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

Claimant

-and-

DR CRAIG STEVEN WRIGHT

Defendant

WITNESS STATEMENT OF
DANIEL J BERNSTEIN

I, **Prof. Daniel J. Bernstein**, of [redacted] will say as follows:

1. I am a cryptographer and professor in the Department of Computer Science at the University of Illinois at Chicago. I prepared this written statement. I received input from Bird & Bird on the requisite format and on requisite declarations in this paragraph and at the bottom, but used my own words for paragraphs 2 through 16. I understand from Bird & Bird that my exchanges with them are subject to privilege, and nothing I say in this statement is intended to waive any such privilege. 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. 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.

2. I am one of the members of the five-person team that jointly developed the digital signature scheme known as EdDSA. The name “EdDSA” stands for “Edwards-curve Digital Signature Algorithm”. EdDSA is different from the pre-existing ECDSA (Elliptic Curve Digital Signature Algorithm). There are similarities but there are also clear differences. EdDSA is not used in Bitcoin as far as I know.

3. Bird & Bird asked me when the term “EdDSA” was coined. Based on my recollection of events and my consultation of the documents listed below, I can narrow down the date to between February and April of 2011.

4. Ed25519, the first example of EdDSA, was the direct successor of a signature scheme called edwards25519sha512batch.

5. The development of edwards25519sha512batch took place as one part of the development of cryptographic software called NaCl. I am one of the members of the three-person NaCl team.

6. NaCl was developed as part of a project called CACE. I recall the CACE project running for three years, specifically from 2008 through 2010. To confirm my recollection of the dates, I have now checked the NaCl web page, {C00002556} https://nacl.cr.yp.to/index.html [a copy of which is at **Exhibit DJB1**].

7. I recall that a report regarding NaCl was due at the end of 2010 as part of the CACE project, but was delayed because the development of edwards25519sha512batch was not completely finished by the end of 2010. To confirm my recollection, I have now checked the PDF of this report at https://cryptojedi.org/papers/caced25-20110211.pdf {C00002553} [a copy of which is at **Exhibit DJB2**], which is dated February 2011.

8. I recall the NaCl team consistently using the name "edwards25519sha512batch" for that signature system. To confirm my recollection, I have now checked the terminology in the aforementioned report regarding NaCl, and in https://web.archive.org/web/20110623140004/http://nacl.cace-project.eu/sign.html. {C00002552} That archived page is dated 23 June 2011 [reproduced at **Exhibit DJB3**]. The text at the bottom of that archived page notes that it was version 2011.04.17 of that page (i.e., last edited 17 April 2011).

9. The EdDSA team developed Ed25519 as a successor to edwards25519sha512batch, and EdDSA as a generalization of Ed25519. The team prepared a paper describing Ed25519 and EdDSA, and submitted the paper confidentially to the CHES 2011 conference.

10. Later in 2011, the EdDSA team put a revised version of the paper online, the first public version of the paper. The team then announced Ed25519 and EdDSA in various venues, including a presentation at CHES 2011.

11. To reconstruct the exact date of the EdDSA team putting that paper online, I have now checked my list of papers at https://cr.yp.to/papers.html [a copy of which is at {C00002555} **Exhibit DJB4**], which indicates that the first public version of this paper was dated 5 July 2011. I have also now checked that version of the paper, the PDF at {C00002554} https://ed25519.cr.yp.to/ed25519-20110705.pdf [a copy of which is at **Exhibit DJB5**].

12. To reconstruct the exact CHES 2011 submission deadline, I have now checked https://www.iacr.org/workshops/ches/ches2011/start.html [a copy of which is at {C00002551} **Exhibit DJB6**], which lists 4 April 2011 as a submission deadline.

13. I am not aware of any publication of EdDSA, or any public usage of the name "EdDSA" in any context, before the public 5 July 2011 version of the paper. As far as I know, the only usage of the term "EdDSA" before the confidential submission to CHES 2011 was in private discussions within the EdDSA team.

14. Ed25519 and EdDSA have clear differences from edwards25519sha512batch. The edwards25519sha512batch software inside NaCl was not Ed25519 software or EdDSA software.

15. I recall that, after EdDSA was announced, the NaCl team announced plans to upgrade NaCl from edwards25519sha512batch to Ed25519. To confirm my recollection, I have now checked https://web.archive.org/web/20120302092534/http://nacl.cace-project.eu/sign.html. That archived page is dated 2 March 2012 [reproduced at **Exhibit DJB7**]. The text at the bottom of that archived page notes that it is version 2011.12.07 of that web page (i.e., last edited 7 December 2011).

{C00002550}

16. I therefore believe that the term "EdDSA" was coined between February 2011 and April 2011, and first used in public on 5 July 2011.

List of documents: I have not referred to any documents other than those mentioned above.

Declaration

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: D. J. Bernstein .....

Date: 6 July 2023 .....