

1 **WO**

2

3

4

5

6

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ARIZONA**

7

8

9

TD Professional Services,  
Plaintiff,

No. CV-22-00018-PHX-MTL

10

**CLAIM CONSTRUCTION ORDER**

11

v.

12

Truyo Incorporated, et al.,

13

Defendants.

14

15

The Court held a *Markman* hearing on January 18, 2023 and now enters the following claim construction Order.

16

17

**I. BACKGROUND**

18

Plaintiff TD Professional Services owns U.S. Patent Nos. 10,304,062 and 10,628,833 (the “’062 Patent” and the “’833 Patent,” respectively; collectively, the “Patents-in-Suit”). The Patents-in-Suit claim a computer system and methods that employ blockchain-based technology for data regulation compliance. Defendants offer a compliance software product for the European Union’s General Data Protection Regulation (“GDPR”). (Doc. 65, ¶ 22.) Plaintiff alleges that Defendant Intraedge Inc.’s products and related methods directly infringe the Patents-in-Suit and that Defendant Intraedge induced Defendant Truyo, Inc. to infringe the same. (Doc. 60, ¶¶ 81–96.)

19

20

21

22

23

24

25

26

The ’062 Patent issued on May 28, 2019. (Ex. 1 to Plaintiff’s Opening Claim Construction Brief, Doc. 94-1.) The ’833 Patent is a continuation from the ’062 Patent that issued on April 21, 2020. (Ex. 2 to Plaintiff’s Opening Claim Construction Brief, Doc.

27

28

1 94-2.) The Patents-in-Suit share a specification, except for three additional paragraphs in  
 2 the '833 Patent that are not relevant here.<sup>1</sup> The field of invention for both Patents-in-Suit  
 3 is described as “computer architectures that automatically comply with data regulations by  
 4 generating or employing immutable audit ledgers;” particularly “computer systems that  
 5 effectively comply with data processing regulations including, but not limited to, the  
 6 [GDPR].” (Doc. 94-1, Column 1, lines 8-14.)<sup>2</sup> The Background of the Invention section of  
 7 the specification provides in part:

8           Ideally, such a computer system architecture would permit the  
 9 data subjects themselves to access the data being stored about  
 10 them, yet also permit merchants, financial, medical and  
 11 academic professionals (and others) to only access  
 12 pseudonymized data about the data subjects (thereby  
 13 maintaining the data subjects’ privacy and anonymity)  
 14 . . . [and] would seamlessly and automatically generate an  
 15 auditably verified record in a timely fashion that the data stored  
 16 therein complies with data processing regulations such as  
 17 GDPR.

18 (Doc. 94-1, 2:13-22.)

19           The '062 Patent issued with 2 independent claims—claims 1 and 17—and 18  
 20 dependent claims. All but one of the disputed terms are in independent claim 17. Dependent  
 21 claim 19 contains the other disputed term, “private blockchain.” (Doc. 94-1, Col. 11-12.)  
 22 The '833 Patent issued with 2 independent claims— claims 1 and 18—and 20 dependent  
 23 claims. All the disputed terms are in independent claim 18, except for three terms that only  
 24 appear in the '062 Patent claims, as noted in the table in Part III, *infra*. (Doc. 94-2, Col.  
 25 10-12.) Only method claims, claims 17-20 of the '062 Patent and claims 18-20 of the '833  
 26 Patent, are at issue in this action. (Doc. 94 at 2.)

27           The parties have asked the Court to construe thirteen terms from the  
 28 Patents-in-Suit.<sup>3</sup> Pursuant to *Markman v. Westview Instruments, Inc.*, 517 U.S. 370, 372

<sup>1</sup> Because of the nearly identical specification, for ease of reference, the Court cites only to the '062 Patent to represent both Patents-in-Suit unless otherwise noted.

<sup>2</sup> Hereinafter, patent citations will identify the column and line numbers using a colon, e.g., 1:8-14.

<sup>3</sup> The parties originally identified twenty-seven terms for this Court’s construction. (*See* Doc. 73.) The parties later stipulated that the Court need not construe six of the original

1 (1996), the Court must construe the claims as a matter of law. The parties have filed briefs  
2 supporting their proposed constructions of the claim terms. (Docs. 94, 96, 99.) Having  
3 considered the arguments and evidence presented in the parties’ briefs, exhibits, and at the  
4 *Markman* hearing, the Court construes the disputed terms as follows.

## 5 **II. LEGAL STANDARD**

6 Claim construction, the determination of the meaning and scope of the asserted  
7 claim terms in a patent, is a question of law exclusively within the province of the Court.  
8 *Markman*, 517 U.S. at 372; *O2 Micro Int’l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d  
9 1351, 1360 (Fed. Cir. 2008). In construing claim terms, considering the intrinsic evidence,  
10 such as the language of the claims, the specification, and the prosecution history, is  
11 paramount. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–17 (Fed. Cir. 2005) (en banc)  
12 (quotation omitted). The Court should first “look to the words of the claims themselves,”  
13 giving them their plain and ordinary meaning, unless clearly stated otherwise. *Vitronics*  
14 *Corp. v. Conceptoronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996). The plain and ordinary  
15 meaning of a claim term is “the meaning that the term would have to a person of ordinary  
16 skill in the art in question at the time of the invention.” *Phillips*, 415 F.3d at 1312–13. The  
17 plain and ordinary meaning of a term should control, unless “a patentee sets out a definition  
18 and acts as his own lexicographer, or . . . disavows the full scope of a claim term either in  
19 the specification or during prosecution.” *Torner v. Sony Computer Entm’t Am. LLC*, 669  
20 F.3d 1362, 1365 (Fed. Cir. 2012). The claim language can provide insight based on the  
21 context of how the terms are used and by comparison to the use of the same or similar  
22 terms in other claims in the patent. *Phillips*, 415 F.3d at 1314.

23 The Court next looks to the patent specification as “the single best guide to the  
24 meaning of a disputed term” and “usually dispositive.” *Id.* at 1315; *see also Merck & Co.*  
25 *v. Teva Pharm. USA, Inc.*, 347 F.3d 1367, 1371 (Fed. Cir. 2003) (explaining that “claims  
26 must be construed so as to be consistent with the specification”). Courts therefore may rely

27 \_\_\_\_\_  
28 terms (Doc. 92) and provided an agreed construction for another eight of those terms (Doc.  
79). A list of the thirteen terms construed in this Order is contained in the table in Part III,  
*infra*.

1 heavily on the written description of the claims in the specification for guidance. *Phillips*,  
2 415 F.3d at 1317. When reviewing the specification, however, courts must avoid reading  
3 limitations from the specification into the claims. *Id.* at 1323 (“[A]lthough the specification  
4 often describes very specific embodiments of the invention, we have repeatedly warned  
5 against confining the claims to those embodiments.”). Courts should also consider the  
6 patent’s prosecution history, or the record of the patent application proceedings before the  
7 United States Patent and Trademark Office (the “USPTO”). *Phillips*, 415 F.3d at 1317. The  
8 prosecution history, although lacking the “clarity” of the specification, is also part of the  
9 intrinsic record and provides evidence of how the USPTO and the inventor understood the  
10 patent and what its claims cover. *Id.* In particular, the prosecution history may provide  
11 evidence on whether the inventor limited the scope of the claimed invention to obtain the  
12 patent, thereby making the claim scope narrower than it otherwise would be. *Id.*

13         The Court may also consider extrinsic evidence, such as technical dictionaries,  
14 learned treatises, and the testimony of experts and inventors.<sup>4</sup> *Id.* For example, expert  
15 testimony can help “ensure that the court’s understanding of the technical aspects of the  
16 patent is consistent with that of a person of skill in the art, or to establish that a particular  
17 term in the patent or the prior art has a particular meaning in the pertinent field.” *Id.* at  
18 1318. But the Court must discount any expert testimony “that is clearly at odds with the  
19 claim construction mandated by the claims themselves, the written description, and the  
20 prosecution history, in other words, with the written record of the patent.” *Id.* (internal  
21 quotations omitted). Although it may prove useful, extrinsic evidence is less significant  
22 than the intrinsic record for determining the meaning of claim language. *Id.* In most  
23 situations, analysis of the patent and its prosecution history will resolve any ambiguity in  
24 a disputed claim term. *Vitronics*, 90 F.3d at 1583.

25  
26  
27  
28  

---

<sup>4</sup> “Because dictionaries, and especially technical dictionaries, endeavor to collect the  
accepted meanings of terms used in various fields of science and technology, those  
resources have been properly recognized as among the tools that can assist the court in  
determining the meaning of particular terminology to those of skill in the art of the  
invention.” *Phillips*, 415 F.3d at 1318.

### III. CLAIM CONSTRUCTION

The following chart summarizes the Court’s adopted constructions for each of the disputed claim terms. The analysis supporting the constructions follows.

Claim Term	Term Location	Adopted Construction
“data input stream”	’062 Patent, Cl. 17(a) ’833 Patent, Cl. 18(a)	A transmission of data related to an exchange or interaction between parties
“data collection terminal”	’062 Patent, Cl. 17(a) ’833 Patent, Cl. 18(a)	A terminal for collecting data that includes a compliance device driver
“compliance markup language tags”	’062 Patent, Cl. 17(b)	Text, defined by a data controller, that instructs the compliance markup language parser to identify, categorize, and forward data elements
“compliance device driver”	’062 Patent, Cl. 17(b) ’833 Patent, Cl. 18(b)	Software, resident in the data collection terminal, that intercepts the data input stream
“compliance markup language parser”	’062 Patent, Cl. 17(c) ’833 Patent, Cl. 18(c)	Software that performs pseudonymization and determines which data is sent to the data output device
“automated compliance network appliance”	’062 Patent, Cl. 17(c) ’833 Patent, Cl. 18(c)	A physical device (having a processor, memory and local storage)
“network interface connection”	’062 Patent, Cl. 17(c) ’833 Patent, Cl. 18(c)	A physical USB drive or physical router
“local storage”	’062 Patent, Cl. 17(c) ’833 Patent, Cl. 18(c)	Plain and ordinary meaning
“pseudonymized data”	’062 Patent, Cl. 17(c) ’833 Patent, Cl. 18(c)	Data in which some portion of the fields are replaced with one or more artificial identifiers (rather than being removed)
“blockchain miners”	’062 Patent, Cl. 17(d) ’833 Patent, Cl. 18(d)	Processors that achieve consensus in a blockchain system by solving mathematical problems
“data lake”	’062 Patent, Cl. 17(e) ’833 Patent, Cl. 18(e)	A data repository that stores raw, unstructured data, and is not a database
(e) . . . , while simultaneously; (f) . . . , and (g) . . . ;	’062 Patent, Cl. 17(e)	Plain and ordinary meaning
“private blockchain”	’062 Patent, Cl. 19	Plain and ordinary meaning

1           **A. “data input stream”**

2           Plaintiff proposes the following construction: “Any data that is input into the  
3 described invention and is capable of being collected by a collection terminal.” (Doc. 104-1  
4 at 1.) Defendants propose the following competing construction: “A continuous  
5 transmission of data related to an exchange or interaction between parties.” (*Id.*) In its  
6 reply, Plaintiff stipulates that the “data” in the “data input stream” is limited to “data  
7 concerning ‘an exchange or interaction between parties,’” but does not agree that the  
8 transmission must be “continuous.” (Doc. 99 at 2-3.)

9           The disputed term is mentioned four times in independent claim 17 of the ’062  
10 Patent. Claim 17 requires:

11                   (a) collecting a data input stream with a data collection  
12                   terminal; (b) selecting in-scope data in the data input stream  
13                   that corresponds to pre-identified data fields by identifying  
14                   compliance markup language tags embedded in the data input  
15                   stream. . . ; (e) transmitting the data input stream into a data  
                    lake as raw, unstructured and unaltered data. . . .

16 (Doc. 94-1, 11:16–12:7.) The specification explains that “[t]he data input stream can  
17 comprise data about can be [sic] purchases, restaurant bills, legal agreements, academic  
18 grades, financial transactions, travel locations and itineraries, etc.” (*Id.* at 5:5-8.)  
19 Importantly, none of these references to the “data input stream” in the patent itself require  
20 that it be input as a continuous transmission, as Defendants suggest. Although Defendants  
21 attempt to rely on extrinsic evidence in the form of expert testimony and a definition of  
22 “streaming data transmission,” the Court finds these sources unpersuasive and unsupported  
23 by the intrinsic record.<sup>5</sup> *Phillips*, 415 F.3d at 1318. On the other hand, Plaintiff’s proposed  
24

---

25 <sup>5</sup> Defendants’ proffered definition for “streaming data transmission” is a “method of  
26 transmitting a media file in a continuous stream of data that can be processed by the  
27 receiving computer before the entire file has been completely sent.” (Doc. 96 at 11.)  
28 Defendants do not point to any support in the intrinsic record that the invention  
contemplates the transmission of media files or should be limited as such. Indeed, the  
preamble of Claim 17, “[a] method of providing an auditable record showing transaction  
compliance with data regulations,” does not suggest that the incoming data stream is a  
media file.

1 construction unnecessarily repeats limitations from the claim language that do not provide  
2 clarity on the meaning of the term. *Bicon, Inc. v. Straumann Co.*, 441 F.3d 945, 950 (Fed.  
3 Cir. 2006) (“[C]laims are interpreted with an eye toward giving effect to all terms in the  
4 claim.”) Thus, the Court construes “data input stream” to mean a transmission of data  
5 related to an exchange or interaction between parties.

6 **B. “data collection terminal”**

7 Plaintiff proposes the following construction: “Any device for collecting a data  
8 input stream, including but not limited to, a point of sale terminal, a web page, a cash  
9 register, a check in counter, a hand held mobile device, a virtual terminal and/or an API.”  
10 (Doc. 101-1 at 2.) Defendants propose the following competing construction: “A terminal  
11 for collecting data that includes a compliance device driver.” (*Id.*)

12 The parties dispute whether the data collection terminal must include a compliance  
13 device driver. “Data collection terminal” is mentioned once in independent claim 17 and  
14 once in dependent claim 18 of the ’062 Patent. Claim 17 requires “collecting a data input  
15 stream with a data collection terminal.” (Doc. 94-1, 11:16-17.) Claim 18 further describes  
16 the same method using “a point of sale terminal, a webpage, a cash register, a check-in  
17 counter, a hand-held mobile device, or an API.” (*Id.* at 12:19-23.) “Compliance device  
18 driver” is also mentioned once in Claim 17: “. . . wherein the in-scope data are selected by  
19 a compliance device driver. . . .” (*Id.* at 11:23-24.)

20 The specification describes the “data collection terminal” and “compliance device  
21 driver” in further detail, in reference to Figures 1, 2, and 3. Figure 1 “is a system diagram  
22 of the present invention.” (*Id.* at 4:26.) In box 1, Figure 1 illustrates a “Data Collection  
23 Terminal with Compliance Device Driver.” (*Id.* at Fig. 1.) Figure 2 “is a system diagram  
24 showing further details of the compliance enabled data collection terminal” of Figure 1.  
25 (*Id.* at 4:27-28.) In box 9, Figure 2 illustrates a “Compliance Device Driver.” (*Id.* at Fig.  
26 2.) Figure 3 “is a system diagram showing further details of the compliance device driver”  
27 of Figure 1. (*Id.* at 4:29-30.)

28 The specification explains:



1 Referring first to FIG. 1, an overview of computer architecture  
2 101 for providing compliance with data regulations is  
3 provided, as follows. A data collection terminal 1 is configured  
4 to receive a data input stream. A compliance device driver (9  
5 in FIG. 2) is resident in data collection terminal 1. The  
6 compliance device driver performs . . . two functions.

7 (*Id.* at 4:49-55). The specification further explains, “[a]s can be seen, the automated  
8 compliance network appliance 2 is in communication with compliance device driver 9  
9 within data collection terminal 1.” (*Id.* at 5:25-27.) The specification goes on:

10 FIG. 2 shows further details of the data collection terminal with  
11 compliance device driver 1, as follows. In various aspects, data  
12 collection terminal 1 can include any suitable data input device  
13 7 for collecting data, including, but not limited to, a point of  
14 sale terminal, a webpage, a cash register, a check-in counter, a  
15 hand-held mobile device, or an API.

16 (*Id.* at 5:54-60.) The specification does not contemplate or describe any variation of a  
17 compliance device driver that is not present in the data collection terminal. Furthermore,  
18 the specification does not suggest that having the compliance device driver within the data  
19 collection terminal is optional or preferred, as it does with other components of the system.  
20 As an example, Figure 2 also illustrates that the data collection terminal contains a “data  
21 input device” in box 7, a “POS application” in box 8, and an “output device” in box 11.  
22 (*Id.* at Fig. 2.) Notably, with reference to these components, the specification explains that  
23 “[t]he data collection terminal *optionally* comprises a data input device and a data output  
24 device.” (*Id.* at 3:51-52 (emphasis added); *see also id.* at 5:61-62 (“*Preferably*, data  
25 collection terminal 1 comprises a data input device 7 and a data output device 11.”)  
26 (emphasis added).) “*In optional preferred aspects*, the data collection terminal includes a  
27 Point Of Sale (POS) Application 8 therein.” (*Id.* at 6:14-15 (emphasis added).) In contrast,  
28 the specification does not use optional language when describing that the compliance  
device driver resides in the data collection terminal.<sup>6</sup> Thus, the Court finds that the

<sup>6</sup> Moreover, as Plaintiff pointed out at the hearing, the specification uses the terms “preferably,” “optionally,” “for example,” or “can be” 28 times to identify preferred



1 specification supports Defendants’ proposed construction requiring the data collection  
2 terminal to contain a compliance device driver.

3 Plaintiff rejects the explanation of these terms in the specification because it is in  
4 reference to the system claims, as opposed to the method claims at issue here. The Court  
5 notes, however, that Plaintiff’s insistence that the detailed description of the invention must  
6 be split into two sections is unsupported by any authority. *See Philips*, 415 F.3d at 1313  
7 (“[T]he person of ordinary skill in the art is deemed to read the claim term not only in the  
8 context of the particular claim in which [it] appears, but in the context of the entire patent,  
9 including the specification.”). Additionally, the prosecution history shows that in making  
10 amendments and arguments to the USPTO, the applicant argued the system and method  
11 claims together, citing the same evidence from the specification for both types of claims.  
12 (See Doc. 94-6 at 2, 5.) Moreover, there are only two paragraphs in the entire specification  
13 that specifically reference the method claims and neither of them discuss the compliance  
14 device driver. (Doc. 94-1, 8:34-56.) Thus, to the extent Plaintiff asks the Court to limit its  
15 consideration to those two paragraphs, the Court declines. Only reviewing that section of  
16 the specification for support would implicate potential written description and enablement  
17 issues related to the “compliance device driver” in claim 17. *See Liebe-Flarsheim Co v.*  
18 *Medrad, Inc.*, 358 F.3d 898, 911 (Fed. Cir. 2004) (holding that where claim terms are  
19 ambiguous, “claims should be so construed, if possible, as to sustain their validity.”). The  
20 parties did not brief these issues and the Court need not reach them to resolve the parties’  
21 dispute.

22 For its part, Plaintiff seeks to define the data collection terminal from claim 17 using  
23 various examples enumerated in claim 18 with the addition of “a virtual terminal.”  
24 Independent claims are presumed to have broader scope than their dependents, however.  
25 *Acumed LLC v. Stryker Corp.*, 483 F.3d 800, 806 (Fed. Cir. 2007). The presence of a  
26 \_\_\_\_\_  
27 aspects of the invention. Such qualifying language is not used with respect to whether the  
28 data collection terminal includes a compliance device driver. *See Rexnord Corp. v. Laitram Corp.*, 274 F.3d 1336, 1345 (Fed. Cir. 2001) (relying on an inventor’s “careful” and “consistent” use of phrases throughout the specification identifying preferred embodiments to find that an inventor has described an invention that encompasses more than one embodiment).

1 particular limitation in a dependent claim raises a presumption that the limitation is not  
2 found in the independent claim. *Id.* “That presumption is especially strong when the  
3 limitation in dispute is the only meaningful difference between an independent and  
4 dependent claim, and one party is urging that the limitation in the dependent claim should  
5 be read into the independent claim.” *Id.* Here, Plaintiff does not adequately explain a  
6 meaningful difference between its proposed construction and the limitations in claim 18.  
7 The addition of “a virtual terminal” to the list from claim 18 does not do enough to  
8 differentiate the claims because it is not a term found in the intrinsic record. Moreover,  
9 Plaintiff’s attempt to limit the data collection terminal to the enumerated list of preferred  
10 embodiments in the specification is contrary to established precedent. *Comark*  
11 *Communications, Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed. Cir. 1998) (holding that  
12 it is generally improper to read a limitation from the specification into the claim). Thus,  
13 the Court declines to adopt Plaintiff’s proposed construction. The Court adopts  
14 Defendants’ proposed construction, a terminal for collecting data that includes a  
15 compliance device driver, for the reasons discussed above.

16 **C. “compliance markup language tags”**

17 Plaintiff proposes the following construction: “Metadata that identifies or bounds  
18 certain information within a data input stream, in relation to pre identified data fields,  
19 including but not limited to any markup language from any text e-coding system.” (Doc.  
20 104-1 at 1.) Defendant proposes the following competing construction: “User-defined text  
21 that instructs the compliance markup language parser to identify, categorize, and forward  
22 data elements related to compliance regulations.” (*Id.*)

23 Claim 17 is directed to “[a] method of providing an auditable record showing  
24 transaction compliance with data regulations.” (Doc. 94-1, 11:14-15.) Claim 17 requires:  
25 “selecting in-scope data in the data input stream that corresponds to pre-identified data  
26 fields by identifying compliance markup language tags embedded in the data input stream,  
27 wherein the pre-identified data fields are determined by data compliance regulations . . .”<sup>7</sup>

28 \_\_\_\_\_  
<sup>7</sup> The ’883 Patent claims do not recite compliance language markup tags.

1 (*Id.* at 11:18-22.) The specification describes the functionality of the compliance device  
2 driver and compliance markup language parser using “compliance markup language tags”:

3 [T]he compliance device driver 9 applies a compliance markup  
4 language parser (15 in FIG. 3) to the selected data, thereby  
5 generating pseudonymized data. . . . Specifically, as seen in  
6 FIG. 3, the compliance markup language parser 15 scans the  
7 data subject receipt data stream 13 and identifies ***compliance***  
8 ***markup language tags*** that are embedded within data stream  
9 13 as defined by a data controller 32 (FIG. 6). ***The compliance***  
10 ***markup language tags*** instruct the compliance markup  
11 language parser 15 to identify, categorize, and forward data  
12 elements within the data stream to automated compliance  
13 network appliance 2.

11 (*Id.* at 5:9-24 (emphasis added).) Additionally, the specification explains that Figure 7,  
12 which “illustrates the use of compliance markup language to generate a printed sales  
13 receipt” is “exemplary” of how the invention uses the compliance markup language tags to  
14 define “data elements that fall within the scope of GDPR or other data regulation[s].” (*Id.*  
15 at 4:39-40; 8:66–9:21.)

16 As Plaintiff notes, the central dispute is “whether the ‘compliance markup language  
17 tags’ are properly limited to ‘data elements related to compliance regulations.’” (Doc. 94  
18 at 10.) Plaintiff argues that the background information on compliance regulations in the  
19 specification is not definitional. Plaintiff further argues that limiting the tags to compliance  
20 regulations is not required because the claims already include that “the pre-identified data  
21 fields are determined by data compliance regulations.” (Doc. 94 at 12-13.) Defendant  
22 argues that the text of the claims themselves clearly require that the tags relate to  
23 compliance regulations, “so any proposed construction should appropriately contextualize  
24 this aspect of the claim term.” (Doc 96 at 14.)

25 The Court finds this limitation unnecessary in view of the claim language. The  
26 disputed term itself includes the word “compliance,” indicating that the markup language  
27 tags are related to compliance. Moreover, claim 17 requires that “the pre-identified data  
28 fields are determined by data compliance regulations.” (Doc. 94-1, 11:21-22.) The claim

1 language explicitly links those pre-identified data fields to the compliance markup  
2 language tags: “selecting in-scope data in the data input stream that corresponds to pre-  
3 identified data fields by identifying compliance markup language tags embedded in the  
4 data input stream. . . .”<sup>8</sup> (*Id.* at 11:18-22.) It is clear from the claim that the data is selected  
5 based on data compliance regulations. Thus, the Court need not look to other evidence to  
6 resolve this dispute. *Vitronics*, 90 F.3d at 1582 (observing that “we look to the words of  
7 the claims themselves . . . to define the scope of the patented invention”). The Court finds  
8 that requiring the tags to be related to compliance regulations is unnecessary.

9         Additionally, the phrase “user-defined text” in Defendants’ construction is too broad  
10 to have intrinsic support in the specification. Instead, it is more accurate to construe the  
11 term to incorporate that the text underlying the tags is defined by the data controller. The  
12 term “user defined” is only used once in the specification, while the term “data controller”  
13 is used nineteen times. In the one instance where “user defined” appears, the specification  
14 notes that the tags “are user defined by [the] data controller.” (Doc. 94-1, 9:3-5.) Data  
15 controllers are defined as “organizations that collect, process, or control [] personal data  
16 from EU residents [] to comply with regulations.” (*Id.* at 1:28-30.) The specification  
17 explains that the compliance markup language parser “identifies compliance markup  
18 language tags that are embedded within data stream [] as defined by a data controller.” (*Id.*  
19 at 5:18-20; *see also* 6:58-59 (the system operates “in accordance with the processing  
20 requirements defined by data controller 32.”).) Although the data controller is a user of the  
21 system, the specification also identifies other users who do not have access to define the  
22 markup language tags. (*See id.* at 2:14-17 (“permit the data subjects themselves to access  
23 the data being stored about them, yet also permit merchants, financial, medical and  
24 academic professionals (and others) to only access pseudonymized data”); 3:34-36 (“data  
25 privacy is maintained such [that] these 3rd parties cannot access the full sets of all of the  
26 data stored corresponding to each data subject”); 3:41-43 (“auditors can view the

---

27  
28 <sup>8</sup> Additionally, the parties agree that the construction of a related term, “compliance markup  
language” is “a language that uses tags to identify compliance-related attributes of elements  
of a data stream.” (Doc. 101 at 8.)

1 compliance data without requiring access to any of the private information or systems”).)  
2 Thus, the Court’s construction substitutes “data controller” for “user” in Defendants’  
3 proposed construction.

4 Finally, the Court finds that describing the tags in terms of their functionality is  
5 appropriate here. In describing the compliance device driver’s functionality, the  
6 specification explains that the tags instruct the compliance markup language parser “to  
7 identify, categorize, and forward data elements within the data stream.” (*Id.* at 4:54-5:24.)  
8 This is the only explanation of the tags’ functionality in the specification and the inventor  
9 did not use suggestive language indicating that these functions are merely a preferred  
10 embodiment. *See Rexnord*, 274 F.3d at 1345. The specification further describes “an  
11 exemplary” use of the tags that is consistent with the functional description identified  
12 above. (Doc. 94-1, 8:66–9:2 (“An opening compliance tag 38 and a closing compliance tag  
13 44 define the opening and closing boundaries for data elements that fall within the scope  
14 of GDPR or other data regulation.”).)

15 Plaintiff’s construction, on the other hand, includes the unsupported terms  
16 “metadata” and “text e-coding system.” The Court finds that introducing these terms of art  
17 without support from intrinsic or extrinsic evidence would unnecessarily complicate the  
18 meaning of compliance markup language tags.<sup>9</sup> Accordingly, the Court adopts the  
19 following construction: text, defined by a data controller, that instructs the compliance  
20 markup language parser to identify, categorize, and forward data elements.

21 **D. “compliance device driver”**

22 Plaintiff proposes the following construction: “Any non-transitory  
23 computer-readable medium having instructions stored therein that when executed by a  
24 computing device selects the in-scope data.” (Doc. 101-1 at 2.) Defendant proposes the  
25 following competing construction: “Hardware and software, resident in the data collection  
26 terminal, that intercepts the data input stream via a piping instruction.” (*Id.*)

27 \_\_\_\_\_  
28 <sup>9</sup> Although Plaintiff proposes this construction, Plaintiff’s arguments are directed towards  
why Defendants’ construction is incorrect, not why its own construction is the right one.  
(*See* Docs. 94, 99.)

1 As discussed above, “compliance device driver” is mentioned once in Claim 17:

2 selecting in-scope data in the data input stream . . . wherein the  
3 in-scope data are selected by *a compliance device driver*  
4 comprising a non-transitory computer-readable medium  
5 having instructions stored therein that when executed by a  
6 computing device selects the in-scope data[.]

6 (Doc. 94-1, 11:18-27 (emphasis added).)<sup>10</sup> The specification explains:

7 The compliance device driver performs the following two  
8 functions. First, it selects data in the data input stream that  
9 corresponds to pre-identified data fields. . . . Second, the  
10 compliance device driver 9 applies a compliance markup  
11 language parser (15 in FIG. 3) to the selected data, thereby  
12 generating pseudonymized data.

12 (*Id.* at 4:54-57; 5:9-11).

13 First, the parties dispute whether the “compliance device driver” includes both  
14 hardware and software. Plaintiff supports its proposed construction based on a definition  
15 of compliance device driver that is already recited in independent claim 17. As such, it  
16 does not provide any additional clarity and would render the entire clause following the  
17 term redundant. *Bicon*, 441 F.3d at 950 (“[C]laims are interpreted with an eye toward  
18 giving effect to all terms in the claim.”). Accordingly, the Court declines to adopt Plaintiff’s  
19 proposed construction. Defendants rely on the specification and prosecution history.  
20 Defendants also argue that to a person of ordinary skill in the art, “a non-transitory  
21 computer-readable medium having instructions stored therein” plainly means that the  
22 compliance device driver is both hardware and software. (Doc. 96 at 18.) The Court finds  
23 that, given the explicit definition in claim 17 that the compliance device driver comprises  
24 “a non-transitory computer-readable medium having instructions stored therein,” there is  
25 no need to include the terms “hardware and software” in the construction. Moreover, the  
26 Court has adopted a construction of “data collection terminal” that includes the compliance

27 <sup>10</sup> Similarly, independent Claim 18 of the ’833 patent recites: “selecting data in the data  
28 input stream, . . . wherein the data are selected by a compliance device driver comprising  
a non-transitory computer-readable medium having instructions stored therein that when  
executed by a computing device selects the data[.]” (Doc. 94-2, 12:14-21.)

1 device driver therein, as discussed above, and nothing in the intrinsic record requires that  
2 the compliance device driver itself be a hardware component within the data collection  
3 terminal. Defendant’s citation to the prosecution history and Plaintiff’s expert’s testimony  
4 both support this.

5 During prosecution, the applicant explained that the invention teaches “a physical  
6 compliance device (having a device driver resident therein)” and the claims were “amended  
7 to describe the compliance device being a non-transitory computer readable medium  
8 having instructions stored therein.” (Doc. 94-6 at 2.) Although Defendant points to this  
9 language as requiring the driver itself to be hardware, the Court disagrees. The applicant  
10 clearly distinguishes between a compliance device and a compliance device driver.  
11 *Phillips*, 415 F.3d at 1317 (“[T]he prosecution history can often inform the meaning of the  
12 claim language by demonstrating how the inventor understood the invention and whether  
13 the inventor limited the invention in the course of prosecution, making the claim scope  
14 narrower than it would otherwise be.”) (citing *Vitronics*, 90 F.3d at 1582–83). This  
15 interpretation is also supported by Plaintiff’s expert testimony that a person of ordinary  
16 skill in the art would ordinarily refer to a driver as software that is stored on hardware, such  
17 as the computer-readable non-transitory medium with stored executable instructions  
18 recited in claim 17. (See Doc. 99 at 9); see also *Philips*, 415 F.3d at 1318 (“[E]xpert  
19 testimony can be useful to a court for a variety of purposes, such as to . . . establish that a  
20 particular term in the patent or the prior art has a particular meaning in the pertinent field.”)  
21 (citing *Pitney Bowes, Inc. v. Hewlett-Packard Co.*, 182 F.3d 1298, 1308–09 (Fed. Cir.  
22 1999)).

23 The parties also dispute whether “intercepts the data input stream via a piping  
24 instruction” is a required limitation. As noted above, the specification describes that the  
25 compliance device driver performs two functions: selecting data from the data input stream  
26 and applying a parser to the selected data to create pseudonymized data. (Doc. 94-1,  
27 4:49-57; 5:9-11). The specification describes these steps in further detail as follows:

28 First, the full data stream 13 relating to a data subject is



1 received. Next, at 14, the data stream is intercepted via a piping  
2 instruction that re-directed the data stream to the compliance  
3 markup language parser 15. After processing by parser 15, the  
4 data is then directed into output device 11. Compliance markup  
5 language parser 15 performs pseudonymisation [sic] (and  
6 optionally encryption as well) at 18, thereby sending  
7 pseudonymized [sic] data to automated compliance network  
8 appliance 2. (In the absence of data stream intercept 14, the  
9 data would instead simply pass directly into output device 15  
10 without being pseudonymised [sic]).

11 (*Id.* at 6:25-36.) This discussion makes it clear that intercepting the data stream is an  
12 important, necessary step in the invention. If there is no interception step, “the data would  
13 instead simply pass directly into output device 15 without being [pseudonymized].” (*Id.*)  
14 One advantage of the invention is to “shield[] private information from public  
15 stakeholders.” (*Id.* at 4:21-22.) Without intercepting the data for pseudonymization, one  
16 purpose of the invention would not be achieved. Courts must construe claims in a manner  
17 that achieves the invention’s contemplated purpose and covers any preferred embodiments  
18 outlined in the specification. *Accent Packaging, Inc. v. Leggett & Platt, Inc.*, 707 F.3d  
19 1318, 1326 (Fed. Cir. 2013) (“[A] claim interpretation that excludes a preferred  
20 embodiment from the scope of the claim is rarely, if ever, correct.”) (citation omitted).  
21 Further, the above excerpt is the only portion of the specification that details how the  
22 compliance device driver selects the in-scope data as claimed in Claim 17.

23 Defendants argue that the data interception must occur “via a piping instruction”  
24 because the specification only teaches intercepting the data in this manner. (Doc. 96 at  
25 20-22.) Plaintiff argues that intercepting the data using a piping instruction is a preferred  
26 embodiment only, so the compliance device driver should not be limited to operating by  
27 this process. (Doc. 99 at 8.) “Our case law is clear that an applicant is not required to  
28 describe in the specification every conceivable and possible future embodiment of his  
invention.” *Rexnord*, 274 F.3d at 1344 (citing *SRI Int’l v. Matsushita Elec. Corp. of  
America*, 775 F.2d 1107, 1121 (Fed. Cir. 1985) (en banc)). “[I]f structural claims were to  
be limited to devices operated precisely as a specification-described embodiment is

1 operated, there would be no need for claims. Nor could an applicant, regardless of the prior  
2 art, claim more broadly than that embodiment.” *Id.* (quoting *SRI Int’l*, 775 F.2d at 1121).  
3 Elsewhere in the specification, this data interception step is described more broadly:

4 [T]he compliance device driver 9 applies a compliance markup  
5 language parser (15 in FIG. 3) to the selected data, thereby  
6 generated pseudonymized data. . . . [T]he compliance markup  
7 language parser 15 scans the data subject receipt data stream  
8 13 and identifies compliance markup language tags that are  
9 embedded within data stream 13 as defined by a data controller  
10 32 (FIG. 6). The compliance markup language tags instruct the  
11 compliance markup language parser 15 to identify, categorize,  
12 and forward data elements within the data stream to automated  
13 compliance network appliance 2.

14 (Doc. 94-1, 5:9-24.) “When the claim language is assessed on its own, and when the written  
15 description is examined carefully, one finds that the patentee has described an invention  
16 that embraces” data interception and routing techniques broadly, and the Court need not  
17 limit the process to occurring via a piping instruction. *See Rexford*, 274 F.3d at 1345; *Valve*  
18 *Corp. v. Ironburg Inventions Ltd.*, 8. F.4th 1364, 1381 (Fed. Cir. 2021) (the proposed  
19 construction “improperly imports a limitation into the claim from a preferred  
20 embodiment”) (quoting *Trebro Mfg., Inc. v. Firefly Equip., LLC*, 748 F.3d 1159, 1166 (Fed.  
21 Cir. 2014)).

22 Accordingly, the Court adopts the following construction: software, resident in the  
23 data collection terminal, that intercepts the data input stream.

24 **E. “compliance markup language parser”**

25 Plaintiff proposes the following construction: “Software that performs or  
26 contributes to the selection of in scope data based on any markup language from any text  
27 e-coding system.” (Doc. 104-1 at 1.) Defendant proposes the following competing  
28 construction: “Software that is part of the compliance device driver that performs  
pseudonymization, and determines which data is sent to the data output device.” (*Id.*)

The parties’ dispute centers on whether the compliance markup language parser is

1 part of the compliance device driver.<sup>11</sup> Neither party argues for or against Plaintiff's  
2 proposed construction, and the Court notes that it is unnecessarily broad and introduces a  
3 "text e-coding system" that has no support in the intrinsic record.

4 Claim 17 provides, in part:

5 (b) selecting in-scope data in the data input stream that  
6 corresponds to pre-identified data fields by identifying  
7 compliance markup language tags embedded in the data input  
8 stream, . . . wherein the in-scope data are selected by a  
9 compliance device driver. . . ;

10 (c) applying a compliance markup language parser to the  
11 in-scope selected data, and wherein the compliance markup  
12 language is applied by an automated compliance network  
13 appliance comprising a network interface connection having a  
14 processor, memory, and local storage, thereby generating  
15 pseudonymized data. . . .

16 (Doc. 94-1, 11:18–12:2). From the claim language alone, it is not clear that the compliance  
17 markup language parser is a required component of the compliance device driver.  
18 Similarly, the specification suggests the parser could be part of the compliance device  
19 driver but also refers to it as a separate component with its own functionality. For example,  
20 the specification describes that the compliance device driver applies the parser to  
21 pseudonymize selected data that is sent to the automated compliance network appliance.  
22 (*Id.* at 5:9-11; 5:27-31 ("Automated compliance network appliance . . . receives the  
23 pseudonymized data generated by the compliance driver [] and then transmits [it] to the  
24 Internet.")) Elsewhere in the specification, the parser performs the pseudonymization and  
25 sends the pseudonymized data to the automated compliance network appliance without  
26 reference to the compliance device driver. (*Id.* at 6:30-33.)

27 Figure 3 "is a system diagram showing further details of the compliance device  
28 driver of FIG. 1" and includes a compliance markup language parser in box 15. (*Id.* at

---

<sup>11</sup> In its reply, Plaintiff clarifies that it does not dispute that the compliance markup language parser performs pseudonymization or determines which data is sent to the data output device. (Doc. 99 at 10-11.)

1 4:29-30; Fig. 3.) In reference to Figure 3, the specification explains that “the data stream  
2 is intercepted via a piping instruction that re-directed the data stream to the compliance  
3 markup language parser 15.” (*Id.* at 6:27-29.) After receiving the data selected by the  
4 compliance device driver, the compliance markup language parser scans it “and identifies  
5 compliance markup language tags . . . embedded within data stream” and uses those tags  
6 “to identify, categorize, and forward data elements within the data stream to [the]  
7 automated compliance network appliance.” (*Id.* at 5:16-24.) These descriptions do not limit  
8 the location of the compliance markup language parser to the compliance device driver.

9 Defendants argue that the specification describes a compliance markup language  
10 parser housed within the compliance device driver and provides no alternative teachings  
11 regarding the parser’s location. (Doc. 96 at 23.) In reference to the method claims, however,  
12 the specification does not limit the location of the parser to the compliance device driver  
13 or any other component of the system. “In another aspect, the present system includes a  
14 method of providing an auditable record showing transaction compliance with data  
15 regulations, by: . . . applying a compliance markup language parser to the selected data,  
16 thereby generating pseudonymized data. . . .” (Doc. 94-1 at 2:51-59; *see also id.* at 8:34-42.)  
17 The Court finds that the specification supports variations of the invention where the  
18 compliance markup language parser is not within the compliance device driver, particularly  
19 in view of the plain language of claim 17. *See Raytheon Co. v. Roper Corp.*, 724 F.2d 951,  
20 957 (Fed. Cir. 1983) (“That claims are interpreted in light of the specification does not  
21 mean that everything expressed in the specification must be read into all the claims.”).  
22 Thus, the Court adopts the following construction: software that performs  
23 pseudonymization and determines which data is sent to the data output device.

24 **F. “automated compliance network appliance”**

25 Plaintiff proposes the following construction: “Any network interface connection  
26 having processor, memory, and local storage and having some physical embodiment.”  
27 (Doc. 104-1 at 1.) Defendants propose the following competing construction: “A physical  
28 device (having a processor, memory and local storage), separate from the data collection

1 terminal and compliance device driver.” (*Id.*)

2 The parties agree that the “automated compliance network appliance” contains a  
3 processor, memory, and local storage in physical form. This is supported by the plain  
4 language of claim 17(c), requiring “an automated compliance network appliance  
5 comprising a network interface connection having a processor, memory and local  
6 storage[.]”<sup>12</sup> There is also support in the prosecution history. The applicant amended the  
7 claims to overcome the examiner’s rejection of the claims as abstract “software per se”  
8 under 35 U.S.C. § 101. (Doc. 94-6 at 2-3.) The applicant noted that the independent claims  
9 were amended to include “a physical network interface connection” and argued that the  
10 amended claims “clearly describe a physical system . . . (i.e.: comprising a network  
11 appliance that is a USB drive or router. . . .)” (*Id.* at 2.) Thus, the parties only remaining  
12 dispute centers on whether the automated compliance network appliance must be separate  
13 from both the data collection terminal and compliance device driver. (Doc. 99 at 12.)

14 Independent claim 17 does not address the present dispute. Independent claim 1  
15 requires “an automated compliance network appliance in communication with the  
16 compliance device driver,” the compliance device driver being “resident in the data  
17 collection terminal.” (Doc. 94-1 at 9:55-56; 10:5-6.) The specification also teaches this.  
18 (*Id.* at 5:25-27.) Figures 1, 2, and 3 all show that the automated compliance network  
19 appliance, box 2, is separate from the data collection terminal and the compliance device  
20 driver. (*See id.* at Figs. 1-3.) Specifically, Figure 3, which shows details of the compliance  
21 device driver, illustrates two pathways from the compliance markup language parser, box  
22 15, that the data may take: one pathway leading to an output device, box 11, and another  
23 pathway leading to the automated compliance network appliance. (*Id.* at Fig. 3.)

24 Defendants argues that the written description and figures require that the automated

25 \_\_\_\_\_  
26 <sup>12</sup> The Court finds that Plaintiff’s proposed inclusion of “any network interface” within the  
27 construction would render the claim language redundant because claim 17 already requires  
28 that the claimed automated compliance network appliance comprise a network interface  
connection. Thus, the Court adopts the portion of Defendants’ construction requiring that  
the automated compliance network appliance simply be a physical device. *Bicon*, 441 F.3d  
at 950 (“[C]laims are interpreted with an eye toward giving effect to all terms in the  
claim.”) This is in accordance with the parties’ agreement.

1 compliance network appliance be separate from the data collection terminal and  
2 compliance device driver.<sup>13</sup> (Doc. 96 at 26-27.) Defendants point to the two pathways for  
3 data transfer in Figure 3, arguing that, “because there are two data streams, the [automated  
4 compliance network appliance] must be separate from the compliance device driver.” (Doc.  
5 96 at 26.) The Court is unpersuaded. The specification expressly contemplates that  
6 including the output device, box 11 of Figure 3, within the data collection terminal is  
7 optional. (Doc. 94-1 at 3:51-52.) The specification does not explicitly reference where the  
8 automated compliance network appliance is housed within the system. That the invention  
9 teaches optionally including the output device within the data collection terminal, however,  
10 undermines Defendants’ logic that the automated compliance network appliance must be  
11 separate based on the flow of data in Figure 3. *See Gart v. Logitech, Inc.*, 254 F.3d 1334,  
12 (Fed. Cir. 2001) (finding a proposed construction improper where it would “add a  
13 limitation appearing in the specification and the drawings, but not appearing in the  
14 unambiguous language of the claim”).

15       Regarding, the prosecution history, Defendants argue that the applicant “clearly  
16 treated the [automated compliance network appliance] and compliance device driver as  
17 being separate from one another by adding different physical limitations to each  
18 element[.]” (*Id.* at 27.) During prosecution, the applicant argued that the amended claims  
19 comprise “a network appliance that is a USB drive or router, operating together with a  
20 physical compliance device (having a device driver resident therein) . . . .” (Doc. 94-6 at  
21 2). The amended claims require that the compliance device driver comprise “a  
22 non-transitory computer-readable medium having instructions stored therein” and the  
23 automated compliance network appliance comprise “a network interface connection  
24 having a processor, memory and local storage.” (Doc. 96-4 at 8.) Defendants’ arguments  
25 fail to clearly explain how these statements during prosecution explicitly disavow

---

26  
27 <sup>13</sup> Defendants also rely on extrinsic evidence, including the deposition testimonies of  
28 inventor Scott Hines and the applicant’s prosecuting attorney Mr. Heckdon, who both  
testified that the figures show that the automated compliance network appliance is separate  
from, but in communication with, the compliance device driver. (*See* Doc. 96-12, 133:7-10;  
*see also* Doc. 96-6, 110:17–113:21.)



1 embodiments of the invention where these components are not separate. *Purdue Pharma*  
2 *L.P. v. Endo Pharmaceuticals Inc.*, 438 F.3d 1123, 1136 (Fed. Cir. 2006) (prosecution  
3 disclaimer requires that a patentee make “a clear and unmistakable disavowal of [claim]  
4 scope during prosecution”). As Plaintiff notes, nothing in the applicant’s responses  
5 explicitly disavowed coverage of an automated compliance network appliance housed  
6 within any other component of the claimed invention. *See Omega Eng’g Inc. v. Raytek*  
7 *Corp.*, 334 F.3d 1314, 1323 (Fed. Cir. 2003).

8 Moreover, neither party requests that the Court construe the term “in  
9 communication with,” which is a term of art in the specification that Defendants argue  
10 definitively establishes that their construction is the correct one. The Court is not persuaded  
11 that sufficient evidence in the intrinsic record exists to limit the term as Defendants  
12 propose, nor that the extrinsic evidence is clear on this issue. The only explicit limitation  
13 on the claim term scope comes from the applicant’s amendments and arguments during  
14 prosecution, limiting the automated compliance network appliance to a physical device.  
15 Accordingly, the Court adopts the following construction: a physical device (having a  
16 processor, memory and local storage).<sup>14</sup>

17 **G. “network interface connection”**

18 Plaintiff proposes the following construction: “USB drive or router which has some  
19 physical embodiment.” (Doc. 104-1 at 1.) Defendant proposes the following competing  
20 construction: “A physical USB drive or physical router.” (Doc. 96 at 27.) Plaintiff concedes  
21 that the parties’ proposed constructions are “not materially different.” (Doc. 99 at 13.)  
22 Given these concessions, the Court adopts Defendants proposed construction as the most  
23 concise version of the parties’ agreed upon meaning. Moreover, Defendants’ construction  
24 is consistent with the intrinsic record, including the specification and the prosecution  
25 history, as discussed above with respect to the term “automated compliance network  
26 appliance.” (Doc. 94-1, 3:60-64; Doc. 94-6 at 2.)

27 \_\_\_\_\_  
28 <sup>14</sup> Although the Court finds that including “having processor, memory, and local storage”  
is likely redundant in view of the claim language, the parties stipulate to include it in the  
Court’s adopted construction.



1           **H.     “local storage”**

2           Plaintiff proposes the following construction of: “Storing data in a hardware device  
3 and/or in memory.” (Doc. 104-1 at 1) Defendant proposes that the term be given its plain  
4 and ordinary meaning. (*Id.*)

5           The parties dispute whether “local storage” is limited to a hardware storage device  
6 or whether it can encompass storing data in memory. The Court resolves the parties’  
7 dispute by adopting the plain and ordinary meaning because the parties agree that a person  
8 of ordinary skill in the art would understand local storage to cover data storage in a  
9 hardware device. Moreover, because claim 17 recites “a network interface connection  
10 having a processor, memory, and local storage,” adding memory to the definition of local  
11 storage would improperly render its inclusion in the claim redundant. *Bicon*, 441 F.3d at  
12 950 (“Allowing a patentee to argue that physical structures and characteristics specifically  
13 described in a claim are merely superfluous would render the scope of the patent  
14 ambiguous. . . .”). The Court’s adopted construction is supported by an absence of inventor  
15 lexicography or claim scope disavowal in the intrinsic record that would give local storage  
16 a specialized meaning in this context. *See Torner*, 669 F.3d at 1365 (holding that unless “a  
17 patentee sets out a definition and acts as his own lexicographer” or disavows claim scope,  
18 the plain and ordinary meaning of the term should control).

19           **I.     “pseudonymized data”**

20           The Court adopts the following construction that the parties have agreed to: data in  
21 which some portion of the fields are replaced with one or more artificial identifiers (rather  
22 than being removed). (*See* Doc. 101-1 at 2.) This is supported by the definition provided  
23 in the specification. (Doc. 94-1, 5:11-16 (“As understood herein, ‘pseudonymized data’ is  
24 data in which most of the identifying fields within a data record are replaced within one or  
25 more artificial identifiers, or pseudonyms, thereby rendering the data less identifying to  
26 provide for greater Data Subject privacy.”)); *Philips*, 415 F.3d at 1316 (Where “the  
27 specification [] reveal[s] a special definition given to a claim term by the patentee that  
28 differs from the meaning it would otherwise possess. . . , the inventor’s lexicography

1 governs.”).

2 **J. “blockchain miners”**

3 Plaintiff proposes the following construction: “Any blockchain network participant  
4 that participates in verifying blocks of data transactions.” (Doc. 101-1 at 2.) Defendant  
5 proposes the following competing construction: “Processors that achieve consensus in a  
6 blockchain system by solving ‘proof of complexity’ mathematical problems.” (*Id.*)

7 The parties’ dispute centers on whether the invention is limited to a blockchain  
8 verification system that utilizes blockchain miners to solve proof of complexity math  
9 problems.

10 Claim 17 mentions the term “blockchain miners” twice:

11 ... (d) transmitting the pseudonymized data of the in-scope data  
12 in batches to blockchain miners; . . . (f) receiving verified  
13 blockchain blocks from the blockchain miners, and (g) storing  
14 the verified blockchain blocks in a blockchain derived  
immutable audit ledger. . . .

15 (Doc. 94-1, 12:4-14.) The specification explains the invention’s blockchain component by  
16 referring to blockchain miners as a preferred embodiment:

17 A first advantage of the present system is that it utilizes  
18 blockchain technology to reliably generate the immutable audit  
19 ledger. . . . The immutable audit ledger is *preferably* generated  
20 by utilizing a private blockchain in which blocks are added to  
21 the blockchain after they have been *verified by dedicated*  
22 *miners*. A “proof of complexity” problem solving system is  
23 used. This approach advantageously *allows dedicated miners*  
24 *to solve the mathematical problem rapidly enough to allow*  
*the miners to achieve consensus within a desired time frame,*  
while still providing sufficient randomness in the selection of  
the miner awarded the right to write the block.

25 (*Id.* at 2:65–3:10 (emphasis added).) The specification further explains:

26 Preferably, the automated compliance network appliance  
27 transmits data to the Internet in batches such that it is  
28 pre-prepared for the blockchain miners. An advantage of  
sending data in batches to a group of pre-selected private  
miners is that the blocks can be solved (i.e.: consensus can be

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

achieved between the miners) and written faster (as compared to using individual data transmissions and a public blockchain approach).

(*Id.* at 3:14-21; *see also id.* at 7:9-11 (“If the data was not sent in batches to the blockchain miners, the blockchain miners will be required to validate each data subject transaction one by one.”).) The specification also explains the use of a private blockchain employing a proof of complexity system as a preferred embodiment:

Preferably, the blockchain is a private blockchain that uses a proof of complexity problem/solution to write individual blocks to the chain. . . . In operation, the validated transactions are recorded by the miners on a shared distributed ledger. Specifically, whichever miner solves the proof of complexity problem first will get to write the block (after independent verification of the block by the other miners). By using a private or permissioned blockchain with a private field of miners. . . , the required proof of complexity can be reduced. This is very advantageous in reducing the time required to verify and add blocks to the chain. . . . In accordance with the present private blockchain system, miner consensus on blocks may be achieved (for example) in as little as 12 hours, and potentially less time. It is to be understood, of course, that the average time to solve and write the blocks will depend both upon the specific numerical problem the miners are assigned and the number of miners working on the problem. . . . Another advantage of using private minors [sic] is that you don't have to pay them.

(*Id.* at 7:40–8:4.) Finally, the specification describes using “hashes” to verify transactions with respect to the same preferred embodiment:

[E]ach line in [the blockchain derived, immutable audit ledger] 5 contains . . . a hash value associated with the contents. Ledger data is hashed together and the collection of the hashes is grouped into a block. The contents of each block is then hashed with the hash of the previous block. The blocks are then validated by other blockchain miners. The hash stored in the blockchain can be compared to the hash of the transaction in the data lake to verify that the contents of the data lake have not been changed.

1 (*Id.* at 8:6-17; *see also id.* at 9:37-42 (“A transaction bundling software system 48 is a  
2 system within the blockchain platform that prepares data blocks received from automated  
3 compliance network appliance 2 into blocks of data that can be hashed and written to the  
4 immutable ledger 5 by the blockchain miners 49.”).) Notably, the specification explicitly  
5 contemplates the use of other types of blockchain verification systems: “In accordance with  
6 the present system, proof of work (i.e.: solving computationally intense mathematical  
7 problem[s]), proof of complexity and proof of stake consensus modeling (which uses less  
8 resources) can be used.” (*Id.* at 7:66–8:2.)

9 Defendants argue that the blockchain verification model in the claimed invention  
10 must be limited to proof of complexity problems solved using computer processors. (Doc.  
11 96 at 35.) Defendants rely on the claim language and the specification’s written description  
12 and figures, arguing that only a proof of complexity model is supported because there are  
13 no details on how a proof of stake model would be integrated into the invention. (*Id.* at  
14 34-36) Specifically, Defendants point to Figure 9, illustrating “the present invention in a  
15 preferred system of operation,” that includes a box for “mining HW.” (*See* Doc. 94-1,  
16 3:5-6, Fig. 3.) Defendants rely on expert testimony, arguing that proof of complexity and  
17 proof of work are synonymous, while proof of stake operates by a different mechanism  
18 that does not use processors to solve complex math problems. (Doc. 96 at 36-37.)  
19 Defendants note that during Plaintiff’s expert’s deposition, when asked if the specification  
20 described algorithms to implement a proof of stake model, the expert stated, “I can’t  
21 imagine that it would or why it would.” (*Id.* at 36 (quoting Doc. 96-11, 279:15-18).) At the  
22 hearing, Defendants’ expert also opined that the terms “proof of complexity,” “blockchain  
23 miners,” and “hashes” are all terms of art that a person of skill in the art would recognize  
24 limit the invention to exclude proof of stake systems.

25 Plaintiff argues that “[n]othing in the claim language limits the ‘blockchain miners’  
26 to ‘proof of complexity.’” (Doc. 94 at 26.) Plaintiff further argued at the *Markman* hearing  
27 that the specification’s use of “preferably” in reference to blockchain shows that a proof of  
28 complexity model is a nonlimiting preferred embodiment. Plaintiff relies on the one

1 sentence in the specification noting that proof of work, proof of complexity, and proof of  
2 stake models can all be used with the present system. (Doc. 94 at 26; *see also* Doc. 94-1,  
3 7:66–8:2.) Plaintiff also cites a Techopedia definition of “mining” to show that a person of  
4 ordinary skill in the art would not understand “mining” to be limited to “proof of  
5 complexity” models.<sup>15</sup> (Doc. 94 at 27.) Defendants argue that Plaintiff’s definition actually  
6 supports Defendants’ position because it defines mining to require a fast computer  
7 processor and references that the term is “best known for its association with bitcoin.”  
8 (Doc. 96 at 37.) Defendant offers the Techopedia definition for “bitcoin mining,” which  
9 references a proof of work consensus model and mining “through mathematical processes.”  
10 (*Id.* at n.14 (citing Doc. 96-14 at 2).)

11 The Court notes that specification contemplates the use of proof of work and proof  
12 of stake iterations of blockchain verification. The Court also notes that each time the proof  
13 of complexity process is explained, the specification uses words to suggest that it is a  
14 preferred embodiment. The claim language itself, however, limits the claimed invention to  
15 the use of “blockchain miners” to verify blockchain blocks. (Doc. 94-1, 12:4-10.) The  
16 specification does not define blockchain miners, indicating that the inventor used that term  
17 in accordance with its commonly understood meaning to a person of skill in the art at the  
18 time of the invention. *See Torner*, 669 F.3d at 1365 (holding that unless “a patentee sets  
19 out a definition and acts as his own lexicographer” or disavows claim scope, the plain and  
20 ordinary meaning of the term should control). Defendants’ expert explained that to a person

21 \_\_\_\_\_  
22 <sup>15</sup> The Techopedia definition states, in relevant part:

23 Mining, in the context of blockchain technology, is the process  
24 of adding transactions to the large distributed public ledger of  
25 existing transactions, known as the blockchain. The term is  
26 best known for its association with bitcoin, though other  
27 technologies using the [blockchain] employ  
28 mining. . . . Mining involves creating a hash of a block of  
transactions that cannot be easily forged, protecting the  
integrity of the entire blockchain without the need for a central  
system. Mining is typically done on a dedicated computer, as  
it requires a fast CPU, as well as higher electricity usage and  
more heat generated than typical computer operations. . . .

(Doc. 96-13 at 2-3.)

1 of ordinary skill in the art, employing blockchain miners is specific to proof of work and  
2 proof of complexity models, while proof of stake models refer to their verification entities  
3 as “validators.” The expert further testified that because miners solve complex math  
4 problems, only computer processors could be used as miners. In other words, the expert  
5 opined that human validators would not be able to verify the data transactions contemplated  
6 in the specification. Plaintiff’s expert did not refute these points. The Court is persuaded  
7 by Defendants’ expert and explanation of the parties’ proffered technical definitions.  
8 *Phillips*, 415 F.3d at 1318 (expert testimony and technical dictionary definitions can help  
9 “ensure that the court’s understanding of the technical aspects of the patent is consistent  
10 with that of a person of skill in the art, or to establish that a particular term in the patent or  
11 the prior art has a particular meaning in the pertinent field”). This extrinsic evidence is  
12 consistent with the usage of “blockchain miners” in the intrinsic record. The Court finds  
13 that, in view of the extrinsic evidence, the claim language itself limits the claimed invention  
14 to those blockchain systems that utilize blockchain miners to verify blockchain  
15 transactions.

16 Courts must be careful not to read preferred embodiments into the claims. *Comark*,  
17 156 F.3d at 1187. The Court finds that although the specification references a proof of  
18 complexity approach as a preferred embodiment, the claim’s use of blockchain miners is  
19 not so limited. The specification explains that the preferred proof of complexity  
20 implementation requires the miners to solve mathematical problems and explains how such  
21 a system would operate to generate the immutable audit ledger. (*See* Doc. 94-1, 2:65–3:21,  
22 7:40–8:15.) The specification also states that “proof of work (i.e.: solving computationally  
23 intense mathematical problem[s]) . . . consensus modeling” can be used. (*Id.* at 7:66–8:2.)  
24 Based on the specification and expert testimony, the Court finds that the inventor’s use of  
25 miners would not preclude any other type of system that utilizes complex math problems  
26 for verification, such as proof of work. Moreover, a person of skill in the art would  
27 understand how to implement different approaches to blockchain validation that use  
28 miners, such as proof of work, without needing a separate detailed description. *Phillips*,

1 415 F.3d at 1323 (“[A]lthough the specification often describes very specific embodiments  
2 of the invention, we have repeatedly warned against confining the claims to those  
3 embodiments.”). On the other hand, other verification approaches that employ techniques  
4 other than complex math problems and miners, such as proof of stake models, are not  
5 sufficiently described to enable a person of ordinary skill in the art to implement the  
6 claimed invention using those methodologies. *Netword, LLC v. Centraal Corp.*, 242 F.3d  
7 1347, 1352 (Fed. Cir. 2001) (“Although the specification need not present every  
8 embodiment or permutation of the invention and the claims are not limited to the preferred  
9 embodiment of the invention, neither do the claims enlarge what is patented beyond what  
10 the inventor has described as the invention.”) (internal citations omitted).

11 Thus, the Court adopts the following construction: processors that achieve  
12 consensus in a blockchain system by solving mathematical problems.

13 **K. “data lake”**

14 Plaintiff proposes the following construction of “data lake”: “Any stored collection  
15 of raw or near raw, structured or unstructured data.” (Doc. 104-1 at 1.) Defendant proposes  
16 the following competing construction: “A data repository that (a) stores raw, unstructured  
17 data, and (b) is not a database.” (*Id.*)

18 The parties dispute whether the data stored in the data lake must be entirely raw and  
19 unstructured, and whether the claimed data lake encompasses a database. Plaintiff concedes  
20 that the plain language of claim 17 of the ’062 Patent requires the data to be raw and  
21 unstructured but argues that this limitation should not apply to the meaning of data lake in  
22 the ’833 patent claims. (Doc. 99 at 16.) Plaintiff also “acknowledges that a ‘data lake’ and  
23 a ‘data base’ generally refer to different things, although companies can and do use data  
24 base software as a data lake.” (Doc. 94 at 27.)

25 Claim 17 of the ’062 Patent requires “transmitting the data input stream into a data  
26 lake as raw, unstructured and unaltered data.” (Doc. 94-1, 12:6-7.) Claim 18 of the ’833  
27 Patent is broader on its face, requiring “transmitting the data input stream into a data lake.”  
28 (Doc. 94-2, 12:29.) As previously noted, the ’062 Patent and the ’833 Patent share a



1 specification, meaning that the detailed description to support both sets of claims is  
2 identical, as relevant here. The '833 Patent also expressly incorporates “the entire  
3 disclosure” of the '062 Patent “by reference in its entirety for all purposes.” (Doc. 94-2 at  
4 1:9-13.) The shared specification does not reference “raw, unstructured data” or otherwise  
5 define “data lake.” During prosecution of the '062 Patent, however, the applicant  
6 characterized the data lake as different from a database to overcome the examiner’s  
7 rejection of the claims as abstract under 35 U.S.C. § 101. The applicant explained that:

8 the presently claimed system stores data in a *data lake*. A data  
9 lake is fundamentally different from a simple *database*. A  
10 database is a very structured system of storing data records. In  
11 contrast, a data lake is basically a *pool of raw, unstructured*  
12 *data*. Data is not prepared, classified, structured, or otherwise  
13 pulled apart or otherwise sorted out in a data lake. Instead, data  
14 is simply dumped into a data lake in its raw form.

15 (Doc. 96-4 at 12-13 (emphasis in original).) The applicant further relies on the use of a data  
16 lake to differentiate the invention from other systems:

17 The presently claimed computer architecture *combines a data*  
18 *lake together with a blockchain generated record* of the data  
19 in the data lake in a single unified system. This is  
20 fundamentally different from existing blockchain systems that  
21 use simple databases. Data in a database can easily be changed,  
22 and it is often impossible to reliably tell if the data in the  
23 database has been changed. The present computer architecture  
24 solves this problem by instead using a *data lake* (not a  
25 database). The present computer architecture simply “tosses all  
26 the raw data into the data lake” so to speak. As such, the data  
27 in the data lake can’t easily be changed. Also, simply tossing  
28 the data into a data lake can be done very quickly. As such, the  
present system’s use of a data lake *increases the overall speed*  
at which the system operates (as compared to existing systems  
that use old fashioned databases).

Importantly, as the data is being tossed into the data lake, the  
present system simultaneously generates a legally auditable  
record of the data in the data lake. The advantage of the present  
approach (i.e.: simply tossing all of the raw data into a data  
lake while simultaneously generating an auditable record of the

1 integrity of this data – all within a single computer architecture)  
2 has not been attempted prior to the present invention. The  
3 present novel architecture provides substantially *increased*  
4 *speed*, greatly *increased security* while using *far less*  
5 *computer resources* as compared to existing computer  
6 systems.

7 (*Id.* at 13 (emphasis in original).) This explanation accompanied an amendment to the  
8 independent claims of the '062 Patent adding “as raw, unstructured and unaltered data” to  
9 the limitation requiring the data input stream to be transmitted into a data lake. (*Id.* at 9.)

10 “The doctrine of prosecution disclaimer is well established in Supreme Court  
11 precedent, precluding patentees from recapturing through claim interpretation specific  
12 meanings disclaimed during prosecution.” *Omega*, 334 F.3d at 1323.<sup>16</sup> Generally, the Court  
13 begins with a heavy presumption that claim terms carry their full ordinary and customary  
14 meaning. *Id.* But, “a patentee may limit the meaning of a claim term by making a clear and  
15 unmistakable disavowal of scope during prosecution.” *Purdue*, 438 F.3d at 1136.  
16 Disavowal may occur, for instance, when the patentee “explicitly characterizes an aspect  
17 of his invention in a specific manner to overcome prior art.” *Id.* The patentee must have  
18 taken a position before the USPTO that would lead a competitor to believe that the  
19 applicant had disavowed coverage of the relevant subject matter. *Omega*, at 1325 (citing  
20 *Schwing GmbH v. Putzmeister Aktiengesellschaft*, 305 F.3d 1318, 1324–25 (Fed. Cir.  
21 2002)). If a patentee “has unequivocally disavowed a certain meaning to obtain his patent,  
22 the doctrine of prosecution disclaimer attaches and narrows the ordinary meaning of the  
23 claim congruent with the scope of the surrender.” *Id.* at 1324.

24 The specification only contemplates that the data stored in the data lake be  
25 “unaltered,” not that it be raw or unstructured. (Doc. 94-1, 8:5-6.) Plaintiff points to Figure  
26 7 for support, arguing that it “clearly identi[fies] an example of structured data submitted  
27 to the data lake” because it “shows a common point of sale transaction that in its raw form

28 <sup>16</sup> Although the parties argue that the similar concept of prosecution history estoppel is at issue here, the Court notes that the proper analysis at the claim construction stage is under the doctrine of prosecution disclaimer. *Omega*, 334 F.3d at 1326 n.1 (Fed. Cir. 2003).

1 is structured into a ‘header section’ and an itemized list of data structured into columns.”  
2 (Doc. 94 at 28.) After reviewing the prosecution history, however, the Court finds that the  
3 applicant’s arguments to the USPTO would lead a competitor to believe that that they were  
4 disavowing coverage of a database with “prepared, classified, structured, or otherwise  
5 pulled apart or otherwise sorted out” data. The applicant’s statements, emphasizing the  
6 advantages of using a data lake over a data base, limit claim 17’s use of “data lake” to “a  
7 pool of raw, unstructured data” and “not a database.” (Doc. 96-4 at 12-13.) The prosecution  
8 history shows that the applicant narrowed the scope of “data lake” to overcome the  
9 examiner’s rejection of the claims as an unpatentable abstract idea. (Doc. 96-3 at 5.) Based  
10 on the intrinsic record, the Court finds that prosecution disclaimer clearly applies to the  
11 ’062 Patent.

12 The Court also finds that the disclaimer applies to the ’833 Patent’s use of the term  
13 “data lake.” “[T]he prosecution history of one patent is relevant to an understanding of the  
14 scope of a common term in a second patent stemming from the same parent application.”  
15 *Microsoft Corp. v. Multi-Tech Systems, Inc.*, 357 F.3d 1340, 1349 (Fed. Cir. 2004). “[T]he  
16 prosecution of one claim term in a parent application will generally not limit different claim  
17 language in a continuation application,” *Invitrogen Corp. v. Clontech labs., Inc.*, 429 F.3d  
18 1052, 1078 (Fed. Cir. 2005), but, “[a] disclaimer in the parent application [can] carr[y]  
19 forward into the construction of the same claim term in the child,” *Cordis Corp. v. Boston*  
20 *Scientific Corp.*, 658 F.3d 1347, 1356 n.5 (Fed. Cir. 2011). *See also Omega*, 334 F.3d at  
21 1333 (“As long as the same claim limitation is at issue, prosecution disclaimer made on the  
22 same limitation in an ancestor application will attach.”). The relevant test is whether “the  
23 purported disclaimers are directed to specific claim terms that have been omitted or  
24 materially altered in subsequent applications (rather than to the invention itself).” *Saunders*  
25 *Grp., Inc. v. Comfortrac, Inc.*, 492 F.3d 1326, 1333 (Fed. Cir. 2007). If so, the prior  
26 prosecution disclaimer does not apply to limit the claimed invention in the later patent  
27 where those same claim terms are not used. *Id.* When the same claim terms are used, it is  
28 possible to explicitly rescind a prosecution disclaimer in an earlier patent such that a

1 continuation patent is not bound by the claim scope limitation, however. *See Hakim v.*  
2 *Cannon Avent Grp., PLC*, 479 F.3d 1313, 1318 (Fed. Cir. 2007). To effectively rescind a  
3 prior disclaimer, the applicant “must be sufficiently clear to inform the examiner that the  
4 previous disclaimer . . . may need to be re-visited.” *Id.*

5 Neither party specifically addresses the relevant tests for prosecution disclaimer and  
6 recission with respect to continuation applications. At the *Markman* hearing, Defendants  
7 argued that courts must interpret common terms in a patent consistently across all related  
8 patents. Plaintiff argued that the ’833 Patent’s use of “data lake” in independent claim 18  
9 is “deliberately” “much broader” because it does not include the “as raw, unstructured  
10 data” limitation added during prosecution of the ’062 Patent. (Doc. 99 at 17.) The parties  
11 both rely on *Microsoft* for support. 357 F.3d 1340. In *Microsoft*, the Federal Circuit  
12 affirmed a district court’s construction limiting claim terms in three related patents based  
13 on the applicant’s statements during prosecution of one of the patents. *Id.* at 1348–1350.  
14 The court found that the applicant’s statements made during prosecution, were “relevant to  
15 an understanding of the common disclosure” in the shared specification because the  
16 applicant’s statement was a representation of its own understanding of the inventions  
17 disclosed in all three patents.”<sup>17</sup> *Id.* at 1350.

18 Here, the Court finds that the ’833 Patent’s use of “data lake” must be limited by  
19 the applicant’s statements during prosecution of the ’062 Patent. As discussed above, the  
20 applicant discussed the advantages of the invention’s data lake for three paragraphs. (Doc.  
21 96-4 at 12-13.) The applicant clearly indicated that the data lake was important to the  
22 overall invention and provided specific advantages over conventional computer systems.  
23 (*Id.*) The Court finds that these statements were not limited to the “raw, unstructured data”  
24 amendment, but were instead intended to convince the examiner that the entire claimed  
25 invention was patentable and not abstract. (*Id.* at 11-13); *see Microsoft*, 357 F.3d at 1350  
26 (“We take the patentee at its word and will not construe the scope of the [continuation]

27  
28 <sup>17</sup> In so doing, the court refused to apply some of the applicant’s statements to all of the  
asserted patents “because they refer[red] more specifically to the references cited against  
the claims of [one] patent only.” *Id.* at 1349 n.5.

1 patent's claims more broadly than the patentee itself clearly envisioned.”).

2 For both the Patents-in-Suit, the claims were rejected under 35 U.S.C. § 101 as  
3 directed to unpatentable subject matter. The applicant's prosecution disclaimer is thus not  
4 specific to the examiner's rejection of the '062 Patent. Indeed, the '833 Patent's own  
5 prosecution history belies Plaintiff's arguments to the contrary. The applicant made the  
6 following remarks when faced with a similar rejection during prosecution of the '833  
7 patent: “The Examiner rejected the pending claims as being directed to non-statutory  
8 subject matter. Suitable amendment has been made to overcome these rejections  
9 (substantially paralleling similar amendments that were made in the parent case (now  
10 issued U.S. Patent 10,304,062)).” (Doc. 96-5 at 8.) The amendments to the '833 Patent  
11 claims did not include the “as raw, unstructured data” limitation, but both independent  
12 claim 17 and 18 require a “data lake.” There is no evidence before the Court that the  
13 applicant sought to recapture a broader scope for data lake in the '833 Patent claims. *See*  
14 *Microsoft*, 357 F.3d at 1350 (“Any statement of the patentee in the prosecution of a related  
15 application as to the scope of the invention would be relevant to claim construction, and  
16 the relevance of the statement made in this instance is enhanced by the fact that it was made  
17 in an official proceeding in which the patentee had every incentive to exercise care in  
18 characterizing the scope of its invention.”). Plaintiff fails to point to any portion of the '833  
19 Patent's prosecution history where the applicant explicitly rescinded the prior disclaimer  
20 or otherwise “inform[ed] the examiner that the previous disclaimer . . . may need to be re-  
21 visited.” *See Hakim*, 479 F.3d at 1318.

22 Accordingly, the Court adopts Defendants' proposed construction for both Patents-  
23 in-Suit: a data repository that stores raw, unstructured data, and is not a database.

24 **L. “(e) ..., while simultaneously; (f) ..., and (g) ...;”**

25 Plaintiff proposes the following construction: “Transmitting, receiving, and storing  
26 as described, in a manner satisfied by the same values.” (Doc. 101-1 at 2.) Conversely,  
27 Defendants argue that “[s]teps (e), (f) and (g) must all be performed at the same time.” (*Id.*)  
28 Plaintiff asserts that “simultaneously,” as used in the patent, is a term of art in computer

1 science, while Defendants seek to rely on the conventional definition of the term.

2 Claim 17 provides, in part:

- 3 (e) transmitting the data input stream into a data lake as raw,  
4 unstructured and unaltered data, while simultaneously;  
5 (f) receiving verified blockchain blocks from the blockchain  
6 miners, and  
7 (g) storing the verified blockchain blocks in a blockchain  
8 derived immutable audit ledger, wherein the blockchain  
9 derived immutable audit ledger certifies that the data stored in  
10 the data lake is correct and unaltered. . . .

11 (Doc. 94-1, 12:6-14.) Simultaneously does not appear in the specification. It was added  
12 during prosecution to overcome an examiner’s rejection under 35 U.S.C. §§ 101, 102, and  
13 103. (See Doc. 96-4.)

14 During prosecution, “the Examiner requested . . . evidence of ‘something more’ than  
15 a conventional computer system” and that the applicant “explain how the present invention  
16 solves [] existing problems.” (Doc. 96-4 at 11.) In response, the applicant discussed the  
17 problem with existing solutions:

18 [P]rior to the present invention, a *single computer architecture*  
19 solution that simultaneously stored all of the data, quickly  
20 verified the integrity of all of the data (i.e.: could produce a  
21 legal audit trail for regulators that proved that the data had not  
22 been altered), yet also permit both data subjects and 3rd parties  
23 to access the data, while still automatically protecting the data  
24 privacy rights of the data subjects from the 3rd parties had not  
25 been achieved. Instead, *existing computer “solutions” were*  
26 *both slow in operation and vulnerable to hacker attacks* that  
27 could compromise data privacy.

28 (*Id.* at 12 (emphasis in original).) The applicant then explained why the present invention  
solved those problems:

Importantly, as the data is being tossed into the data lake, the  
present system simultaneously generates a legally auditable  
record of the data in the data lake. The advantage of the present  
approach (i.e.: simply tossing all of the raw data into a data  
lake while simultaneously generating an auditable record of the  
integrity of this data – all within a single computer architecture)



1           has not been attempted prior to the present invention. The  
2           present novel architecture provides substantially *increased*  
3           *speed*, greatly *increased security* while using *far less*  
4           *computer resources* as compared to existing computer  
5           systems.

6           (*Id.* at 13 (emphasis in original).)

7           Plaintiff offers expert testimony and a secondary dictionary definition to argue that  
8           persons of skill in the art of computer science use the term simultaneously differently than  
9           its commonly understood meaning. (Doc. 94 at 31.) Specifically, Plaintiff’s expert testified  
10          at the hearing that time is not a relevant factor in “simultaneous sequences” in computer  
11          science. As an example, Plaintiff’s expert explained that, to a person of ordinary skill in  
12          the art, “simultaneous equations” means that two or more equations are necessary to solve  
13          a math problem, but they are not necessarily solved at the same time. Defendants, on the  
14          other hand, offer a primary definition for the word simultaneously arguing that the term  
15          refers to events happening at the same time. (Doc. 96 at 41.)

16          The Court finds that no construction is necessary in this case because the plain and  
17          ordinary meaning of the term is clear. “Simultaneously” is straightforward and readily  
18          understandable by lay juries, so it does not require further clarification. *See Phillips*, 415  
19          F.3d at 1314. Further, the applicant’s statements during prosecution regarding the  
20          advantage of speed over other inventions are directly related to the term “simultaneously”  
21          being added to the claims to secure a patent. (*See* Doc. 96-4 at 12-13.) These statements  
22          provide support that the applicant intended “simultaneously” to represent its commonly  
23          understood meaning related to events that occur at or near the same time. *Phillips*, 415 F.3d  
24          at 1317 (“[T]he prosecution history can often inform the meaning of the claim language by  
25          demonstrating how the inventor understood the invention. . . .”) (citing *Vitronics*, 90 F.3d  
26          at 1582–83).

27          Plaintiff fails to explain how its preferred construction, relying on an unsupported  
28          term of art, can be reconciled with the speed advantages touted during prosecution.  
29          Plaintiff’s expert also relied on a definition for “simultaneous equations” at the hearing,



1 which is a phrase not found in the intrinsic record. At bottom, Plaintiff’s dictionary  
2 definitions and expert testimony are unsupported extrinsic evidence. *Philips*, 415 F.3d at  
3 1318 (“[C]onclusory, unsupported assertions by experts as to the definition of a claim term  
4 are not useful to a court.”). As such, the extrinsic evidence is “unlikely to result in a reliable  
5 interpretation of patent claim scope unless considered in the context of the intrinsic  
6 evidence.” *Id.* at 1318–19. Moreover, given that the intrinsic record supports the common  
7 usage of the word simultaneously, Defendants’ proposed construction is unnecessary.  
8 Thus, the Court adopts the plain and ordinary meaning of the term “simultaneously,” as  
9 used in claim 17.

10 **M. “private blockchain”**

11 Plaintiff proposes the following construction: “A distributed transaction ledger  
12 controlled by a central authority.” (Doc. 101-1 at 2.) Defendant proposes the following  
13 competing construction: “A blockchain system requiring a proof of complexity solution,  
14 where only preselected members can record transactions to the blockchain.” (*Id.*)

15 Dependent claim 19 recites “[t]he method of claim 17, further comprising: utilizing  
16 a private blockchain to verify the data in the immutable audit ledger.” (Doc. 94-1,  
17 12:24-26.) The specification describes using “a private or permissioned blockchain with a  
18 private field of miners (i.e.: a blockchain system in which anyone can read, but only pre-  
19 selected members can record transactions to the blockchain).” (*Id.* at 7:52-55.)  
20 Additionally, the specification uses the term “private” in four other contexts. (*See id.* at  
21 1:31-34 (“‘[P]ersonal data’ is any information relating to an individual, whether it relates  
22 to his or her private, professional, or public life.”); *id.* at 3:41-43 (“[A]uditors can view the  
23 compliance data without requiring access to any of the private information or  
24 systems. . . .”); *id.* at 4:16-22 (“[T]he present system can . . . still shield[] private  
25 information from public stakeholders.”); *id.* at 6:41-44 (“[The system] should provide a  
26 secure bridge of communication between the private network . . . and the public  
27 Internet.”).) In each instance, the specification clearly uses the term “private” to mean not  
28 public, which comports with the common usage of the word. Moreover, the parties do not

1 appear to dispute the meaning of “blockchain” itself, which is a term of art readily  
2 understood by a person of ordinary skill in the art. Such a person would presumably  
3 understand the difference between a public blockchain and a private blockchain.  
4 *Innova/Pure Water, Inc. v. Safari Water Filtration Systems, Inc.*, 381 F.3d 1111, 1116 (Fed.  
5 Cir. 2004) (“A court construing a patent claim seeks to accord a claim the meaning it would  
6 have to a person of ordinary skill in the art at the time of the invention.”).

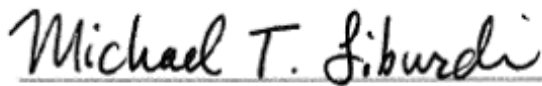
7 As discussed above with respect to “blockchain miners,” the Court does not find  
8 support in the intrinsic record to limit the invention to blockchain systems that only utilize  
9 proof of complexity solutions. For those same reasons, the Court rejects Defendants’  
10 proposed construction requiring “a blockchain system requiring a proof of complexity  
11 solution.” Moreover, claim 19, where private blockchain appears, is dependent on claim  
12 17. It follows, then, that the private blockchain of claim 19 already includes the limitations  
13 to claim 17 imposed via this Court’s construction of “blockchain miners” above. *See* 35  
14 U.S.C. § 112(d) (a dependent claim does not recite the elements of the referenced  
15 independent claim but is construed to incorporate all the limitations of that claim).

16 Thus, the Court adopts the plain and ordinary meaning of the term “private  
17 blockchain.”

18 **IV. CONCLUSION**

19 For the foregoing reasons, the Court construes the disputed claim terms as set forth  
20 in the table above in Part III, *supra*.

21 Dated this 3rd day of February, 2023.

22  
23 

24 

---

Michael T. Liburdi  
25 United States District Judge  
26  
27  
28