On behalf of the Claimant
Witness: N Bohm
Exhibits: NB1
July 2023

IN THE HIGH COURT OF JUSTICE **Claim No: IL-2021-000019**

BUSINESS AND PROPERTY COURTS OF ENGLAND & WALES

INTELLECTUAL PROPERTY LIST (ChD)

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

WITNESS STATEMENT OF
NICHOLAS BOHM

I, **Nicholas David Frederick Bohm**, of [redacted] will say as follows:

1. I am a retired solicitor who corresponded with the pseudonymous "Satoshi Nakamoto" regarding Bitcoin, shortly after its release in January 2009. This written statement has been prepared by Bird & Bird to record my own evidence and answers given to Bird & Bird during a face-to-face interview. The evidence given in this statement is written in my own words as far as practicable. The facts and matters set out in this statement 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, those facts and matters are true to the best of my knowledge and belief and I have identified my sources.

2. Bird & Bird has pointed out the declaration at the bottom of this statement to me and asked me in particular to bear in mind that 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. I am however only generally familiar with the issues in the case which I have been informed by Bird & Bird concerns whether or not Dr Craig Wright is or was Satoshi Nakamoto.

3. I was contacted by Bird & Bird who asked me whether I would be willing to provide this evidence, and I agreed to. I understand that they had got my name from the cryptography mailing list, which I discuss below. Before I was contacted, I did not know about the existence of this dispute. I do not know anything about Dr Wright himself except that he claims to be Satoshi. From what has passed in front of me (which isn't much as I haven't followed the issue particularly closely) he doesn't seem to have explained his claim, but beyond minor scepticism I do not have any opinion about him at all. I do not know whether Satoshi and Dr Wright are the same person and for all I know he could be. I am not really in a position to say anything more than that: the best I could say is that when you correspond with someone in a particular way you develop a mental picture of them, as I did with Satoshi, but that was only a mental picture and it is often the case that when you meet them they can be starkly different.

My own background

4. I have always been interested in mathematics and science; my father was an engineer, as were his two brothers, and my mother's brother was a nuclear physicist. However, I wasn't good enough at maths to do "serious" science, and so read law at university.

5. I was admitted to the Roll in 1968, joined Norton Rose in 1972, and was made partner there in 1975. As a commercial solicitor, I was involved in company and commercial law. I have always been interested in technology and as a result of my practical interest in computers, I was particularly involved in software procurement contracts, the commercial underpinning of computers, and technology more generally. I was even involved in the early application of computers within Norton Rose itself. I

retired from Norton Rose in 1994. I maintain voluntary roles as an advisor to the Foundation for Information Policy Research and the Open Rights Group.

6. My interest in cryptography began while I was at Norton Rose, somewhere between 1976 and 1978 when I remember reading Martin Gardner's column in the Scientific American about a new form of cryptography called "RSA". I thought that the technology was fascinating, and thought that I was going to be hearing more about this technology in the future. However, it was only some time later, in the early 1990s, that it came to the forefront of my mind again, when I was asked by the Law Society to explain digital signatures to them, as there was an impending EU directive about that. I had previously been involved with the Law Society on data privacy issues, and as a member of a joint working group between the Law Society and Bar Council on other issues of intellectual property, and implications for lawyers, of various topics. So I have always been quite involved with the application of technology.

7. One of the things that went on in those early years was factoring competitions as a distributed effort. People would lend computer cycles (i.e. processing power from different computers located in different places) to distributed efforts to factor very large numbers. (This was a way of testing the security of algorithms which were dependent on the difficulty of factoring large numbers.) I had experience of joining collaboratively with a friend's team although we didn't win. I mention this as it is relevant to my initial interest in the Bitcoin White Paper as I will explain later.

8. It was part of my general interest in cryptography that led me to join first a cryptography mailing list in the UK, and through that, find out about and sign up to an American cryptography mailing list. I was sufficiently interested in this area to be reading the (American) cryptography mailing list attentively when Satoshi Nakamoto dropped his White Paper on it.

Downloading the White Paper and Bitcoin Code

9. I do not recall precisely when I downloaded and read the White Paper (although I have since checked as I explain later in this statement). When I saw the white paper this seemed similar to the distributed number factoring I mentioned above, at least in the sense of setting up a collaborative experiment. It seemed to me that Satoshi was describing a model of a financial system which could exist, and he wanted people to join in experimenting and seeing whether it would work. So I thought "why not"?

10. So I downloaded the Bitcoin software, and let it run and it chugged away. I got it from one of the repositories, I can't remember which repository it was but I think it was either Sourceforge or Github. I watched the system doing its thing, though I perhaps didn't understand what it signified very well. I also discovered that there was a forum (the Bitcoin Mailing List, on SourceForge) and so I signed up to that.

11. At length I ran into the odd problem which I reported on the forum or mailing list, and Satoshi took that dialogue offline (in the sense of making it a private exchange of emails not shared on the forum). It wasn't my particular purpose to hold a private correspondence with him, but it seemed to work for his purpose.

12. I have never before made my private correspondence with Satoshi public or I believe shown it to anyone else.

{D/91}-{D/173}

13. **Exhibit NB1** is a zip archive of electronic documents that I created myself. I created it on my personal computer which is the same personal computer that I refer to below. It contains:

    a. copies of all my correspondence with Satoshi Nakamoto. These were created by exporting them directly from Mozilla Thunderbird using its "import/export" plugin. The process exports emails as a series of files in different formats, so I have included all of the formats "**.eml**", "**.html**", "**.pdf**" and "**.txt**" so that anyone reading can consider what's most useful; and

    b. It also includes my PDF copy of the paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" with the filename "bitcoin.pdf", which I first downloaded in January 2009, and which I discuss further below.

14. I believe, having checked carefully, that the archive at Exhibit NB1 is complete in the sense that it covers all of my correspondence with Satoshi Nakamoto. The set begins with a message from me to a mailing list, followed by Satoshi's reply to that message but to me direct, which is how our correspondence began. I did not include any earlier messages that Satoshi sent to the list generally, which were not specifically to me.

15. On 1 February 2009, (a date which I have remembered by checking Exhibit NB1), Satoshi sent me a transfer of 100 Bitcoin. This transfer was unprompted (in the sense that we had not discussed a transfer being made). This prompted a discussion which is within Exhibit NB1. I was not discussing this with any sense of the constraints that Satoshi might be working within; I was merely trying to explain things that didn't

make sense to me. There are also two other Bitcoin transactions referred to in that correspondence, which I remember did take place as described there. It did not occur to me that Bitcoin were of any value, or that they were likely to be.

16. The early versions of the Bitcoin wallet software were set up as nodes on the network, to mine Bitcoin, and so were part of a mining operation. But the difficulty of mining bitcoin increased with time and there came a point when the latest version of the wallet no longer supported mining. (Separate software would have been needed.) At that point I stopped mining, as I wasn't mining for any purpose other than to support the experiment I thought it represented. The wallet contained something in excess of 100,000 Bitcoin, so I thought "oh well" and that's when it came to an end so far as my participation in Bitcoin as a miner went.

17. After some time Satoshi disappeared – that is to say he ceased to correspond with me. It wasn't that he owed me any correspondence though, and I thought nothing of it at the time. I then realised after a while that he wasn't being heard of anywhere. Around then (maybe before or after, I can't remember) I discovered to my complete astonishment that Bitcoin had a value. I discovered that someone called Jeremy West had set up a platform that allowed you to buy Amazon gift vouchers with Bitcoin.

18. I can't quite remember where in the course of all this I became aware that Satoshi had vanished and that it had been a pseudonym. It's not obvious to me why someone doing that would have wished to be pseudonymous. It's a curious thing but I don't have any more information about it. Of course I've seen various people speculate 'I think it was so-and-so', such as Hal Finney, who I believe died at around the relevant time. But I do not know and the closest thing I have is only my mental image which, as I mentioned earlier, is not a good basis for any conclusion.

The Bitcoin White Paper

19. During one of my meetings with Bird & Bird, I searched my hard drive to check whether I had any old versions of the Bitcoin White Paper. Having checked the files, I was able to locate a version (which I have then included within my zip file **Exhibit NB1**) which according to the metadata on my system was downloaded on 18 January 2009 at 13:27 GMT. The metadata also states that the file has a creation date of 11 November 2008, at 08:00:34 in the time zone UTC-08:00.

My Computer Set Up History and file archives

20. I used a PC when I corresponded with Satoshi. I have never used anything other than a PC running Windows for computing. I do have an iPhone, but have never used it or its predecessor mobile phones to house documents and have only rarely and temporarily used them for email. I do think that by this time I was already using Mozilla Thunderbird as my email client on the old machine but cannot be sure from memory.

21. The PC that I had in 2008 I kept until 2011. At one point in my correspondence with Satoshi I mentioned some of the specs of that computer and having checked, I believe that is accurate. In 2011 I had a new computer built and I transferred all the data from the 2008 computer to the 2011 one when I switched. I did this myself without assistance from others.

22. During the switch in 2011 I transferred all my emails from the old machine. I don't think that I have any emails from before about 2000, as I remember that the older email clients were less easy to move around between computers at that time.

23. I would not have kept many attachments so those would not have been moved over:

    a. My general approach has been to delete all attachments from emails at the time I read them, unless I specifically want to retain them (for example if they are family photographs), or if the file is extremely small.

    b. The reason for this is that the way Mozilla Thunderbird works is to store all emails in a folder database (or perhaps it is as a large database file), and attachments are also added to the database, which gradually makes it bigger and bigger.

    c. So generally I remove attachments: if I want to keep them I save them separately, for example family photographs I want stored as separate files as photographs in my filing system, not as attachments to emails, and it would be a nuisance to have them twice because it would be doubling the bulk.

    d. I am fairly – though not obsessively – organised with filing on the computer, with deciding where I want to put things and where they should be stored. I have checked and confirmed that there are no attachments to emails still on my computer other than those I have provided.

24. The only problem I encountered with the 2011 switch was that it lost me access to my Bitcoin wallet. Although I thought I knew which files to move and how to do it to keep access to the wallet, when I came to do it, I found it didn't work. The wallet was empty by then (I had variously spent / transferred the bitcoins in it) so it was not important to me.

25. The old (2008) machine I wiped and gave to a charity that purported to repurpose old machines.

26. I next replaced the 2011 PC in 2017 with a refurbished Dell from a company called Genmar that is local to me. They will have arranged the transfer of data onto it when I bought the refurbished machine. That would have included all my emails and filing system (and having checked I believe this to be the case). That Dell is my present machine.

27. Having thought carefully, I cannot think of anything that has happened to any of my machines which could have affected the data (including metadata) on them in any way relevant. I can't think of any instances of data being wiped, or data corruption (such as files going missing which ought to have been there, or files refusing to open because they had been corrupted). My files have been pretty stable for quite a long time. I have always run anti-virus and anti-malware software which occasionally deletes or quarantines emails, but I can't think of any reason that would have affected the emails in question.

28. Nobody else but me has ever managed my filing system. I've had very few external services. I had some serious trouble with one machine, which I think was the machine I got in 2011 (it was not the present one), and got someone in from the "PC Doctor" franchise who sorted it out for me, but they had quite brief contact with the machine and all of it under my direct observation. Bird & Bird has asked me if this could have affected my documents but I do not think it could have. Genmar moved my files onto my present machine. I did also have to give my present machine to Genmar for some servicing, which I think was for an unrelated software problem, and should not have made any difference to any of the relevant data at all. The machine has very rarely been touched by anyone else but me.

29. I routinely keep backups of my files on a separate encrypted drive. I usually keep up to a month or so's worth of backups. However the documents I supplied to Bird & Bird were taken from my machine directly, not from any restored backup, so I think this is not relevant.

Completeness of the Exhibit

30. I have cross-checked my correspondence with Satoshi (I checked in the form of PDF) and confirmed it is complete to the best of my knowledge, and I also checked when Bird & Bird visited and confirmed that the date range of emails in that printout matches my local system too. I also run on my machine some software called dtSearch which indexes my files for easy searching, and I have used this to check that the archive is as complete as possible, by doing searches for keywords including "Satoshi" and "Bitcoin" as well as seeing if this would find any of the missing attachments (which it did not).

I have not referred to or been referred to any documents for the purposes of giving my evidence other than the documents exhibited here.

Declaration of Nicholas Bohm

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 Nicholas Bohm: DocuSigned by: Nicholas David Frederick Bohm 1AA4C48AF79B40B...

Date: 21/7/2023