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

Claim No: IL-2021-000019

B E T W E E N :

CRYPTO OPEN PATENT ALLIANCE

(for itself and as Representative Claimant on behalf of Square, Inc., Payward Ventures, Inc. (DBA Kraken), Microstrategy, Inc., and Coinbase, Inc.)

Claimant

-and-

DR CRAIG STEVEN WRIGHT

Defendant

SECOND WITNESS STATEMENT OF

DR ADAM BACK

I, DR ADAM BACK, of [redacted] will say as follows:

1. I am the same Adam Back that made an earlier witness statement in these proceedings. This statement has been prepared by Bird & Bird using my own words and sets out facts and matters that are within my own knowledge unless otherwise stated: Where I refer to facts within my own knowledge, I believe them to be true. Where I refer to information from other sources, I have identified my sources and the information it is true to the best of my knowledge and belief. On points that I understand to be important in the case, I have stated honestly (a) how well I recall matters and (b) whether my memory has been refreshed by considering documents, and if so how and when.

{E/1}

2. Bird & Bird has provided me with the First Witness Statement of Dr Craig Wright, which mentions me. I have been asked whether I have any factual comments in response to that witness statement.

My correspondence with Satoshi Nakamoto

{E/1/18} {D/74} {D/76} {D/78}{D/80} {D/82}

3. At paragraph 92 Dr Wright claims his thinking was profoundly influenced by Wei Dai, however it seemed to me (from Satoshi's email's to me which are exhibited to

my first statement), that he was not previously aware of Wei Dai's B-money proposal which would make it hard to be significantly influenced by it. I am aware that Wei Dai has said subsequently of the sequence of events that Satoshi had not even heard of B-money before so he (Wei) couldn't have influenced Bitcoin. Wei's email exchanges with Satoshi were shared and published on Gwern' blog at *blog.gwern.net*. I am also aware that Satoshi later wrote on bitcointalk that he implemented bitcoin before writing the paper, so learning about Wei's B-money after writing the paper would not affect the design.

{E/1/19}

4. At 93 Dr Wright wrote about me that "His attitude was quite dismissive; he stated that digital cash had been attempted before and was bound to fail." I did not say that in the emails exchanged with Satoshi. I did not say that at any time since that I recall.

5. The claim that I would be dismissive of attempts to create digital cash is even more opposite - I was one of the applied researchers who continued to work on making p2p electronic cash a reality, after the failure of digicash in 1998. Hashcash was a building block used by others in their designs, including Wei Dai in 1998, Nick Szabo in 1998, and Hal Finney in 2004.

{E/1/19}

6. At 94 Dr Wright cites a 2000 paper by Aura et al, and claims that Bitcoin uses this algorithm and not Hashcash. I don't think that is correct:

    a. Hashcash is cited in the Bitcoin White Paper.

    b. The original, 1997, version of Hashcash (version 0) used a double hash. I modified it in 2002 with version 1. That used a single hash, based on an optimization suggestion made to me by Hal Finney, and also independently by Thomas Boschloo at around the same time March 2002 (which I cite in the 2002 Hashcash paper).

    c. Hashcash version 0 (1997) predates Auro's 2000 paper, and Hashcash version 1 is a minor optimization of version 0.

    d. Hashcash and the Aura et al paper are different. Aura's work is about an interactive client-server protocol, while Hashcash is a non-interactive proof. Bitcoin, being peer-to-peer, necessarily cannot involve a server.

    e. The Aura paper describes their work as an optimization of Juels & Brainard's 1999 client-puzzles paper, which is also similar to Hashcash in some ways, but is different in that it is an interactive client-server protocol. Hashcash

version 0 (1997) also predates the Juels & Brainard 1999 client-puzzles paper.

7. I first became aware of the Aura paper some years ago, long after bitcoin was published, I think as a result of Dr Wright's or other employees of nChain talking about it online. I was not aware of it previously.

DECLARATION OF ADAM BACK

I understand that the purpose of this witness statement is to set out matters of fact of which I have personal knowledge. I understand that it is not my function to argue the case, either generally or on particular points, or to take the court through the documents in the case. This witness statement sets out only my personal knowledge and recollection, in my own words.

On points that I understand to be important in the case, I have stated honestly (a) how well I recall matters and (b) whether my memory has been refreshed by considering documents, if so how and when.

I have not been asked or encouraged by anyone to include in this statement anything that is not my own account, to the best of my ability and recollection, of events I witnessed or matters of which I have personal knowledge. I believe the facts stated in this statement 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 an honest belief in its truth.

Signed by ADAM BACK: ..... DocuSigned by: Dr Adam Back C02B0BCCAF224B6... **.....**

Date: ..... 7/11/2023 **.....**