<u>IN THE HIGH COURT OF JUSTICE</u>	**Claim No: IL-2021-000019**

<u>BUSINESS AND PROPERTY COURTS OF ENGLAND & WALES</u>

<u>INTELLECTUAL PROPERTY LIST (ChD)</u>

BETWEEN:

CRYPTO OPEN PATENT ALLIANCE	**<u>Claimant</u>**
-and-	
DR CRAIG STEVEN WRIGHT	**<u>Defendant</u>**

SECOND EXPERT REPORT OF
PROFESSOR SARAH MEIKLEJOHN

Context, Background, and Instructions

{G/2/1} 1. This is my second expert report in these proceedings. I have been instructed by Bird & Bird to prepare this report in response to statements made by Dr Wright during his oral evidence in these proceedings relating to the signing sessions. In doing so, I have also considered statements on similar topics that Dr Wright made in his ninth witness statements in these proceedings. I address these new points below so that the Court can be aware of my views on them before I give evidence.

{8/1:1} {E/26/1} 2. In preparing this report, I have reviewed the transcript of Day 8 in these proceedings, as well as Dr Wright's ninth witness statement. However, where I do not address matters raised in Dr Wright's evidence, that does not mean I agree with it.

Background on certificates

3. When visiting a website, users (and their browsers) are presented with multiple pieces of information. In addition to the contents of the website, they are given a *certificate* containing (1) a public key of the *domain operator* (i.e., the entity with which users believe they are communicating by visiting that website) and (2) a digital signature on that public key by a trusted entity known as a *certificate authority* (CA for short).

4. This public key allows users to establish a secure channel with the domain operator (i.e., a channel in which all messages are encrypted and signed), meaning these certificates and the *public key infrastructure* (PKI) they provide form the basis of secure online communication. However, users can establish this secure channel with the domain operator only if they have the right public key for them. This promise (that users have the right public key for the domain they are visiting) is the purpose of the signature provided by the CA.

5. To obtain a signature from a CA on their public key (i.e., the public key for which they know the corresponding private key), a domain operator thus needs to prove to the CA that they are indeed responsible for operating a given domain. This in turn ensures that when users visit that domain and use the public key provided in the certificate, they are securely communicating with that domain operator and not an attacker impersonating them.

6. There are three levels of validation a CA can provide; in order from easiest to most difficult (and thus cheapest to most costly to obtain), these are: domain validation (DV), organizational validation (OV), and extended validation (EV). Certificates of each type can be identified by

specific object identifiers (OIDs) in the policy extension field of the certificate. While OIDs can differ depending on the CA, the ones most commonly used are 2.23.140.1.2.1 for DV certificates, 2.23.140.1.2.2 for OV, and 2.23.140.1.1 for EV.[1]

{E/26/27} {8/61:1)-{8/61:25} 7. As has been suggested by Dr Wright (in paragraph 104(6) of his ninth witness statement and page 69 of the Day 8 transcript), until 2019 most browsers displayed an extended green bar when given an EV certificate, containing the legal identity of the domain operator, as compared to the smaller green padlock shown for DV and OV certificates. If the browser had not been given any certificate for this domain (meaning the connection was over HTTP rather than HTTPS), it would not display any padlock.[2] This last point runs contrary to Dr Wright's assertion that having no certificate would cause the browser to display "a big red thing saying 'not secure'" (line 20 on page 69 of the Day 8 transcript). {8/69:20}

{E/26/26} 8. Dr Wright also claims, however, that electrum.org uses EV certificates (in paragraph 104(2) in his ninth witness statement). This is incorrect.

9. To show this, I first note that the Certificate Transparency (CT) security standard makes it possible to obtain certificates issued for electrum.org (or any other domain) as far back as 2013, when the first CT logs were deployed. We can thus obtain a list of certificates for electrum.org from a third-party CT monitor called crt.sh at https://crt.sh/?q=electrum.org **(Exhibit SM-38)**.[3] {H/374}

10. If we look at the certificate valid between 14 December 2015 and 30 December 2016 (https://crt.sh/?id=11483563)[4], we can see that the 'X509v3 Certificate Policies' field contains a subfield 'Policy', whose value is listed as 2.23.140.1.2.1. As indicated above, this is the OID associated with a DV certificate, not an EV certificate.

11. If we look through the entire list, we see that 130 of 137 certificates contain this OID. The remaining seven, which were all valid on or after 27 June 2019, contain the OID 2.23.140.1.2.2, which is the OID associated with an OV certificate. In other words, none of the certificates in this list are EV certificates.

12. It is possible that there were EV certificates issued for electrum.org but not captured in CT logs. CT has been enforced in Chrome for all EV certificates since 2015, however, and for all

{H/370} {H/371} {H/372} {H/373}

[1] Copies of the records referred to in this paragraph are also included at **Exhibit SM-36.1 – Exhibit SM-36.3.**

[2] Examples of security indicators are in Figure 2 in a 2016 research paper by Felt et al., obtained at https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-porter-felt.pdf. (**Exhibit SM-37**)

[3] CT logs typically contain up to a billion entries, so for a single domain it is significantly cheaper to use a third-party monitor rather than obtaining the entries from the logs directly.

{H/375} [4] **Exhibit SM-39**

certificates since 2018. Such a certificate could thus have been used only in non-Chrome browsers, which seems unlikely given the high cost of an EV certificate and the popularity of Chrome. Furthermore, it would have been impossible in 2016 for an EV certificate that was not included in a CT log to be accepted by Chrome, which is what Dr Wright indicated he used in the signing session with Gavin Andresen (saying "I think we actually downloaded Chrome" at line 22 on page 75 of the Day 8 transcript). {8/75:22}

Visiting a spoofed website in an honest computational setting

13. I now consider how it would be possible, in an "honest" computational setting, for someone to believe they are visiting electrum.org but to in fact be visiting another website. By honest I mean that the computer and browser being used are assumed to be operating as intended. This is in response to Dr Wright's claim that "it is not feasible and there is no known way to spoof the electrum website and the download the software from some other system" (paragraph 104(2) of his ninth witness statement). {E/26/26} I stress that this list is not exhaustive and there are other options available in a "dishonest" setting (i.e., if the computer or browser are compromised).

    a. First, a user might visit a domain like electrurn.org, electrum.com, or wwwelectrum.org rather than www.electrum.org. This is a technique called *typosquatting* that is commonly used in phishing attacks. In a more sophisticated version, sometimes called a *homograph* attack, characters in one alphabet could be replaced with characters from another, so the URL could be еlectrum.org instead of electrum.org (which appear identical, but the latter uses all Latin characters and the former uses an 'e' from the Cyrillic alphabet). A basic typosquatting attack can be detected by a careful visual inspection of the URL displayed in the browser, but a homograph attack cannot be detected visually. Instead, defences against this type of attack have been implemented in all major browsers since at least 2017 (e.g., Chrome released a defence in version 51, which was released on 25 May 2016).

    b. In terms of certificates, the domain of the spoofed website is different from the original one. It would thus be easy for the operator of the spoofed domain to obtain a certificate for it, using a public key for which they know the private key, as they are the genuine domain operator (of the spoofed domain). This means the browser would show a green padlock as expected and the attacker would be able to securely communicate with the victim using a key under their control.

c. Second, the way that website content is obtained is by requesting it from the IP address to which the URL resolves, via a process known as *domain name resolution* (or the domain name system; DNS for short). This resolution process is carried out by DNS servers (which Dr Wright has experience operating; see paragraphs 23(1) and 24 in his ninth witness statement). A computer can be easily configured, in the process of setting up the Internet connection, to use a custom DNS server. This custom DNS server could be set up to resolve electrum.org to a custom IP address, meaning the URL displayed in the browser would be correct but the website contents would be different. This is an attack called *DNS hijacking*. After the Internet connection is configured in this way, there is no way for a user to detect they are visiting a different version of the website (unless the website has been visually altered in a noticeable way). {E/26/9}

d. Obtaining a certificate would be harder in this scenario: the attacker does not genuinely control electrum.org, so it would be difficult (but not impossible[5]) to get a CA to link that domain to a public key for which they control the private key. Thus, the attacker might choose to provide no certificate. As described in Paragraph 7, this means this attack could not be detected by a visual inspection of the URL but could be detected by checking for a green padlock.

Other aspects of the signing sessions

14. On Day 8, Dr Wright claimed that "by downloading and revalidating the blockchain, I've showed that the software is actually correct" (line 21 on page 57 of the transcript). By this, I understand Dr Wright to have been saying that it would not be possible to successfully download and verify the blockchain (i.e., check the validity of all blocks and transactions, and reconstruct the UTXO set) if the software had been modified in any way. This is incorrect. The software could have been altered to always output 'true' (or some other indication of successful signature verification) only when specific conditions were met: e.g., the signature verification function was given the key from the block 9 coin generation transaction, a message ending in 'CSW', and an arbitrary signature (i.e., one that does not necessarily pass honest signature verification). This would not affect the operation of the signature verification function when downloading and verifying the blockchain, because none of the inputs from the blockchain would satisfy these specific conditions (and thus trigger this {8/57:21}

[5] A 2022 research publication by Akiwate et al., available at https://zakird.com/papers/dnshijack.pdf, explains how an attacker could obtain a certificate and points to several examples of when this has happened (**Exhibit SM-40**). {H/376}

deviation from the normal behaviour). Thus, the software would proceed normally when processing the blockchain, but would have been modified in a way that would significantly impact the signing sessions (in which these conditions would be satisfied and thus the software, if modified as described, would produce a misleading output).

15. On Day 8, Dr Wright also claimed that adding the extra "CSW" letters to the message "makes it more likely that someone hasn't planned anything" (line 4 on page 73 of the transcript). By this, I understand Dr Wright to have been saying that having him contribute to the message being signed increased the security of the process (as compared to having Mr Andresen pick the message entirely on his own). As described in Paragraph 103a of my report, this is incorrect. {8/73:4} {G/2/43}

Declaration

1. I understand that my duty is to help the Court to achieve the overriding objective by giving independent assistance by way of objective, unbiased opinion on matters within my expertise, both in preparing reports and giving oral evidence. I understand that this duty overrides any obligation to the party by whom I am engaged or the person who has paid or is liable to pay me. I confirm that I have complied with and will continue to comply with that duty.

2. I confirm that I have not entered into any arrangement where the amount or payment of my fees is in any way dependent on the outcome of the case.

3. I know of no conflict of interest of any kind, other than any which I have disclosed in my report. I do not consider that any interest affects my suitability as an expert witness on any issues on which I have given evidence.

4. I will advise the party by whom I am instructed if, between the date of my report and the trial, there is any change in circumstances which affects this.

5. I have shown the sources of all information I have used.

6. I have exercised reasonable care and skill in order to be accurate and complete in preparing this report.

7. I have endeavoured to include in my report those matters, of which I have knowledge or of which I have been made aware, that might adversely affect the validity of my opinion. I have clearly stated any qualifications to my opinion.

8. I have not, without forming an independent view, included or excluded anything which has been suggested to me by others including my instructing lawyers.

9. I will notify those instructing me immediately and confirm in writing if for any reason my existing report requires any correction or qualification or my opinion changes.

10. I understand that:

    a. my report will form the evidence to be given under oath or affirmation;

    b. the court may at any stage direct a discussion to take place between experts and has done in this case;

    c. the court may direct that, following a discussion between the experts, a statement should be prepared showing those issues which are agreed and those issues which are not agreed;

    d. I may be required to attend Court to be cross-examined on my report; and

    e. I am likely to be the subject of public adverse criticism by the judge if the Court concludes that I have not taken reasonable care in trying to meet the standards set out above.

11. I have read Part 35 of the Civil Procedure Rules and I have complied with its requirements. I am aware of the requirements of Practice Direction 35 and the Guidance for the Instruction of Experts in Civil Claims 2014.

12. I confirm that I have acted in accordance with the Code of Practice for Experts.

13. I confirm that I have made clear which facts and matters referred to in this report are within my own knowledge and which are not. Those that are within my own knowledge I confirm to be true. The opinions I have expressed represent my true and complete professional opinions on the matters to which they refer.

Signed: Sarah Meiklejohn Dated: 19 February 2024