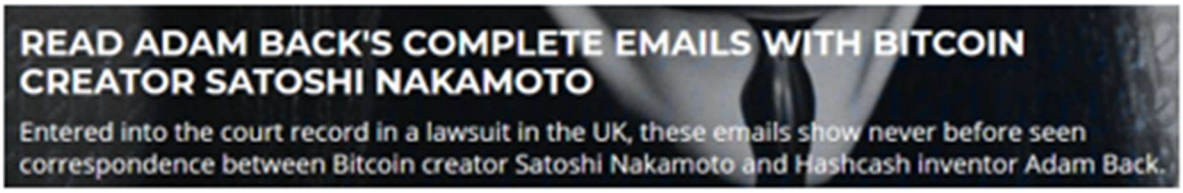
Adam Back's Checkmate Testimony at the 2024 COPA v. Wright Trial

- **Craig Steven Wright's absolute worst nightmare at the 2024 COPV v. Wright trial had to have been the testimony of cryptographer Adam Back, who was COPA's star witness. Why? Back produced a previously unconfirmed treasure trove of information from Satoshi himself.**



- **The 2008 email correspondence with Satoshi that Back produced is consistent with information on page 13 of Duality, a 21-page paper Satoshi posted online in 2018 about his early work on Bitcoin.**

EMAIL #1: SATOSHI REACHES OUT TO ADAM BACK

From: "satoshi@anonymousspeech.com" <satoshi@anonymousspeech.com>
Sent: Wed 8/20/2008 6:30:39 PM (UTC+01:00)
To: adam@cypherspace.org
Subject: Citation of your Hashcash paper

I'm getting ready to release a paper that references your Hashcash paper and I wanted to make sure I have the citation right. Here's what I have:

[5] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

I think you would find it interesting, since it finds a new use for hash-based proof-of-work as a way to make e-cash work. You can download a pre-release draft at http://www.upload.ae/file/6157/ecash-pdf.html Feel free to forward it to anyone else you think would be interested. I'm also nearly finished with a C++ implementation to release as open source.

Title: Electronic Cash Without a Trusted Third PartyAbstract: A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution. Digital signatures offer part of the solution, but the main benefits are lost if a trusted party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

satoshi@anonymousspeech.com

EMAIL #2: Adam points to Satoshi to Wei Dei's work

From: "Adam Back" <adam@cypherspace.org>

Sent: Thur 8/21/2008 1:55:59 PM (UTC+01:00)

To: satoshi@anonymousspeech.com

Cc: adam@cypherspace.org

Subject: Re: Citation of your Hashcash paper

Yes citation looks fine, I'll take a look at your paper. You maybe aware of the "B-money" proposal, I guess google can find it for you, by Wei Dai which sounds to be somewhat related to your paper. (The b-money idea is just described concisely on his web page, he didnt write up a paper).

Adam

On Wed, Aug 20, 2008 at 6:30 PM, satoshi@anonymousspeech.com <satoshi@anonymousspeech.com> wrote:
> I'm getting ready to release a paper that references your Hashcash paper and I wanted to make sure I have the citation right. Here's what I have:
>
> [5] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.
>
> I think you would find it interesting, since it finds a new use for hash-based proof-of-work as a way to make e-cash work. You can download a pre-release draft at http://www.upload.ae/file/6157/ecash-pdf.html Feel free to forward it to anyone else you think would be interested. I'm also nearly finished with a C++ implementation to release as open source.

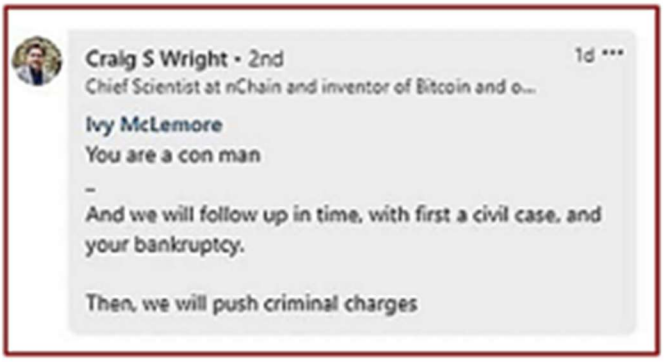
- **And here's Satoshi's version of his email correspondence with Back taken verbatim from page 13 of Duality:**

I emailed Adam first, who then pointed me to Wei, both of which I included in my original design paper. I shared with them the prerelease draft of the design paper, but I suspect neither of them have it any longer (actually I know this for a fact—if you don't believe, then ask), and the only paper that is available today is the one I sent to the mailing list, which was after the fact. When I refer to the design paper, I refer to what is known today as the **whitepaper**. I renamed it, upon public release.

Adam Back had been a regular on the mailing lists, and one of the few people thinking about how someone could come up with a true untraceable ecash around the same time as me. He was a big proponent of distributed ecash, something that many people had tried to do, but none had done successfully. For Adam, I believe his concern was how do you stop it from hyper inflating at the rate of Moore's law, which until Bitcoin, no one had found a way to do this. Most of the early ideas proposed in the cypherpunks community either remained contained to academic papers, or had been deployed but never found traction and didn't work for various reasons (a notable example is Digicash).

- **Back's email correspondence confirmed Satoshi as the author of Duality, which closely parallels the same information Satoshi told me about in 2019 that I wrote in 2022 in *Finding Satoshi.* I had pushed Satoshi hard in 2019 to come up with examples of electric communications he made with developers in 2008-2010 without success. [FS/p204, 213]**

- It's the reason the serial fabulist Wright royally freaked out – even by his standards - and threatened me with bankruptcy and criminal charges the same week my book came out.



- **Here's an essential point that underscores Satoshi's secret nature and his credibility. He was always willing to answer my questions in 2019-2020, but seldom offered new information on his own. That's why I didn't know about Duality until after my book was self-published.**

- **When I came across Duality, I reviewed all 21 pages and found 18 sentences that were verbatim or almost word-for-word what Satoshi told me orally or in writing that appear in my book. All 21 pages and the cryptogram follow.**

- Had I been on COPA's legal team, I'd have put Wright on the stand and ask him why Duality's length was specifically set at 21 pages. **A) Later in this compendium, you'll see how and why Satoshi encrypted the number 21 many times in Bitcoin's early days.**

- I'd have asked Wright why Satoshi included a separate cryptogram when he posted Duality. **A) Satoshi thought making and solving encryptions was fun.**

- I'd have questioned Wright about his testimony on how he came up with the Satoshi Nakamoto pseudonym in 2008 when the real Satoshi first posted his anonymous forename online in his online P2P profile in 2005. **A) Wright couldn't have.**

- I'd have queried Wright on how he could have used the 01-03-2009 front-page headline from *The Times* in the Genesis block when it only appeared in UK print editions and Wright resided in Australia. Satoshi was living in England then and still resides there. **A) Wright couldn't have.**

- I'd have asked Wright why he specifically chose the Satoshin@gmx.com email address he used in the Bitcoin white paper. **A) Satoshi told me the only time he used that email address was in the Bitcoin white paper because its Chaldean value is 55, the same as Satoshi Nakamoto. More on that later.**

- **The 21-page Duality follows. (The pages are numbered 25-46 in this part of the Compendium because my computer has automatically changed the numbers to match the Compendium.) Here is the preface Satoshi wrote. "Announcing the first excerpt to a literary work consisting of two parts. The excerpt is provided. I wanted to include it as a brief glimpse of history. Even for those that can't read the full book, I wanted to make this available to everyone. A short story if you will, with some of the most brought up questions and answers. I wanted the people and the facts to be known. Or as much of it. I'm still saving most for the books, the best parts hopefully. It's currently just a possibility for now. In the meantime the excerpt is included."**

- **Below is the separate cryptogram Satoshi posted with Duality.**