

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

JPMorgan Chase Bank, N.A.
Petitioner

v.

Identitii Limited
Patent Owner

Case IPR2024-00590
U.S. Patent 10,984,413

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I.	Introduction.....	1
II.	The Parties	4
III.	The '413 Patent.....	5
	A. Person of Ordinary Skill in the Art (POSITA)	15
IV.	Summaries of the Asserted References	16
	A. Smith (EX1004)	16
	B. Seger (EX1005).....	20
V.	The Petition fails to demonstrate a reasonable likelihood that The Challenged claims would have been obvious.....	21
	A. The proposed combination would not have rendered obvious a “first intermediary server.”	23
	1. The concept of an “intermediary” server in processing financial transactions.	23
	2. The proposed combination does not teach or suggest the claimed “first intermediary server.”.....	26
	B. The proposed combination would not have rendered obvious “a first intermediary server in a centralised financial system.”	28
	C. The proposed combination would not have rendered obvious “generate/generating an enriched data record from the one or more documents.”	31
	D. The proposed combination would not have rendered obvious the claimed “token.”	38
	E. The proposed combination would not have rendered obvious “requesting generation of a token corresponding to the financial transaction”	41
	F. It would not have been obvious to combine Smith and Seger as proposed.	44

1.	Smith and Seger are directed to two different types of “verification.”	47
2.	The proposed combination is less secure, and Smith teaches away from the less secure system.	50
3.	The combination would frustrate a key purpose of Smith by allowing other parties, such as unaffiliated businesses, to add information to the blockchain.	51
4.	Smith and Seger are in different fields.	52
5.	Petitioner’s motivations to combine fail.	52
VI.	Grounds 2 and 3 fail	55
VII.	Conclusion	55

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Callicrate v. Wadsworth Mfg., Inc.</i> , 427 F.3d 1361 (Fed. Cir. 2005)	43
<i>Seabery N. Am., Inc. v. Lincoln Global, Inc.</i> , IPR2016-00749 (Sept. 21, 2016)	54
<i>SIMO Holdings Inc. v. Hong Kong uCloudlink Network Tech. Ltd.</i> , 983 F.3d 1367 (Fed. Cir. 2021)	23
<i>Unique Concepts, Inc. v. Brown</i> , 939 F.2d 1558 (Fed. Cir. 1991)	43
<i>Virtek Vision Int'l ULC v. Assembly Guidance Sys., Inc.</i> , 97 F.4th 882 (Fed. Cir. 2024)	55
<i>William Wesley Carnes, Sr., Inc. v. Seaboard Int'l Inc.</i> , IPR2019-00133 (May 8, 2019)	54
<i>Xerox Corp. v. Bytemark</i> , IPR2022-00624 (PTAB Feb. 10, 2023)	28, 31

Statutes

22 U.S.C. § 2214(a)(8)	26
------------------------------	----

PATENT OWNER'S APPENDIX OF EXHIBITS

Exhibit	Description
EX2001	Declaration of Dr. James L. Olivier (“Olivier Dec.”)
EX2002	Dr. James L. Olivier Curriculum Vitae
EX2003	Website Printout entitled “About Us Onyx by J.P.Morgan,” available at https://www.jpmorgan.com/onyx/about
EX2004	Non-Final Office action to U.S. Patent Application No. 15/797,602, dated October 22, 2020
EX2005	Website Printout entitled “Onyx by J.P.Morgan,” available at https://www.jpmorgan.com/onyx/index.htm
EX2006	Quinlan & Associates, ‘From KYC To KYT: Blockchain’s Emerging Role In The Global Payments System’, November 2016, available at: https://www.quinlanandassociates.com/insights-from-kyc-to-kyt/
EX2007	Website Printout entitled “Financial Intermediary: What It Means, How It Works, Examples,” available at https://www.investopedia.com/terms/f/financialintermediary.asp
EX2008	Website Printout entitled “Financial Intermediary - How it Works, Defined, Example,” available at https://corporatefinanceinstitute.com/resources/economics/financial-intermediary-transactions/
EX2009	Website Printout entitled “Innotribe Swift,” available at https://www.swift.com/about-us/innovate-swift/innotribe
EX2010	Website Printout entitled “Rising to the challenge Swift,” available at https://www.swift.com/news-events/news/rising-challenge
EX2011	Innotribe Industry Challenge Presentation Agenda and Presenters, dated July 6-7.

Exhibit	Description
EX2012	“Blockchain as a Public Ledger and Means of Exchange: Policy Considerations” Madeline J. Diab, Seton Hall Law 2023

I. INTRODUCTION

The Board should deny institution of *inter partes* review of U.S. Patent No. 10,984,413 (the “’413 patent”) because Petitioner fails to demonstrate a reasonable likelihood that any challenged claim would have been obvious.

The inventors of the ’413 patent foresaw what would become significant drawbacks to traditional banking payment rails such as SWIFT. To process a financial transaction using traditional payment rails, an intermediary, such as a buyer’s financial institution, communicates a fixed message to another financial intermediary, such as a seller’s financial institution. Often times, the message passes through multiple intermediaries. These fixed messages could only send set, specific information in a one-way communication. With the rise of differing regulatory requirements, the static information became insufficient, and it was difficult, if not nearly impossible for intermediaries to confirm or gather additional information to complete the processing of a financial transaction efficiently.

However, replacing traditional payment rails, used by most financial institutions in the world, was not, and is not, feasible. The inventors therefore invented a system to work in conjunction with and serve as an overlay to traditional payment rails. In the new system of the ’413 patent, an intermediary server generates an enriched data record, which can include not only the static information of a traditional payment message, but any additional information necessary for

completing the financial transaction, such as information required for anti-money laundering regulations. The information is included in a newly generated, enriched data record that is placed on a blockchain, which can be accessed by financial institutions at any point while processing the transaction by using a pointer to the information. Patent Owner's invention has enjoyed great success, including awards and industry recognition. Indeed, Petitioner has implemented the inventions of the '413 patent and has recently touted the implementation as "[t]ransforming the future of banking." EX2003.

Petitioner's proposed combination here fails to demonstrate any reasonable expectation that the claims would have been obvious. Petitioner's primary reference, Smith, is not directed to processing transactions between intermediaries via traditional payment rails. Instead, Smith is directed to verifying information of a transaction *before* submitting the transaction via traditional payment rails. Specifically, Smith discloses communications between a "business," a transacting entity such as a merchant, and a "third-party payment processor" ("TPPP"). The "business" passes along information such as licensing and identification information to the TPPP. The TPPP verifies the information (e.g., by confirming business licensing information with a state agency). After verification, the TPPP submits the transaction for processing using traditional methods and traditional payment rails.

Smith's idea (pre-verification before processing) ends before the '413 patent's novel architecture begins (the processing of the financial transaction).

As Smith is in a different context, dealing with different problems than the '413 patent, it fails to teach or suggest numerous claim elements. Attempting to cure one of the deficiencies—Smith's lack of a blockchain—Petitioner proposes to combine Smith with Seger. However, the proposed combination only creates more problems under Petitioner's theories. While Seger discloses a blockchain, it makes no sense to combine it with Smith as Petitioner proposes. Indeed, Petitioner and its expert never explain how, specifically, the two references could be combined. Instead, Petitioner identifies some generic "motivations" to combine, but in considering the purported motivations at anything more than a superficial level, it becomes apparent that a POSITA would not have combined Smith and Seger, as it results in a less secure and more complicated system that frustrates the purpose of Smith's system.

Because there is no reasonable expectation of success, the Petition must fail.

II. THE PARTIES

United States Patent No. 10,984,413 issued on April 20, 2021, to Patent Owner Identitii Limited.¹ Identitii is a publicly-held Australian entity that develops and licenses enterprise solutions and software for regulated entities. Identitii offers products and platforms to financial entities in the United States, Australia, and Asia. The products allow entities to comply with financial regulations while leveraging the entities' current technology systems.

After filing a patent application for the technology of the '413 patent, Identitii approached Petitioner, who was interested in learning about Identitii's technology. Identitii confidentially provided Petitioner information about its innovative technology. Rather than taking a license after receiving the confidential information, Petitioner filed its own patent applications and began offering its own product. Petitioner's patent applications were rejected in view of Identitii's published patent application. *See, e.g.*, EX2004, 8 (rejecting Petitioner's claims in view of the pre-issuance publication of the '413 patent).

Petitioner, who uses Patent Owner's technology, has recognized the novel architecture of the '413 patent. For example, years after the conception of the '413

¹ The '413 patent was assigned to Identitii Pty Limited, which changed its name to Identitii Limited.

patent, Petitioner advertises that its practicing product “is at the forefront of a major shift in the financial services industry ... by “offer[ing] a blockchain-based platform for wholesale payments transactions, helping to re-architect the way that money, information and assets are moving around the world.” EX2003. To this day, Petitioner publicly admits that such a system, using “blockchain innovation,” is a “re-architected ... infrastructure ... [that] unlock[s] the potential of distributed ledger technology.” EX2003. Therefore, Petitioner’s assertion here that the ’413 patent merely “takes conventional financial transactions and records them on a generic blockchain,” (Pet., 1) is not only incorrect technically, but the assertion is also incredible in view of Petitioner’s public pronouncements outside the context of this dispute.

III. THE ’413 PATENT

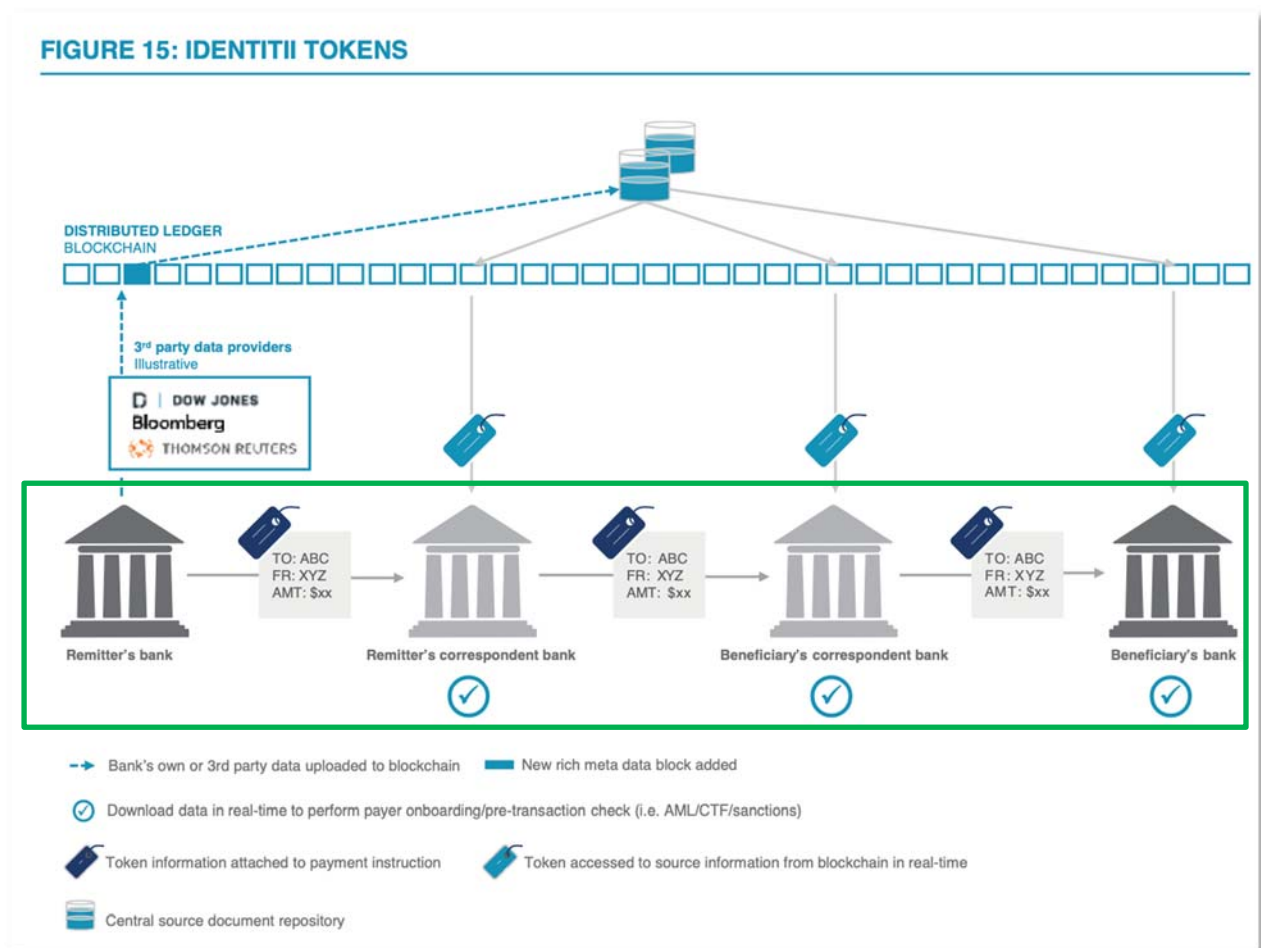
The ’413 patent relates to improved methods and systems for solving growing regulatory compliance issues in processing financial transactions. Particularly, the ’413 solves problems of the conventional banking infrastructure and payment rails, such as SWIFT, by introducing a new infrastructure that overlays conventional payment rails. The ’413 patent allows financial intermediaries that are processing financial transactions to utilize conventional payment rails while also allowing them to comply with growing, and changing, regulatory requirements to more efficiently reconcile financial transactions.

At the time of the invention of the '413 patent, existing technology and infrastructure for executing financial transactions between financial intermediaries, such as banks and brokerage firms, suffered from numerous problems. For example, the Society for Worldwide Interbank Financial Telecommunications (SWIFT)² was (and still is) the main network for executing financial transactions between banks around the globe, including across borders of countries having various governmental regulatory requirements. SWIFT provides one of the largest worldwide financial messaging systems for financial institutions to send and receive information to support global payment orders. A key characteristic of conventional payment rails, such as SWIFT, is standardized messaging and a relatively secure network. EX2001 ("Olivier Dec."), ¶ 33; EX2006, 22, 35. However, the standardized messaging in conventional payment rails did not allow for including information in addition to that for the standardized, fixed length messages. EX1001, 26:1-2. As such, conventional messages lack flexibility and fail to include information required for ongoing and everchanging regulatory developments, e.g., to enforce sanctions or combat money laundering, fraud, and financing of terrorism, which require sanctions screening, address proof, or other additional information to comply with government

² Other existing networks include Automated Clearing House (ACH) and Real Time Gross Settlement (RTGS). EX1001, 26:49.

regulations, such as “know your customer” (“KYC”). EX1001, 12:31-39; 13:48-60.

Another drawback of conventional payment rails and messaging, such as SWIFT messaging, is that the conventional systems “are characterised by effective one-way transmission.” EX1001, 1:44-51. This is illustrated, for example, in the image below:



EX2006, 34 (annotated)

As shown in the annotated in the green square, a fixed message travels one-way through multiple financial intermediaries (e.g., from Remitter's bank to

Remitter's correspondent bank to Beneficiary's correspondent bank to Beneficiary's bank). A drawback of this one-way transmission of fixed data is that if there are deficiencies in the data being transmitted or if more data is required to process the transaction, there was no support in the network architecture for communicating, confirming, or requesting additional data. EX1001, 1:44-51. Instead, the transaction simply failed or required manual "time consuming checking and querying operations and correspondence" outside the conventional payment messaging network before a financial transaction can be effected. *Id.*, 26:46-62. This issue was exacerbated by growing and changing regulatory requirements of numerous agencies of various governments.

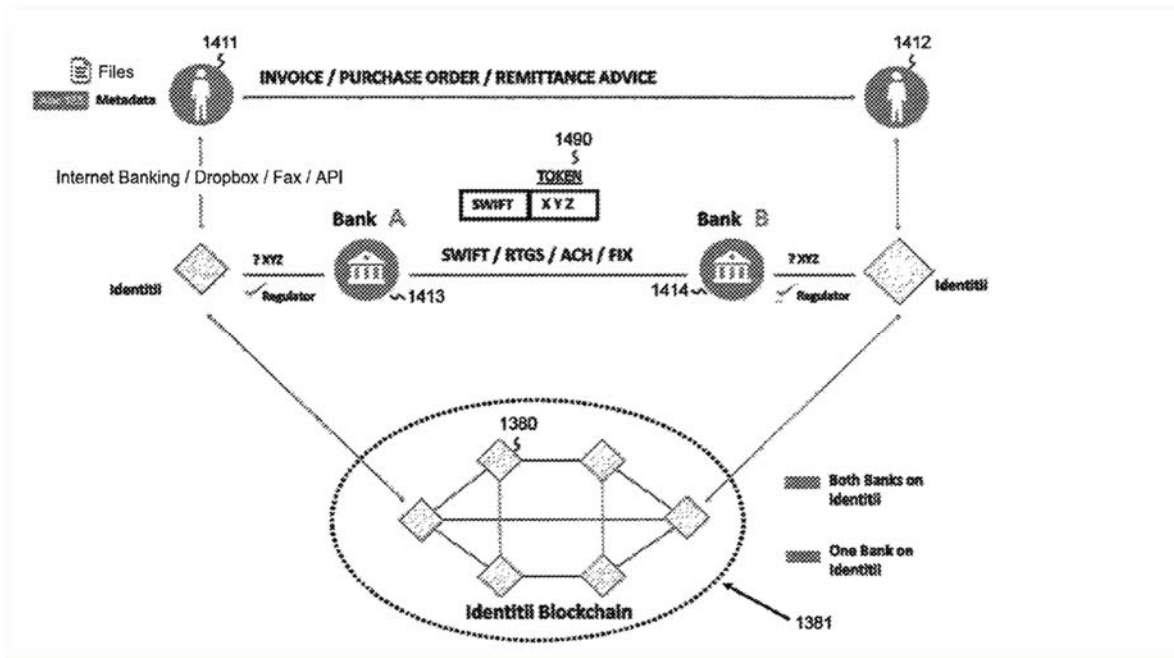
Identitii reimagined an architecture to eliminate these problems of the conventional payment rail infrastructure. At the time of the invention, the inventors envisioned using blockchain technology that overlaid the traditional architecture of global payment systems to support real-time, two-way communication to ensure the integrity and validation of the data at any point during and after the financial transaction. EX1001, 3:32-33; 13:44-14:4; 14:53-15:7; 19:11-39; 23:1-5; 23: 45-65; 24:21-27; 26:46-62; 31:46-50. Blockchain is a type of distributed ledger database that records and maintains a constantly growing list of transactions in sequential blocks. As a result, those with access to the network have shared access to information in the blockchain. *Id.*, 12:65-13:8; 25:14-46; Fig. 15.

Identitii's novel architecture generates an enriched data record from one or more documents of a financial transaction as described, for example, in claim 15. As the inventors recognized, processing transactions often requires far more underlying information than simply, for example, information in a standardized SWIFT message. EX1001, 26:34-38 ("the additional information is to enrich payments with more information given the inability of existing payment systems to communicate enriched information."); 28:46 ("the existing financial messaging systems allow only specific information to be attached to the financial transaction."); 12:19-48. Many transactions require regulatory documents, including sanctions screening results, purpose of payments, and other types of documents required to comply with government regulations. *Id.*, 12:31-48. As the '413 patent described, the new architecture generates the enriched data record from one or more documents by "extract[ing] a plurality of attributes from the one or more documents" and "combin[ing] the plurality of attributes to generate the enriched data record." *Id.*, 12:15-18; 12:46-53. In addition, the architecture may de-identify and/or hash the attributes in generating the enriched data record. *Id.*, 12:53-64. The enriched data record thus can include information that may be pulled from underlying documents.

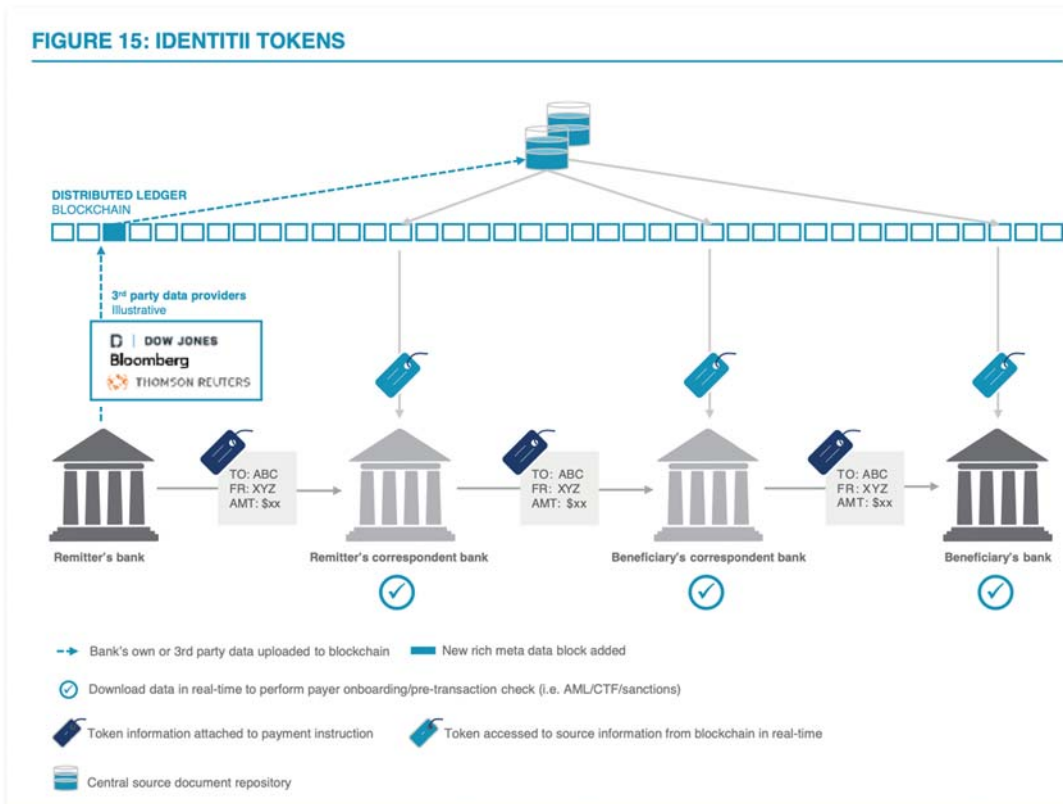
Identitii's new architecture further uses a token associated with the enriched data record stored in the blockchain, regardless of the legacy system being used, to create a full data payment record containing all the data required to settle the

financial transaction. EX1001, 22:50-67; 26:46-62. “The token provides a pointer to the enriched data record.” *Id.*, 28:66-29:1. “The token can be included in all the financial messages sent between a plurality of financial intermediaries, and the token can be used by any of the plurality of intermediaries to verify the financial transaction from the enriched data record, before taking any further steps in the process.” *Id.*, 31:38-45. The token may be included in conventional messaging, such as SWIFT messages between banks, bank branches, other financial institutions, or other entities, making this “interoperability” a unique feature of the ’413 patent as well. *Id.*, 25:1-13. And each entity may utilize the token to access additional data for the transaction that could not be communicated using traditional payment rails. *Id.*, 31:38-45.

The enriched data record and its associated token is added to and stored in a blockchain as described in, e.g., claim 15 and illustrated in the images below:



EX1001, Fig. 14



EX2006, 34

As illustrated, a Remitter and a Beneficiary enter into a transaction. Intermediary entities in the transaction process have real-time access to the blockchain and the information stored thereon—and thus an enriched data record that includes information for the transaction can be retrieved and audited/verified at any time when queried with the token.

The structure of Identitii's new architecture is described in the '413 patent's specification and is embodied in claim 15 of the '413 patent:

15. A system for processing a financial transaction, the system comprising:
a first intermediary server in a centralized financial system, the first intermediary server being operably connected to a network and a first document store;
a token server operably connected to the network;
a messaging bus in the centralized financial system, the messaging bus being operably connected to the network; and
a blockchain operably connected to the network, the blockchain being a distributed ledger;
wherein the first intermediary server is configured to:
transmit one or more documents pertaining to the financial transaction, to the first document store;
generate an enriched data record from the one or more documents and add the enriched data record into the blockchain;
request generation of a token corresponding to the financial transaction to identify the one or more documents, to the token

server, via the messaging bus; and
transmit the token to the first document store;
wherein the token server is configured to:
generate the token and add the token into the blockchain in
association with the enriched data record; and
transmit the token to the first intermediary server, via the
messaging bus.

In accordance with the claimed invention, Identitii invented a server-system that generates an enriched data record from documents regarding a financial transaction and that enriched data record is inserted on a blockchain. Additional information is used to enrich payments with more information given the inability of existing payment systems such as SWIFT to communicate enriched information. EX1001, 26:34-38. The system also has a token server [which] generates a token associated with the enriched data record and that token is stored in the blockchain in association with the enriched data record. *Id.*, 13:9-14. The token provides a pointer to the enriched data record in the blockchain and can be used to retrieve the enriched data record at, for example, the time of an audit. *Id.*, 2:12-15; 16:1-3; 22:45-57; 22:61-67; 23:19-29; 23:66-24:2; 28:66-29:7. The system leverages blockchain and tokenization technology to create an unconventional architecture that is a departure from prior architectures like SWIFT.

With the invention of the '413 patent, financial intermediaries can now transmit, receive, and confirm sensitive banking information securely and without any need to contact other entities or access the internal data stores of those entities. Instead, the processing entities can gather the information using the tokens and enriched data records by directly accessing the blockchain. The financial institutions involved in the transaction may communicate in real-time and ensure, for example, that the payer, the beneficiary and all the parameters corresponding to the financial transaction are validated. EX1001, 31:46-50.

Identitii's new architecture, which includes, inter alia, an enriched data record, a token, and a blockchain provides a robust information overlay over existing payment systems like SWIFT to enrich payments with supporting information that is accessible at each step of the payment process, enabling banks to clear transactions more quickly and reliably. EX1001, 25:2-7; 26:46-62; 28:44-60.

Petitioner states that "[t]he '413 Patent takes conventional financial transactions and records them on a generic blockchain." Pet., 1. This is incorrect. Instead, as discussed, the '413 patent describes a new overlay over existing architecture for "conventional financial" payment systems to improve electronic payment processing. JPMC's mischaracterization dooms the Petition, as it results in numerous failures with respect to the independent claims alone.

Indeed, in addition to Petitioner's recognition of the technological

advancements of the '413 patent, the industry as a whole has likewise recognized Patent Owner's novel architecture. For example, SWIFT itself acknowledged the innovation by selecting Patent Owner as the winner of the 2016 SWIFT Innotribe³ Compliance Challenge based on Patent Owner's new patented architecture. EX2006 at 33; EX2010; EX2011.

A. Person of Ordinary Skill in the Art (POSITA)

Petitioner and its expert state that a POSITA “would have at least a bachelor's degree in computer science, computer engineering, applied mathematics, or equivalent and at least 2 years of experience researching, implementing, programming, or designing computer networks, distributed systems, blockchain technology, applied cryptography, or security. Additional education can supplement practical experience, and vice-versa.” Pet., 6. For purposes of this POPR, Patent Owner and its expert apply this definition, as the Petition fails under any definition of a POSITA. See Olivier Dec., ¶ 31.

Petitioner's expert also notes that a POSITA would have familiarity with “concepts and developments in the areas of ... payment networks.” EX1003, ¶ 21. However, Petitioner has not alleged or shown that Dr. Shen has any such experience. See *generally* EX1003, ¶¶ 4-10; EX1036. Dr. Shen's lack of familiarity with these

³ Innotribe is SWIFT's innovation arm. EX2009.

concepts is highlighted by a significant failure in the Petition, where Petitioner and its expert fail to recognize the meaning of the claimed “intermediary” to a financial transaction.

IV. SUMMARIES OF THE ASSERTED REFERENCES

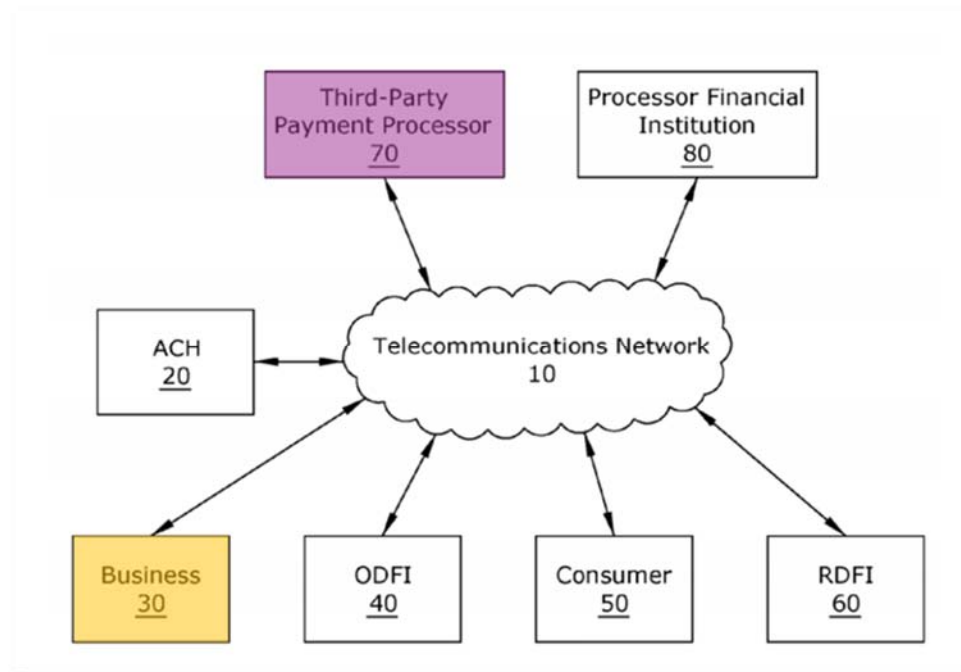
A. Smith (EX1004)

U.S. Pub. 2015/0081553 by Smith (EX1004, “Smith”) discloses functionality of what happens *before* banks or other financial institutions process payments using traditional payment rails. Smith is related to a third-party payment processor, such as PayPal, verifying payment authorization before the financial transaction is processed using conventional messaging and payment rails, such as ACH. EX1004, ¶ 11.

As Smith describes, “[c]onsumers who choose ACH payment must first authorize the business to debit or credit their financial account for a financial amount.” *Id.* “The consumer authorization must conform to the requirements of the ACH Operating Rules . . . and must be either written and signed, or electronically displayed.” *Id.* When the third-party processor is used in ACH transactions, it “receives the ACH payment information from the business and then submits the ACH payment information to an originating depository financial institution (ODFI).” *Id.* Smith then recognizes that the originating bank processes the ACH transaction using conventional payment messaging. *Id.*

Smith disclosed that before sending a transaction to an originating bank for processing, the third-party processor should verify that the transaction was authorized, including determining that a consumer authorized the transaction in accordance with rules (e.g., by a signature or other identification such as a driver's license) and that the business is authorized to do business in a state. *Id.*, ¶11, 13, 34.

Smith describes a “business” that communicates with a third-party payment processor, “TPPP” via a network.



EX1004, Fig. 1 (annotated by Petitioner)

“The business 30 sends one or more transaction data files to the third-party payment processor 70 such as a copy of a state license, a signature of the consumer 50, an ACH authorization by the consumer 50, a copy of an agreement with the consumer 50, and a copy of a driver's license or other identification for the consumer

50.” *Id.*, ¶ 52. The business also sends an ACH record to the TPPP. *Id.*, ¶ 54. The TPPP uses the transaction data files to verify the transaction is authorized: by verifying the business’s license with a state agency and verifying the consumer’s identity with a “consumer ID and address validation network.” *Id.*, ¶¶ 53, 65. That is, the TPPP verifies that accuracy of the data (not that the data is unchanged). Olivier Dec., ¶¶ 64-65. Smith’s TPPP stores this information within its own internal database that it, alone, controls and maintains. EX1003, ¶ 77; *see also* EX1004, ¶ 53 (the TPPP adds the ACH request, the transaction files from the business, and transaction files from the state agency to its own database).

In storing the information, the TPPP also includes a “transaction key” for identifying the stored information for the transaction. *Id.*, ¶¶ 54-56. The transaction key can be used to identify the information on the database. *Id.* Figure 5 shows “a database table for a database used by the third-party payment processor”:

Transaction Key	ACH Transaction Detail Record	Transaction Data File(s)
ABCD1	Detail Record #1	-ACH Authorization File
ABCD2	Detail Record #2	-ACH Authorization File -Drivers License File -Social Security Card File
ABCD3	Detail Record #3	-ACH Authorization File -Business State Licenses File
ABCD4	Detail Record #4	-ACH Authorization File

EX1004, Fig. 5

As shown, the TPPP receives and stores “transaction data files,” which are image files such as a copy of state license, driver’s license, etc. (*id.*, ¶ 44) and “ACH Transaction Detail Record,” which is a conventional ACH message (*id.*, ¶¶ 43-47). The stored information can be identified using a transaction key.

As Petitioner admits, there is no blockchain in Smith’s system. Nor would it have been obvious to modify Smith to add one: the TPPP receives all data and maintains and updates that data in its own internal and secure database. In fact, Smith teaches that the database should be a PCI level 1 environment that “maintains the highest level of compliance and encryption.” *Id.*, ¶ 59. There is no reason to open up the internal, secure database to the outside using a blockchain—allowing others to add and retrieve data—making the system less secure.

B. Seger (EX1005)

As Smith does not disclose a blockchain, Petitioner adds U.S. Patent No. 9,397,985 to Seger (EX1005, “Seger”). While Petitioner relies on Seger to tout the benefits of a blockchain generally, the benefits would not apply to the proposed combination with Smith. In fact, a POSITA would have recognized the detriment of adding Seger’s blockchain to Smith. Olivier Dec., ¶¶ 45-46.

Seger recognizes that parties may communicate electronically via email, SMS, or direct messages, but that those the communications are “not recorded in a log that can be audited after the fact by a third-party.” EX1005, 1:16-21. Seger therefore proposed placing “information transactions” containing the communications on a blockchain. *Id.*, 5:7-14. Seger explains that the distributed ledger may be immutable. *Id.*, 10:19-23. That is, the information cannot be modified. Olivier Dec., ¶ 65. Because the ledger is immutable, it “may provide a verifiable record of all the information exchanges.” *Id.*

Petitioner latches onto the use of the word “verified” in both Smith and Seger as the primary reason to combine the two references. Pet., 21-22. However, Smith provides a different verification than Seger. In Smith, as discussed above, the TPPP receives, maintains, and stores the information: knows when it receives the information and when/how/if it was modified. Smith verifies that the data is *correct* by, e.g., confirming with a state agency that a business’s state license is not

fraudulent and matching account numbers to entities. EX1004, ¶¶ 53, 59. Seger, on the other hand, does not verify that the underlying information of the data is true and correct; it instead uses a blockchain to “verify” that information on the blockchain is unmodified. EX1005, 10:19-23.

V. THE PETITION FAILS TO DEMONSTRATE A REASONABLE LIKELIHOOD THAT THE CHALLENGED CLAIMS WOULD HAVE BEEN OBVIOUS.

The Petition presents three obviousness grounds. In ground 1, Petitioner challenges claims 1-2 and 5-20 as obvious over Smith in view of Seger. Pet., 3. For ground two, Petitioner challenges claim 3 by adding Yago to the Smith/Seger combination. *Id.* For ground three, Petitioner challenges claim 4 by adding Kurani-274 to the Smith/Seger combination. *Id.*

All of Petitioner’s grounds fail to demonstrate a reasonable likelihood that the challenged claims would have been obvious.

Even if it would have been obvious to combine Smith and Seger, the table below highlights the limitations of claim 1 that are missing, completely, from the proposed Smith/Seger combination. These limitations are present in all independent claims (i.e., claims 1, 15, and 16).

Claim 1
Preamble: A computer implemented method for processing a financial transaction, the method comprising the steps of:

Element 1: transmitting one or more documents pertaining to the financial transaction, from a first intermediary server in a centralised financial system to a first document store;
Element 2: generating an enriched data record from the one or more documents , at the first intermediary server , and adding the enriched data record into a blockchain being a distributed ledger, from the first intermediary server ;
Element 3: requesting generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, from the first intermediary server , via a messaging bus in the centralised financial system;
Element 4: generating the token at the token server and adding the token into the blockchain from the token server in association with the enriched data record ;
Element 5: transmitting the token to the first intermediary server from the token server, via the messaging bus; and
Element 6: transmitting the token from the first intermediary server to the first document store in association with the one or more documents.

Further, in addition to the missing limitations above, it would not have been obvious to modify Smith in view of Seger to include multiple additional limitations. The Petition fails.

A. The proposed combination would not have rendered obvious a “first intermediary server.”

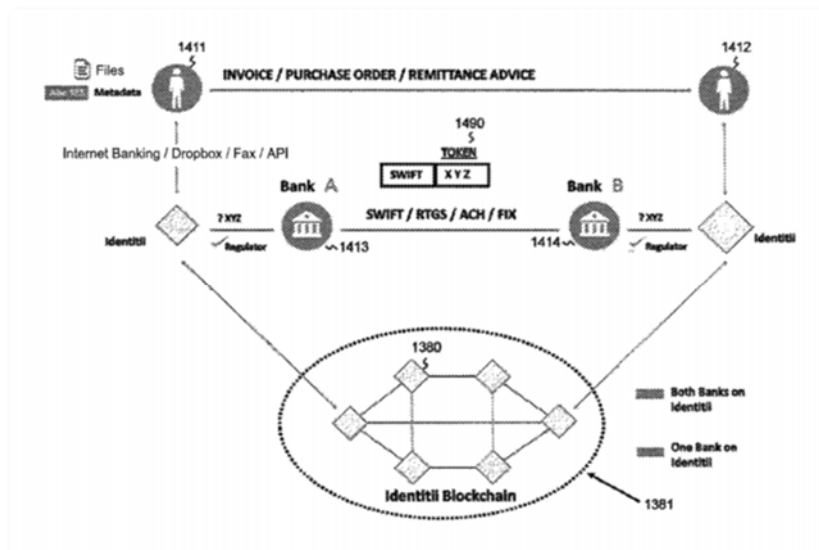
Every claim of the '413 patent requires a “first intermediary server.” EX1001, claims 1, 15-16.⁴ As Petitioner’s expert has no experience with payment networks or financial transaction processing, he fails to recognize the concept of an intermediary, despite the concept being explained in the specification of the '413 patent. As the proposed combination does not teach or suggest the claimed first “intermediary server,” the Petition fails to present any reasonable expectation of success.

1. The concept of an “intermediary” server in processing financial transactions.

The '413 patent explains that a financial transaction occurs between two or more “transacting entities.” EX1001, 22:35-44 (a “first transacting entity 911 which enters into a financial transaction with at least a second transaction entity 912.”). An intermediary entity, on the other hand, is an entity that facilitates the processing of a financial transaction: processing the financial transaction may require transferring

⁴ The term is recited in the limiting preamble of claim 16. The preamble is limiting, as it provides structure for the claim and antecedent basis for numerous terms. *See, e.g., SIMO Holdings Inc. v. Hong Kong uCloudlink Network Tech. Ltd.*, 983 F.3d 1367, 1375 (Fed. Cir. 2021).

and processing of information not directly between the transacting entity, but through non-transacting entities “in the middle,” which can include one or more banks. As an example, the ’413 patent describes that the first and second transacting entities “are associated with a respective first intermediary entity 913 and a second intermediary entity 914 in the form of bank A and bank B. Each of the first transacting entity 911 and a second transacting entity 912 has a respective account ... at their respective intermediary entities.” *Id.* This basic financial concept is illustrated in Figure 14:



EX1001, Fig. 14

Transacting entities 1411 and 1412 (*see* EX1001, 25:59) transmit an invoice, purchase order, and remittance advice. Non-transacting intermediaries, entities between the transacting entities for processing the transaction, then process the transfer of funds. As shown in Figure 14, for example, an intermediary Bank A sends

a message on a traditional payment rail (e.g., SWIFT) to an intermediary Bank B. The same concept is likewise illustrated in Figure 8A, which is a block diagram of the transacting entities and non-transacting intermediaries involved in a prior art electronic settlement system.



EX1001, Fig. 8A

As shown, the “intermediaries,” banks in this case, are not parties to the transaction, but are between the transacting entities for purposes of processing the financial transaction: transacting Entity A sends information to intermediary Bank A, which sends it to intermediary Bank B, resulting in payment to transacting Entity B.

The '413 patent also makes clear that an “intermediary server” is, unsurprisingly, a server of an intermediary. In the embodiments, the '413 patent describes the intermediary entities as banks that are not part of the transaction and, describes, an “intermediary server” as representing a “financial institution,” such as banks, bank branches, commercial banks, investment banks, brokerage, investment companies etc. *Id.*, 10:56-11:5.

The '413 patent uses the term “intermediary” consistently in the context of financial transactions as it is understood in the field. EX2007 (“financial intermediary is an entity that acts as the middleman between two parties in a

financial transaction, such as a commercial bank, investment bank, mutual fund, or pension fund.”); EX2008 (“[A]n institution that acts as a middleman between two parties to facilitate a financial transaction”) *see also* Olivier Dec., ¶¶ 77-81. Indeed, the concept of a financial intermediary is recognized by federal statute, where it is described as an “entity that acts as the intermediary between parties in a financial transaction” 22 U.S.C. § 2214(a)(8).

2. The proposed combination does not teach or suggest the claimed “first intermediary server.”

Petitioner alleges that Smith’s “computer for the business 30” discloses the “first intermediary server.” Pet., 13. But Smith’s “business” is not an intermediary; it is a transacting entity, as it transacts with a consumer. Indeed, Smith discloses that its system is for “**business to consumer transactions.**” EX1004, ¶ 12 (emphasis added); *see also id.*, ¶ 34 (“[t]he consumer 50 may be any individual or legal entity that is authorizing an ACH transaction with business 30.”), ¶ 44 (“Each ACH detail record corresponds to an ACH transaction for the business”). Smith discloses that the business may be comprised of various entities “including, but not limited to, merchants, online retailers, financial institutions, banks, credit unions or payday lenders” all of which enter into transactions with a consumer. *Id.*, ¶ 35. Regardless of the type of entity represented by Smith’s business, Smith is clear that its “business” is a transacting entity, and there is no teaching or suggestion of the

business being a non-transacting entity that facilitates the processing of the transaction of two transacting entities. Olivier, Dec., ¶ 84; EX1004, ¶¶ 12, 24, 44.

Smith's system may include intermediaries in the form of the originating depository financial institution (ODFI), "the financial institution for the business," and the receiving depository financial institution (RFDI), "the financial institution for the consumer." *Id.*, ¶ 37. However, Smith does not teach or suggest—and Petitioner does not allege—that any server of any intermediary in Smith practices the claimed requirements of the "first intermediary server." As such, the Petition fails.

Petitioner argues that the "business computer" is an "intermediary between other devices" or an intermediary between "a user on the business side" and the verification system. Pet., 15. Petitioner never identifies what "other devices" the business computer is between, or how. *See id.* The statement makes little sense in any context: it is the business that initiates the financial transaction—there are no "other devices" it is between. Olivier Dec., ¶¶ 85-86. Nor does a user using a server somehow transform the server into an intermediary server. *Id.*

Moreover, given the context of Smith, and the disclosures therein, it is even more clear that the "business computer" does not disclose or suggest the claimed "first intermediary server." The Petition simply fails to recognize that in a patent having "processing a financial transaction" in both the title and claim preambles, an

intermediary has a known and understood meaning; it is not just a network device that is between (somehow) “other devices.” Petitioner’s expert likewise fails to recognize this well-known term in the field of invention. Instead, he merely parrots the single sentence of the Petition, offering no reliable evidence that the proposed combination would have taught or suggest the claimed “first intermediary server.” See EX1003, ¶ 67; *Xerox Corp. v. Bytemark Inc.*, IPR2022-00624, Paper 12, at 2 (PTAB Feb. 10, 2023) (Director review designating institutional denial decision as precedential, where institution was denied when declaration merely parroted petition, “was conclusory and added little to the assertions the testimony was offered to support.”). Seger does not cure these deficiencies of Smith, and Petitioner makes no argument to the contrary.

This failure highlights the proposed Smith / Seger combination as a whole, as discussed below: because Smith’s business is a non-intermediary, non-trusted entity that does not perform verification, a POSITA would not allow the business to store, access, and add information to the trusted database of the independent third-party payment processor, as required by the proposed combination.

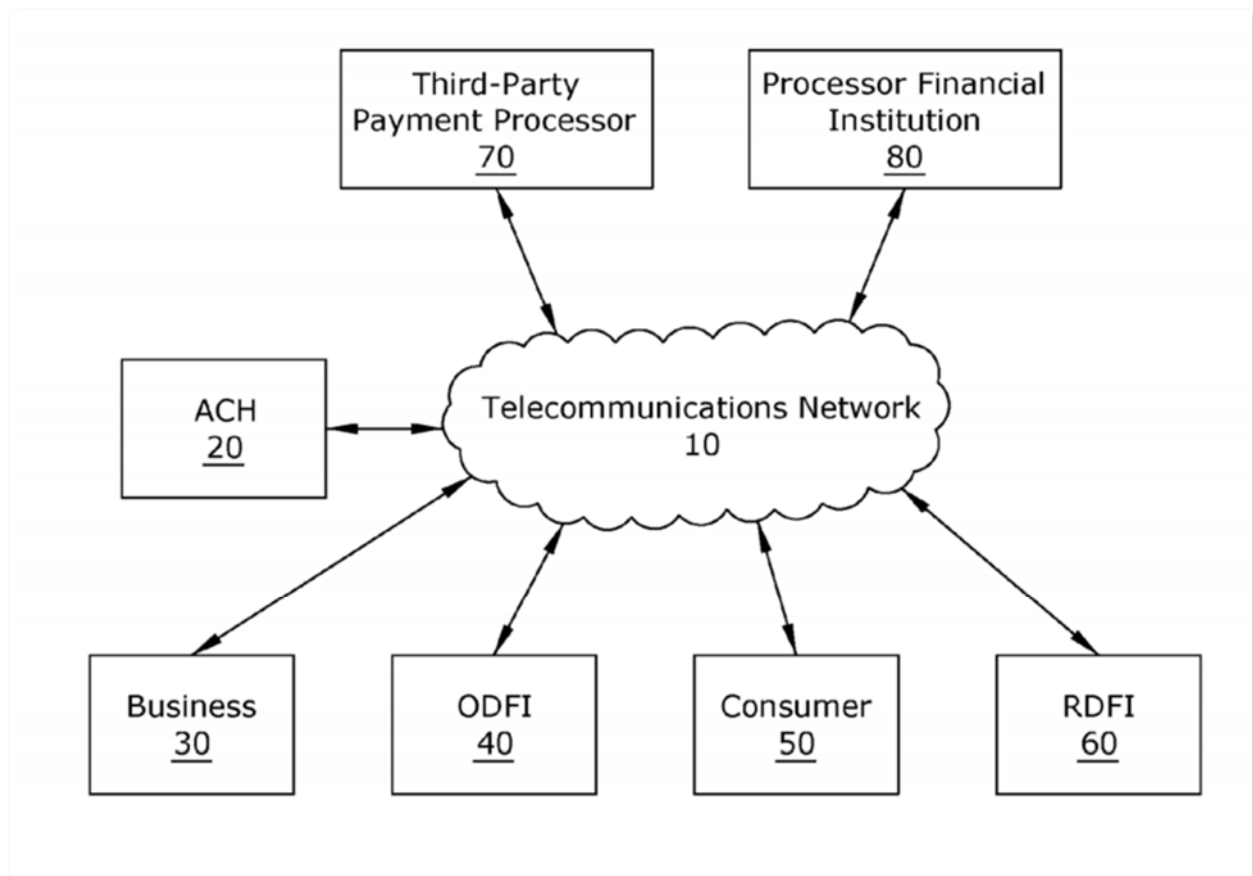
B. The proposed combination would not have rendered obvious “a first intermediary server in a centralised financial system.”

Each claim requires “a first intermediary server [in/for use in] *a centralised financial system.*” EX1001, claims 1, 15-16 (emphasis added). For this limitation,

Petitioner primarily addresses only the words “intermediary” and “server.” Pet., 14-16. Petitioner addresses the requirement of a “centralised financial system” in a single sentence, baldly stating that Smith’s “electronic funds transfer consumer authorization verification system” is a “centralised financial system.” Pet., 13. Petitioner offers no reason why Smith’s system is a “centralised financial system.” And while Petitioner does not rely on its expert for this limitation, Dr. Shen merely copies the lone sentence in the Petition verbatim, also with no explanation. EX1003, ¶ 63. Petitioner thus cannot show that the requirement of a first intermediary server in “a centralised financial system” would have been obvious.

Indeed, Smith’s “electronic funds transfer consumer authorization verification” system is not a “centralised” financial system. Olivier Dec., ¶¶ 89-93. As the patent describes, “centralised systems ... rely on a single authority.” *Id.*, 25:40-42.

Smith’s “electronic funds transfer consumer authorization verification system,” shown below, is not a centralised financial system.



EX1004, Fig. 1

As shown, Smith’s system includes, for example, a business (e.g., a merchant or realtor, ¶ 35); it includes a non-affiliated third-party payment processor (e.g., PayPal, ¶ 11); it includes an ODFI (depository financial institution, ¶ 11). This is not a “centralised system,” as it includes multiple unaffiliated entities with no source of authority. Olivier Dec., ¶ 92. Even if Smith’s system were a centralised financial system, Petitioner proposes to modify Smith’s system to include a blockchain. Pet., 21-26. And as Petitioner’s own expert opined, a blockchain “is a **decentralized** distributed ledger.” EX1003, ¶ 25 (emphasis added).

Petitioner's identified system is not a centralised financial system, and Petitioner offers no evidence or even explanation to the contrary. While Petitioner does not rely on its expert for this proposition, Dr. Shen's single sentence—a sentence contradicted by his previous explanations—is copied verbatim from the Petition with no explanation. It is not evidence that can be credited to overcome the Petition's failure. *See Xerox Corp. v. Bytemark*, IPR2022-00624, Paper 12, at 2 (PTAB Feb. 10, 2023).

As with the Petition's failure related to the “intermediary” limitation discussed above, the Petition's failure with respect to the “centralised financial system” limitation is a symptom of a larger failure: the Smith/Seeger combination is in a different context than the '413 patent and, as a result, fails for numerous distinct reasons.

C. The proposed combination would not have rendered obvious “generate/generating an enriched data record from the one or more documents.”

Independent claim 1 requires “generating an enriched data record from the one or more documents, at the first intermediary server.” EX1001, claim 1. The remaining independent claims similarly require a “first intermediary server” that is “configured to ... generate an enriched data record from the one or more documents.” *Id.*, claims 15, 16. Petitioner relies on Smith as allegedly disclosing this functionality of the claims. Pet., 19, 57, 59. Smith does not. The Petition fails.

The specification of the '413 patent provides context for generating the enriched data record through its disclosed embodiments. The '413 patent describes document stores that are “configured to store a plurality of documents. Each one of the documents comprise data pertaining to a financial transaction.” EX1001, 11:11-13. For example, the documents may comprise data such as account numbers, BICs, transaction amounts, and currency type, sanctions screening information, date of birth, etc. *Id.*, 12:19-13:37.

The first intermediary server is “configured to generate an enriched data record from the one or more documents.” *Id.* 12:39-41. As the '413 patent explains, the enriched data record is not merely a received document but includes data from one or more documents that may actually be needed to process a transaction. As an example, the first intermediary server generates the enriched data record by “extract[ing] a plurality of attributes from the one or more documents” and “combin[ing] the plurality of attributes to generate the enriched data record.” *Id.*, 12:46-53. As another example, the enriched data record may be generated by “extract[ing] the plurality of attributes from one or more documents, de-identify[ing] the plurality of attributes to obtain a plurality of de-identified attributes and combin[ing] the plurality of de-identified attributes to generate the enriched data record. *Id.*, 12:53-58. Yet another example is the enriched data record being generated by “extract[ing] the plurality of attributes from the one or more

documents, hash[ing] the plurality of attributes to generate a plurality of respective hashes and combin[ing] the plurality of hashes to generate the enriched data record.” *Id.*, 12:58-64. The “definitions” section of the ’413 patent provides that the “enriched data record” includes “a plurality [of] data required to process a financial transaction,” and that “plurality of data is rendered, formatted or passed through an algorithm in a predetermined manner.” *Id.*, 28:67-29:3. It is the rendering, formatting, or passing of the plurality of data from the one or more documents that generates a data record that is “enriched.” *Id.* Olivier, Dec. ¶ 96.

Petitioner relies on Smith as purportedly disclosing this limitation. However, Smith fails to teach or suggest generating an enriched data record from the one or more documents. Smith instead discloses “a computer for the business 30” that passes along received information; there is no disclosure of any *generation of an enriched data record*, especially *from* the one or more documents. Olivier Dec., ¶¶ 97-103.

Petitioner alleges that the claimed “generated enriched data record” is disclosed in Smith by “the ACH detail record and its corresponding transaction data file, individually and together.” Pet., 20. However, Smith does not disclose generating an enriched data record to arrive at either of these, much less from the alleged “one or more documents.” Smith discloses that a “transaction data file” is “image data” for “verifying a transaction.” EX1004, ¶ 50. As an example, a

transaction data file may be an image of a signature of a consumer, a copy of a driver's license, a copy of a Social Security card, or a copy of a state business license. *Id.*, ¶ 51. Plainly, Smith's business does not generate these image files, e.g., a copy of a consumer's driver's license, from the alleged one or more documents by the rendering, formatting, or passing of the plurality of data. Olivier Dec., ¶ 98. Instead, a POSITA would understand that the business receives a copy of the image file from, e.g., the consumer, and merely passes it along to the third-party payment processor (TPPP). *Id.*

Petitioner never explains how a business generates an enriched data record to arrive at a transaction data file, such as an image file of a driver's license, using underlying information of the license. Petitioner only states, without explanation, that the alleged enriched data record is "generated by the business computer ... by 'combin[ing] a plurality of attributes' of the one or more documents." Pet., 20. And while Petitioner relies on its expert, he provides no additional detail; indeed, the expert declaration here is a near copy/paste of the Petition with one exception: unsurprisingly, Petitioner's expert did not even opine here that the *business computer* (the alleged first intermediary server) does any generating. EX1003, ¶ 79. In any event, it is not credible that a POSITA would understand the business to generate an enriched data record to arrive at an image file such as a Social Security

card image, by combining attributes, much less performing any such generation from the “one or more documents.” Olivier Dec., ¶¶ 98-99.

Nor does Smith disclose the business generating an enriched data record from the alleged one or more documents to arrive at an “ACH detail record.” As an initial matter, Smith’s ACH detail record adheres to specific standardized messaging of traditional payment rails—exactly the type of message for which the “enriched data record” was invented to supplement. EX1004, ¶ 44; Olivier Dec., ¶ 100. Smith discloses that an ACH detail is part of an ACH file that “is a simple ASCII-format file that adheres to the Automated Clearing House specifications.” EX1004, ¶ 43.

Petitioner fails to identify any portion of Smith that describes or suggests that the ACH detail record is an enriched data record generated by the business by rendering, formatting or passing through an algorithm in a predetermined manner, nor that it is generated from the alleged one or more documents at all. *See* EX1004, ¶¶ 43-48. Olivier Dec., ¶ 100. For this requirement, Petitioner does not even cite to Smith. Instead, Petitioner relies exclusively on its expert’s declaration at paragraph 79. Pet., 20 (citing only EX1003, ¶ 79). But again, the expert does not opine that Smith’s business generates an enriched data record to arrive at the ACH detail record. *See* EX1003, ¶ 79. Nor does the expert offer any explanation of how the ACH detail record is generated *from* the alleged one or more documents. *Id.*

For the avoidance of doubt, the transaction file and the ACH detail record, together, do not disclose this element. As Petitioner cannot show that Smith's alleged intermediary server generates an enriched data record by generating either the ACH data record or the transaction file from the alleged one or more documents, it likewise cannot show that it generates the two from the alleged one or more documents. Moreover, the transaction file and ACH detail record are separate. Olivier Dec., ¶ 101. Smith discloses that the transaction file and ACH record may be transmitted separately and that they are stored separately. EX1004, ¶ 50 and Fig. 5; Olivier Dec., ¶ 101. For the reasons above, the Petition fails.

Petitioner's expert appears to have unknowingly agreed with Patent Owner's position on this point. While Petitioner's expert argues that the business generates the transaction data file and/or ACH record *from* the one or more documents (EX1003, ¶ 87), he opined earlier in his declaration in relation to element 1 that a transaction data file and/or ACH record *is* the "one or more documents." EX1003, ¶¶ 71-72 (alleging the "one or more documents" are the transaction data information "aggregated together"). While no "aggregation" is described in Smith, the ACH record nevertheless cannot simultaneously be the "one or more documents" and be a "generat[ed] enriched data record from the one or more documents."

At bottom, Petitioner alleges that Smith stores some information, and then later sends a transaction file and ACH detail record that might include some of that

information. EX1003, ¶¶ 78-79; Pet., 19-20. However, Petitioner cannot show that the ACH detail record and transaction data file are generated *from* the allegedly stored information. Indeed, it makes no sense how a business could generate an image of a driver's license by having some underlying information of the license.

The Petition's failure here is highlighted by Petitioner's expert's explanation for claim 5. There, Petitioner's expert opines that the business computer "extract[s] a plurality of attributes from the one or more documents." EX1003, ¶ 119. But Petitioner's expert again fails to identify any such disclosure in Smith, only that the ACH detail record includes some of the same information as some amorphous "ACH transaction information." *Id.* But for the requirement to "combin[e] the plurality of attributes to generate the enriched data record," Petitioner's expert all but concedes there is no generation of an enriched data record at all. Instead, Petitioner's expert can only state that it would have been "obvious" to "combine" the ACH detail record and transaction file—and by combine, he means send the two in a single transmission. *Id.* ¶ 121. Sending two separate files together in a single transmission is not generating an enriched data record as defined by the specification. Olivier Dec., ¶ 103.

Seeger does not cure these deficiencies of Smith, and Petitioner makes no argument to the contrary.

D. The proposed combination would not have rendered obvious the claimed “token.”

Each independent claim requires a specific “token.” EX1001, claims 1, 15, 16. The “definitions” section of the ’413 patent provides that a “token” is “a pointer to an enriched data record of a plurality data required to process a financial transaction and wherein the plurality of data is rendered, formatted or passed through an algorithm in a predetermined manner.” *Id.*, 28:66-29:3. Petitioner fails to show that the Smith/Seeger combination discloses or suggests the claimed token limitations of the independent claims.

First, as discussed above, Petitioner’s proposed combination does not teach or suggest generating an enriched data record. Thus, the proposed combination cannot teach or suggest a token that points to the enriched data record.

Second, Petitioner offers no explanation of how its alleged token is “a *pointer to an enriched data record of a plurality data* required to process a financial transaction and *wherein the plurality of data is rendered, formatted or passed through an algorithm in a predetermined manner.*” As the specification makes clear, data from documents is rendered, formatted, and/or passed through an algorithm (tokenised) to create an enriched data record. EX1001, 28:66-29:5. And the claimed token is a pointer to that enriched data record (which includes the rendered formatted data). *Id.*

Petitioner appears to recognize that a token is a pointer to an enriched data record, where the enriched data record includes data rendered, formatted or passed through an algorithm in a predetermined manner. Pet., 29. However, Petitioner wholly fails to offer any explanation or allegation that the Smith/Seeger combination discloses this. *See id.* Curiously, instead of alleging that the token is a pointer to “data rendered, formatted or passed through an algorithm,” Petitioner argues that the token can be *generated* by passing data through an algorithm. Pet., 28 (alleging “generating a unique identifier for a transaction by applying a predetermined algorithm to some or all of the transaction data”). Regardless of whether that would have been obvious, it is not the requirement of a token (i.e., to serve as a pointer to an enriched data record that comprises a plurality of data that is rendered, formatted or passed through an algorithm in a predetermined manner).

Even if Petitioner’s misunderstanding of the plain language of the specification were correct, neither Smith nor Seeger disclose or suggest generating a token by passing transaction data—including images of drivers’ licenses and state licenses—through an algorithm. Instead, Smith discloses generating transaction keys sequentially. *See* EX1004, Fig. 5 (ABCD1, ABCD2, etc.). And while Smith’s generating is non-limiting for purposes of Smith’s claims, that does not mean that Smith discloses or renders obvious every possible way to make a token. Petitioner provides no reason to modify the *disclosure* of Smith. Petitioner only alleges that

generating a token in a new way—not contemplated by any alleged reference—would avoid having two identical transaction keys. Pet., 28. But Smith’s much simpler method, to assign transaction keys sequentially, already avoids identical transaction keys. Olivier Dec., ¶ 108. Moreover, Petitioner’s expert attempts to add references to the combination with no reasoning by using string cites to opine that tokens may be generated from underlying data. However, he offers no explanation how a POSITA could have (or would have) generated tokens from Smith’s “transaction data” of “image files.” See EX1003, ¶ 91. Nevertheless, this explanation is not a requirement of the claims: Petitioner fails to address the actual claim requirements of a token.

Petitioner’s irrelevant argument here only highlights a problem pervasive in the Petition: hindsight. Because the references alone consistently fail, Petitioner and its expert propose drastic modifications to the disclosures of the reference without consideration of how the system as a whole would be affected or how a POSITA would have even gone about making such modifications—or whether the POSITA even could. This is an improper obviousness analysis that must fail.

Petitioner’s inapplicable modification aside, Petitioner offers no explanation how the token is a pointer to an enriched data record, which is data that is rendered, formatted or passed through an algorithm in a predetermined manner, as defined in the specification. As such, the Petition fails.

E. The proposed combination would not have rendered obvious “requesting generation of a token corresponding to the financial transaction”

Each independent claim requires “request/ing generation of a token.” EX1001, claims 1, 15, 16. Petitioner cannot show that the Smith/Seeger combination discloses or suggests this limitation. For this functionality, Petitioner relies only on Smith’s alleged functionality that “TPPP generates and returns the [alleged token] in response to receiving communications from the business computer.” Pet., 30-31. Notably, the Petitioner makes no argument that the “communications” include any “request” to generate a token—because they do not.

In Smith, “[t]he business 30 sends one or more transaction data files to the third-party payment processor 70.” EX1004, ¶ 52. The third-party payment processor verifies the authenticity of the transaction data files, e.g., “verifies via a state agency that the business 30 is authorized to do business 30 in the state alleged to be licensed. If the business 30 is verified by the third-party payment processor 70 to be licensed in a state, the third-party payment processor 70 then updates its database to include a unique transaction key.” *Id.*, ¶ 53. After verification, the TPPP may transmit the transaction key to the business. *Id.*

Smith discloses communicating “transaction data files” to the TPPP. Transaction files are not a request to generate a token; they are image files, including a signature of a consumer, a scan of an ACH agreement, a copy of a driver’s license,

a copy of a Social Security card, etc. EX1004, ¶ 51. Nowhere in this image data is a request to generate a token. Indeed, there is no disclosure in Smith that the transaction data files mention the alleged token at all. As discussed in the paragraph below, the only time the “communications” mention the transaction key, is when it has already been generated and provided to the business.

Petitioner argues that Smith’s request is the TPPP “receiving the transaction data record and ACH detail record” from the business, and that the TPPP transmits the transaction key “in response to receiving communications from the business.” Pet. 30-31. Petitioner argues that the communications are the alleged “request.” *Id.* However, there are circumstances where Smith’s business sends these communications to the TPPP when it already has the transaction key. Smith describes that the business can provide the detail record “without a transaction key”) or with the transaction key “entered into ... the detail record ... by the business.” EX1004, ¶ 41. The communication is clearly not a request to generate the transaction key if it is already generated. And the same communication is not somehow transformed into a request to generate the transaction key if it is not included in the communication. Olivier Dec., ¶ 112.

Moreover, contrary to Petitioner’s argument, the TPPP does not generate a token in response to communications from the business. *See* Pet., 30-31. Instead, the TPPP only updates its database to include a transaction key after it verifies

information with a state. EX1004, ¶ 53. Indeed, Smith does not disclose that a business 30 would even be aware of a transaction key. While a TPPP may generate a transaction key eventually after receiving documents from the business, Smith does not disclose the business requesting the generation of a token. Petitioner offers no reason why it would have been obvious and with good reason. It would not have been obvious because the TPPP sends the transaction key to the business without any request (EX1004, ¶ 53); there would be no reason to modify the programming of the TPPP to accept and respond to requests for generation, and Petitioner offers none.

At bottom, Petitioner's theory reads out the "request" limitation. Claim 1 separately requires "requesting generation of a token . . . to a token server, from the first intermediary server" and "transmitting the token to the first intermediary server from the token server." Petitioner's argument is that because the TPPP transmits the alleged token, there must have been a request. Pet., 30-31. Not only is this theory incorrect, but it also improperly reads out the "request" functionality of the claims. *Callicrate v. Wadsworth Mfg., Inc.*, 427 F.3d 1361, 1369 (Fed. Cir. 2005) (holding that it is improper to read out a limitation clearly required by the claim language and specification); *Unique Concepts, Inc. v. Brown*, 939 F.2d 1558, 1562 (Fed. Cir. 1991) ("All the limitations of a claim must be considered meaningful.").

F. It would not have been obvious to combine Smith and Seger as proposed.

In its arguments for the independent claims of the '413 patent, Petitioner relies primarily on Smith. Because Smith is attempting to solve a different problem than the '413 patent, there are numerous differences between Smith and the independent claims of the '413 patent. While not relevant here under the Supreme Court's *SAS* decision, Petitioner's theories for the independent claims become shockingly tenuous. Recognizing one major deficiency in Smith—that it does not disclose a blockchain ledger—Petitioner adds Seger.

In its hindsight-based analysis, Petitioner and its expert argue that it would have been “obvious” to add Seger, noting some benefits to blockchain generally. But in considering the actual proposed combination, the purported benefits are inapplicable, and a POSITA would have been dissuaded to attempt to modify Smith to include a blockchain as proposed. *Olivier Dec.*, ¶¶ 45-75. In viewing the actual proposed combination, Petitioner's reasons to include Seger's blockchain do not make sense. *Id.*

Smith discloses that the “business” “sends [an] ACH transaction detail record ... to the third-party payment processor.” EX1004, ¶ 54. The “business” also “sends one or more transaction data files to [a] third-party payment processor.” *Id.*, ¶ 52. “The third-party payment processor 70 stores the ... ACH transaction detail record

and the corresponding transaction data files in a database on a computer for the third-party payment processor 70.” *Id.*, ¶ 41. Under Petitioner’s theory, Smith’s system would instead include a blockchain. Pet., 22-26. Petitioner then argues that the “third-party payment processor” would add information into the blockchain and that the business could also separately add information into the blockchain. Pet., 26, 33.

Petitioner and its expert never discuss the combination of Smith and Seger, what it would look like or how (or if) a POSITA could have combined the two. *See generally* Pet. 21-26; EX1003, ¶¶ 81-87. Instead, Petitioner’s argument is that Smith teaches everything but a blockchain and Seger discloses a blockchain. Pet., 2. In its element-by-element claim discussion, Petitioner and its expert just pull pieces of Seger as needed, in a quintessential hindsight-based analysis.

Indeed, Petitioner’s expert’s only explanation of the combination is that “[it] would have been obvious to a POSITA to [somehow] apply Seger’s blockchain ledger into Smith’s system.” EX1003, ¶ 83; *see also* Pet., 23. While not explained, the proposed combination is not as simple as “swapping out” a database with a blockchain. In not considering or discussing what the combination would be, Petitioner and its expert fail to recognize that multiple aspects of Smith would need to be modified.

Not only would the alleged “token server” include a blockchain component, the “business computer,” the alleged intermediary server, would include one as

well since Petitioner proposes that the “business computer” would add information into the blockchain. Olivier Dec., ¶ 49. As such, under Petitioner’s proposed combination, Smith’s TPPP and all its business computers would need to be substantially modified. *Id.*

Moreover, a POSITA would understand that in Smith’s system, Smith’s “business” would include numerous computers from multiple, distinct entities. Olivier Dec., ¶ 48. As Smith describes, the “business 30 may be comprised of various entities.” EX1004, ¶ 35. For example, the business 30 may comprise numerous merchants and online retailers. *Id.* This makes sense, as Smith’s TPPP, such as PayPal, would process transactions from numerous businesses. *See id.*, 11. Thus, Smith’s system, as modified, would include numerous distinct businesses, each having access to the blockchain.

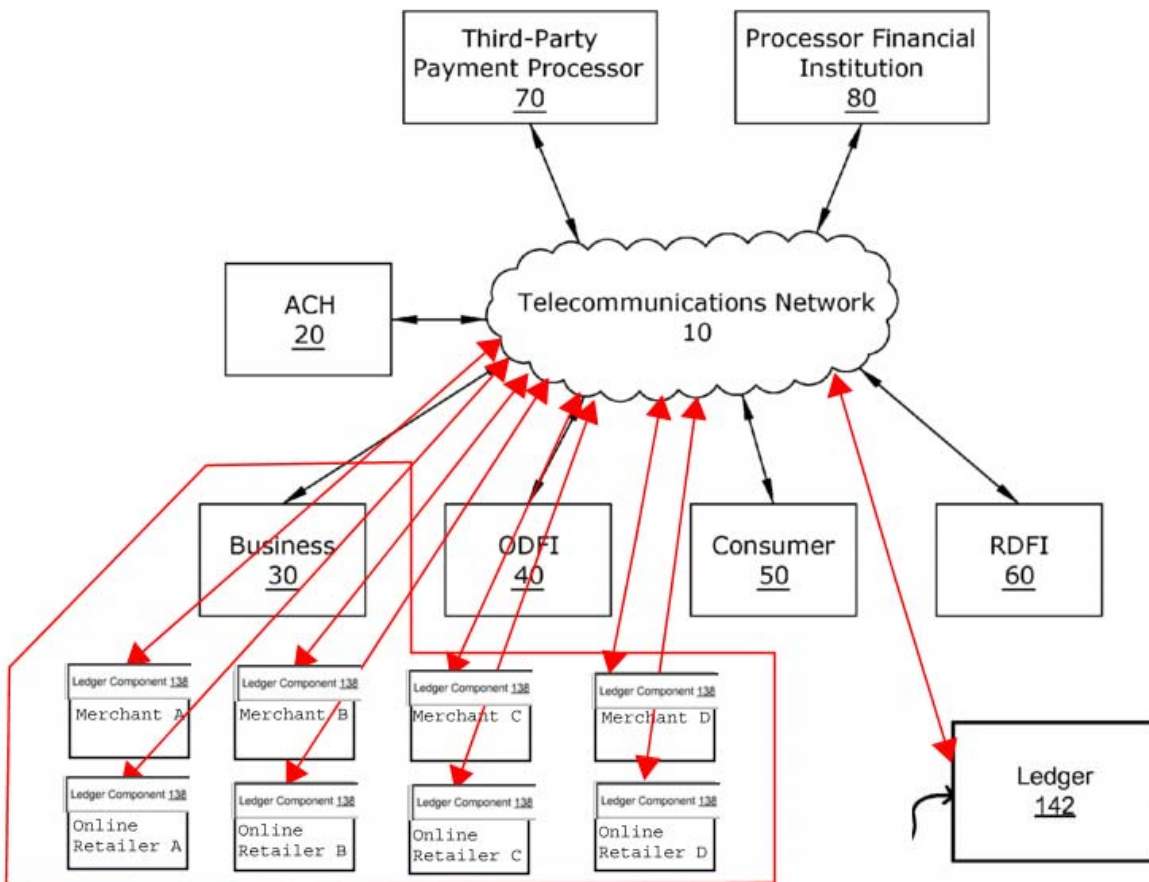


FIG. 1

Olivier Decl., ¶¶ 48-49.

Regardless of *how* Smith’s business could be modified to add the alleged enriched data record to a blockchain, a POSITA would not have done so. Olivier Dec., ¶ 51.

1. Smith and Seger are directed to two different types of “verification.”

As an initial matter, Petitioner’s primary reason to combine, “verification,” is inapplicable in the context of what the references describe as being “verified.” Smith

discloses a “transaction data file” and “ACH detailed record.” EX1004, Abstract. Smith proposed sending the files to a third-party payment processor. The third-party payment processor uses the transaction data file to (1) independently verify the *accuracy* of received data—such as to confirm with a state agency that the business is licensed or confirm the identity of a consumer using the files; (2) to modify the database to include the verification data; and (3) to initiate processing the transaction by sending it to a payment network. *Id.*, ¶ 59. A key purpose of Smith is thus having an independent, third-party payment processor that independently verifies data and maintains, controls, and modifies information in its secure database. Olivier Dec., ¶¶ 63-67.

Seeger, on the other hand, is directed to logging communications on a blockchain. Olivier Dec., ¶ 65. As Seeger explains, while parties could communicate electronically via email, SMS, or direct messages, the communications are “not recorded in a log that can be audited after the fact by a third-party.” EX1005, 1:16-21. To solve this issue, Seeger proposed that the parties record communications on a blockchain. *Id.*, 5:7-14. Seeger explains that the distributed ledger may be immutable. *Id.*, 10:19-23. That is, the information cannot be modified. Olivier Dec., ¶ 65. Because the ledger is immutable, it “may provide a verifiable record of all the information exchanges.” *Id.*

A POSITA would not have been motivated to modify Smith to include the distributed ledger of Seger. Olivier Dec., ¶¶ 66-67. As an initial matter, Seger would not supplement Smith’s verification because they are directed to two different types of verification: nothing in Seger verifies the authenticity or accuracy of the underlying data, which is the purpose of Smith. Seger only verifies that data was not changed. Olivier Dec., ¶ 66.

Indeed, Seger would limit Smith’s verification techniques. Seger describes two non-trusted parties, logging communications on a blockchain so they cannot be altered. EX1005, 1:16-21. Smith, on the other hand, describes a trusted “third-party” payment processor whose purpose is to modify and supplement communicated information. Smith discloses that after the third-party payment processor receives data it performs “a number of checks” to verify the information. EX1004, ¶ 59. For example, “[t]he merchant has to be licensed in the state.” *Id.* To perform this check, the third-party payment processor “verifies via a state agency” that the business is licensed and then “updates its database” to attach “additional transaction data files ... to provide additional evidence of the business’s verified licensing in a state.” *Id.*, ¶ 53. Thus, Smith discloses that a trusted third-party should be able to update its own database. Olivier Dec., ¶ 66. A POSITA would not have modified Smith’s disclosure to include a distributed ledger that could not be updated. *Id.*

2. The proposed combination is less secure, and Smith teaches away from the less secure system.

Moreover, a POSITA would recognize that modifying Smith in view of Seger results in a less secure system and that Smith explicitly teaches *not* to use such a less secure system. Olivier Dec., ¶¶ 47-51. Smith recognizes that the information stored by the third-party payment processor is “sensitive information [that] is to be stored in a Payment Card Industry (aka PCI) level 1 environment. This environment maintains the highest level of compliance and encryption within the Payment Card Industry.” EX1004, ¶ 59. Smith’s third-party processor maintains the data only within a database that it completely controls to the highest standards. Olivier Dec., ¶ 52. Including the information on Seger’s “distributed” ledger makes the information stored by multiple parties who can all control access less secure. Olivier Dec., ¶¶ 53-54. Indeed, Seger recognizes that the distributed ledger, itself, is not secure. As Seger’s distributed ledger is maintained and can be accessed by various parties, Seger discloses encrypting using public/private keys, and Seger explicitly recognizes the security concerns of communicating the private keys to the proper entities. EX1005, 1:22. Smith is much more secure in that the TPPP can control who has access to its own database and does not require transferring private keys. Olivier Dec., ¶¶ 53-59.

Likewise problematic in the combination is that a POSITA would recognize that such a system would have multiple “businesses.” Olivier Dec., ¶ 48. And in Smith’s system, each business—unaffiliated merchants, retailers, etc.—would each have access to the distributed ledger. Olivier Dec., ¶¶ 53-54. The confidential information for each and every transaction of each business would be stored on the distributed ledger. This would drastically increase exposure of not only the confidential information of each consumer, but also the information of each business.

3. The combination would frustrate a key purpose of Smith by allowing other parties, such as unaffiliated businesses, to add information to the blockchain.

Smith discloses that the TPPP is responsible for receiving and storing data from multiple entities and maintaining the database. EX1004, ¶ 53 (the TPPP independently verifies the business is authorized and adds additional transaction data files as evidence); Olivier Dec., ¶ 64. If the business could upload documents to the alleged ledger as it wished, the TPPP could not provide the independent verification and control of the data stored in the alleged ledger. Olivier Dec., ¶¶ 66-67. Nor could the TPPP control access to the ledger, as the ledger would be distributed outside of the third-party processor.

4. Smith and Seger are in different fields.

Smith and Seger are directed to two distinct systems in very different fields. Smith is related to a business initiating a financial transaction by sending information to a third-party payment processor. Olivier Dec., ¶¶ 46-47. Seger, on the other hand, is directed to a cryptographic platform that stores information transactions. *Id.* Petitioner provides no sufficient reason why a POSITA would have looked to modify Smith, a reference dealing with financial transactions and no suggestion of blockchain, with Seger, a reference dealing with blockchain and no suggestion of completing financial transactions.

5. Petitioner’s motivations to combine fail.

None of Petitioner’s reasons to combine are availing, and certainly would not lead a POSITA to make the proposed combination that is less secure and would not work for its intended purpose. Indeed, Petitioner’s proposed motivations demonstrate the hindsight nature of the analysis.

First, Petitioner argues that Smith proposes verifying transaction files, but is silent on how. Pet., 21-23. This is incorrect. As discussed above, Smith discloses, for example, receiving state licensing information from a business and confirming, with a state agency, that the business is actually licensed, including by using an API that “accept[s] input from a state agency website . . . to validate that a business is licensed in that said state.” EX1004, ¶ 65 (also discussing APIs for other

verifications). Smith also explains how consumers' identity information is verified. *Id.* (the TPPP accepts "input from a consumer ID and address validation network ... to validate identification numbers and address of consumers.").

As such, a key purpose of Smith is to provide an independent third-party that verifies the *authenticity* and *accuracy* of data. While Petitioner fixates on the word "verify" in both Smith and Seger, Seger's distributed ledger is only "verified" in that parties can verify that the data does not change, as it is immutable. EX1005, 1:16-21, 10:19-23. Seger's distributed ledger does not verify the *accuracy* of the data. Olivier Dec., ¶ 64. For example, a first non-trusted party in Seger could communicate fraudulent licensing information to a second party for inclusion in the distributed ledger. While the ledger verifies that the information has not changed, it does not verify whether the information is fraudulent. Olivier Dec., ¶ 69.

Smith and Seger are discussing two different types of verification. And in Smith, the third-party system does not need to verify that the information is unchanged; Smith controls and maintains the information it receives; Smith's system already knows whether the data is changed, without the need for a less secure, unworkable system like Seger.

Second, Petitioner notes that Seger provides a system "for secure financial transactions." Pet., 24. But as discussed above, Smith does as well—and Smith's system is more secure. This motivation fails.

Third, Petitioner argues that both Seger and Smith are in the same art and “apply similar approaches.” Pet., 24. Not only is this incorrect as described above, but it does not constitute an articulated reason to combine one reference with another. *See William Wesley Carnes, Sr., Inc. v. Seaboard Int’l Inc.*, IPR2019-00133, Paper 10 (May 8, 2019) (finding that mere allegation that references are in same field and address common problems “does not constitute an articulated reasoning . . . why a POSITA would combine elements of one reference with another.”); *Seabery N. Am., Inc. v. Lincoln Global, Inc.*, IPR2016-00749, Paper 13, 11-12 (Sept. 21, 2016) (“Merely asserting that [two] prior art references are analogous art to each other, however, is not a sufficient articulated reason with a rational underpinning to combine their respective teachings.”).

Fourth, Petitioner argues that Seger teaches the “advantage of providing an ‘immutable’ record, ensuring the transaction data cannot be altered once written.” Pet., 25. This argument fails: as discussed above, Smith teaches that data *should* be altered. And nevertheless, the third-party verification entity in Smith already knows whether the data has been altered, as it is in complete control of the storage, maintenance, and alterations of its database. *Olivier Dec.*, ¶ 73.

Lastly, Petitioner argues that it would have been obvious to modify Smith because distributed ledgers and blockchain were known. Pet., 25-26. This is not a reason for a POSITA to make a combination with an unworkable and less secure

system. Indeed, the Federal Circuit has rejected this argument. *Virtek Vision Int'l ULC v. Assembly Guidance Sys., Inc.*, 97 F.4th 882, 887 (Fed. Cir. 2024) (“The mere fact that these possible arrangements existed in the prior art does not provide a reason that a skilled artisan would have substituted” disclosure of one reference with disclosure of another.). Petitioner fails to articulate any credible reason why a POSITA would combine Smith and Seger. In fact, there are multiple reasons why a POSITA would not.

VI. GROUNDS 2 AND 3 FAIL

The Petition fails to demonstrate a reasonable likelihood of success for grounds 2 and 3 for at least the same reasons discussed with respect to ground 1. For ground 2, Petitioner adds the Yago reference only to address additional limitations of claim 3. Similarly for ground 3, Petitioner adds the Kurani-274 reference only to address additional limitations of claim 4. Neither Yago nor Kurani-274 cure the deficiencies of Smith and Seger discussed in relation to ground 1, and Petitioner makes no argument to the contrary. Grounds 2 and 3 thus fail.

VII. CONCLUSION

It would not have been obvious to combine Smith and Seger as proposed to arrive at a more complicated, less secure system with no added benefits. Even if it were, the proposed combination still fails to teach or suggest numerous elements of the independent claims. The Petition fails to present any likelihood of success on

any ground. Institution should be denied.

Dated: May 28, 2024

/s/ Richard C. Lin

Richard C. Lin, Lead Counsel

Reg. No. 56,682

Jerry D. Tice II, Back-up Counsel

Reg. No. 73,582

Bunsow De Mory LLP

701 El Camino Real

Redwood City, CA 94063

Telephone: 650-351-7248

Facsimile: 415-426-4744

rlin@bdiplaw.com

jtice@bdiplaw.com

Counsel for Patent Owner

**CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION,
TYPEFACE REQUIREMENTS, AND TYPE STYLE REQUIREMENTS**

1. This Patent Owner's Preliminary Response complies with the type-volume limitation of 14,000 words, comprising 11,067 words, excluding the parts exempted by 37 C.F.R. § 42.24(a)(1).

2. This Patent Owner's Preliminary Response complies with the general format requirements of 37 C.F.R. § 42.6(a) and has been prepared using Microsoft® Word 2016 in 14 point Times New Roman.

Dated: May 28, 2024

/s/ Richard C. Lin
Richard C. Lin
Reg. No. 56,682
Bunsow De Mory LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: 650-351-7248
Facsimile: 415-426-4744
rlin@bdiplaw.com

Lead Counsel for Patent Owner

CERTIFICATE OF SERVICE

Petitioner has consented to e-mail service in this proceeding. Pursuant to 37 C.F.R. §42.6, the undersigned certifies that on May 28, 2024, a copy of the foregoing document was served by email upon the following counsel at the below email addresses:

JONES DAY

H. Albert Liou – aliou@jonesday.com

Rita J. Yoon – ryoon@jonesday.com

I. Sasha Mayergoyz – smayergoyz@jonesday.com

Matthew W. Johnson – mwjohnson@jonesday.com

Marlee R. Hartenstein – mhartenstein@jonesday.com

Stephen M. Bradley – sbradley@jonesday.com

Dated: May 28, 2024

/s/ Richard C. Lin

Richard C. Lin

Reg. No. 56,682

Bunsow De Mory LLP

701 El Camino Real

Redwood City, CA 94063

Telephone: 650-351-7248

Facsimile: 415-426-4744

rlin@bdiplaw.com

Lead Counsel for Patent Owner