet addresses:

   (i) 1JzzLXxuwn45S9HvBqAhkhWa3GhyG3zm64;

   (ii) 168Rc6wJdL4chWhΞUQwyywi4sHub6erf2s;

   (iii) 1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF;

   (iv) 1933phfhK3ZgFQNLGSDXvqCn32k2buXY8a; and

   (v) 16cou7Ht6WjTzuFyDBnht9hmvXytg6XdVT (**Bitcoin wallet addresses**).

4. I viewed the Bitcoin wallet addresses by scrolling down the screen on the Wright mobile.

5. It appeared to me that if Mr Wright wanted to, he could control all of, and make transactions in, the Bitcoin wallet addresses.

Forgery from the early days of Craig's Bitcoin fraud

However, on May 16, 2019 the real owner of the 16cou Bitcoin address had enough of this abuse of his property when he or she became aware of it, and left the following information on social media for the general public to verify.

On a related sidenote, while talking about or examining Craig Wright's forgeries, a list that has grown into the hundreds if not thousands by now, there is a rule of thumb that never fails so far.

This rule of thumb is:

Everything Craig Wright and Bitcoin dated before April 2013 is a forgery created after April 2013 (except for a handful of public comments online in July/August 2011 when Craig apparently had just learned about Bitcoin).

With that said, no doubt most of you will have heard, or read, bits and pieces of the story that will unfold now. But here it is, Craig Wright's full diary of what most now (correctly) perceive as the failed signing sessions in May 2016, as told by the insiders, the journalists and other witnesses.

With a lot of quotes from articles, many snippets from lawsuit depositions and intertwined with notes from the undersigned (always in italics), we will learn the full context of Craig Wright "signing" in his Faketoshi career with the 2016 sessions as a centerpiece. So brace yourself, and join me for a deep dive into this remarkable piece of Craig Wright's history.

And remember, after these disastrous events 5 years ago in May 2016, Craig Wright's reputation as a lying and forging Satoshi Nakamoto cosplayer was set in stone — forever.

Did Craig Wright ever sign anything Bitcoin before May 2016?

We can be brief here: never in public, as far as we know. We know, of course, of those few times that Craig has been transacting with a few handful of Bitcoin bought on the Mt Gox exchange from April 2013 onward (until Mt Gox collapsed in February 2014), so Craig must have had access to a few private keys at some point in that period. But there is no evidence known that Craig Wright ever used these private keys for a signing.

Way more telling in this context, however, is how Craig dealt with the ATO in the 2013–2015 era, as he ducked numerous requests from the ATO to show signing proof, and purported financial transactions were always done by "assigning rights to Bitcoin" or "providing private keys". In the ATO reports about Craig's tax fraud from that period, we find several hilarious descriptions of these events.

For example, have a look at this somewhat creative way to offer, and duck, a Bitcoin message signing at the same time. ATO however quickly figured out it was another email forgery created by Craig Wright:

163. On 27 November 2015, the taxpayer also provided a copy of an email purportedly sent from Dr Wright to Celso Tomas of the ATO on 17 October 2013 to further evidence the contention that Dr Wright offered to sign messages for the ATO.[210] The email states:

> If there is a simple means to offer ongoing proof, we will do this now. As we are moving forward in business, we cannot promise that the same information will always be available. If you allow us, we will prove how we can transfer keys on and off block. Once a transfer has occurred offblock, the scheme we use wipes information. I did a paper on data wiping in 2008, so I can assure you that I would like to ensure the information is exchanged in a format the ATO can use prior to losing this ability.'

164. This email was never received by ATO servers.

Source ATO report: https://www.courtlistener.com/docket/6309656/547/7/kleiman-v-wright/

Another example is where Craig Wright was asked to sign messages on no less than 9 Bitcoin addresses, and none of them happened. None. Nada.

157. On 25 May 2015, we requested that the taxpayer and related entities show control of the private keys of certain Bitcoin addresses (including 1PbX, 1P57, 1CXn, 146m, 168R, 19dQ, 1Jzz, 1M7c and 153R) by signing messages within the addresses using the private keys.[204] This can be performed by the holder of a private key even once the Bitcoin in the address has been spent. The taxpayer and related entities did not sign any messages and on 26 May 2015, made a new claim that address 1Jzz had 'transferred out of Dr Wright's control as part of the MJF transactions by transfer of private keys'.[205] However, previous advice provided to the ATO indicated this address was not transferred to MJF.[206]

Source ATO report: https://www.courtlistener.com/docket/6309656/547/7/kleiman-v-wright/

And, as said, Craig Wright is always executing Bitcoin "transactions" by either "assigning rights", in this case by "instructing to put Bitcoin in a trust" for Professor Rees, followed by the excuse that "private keys were provided" to Professor Rees, followed by a mixture of these excuses. And again, the ATO didn't buy it.

267. The taxpayer has not substantiated that it paid Professor Rees, and has provided anomalous accounts of this. The taxpayer first advised that it had instructed an amount be held in trust for Professor Rees. The taxpayer then advised that it provided private keys to Professor Rees on 28 June 2013. Then it advised the Bitcoin was held in trust for Professor Rees until the keys were released. We note the following anomalies:

267.1. The taxpayer claims that Professor Rees was provided with private keys to seven addresses. At 28 June 2013, the contents of these addresses was 34,512.57 Bitcoin, greater than the 27,636.38 Bitcoin the taxpayer claims to have been in them.

267.2. The taxpayer claims that the contents of the addresses were forwarded to a new address, 1LXc on 13 August 2013. The taxpayer claims that that this was held for Professor Rees, a position that is inconsistent with Professor Rees having the private keys to the seven addresses. Further, if the private keys were transferred to Professor Rees on 28 June 2013 and the taxpayer was unable to recreate them as it contends, Professor Rees must have transferred the Bitcoin to 1LXc three days before his death. At 28 June 2013, Professor Rees was in a nursing home, declining in health and had ceased using a computer.

Source ATO report: https://www.courtlistener.com/docket/6309656/547/7/kleiman-v-wright/

The Prelude

June 2015 — November 2015

Knowing the background of how Craig Wright approaches Bitcoin "signing" and "transacting" by never doing anything, let's move to the meat of this article. Due to the ATO troubles building since 2013, Craig needed a bailout which was provided in June 2015 by Calvin Ayre. The people fronting Calvin were Stefan Matthews and Robert McGregor, who will play important supportive roles in the upcoming period.

On June 29, 2015 a contract was signed with Craig Wright, Ramona Watts (Craig's wife) and Stefan Matthews that contains the following paragraph about "the exclusive rights to Craig's life story for subsequent publication or release (suggest NewCo retain a researcher and ghost writer to begin background research and preparation, as precautionary measure).".

- **$3,500,000 Rights and Services Agreement.** NewCo will enter into a direct exclusive services agreement with Craig as Chief Scientist.

  [Notes: This would consist of a $1,000,000 initial rights payment, followed by an annual services arrangement for R&D of $500,000 for five years, and renewable for subsequent periods. This would provide supplemental income to the Wrights and would cover any IP developed outside of Company, and would also grant NewCo the exclusive rights to Craig's life story for subsequent publication or release (suggest NewCo retain a researcher and ghost writer to begin background research and preparation, as precautionary measure).]

Source: https://www.courtlistener.com/docket/6309656/550/45/kleiman-v-wright/

We will also find an early appearance of Jimmy Nguyen, (who, after being employed by a lawyer firm, moved from CEO of nChain in the early days to Founding President of Bitcoin Association for BSV in his current employment) as we learn from The Satoshi Affair.

“A few weeks before the raid on Craig Wright’s house, when his name still hadn’t ever been publicly associated with Satoshi Nakamoto, I got an email from a Los Angeles lawyer called Jimmy Nguyen, from the firm Davis Wright Tremaine (self-described as ‘a one-stop shop for companies in entertainment, technology, advertising, sports and other industries’). Nguyen told me that they were looking to contract me to write the life of Satoshi Nakamoto. ‘My client has acquired life story rights … from the true person behind the pseudonym Satoshi Nakamoto — the creator of the bitcoin protocol,’ the lawyer wrote. ‘The story will be [of] great interest to the public and we expect the book project will generate significant publicity and media coverage once Satoshi’s true identity is revealed.’” — Andrew O’Hagan (1)

This makes it clear that the ghost writer from the June 29, 2015 contract will become Andrew O’Hagan. It is, of course, also perfectly clear that the

financial stakes are high for camp Craig Wright.

"The plan was always clear to the men behind nCrypt. They would bring Wright to London and set up a research and development centre for him, with around thirty staff working under him. They would complete the work on his inventions and patent applications — he appeared to have hundreds of them — **and the whole lot would be sold as the work of Satoshi Nakamoto, who would be unmasked as part of the project. Once packaged, Matthews and MacGregor planned to sell the intellectual property for upwards of a billion dollars**. MacGregor later told me he was speaking to Google and Uber, as well as to a number of Swiss banks. 'The plan was to package it all up and sell it,' Matthews told me. 'The plan was never to operate it.'" — Andrew O'Hagan (1)

February 3, 2016

At first, the next happening appears unrelated to the upcomings events in May 2016. A copy of the siliconANGLE [the voice of enterprise and emerging tech] news website is set up under almost the same domain name, note the double "l" used in silicon. But knowing what is going to happen in the upcoming 3 months, there is hardly any doubt (with me at least) that the setup of the forgery described is executed by Craig Wright himself.

"It appears that Craig Wright planned this exit-strategy for the May 2016 signing sessions 3 months in advance, as on February 3, 2016 the registration of silliconangle dot com took place.

Historic Whois Record

Domain Name: SILLICONANGLE.COM
Registry Domain ID: NA
Registrar WHOIS Server: whois.enom.com
Registrar URL: www.enom.com
Updated Date: 2016-02-03T05:54:13.00Z
Creation Date: 2016-02-03T13:54:00.00Z

Nameservers

Date	Status	Name Server
2019-02-12	Deleted	dnsowl.com
2018-02-13	New	dnsowl.com
2017-03-18	Deleted	name-services.com
2017-02-04	Transferred to	name-services.com
2016-02-03	New	namecheaphosting.com

Then, a full copy of the Silicon ANGLE website was created under the newly bought domain. Would that have been a hard task for our #Faketoshi?

Nah." — Arthur van Pelt (2)

> Applications like HTTrack give users the ability to download entire websites, mirroring the directory structure, files, and images that would be present on the server. You can then view the code and update your own as desired. This allows you to view the actual HTML and CSS used by the site you wish to copy, before testing locally and offline. This is the closest way to actually "copy" a website.

February 16, 2016

The domain drcraigwright dot net is obtained by camp Craig Wright, and from this place Craig (and/or Robert MacGregor as we will learn from The Satoshi Affair) will publish a few blog posts in early May later this year, before taking it offline altogether after less than two weeks later. As we speak this domain is forwarded to his current blog on craigwright dot net.

The Signings

March 2016

"As Andresen tells it, a firm representing Wright [*Outside Organisation, according The Satoshi Affair*] contacted him in March and invited him to London for a private, in-person demonstration designed to prove Wright created Bitcoin." — Andy Greenberg (3)

"To add, in the recent court filings we learned that Craig's media training before the failed 2016 signing sessions was provided by Milk Publicity

(https://milkpublicity.com) and Outside Organisation (https://outside-org.co.uk).” — Arthur van Pelt (4)

VIDEO-TAPED DEPOSITION OF

DR. CRAIG WRIGHT

On

Monday March 16, 2020

Page 62

doing. It would be as if I was -- I guess on a US presidential campaign where people would stand in front and ask questions from a media thing randomly, but that is not how any of these media meetings actually occurred, so.

Q. Do you recall if these training sessions were recorded?

A. I do not know.

Q. Do you remember a training session you had on March 18, 2016?

A. I do not.

Q. Do you recall a training session you had on March 22, 2016?

A. I do not.

Q. Dr. Wright, I am going to upload to the share file 172509?

(Exhibit Defense 172509 referred to)

BY MR. FREEDMAN:

Q. Do you have that there?

A. I have an e-mail up on screen.

Q. Okay, who is that e-mail from?

A. The from statement is a Nick Caley.

Q. Who is it to?

A. Multiple people including myself, Ramona, Catherine Kauchemann, Robert McGregor,

Page 63

Stefan Matthews, which is "Stefan nCrypt" in there, Alan Edwards and Victoria Brookes.

Q. What is the subject?

A. "Media training notes".

Q. Can you read it for the record?

A. Yes, I can.

Q. Can you go ahead and do that?

A. "Hello, Craig and Ramona. Please find the attached notes and transcripts from the first two media training session[s] to consider ahead of our next one on Thursday 7th April. Also it would be useful if we could see a draft of what you might say at the press conference on 26th April so we can discuss that in the session next week also. Many thanks. Nick."

Q. I am uploading to the share file defense 172510?

(Exhibit Defense 172510 referred to)

Q. Do you guys have the document in

Page 64

A. That is correct.

Q. Do you see in bold and then not bold underneath it, just read the first one for the record, the question and answer?

A. The bolded one?

Q. Yes.

A. "Craig, how much does a White Paper take to construct? I know it's a daft question... it could be hundreds of thousands of dollars? Quite easily, including patenting, yes".

Q. Do you recall that question and answer?

A. No.

MR. RIVERO: Object to the form.

BY MR. FREEDMAN:

Q. Can you go down to page 14 for me. This is a note, the answers across the top, let me know when you get there, Bates label 172523?

A. I am on page 14, "notes and alternative answers".

Q. Can you read that bold paragraph under the word overview for the record?

A. I can. I assume you want me to read it?

Q. Please.

Page 65

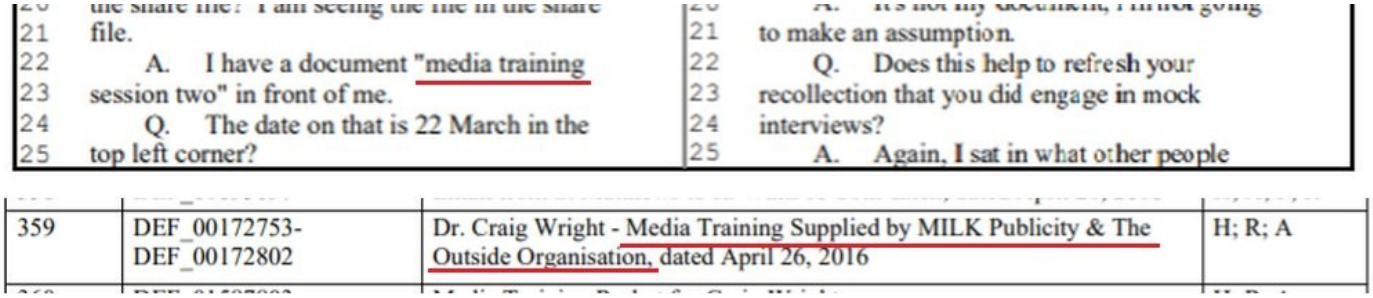
A. "Our second training session was different to the first in that rather than a full on mock interview, we moved on to analysis of harder questions and how they might be better answered. We then picked up the mock interview as the answered were practiced. The session saw a real move forward for CW in terms of both tone and content. He was far less defensive on difficult questions. He dominated the interview in the right way and he shows humility at the right level. Even on technical subjects he made complicated matters (to the layperson) very clear. His passion drew you in and he importantly didn't lose his temper on the tricky subjects."

Q. CW in that paragraph is Craig Wright?

A. I didn't write the document.

Q. Do you take that as a reference to Craig Wright?

A. It's not my document. I'm not going



file.
A. I have a document "media training session two" in front of me.
Q. The date on that is 22 March in the top left corner?

to make an assumption.
Q. Does this help to refresh your recollection that you did engage in mock interviews?
A. Again, I sat in what other people

359	DEF_00172753- DEF_00172802	Dr. Craig Wright - Media Training Supplied by MILK Publicity & The Outside Organisation, dated April 26, 2016	H; R; A

Mockup of two Kleiman v Wright court filings

Apparently, somewhere in March 2016, Craig Wright signed block 1 for Andrew O'Hagan, author of The Satoshi Affair. It appears he did not use the string "CSW" in the text, like he did later with Gavin Andresen on April 7, 2016. From The Satoshi Affair we also learn that "All the journalists had signed NDAs and embargos. (1)"

"Just before these sessions took place, in April, I asked Wright what had happened in Antigua. 'We discussed the whole PR strategy,' he said. 'The truth thing is going to happen.' He talked about Matonis and Andresen. 'We're going to bring them in on reveal sessions in the next few weeks. I guess that's the way it has to be. Do I like it? No. But I haven't really been given a choice. I'm between a rock and a hard place because of whoever outed me last year.' **He said very clearly at a meeting with me that he would not sign with the key in public.** [*This is, of course, an immediate red flag!*] We agreed that he would do it for me at home, signing with the private key from one of Satoshi's original blocks. He would do for me what he was going to do for Matonis and Andresen, and this would prove beyond doubt, he said, that he was Satoshi."

Photo credits: Andrew O'Hagan

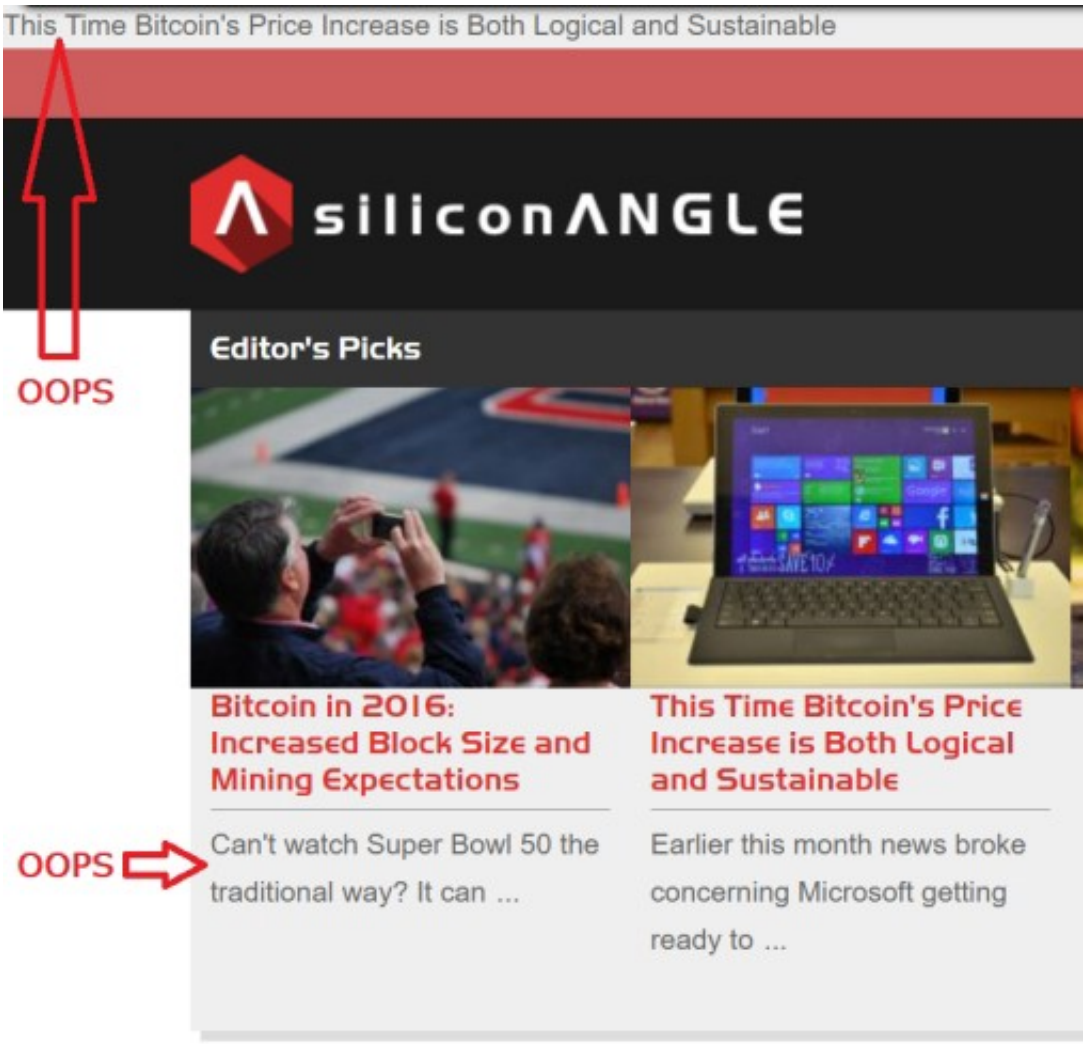
"He was about to use the original cryptographic key to sign a message to me and it was as if he was dropping a sugar lump into my tea. He typed the words, 'Here I am, Andrew,' and rested his fingers. 'This gives us that little block there,' he said, before verifying the signature. He looked sheepish and resigned in his blue checked shirt. 'Welcome to the bit I was hoping to bury,' he said. He leaned back and I noticed a samurai sword by the desk. I shook his hand. Then I stared at the screen and considered how strange it would be to live with a secret for seven years and then feel no relief when it finally came out. Perhaps it never felt like a professional secret; it felt like a part of his being, and now he was giving it up. 'I want it in layman's terms,' I said. 'Explain what you just did.'

'I just digitally signed a message using the first ever mined address on bitcoin.'" — Andrew O'Hagan (1)

March 6, 2016

"Early March 2016, we notice that Craig had started to practice how to adjust

the Silicon ANGLE website copy, and its articles." — Arthur van Pelt (5)



"Note, for example, that the February 17, 2016 article "This Time Bitcoin's Price Increase is Both Logical and Sustainable" by James Farrell is a full copy text-wise of a January 7, 2016 Nasdaq article by Martin Tillier." — Arthur van Pelt (6)

March 23, 2016

The second of several signing sessions, sometimes called proof sessions, is for Jon Matonis. Note again that they are all private, with no exceptions. Jon Matonis his blog post explains on May 2, 2016:

"Then, on June 4th 2015 during a conference, I arranged to meet fellow Bitcoin advocate, Craig Steven Wright, for a cup of coffee at the top floor of the AMP headquarters building in Sydney, Australia. After discussing many technical and economic aspects of the current Bitcoin protocol debates, I returned to my hotel room after an exhausting day. I remember saying to my wife that I had this weird feeling of having just met Satoshi. Of course, I continued the dialogue with Craig in the months after returning from Sydney and leading up to a private proof session in late March 2016."

"During the London proof sessions, I had the opportunity to review the relevant data along three distinct lines: cryptographic, social, and technical. Based on what I witnessed, it is my firm belief that Craig Steven Wright satisfies all three categories. For cryptographic proof in my presence, Craig signed and verified a message using the private key from block #1 newly-generated coins and from block #9 newly-generated coins (the first

transaction to Hal Finney). The social evidence, including his unique personality, early emails that I received, and early drafts of the Bitcoin white paper, points to Craig as the creator. I also received satisfactory explanations to my questions about registering the bitcoin.org domain [*this has been thoroughly debunked elsewhere, but that's another story for another day*] and the various time-of-day postings to the BitcoinTalk forum. Additionally, Craig's technical working knowledge of public key cryptography, Bitcoin's addressing system, and proof-of-work consensus in a distributed peer-to-peer environment is very strong [*it isn't, it's easily debunkable technobabble, obfuscated with rants about totally unrelated subjects, but that's also another story for another day*].

According to me, the proof is conclusive and I have no doubt that Craig Steven Wright is the person behind the Bitcoin technology, Nakamoto consensus, and the Satoshi Nakamoto name." — Jon Matonis (7)

Okay, Jon.

March 29, 2016

Then, the rumours that camp Craig Wright is up to something start spreading…

“During the last few months Craig and his accomplices have been very active quietly networking in the Bitcoin industry. Their pitch: Craig is the real thing and the press got it wrong. Their elaboration on the details would lower your IQ to hear it, so I won’t bore you with it — needless to say, few who are

thinking critically and understand the technology would believe it and that's probably the point: it's a filter. If you do listen long enough you find out that Craig, earnest creator of Bitcoin, and true heir to a MILLION BTC apparently has some procedural issues with a trust securing his funds, which could all be resolved with a bit of money — but unfortunately, the evil dictators controlling his country have frozen all of his money… and that's where you come in dear reader. You see, he just needs a bit of money to complete the paperwork to obtain the coins, and — of course — secure safe passage to free-er lands…" — Reddit user runtrage (8)

March 31, 2016

Which even leads to an article in the Financial Times AlphaVille section.

"Bitcoinland is abuzz with speculation Craig Steven Wright will out himself as Satoshi Nakamoto, the cryptocurrency's pseudonymous creator, within the next two weeks and that he is looking for backing in his verification from some of the industry's biggest players."

"Now, after nearly four months of silence — and a bitcoin community mostly resigned to the notion that the story was an elaborate hoax — conditional approaches are being made to media and other institutions in connection to an upcoming "big reveal" of Wright as Satoshi Nakamoto.

The narrative being pitched is that on a pre-agreed date — ranging from April 7 to April 14 — Wright will publicly perform a cryptographic miracle which proves his identity once and for all. Those institutions being offered the inside scoop on his life story, meanwhile, are supposedly being asked by those claiming to be Wright's legal representatives to abide by strict embargoes, timed to pre-empt the stage-managed revelations and the public press conference to follow.

Screenshot from the article.

The attempt at media management, however, echoes a familiar pattern.

The dossier of leaked emails used by Wired and Gizmodo as the source for their story was also heavily circulated to rival media outlets by anonymous parties weeks ahead of its ultimate publication." — Izabella Kaminska (9)

April 2, 2016

The first direct contact between Craig Wright and Gavin Andresen is being established. Over the next few days, Craig and Gavin keep sending each other emails.

"In December, after Wired published the story about Wright possibly being Satoshi, Andresen told the magazine he'd never heard of Craig Wright. But he began to believe in Wright once he started corresponding with him by email in early April." — Andrew O'Hagan (1)

"Q: Okay. And just — this is about five days or so before the proof session in London that took place on April 7th?
A: Correct." — Vel Freedman, Gavin Andresen (10)

April 6, 2016

"Q: Do you recognize this email — or these emails, I should say?
A: Yes.
Q: And it's a — it's a series of emails between you and Craig?
A: Yes.
Q: On or about April 6, 2016?
A: Yes."

"Q: And then way at the bottom, you've told him — and this is a paraphrase, but let me know if it's fair — that you've given some thought to the meeting with him tomorrow; you'll be bringing your laptop and a new USB stick, and you'd like a couple of things to verify, one being a PGP signed message, like you had said earlier, and you even gave the phrase "so it goes" as what you wanted him to sign, right?

A: Yes.
Q: And then one or more messages signed using keys from the early Bitcoin blocks, right?
A: Yes.
Q: And then copies of never-before published private emails or forum posts between you and Satoshi?
A: Yes.
Q: And consistent with your — would it be consistent with your testimony earlier that you may have gotten №2 [*signed message from early Bitcoin block*], but you did not get №1 [*PGP signed message*] and №3 [*private emails*]?
A Yes.
Q: Okay. Thank you. And this was the day before you met Craig in London for the proof session, right?
A: Yes." — Vel Freedman, Gavin Andresen (10)

April 7, 2016

The Big Day. Gavin Andresen gets his signing. Or did he? Watch the red flags.

"On the morning of April 7, Andresen took a red-eye to London and proceeded directly to a hotel in the Covent Garden district. He met Wright and two associates [*Stefan Matthews, Robert MacGregor*] in a conference room" — Andy Greenberg (3)

Clockwise from top left: Hal Finney, Gavin Andresen, Robert MacGregor, Stefan Matthews (The Satoshi Affair)

“Andresen crossed the Atlantic overnight, arriving at the Covent Garden Hotel at 11 a.m. on 7 April. He went to his room — which had been booked, as had his flight, by nCrypt — and had two hours’ sleep, after which MacGregor and Matthews turned up. ‘They gave me a lot of the background and explained their involvement,’ Andresen told me. When Wright turned up at the hotel, Andresen found it easy to talk to him, ‘although I was so jet-lagged at one point,’ he wrote, ‘I had to stop him from diving deep into a mathematical proof he’d worked out related to how blocks are validated in bitcoin.’

Matthews had booked a conference room in the basement, and MacGregor could see that Wright was very emotional when he entered the room. ‘He knew this was it,’ MacGregor said to me. ‘It’s one thing to prove his identity to you and me, but the bitcoin community is something else. He knew that they would believe Gavin.” — Andrew O’Hagan (1)

“Mr Andresen said he travelled to London to meet Mr Wright who showed him proof that he and Satoshi Nakamoto — the pseudonym adopted by Bitcoin’s creator — were one and the same.

“He signed in my presence using the private key from block one, the very first mined Bitcoin block, on a computer that I am convinced had not been tampered with,” he said.” — Zoe Thomas (11)

Note that this “Bitcoin block one” anecdote is not confirmed by Gavin Andresen in his deposition (way more about that later), where Gavin only talks about Bitcoin block 9, or sometimes 10 when the Bitcoin Genesis block, many times also labelled as Bitcoin block 0, is included in the count.

“It was about 5.30 p.m. when he finally logged on to his laptop to do for Andresen what he had done for me in his office at home, sign a message with the key and have it verified. Andresen looked on. Wright had just used Satoshi’s key. At that point, it seemed to some of those in the room that Andresen’s body language had changed; he seemed slightly awed by the situation. He reached over to his bag and took out a brand-new USB stick and removed it from its wrapping. He took out his own laptop. ‘I need to test it on my computer,’ he said. He added that he was convinced, but that if people were going to ask him, he had to be able to say that he’d checked it independently. He pointed to Wright’s laptop and said it could all have been pre-loaded on there, though he knew that was unlikely. But he had to check on his own computer and then they would be done. He said the key could be used on his laptop and saved to the memory stick and that Wright could keep it. But for his own peace of mind, and for due diligence, so that there wasn’t a chance of fraud, he had to see it work on a computer that wasn’t

Wright’s own.

Wright suddenly baulked. He had just signed a message to Andresen from Satoshi, he said, and had demonstrated his complete familiarity with their correspondence, but, in his mind, what Andresen was now asking for was of a different order. 'I had vowed,' Wright told me, 'never to show the key publicly and never to let it go. I trusted Andresen, but I couldn't do it.' Wright got up from the table and started pacing. He had clearly believed he would be able to get through the proof session without this. In fact, he had said in my presence several times over the preceding months that he would never hand the key over to anyone or allow it to be copied or used on someone else's machine. 'I do not want to categorically prove keys across machines,' he wrote to me in an email."

This is TOTALLY inconceivable. It appears that Andrew O'Hagan is not wording it correctly, which is not helpful in understanding what exactly is happening here. What Gavin is asking is not the private key itself to be moved from one place to the other, but the verification outcome (which does not contain the private key, but the digital signature) that can and should be independently verified everywhere. Craig obviously has big issues with this standard procedure, which, in my opinion, clearly indicates that this type of signing is only meant to work on his own controlled (read: hacked) technical environment.

"The solution had to be a fresh computer straight out of the box. MacGregor called his assistant and gave her the task. 'This is how you get your One,' he said to her. (In his company the best score you could get in a staff appraisal was a One.) It was just before 6 p.m. on a Friday night and they needed a brand-new laptop in Covent Garden. The assistant got hold of one and rushed over from Oxford Circus to the hotel. The new laptop was lifted out of the box. It took a while to connect it to the hotel's wifi and to load the basic software. 'During all that time,' Andresen told me, 'it was obvious Craig was still, even then, deeply hoping his secret identity could remain secret. It was

emotionally difficult for him to perform that cryptographic proof.'"

"Everyone waited with bated breath as Wright used the new laptop to open the Satoshi wallet and set about signing a new message to Andresen. It failed. It wouldn't verify. He tried it again and again, until Andresen remembered that Wright hadn't typed 'CSW' at the end of the message the way he had in the original, the one he was seeking to verify. When he put 'CSW' at the end of his message to Gavin it said: 'Verified'. Wright had demonstrated, on a brand-new laptop, that he held Satoshi's private key." — Andrew O'Hagan (1)

To add, note that Electrum, who builds the Python-based Electrum Wallet that, as far as we know, has been used by Craig throughout all the signing sessions, provided the following information on May 3, 2016 about April 7, 2016 on the Twitter platform. Red flag? One would think so, as a new installation of Electrum Wallet software should have been verified before any usage, especially in this high profile case! We will learn that Gavin Andresen hardly paid any attention to these important details.

Source: https://mobile.twitter.com/ElectrumWallet/status/727366861592076288

Now let's see how Gavin Andresen describes the whole signing session. Gavin was deposed in the Kleiman v Wright lawsuit on Wednesday, February 26, 2020.

"Q: Okay. So after you — you met with Craig in this initial conversation, did you go right to the proof section — proof session?
A: Yes. The proof session was — it was one continuous meeting in that room at the hotel.
Q: Can you — can you walk me through that proof session?
A: Sure. I — I do recall producing a brand-new USB stick. So I had my laptop with me and a — put a brand-new, sealed-in-the-package USB stick on the table, which I expected Craig to take and produce some digital signatures that I could then verify on my laptop. [*note that Gavin indeed did not expect*

the private key itself!] That did not happen. Instead, a laptop was procured, a brand-new laptop was procured by an assistant [*huge red flag again, it is inconceivable that a digital signature, not being the private key itself, should not be allowed on Gavin's laptop*]. I think it was an assistant for one of the — I don't know whose assistant it was. Craig and I waited in the room while the laptop was purchased. It was then unpacked and booted up for the first time in front of me. And the proof then was Craig downloaded and installed software. And then, after some — many hours, I don't recall how many hours, but it took much longer than — than expected [*red flag again, downloading Electrum Wallet and installing it indeed takes minutes, not hours*], at the end of that, I was convinced that he had taken one of the early blocks and signed a message [*"Gavin's favorite number is 11-CSW"*] using its private key.
Q: Which block did he use?
A: It was the block that — I believe it was block 10, the block that — that had the 10 transaction from Satoshi to Hal Finney."

"Q: Did you choose the message you wanted signed?
A: Yes.
Q: Including the CSW at the end of the message?
A: No, I did not choose the including CSW at the end of the message.
Q: So he added that on his own?
A: Yes."

Crucial information here. Craig Wright added "CSW" at the end of Gavin's message. Please keep this in mind, as I will come back to this later.

"Q: Okay. Now, you previously testified about a cryptographic proof session in London. Do you recall that?
A: Yes.
Q: And that cryptographic proof was related to either block 9 or 10, depending on how you count, correct?
A: Yes.
Q: Did — did Dr. Wright show you any cryptographic proofs for any other

blocks?
A: No.
Q: Do you have any knowledge as to whether he has the ability to control any other Bitcoin blocks?
A: No."

Note that no block one is mentioned.

"Q: Okay. Do you recall the date that you had the proof session with Dr. Wright in London?
A: That was one of the things I looked at this morning, and I believe it was April 7th.
Q: Okay. All right. And do you recall what time of day it was that the actual proof was shown to you?
A: I think it was late afternoon.
Q: Okay. So would it be fair to say that, at most, you can know that in the late afternoon of April 7th, Dr. Wright could have had the private key to block 9 or block 10, correct?
A: Yeah. Yes."

"Q: Okay. Got it. Now, I want to go to when you flew to London to attend the private proof session with Dr. Wright. You stated that you met Dr. Wright I believe it was maybe two hours after you got off the flight. Do you recall something along those lines?
A: If I recall correctly, I got a little bit of sleep at the hotel room.
Q: Um-hm.
A: And then I met with the, quote-unquote, money guys [*Gavin Andresen refers to Stefan Matthews and Robert MacGregor as "the money guys or — men" several times in his deposition, as he correctly thought there was a financial motivation behind Craig Wright signing for him*]; and then, yeah, an hour or two after meeting with them, Craig Wright came into the room.
Q: Okay. And do you recall how much sleep you got?
A: Just a couple of hours, one or two hours." — Vel Freedman, Gavin

Andresen (10)

So, question remains how Craig Wright implemented his "hack" (I will come back to that in more detail) to do a successful signing on another machine. One of the theories is that since Craig knows how to set up fake websites (ATO's finding of Craig's virtual set up of a fake Al Baraka office and the siliconANGLE website forgery come to mind), that he had also prepared a fake Electrum Wallet website with the hacked software as a download.

Another theory is that Craig implemented the hack on the fly in the genuine Electrum Wallet software downloaded on the newly bought laptop, as the session took many hours, according a perplexed Gavin Andresen.

Craig Wright Signing Sessions 2016

April 11, 2016

Wired magazine (Andy Greenberg) is also sensing that something is going on.

"FOUR MONTHS HAVE passed since the world learned the name of Craig Wright, a man who, as WIRED wrote in December, either created Bitcoin or very badly wants someone to believe he did.

Now rumors are swirling through the Bitcoin world that Wright himself is poised to publicly claim — and possibly offer some sort of proof — that he really is Satoshi Nakamoto, the mysterious inventor of Bitcoin. If he does, he'll have to convince a highly skeptical cryptography community for whom "proof" is a serious word, and one that requires cryptographic levels of certainty.

The suggestion is that Wright, an Australian cryptographer and security professional, has arranged to perform a demonstration for media in London sometime in the next week that's intended to convince the world he's bitcoin's creator. Luckily for any legitimate claimant to the Satoshi throne —

and for bitcoiners tired of the long succession of unproven candidates and speculation — there are some clear, almost incontrovertible ways for Satoshi Nakamoto to prove himself." — Andy Greenberg

Source: http://web.archive.org/web/20160412132405/http://www.wired.com/2016/04/prove-youre-bitcoin-creator-satoshi-nakamoto/

April 26, 2016

"[*The journalists*] would each be allowed a brief interview with Wright after he had demonstrated to them his use of the Satoshi key. These meetings would take place at the offices of the PR company in Tottenham Court Road on Monday, 24 April and Tuesday, 25 April." — Andrew O'Hagan (1)

Although we can consider the information of Andrew O'Hagan highly trustworthy, here is where a few typos have slipped through and made it to the final article nevertheless. Let's first note that April 24, 2016 was on a Sunday, and April 25, 2016 was on a Monday.

But also note that we know the exact dates, Tuesday April 26, 2016 and Wednesday April 27, 2016 from an exhibit that has been filed in the Kleiman v Wright lawsuit (source of the filing under the image).

Source: https://www.courtlistener.com/docket/6309656/550/4/kleiman-v-wright/ (page 209–210)

This article will continue the timeline with the dates and times from the planning above as a guideline.

April 27, 2016

The BBC was the first to arrive for their signing session with Craig Wright.

"At our first meeting — without a television camera — we roamed freely over all sorts of territory."

"It was in a conference room above a coffee shop a fifteen minute walk from

BBC Broadcasting House that we first met the man who says he is Bitcoin creator Satoshi Nakamoto. As we walked in, three or four people [*Stefan Matthews, Jon Matonis, Craig Wright, Ramona Watts*] were waiting around a table — but which one, I wondered, was the father of Bitcoin?" — Rory Cellan-Jones (12)

"When I turned up at Starbucks in Tottenham Court Road, Wright, Ramona and Matthews were already there. Wright was sulking a little. It had been decided that, as well as the demonstration, **the journalists would be given a memory stick to take away with them, showing the signed Satoshi message.** (**Wright later told me the stuff he put on it was fake. There wasn't anything on there they could understand, but it certainly bore no relation to any of Satoshi's keys.**)"

And here we find another red flag. At all costs is Craig Wright avoiding that anything from the signing sessions goes to the public for further scrutiny. He even goes as far as putting "fake stuff" on memory sticks.

Craig Wright and Rory Cellan-Jones (Photo credits: BBC)

"Rory Cellan-Jones, the BBC's technology correspondent, was led into a conference room with his producer, Priya Patel, and Mark Ward, a technology correspondent for the BBC News website. Wright sat at his laptop, hardly looking up, and a screen on the wall showed what he was looking at. Matonis was in the room, and so was Matthews. Ramona had gone upstairs."

"He then went into more detail about the cryptographic proof. 'The Genesis block is block zero,' Matonis said. 'And you can't spend any of the blocks in that chain — which means that the ones that come after that (which are spendable) can be attributed to the creator of bitcoin.'

'And what would they be called?' Cellan-Jones asked.

'In succession they'd be called block 1, block 2 etc. Now this morning, Craig

is going to demonstrate signing blocks 1 through 9. I personally witnessed the signing of blocks 1 and 9, so this is not going to be a transfer of bitcoins, it's going to involve a signing of a message, which he'll do with the private key and which will be verified by the public key. Are we clear on that?'

Eventually, Wright asked Cellan-Jones to give him a message. 'Um. "Hi, historic message to the BBC."' Wright typed the message and added a bit of commentary as he did so.

'This message will verify, but if I change a single digit, it won't,' Wright said as he signed the message using block 9.

'This is the only key that we know is definitely owned by Satoshi because it was used with Hal Finney,' Matonis added."

Note that Craig Wright "added a bit of commentary". Did he maybe add "CSW" here (again)?

"The BBC planned to come back the next day with cameras."

"Then a man arrived from the Economist, Ludwig Siegele, a man in a grey suit. He was less immediately friendly but his questions were fine-grained. You could see he wasn't entirely comfortable with this very PR-managed way of outing Satoshi. Wright signed a message for Siegele using block 9, and had the private key verified by the computer. 'I'm sorry,' Siegele said, 'but I'm still a little unsure what that proves.' 'It proves I have the private keys,' Wright said. 'All the original private keys.'"

"That afternoon, [...] Wright went off to Parsons Green to have his photograph taken for GQ." — Andrew O'Hagan (1)

"Mr Wright has also demonstrated this verification in person to The Economist — and not just for block 9, but block 1 [*This is not confirmed by Andrew O'Hagan in The Satoshi Affair, who only talks about block 9*]. Such demonstrations can be stage-managed; and information that allows us to go

through the verification process independently was provided too late for us to do so fully. Still, as far as we can tell he indeed seems to be in possession of the keys, at least for block 9." — Ludwig Siegele (13)

According the planning, the next session, with people from GQ, happened also on April 27, 2016.

"[*Stefan*] Matthews described what happened at the interview with the [*GQ*] magazine's senior commissioning editor, Stuart McGurk. 'It actually went quite well,' Wright told me. 'The journalist was nice, but he brought along this complete wanker of an "expert"!'

The man they were talking about is a university lecturer in cryptology. McGurk brought him along to help verify the claims. 'It was hilarious,' Matthews said. 'Craig threw the guy out.' According to one witness, he'd questioned Wright quite forcefully about his understanding of public and private encryption keys. 'He was totally in the guy's face at one point.'

'He was telling me he was more qualified than I am,' Wright said. 'It became a nice interview but this guy was a complete idiot and I told him to get the fuck out.' Matonis — who was there — said the scene was intense." — Andrew O'Hagan (1)

Intense is probably a bit of an understatement, listening at the material that GQ released.

"The other people in the room are economist and Bitcoin Foundation founding director Jon Matonis, the expert witness for the PR agency brokering the interview, and its two representatives, attempting not to look too panicked." — Stuart McGurk (14)

Let's move on with The Economist session.

"The Economist — along with the BBC and GQ Magazine — had access to Mr Wright before the publication of his post (see footnote). We interviewed him,

reviewed the documents he has provided and talked to bitcoin insiders [*likely Stefan Matthews, Robert MacGregor and Jon Matonis*] who have communicated with Mr Nakamoto in the past and who had access to the same information." — Ludwig Siegele (13)

April 28, 2016

It appears that BBC did not strictly follow the original planning, as they didn't do the television interview on the same day but returned the next day as Andrew O'Hagan describes.

"The second time we met, to film a television interview, the mood changed." — Rory Cellan-Jones (12)

Which is visible in the material that BBC filmed.

"Mr Wright has revealed his identity to three media organisations — the BBC, the Economist and GQ. At the meeting with the BBC, Mr Wright digitally signed messages using cryptographic keys created during the early days of Bitcoin's development. "These are the blocks used to send 10 bitcoins to Hal Finney in January [*2009*] as the first bitcoin transaction," said Mr Wright during his demonstration." (15)

April 29, 2016

Milk Publicity, one of two parties (the other being The Outside Organisation) involved with Craig Wright's reveal as Satoshi Nakamoto, supported by his 'signings' for several parties, sends the agenda around for the upcoming May 2. It is visible how meticulously, almost desperately, parties are trying to keep control of the narrative for every detail that might pop up during the reveal.

Source: https://www.courtlistener.com/docket/6309656/550/4/kleiman-v-wright/

May 2016

The big month has arrived. The NDAs that all media parties had signed had a deadline of May 2, the day that the press was allowed to start publishing their material about the signing sessions they had experienced. But in the meantime, Craig was also working on his siliconANGLE website forgery.

"But, by May 2016, Craig got it right. He knew how to add (Bitcoin related) articles by adjusting existing articles on his copy of the real Silicon ANGLE website.

No more oopsies. At first glimpse, that is..."

Source: https://web.archive.org/web/20160509152048/http://silliconangle.com/

"As the "Craig Wright faces criminal charges..." article itself shines a painful light on how Craig performs plagiarisms: shameless, and by the boatloads.

No less then 8 sources were used to create this article, while only 1 sentence has not been copied from elsewhere." — Arthur van Pelt (2)

Note that it is not unlikely that these quotes come from one or a few articles only, but the main message remains: it has Craig Wright's plagiarizing fingerprints all over it.

May 2, 2016

On this day, Craig Wright publishes the now infamous Sartre blog post. It was not received well, and that is an understatement.

"In the remainder of this post, I will explain the process of verifying a set of cryptographic keys." — Craig Wright (16)

"At 7.51 a.m. on 2 May 2016 all was quiet on the Twitter front. Well, not quiet, but the names Satoshi Nakamoto and Craig Wright were nowhere to be seen. This was the day of reckoning, the day the embargo would lift and the media outlets could run their pieces and name Satoshi. [...] At 8 a.m., Wright posted a blog containing the supposed hash of the Sartre speech and

various postings about himself as Satoshi. At the same moment, Gavin Andresen posted a message to his blog. Title: 'Satoshi'. 'I believe Craig Steven Wright is the person who invented bitcoin,' it began."

"By midday the blog was receiving the wrong sort of attention. A number of researchers had studied what Wright had written and noticed that the explanation was fudged — worse than fudged, it was faked. Something that he said was signed with the Satoshi key had, in fact, been cut and pasted from an old, publicly available signature associated with Nakamoto. It was astonishing and the buzz quickly grew fierce." — Andrew O'Hagan (1)

Gavin Andresen receives a rather crucial email from Craig Wright during the day, after things went haywire with the Sartre blog post. Craig admits he is the one adding blog posts to drcraigwright dot net.

"Q: Is this an email from Craig to you?
A: Yes.
Q: And you start off by saying to him, "I'm starting to doubt myself and imagining clever ways you could have tricked me." Well, let me take that back. He wrote you an email on May 2nd saying, We F'd up and I loaded the wrong post. I'll be loading the correct one shortly."

Next is an email from an unknown date, as the date is not mentioned during the deposition quoted, but the content appears to refer to the just-failed Sartre blog post, and "loading the correct one shortly":

"Q: So I am handing you what's been marked as Plaintiffs' Exhibit 24, and it's Bates-labeled Gavin 161. And Craig says — this is an email from you — do you recognize this email?
A: Yes.
Q: It's an email from Craig to you?
A: Yes, and Jon Matonis.
Q: And Stefan Matthews?
A: And Stefan Matthews.

Q: And he says, "Please hold that thought. **I'm going to re-sign the message and post a new, never-used signature from 9.**" So he has clearly committed to sign using the block key — using the private key of block 9; is that right?
A: Yes.
Q: Did he?
A: No.
Q: Even though it would have been simple for him to do so?
A: Yes.
Q: Okay." — Vel Freedman, Gavin Andresen (10)

There you go, another red flag. Promising to make a public signing on a block used before for a private signing, and not doing it. Because Craig knows he can't genuinely sign, except fake a signing on his own controlled environment.

Meanwhile, on Craig's Twitter account, a flurry of somewhat mysterious messages appear on May 2, 2016. They represent to be written by someone else, the tone and writing style is clearly Craig Wright himself, however.

Source: http://web.archive.org/web/20160508181815/https://twitter.com/dr_craig_wright

May 3, 2016

*Despite the turmoil, Craig finds time in the early morning of May 3rd to write a little, somewhat bizarre and obfuscating, article that gets an immediate publication on The Register website: "**I am Craig Wright, inventor of Craig Wright**". A quote, where Craig shows he has relentlessly been reading the online critics:*

"There are some people who claim there is a mountain of evidence that I am the *Craig Wright* who edited old blog posts to make it look like he invented Bitcoin; backdated PGP keys to make it look like he is *Satoshi Nakamoto*; claimed he has a supercomputer partnership with SGI that SGI has never

heard of; obtained two PhDs at a university that strangely can't find any record of those qualifications; and offered a worthless verification signature as proof that he is *Satoshi*.

Well, I am not that *Craig Wright*.

Nor I am the *Craig Wright* who published buggy bash scripts and command-line snippets to his blog for verification that simply don't work — or quietly load files pointed to by an environment variable."

Craig Wright also emails with Gavin Andresen on this day.

"And then you respond the next day, on May 3rd, saying, "Today, pretty please. I'm starting to doubt myself and imagining clever ways you could have tricked me." Is that accurate?
A: Yes.
Q: And what does Craig say in response?
A: Do you want me to read that?
Q: Sure.
A: He says, "There will be a post soon. It is in review to ensure it is all okay. **We are going to move coin as well**, but we need to get the trust permissions in place. Lawyers..."" — Vel Freedman, Gavin Andresen (10)

"MacGregor said that he and Matthews had since been with Wright and indicated that the encounter had been shouty and ugly. But he said it was OK now. 'We have verbal consent from the trustees to move coin, and we're just waiting on the written consent.'

MacGregor and Matthews had been in the meeting room for hours trying to work everything out. They thought it could all still be kept on track. MacGregor was writing new blog posts for Wright. He asked for my help with one of them and I explained that I had now to distance myself from the whole thing. I had got too close. MacGregor said they were going to 'flood the blog with evidence' and get Wright to 'move' some of the Satoshi bitcoin, to

transfer it to someone else in a way that only someone in possession of Satoshi's private keys could do. Andresen had agreed to be on the other end of the coin transaction."

"Rob removed his glasses. 'The first meeting we had with him yesterday ended with: "You're fired. Buy a ticket to Sydney. You fucked us. Good luck with the ATO."'

'He risks destroying his entire reputation.'

'His and ours,' MacGregor said. 'I've been taking meetings with investment bankers for the last two months. I've pulled every string I know to get meetings with Google and Uber. If he goes down in flames, I'll go down with him. I mean, he's fucked me. Millions of dollars out of my pocket, nine months out of my life. But what we have now is a very pliant Craig Wright. We're going to drag this back from the brink.'

This is where I'm thinking, here is the point where "the money men" should have stopped giving Craig Wright the benefit of the doubt. Except for Robert McGregor, who would sell his share in the whole Faketoshi endeavor and quietly leave, they didn't, and here we are. Still no proof whatsoever that Craig is Satoshi (and that will never come either, of course), a list of lies and forgeries that is still growing by the week, and Craig slowly digging his grave with numerous lawsuits with only 1 inevitable outcome: a total collapse of the Faketoshi scheme, only because of sunk cost fallacy.

'He didn't sleep last night,' Matthews said. 'He looks fucking terrible.'"

"We spoke about Wright's possible lies. I said that all through these proof sessions, he'd acted this like this was the last thing he ever wanted.

'That's not true,' MacGregor said. 'He freaking loves it. Why was I so certain he'd do that BBC interview the next day? It's adoration. He wants this more than we want this, but he wants to come out of this looking like he got

dragged into it.' He told me if everything had gone to plan, the groundwork was laid for selling the patents. It was a really big deal." — Andrew O'Hagan (1)

Then, Craig Wright publishes a second blog post, in line with the promises made to Gavin Andresen.

Screenshot from the blog post

"So, over the coming days, I will be posting a series of pieces that will lay the foundations for this extraordinary claim, posting independently-verifiable documents and evidence addressing some of the false allegations that have been levelled, **and transferring Bitcoin from an early block**." — Craig Wright (17)

May 4, 2016

"The next day, Wednesday, 4 May, Matthews was at Wright's house organising the movement of coin. The new (and final) proof session was intended to blow away the doubts created by the first. Many commentators felt it was too late, that Wright was beyond the pale, but Matthews and MacGregor had agreed with Andresen that the movement of coin, to Andresen and also to Cellan-Jones at the BBC, would undo the damage. Wright spoke to Andresen on the phone from his house — Andresen was in New York — and told him he was worried about a security flaw in the early blockchain, a problem in the way those first blocks were constructed that would make it dangerous for him to move coin, exposing him to exploitation or theft. My sources say that Andresen understood the problem and confirmed that it was all right, it had been fixed. But Wright continued to worry and was showing great reluctance about offering the final proof. Then he left the room abruptly and didn't come back." — Andrew O'Hagan (1)

"On Monday evening [*May 2, 2016*], I suggested to Wright's PR firm that if he could send me a fraction of a coin from an early Bitcoin block — which of

course I would return — that might show he had Satoshi's keys. But Wright's team [*Stefan Matthews*] came up with a different plan on Wednesday afternoon [*May 4, 2016*]. They sent me a draft blog in which he outlined a scheme that would see Matonis, Andresen and the BBC all send small amounts of Bitcoin to the address used in the first ever transaction. Then he would send it back, in what would be the first outgoing transactions from the block since January 2009. We went ahead with our payments — I sent 0.017BTC (about £5), which you can still see in the online records. Matonis and Andresen sent similar amounts. Then we waited. And waited. Then my phone rang — with the news that the whole operation was "on hold", with no reason given." — Rory Cellan-Jones (18)

"Q: And Stefan Matthews says, "CSW" — it's Craig Steven Wright — "has committed to moving a coin associated with block 9 address. The intent is for you to send a coin to that address, and then for CSW to return that coin to you." Do you see that?
A: Yes.
Q: And you provided the address?
A: Yes.
Q: Did you send the coin?
A: I did.
Q: And you never got 'em back. We covered that already, right?
A: Correct."

"Q: I'm handing you what's been marked as Plaintiffs' Exhibit 27; it's Bates-labeled Gavin 18. And this is a — does this — do you recognize this email?
A: Yes.
Q: And does it reflect an email chain between you and Stefan Matthews and Craig Wright?
A: Yes.
Q: And you initially reach out to the two of them saying that you have sent, at the time, $50 worth of Bitcoin to the block 9 address?
A: Yes.

Q: And Stefan Matthews, the money man, writes back that he sees the transaction, and then he says, “Will let you know when we do the transfer. It could be several days before we get the necessary authorization fully documented,” et cetera. Do you see that?
A: Yes.” — Vel Freedman, Gavin Andresen (10)

Then something dramatic happens. Craig Wright appears to have attempted to commit suicide. Other sources told me this attempt appeared very “staged”, as the wounds healed within days.

“Q: And then Robert MacGregor sends a message on May 4th, 2016, you’re all waiting for Craig to send this transaction, and can you read what he says to you?
A: “All Stop. Craig has just tried to injure himself and is bleeding badly in the washroom. Stefan is there with him and Ramona and I am en route. Ambulance is on its way.”
Q: So Craig tried to hurt himself?
A: That was my understanding, yes.
Q: Did you get any more details then beyond this email?
A: I believe there was a phone call, I don’t recall with who, who said that — were they at Craig’s house? I don’t recall the location, but they were somewhere. Craig disappeared upstairs and then was found bleeding with cuts to his neck, and then was taken to the hospital in — in an ambulance with an apparent suicide attempt. I think the word “suicide” was — was used.
Q: And this was by someone who was at the locale?
A: If I recall correctly, yes.
Q: And they were describing what was going on at the time?
A: I believe this happened — several days or maybe a week or more later, the phone call happened recounting events.
Q: That had — that had happened —
A: That had happened in the past, on May 4th.
Q: But you don’t recall who that was?
A: No, I don’t recall.

Q: Did you ever talk to Craig about this?
A: No. Things get dark.
Q: This stopped the public proof — this stopped the transfer of Bitcoin?
A: Yes." — Vel Freedman, Gavin Andresen (10)

May 5, 2016

On this day the sil(l)iconANGLE article forgery about Craig Wright *kicks in. On May 3, 2016 Craig Wright had created a (shortlived) article that got* picked up by the Bitcoinist website on the early morning of May 5, 2016*, allowing Craig to send this Bitcoinist article to Andrew O'Hagan, which lead to an anecdote in Satoshi Affair.*

** Date not visible in article, but the webpage metadata shows: <meta property="article:published_time" content="2016–05–05T06:58:01+00:00">*

"The next day, he sent me an email. It linked to an [*Bitcoinist*] article headlined 'UK Law Enforcement Sources Hint at Impending Craig Wright Arrest'. The article suggested that the father of bitcoin might be liable, under the Terrorism Act, for the actions of people who used bitcoin to buy weapons. Under the link, Wright had written an explanation: 'I walk from 1 billion or I go to jail. I never wanted to be out, but if I prove it, they destroy me and my family. I am the source of terrorist funds as bitcoin creator or I am a fraud to the world. At least a fraud is able to see his family. There is nothing I can do.'" — Andrew O'Hagan (1)

"The money was sent but never returned. What was going on in the hours between us being invited to take part in this proof and the moment when we were told it was "on hold"? The only reason we get for Dr Wright's bizarre behaviour, which sabotaged everything he had worked for, comes in the form of an email to O'Hagan. He sends the writer a news story that suggests the father of Bitcoin might be arrested for helping to facilitate terrorism by allowing people to buy weapons anonymously.

Dr Wright, it seems, decided he would prefer to be called a fraud than risk spending years in jail. This seems unconvincing." — Rory Cellan-Jones (19)

As we learned from The Satoshi Affair ("That afternoon, he closed down the blog — the one that was intended to lead cryptocurrency fans into a new era — but left a final posting"), Craig Wright deletes everything from his blog, and posts an image with excuse on the homepage. A few days later, the whole domain goes offline.

Irony has it that the real siliconANGLE website had paid attention to Craig's struggles during the week, which ended in the goodbye letter above, and they wrote a lengthy but very readable article on this very same day:

"The easy way for Wright to prove his connection to Satoshi, critics say, would be for him to use private Bitcoin keys that only Satoshi would likely have access to and sign a message in a publicly verifiable way. Due to the public-private key nature of Bitcoin's cryptographic security doing this would be trivial — in fact, the signature and the signed message text from Wright's private meetings could have been released publicly as proof." — Kyt Dotson (20)

Screenshot of the siliconANGLE article

May 6, 2016

For Gavin Andresen, the endorsement of Craig Wright as Satoshi Nakamoto came with consequences: although Gavin hadn't been active in Bitcoin development for a long while already (and had handed daily activities to others like Wladimir van der Laan), his Github account was blocked. Wladimir explains on his blog:

"But now something truly fishy is going on. Someone is claiming to be that creator, but is surrounded by technological and social trickery, based on backdated GPG keys, faked digital signatures, maybe classic bait-and-switch parlor tricks. Despite various red flags, many people are convinced

that a certain person is the creator of Bitcoin. There is a larger confusion than ever where truth starts and where misdirection and scams end. I am extremely concerned about this.

I wasn't sure, and am still not sure how Gavin is involved in this. It is no longer likely that he was hacked, but at the very least he is confused. When we saw the blog post convinced he found Satoshi, the prudent thing to do was to revoke his ownership of the 'bitcoin' organization on github, under which the Bitcoin Core repository currently lies, immediately.

In the past he has stated that "Satoshi can have write access to the github repo any time he asks.", so if he is absolutely convinced that this is Satoshi, there is a risk that he'd give away the repository to a scammer."

And here we pick up the rest of the story line with Andrew O'Hagan again.

"The next morning I drove through the traffic to a London suburb. It was early in the day and the high streets were empty, the happy boutiques, the delis and the wicker-and-candle dens where people come to improve their mood or do something about their lifestyle. Craig and Ramona were sitting in the corner of a popular café. They were holding hands and staring at the table. He was wearing his Billabong T-shirt — I remembered it from his description of the clothes he'd bought in Auckland when he began his long-distance run last December. He looked as he'd looked the first night I met him in Mayfair: unshaven, unslept, the scar on his face more livid, his pupils like pinpricks and his breathing heavy. He wasn't just white, he was empty-looking, and his hands were trembling. Ramona was crying."

"'So what happened on Monday,' I asked, 'when it came to writing that blog?'

'I gave them the wrong thing,' he said. 'Then they changed it. Then I didn't correct it because I was so angry. Which was stupid. I put up the wrong one. No one wants Satoshi Nakamoto. I will never be Satoshi Nakamoto. I'm not personable. You can lock me in a room and I'll write papers, I'll never be

personable.'

Ramona was crying. 'They could take us down,' she said. 'They could really take you down if they want to.'" — Andrew O'Hagan (1)

Meanwhile, Bitcoinist finds out they have been citing the fake siliconANGLE website that hosted Craig's fake article, and they feel obliged to post a public excuse.

"Editor's Note (5–6–2–16, 2:43 AM EST): The SiliconAngle piece cited in this article was produced by an impostor site posing as the real SiliconAngle. This source article does not appear on the real SiliconAngle website, and was not written by SiliconAngle reporter Collen Kriel. Bitcoinist would like to apologize to SiliconAngle and our readers for any confusion. To ensure that you are reading articles produced by the real SiliconAngle, make sure you are using the correct URL: www.siliconangle.com."

May 7, 2016

After 5 intense days, Craig Wright sends an excuse to Gavin Andresen that is not believed by the latter. Gavin calls the May 2 blog post "gobbledygook proof" with which he was "bamboozled", and in later years Gavin will also question the legitimacy of the private signing proof.

"Q: I'm handing you what's been marked as Plaintiffs' Exhibit 31. It's Gavin 41. Do you recognize this email?
A: Yes.
Q: It's an apology email from Craig Wright to you?
A: Yes.
Q: Sent May 7, 2016?
A: Yes.
Q: And in the third paragraph down, it says — Craig tells you, "At no point did I lie to you nor deceive you, but it is better that I am a hoaxer"?
A: Yes, I see that he said that.

Q: Do you believe that?
A: No.
Q: What do you really believe?
A: **He certainly deceived me about what kind of blog post he was going to publish, and that gobbledygook proof that he published was certainly deception, if not an outright lie. So at the very least, that, I consider, you know, that — he bamboozled me there.**" — Vel Freedman, Gavin Andresen (10)

The Aftermath: Other sources about the May 2016 events

A.P. Goucher (snippet from his article: Is Craig Wright?) May 2, 2016

"Anyway, this error is just about excusable since it pertains to the obscured internal details of an algorithm which people often use simply as a 'black box' for generating cryptographically secure message digests. The next sentence was much more concerning, since it suggests a serious mathematical misconception:

> ***Wright writes:*** *The number of possible messages that can be input into the SHA256 hash function totals* $(2^{128} - 1)!$ *possible input values ranging in size from 0 bits through to the maximal acceptable range that we noted above.*

This does not even remotely resemble the correct number of possible inputs, which is:

$$2^{2^{64}} - 1$$

The use of a factorial to count the number of binary strings should immediately trigger alarm bells in anyone with a rudimentary undergraduate-level understanding of discrete mathematics"

Nicholas Courtois, May 2, 2016

“Hours after his TV interview and his coming out in The Economist and elsewhere, I can confirm beyond reasonable doubt that Craig Wright (CW) has cheated us about his ability to sign messages with Satoshi’s private key.

Here is a short executive summary of facts guaranteed to be 100% exact. This is also a short and easy to check **PROOF** that Craig has lied and cheated.” (21)

Nik Cubrilovic, May 2, 2016

“Craig Wright is not Satoshi Nakamoto. He wasn’t Satoshi Nakamoto before or after Wired and Gizmodo suspected him to be last year, and he still isn’t Satoshi Nakamoto after trying to reveal himself to be on his own blog and to The BBC, The Economist, GQ, Jon Matonis and Gavin Andresen.

There is a long and fraught history in Bitcoin of claims and counterclaims about who Satoshi is, and one would think that lessons had been learned and a high standard would be set for subsequent claims regarding Satoshi Nakamoto. The proof posted today by Wright and others does not meet any standard for identifying him as Nakamoto.” (22)

David, May 2, 2016

“What I will be talking about, is how **Gavin Andresen**, a main bitcoin developer, could have been duped into thinking Wright was Satoshi. First. How weird is it that instead of just signing something with Satoshi’s public key and **releasing it on the internet**, Mr. Wright decides to **demo a signature verification on closed door** to TV channels, magazines and some bitcoin dev **on a trip to London**?” (23)

Hacker News user mappum, May 2, 2016

“Debunked! The signature in Wright’s post is just pulled straight from a transaction on the blockchain. Now the only question is how he fooled Gavin.” (24)

Let's try to answer that question in a bit. Not only Gavin Andresen but also several other people have been shown a signing that appeared legit, but came with many, many red flags. Combining these red flags, we will learn that a signing bamboozlement is very well possible, and certainly within the technical capabilities of Craig Wright.

Ryan Castellucci, May 2, 2016 (1)

"Wright's post is flimflam and hokum which stands up to a few minutes of cursory scrutiny, and demonstrates a competent sysadmin's level of familiarity with cryptographic tools, but ultimately demonstrates no non-public information about Satoshi." (25)

Ryan Castellucci, May 2, 2016 (2)

"By the time I had a look into Craig Wright's blog post that seemed to imply that he is Satoshi, others had already pointed out that the signature was copied from a 2009 transaction. The contents of the "Sartre" file, however, were still a mystery. Dan Kaminsky had a blog post up analyzing the commands from CW's post, but hadn't been able to figure that bit out, so he asked me to have a look.

Following a screenshot of the output of sha256sum Sartre, there's a screenshot purportedly the file being displayed through a program called more, but only the first 14% can be seen, making it impossible to verify. How *convenient*." (26)

Dan Kaminsky, May 2–3, 2016

"The guy took an old Satoshi signature from 2009 and pretended it was fresh and new and applied to Sartre. It's like Wright took the final page of a signed contract and stapled it to something else, then proclaimed to the world "See? I signed it!". That's not how it works. Say what you will about Bitcoin, it's given us the world's first cryptographically provable con artist." (27)

Kastalia Medrano, May 3, 2016

*Writing for Inverse online magazine, Kastalia brings together several responses to Craig Wright's failed reveal as Satoshi Nakamoto in her article "**MEET THE BITCOIN EXPERTS WHO DON'T BELIEVE CRAIG WRIGHT IS SATOSHI NAKAMOTO**". A few quotes:*

"Wright is lying," security researcher Dan Kaminsky writes to *Inverse*. "It's rare I can be so definitive, but the math isn't subtle. He says he (as Satoshi) signed some writings from the French philosopher Sartre, but the signature is seven years old and comes from Bitcoin itself. I have no idea why Wright would say these things, and I wouldn't normally care. Lots of people lie. But very credible people in the Bitcoin community are backing Wright in unusual ways and frankly they're becoming less credible."

"There are a lot of people trying to get their name out there," Green says

when asked why someone would claim to be Nakamoto if, in fact, he is not. "Even if a small percentage of people believe the claim, that's more than zero. Maybe you come out of it better off. Doesn't mean the rest of us have to pay him the attention. There's always the possibility he does come along with some real proof, but that will still require him answering why he's fooling around and not responding to the real questions. If he doesn't, I think we pretty much just forget about him. But even if he does, it leaves a lot of questions still about his credibility. By pussyfooting around so much, he's raised the bar for what he has to prove."

Kaminsky contacted *Inverse* to say that Andresen responded to him on his website. The Bitcoin Foundation Chief Scientist appears to backtrack in his support of Wright:

> *"I was as surprised by the 'proof' as anyone, and don't yet know exactly what is going on. It was a mistake to agree to publish my post before I saw his — I assumed his post would simply be a signed message anybody could easily verify. And it was probably a mistake to even start to play the Find Satoshi game, but I DO feel grateful to Satoshi. If I'm lending credibility to the idea that a public key operation should remain private, that is entirely accidental. OF COURSE he should just publish a signed message or (equivalently) move some btc through the key associated with an early block."*

Guardian Magazine, on May 3, 2016, is ruthless.

"**Craig Wright's claim to be bitcoin founder labelled a 'scam'**"

"Security researchers say that the discrepancy, combined with the absence of any other public technical evidence, suggests that Wright's post is a "scam". "That's how Craig Wright tried to fool us," writes security researcher Robert Graham. "Craig Wright magically appears to have proven he knows Satoshi's private-key, when in fact he's copied the inputs/outputs and made us think we calculated them. It would've worked, too, but there's too many

damn experts in the blockchain who immediately pick up on the subtle details."

Dan Kaminsky, another security researcher, is equally damning.

"Yes, this is a scam. Not maybe. Not possibly," he says. "Wright is pretending he has Satoshi's signature on Sartre's writing. That would mean he has the private key, and is likely to be Satoshi. What he actually has is Satoshi's signature on parts of the public Blockchain, which of course means he doesn't need the private key and he doesn't need to be Satoshi. He just needs to make you think Satoshi signed something else besides the Blockchain — such as Sartre. He doesn't publish Sartre. He publishes 14% of one document. He then shows you a hash that's supposed to summarise the entire document. This is a lie.""

Robert Graham, May 5, 2016

"Notice that the algorithms are the same. That's how Craig Wright tried to fool us." (28)

Gavin Andresen

And even Gavin Andresen already had serious reservations about his signing session back then. From his February 26, 2020 deposition in the Kleiman v Wright lawsuit, where they discuss a private email from 2016 (send by Gavin

shortly after the May debacle), he cites:

"Q: And then you say — well, why don't you read the second paragraph for me, of your email.
A: **"Given his extreme efforts to avoid releasing a public signature, I'm starting to doubt that Craig actually possesses the key he claims he has, and he did somehow manage to trick me and, perhaps, has been deceiving people for many years."**
Q: What do you think now? Was — let me take a step back. Was that an accurate statement when — when you made it?
A: Yes.
Q: And what do you think now?
A: I'm not sure what to think. I am — I might have been bamboozled." — Vel Freedman, Gavin Andresen (10)

June 20, 2016

*One day earlier, on June 19, 2016, Andrew O'Hagan published his long form article The Satoshi Affair. We've seen many quotes in this piece from that from a historical viewpoint very interesting write up. Gizmodo wrote a review of The Satoshi Affair a day later, under the title "**Craig Wright's Claims About Inventing Bitcoin Still Don't Make Any Goddamn Sense**". A quote:*

"When it comes to the supposed hack of Wright's personal emails that link him to Bitcoin's creation, Wright says they were leaked from a hard drive stolen by a disgruntled employee. That seems dubious, considering Wright's noted obsession with encryption and security (the story details Wright's multiple encrypted computers and his history as a security specialist). It's hard to imagine that someone who walked away with a hard drive belonging to Wright would be able to access the contents." — William Turton

Source: https://gizmodo.com/craig-wrights-claims-about-inventing-bitcoin-still-dont-1782303576

This anecdote about the "disgruntled employee that stole a hard drive" has

now become one of the most prolific "the dog ate my homework" memes surrounding Craig Wright, as he constantly claims to have been hacked (specifically when his Faketoshi proof is failing for the umpteenth time), meanwhile never having started an inquiry let alone put someone in court for any of the alleged hacks.

Stuart McGurk, May 2, 2016

You've not seen many quotes yet from Stuart McGurk, author employed by GQ Magazine. Reason is, his articles were published much later and more importantly, they deserve an individual highlight. It started with some background information in (now deleted, link goes to Wayback Machine) "DR CRAIG WRIGHT OUTS HIMSELF AS BITCOIN CREATOR SATOSHI NAKAMOTO" and the announcement that the interview would become available later.

"Via Mr Wright's representatives, *GQ*'s Senior Commissioning Editor Stuart McGurk was afforded a remarkably rare and candid interview with Dr Wright to verify his claims: an encounter that was also occasionally fractious and incredibly heated.

"Look, I'm doing this, then I'm disappearing," he said at one point. "I'm not doing this to try and get in the media. This will never happen again. You've got this one thing. If you don't like it, fuck off."

The interview will appear in a forthcoming issue of *GQ*."

Stuart McGurk, August 3, 2016

*Readers of GQ Magazine had to wait till August before Stuart put "**IS CRAIG WRIGHT THE BITCOIN GENIUS?**" (now deleted) online, but it was worthwhile the wait. As it contained the now infamous recording of a heated Craig Wright and a full transcript of it.*

Stuart McGurk, September 13, 2016

*Then, his first article came out in the UK: "**Bitcoin: inside the £8bn swindle**".*

"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."

Stuart McGurk, November 18, 2016

*Stuart published his most damning piece about the signing sessions debacle only by November 2016 in Australia, under a title that leaves no room for doubt about his opinion: "**Craig Wright: The Man Who Didn't Invent Bitcoin**". In it, we find nuggets like these:*

"Kleiman's former colleague at Computer Forensics LLC, Patrick Paige, contacted for his input, asks after Craig Wright: "Is he on suicide watch yet?"

His tone doesn't suggest concern."

Jimmy Nguyen Deposition

As said earlier, Robert McGregor would abandon the Faketoshi endeavor. From Jimmy's deposition on April 30, 2020 in the Kleiman v Wright lawsuit we learn more about how that went.

"Q: I'll just go where I'm getting to maybe you can help me make it easier which is I'm trying to find out how Robert MacGregor ended up out of the picture. Because you told me he was the one that purchased everything from Craig then you told me he no longer has interest in nChain. How did he get removed?
A: He became unhappy with Craig at a certain point and again I'm telling you this all second hand because I wasn't there. So it's what I've heard from other people and **he thought about closing the nChain operation at one point**. Stefan Matthews wanted to continue it and there was a transaction

which was announced in 2017 about a public investment fund in Malta acquiring the nChain set of companies from Rob's company. Basically he was unhappy with Craig and didn't necessarily want to be involved any more.
Q: Do you know why he was unhappy with Craig?
A: Yes. Well, Craig is — can be a difficult business colleague. You know, has been widely reported in the media there was an effort in the spring of 2016 I believe it was or in 2016 to show that Craig is Satoshi Nakamoto, creator of Bitcoin. It happened after there was some media articles that tried to out Craig as Satoshi I believe in the December before that this process to establish Craig as Satoshi at the end did not go well and as I understand it Rob was upset with Craig.

Source: https://www.courtlistener.com/docket/6309656/600/16/kleiman-v-wright/

Q: Can you explain what you mean "did not go well?"
A: Well, I'm telling you all that from reports obviously because I wasn't — I knew it was happening because this was when I was in talks with Rob to start working for nChain but I wasn't directly involved with it. Craig did not media interviews to come out and say I am Satoshi Nakamoto creator of Bitcoin. The Bitcoin community, you know, they're very technical people involved in cryptography. They would not believe a statement like that without some other proof and there was supposed to be — I can't remember the date it was a date in May where he was supposed to — I am not exactly sure what he was supposed to do. I think he was supposed to either sign a transaction using private keys from one of the early Bitcoin blockchain blocks which the Bitcoin community would recognize as only being held or owned or accessible by Satoshi Nakamoto and he did a — I don't know if he was supposed to sign a transaction or move a coin, I'm not entirely sure but something using private key associated with one of the first early Bitcoin blocks. He did something but — that the Bitcoin community then quickly thought well, that's — it's using — it wasn't using that private key of Satoshi. It was using information he could have found publicly so people thought well, he's just — that doesn't prove he is Satoshi.

Q: It's fair to say it was a pretty big issue at the time, right?
A: Yes, very much. There was a lot of news about both his claim coming forward saying I'm Satoshi and then there was a lot of news that came when the proof — proof, you know, session, proof providing not believed by the Bitcoin community and I think he posted something on the blog he had at the time saying I'm sorry." — Vel Freedman, Jimmy Nguyen

The Analysis

Signing Sessions List of Excuses

Before we dive into Craig's bamboozlements during the signing sessions themselves, let's first list how he is trying to avoid signing in the first place. What is notable, before, during and after the signing sessions debacle, Craig has been using an impressive list of excuses to explain away the reluctance to, or failure of the (public) signing of any early block address or sending back the BTC that Rory Cellan-Jones, Jon Matonis and Gavin Andresen send to the Bitcoin address of block 9 in May 2016 (where they remain till today).

Dorian Nakamoto, who was wrongly identified as Satoshi Nakamoto in March 2014

- Refusing without any reason given
- Making empty promises
- Trust permission not in place
- Security flaw in the early blockchain
- Suicide attempt
- siliconANGLE article (forgery) that Craig might have to go to jail
- No courage
- Only in combination with other (social) evidence (which up till today was never delivered)
- Hard drive with keys is destroyed
- Wouldn't prove ownership anyway (only possession)
- Wouldn't prove identity anyway (but does not register public Bitcoin

addresses with private keys at notary followed by a signing or transaction to make his point)
- Never agreed to do the exercise (was forced by Robert MacGregor)

As one of my friends once said: either you have 1 good excuse, or you have no excuse at all. This long list of mostly lame excuses of Craig Wright only leads to one conclusion: the guy just can't genuinely sign. He can't, and he won't, ever.

Technical debunk of the Gavin Andresen and other signings

But knowing now that several people have reported about Craig Wright signing several early Bitcoin addresses between blocks 1 and 9 (mostly block 9), let's try to find out how it is possible to bamboozle a signing. First, let's run down the most important red flags in this article.

· Signing only in private sessions, never releasing the signature to the public

· Craig Wright adds his own text, for example "CSW"

· Only Electrum Wallet is used

· Only Craig's laptop is used (with 1 exception)

· When Gavin wanted to verify the signing results on his laptop, this was refused and a new laptop was needed, which took "many hours" to set up (without verification on the Electrum website, as it appears)

Since Gavin mentioned in deposition Kleiman v Wright that during the signing session Craig added "CSW" to the text that Gavin proposed, it is worthwhile to explore this a bit more. As it appears, Gavin mentioned this red flag already to Emin Gün Sirer on May 4, 2016:

"Gavin Andresen's social authentication carries a lot of weight. And that is the implicit reason why Craig Wright's latest claim to Satoshi's crown caught

public attention: people assumed Gavin had vetted Satoshi using multiple factors. Yet when I asked Gavin about how he certified Wright, he described the process he used:

"It is possible I was tricked, but it wouldn't be an eclipse/hijack of the chain — I brought a list of the first 100 block's keys with me and verified the public key against that list. That was the only connection to the chain.

A hijack of the wifi used to download Electrum is possible; **if we were running an Electrum that reported 'verified' for any message ending with 'CSW' and not verified for anything else that would fit what happened**. I didn't bring checksums of Electrum downloads with me." (29)

So how to hack a signing with Electrum Wallet? Twitter user "Zectro" figured out, Electrum Wallet can be hacked with a few lines of code. Here an example how to change the BTC address in the background (green rows).

Source: https://twitter.com/Zectro1/status/1192576225413222405

This finding, the missing link between private signing sessions and (not) publicly releasing the signing sessions' outcome, is crucial in understanding how Craig Wright's bamboozlements with "signing" works. And knowing about Zectro's finding, it makes it understandable how a man-in-the-middle type of hack like this could also easily be made with a few lines of code that looks for a fixed string (like: just one of the letters of the alphabet, one of the numbers 0 to 9, or, indeed: the text "CSW") in the text to be signed. The consequence of such type of hack however, is that a successful verification of the signing can only be performed with the Electrum Wallet on the device it is installed upon.

And make no mistake, this text-to-be-signed hack would be an extremely simple yet powerful hack, as it would enable fraudulently signing any -fake or real- random BTC address from any Bitcoin block header, with any -fake or real- random private key! To add, as noted before, any fixed text string

could be put in the code hack before any (private) signing session to make the text that Craig Wright is using give the appearance of randomness.

But is Craig Wright even able to execute such hack on the Electrum Wallet? Most of his forgeries are quite sloppy and not very sophisticated. On the other hand, Craig does know his way in digital metadata, and earlier in his career [he hacked a coffee machine in 2008] and in 2011 he even hacked a Boeing 747 airplane!

Since this type of fraudulent signing would, of course, not survive public scrutiny, it now starts to make sense why Craig Wright never performs public signings, but reportedly only private signings where he fully controls the technical signing environment.

And since Craig Wright fails to deliver on any of his other empty promises over the years, it appears he is ramping up the performance of his only trick left from the Faketoshi bamboozle box: he is now signing "for many" and even "for groups" these days, according Calvin Ayre on Twitter on March 11, 2021.

And let's not forget about the announcement that Calvin Ayre made in August 2020: he started filming a documentary on Craig's life.

Source: https://tokenhell.com/calvin-ayre-starts-filming-a-documentary-on-craig-wrights-life-creating-bitcoin/

Will Craig Wright perform a signing in front of the camera? Will we finally see the Bitcoin whitepaper with rusty staples and coffee stains? The explanation how Microsoft patch Tuesday (released January 13, 2009) made Craig's Bitcoin network reboot 10 days earlier on January 3, 2009? Will we meet the

bonded courier that Dave Kleiman hired, and witness the unlocking of encrypted Tulip Trust files? Will we get a close up of the famous Pineapple Wifi from where 110,000 BTC was hacked from Craig's network?

Or will Craig his Faketoshi scheme have collapsed before this documentary is going to see the day of light? To be continued...

The end

Photo credits: Kristina Uffe, The Economist

Sources:

(1) https://www.lrb.co.uk/the-paper/v38/n13/andrew-o-hagan/the-satoshi-affair
(2) https://twitter.com/MyLegacyKit/status/1362173057289375754
(3) https://www.wired.com/2016/05/craig-wright-privately-proved-hes-bitcoins-creator/
(4) https://twitter.com/MyLegacyKit/status/1373178214441451524
(5) https://web.archive.org/web/20160306234354/http://silliconangle.com/
(6) https://www.nasdaq.com/articles/time-bitcoins-price-increase-both-logical-and-sustainable-2016-01-07
(7) https://jonmatonis.medium.com/how-i-met-satoshi-96e85727dc5a
(8) https://www.reddit.com/r/Bitcoin/comments/4cdsna/craig_wright_nigerian_prince_and_other_unlikely
(9) https://web.archive.org/web/20160331155411/http://ftalphaville.ft.com/2016/03/31/2158024/craig-wrights-upcoming-big-reveal/
(10) https://www.courtlistener.com/docket/6309656/599/3/kleiman-v-wright/
(11) https://www.bbc.com/news/technology-36185622
(12) https://www.bbc.com/news/technology-36185267
(13) https://www.economist.com/briefing/2016/05/02/craig-steven-wright-

claims-to-be-satoshi-nakamoto-is-he
(14) https://www.gq.com.au/entertainment/tech/craig-wright-the-man-who-didnt-invent-bitcoin/news-story/d17a269e4b2aeb331dad51e1c3e2d7cf
(15) https://www.bbc.com/news/technology-36168863
(16) http://web.archive.org/web/20160502203734/http://www.drcraigwright.net/jean-paul-sartre-signing-significance/
(17) http://web.archive.org/web/20160503160003/http://www.drcraigwright.net/extraordinary-claims-require-extraordinary-proof/
(18) https://www.bbc.com/news/technology-36213588
(19) https://www.bbc.com/news/technology-36575524
(20) https://siliconangle.com/2016/05/05/craig-wright-most-recent-alleged-inventor-of-bitcoin-says-im-sorry-and-quits/
(21) http://blog.bettercrypto.com/?p=2614
(22) https://nikcub.me/posts/craig-wright-is-not-satoshi-nakamoto
(23) https://www.cryptologie.net/article/350/how-gavin-andresen-was-duped-into-believing-wright-is-satoshi/
(24) https://news.ycombinator.com/item?id=11609707
(25) https://github.com/patio11/wrightverification
(26) https://rya.nc/sartre.html
(27) https://dankaminsky.com/2016/05/03/the-cryptographically-provable-con-man/
(28) https://blog.erratasec.com/2016/05/satoshi-how-craig-wrights-deception.html#.YM0H62gzbb0
(29) https://hackingdistributed.com/2016/05/04/logical-fallacies-hunt-satoshi/