Defendants
Pieter Wuille
Second
26 January 2024

IN THE HIGH COURT OF JUSTICE **CLAIM NO. IL-2022-000069**
BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES
INTELLECTUAL PROPERTY LIST (CHD)

BETWEEN

DR CRAIG STEVEN WRIGHT & Ors

Claimants

—and—

BTC CORE & Ors

Defendants

SECOND WITNESS STATEMENT OF PIETER WUILLE

I, **PIETER WUILLE**, of c/o Macfarlanes LLP, 20 Cursitor Street, London EC4A 1LT, WILL SAY as follows:

1 I am the Fourth Defendant in these proceedings and made a first witness statement dated 13 October 2023.

2 I make this witness statement to respond to two points made by Dr Wright in his eleventh witness statement ("**Wright 11**"), which I have read.

3 This witness statement has been prepared following a videoconference call with my solicitors, Macfarlanes LLP (over which privilege is not waived). After the call, Macfarlanes prepared a written draft of this statement, which I reviewed and amended before signing the Statement of Truth below.

4 Unless otherwise stated, the facts and matters set out in this witness statement are within my own personal knowledge and recollection and I believe them to be true. Where the facts and matters are not within my knowledge, I have given the source of my belief and I believe them to be true.

5 In order to make this statement, I have refreshed my memory by:

5.1 reviewing certain disclosed documents pointed out to me by Macfarlanes; and

5.2 reviewing other public documents, in particular the log of changes ("commits" or "revisions") made to the Bitcoin software code, which records when and by whom certain changes were made to the code.

6 I have included these documents in the list appended to the end of this statement. I have indicated below what I remember independently, and what I know from reviewing documents.

Byte limit

7 At paragraph 545(f) of Wright 11, Dr Wright says that "*BTC has limited the ability to use script"* by limiting the size of the objects on which scripts operate on (which Dr Wright calls "data packets" but are usually called "stack elements") to 520 bytes. He includes a footnote as the source of this statement, with a link to Bitcoin Core 0.10.0rc3 code. This rule still exists in Bitcoin today.

8 When I read the statement, my memory was that it was Satoshi who introduced the 520-byte limit on stack elements in the Bitcoin source code, and that this had happened before I had involvement with Bitcoin.

9 I confirmed my memory by reviewing the commit history on GitHub and the subversion (sometimes referred to as SVN) history on SourceForge (which was where the development took place prior to the move to GitHub). That shows that:

9.1 The original version of the Bitcoin source code, version 0.1.0, did not apply any limit.[1]

9.2 A 5,000-byte limit was then added. This was added in version 0.3.6 on July 29, 2010. The SVN history shows that the change was authored by "*s_nakamoto*"[2].

9.3 The byte limit was then tightened to 520 bytes. This was done in v0.3.9 on August 15, 2010. Again the SVN history shows that the change was authored by "*s_nakamoto*"[3].

[1] See the EvalScript function in https://github.com/trottier/original-bitcoin/blob/master/src/script.cpp#L44. There is no SVN revision number for this code, as it was only adopted in August 2009, after version 0.1.5 was released.
[2] See SVN revision 119. I found a page on Archive.org, which shows that this revision was visible in 2014 on SourceForge: https://web.archive.org/web/20141122053424/http://sourceforge.net/p/bitcoin/code/119/.
[3] See SVN revision 131. As with SVN revision 119, I found an Archive.org page which shows this revision was visible in 2014 on SourceForge: https://web.archive.org/web/20141122052926/http://sourceforge.net/p/bitcoin/code/131/

10 These changes were made during the period that Satoshi was actively involved in developing the Bitcoin source code. I have also confirmed my memory by reviewing emails dated July 29, 2010 and September 4, 2010, sent by Satoshi to Gavin Andresen which include this code.[4]

11 The code referenced at footnote 287 of Wright's eleventh witness statement shows a purely cosmetic change to how the code deals with the 520-byte limit. It introduced a named constant ("MAX_SCRIPT_ELEMENT_SIZE") for the 520-byte value; it did not introduce the limit.[5]

Opcodes

12 Wright 11 also makes several claims about disabling of Bitcoin script opcodes (including OP_2MUL), disabling of script entirely, and disabling of versioning. It is unclear exactly what "versioning" Dr Wright is referring to, but I believe it may be the OP_VER opcode.

13 The normal spelling of OP_CODE is "opcode" (lowercase, no underscore). That is a standard term in computer systems design.[6] Satoshi used the spelling "opcode" in code.[7] Craig Wright's eleventh witness statement refers to "OP_codes" or "OP_Codes".

14 My recollection when I read Wright 11 was that several opcodes have indeed been disabled (including OP_VER, OP_MUL, OP_DIV, and OP_2MUL), but only by Satoshi. Script has never been disabled in its entirety.

15 After reviewing the commit history on GitHub and the SVN history on SourceForge, emails disclosed in this case, and re-reading my first witness statement, I found that my recollection was correct.

15.1 The original 0.1.0 release of bitcoin included all the opcodes mentioned above.

15.2 OP_VER and related opcodes were disabled by Satoshi in v0.3.6 (SVN revision 119, the same revision that introduced the 5000-byte limit referred to above[8]). I believe that these opcodes were disabled because they were not consensus-safe. OP_VER basically checks the version number of the software used to verify the

[4] See GAVIN_00001636 (email)(MACPROD_0000774) and GAVIN_00001637 (attachment) (MACPROD_0000774), and GAVIN_00001896 (email)(MACPROD_0000903) and GAVIN_00001897 (attachment)(MACPROD_0000904)
[5] For completeness, the code referenced is PR 2188, which was carried out by Matt Corallo on January 18th 2013. See https://github.com/bitcoin/bitcoin/pull/2188/commits/192cc910ec7cade1d0dce7f3b111e7fc7720e607
[6] See e.g. https://en.wikipedia.org/wiki/Opcode.
[7] See e.g. the Bitcoin source code in the script.h file (https://github.com/trottier/original-bitcoin/blob/92ee8d9a994391d148733da77e2bbc2f4acc43cd/src/script.h#L140) and many more examples in the script.cpp file at https://github.com/trottier/original-bitcoin/blob/92ee8d9a994391d148733da77e2bbc2f4acc43cd/src/script.cpp
[8] See the archive link provided at fn. 2. The patch at GAVIN_00001637 (MACPROD_0000775) also includes the code that does this disabling.

blockchain. Any time the version number changes, it's possible the chain would fork.

15.3 More opcodes were disabled by Satoshi in v0.3.9 (SVN revision 131, the same revision that introduced the 520-byte limit[9]). These were: OP_CAT, OP_SUBSTR, OP_LEFT, OP_RIGHT, OP_INVERT, OP_AND, OP_OR, OP_XOR, OP_2MUL, OP_2DIV, OP_MUL, OP_DIV, OP_MOD, OP_LSHIFT, OP_RSHIFT.

16 For many of these, it is unclear to me why they were disabled. My assumption is that this was because of denial of service concerns. In fact, I asked the '[Bitcoin-development]' mailing list that question in August 2011.[10]

17 Script was never disabled entirely, though in v0.3.18 (which was created by "*s_nakamoto*" as shown in SVN revision 198) the potentially related concept of standard script templates was added to the code. These are a 'relay' policy which has existed and exists in the Bitcoin reference client. It does not disable opcodes, but it would not relay or accept transactions that fall outside a restricted set of standard scripts. This change was made by Gavin Andresen, but having reviewed some of the documents disclosed in this case, I believe he was directed to do this by Satoshi.[11]

18 In the years after Satoshi left, no opcodes have been disabled as far as I am aware, and the set of standard script templates has expanded significantly (contrary to what Dr Wright says at paragraph 1402 of Wright 11, this includes those needed for escrows).

Confirmation of compliance

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.

[9] See the archive link provided at fn 3. The line that disabled these is also in surrounding code in GAVIN_00001897 (MACPROD_0000904) (search for 'OP_RSHIFT', it's the line of code below).
[10] See https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2011-August/000398.html
[11] See GAVIN_00001560 (MACPROD_0000752): " *I've come to agree with you about only accepting transactions that match the standard templates… The patch is attached. Test it a little and if it looks fine, go ahead and commit it.*" And GAVIN_00001561 (MACPROD_0000753).

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.

Statement of Truth

I believe that the facts stated in this witness 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: DocuSigned by: Pieter Wuille F17A5EE97D82485...

PIETER WUILLE

Dated: 26 January 2024

Certificate of compliance

I hereby certify that:

1. I am the relevant legal representative within the meaning of Practice Direction 57AC.

2. I am satisfied that the purpose and proper content of trial witness statements, and proper practice in relation to their preparation, including the witness confirmation required by paragraph 4.1 of Practice Direction 57AC, have been discussed with and explained to Pieter Wuille.

3. I believe this trial witness statement complies with Practice Direction 57AC and paragraphs 18.1 and 18.2 of Practice Direction 32, and that it has been prepared in accordance with the Statement of Best Practice contained in the Appendix to Practice Direction 57AC.

DocuSigned by: Christopher Charlton 20B7F0A905F6416...

Name: Christopher Charlton

Position: Partner, Macfarlanes LLP

Date: 26 January 2024

APPENDIX

List of documents the witness has referred to or been referred to for the purposes of providing this statement.

Document IDs:

GAVIN_00001636 (MACPROD_0000774)

GAVIN_00001637 (MACPROD_0000775)

GAVIN_00001896 (MACPROD_0000903)

GAVIN_00001897 (MACPROD_0000904)

GAVIN_00001560 (MACPROD_0000752)

GAVIN_00001561 (MACPROD_0000753)

Pull Requests / SVN Revisions:

SVN revision 119
(https://web.archive.org/web/20141122053424/http://sourceforge.net/p/bitcoin/code/119/)

SVN revision 131
(https://web.archive.org/web/20141122052926/http://sourceforge.net/p/bitcoin/code/131/)

PR 2188
(https://github.com/bitcoin/bitcoin/pull/2188/commits/192cc910ec7cade1d0dce7f3b111e7fc7720e607)

Witness Statements:

First witness statement of Pieter Wuille

Eleventh witness statement of Craig Steven Wright

Other:

Email from Pieter Wuille to [Bitcoin-development] distribution list (24 August 2011):
https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2011-August/000398.html

Wikipedia entry for ‘opcode’: https://en.wikipedia.org/wiki/Opcode

Bitcoin source code, script.cpp file: https://github.com/trottier/original-bitcoin/blob/92ee8d9a994391d148733da77e2bbc2f4acc43cd/src/script.cpp

Bitcoin source code, script.h file: https://github.com/trottier/original-bitcoin/blob/92ee8d9a994391d148733da77e2bbc2f4acc43cd/src/script.h#L140