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**

SECOND EXPERT REPORT
OF ARTHUR ROSENDAHL

---

1 Introduction and overview

1.1 Scope of this report

1. I am the same Arthur Rosendahl who has made one previous expert report in these proceedings. I have approached this Report bearing in mind the same duties and in the same way as my first report. As before, this Report has been prepared by me in my own words, with input from Bird & Bird.

2. I have been provided by Bird & Bird with two sets of metadata information and their associated files, which I understand to be metadata relating to the project editing history and creation of the LaTeX files that I analysed in my First Report (the **"Editing History"**).

3. Bird & Bird have instructed me to prepare a short report explaining the Editing History, and to provide my opinions about how it relates to the analysis in my First Report.

4. My objective is not to provide exhaustive detail, but to provide a general narrative to explain the effect of the Editing History.

5. Finally, I take the opportunity to list a few errata which I have discovered in my First Report, which I have set out in an Appendix.

1.2 Overview of Editing History

6. The Editing History has been supplied in two zip files, which appear to be data exports from Overleaf:

    a. a first tranche, relating to the history of an Overleaf LuaLaTeX project called the "BitCoin Project" from 19 November 2023 to 13 December 2023, including the LaTeX files that I analysed in my First Report, ultimately leading to the creation of a file named `main.tex`; and

    b. a second tranche, relating to the history of the same project over a 50-hour period prior, from 17 to 19 November 2023, where almost all edits are made to a single file, named `BitcoinSN.tex`.

7. Each zip file contains further zip files in turn, with a large amount of data including a project history, compilation logs, version history, and a Readme file. The Readme file provides some information about the other data in the Overleaf exports, and a copy is at **Exhibit AR38**. However, out of all this data the main source of information for this Report has been the project history section of the exports, which is described in the Readme files as follows:

    "The project history of new projects and those imported from Overleaf can be

found in the `projectHistory/chunks.json` file. The history is made of two parts: a snapshot that contains all files, as they appeared at the beginning of history, and a list of changes.

Each change contains file operations (add/delete/move) and text operations. [...] Text operations are in a format described in the `ot.js` library[1]*. In a nutshell, each text operation is a list of sub-operations. These sub-operations operate on an imaginary cursor that starts at the beginning of the document. Each element in the list is either:*

- *a positive number N, meaning keep the following N characters*
- *a negative number N, meaning delete the following N characters (advance the cursor without keeping the characters)*
- *a string S, meaning insert S at the current cursor position*

Project history contains references to files in the form of hashes. The actual files referenced by these hashes can be found in the `projectHistory/blobs` directory."

8. Each edit to the file is listed as a **"chunk"**, with each chunk corresponding to a change made to a single file, which is in this case mainly adding or deleting text in the document. A chunk consists of an indication of what data was added or deleted, the file this was added to, the date and timestamp of the edit itself, and the identity of the author (among other information, such as the hash of the resulting file).

9. The chunks are very granular, in that edits to a single file are usually represented by several consecutive entries covering a period of a few minutes each. This can also be rather complex to follow because it's so detailed; fortunately the delivery contains a helpful snapshot of the oldest few as well as the newest few states of the project, showing the effect of each of these edits. However, not all of the snapshots have been provided, which would have been more helpful.

10. The chunks themselves are delivered by Overleaf in the `JSON` format, a common format for storing structured data in a human-readable way; but the disclosure contains instead a file called `chunks.xlsx`, a Microsoft Excel spreadsheet document which contains essentially the same data except for some deviations I detected, on which I will now expand. I would have preferred `JSON`, but I work with what I have.

11. The Chunks file for the first Overleaf export is at **Exhibit AR39**. The Chunks file for the second Overleaf export is at **Exhibit AR40**.

[1] `https://github.com/Operational-Transformation/ot.js/blob/298825f58fb51fefb352e7df5ddbc668f4d5646f/lib/text-operation.js`

1.2.1 Redactions and missing data in `TC`

12. There are three ways in which the data provided is incomplete. Ultimately this has not mattered for my ability to get through the data, but it has slowed down my analysis somewhat.

13. First, only a sample of snapshots seems to be provided: the few most recent snapshots and the few oldest states are included for the first tranche of data. No snapshots are included in the disclosure of the second tranche. Nonetheless, the snapshots are a big help in understanding how the chunks work as a record of the editing process; but having come to such an understanding, I will mostly refer to chunks in the below since they contain more information about the history of the Overleaf project.

14. Second, I understand from Bird & Bird that redactions have been made to the data for legal reasons. The Excel files are noted as being redacted and only contain editing information for files in the relevant folders, as do the `JSON` files. Some of the redactions are identified as having been made by or on behalf of Stroz Friedberg, but not all.

15. Third, I would like to share my impression that there have been amendments to the delivery from Overleaf that go beyond redacting some parts. The one clear sign of that is that the two-character string "`\n`", that codes for the line-break character in many programming languages, has been replaced by "`/n`", i.e. with a forward slash instead of a backslash. This happens not only at places where one can reasonably expect a line break character, but also in the name of some of the actual TEX commands, since those are almost always prefixed with the backslash character too. This meant that whenever the command name starts with the letter 'n', it seems to have been replaced by '`/n`' even though it is not a line break, as for example in "`/numexpr`" in chunk 756 (where I would have expected "`\numexpr`"). In addition, there have been unfortunate modifications to the file `project.json`, as well as to the appendices in the `projectHistory` folder, so that as a result they are no longer valid `JSON`; but that was easy to rectify. I have the impression that these are almost certainly honest mistakes — I just wanted to note the situation.

2 The first tranche: The `TC` folder and `main.tex`

16. I first explain the editing history of the first tranche of editing data `TC` folder. As mentioned, the timestamps of the chunks show that this was edited a bit later than the second tranche of editing history, but since I was provided with this first, I set out this analysis first.

2.1 Dates and number of edits

17. According to the Readme information, the main part of the zip file would have originally contained a full history of the contents of an Overleaf project running from 19 November 2023 to 13 December 2023 (although the information provided is partial). We can see several files being added to the project, then edited, and in some cases removed.

18. The Excel file `chunks.xlsx` contains information for each of these edits, amounting to 1505 edits in total. Of those, 379 relate to the file **L** `main.tex`, and the rest to other files or redactions.

2.2 Editing history and L `main.tex`

2.2.1 Creation and initial editing of L `main.tex`

19. Starting with the earliest available snapshot of the folder, I note that the folder structure of the project is very similar to the one from the zip file of my Stage 2 instructions referred to in my First Report. However there were are somewhat fewer files. Most notably, several of the fourteen candidate files are missing, namely (using my capital-letter labels along with the full name): **A** `BitCoin 2007.tex`, **C** `E-Cash-main.tex`, **D** `ECash-Main01.tex`, **L** `main.tex`, and **N** `main02.tex`.

20. The file `main.tex`, which was identified by Dr Wright's team as the source of the compiled White Paper they provided, is not initially present. However, that was created on 19 November 2023 at 18:24:13.564 UTC (at chunk number 138) and at that point was a blank file with no content.

21. A substantial amount of text was then added, presumably by uploading a file, or copying from another Overleaf project, a few seconds afterwards at 18:24:27.559 UTC (chunk 140), corresponding to the text, images, and formulae of the entire Bitcoin White Paper under the title "Bitcoin: A Peer-to-Peer Electronic Cash System", but without the bibliography. I later discovered the origin of this copied material to be an earlier version of **B** `BitcoinSN.tex` which had been edited in the days and minutes leading up to the creation of **L** `main.tex`, and which I will explain in more detail below in the next section, in to the second tranche of metadata.

22. Because of the coincidence in name I will refer to it as **L** below; but it did not yet match the file which would eventually be compiled into Dr Wright's compiled White Paper and would not do so until further edits had been completed over the next days.

2.2.2 Further edits from 19 November onwards

23. Almost immediately after the creation of **L**, we can see that some additional '`\;`' space commands are added, from 18:39:18.935 onwards. There are also a series of edits to the other content.

24. Chunks 298 to 370 record edits to **L** and are exclusively concerned with fine-tuning the LaTeX code of a very specific part of the document, namely the first formula, over the course of 72 edits on 20 November 2023 at 08:51:29.003 to 09:28:17.964. The changes are mostly to font commands (changing back and forth between different variants), but also include different ways to code the curly braces. I would point out that in the end, no amount of LaTeX coding in the candidate files could reproduce the main maths font of the original Bitcoin White Paper, namely Times New Roman.

2.2.3 Setting the metadata of L `main.tex`

25. In the following days, among other things, various commands were introduced into **L** `main.tex` to control the PDF metadata of the files:

    a. The initial metadata was set in the edit at chunk 140, which included the following commands (which were sourced from **B** `BitcoinSN.tex`, having been introduced there on 18 Nov 2023 at 18:01:29):[2]

    ```
    pdftitle={Bitcoin},
    pdfauthor={Craig Wright (Aka Satoshi)},
    pdfproducer={OpenOffice.org 2.4},
    pdfcreator={Writer}
    ```

    b. At chunk 746, on 22 November 2023 commands are first introduced which begin to expressly set the creation and modification date metadata of the resulting PDF (as opposed to just setting details such as the author and creator). This was on 22 November 2023 at 18:58:04.585, and the metadata was set as follows, to the same date one year forward (2024):

    ```
    pdfcreationdate={D:20241122010000}
    pdfmoddate={D:20241122010000}
    ```

    c. A series of further changes to control other parts of the metadata in various ways and using different methods then followed over the next 47 minutes to 19:44:25.537 (chunk 761), setting the metadata for the PDF producer, PDF major version, PDF minor version, and suppressing optional information.

    d. On 24 November 2023 at 17:05:18.465 (chunk 769), the text `90324173315` was added, a string which matches the creation date of the 2009 Bitcoin White Paper

[2] I have edited this chunk slightly to reflect what I consider to be its original contents in the data export from Overleaf, which has been altered slightly as I have explained at section 1.2.1. Here, each key-value pair ends in `'/n'` which must have been `'\n'` originally. Instead of simply substituting the latter for the former, I give it its natural interpretation, i.e., a line break. I do the same with similar examples later on.

of Tuesday 24 March 2009 at 17:33:15 UTC, the full string being accordingly `20090324173315`. I note however that the time is actually coded inside the PDF file as 11:33:15 UTC-6, which results in a full timestamp string of `D:20090324113315-06'00`. A PDF viewer will usually display times in the user's time zone, regardless of the time zone of the timestamp string.

e. A series of 41 further edits took place on 1 December 2023. These included setting PDF XMP metadata as `pdfxmpcreatedate={2008-10-03T13:49:58-07:00}` (a date and time corresponding to the creation date of the 2008 version of the Bitcoin White Paper - chunk 931, at 10:13:47 AM), and then 15 minutes later, setting the XMP metadata to `pdfxmpcreatedate={2009-03-24T11:33:15-06:00}` (chunk 944, 10:28:40 AM), as well as other modifications to how the metadata was coded. Although these dates match the creation dates and times of the different versions of the Bitcoin White Paper, the field in question in fact refers to something different, called "metadata stream" in the specification of the PDF format. The BWP stores its metadata in a structure called the "document information dictionary" (this is what I refer to as metadata elsewhere in my reports). These fields are not present in the original BWP documents. The commands then deleted these XMP fields a few minutes later (at 10.29.53 AM).

f. Three days later, on 4 December 2023, at chunks 1097 to 1106, different values of the author key are typed in the PDF metadata. First, the name '`Michael Hicks`' being set as the metadata author at 16:33:28, with that text being deleted three minutes later and replaced with '`Satoshi Nakamoto`'.

26. In this way, the commands used to specifically set metadata evolved from 22 November 2023 to 4 December 2023, with some changes being reverted (such as the author name key and XMP metadata shown above), with others being introduced in the final version (such as the `pdfcreationdate` and `pdfmoddate` keys).

2.2.4 Final edits in December 2023 to file L `main.tex`

27. 5 December 2023 then saw extensive activity in the domain of editing and setting of fonts, formulas, and metadata, with chunks 1107 to 1252 recording edits in mostly **L** `main.tex`, and a further 8 edits the following day. This included specifying specific fonts files to be used (such as `OpenSymbol.ttf`) and edits to formulae (such as replacing the literal Greek letter λ with the LaTeX command `\lambda`.

28. The file was then edited a further 7 times on 10-12 December 2023, with an alteration to an embedded diagram and deletion of a small amount of text.

2.3 Other edits and other files

29. I will not go through all the other 1505 chunks in detail as it would be extremely tedious and will instead focus on a few salient ones, as follows:

    a. chunk 681 sees the creation of **C** `E-Cash-main.tex` with a prose similar to the Bitcoin White Paper from March 2009. At that point it was given the same title as the March 2009 Bitcoin White Paper, but less than five minutes later, at chunk 694, we can see the title being altered to what I understand to be an earlier one ("*Electronic Cash Without a Trusted Third Party*");

    b. immediately afterwards, from chunks 697 to 744, we can see the text is edited backwards to match the text of the abstract. I note that the Excel file at this place reads almost exactly like my comparison table 3.5 from my First Report;

    c. at chunk 762, file **A** `BitCoin 2007.tex` is created on 22 November 2023 at 19:47:50.435. A large amount of file content is then pasted in shortly afterwards 10 seconds later, with further edits taking place over the next minute including the addition of the word `Nakamoto`;

    d. at that point a new file `BC2.tex` is created, quite a short file, which contains Lua code in an apparent attempt at combining two fonts together in one a maths formula. This is similar to formulae in the BWP (which use the main maths font Times New Roman, but the font OpenSymbol for a few characters within those formulae). I do not think this Lua code could ever work but did not investigate further for the purpose of this Report;

    e. similar edits are made to many other files in the project over the TC period up to 13 December 2023 at 13:10:15.858; and

    f. last but not least, at chunk 1405 (still on 5 December 2023), **L** `main.tex` is created anew, and contents added to it resulting in a file identical to the document that was provided to me in the course of my Stage 2 instructions in my First Report.

30. I note that this is consistent with the findings in the genealogy in my First Report.

2.3.1 Other candidate documents

31. Over the course of all these edits and additions, several other files are created, five of which attracted my attention because I realised they were further candidates for being the LaTeX source of the original Bitcoin White Paper, in addition to the fourteen from my First Report. Out of completeness, I have looked at these against the table of "problematic packages" to which I refer in my First Report — they align with my analysis and I am informed by Bird & Bird that it is not necessary to do a deeper

analysis of these. Nevertheless, I will also assign single capital letters to them (skipping O to avoid confusions) and give an quick summary:

P `Shoosmiths.tex` (1068 lines): contains all 7 problematic packages identified in section 3.7 of my First Report;

Q `mBitcoin.tex` (1136 lines): all 7 packages;

R `main03.tex` (1091 lines): all 7 packages;

S `main310.tex` (534 lines): only 2 out of the 7 packages: fontspec, and luacode; and

T `mainpdf.tex` (1121): all 7 problematic packages.

3 The second tranche

3.1 Introduction

32. Although this export from the "Maths (OLD)" project was provided to me later, it actually provides data about prior editing, as is clear from the timestamps. The data in this project was edited in the few days immediately prior to the re-creation[3] of `main.tex`, and the data was subsequently copied into `main.tex` leading to the series of further edits described above.

33. The most relevant file for analysis in this project is the file named `BitcoinSN.tex`. This is clear because the vast majority of edits recorded in `chunks.xlsx` are made to that one file (1369 out of a total 1602), and because the final state of the file `BitcoinSN.tex` precisely matches the initial state of `main.tex` from the later dataset, discussed above — the file which would eventually turn into Candidate **L**.

34. This can be confirmed by calculating the SHA-256 digest of the final state of **B** `BitcoinSN.tex` in the second (earlier) tranche, and the earliest non-empty state of **L** `main.tex` in the first (later) tranche. Both files are 1005 lines long and have the same SHA-256 checksum:

`77220d9db8c5e7b42df51cebf89b57d84fac43cfe00982352ac9358cb293f30a`

35. As I have explained above, **L** `main.tex` was created as a a blank file and within seconds populated with contents identical to **B** `BitcoinSN.tex`. It is therefore clear that the file **L** `main.tex` sourced its content from the earlier **B** `BitcoinSN.tex`. The chronology confirms that: only a few minutes elapsed between the last edit to **B** `BitcoinSN.tex` and the creation of **L** `main.tex`.

[3] In this earlier state, the project already had a file under the name of `main.tex`, but since that one was later overwritten I did not look into it further.

3.2 Redactions and missing data in the second tranche

36. I note the same slight difficulties with the redactions by Stroz Friedberg.

37. However, in this case I looked in vain for what could be the earliest state of **B** `BitcoinSN.tex` in `chunks.xlsx`, but could not find it. This makes me suspect that it may have been redacted away: I had expected one chunk that registered the creation of the file with content being added after that, but I couldn't find any. Instead, the first relevant chunk is chunk 275 with the deletion of 14 characters (indicating that some characters must have already present in some form, in order to be deleted). It would be more helpful if the early versions of the second tranche, including the file **B** `BitcoinSN.tex`, were provided in snapshots as was done with the first tranche.

38. In the absence of a direct reference to the original `BitcoinSN.tex`, I went looking in the `blobs` folder and identified something that must have been close: `999920a75ee445cfa0 19cef46d103adf9cb0da5b` (which can be determined based on file size, and the general match in content). I used that as a guide for interpreting the chunks, but primarily I looked at the chunks themselves, and I am not certain the file is the right one so have not analysed it as if it might be.

3.3 Summary of editing history of B `BitcoinSN.tex`

39. As before, I will not go over every single chunk individually but I'll sum up some of the most interesting parts to provide a narrative of the edits that took place.

3.3.1 First edits provided

40. The first chunk provided, number 275, is dated 17 November 2023 at 17:33:08.989. As I have said above, this is not the first state of the document, information about which has been redacted.

41. Over the next few minutes, in chunks 275 to 281, the title block visible on the page (not the metadata) is changed. 14 characters are deleted, which appear to correspond to the deletion of `Craig S Wright`, and the author name `Satoshi Nakamoto` is inserted with the email address `satoshin@gmx.com`. The word 'bitcoin' is then added in two places, among other edits.

3.3.2 Edits to paragraph spacing

42. At chunk 318, timed at 18:20:28.096, Dr Wright[4] adds a `\spaceskip` command at the top of the abstract with an incorrect syntax. The command is a TEX 'primitive' (i.e. it comes from the underlying engine, not the top layer) and is extremely specialised: I

[4] I am informed by Bird & Bird that this metadata relates to Dr Wright's edits, and this is confirmed by the contents of `chunks.xlsx` where all entries show the same Overleaf user ID, unless redacted. The name associated with that ID in the file `collaborators.json` is "Craig Wright".

can't remember using it much, if at all. While it can be used to adjust the spacing in a document, it can have a very complex influence on the spacing of all paragraphs and it is thus quite hard to get the desired results from it; the syntax of its invocation, however, is rather simple so it is unexpected to see it being wrong. Anyway, Dr Wright eventually gets the syntax right (at chunk 345), timed at 17 November 2023 at 19:07:16.986.

43. However, that is but not before introducing the textcomp package and its `\textquotesingle` command in some intervening edits. That command typesets a straight quote (instead of the default, curly one). Over the course of the following 71 minutes, 79 edits are made which fiddle with spacing, between chunk 345 and chunk 424. These concern the abstract, which is is essentially re-created line by line, with `\spaceskip` commands interspersed allowing the individual line spacing to be controlled. This does not fit with any kind of typographic practice and struck me as an absurd approach to typesetting. Figure 1 shows an example of the resulting LaTeX code, from the latest available revision of `main.tex`.

3.3.3 Edits to position and scale of images

44. After setting the spacing of the abstract in that way, Dr Wright moved on to edit the position and scale of the images. Between 20:20:40.062 on 17 November 2023 and 17:40:04.236 on 18 November 2023, there are just over 350 edits recorded which are mostly concerned with those matters (chunks 425 to 788). It is in the course of this editing that the eso-pic package is first loaded, with its `\AddToShipoutPictureBG*` command which I reported on in my First Report.

3.3.4 Edits to set the metadata of the resulting PDF

45. At chunk 789 the metadata are altered for the first time, with edits continuing until chunk 812. These edits started on 18 November 2023 at 17:47:47.934 and continued for just over 24 minutes. The first metadata setting commands were as follows:

```
pdftitle={Your Document Title},
pdfauthor={Author Name},
pdfsubject={Subject of the Document},
pdfkeywords={keyword1, keyword2, keyword3},
% other options
```

46. Later changed to:

```
pdftitle={Bitcoin},
pdfauthor={Craig Wright (Aka Satoshi)},
pdfproducer={OpenOffice.org 2.4},
pdfcreator={Writer}
```

```
\begin{center}
  \begin{adjustwidth}{13.48mm}{14.81mm} % Set left and right margins
    \noindent {\boldtimes\fontsize{9}{9.0}\textbf{Abstract}.} % "Abstract." in Times New Roman Bold
    \setstretch{0.96} % Adjust the line spacing as needed
    \fontsize{9}{9.0}\spaceskip=0.520\fontdimen2\font plus 1.4\fontdimen3\font minus 1.25\fontdimen4\font % Adjust w
    \spaceskip=0.30em plus 2.0em minus 0.16em
    \scalebox{0.98}[0.9570]{
    A purely peer-to-peer version of electronic cash would allow online}
    payments to be sent directly from one party to another without going through a

    \spaceskip=0.24em plus 1.0em minus 0.16em
    financial institution.\; Digital signatures provide part of the solution, but the main

    benefits are lost if a trusted third party is still required to prevent double-spending.
    \spaceskip=0.16em plus 0.6em minus 0.20em
    We propose a solution to the double-spending problem using a peer-to-peer network.
    \spaceskip=0.26em plus 2.0em minus 0.16em
    The network timestamps transactions by hashing them into an ongoing chain of
    \spaceskip=0.16em plus 0.6em minus 0.20em
    hash-based proof-of-work, forming a record that cannot be changed without redoing

    the proof-of-work.\; The longest chain not only serves as proof of the sequence of

    events witnessed, but proof that it came from the largest pool of CPU power.\;\; As

    long as a majority of CPU power is controlled by nodes that are not cooperating to

    attack the network, they\textquotesingle ll generate the longest chain and outpace attackers.\;\; The

    network itself requires minimal structure.\;\; Messages are broadcast\; on a best effort
        \spaceskip=0.16em plus 0.6em minus 0.26em
    basis, and nodes can leave and rejoin the network at will, accepting the longest
    \spaceskip=0.12em plus 0.6em minus 0.28em
    \scalebox{0.9718}[0.959]{
    proof-of-work chain as proof of what happened while they were gone.}
  \end{adjustwidth}
\end{center}
```

Figure 1: LaTeX code for the abstract in `main.tex`, as of 13 December 2023. The overflowing comment reads "Adjust word spacing".

3.3.5 Edits to add individual letter spaces

47. Then it's back to spacing commands, this time with a very large number of `\;` commands added in many places, interspersed between words. This goes on until chunk 1421, with a few more tweaks to the image commands in between.

48. These spacing comments are those which I explained at paragraph 119 of my First Report, which each cause a small horizontal space to be added to the text. In that part of my First Report, I pointed out that the spacing of the words seemed to be due to a deliberate change to the source code, which caused results that were sometimes really odd, with different lengths set for the interword spaces (see paragraph 120 and figure 3.8).

49. The spaces were not set all at once, but iteratively one by one, with several hundred 'chunk' edits. Those took place over the course of just under 24 hours on 18 and 19 November 2023, in two sessions. Adding up the total time of those sessions amounts to a cumulative time of around 9 hours of editing across this 24-hour period, predominantly (though not entirely) occupied with adding these individual `\;` spacing commands.

50. The setting of those spaces in so many places is what results in the interword spaces broadly matching what appears to be the default spacing output of OpenOffice in the final output.

3.3.6 Final edits: formulae and code sections, and commented-out essays

51. From chunks 1422 to 1583 (on 19 November 2023), it's the formulae's turn to be tortured, with edits appearing to show experimentation about different ways to change maths fonts. These would eventually all be fruitless, as the maths font in all the disclosed candidate files was always a variant of Computer Modern.

52. After that, chunks 1589 to 1614 show some adjustments to the typesetting of the code listings (C code and its results) and, finally, two little essays about steganography in LaTeX are introduced as code comments, one at the top of **B** `BitcoinSN.tex` at chunks 1659, and another one at the bottom of the file, at chunk 1663.

4 Overall conclusions

4.1 Graph of edits

53. Bird & Bird has produced a graph of the timestamps of the edits which is shown as Figure 2.

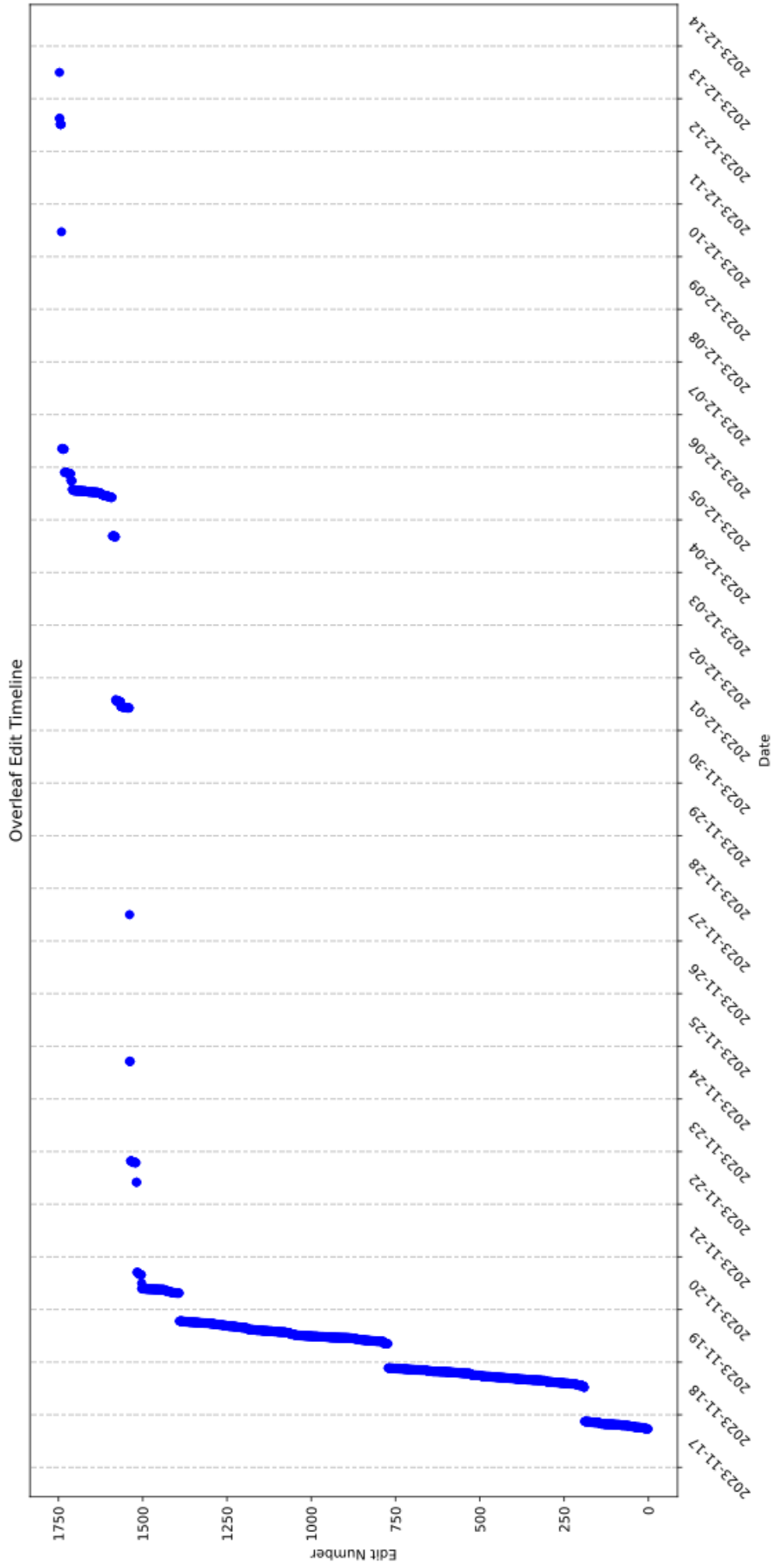


Figure 2: Graph of changes made to `Bitcoin.SN` (first) and `main.tex` (after that)

4.2 Conclusion on edits

54. The overall conclusion is obvious: Dr Wright has been, over the course of 48 hours (from 17 November 17:33 UTC to 19 November 18:21 UTC), editing a single LaTeX file, adding commands to better match the visual appearance of the original Bitcoin White Paper as closely as possible.

55. After finishing the edits to spacing, image scale and position, and formuale to `BitcoinSN.tex` on 19 November 2023, Dr Wright then created a new blank file `main.tex`. The text of `BitcoinSN.tex` was then pasted into `main.tex`, resulting in a hash-identical copy. At that point, further edits were made including commands to set the metadata of the resulting PDF file so that the face-value metadata would resemble an output from OpenOffice. Editing continued up to 12 December 2024, at which point the file `main.tex` found its completed form, and was disclosed as the file I analysed in my First Report as **L**.

56. This was done without regard for the low-level coding of the resultant PDF file (which is very different to the Bitcoin White Paper itself, as I have explained extensively in my First Report); or the fact that some packages and options used were not available in 2008/2009.

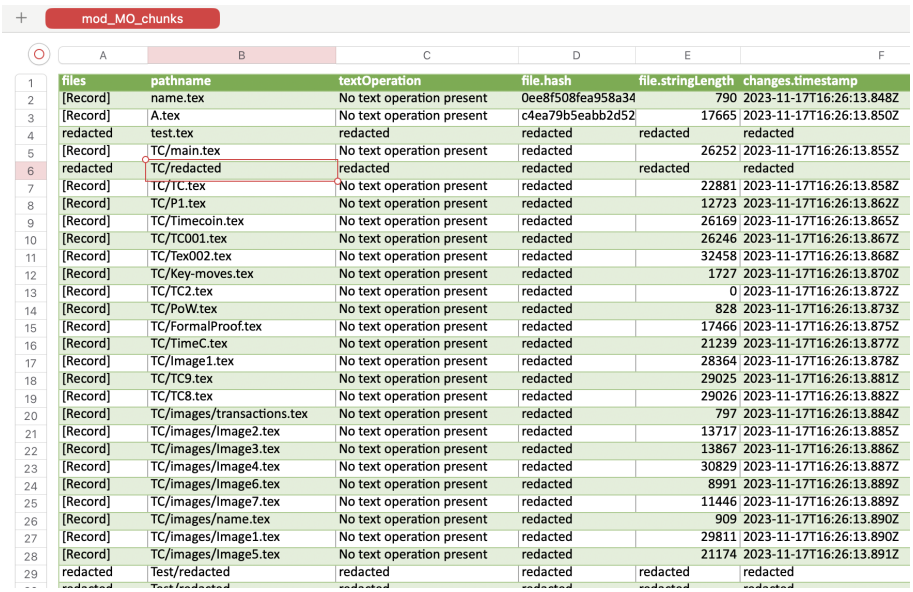
4.3 Conclusion on spacing

57. I understand from Bird & Bird that the steganography essays, as I have been calling them, relate to Dr Wright's explanation of the interword spaces in the document, which is to say that the spaces encode a hidden message.

58. As can be seen from the chunks and my explanation of them above, the interword spacing was not added to the files programmatically or in any obvious pattern, but iteratively by the same user logged in as Dr Wright, during around 22 hours' work across three days. The addition of spaces in this way makes it very difficult to accept that the resultant, odd spacing is part of a steganographic scheme. Rather, it appears to approximate the default output of OpenOffice 2.4, and thus the output of the original Bitcoin White Paper.

4.4 Redactions and missing information

59. The redactions have made it considerably slower to analyse this information, but one omission in particular may be important. After checking thoroughly, I still cannot find the original file `BitcoinSN.tex` anywhere. I see its name mentioned in the `project.json` file, with only an identifier: this means that we should expect to see an entry about the file in `chunks.xlsx`, together with a reference to a file in the `blobs` folder (a "hash



mod_MO_chunks

	files	pathname	textOperation	file.hash	file.stringLength	changes.timestamp
2	[Record]	name.tex	No text operation present	0ee8f508fea958a34	790	2023-11-17T16:26:13.848Z
3	[Record]	A.tex	No text operation present	c4ea79b5eabb2d52	17665	2023-11-17T16:26:13.850Z
4	redacted	test.tex	redacted	redacted	redacted	redacted
5	[Record]	TC/main.tex	No text operation present	redacted	26252	2023-11-17T16:26:13.855Z
6	redacted	TC/redacted	redacted	redacted	redacted	redacted
7	[Record]	TC/TC.tex	No text operation present	redacted	22881	2023-11-17T16:26:13.858Z
8	[Record]	TC/P1.tex	No text operation present	redacted	12723	2023-11-17T16:26:13.862Z
9	[Record]	TC/Timecoin.tex	No text operation present	redacted	26169	2023-11-17T16:26:13.865Z
10	[Record]	TC/TC001.tex	No text operation present	redacted	26246	2023-11-17T16:26:13.867Z
11	[Record]	TC/Tex002.tex	No text operation present	redacted	32458	2023-11-17T16:26:13.868Z
12	[Record]	TC/Key-moves.tex	No text operation present	redacted	1727	2023-11-17T16:26:13.870Z
13	[Record]	TC/TC2.tex	No text operation present	redacted	0	2023-11-17T16:26:13.872Z
14	[Record]	TC/PoW.tex	No text operation present	redacted	828	2023-11-17T16:26:13.873Z
15	[Record]	TC/FormalProof.tex	No text operation present	redacted	17466	2023-11-17T16:26:13.875Z
16	[Record]	TC/TimeC.tex	No text operation present	redacted	21239	2023-11-17T16:26:13.877Z
17	[Record]	TC/Image1.tex	No text operation present	redacted	28364	2023-11-17T16:26:13.878Z
18	[Record]	TC/TC9.tex	No text operation present	redacted	29025	2023-11-17T16:26:13.881Z
19	[Record]	TC/TC8.tex	No text operation present	redacted	29026	2023-11-17T16:26:13.882Z
20	[Record]	TC/images/transactions.tex	No text operation present	redacted	797	2023-11-17T16:26:13.884Z
21	[Record]	TC/images/Image2.tex	No text operation present	redacted	13717	2023-11-17T16:26:13.885Z
22	[Record]	TC/images/Image3.tex	No text operation present	redacted	13867	2023-11-17T16:26:13.886Z
23	[Record]	TC/images/Image4.tex	No text operation present	redacted	30829	2023-11-17T16:26:13.887Z
24	[Record]	TC/images/Image6.tex	No text operation present	redacted	8991	2023-11-17T16:26:13.889Z
25	[Record]	TC/images/Image7.tex	No text operation present	redacted	11446	2023-11-17T16:26:13.889Z
26	[Record]	TC/images/name.tex	No text operation present	redacted	909	2023-11-17T16:26:13.890Z
27	[Record]	TC/images/Image1.tex	No text operation present	redacted	29811	2023-11-17T16:26:13.890Z
28	[Record]	TC/images/Image5.tex	No text operation present	redacted	21174	2023-11-17T16:26:13.891Z
29	redacted	Test/redacted	redacted	redacted	redacted	redacted

Figure 3: Row 6 redacted

value")[5]. Instead I see a omission in the Excel file that is suspicious to me: row 6 has been redacted, as shown in figure 3.

60. I strongly suspect that that row contained information about `BitcoinSN.tex`. It can be seen that it refers to a file inside the `TC` folder, that was created at the inception of the Overleaf project. The row above it, and the 22 rows below, all refer to files in `TC` and have been created within milliseconds of each other (24 files in 36 milliseconds in total): it is not reasonable to suppose that row 6 contained information about a file created by anyone else than the same user. If my understanding is correct then the most likely candidate is `BitcoinSN.tex`.

61. I also note that the "file.hash" column is redacted for almost all rows in the screenshot from figure 3, making it hard to identify which actual files they refer to.

62. Analysing `BitcoinSN.tex` in its original state would have been very instructive, but I do not have it.

[5]When the file is present at the inception of a project (which can be created by uploading a zip file), its hash value is included in `project.json`.

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: 

Dated: 12 February 2024

A Appendix: Errata to my First Report

1. In para 49, in "the 'composite fonts' I introduced in section 2.2", the section number should read "2.2.1";
2. in para 92, "diagrams 2 and 7" should read "diagrams 2 to 7";
3. in para 111, "to define settings, or alter pre-defined defaults, or to create new commands" is unclear and should read "to on the one hand define settings, or alter pre-defined defaults, or to on the other hand create new commands.";
4. in table 3.6 ("the matrix"), the "Maths" row, showing the name of the main maths font, should be corrected in three places: columns B and D should read "Cambria Math", and column M should read "blank boxes". I refer to these values in para 153 but did not tabulate them correctly in my matrix;
5. in para 117, "monospaced" should be deleted. While it is correct that most of the fourteen LaTeX files do indeed use a monospaced font at that place, the particular file I'm commenting on there does not;
6. the phrase "not unreasonable" in para 141 should read "not reasonable";
7. At paras 143 to 147, I discuss the TikZ and its arrows.meta library, the latter being one of the packages I discovered to be problematic. It was only released in September 2013 and calls into question the dating of any Candidate File that uses it (as do 9 out of the 14 files analysed in the First Report). It provides, amongst other things, alternative arrowheads, but I realised since completing my First Report that that library is actually *never used at all* by any of the Candidate Files, or files included by them. The library is loaded, but not actually used because the arrowheads are drawn and filled line-by-line, not by using the command to set the alternative arrowheads. I went halfway towards to this realisation at para 146, and this does not weaken my conclusions in any way; I just wanted to note this curious incident.
8. in para 157, "as seen in 2.6" should read "as seen in figure 2.6"; and
9. in para 198 I observed that the Aspose files were exactly the same as some of Dr Wright's, "up to a possible translation and scaling factor: the reference point may have been different, and possibly the scale too". Having checked the file generated by Aspose against the relevant files of Dr Wright's LaTeX disclosure, I can confirm that the parts that code for the images are identical, up to and including the coordinates, that all have four significant digits.