Claim No. IL-2021-000019

IN THE HIGH COURT OF JUSTICE
BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES
CHANCERY DIVISION
INTELLECTUAL PROPERTY LIST (ChD)

BETWEEN:

CRYPTO OPEN PATENT ALLIANCE

Claimant

- and -

DR CRAIG STEVEN WRIGHT

Defendant

DEFENDANT'S RESPONSE TO THE CLAIMANT'S REQUEST MADE PURSUANT TO CPR PART 18 DATED 4 AUGUST 2021

This is Dr Wright's response to COPA's request dated 4 August 2021 seeking further information in relation to and clarification of the defence.

The provision of the information provided below in respect of any particular request is without prejudice to any contention that Dr Wright may wish to make that the request is not strictly confined to matters which are reasonably necessary and proportionate to enable COPA to prepare its own case or to understand the case it must meet as required by paragraph 1.2 of CPR PD 18.

Under paragraph 13(2) of the defence

Of: *"Bitcoin was developed before and during 2008. Although Dr Wright's White Paper was first released in 2008, it is based on concepts Dr Wright been [sic] working on for many years previously. Dr Wright started to write the White Paper and the Bitcoin Code in 2007. The White Paper also references earlier work of others."*

Requests

1. Please identify which concepts Wright had been working on prior to the White Paper and upon which Wright alleges the White Paper is based. Please specify when Wright worked on these.

2. Please identify what earlier works are referenced in the White Paper. Please specify the identity of the work, the author(s) of the work and the date of the work.

Responses

1. The information requested is not necessary or proportionate to enable COPA to prepare its own case or to understand the case it must meet. Dr Wright will identify and provide evidence for trial as necessary and appropriate. Without prejudice to the foregoing and without limitation to such evidence, the concepts included (i) digital currency systems (ii) audit technologies (iii) incentive systems (iv) peer networks and (v) digital signatures and key exchange systems.

2. The earlier works referred to are those listed on page 9 under the heading *"**References**"*. They are as follows:

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

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

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

Under paragraph 16(3) of the defence

Of: *"…on or about 24 March 2009 Dr Wright uploaded a further version of the White Paper to the SourceForge Bitcoin Project"*

Request

3. Please specify whether this 24 March 2009 version was identical in all respects to the version uploaded on 9 December 2008. If it is not identical, please specify how the two versions differed.

Response

3. The version of the White Paper uploaded to SourceForge on 24 March 2009 was not "identical in all respects" to the version Dr Wright previously uploaded to SourceForge on 9 December 2008. Dr Wright does not recall precisely what the differences were, they were minor (such as formatting and typographical points, rather than substantive.

Under paragraph 16(4)

Of: *"Dr Wright's White Paper was not published or made available or made subject to the terms of the MIT Licence and the assertion to the contrary in paragraph 7 of the Particulars of Claim is denied"*

Requests

4. Please state whether the Defendant accepts factually that when the Bitcoin White Paper was published on its own in 2008 (whether in November or December) on SourceForge.net that it stated under the 'Details' heading that the 'License' was the 'MIT License' (as seen in the Claimant's Initial Disclosure List at document C0002).

5. If the Defendant does accept the above fact, please explain why he says the MIT License does not apply to the Bitcoin White Paper.

6. If the Defendant does not accept the fact stated in Request 4, please explain the basis for stating that the Wayback Machine printout embodied in document C0002 is false and/or otherwise incorrect.

Responses

4. Not accepted. In particular, Dr Wright does not accept that document C0002 is an accurate representation of the manner in which the page on SourceForge would have appeared to a user of SourceForge in either November or December 2008. If such is a case made by COPA (notwithstanding that C0002 on its face purports to be a capture of the website as at 6 January 2009 and not as at November or December 2008), Dr Wright requires COPA to prove that fact.

5. Not applicable.

6. This request proceeds on a false premise because COPA misinterprets and misunderstands what is presented on C0002—

(1) The "Details" entry shown in the screenshot at C0002 refers to the Bitcoin Software and Code which, as stated in paragraph 11 of the Defence, was uploaded on 9 January 2009 (Australian Eastern Daylight Time). On 6 January 2009 these materials were work in progress which had not been uploaded. Nevertheless, certain details were provided by Dr Wright about the Bitcoin Software and Code in the "Details Entry".

(2) It is apparent that the Details entry refers to computer software from the fact that it refers (amongst other things) to (a) the development status (a term applicable to software) (b) the operating system (c) the programming language and (d) the user interface (wxWidgets). When subsequently uploaded the code was made subject to the MIT Licence.

(3) The White Paper is not referred to in any of the 'Details' fields.

(4) The "Download" link shown on C0002 with regard to "bitcoin.pdf" takes the user to a separate page where there is no software which was also archived on the "Wayback Machine" on 6 January 2009 and which is accessible at the following URL—

http://web.archive.org/web/20090106085812/http://sourceforge.net/project/showfiles.php?group_id=244765

Under paragraph 25

Of: "…during 2008 and 2009, Dr Wright had discussed with a number of individuals that he was working on and had subsequently released Bitcoin and had notified various individuals that he was working on the project."

Requests

7. Please specify the names of the individuals with whom Wright discussed his working on the Bitcoin White Paper. Please specify the nature of these communications and the date on which said communications happened.

8. Please specify the names of the individuals that Wright told he had released the Bitcoin White Paper. Please specify the nature of these communications and the date on which said communications happened.

9. Please specify the names of the individuals that Wright subsequently told he had released the Bitcoin White Paper and been working on that project. Please specify the nature of these communications and the date on which said communications happened.

Responses

The information sought in Requests 6, 7 and 8 is not necessary or proportionate to enable COPA to prepare its case or to understand the case it must meet. So far as appropriate the matter will be dealt with in evidence and relevant documents disclosed. The Responses below are without prejudice to that contention, and without limitation to the evidence that Dr Wright will adduce at trial.

7. The quoted passage from paragraph 25 refers to Bitcoin generally and the Bitcoin project and not specifically to the White Paper. The individuals with whom Dr Wright discussed his working on Bitcoin included: Wing Commander Donald Lynam OM; Stefan Matthews; and David Kleiman. Moreover, Dr Wright discussed concepts underlying Bitcoin with employees of BDO and Centrebet.

8. Response 7 is repeated.

9. See Responses 7 and 8.

Under paragraph 34

Of: *"…Dr Wright has publicly stated that it is not possible to use the Genesis Block to verify his identity as Satoshi Nakamoto and such is the case."*

Requests

10. Please specify each occasion on which Wright has stated that it is not possible to use the Genesis Block to verify his identity as Satoshi Nakamoto.

11. Please specify why Wright says it is the case that the Genesis Block cannot be used to verify his claim to be Satoshi Nakamoto.

Responses

10. COPA is not entitled to a response because the information requested is not necessary or proportionate to enable it to prepare its own case or to understand the case it has to meet.

11. Dr Wright will adduce fact and expert evidence on this point in due course. In brief summary and without limitation to the evidence he will adduce at trial, the reason is as follows—

(1) The Genesis Block is an anchor block to the Bitcoin Blockchain. It is not a mined/transactional block, meaning that it was created not to be used, whether in the same manner as the mined blocks, or at all.

(2) As such, the Genesis Block address (1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa) is not linked to any private key(s) but is formulated as a Pay to Public Key Hash System (P2PKH), which can be found at line 1462 of the original Bitcoin Source Code main.cpp file.

(3) Accordingly, the Bitcoin or the BTC which have been sent to that address are not capable of being spent or otherwise transferred.

(4) Moreover, it is not possible to sign and verify a message on the Genesis Block in the manner in which Dr Wright successfully demonstrated in respect of blocks 9 and 11 in 2016.

Under paragraph 37

Of: In April 2016, Dr Wright held back-to-back interviews with Rory Cellan-Jones of the BBC and Ludwig Siegele of The Economist. During those interviews, Dr Wright demonstrated that he was in possession of the private key for block 9 of the Bitcoin Blockchain…"

Requests

12. Please particularise the technical means by which Wright says he demonstrated that he was in possession of the private key for block 9 of the Bitcoin Blockchain.

13. Please state whether Wright is still in possession of the private key for block 9 of the Bitcoin Blockchain. If Wright is no longer in possession of this private key, please explain why.

Responses

12. COPA is not entitled to a response. The information is not reasonably necessary or proportionate for COPA to prepare its own case or to understand the case it must meet. Notwithstanding the foregoing, in general terms, Dr Wright signed messages using the private key to block 9 of the Bitcoin Blockchain, which messages Messrs Cellan-Jones and Siegele each then verified using the public key to that block. Dr Wright will provide further evidence regarding the interviews in his witness statement for the trial.

13. Dr Wright is not in possession of the private key, as stated in paragraph 83(3) of the defence. In early May 2016, Dr Wright destroyed the hard drive which contained the private keys which he had used in the private demonstrations – including the private key to block 9 of the Bitcoin Blockchain.

Under paragraphs 49 and 50

Of: *49. "The email reproduced under paragraph 28 of the Particulars of Claim is not an identical copy of an email Dr Wright sent to Mr David Kleiman on 12 March 2008."*

And: *50. "While the body of the email is the same as that of the email which Dr Wright sent on 12 March 2008, the header is different."*

Request

14. Please specify what the difference in the header is said to be.

Response

14. The email address which Dr Wright used to send the email was *wright_c@ridges-estate.com*, not *craig.wright@information-defense.com*.

Under paragraph 83(3)

Of: *"It is admitted that at one time Dr Wright had access to the private keys associated with the earliest blocks in the Bitcoin Blockchain. He no longer has such access."*

Request

15. Please explain why Wright no longer has access to the private keys associated with the earliest blocks in the Bitcoin Blockchain.

Response

15. See the response to Request 13.

MICHAEL HICKS

Statement of Truth

I believe that the facts stated in this Response to the Claimant's Part 18 Request dated 4 August 2021 are true. I understand that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without honest belief in its truth.

Signed: .....

Full Name: Dr Craig Steven Wright

Date: 10 September 2021

Served this 10th day of September 2021 by ONTIER LLP, Halton House, 20-23 Holborn, London EC1N 2JD (Ref: PF/SC/WRI2.31), solicitors for the Defendant.