

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 No. IPR2024-00590
U.S. Patent No. 10,984,413

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 10,984,413**

TABLE OF CONTENTS

'413 PATENT CLAIM LISTING	iii
I. INTRODUCTION	1
II. REQUIREMENTS FOR IPR UNDER 37 C.F.R. § 42.104.....	2
A. Grounds For Standing Under 37 C.F.R. § 42.104(a)	2
B. Precise Relief Requested And Grounds Under 37 C.F.R. § 42.104(b)	2
C. Claim Construction Under 37 C.F.R. § 42.104(b)(3)	3
III. '413 PATENT.....	3
A. Alleged Invention	3
B. Prosecution History	5
C. POSITA	6
IV. THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	6
A. Prior Art.....	6
1. Smith	6
2. Seger.....	9
3. Kurani-274	11
4. Yago	12
B. Ground 1: Claims 1-2 And 5-20 Would Have Been Obvious Over Smith In View Of Seger	13
1. Claim 1	13
2. Claim 2	36
3. Claim 5	38
4. Claim 6	40
5. Claim 7	42
6. Claim 8	43
7. Claim 9	50
8. Claim 10	51
9. Claim 11	54
10. Claim 12	54

TABLE OF CONTENTS

(continued)

11.	Claim 13	55
12.	Claim 14	55
13.	Claim 15	55
14.	Claim 16	58
15.	Claim 17	59
16.	Claim 18	60
17.	Claim 19	60
18.	Claim 20	61
C.	Ground 2: Claim 3 Would Have Been Obvious Over The Smith/Seeger Combination In View Of Yago	61
D.	Ground 3: Claim 4 Would Have Been Obvious Over The Smith/Seeger Combination In View Of Kurani-274	64
V.	DISCRETIONARY INSTITUTION	67
A.	The <i>Fintiv</i> Factors Favor Institution	67
B.	The <i>Becton</i> Factors Favor Institution	69
VI.	CONCLUSION	69
VII.	MANDATORY NOTICES PURSUANT TO 37 C.F.R. § 42.8(a)(1)	70
A.	37 C.F.R. § 42.8(b)(1): Real Parties-In-Interest	70
B.	37 C.F.R. § 42.8(b)(2): Related Matters	70
C.	37 C.F.R. § 42.8(b)(3), (4): Counsel And Service Information	70
	CERTIFICATE OF SERVICE	73
	CERTIFICATE OF WORD COUNT UNDER 37 C.F.R. § 42.24(a)	74
	APPENDIX OF EXHIBITS	75

'413 PATENT CLAIM LISTING

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

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;

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;

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;

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;

transmitting the token to the first intermediary server from the token server, via the messaging bus; and

transmitting the token from the first intermediary server to the first document store in association with the one or more documents.

2. The computer implemented method as claimed in claim **1**, further comprising the step of sending a first financial message comprising the token, from the first intermediary server to a second intermediary server in the centralised financial system, indicative of making a payment to a second user.

3. The computer implemented method as claimed in claim **1**, further comprising the steps of:

implementing a smart contract at the token server; and

adding the smart contract into the blockchain, from the token server.

4. The computer implemented method as claimed in claim **1**, further comprising the steps of:

transmitting the token from the first intermediary server to a first digital device available with a first user;

providing the token to a second user, by the first user;

providing the token to a second intermediary server in the centralised financial system, from a second digital device;

transmitting the token to a second document store, from the second intermediary server; and

sending a second financial message comprising the token, from the second intermediary server to the first intermediary server, indicative of making a payment to the first user.

5. The computer implemented method as claimed in claim **1**, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server; and

combining the plurality of attributes to generate the enriched data record, at the first intermediary server.

6. The computer implemented method as claimed in claim **1**, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server;

de-identifying the plurality of attributes to obtain a plurality of de-identified

attributes, at the first intermediary server; and

combining the plurality of de-identified attributes to generate the enriched data record, at the first intermediary server.

7. The computer implemented method as claimed in claim **1**, wherein the step of generating the enriched data record comprises:

extracting a plurality of attributes from the one or more documents, at the first intermediary server;

hashing the plurality of attributes to generate a plurality of respective hashes, at the first intermediary server; and

combining the plurality of hashes to generate the enriched data record, at the first intermediary server.

8. The computer implemented method as claimed in claim **1**, further comprising the steps of:

transmitting one or more first requests, each comprising the token, from the first intermediary server to a second intermediary server in the centralised financial system, via the messaging bus;

receiving the one or more first requests at the second intermediary server and transmitting the one or more first requests and the token from the second intermediary server to a second document store;

generating one or more first responses, each comprising the token, corresponding to the respective one or more first requests, at the second intermediary server;

transmitting the one or more first responses from the second intermediary server to the first intermediary server, via the messaging bus;

hashing the one or more first requests and the one or more first responses at the

second intermediary server to generate one or more first request hashes and one or more first response hashes, respectively;

adding the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain, from the second intermediary server; and

receiving the one or more first responses at the first intermediary server and transmitting the one or more first responses to the first document store.

9. The computer implemented method as claimed in claim **8**, further comprising the steps of:

hashing the one or more first responses at the first intermediary server to regenerate the one or more first response hashes; and

verifying the one or more first response hashes with the blockchain from the first intermediary server, using the token.

10. The computer implemented method as claimed in claim **8**, wherein each one of the one or more first requests are:

encrypted with a second public key and signed with a first public key at the first intermediary server, before transmission to the second intermediary server; and

decrypted with a second private key at the second intermediary server after reception from the first intermediary server; and

wherein each one of the one or more first responses are:

encrypted with the first public key and signed with the second public key at the second intermediary server, before transmission to the first intermediary server; and

decrypted with a first private key at the first intermediary server after reception from the second intermediary server.

11. The computer implemented method as claimed in claim **10**, further comprising the steps of adding the first public key from the first intermediary server into the blockchain and adding the second public key from the second intermediary server into the blockchain.

12. The computer implemented method as claimed in claim **1**, further comprising the steps of:

transmitting one or more second requests, each comprising the token, from a second intermediary server in the centralised financial system to the first intermediary server, via the messaging bus;

receiving the one or more second requests at the first intermediary server and transmitting the one or more second requests from the first intermediary server to the first document store;

generating one or more second responses, each comprising the token, corresponding to the respective one or more second requests, at the first intermediary server;

transmitting the one or more second responses from the first intermediary server to the second intermediary server, via the messaging bus;

hashing the one or more second requests and the one or more second responses at the first intermediary server to generate one or more second request hashes and one or more second response hashes, respectively;

adding the one or more second request hashes and the one or more second response hashes to the enriched data record in the blockchain, from the first intermediary server; and

receiving the one or more second responses at the second intermediary server and transmitting the one or more second responses to the second document store.

13. The computer implemented method as claimed in claim **12**, further comprising the steps of:

hashing the one or more second responses at the second intermediary server to regenerate the one or more second response hashes; and

verifying the one or more second response hashes with the blockchain from the second intermediary server, using the token.

14. The computer implemented method as claimed in claim **12**, wherein each one of the one or more second requests are:

encrypted with a first public key and signed with a second public key at the second intermediary server, before transmission to the first intermediary server; and

decrypted with a first private key at the first intermediary server after reception from the second intermediary server; and

wherein each one of the one or more second responses are:

encrypted with the second public key and signed with the first public key at the first intermediary server, before transmission to the second intermediary server; and

decrypted with a second private key at the second intermediary server after reception from the first intermediary server.

15. A system for processing a financial transaction, the system comprising:

a first intermediary server in a centralised 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 centralised 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.

16. A first intermediary server for use in a centralised financial system to facilitate processing of a financial transaction, operably connected to a network and a first document store, and 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 a blockchain being a distributed ledger;

request generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, via a messaging bus in the centralised financial system; and

transmit the token to the first document store.

17. The first intermediary server as claimed in claim **16**, further configured to send a first financial message comprising the token, to a second intermediary server in the

centralised financial system, indicative of making a payment to a second user.

18. The first intermediary server as claimed in claim **16**, further configured to transmit the token to a first digital device.

19. The first intermediary server as claimed in claim **16**, further configured to:

transmit one or more first requests, each comprising the token, to a second intermediary server in the centralised financial system, via the messaging bus; and

receive one or more first responses from the second intermediary server and transmit the one or more first responses to the first document store.

20. The first intermediary server as claimed in claim 19, wherein the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.

I. INTRODUCTION

JPMorgan Chase Bank, N.A. (“Petitioner”) requests *inter partes* review (“IPR”) of claims 1-20 (“Challenged Claims”) of U.S. Patent No. 10,984,413 (“’413 Patent”) (Ex. 1001). This petition is based on the ’413 Patent’s earliest possible priority date—August 14, 2015. Petitioner files a separate petition with different grounds and a priority-date challenge.

The ’413 Patent takes conventional financial transactions and records them on a generic blockchain. Purporting to address the “difficult[y]” of “keep[ing] track of the plurality of data during the financial transaction,” the ’413 Patent uses a “token” and “enriched data record” stored on “any blockchain.” (Ex. 1001, 1:39-51, 24:21-23). The patent acknowledges that the “token” and “enriched data record” were well-known before the filing date. (*Id.*, 27:16-19, 29:1-7, 36:26-28). The ’413 Patent acknowledges it applied these well-known elements to “any blockchain based framework.” (*Id.*, 24:21-23). Indeed, the ’413 Patent acknowledges that blockchain was also well-known before the filing date. (*Id.*; *see also* Ex. 1003, ¶¶ 84-86). This Petition demonstrates that the Challenged Claims merely combine well-known elements and are unpatentable under Section 103.

As explained below, the Smith reference teaches a system for “proving that a consumer authorized a financial transaction via an [Automated Clearing House] network.” (Ex. 1004, [0004]). Smith teaches every element of claim 1 of the ’413 Patent except for a “blockchain.” Smith stores a plurality of data about the financial transaction

in a transaction data file and a detail record (“enriched data record”), which are identified and tracked using a “transaction key” (“token”). Smith describes the need for storing transaction data such that “[i]f there is a dispute to the validity” of the transaction data, it be “easily identif[ied] and view[ed].” (*Id.*, [0056]). The Seger reference, in turn, teaches a blockchain ledger for “confidential, verifiable, and immutable recording and/or reporting” of financial transactions. (Ex. 1005, 1:43-44, 6:8-11). Thus, “the undisputed teaching of [Smith] leads one to within a hairsbreadth of anticipation of [claim 1]. The express teachings in the art provide the motivation and suggestion to modify [Smith] such that” Seger’s blockchain is applied to Smith’s funds transfer verification system. *SIBIA Neurosci. v. Cadus Pharm.*, 225 F.3d 1349, 1359 (Fed. Cir. 2000).

II. REQUIREMENTS FOR IPR UNDER 37 C.F.R. § 42.104

A. Grounds For Standing Under 37 C.F.R. § 42.104(a)

Petitioner certifies that the ’413 Patent is available for IPR and Petitioner is not barred or estopped from requesting IPR on the identified grounds.

B. Precise Relief Requested And Grounds Under 37 C.F.R. § 42.104(b)

The Challenged Claims should be cancelled on the following grounds:

Unpatentability Grounds	Exhibits
<u>Ground 1:</u> Claims 1-2 and 5-20 would have been obvious over U.S. Pub. 2015/0081553 (“Smith”) combined with U.S. Patent 9,397,985 (“Seger”)	1004-1005
<u>Ground 2:</u> Claim 3 would have been obvious over Smith and Seger combined with U.S. Pub. 2015/0206106 (“Yago”).	1004-1005, 1011
<u>Ground 3:</u> Claim 4 would have been obvious over Smith and Seger combined with U.S. Patent 11,270,274 (“Kurani-274”).	1004-1005, 1007

Section IV explains where the prior art discloses each element of the Challenged Claims. 37 C.F.R. § 42.104(b)(4). An appendix with exhibit numbers of supporting evidence is at the end. Section IV explains the relevance of the evidence, as supported by Dr. Chien-Chung Shen’s declaration (Ex. 1003). 37 C.F.R. § 42.104(b)(5).

C. Claim Construction Under 37 C.F.R. § 42.104(b)(3)

In this proceeding, claims are interpreted to have their plain meaning in view of the specification and file history. *Phillips v. AWH*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005). For this proceeding, Petitioner believes no special constructions are necessary to assess whether the Challenged Claims are unpatentable.

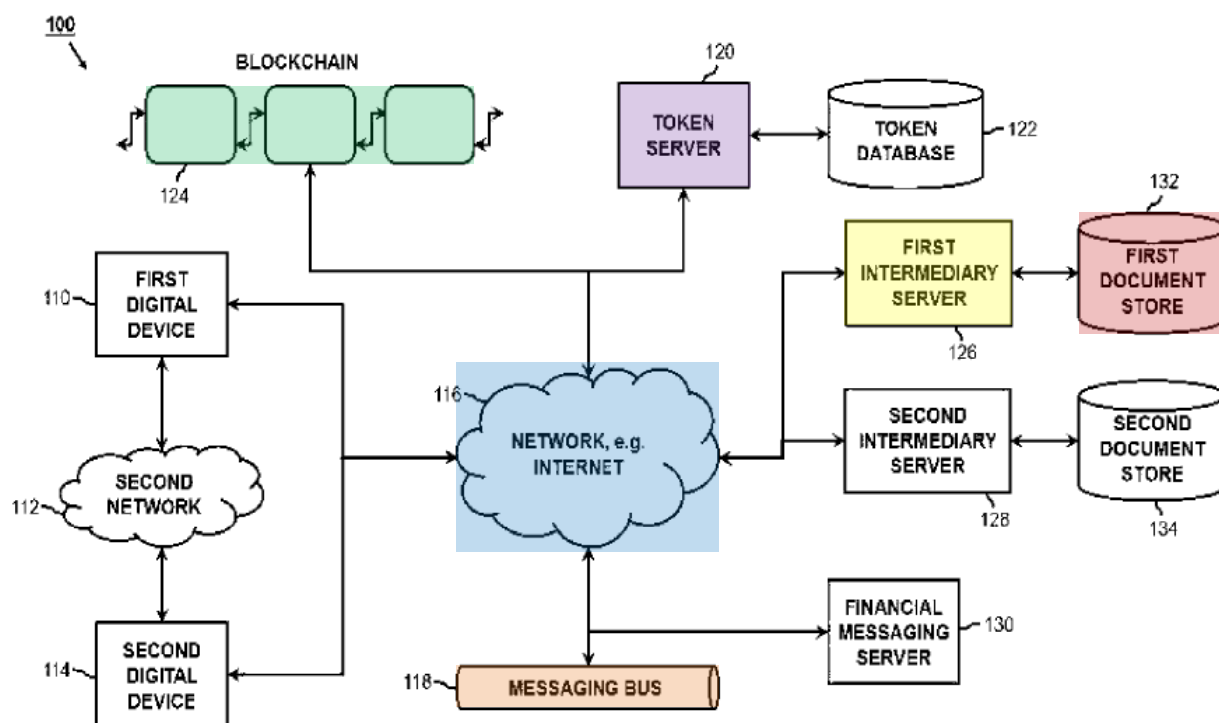
III. ’413 PATENT

A. Alleged Invention

The ’413 Patent takes conventional financial transactions and records them on a

generic blockchain. The '413 Patent purportedly addresses problems with “keep[ing] track of the plurality of data during the financial transaction,” stating that if there are “deficiencies in the plurality of data transmitted, time consuming checking and querying operations and correspondence often ensues before the financial transaction can be effected.” (Ex. 1001, 1:39-51).

Figure 1 shows a system for processing a financial transaction where a “first intermediary server” (yellow) connects with a “token server” (purple) and a “blockchain” (green) over a “network” (blue):



(*Id.*, Fig. 1).¹

¹ Colors added to Figures throughout, unless indicated otherwise.

The “first intermediary server” transmits “one or more documents pertaining to [a] financial transaction” to the “first document store.” (*Id.*, 18:20-23). An “enriched data record is generated from the one or more documents, at the first intermediary server.” (*Id.*, 18:31-32). The ’413 Patent explains that the “enriched data record” comprises “a plurality of attributes from the one or more documents.” (*Id.*, 2:36-41). The “enriched data record is added into the blockchain 124, from the first intermediary server.” (*Id.*, 18:33-34).

The “first intermediary server” requests, via a “messaging bus” (orange), the “token server” (purple) to “generate [a] token corresponding to the financial transaction.” (*Id.*, 18:63-65). The “token is added into the blockchain, from the token server.” (*Id.*, 18:66-19:1). The token is also “transmitted from the token server” to the first intermediary server and then stored in the “first document store” “in association with the one or more documents.” (*Id.*, 19:1-6). As a “pointer to an enriched data record,” the token can “retrieve the enriched data record at a time of an audit.” (*Id.*, 2:14-15, 28:66-29:3).

B. Prosecution History

The ’413 Patent issued from U.S. Application 15/752,711 (“’413 Application”), which claims priority to a date of August 14, 2015 applied herein. (Ex. 1001). Prosecution was brief. In a Non-Final Office Action, the Examiner rejected all claims as obvious. (Ex. 1002, 299-333). Rather than substantively amending the claims, Applicant argued that the elements of the independent claims distinguish over the prior

art. (*Id.*, 289-293). The Examiner issued a Notice of Allowability, noting that the “claim limitations can be found in prior art references” but the record prior art did not render obvious “the combination of claim elements.” (*Id.*, 239, 244). The ’413 Patent issued on April 21, 2021.

C. POSITA

A person of ordinary skill in the art at the time of the claimed invention (“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. (Ex. 1003, ¶ 46).

IV. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Prior Art

The prior-art references described below were not considered during prosecution of the ’413 Patent.

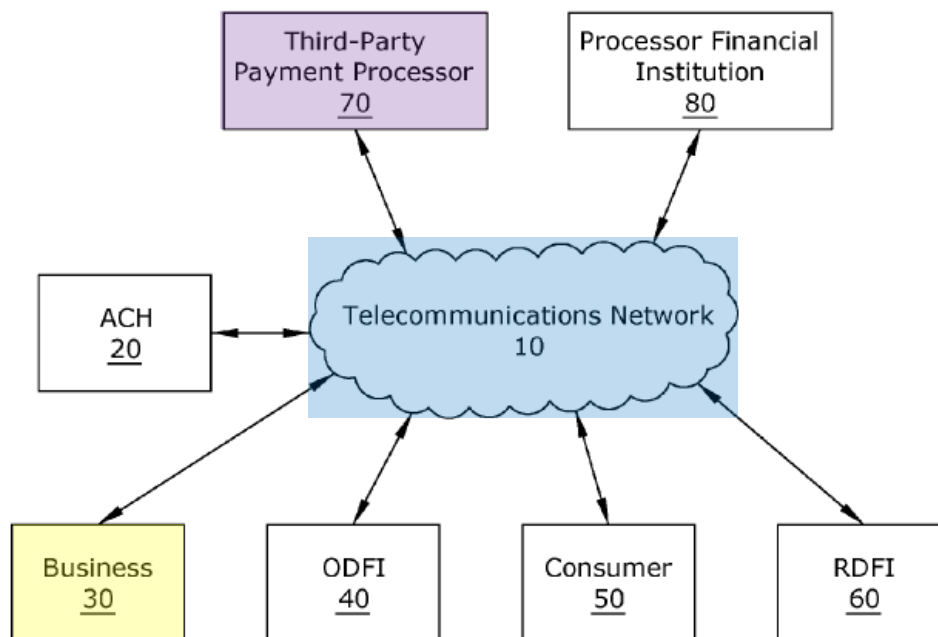
1. Smith

Smith, entitled “Electronic Funds Transfer Consumer Authorization Verification System,” was filed on September 17, 2014 and published on March 19, 2015. (Ex. 1004). Smith is prior art under at least Section 102(a)(1).

Smith describes “an electronic funds transfer consumer authorization verification system for efficiently proving that a consumer authorized a financial transaction via an

ACH network.” (*Id.*, [0004]). Smith explains that in traditional ACH (Automated Clearing House) systems, “the business is unable to attach the consumer’s authorization to the ACH transaction thereby inherently creating a risk for the business that the ACH transaction will be returned because the consumer (or another party) disputes that it was authorized.” (*Id.*, [0013]). Smith teaches an “improved ... system for efficiently proving that a consumer authorized a financial transaction via an ACH network.” (*Id.*, [0014]).

Smith teaches “accepting by a business 30 an authorization from a consumer 50 to debit and/or credit the consumer’s financial account in a specified amount via an ACH network, communicating the ACH detailed record for the ACH transaction along with a transaction data file from the business 30 to a third-party payment processor 70, and communicating to the business 30 a unique transaction key associated with both the ACH detailed record and the transaction data file.” (*Id.*, [0030]).



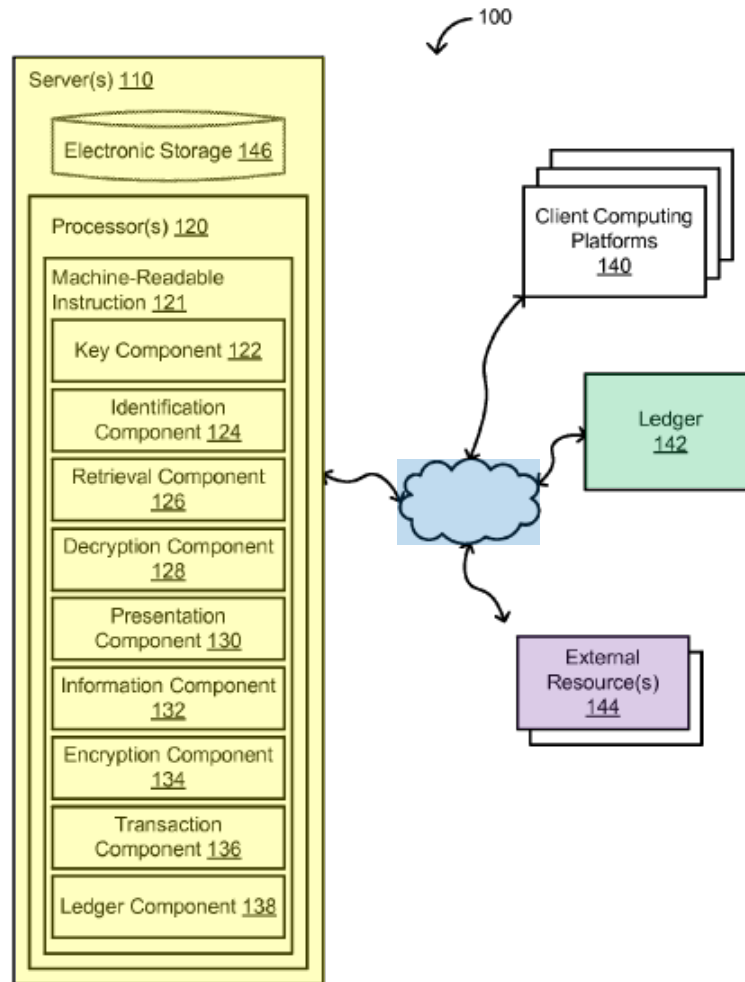
(*Id.*, Fig. 1). Smith’s Figure 1 shows “a plurality of electronic devices” including “devices for each entity” (such as “business 30,” “consumer 50,” and “third-party payment processor 70”) that “communicate via a single telecommunication network.” (*Id.*, [0031]). The business (yellow) to “sends one or more transaction data files to the third-party payment processor” (purple). (*Id.*, [0052]). The “third-party payment processor” then “updates its database to include a unique transaction key that is associated with the transaction data file(s) provided by the business.” (*Id.*, [0053]). The “business 30 and/or third-party payment processor 70 can easily identify and view the transaction data files associated with the ACH transaction using the transaction key,” and the “transaction can then be verified (or not verified) based upon the transaction data files.” (*Id.*, [0056]).

2. Seger

Seger, entitled “System And Method For Providing A Cryptographic Platform For Exchanging Information,” was filed on April 14, 2015. (Ex. 1005). Seger is prior art under at least Section 102(a)(2).

Seger provides “a cryptographic platform for exchanging information” that “enables confidential, verifiable, and immutable recording and/or reporting of information transactions.” (*Id.*, 1:7-8, 1:43-44). Seger’s system “enable[s] one or more auditors to audit the information transactions held within [a] distributed ledger.” (*Id.*, 7:10-12).

Seger’s Figure 1 shows “one or more servers 110” (yellow) that “communicate with client computing platform(s) 140 according to a client/server architecture.” (*Id.*, 4:31-33). Seger teaches a “distributed ledger” (green) to “provide a verifiable record of various information transactions, including various information payloads that include various encrypted information.” (*Id.*, 4:22-26). This “information may include and/or be associated with...financial data.” (*Id.*, 6:8-11).



(*Id.*, Fig. 1).

Seeger explains that “a record of all instances of the distributed ledger (e.g., a ledger chain, a ***blockchain***) is generated to provide a verifiable record of all instances of the distributed ledger.” (*Id.*, 10:23-26).² Seeger “enables confidential, verifiable, and immutable recording and/or reporting of information transactions including various

² Emphasis added throughout unless indicated otherwise.

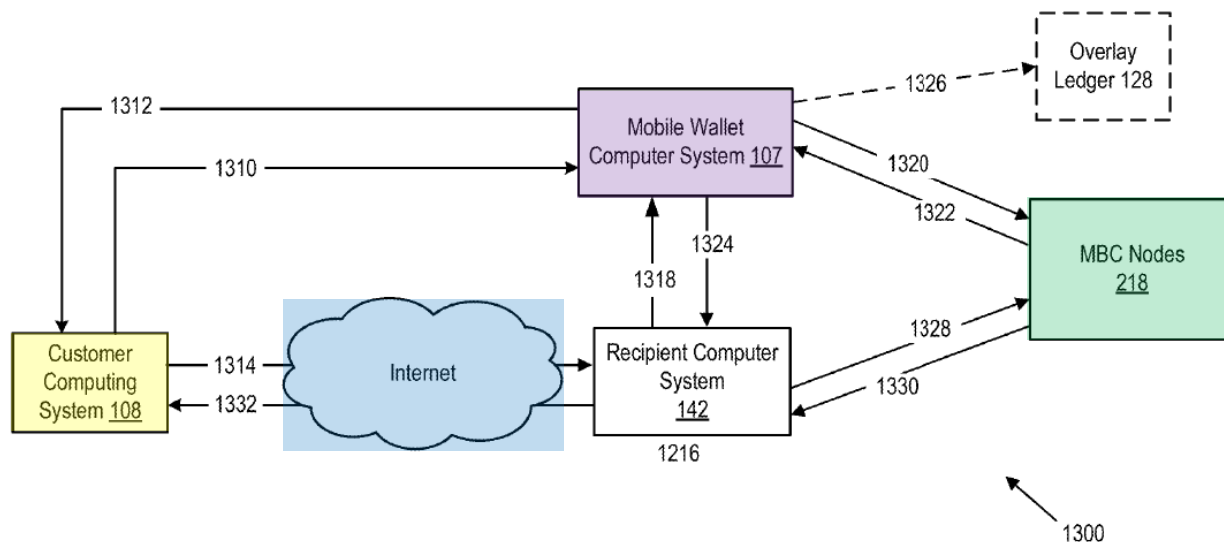
encrypted information (e.g., private communications) that may be audited by a third party.” (*Id.*, 1:43-46).

3. Kurani-274

Kurani-274, entitled “Mobile Wallet Using Math Based Currency Systems And Methods,” was filed on July 3, 2014. (Ex. 1007). Kurani-274 is prior art under at least Section 102(a)(2).

Kurani-274 discloses “banking systems and methods for a mobile wallet system implemented using math-based currency (“MBC”).” (*Id.*, 2:66-3:1). Kurani-274’s mobile wallet system “includes a code/token generator 131,” which “generates a code that is uniquely associated with the transaction.” (*Id.*, 5:45-46, 6:21-23).

In Kurani-274’s Figure 13, the code/token generator “receiv[es] a message from the customer computing system 108 to generate a token.” (*Id.*, 21:28-29). The system also communicates with MBC Nodes 218 (green) that publish transaction information “in a chain of transactions (i.e., a **blockchain**),” which allows verification “via the MBC nodes.” (*Id.*, 17:18-19, 21:17-18).



(*Id.*, Fig. 13).

4. Yago

Yago, entitled “Method For Creating, Issuing, And Redeeming Payment Assured Contracts Based On Mathematically And Objectively Verifiable Criteria,” was filed on January 13, 2015 and published on July 23, 2015. (Ex. 1011). Yago is prior art under at least Section 102(a)(1).

Yago’s system “allow[s] parties to transact with the guarantee of settlement upon completion of all elements for that trade.” (*Id.*, [0045]). Yago’s “payment assured contract” operates as follows: “buyers and sellers desire to perform a trade. The terms of their agreed trade define the criteria for a contract (which could be an automatically created digital contract). The contract is communicated to a credit issuer.” (*Id.*, [0046]). Yago adds the contract to a “CDI network” (*i.e.*, “a

blockchain”). (*Id.*, [0054], [0042], [0013]). A “payment issuer will be able to objectively (and automatically), confirm performance by the seller.” (*Id.*, [0047]).

B. Ground 1: Claims 1-2 And 5-20 Would Have Been Obvious Over Smith In View Of Seger

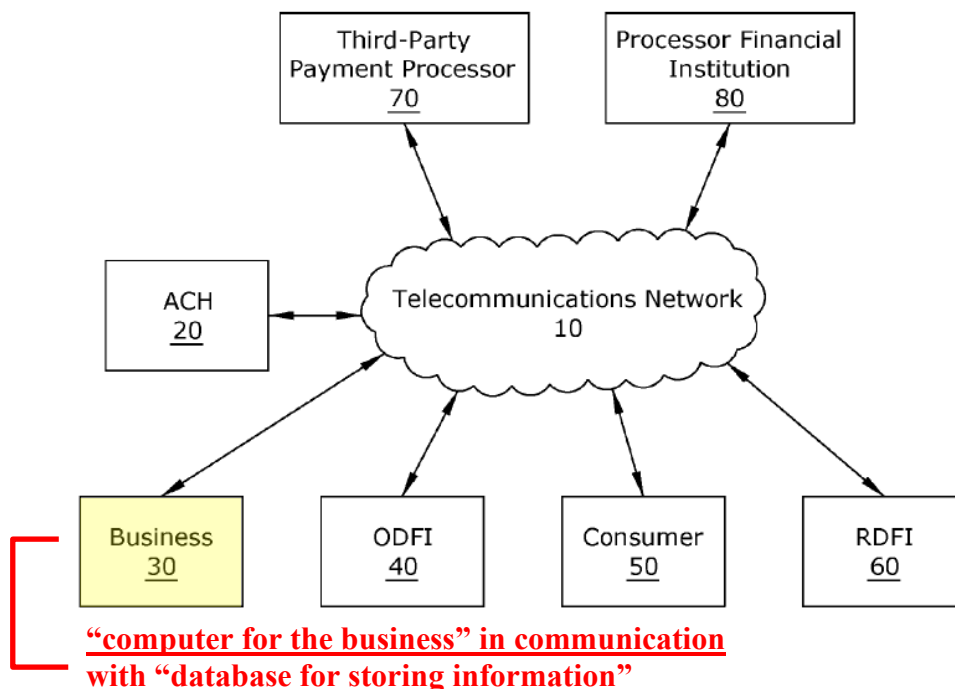
1. Claim 1

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

If the preamble is limiting, Smith discloses it. Smith describes “an electronic funds transfer consumer authorization verification system for efficiently proving that a consumer authorized a financial transaction via an ACH network.” (Ex. 1004, [0004]; Ex. 1003, ¶ 61).

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;

Smith, alone or in combination with Seger, discloses or renders this element obvious. Smith describes an “electronic funds transfer consumer authorization verification system” (*i.e.*, “centralised financial system”). (Ex. 1004, [0030]). Smith’s system includes “a computer for the business 30” (“business computer 30”) (*i.e.*, “first intermediary server”) connected with other entities and in communication with “a database that stores [] information for later access.” (Ex. 1004, [0031], [0034]).



(*Id.*, Fig. 1).

First, Smith discloses a “first intermediary server in a centralised financial system.” POSITA would have considered it obvious for Smith’s business computer 30 to be a server. (Ex. 1003, ¶¶ 64-67). POSITA would have understood that a server is a computer or program responding to commands from a client. (Ex. 1003, ¶ 65; Ex. 1006 (defining “server”)). Business computer 30 comprises “an electronic device capable of receiving, transmitting and storing electronic data.” (Ex. 1004, [0036]). Business computer 30 “receives the authorization for the ACH transaction and other required information from the customer 50” and provides “one or more transaction data files” to the TPPP 70. (*Id.*, [0048], [0047]). Smith further teaches that the various devices (*e.g.*, business computer 30) “can be implemented by special-purpose, hardware-based computer systems that perform the specified functions ... or combinations of special-

purpose hardware and computer instructions” (*Id.*, [0084]), which aligns with the ’413 Patent’s statement that a “computing device” may “take[] the form of the first intermediary server.” (Ex. 1001, 16:43-44).

POSITA would have understood that business computer 30 is a server that receives authorization and other information from the consumer and, through computer instructions, subsequently creates and transmits transaction data files to the TPPP. (Ex. 1003, ¶ 67). The business computer is also an intermediary between other devices, or a user on the business side and the authorization verification system. (*Id.*). POSITA would understand Smith discloses “a first intermediary server in a centralised financial system.” (*Id.*).

Should Smith alone be found not to disclose “a first intermediary server in a centralised financial system,” it would have been rendered obvious by Smith in view of Seger. (*Id.*, ¶¶ 68-69). Seger teaches “one or more servers 110” accessing a “system 100 configured for providing a cryptographic platform for exchanging information”. (Ex. 1005, 4:7-8, 4:31; Ex. 1003, ¶ 68). Seger explains that servers “communicate with client computing platform(s) 140 according to a client/server architecture.” (*Id.*, 4:32-34). For example, Seger’s system server 301 obtains “information” from a party, and using “one or more processors configured to execute a transaction component,” “generate[s]” an “information transaction.” (*Id.*, 13:38-39, 14:37-38, 14:48-58). System server 301 then “provide[s]” the “information transaction” to the distributed ledger 302. (*Id.*, 14:58-61).

In view of Seger's teachings, it would have been obvious to POSITA to implement Smith's business computer as a server, using a client/server architecture, to receive information from other entities in Smith's "telecommunications network," and generate transaction information for transmittal and storage on Seger's ledger, providing various advantages explained below for element 2. (Ex. 1003, ¶ 69). POSITA would have understood that using Seger's teachings with Smith's system would be accomplished by known methods (*i.e.*, client/server architecture), and yielding predictable results with no change in the components' respective functions. (*Id.*). Accordingly, POSITA would have found it obvious, in view of Seger, that Smith's business computer connects to the electronic funds consumer authorization verification system via a "first intermediary server." (*Id.*).

Second, Smith discloses "a first document store." Smith explains that during financial transactions, the business computer records "information received from the consumer 50 into a database that stores the information for later access" (*i.e.*, "first document store"). (Ex. 1004, [0034], [0036]; Ex. 1003, ¶ 70). The "database that stores the information for later access" is the claimed "first document store." (Ex. 1003, ¶ 70). This aligns with the '413 Patent's statements that a "document store" "represent[s] databases configured to store a plurality of documents." (Ex. 1001, 11:9-11).

Third, Smith discloses "one or more documents pertaining to the financial transaction." Smith teaches that information entered into the business computer's database includes financial transaction data including "the legal name of the consumer,

state of residency, residential address, amount of the credit or debit, a maximum amount for the credit or debit, a routing number for the financial institution...a checking/savings account number at the financial institution for the consumer...copy of driver's license, copy of Social Security card, picture taken of the consumer 50 by the business 30 and the like.” (Ex. 1004, [0034]). The business computer (*i.e.*, “first intermediary server”) is “utilized by the business to store...fund transfer information, payment information, purchase information, ACH payment information, ACH authorization” and more. (*Id.*, [0036]). Other information provided by the consumer to the business computer include “a complete ACH authorization agreement signed by the consumer 50, a statement by the consumer 50 authorizing the ACH transaction,” and “various other types of documents desirable for verifying a transaction.” (*Id.*, [0051]). POSITA would have understood this information provided by the consumer to the business computer constitutes “one or more documents pertaining to the financial transaction.” (Ex. 1003, ¶¶ 71-72).

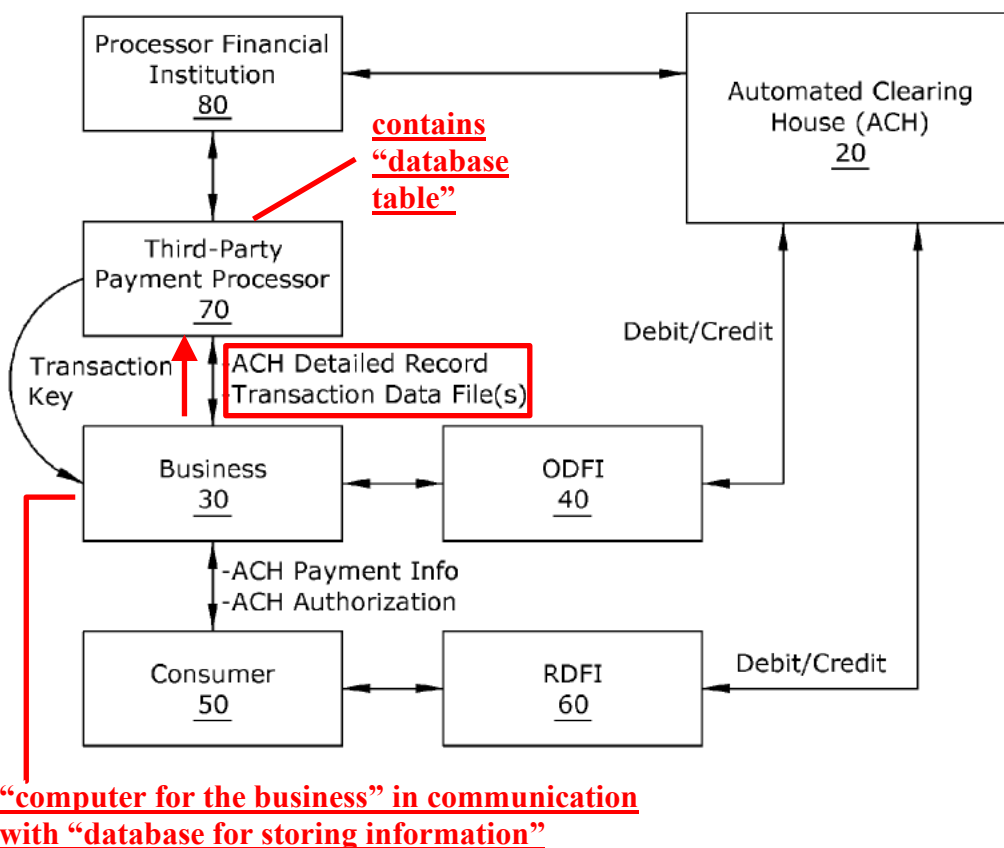
Finally, Smith discloses “transmitting one or more documents” from the “first intermediary server ... to the first document store.” (*Id.*, ¶¶ 73-75). Smith's business computer discloses or would have rendered obvious (in view of Seger) “a first intermediary server” that is “capable of receiving, transmitting and storing electronic data.” (Ex. 1004, [0036]; Ex. 1003, ¶ 73). When the consumer “provides various [] information required by the business” to execute a transaction, that information (*i.e.* “one or more documents”) is provided to the business computer 30. (Ex. 1004, [0034], Ex.

1003, ¶ 73). By recording “the information received from the consumer 50 into a database” (Ex. 1004, [0034]), the business computer (*i.e.*, “first intermediary server”) transmits the received information (*i.e.* “one or more documents”) to the database (*i.e.* “first document store”) for storage. (Ex. 1004, [0034], Ex. 1003, ¶¶ 73-75).

Accordingly, Smith discloses or renders obvious transmitting one or more documents pertaining to the financial transaction (financial transaction data and other information provided by the consumer to the business), from a first intermediary server (business computer 30) in a centralised financial system (Smith’s electronic funds transfer consumer authorization verification system) to a first document store (database in communication with business computer 30). (*Id.*, ¶ 75).

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;

The Smith/Seeger combination would have rendered this element obvious. Smith discloses that the business computer 30 transmits “ACH detailed record for the ACH transaction along with a transaction data file” to third-party payment processor 70, which stores them into a “database table” (Ex. 1004, [0022], [0030], [0041]).



(*Id.*, Fig. 2).

Smith discloses “generating an enriched data record from the one or more documents.” (Ex. 1003, ¶¶ 77-79). The ’413 Patent discloses exemplary “enriched data records,” such as, for example, “a plurality of attributes from the one or more documents. (Ex. 1001, 2:36-62). In Smith, both the transaction data file and ACH detail record comprise components of transaction information that are stored in the business computer’s database. (Ex. 1004, [0034-0036], [0046-0047], [0051]). Smith teaches that both the stored transaction information and the transaction data file may comprise a “copy of the driver’s license” and a “copy of the Social Security card.”

(*Id.*, [0034], [0051]). Similarly, the stored transaction information and ACH detail record both include “ACH payment information” and other data such as the consumer’s “name” and “account number.” (*Id.*, [0034-0036], [0046-0047]). Smith teaches that the business computer “communicat[es] the ACH detailed record for the ACH transaction along with a transaction data file from the business 30 to a third-party payment processor 70.” (*Id.*, [0030]).

POSITA would have understood both the ACH detail record and the transaction data file to be a collection of various “attributes” from the stored transaction information (*i.e.*, “one or more documents”) and, as such, is generated by the business computer (*i.e.*, “first intermediary server”) by “combin[ing] a plurality of attributes” of the one or more documents. (Ex. 1003, ¶ 79). POSITA would understand the ACH detail record and its corresponding transaction data file, individually and together, to be “an enriched data record” of the underlying financial transaction. (*Id.*). This aligns with ’413 Patent’s statement that “an enriched data record comprises...a plurality of attributes from the one or more documents.” (Ex. 1001, 2:36-41).

Smith further discloses “adding the enriched data record into a ... ledger.” Smith teaches storing “the ACH transaction detail record and the corresponding transaction data files in a database on a computer for the” TPPP 70. (Ex. 1004, [0041]). Smith’s Figure 5 shows that the database comprises a table maintaining a record of transactions (*i.e.*, “ledger”):

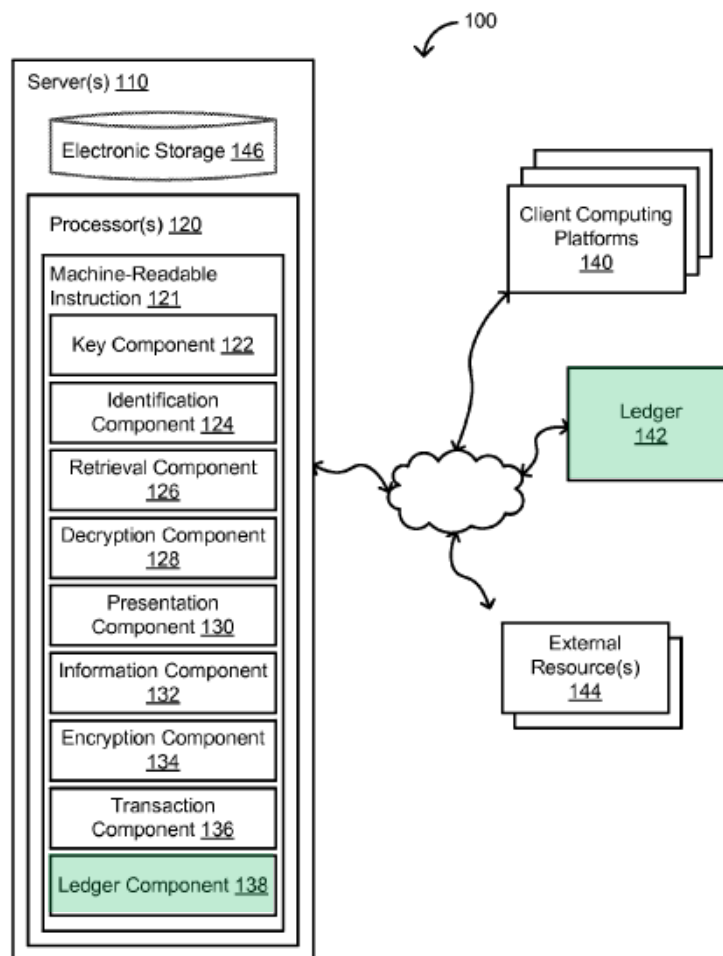
Transaction Key	ACH Transaction Detail Record	Transaction Data File(s)
ABCD1	Detail Record #1	-ACH Authorization File
ABCD2	Detail Record #2	-ACH Authorization File -Drivers License File -Social Security Card File
ABCD3	Detail Record #3	-ACH Authorization File -Business State Licenses File
ABCD4	Detail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

(Ex. 1004, Fig. 5; Ex. 1003, ¶ 80). Figure 5’s “database table” “illustrat[es] the connection of each ACH entry detail record with one or more consumer data files using a common transaction key.” (*Id.*, [0022]). Smith thus discloses adding “the enriched data record” (outlined in red) to a ledger. (Ex. 1003, ¶ 80).

While Smith does not explicitly disclose that its ledger is a blockchain distributed ledger, POSITA would have understood that using a blockchain ledger would be an obvious way for achieving Smith’s objective of providing a “verification system for efficiently proving that a consumer authorized a financial transaction via an ACH network.” (Ex. 1004, [0014]; Ex. 1003, ¶ 81). Indeed, Smith expressly contemplates the need to verify transactions “based upon the transaction data files” stored in the TPPP’s ledger (Ex. 1004, [0056]), but Smith is silent regarding a mechanism for verifying and ensuring the continued accuracy of that ledger. Seger discloses precisely

such a mechanism for providing a verifiable ledger via blockchain technology for tracking financial data. (Ex. 1005, 6:8-11). POSITA would have pursued a more all-encompassing verification system and turned to Seger which, as described below, identifies a blockchain as a means to provide a “verifiable, and immutable record[.]” (Ex. 1005, 1:43-44, Ex. 1003, ¶ 81). In such instances, “the effects of demands known to the design community or present in the marketplace” often provide “an apparent reason to combine [] known elements.” *KSR v. Teleflex*, 550 U.S. 398, 418 (2007).

In turn, Seger discloses adding data into a blockchain being a distributed ledger. Seger teaches that transaction information “may be provided to ledger 302 (e.g., the distributed ledger). The [transaction information] provided to ledger 302 may include the second information payload.” (Ex. 1005, 14:58-61). Seger’s Figure 1 shows that “intermediary servers 110” comprise a “ledger component 138...configured to provide one or more information transactions to the distributed ledger.” (*Id.*, 9:43-54).



(*Id.*, Fig. 1). Seger’s “distributed ledger may provide a verifiable record of all of the information exchanges including various information transactions including encrypted information,” including “a record of all instances of the distributed ledger (*e.g.*, a ledger chain, a blockchain) may be generated to provide a verifiable record of all instances of the distributed ledger.” (*Id.*, 10:20-26). Seger discloses “adding the enriched data record into a blockchain being a distributed ledger.” (Ex. 1003, ¶ 82).

It would have been obvious to POSITA to apply Seger’s blockchain ledger to Smith’s centralised financial system (Smith’s “electronic funds transfer consumer authorization verification system”) to add the enriched data record into a blockchain

being a distributed ledger (Seger's ledger 142), from the first intermediary server (Smith's business computer"). (Ex. 1003, ¶¶ 83-87).

Seger and Smith both provide systems for secure financial transactions. Seger teaches "a cryptographic platform for exchanging information" that includes "storing and exchanging transaction-specific payment tokens; facilitating remittance services; [and] reconciling accounts across disparate entities...." (Ex. 1005, 3:6-15). Smith teaches "an electronic funds transfer consumer authorization verification system for efficiently proving that consumer authorized a financial transaction via an ACH network." (Ex. 1004, [0004]). Seger and Smith address similar problems. Seger relates to "confidential, verifiable, and immutable recording and/or reporting of information transactions...that may be audited by a third party." (Ex. 1005, 1:42-46). Smith addresses the need for "efficiently proving that a consumer authorized a financial transaction via an ACH network." (Ex. 1004, [0014]). Seger and Smith apply similar approaches to address similar issues. Seger teaches "a record of all instances of the distributed ledger (e.g., a ledger chain, a blockchain) may be generated to provide a verifiable record" of all transactions. (Ex. 1005, 10:20-31). Smith teaches a database storing transaction data such that "[i]f there is a dispute as to the validity of the ACH transaction [entities] can easily identify and view" the transaction data. (Ex. 1004, [0041], [0056]). Thus, both Smith and Seger use transaction logs or records to verify transaction integrity. (Ex. 1003, ¶ 84).

"[L]ook[ing] to interrelated teachings of multiple patents" often provides "an

apparent reason to combine” known elements because “in many cases a [POSITA] will be able to fit the teachings of multiple patents together like pieces of a puzzle.” *KSR*, 550 U.S. at 418, 420. The same is true here. POSITA would have found it obvious to use a blockchain ledger as taught in Seger because it offers the advantage of providing an “immutable” record, ensuring that transaction data cannot be altered once written. (Ex. 1003, ¶ 85). POSITA would have been motivated to apply Seger’s teaching to Smith to include the well-known benefits of a blockchain that allows entities to verify the TPPP’s transaction information against an immutable record, thereby enabling quick detection of any data alterations and providing the specific benefit of ensured integrity and accuracy of the system data if the TPPP were compromised. (*Id.*).

Before the ’413 Patent’s filing date, POSITA would have understood that using distributed ledgers and blockchain for recordkeeping was conventional. (Ex. 1008, 2 (blockchain “proponents say it is the most secure record-keeping technology ever devised”); Ex. 1009, 1 (“Blockchain...provides a secure and transparent platform for recording and verifying transactions....The immutable nature of blockchain ensures that every transaction and movement of goods can be recorded and tracked in real-time.”); Ex. 1010, 29-37 (companies using permissioned distributed ledgers for recordkeeping)). Thus, applying blockchain to Smith’s system involved the predictable use of prior-art elements—Smith’s “consumer authorization verification system” and Seger’s blockchain technology—according to their established functions. (Ex. 1003, ¶ 86).

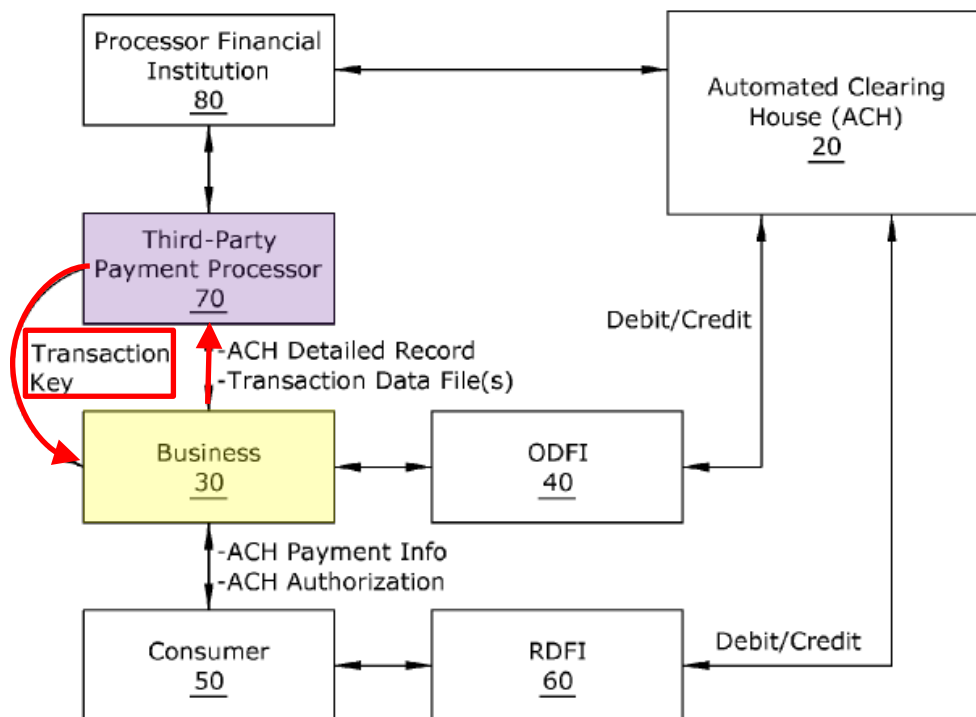
POSITA would have reasonably expected success in applying blockchain to

Smith's system. Seger describes well-known blockchain ledgers that "provide a verified record" of transactions, including "the Ripple® Protocol, the 'mining' proof of work protocol implemented by Bitcoin and/or other public consensus protocols." (Ex. 1005, 10:1-4). These examples were well-known to POSITA. (Ex. 1003, ¶ 86). Combining Seger and Smith involves well-understood and predictable technologies yielding predictable results. (*Id.*; *KSR*, 550 U.S. at 416).

Thus, the Smith/Seger combination discloses or renders obvious generating an enriched data record (Smith's ACH detail record and transaction data file) from one or more documents, at the first intermediary server (Smith's business computer 30), and adding the enriched data record into a blockchain being a distributed ledger (Smith's system as combined with Seger's teaching relating to blockchain ledger 142), from the first intermediary server. (*Id.*, ¶ 87).

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;

Smith discloses or renders obvious this element. Smith discloses that in response to the business computer 30 sending the ACH detailed record and transaction data file to the third-party payment processor 70, the third-party payment processor 70 generates a "unique transaction key" associated with both the ACH detailed record and transaction data file. (Ex. 1004, [0041], [0053]).



(*Id.*, Fig. 2).

In doing so, Smith discloses “a token corresponding to the financial transaction to identify the one or more documents.” Smith teaches the TPPP “determines what the *unique transaction key* is for each ACH transaction that corresponds to one or more transaction data files” and generates the “unique transaction key for each ACH transaction.” (*Id.*, [0041]). Because it “associate[s] the ACH transaction entry detail record with one or more transaction data files” (*Id.*, [0047]), Smith’s “unique transaction key” is a pointer to the ACH transaction entry detail record and transaction data files (*i.e.*, “enriched data record”). (Ex. 1003, ¶ 90). Further, Smith discloses “[t]he transaction key may be comprised of any format capable of identifying the ACH transaction separately from other ACH transactions” including “letters, numbers,

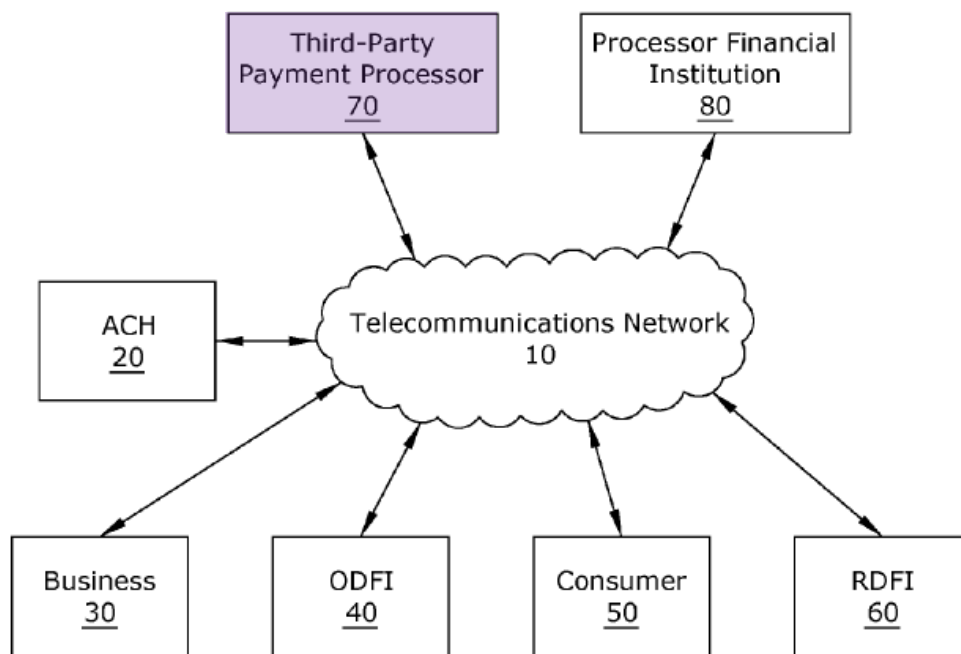
characters” and the like. (Ex. 1004, [0030], [0055]).

POSITA would have understood Smith’s “transaction key” as the claimed “token.” (Ex. 1003, ¶¶ 89-91). POSITA would also understand that because Smith’s transaction key is a “unique” key “for each ACH transaction” (Ex. 1004, [0041]), it identifies information relating to the transaction stored by the business computer (*i.e.*, “one or more documents”). (Ex. 1004, [0034-0036]; Ex. 1003, ¶ 91). By the ’413 Patent’s filing date, generating a unique identifier for a transaction by applying a predetermined algorithm to some or all of the transaction data was well-known. (Ex. 1003, ¶ 92; *see, e.g.*, Ex. 1007, 6:28-33 (generating “a code that is uniquely associated with a transaction” by “including a combination of random digits and a portion of a payment card number”); Ex. 1018, [0006], [0019] (generating a token by “substitut[ing]” a string of characters for an input string of characters”).

POSITA would have known that Smith’s “unique” key “capable of identifying” an ACH transaction could be generated using transaction data as an input into an algorithm to generate an identifying output in the form of “letters, numbers, and characters” and the like. (Ex. 1003, ¶ 92). POSITA would have understood that ensuring the uniqueness of the transaction key can avoid the known problem of “collision” (*i.e.*, identical keys for more than one transaction), and one way to achieve uniqueness is via generic data manipulation processes that use transaction data as an input to an algorithm in order to generate a unique output. Doing so would have mitigated the risk of collision and would have been obvious to POSITA. (*Id.*, ¶ 93).

Thus, Smith's transaction key aligns with the '413 Patent's statement that a "token is a pointer to an enriched data record of a plurality of data...rendered, formatted or passed through an algorithm in a predetermined manner." (Ex. 1001, 28:66-29:3). Accordingly, it would have been obvious to POSITA to generate Smith's transaction key (*i.e.*, "token") in this manner, to effectuate Smith's goal of achieving a transaction key that is "unique" and "capable of identifying" the transaction. (Ex. 1003, ¶¶ 89-94).

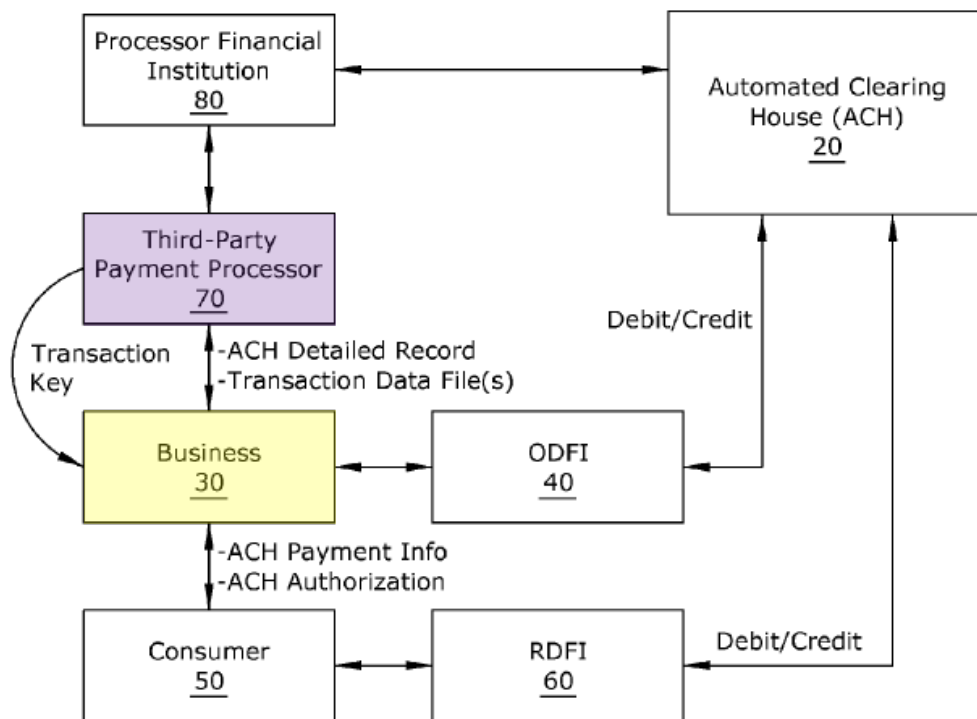
Smith further discloses a "token server." Smith teaches the "unique transaction key" (*i.e.*, "token") is generated by a "third-party payment processor [TPPP]" (*i.e.*, "token server"). (Ex. 1004, [0041]). Smith's Figure 1 shows the TPPP "communicates with [other devices] via one or more networks." (*Id.*, [0031]).



(*Id.*, Fig. 1). The TPPP performs actions like generating a transaction key in response

to communications from other computers on the network, and is therefore “a server.” (Ex. 1003, ¶ 95). Because the TPPP generates this unique transaction key (*i.e.*, “token”), the POSITA would understand the TPPP to comprise a “token server.” (*Id.*).

Smith further discloses requesting generation of a token, sent “to a token server, from the first intermediary server.” Smith explains that after receiving the transaction data record and ACH detail record, the TPPP “updates its database to include a unique transaction key that is associated with the transaction data file(s) provided by the business 30.” (Ex. 1004, [0053]). Smith’s Figure 2 shows that the TPPP “transmits the transaction key to the business 30 for use when the business 30 sends the ACH transaction detail record.” (*Id.*).



(*Id.*, Fig. 2). Because the TPPP generates and returns the “unique transaction key” (*i.e.*

“token”) in response to receiving communications from the business computer 30 (*i.e.*, “first intermediary server”), POSITA would have understood these communications as the first intermediary server “requesting generation of a token.” (Ex. 1003, ¶¶ 96-97).

Smith discloses or renders obvious requesting generation of the token “via a messaging bus.” Smith teaches communicating data between various computing devices through telecommunications networks. (Ex. 1004, Fig. 1, [0032]). Smith explains that the business computer “provides the transaction data files to the [TPPP] 70 by a secure telecommunication network.” (*Id.*, [0050]). This aligns with the ’413 Patent’s statement that “bus” “should be construed...as any system for communicating data.” (Ex. 1001, 33:35-45). Smith discloses or renders obvious “requesting...via a messaging bus.” (Ex. 1003, ¶¶ 98-99).

Accordingly, the Smith/Seeger combination discloses or renders obvious requesting generation of a token (Smith’s unique transaction key) corresponding to the financial transaction to identify one or more documents, to a token server (third-party payment processor), from the first intermediary server (business computer), via a messaging bus in the centralised financial system. (*Id.*, ¶ 100).

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;

The Smith/Seeger combination would have rendered this element obvious.

Smith teaches the TPPP (*i.e.*, “token server”) “updates its database to include a unique transaction key” that “is associated with the transaction data file(s) provided by

the business 30.” (Ex. 1004, [0053]).

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

(*Id.*, Fig. 5).

Smith discloses “generating the token at the token server.” (Ex. 1003, ¶ 102). As described above for element 3, the TPPP generates the “unique transaction key []” for each ACH transaction” (*i.e.*, “token”). (Ex. 1004, [0041]).

Smith further discloses “adding the token into” a record, “from the token server, in association with the enriched data record.” Smith’s Figure 5 above shows a “database table” using “a simple transaction key for both an ACH transaction detail record and the transaction data file(s).” (*Id.*). Smith teaches that the TPPP “stores the transaction key, the ACH transaction detail record and the corresponding transaction data files in a database.” (*Id.*). POSITA would have understood that the TPPP (*i.e.*, “token server”) generates the “transaction key” (purple) (*i.e.* “token”) and “updates its database to include [the] unique transaction key” (*Id.*, [0053]) in association with the transaction

records (yellow) (*i.e.*, “enriched data record”). (Ex. 1003, ¶ 103).

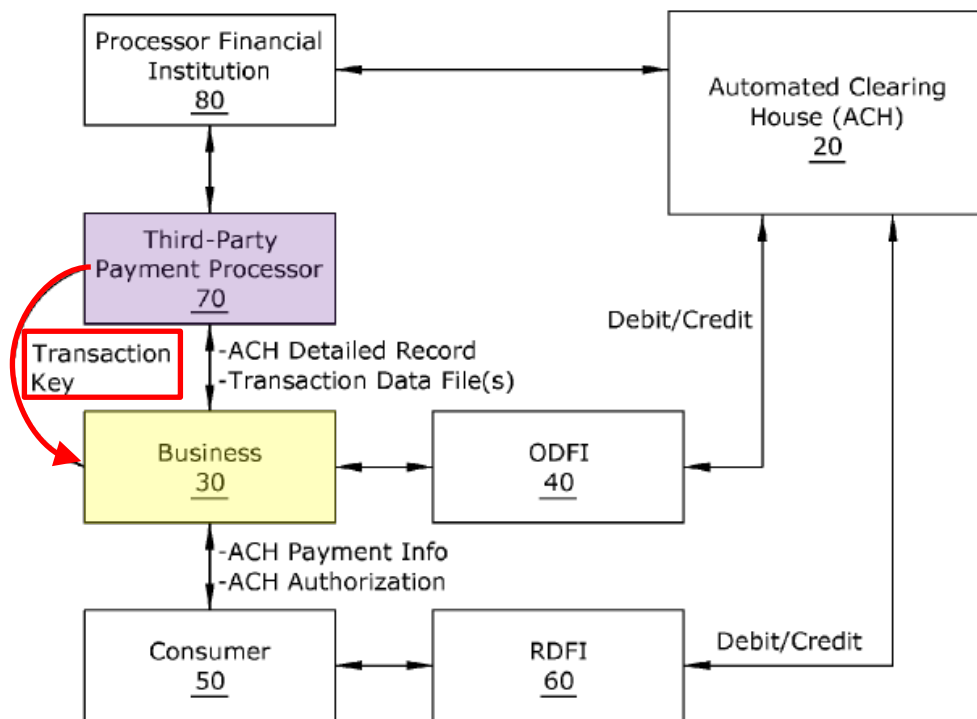
Smith discloses the entirety of this element except for “the blockchain.” As explained for element 2, applying Seger’s teaching of a blockchain to Smith’s authorization verification system would have been obvious to POSITA. For Smith’s transaction key, POSITA would have recognized that having the TPPP (which generated the key) add the key to the blockchain would help ensure the accuracy and integrity of the transaction key. (*Id.*, ¶¶ 104-105). POSITA would have been motivated to do so given Smith’s teaching to use transaction keys to resolve “dispute[s] as to the validity of the ACH transaction,” including using the key to “easily identify and view the transaction data files.” (Ex. 1004, [0056]). Smith explains the importance of the transaction key: “if no transaction key is provided by the business 30, then the transaction is declined and returned to the business 30.” (*Id.*, [0057]). Thus, adding the transaction key (*i.e.*, “token”) into the blockchain from the TPPP (*i.e.*, “token server”) would have been obvious to POSITA. (Ex. 1003, ¶¶ 104-06).

The Smith/Seeger combination would have rendered obvious generating the token (Smith’s unique transaction key) at the token server (TPPP) and adding the token into the blockchain from the token server (TPPP as combined with Seger’s teaching relating to blockchain ledger 142) in association with the enriched data record. (*Id.*, ¶ 107).

Element 5: transmitting the token to the first intermediary server from the token server, via the messaging bus.

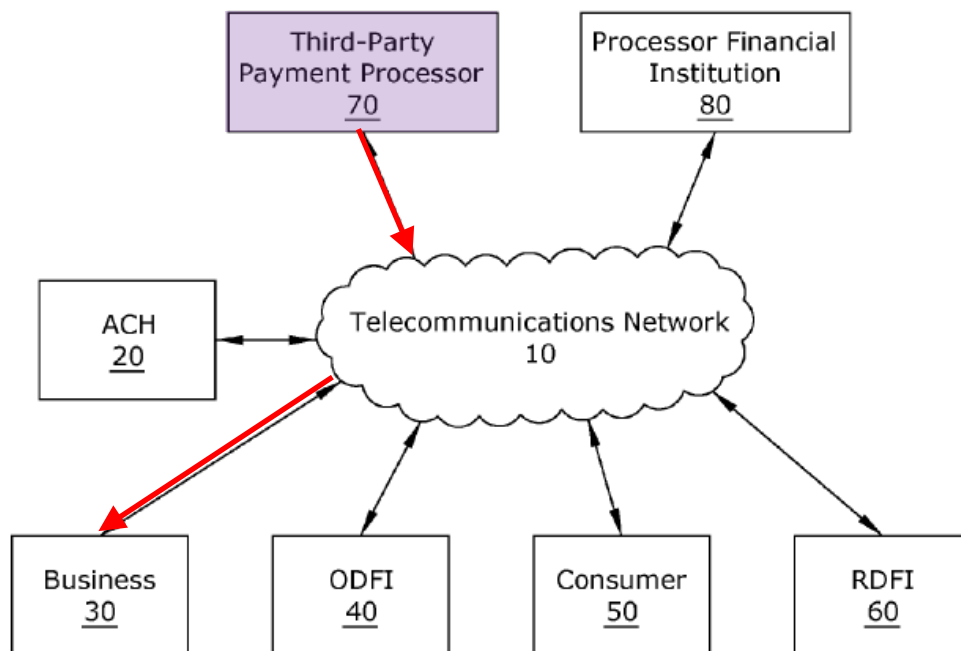
Smith discloses or would have rendered obvious this element.

Smith teaches that the TPPP “provides the transaction key to the business 30 after receiving the ACH transaction detail record for the business 30 to use with any transaction data files uploaded to the third-party payment processor.” (Ex. 1004, [0041]).



(*Id.*, Fig. 2).

Figure 1 shows the TPPP communicating with the business computer via a “telecommunications network” (*i.e.*, “messaging bus”).



(*Id.*, Fig. 1). If Smith does not disclose transmission via the messaging bus, this would have been obvious to POSITA from Smith’s teachings as explained for element 3. (Ex. 1003, ¶¶ 108-09).

Thus, Smith discloses or renders obvious transmitting the token (unique transaction key) to the first intermediary server (business computer 30) from the token server (TPPP), via the messaging bus.

Element 6: transmitting the token from the first intermediary server to the first document store in association with the one or more documents.

Smith discloses or would have rendered obvious this element.

As explained for element 1, Smith teaches that “business 30 enters the information received from the consumer 50 into a database that stores the information

for later access.” (Ex. 1004, [0034]). The TPPP “passes back a unique transaction key to the business 30 that is associated with both the ACH transaction (including the ACH transaction detail record) and the transaction data file(s).” (*Id.*, [0058]). POSITA would have found it obvious for the business computer (*i.e.*, “first intermediary server”) to transmit the transaction key (*i.e.*, “token”) to the database (*i.e.*, “first document store”) in “association with the one or more documents.” (Ex. 1003, ¶ 111). POSITA would have been motivated to allow the business computer to store the transaction key “for later access,” for example, to later send to other entities or to recall transaction information to compare against the TPPP’s record. (Ex. 1004, [0034], [0041]; Ex. 1003, ¶ 111). Including the transaction key (*i.e.*, “token”) in such communications would allow the receiving entity to easily identify the transaction to which the communication pertains. (Ex. 1003, ¶ 111).

Accordingly, Smith discloses or renders obvious transmitting the token (transaction key) from the first intermediary server (business computer 30) to the first document store (database in communication with business computer 30) in association with one or more documents.

2. Claim 2

Claim 2 depends from claim 1, reciting “sending a first financial message comprising the token, from the first intermediary server to a second intermediary server in the centralised financial system, indicative of making a payment to a second user.” The Smith/Seeger combination would have rendered claim 2 obvious.

Smith explains that the transaction key (*i.e.*, “token”) is communicated to the business computer (*i.e.*, “first intermediary server”) “so the business 30 (or any third-party the business gives the transaction key to such as the RDFI 60 or the ODFI 40) can access the ACH detail record and the transaction data files associated with the ACH detail record.” (Ex. 1004, [0041]). In “giv[ing] the transaction key” to other parties, the business computer “send[s] a first financial message comprising the token from the first intermediary server to a second intermediary server in the centralized financial system” as claimed. (Ex. 1004, [0041]; Ex. 1003, ¶ 114).

The transaction key is “unique...for each ACH transaction.” (Ex. 1004, [0047]). Smith explains to process each transaction, “[t]he ODFI 40 has a financial account for the business 30 [] where funds may be transferred to and from...Each financial account has a financial institution routing number and account number associated with it for facilitating the transfer of funds to and from.” (*Id.*, [0037]). In Smith, the “automated clearing house 20 (e.g. Federal Reserve) credits/debits the ODFI 40 and debits/credits the RDFI 60 accordingly to transfer the funds as requested by the ACH authorization by the consumer 50.” (*Id.*, [0055]). Thus, the transaction key (*i.e.*, “token”) is associated with an ACH transaction that indicates payment from the business to a consumer (*i.e.*, “second user”). (*Id.*, [0047], [0055]; Ex. 1003, ¶ 115). POSITA would have understood that by giving the transaction key (*i.e.*, “token”) to the ODFI (*i.e.*, “second intermediary server”), the business computer (*i.e.*, “first intermediary server”) informs the ODFI about the ACH transaction, and therefore this message is “indicative of a making

payment to a second user.” (Ex. 1003, ¶ 115).

3. Claim 5

Claim 5 depends from claim 1, reciting “generating the enriched data record comprises: extracting a plurality of attributes from the one or more documents, at the first intermediary server; and combining the plurality of attributes to generate the enriched data record, at the first intermediary server.” The Smith/Seeger combination would have rendered claim 5 obvious. (Ex. 1003, ¶¶ 118-19).

First, Smith discloses or would have rendered obvious “extracting a plurality of attributes from the one or more documents, at the first intermediary server.” As explained for element 2, Smith describes “transaction data files” and “ACH transaction detail records.” (Ex. 1004, Fig. 5). Smith teaches that the “entry detail record in the ACH batch file includes various fields such as record type code, transaction code, identification of RDFI 60, identification of the ODFI 40, check digit, DFI account number, funds transfer amount, individual identification, individual name...addenda record indicator and trace number.” (*Id.*, [0047]).

Smith teaches “[t]he ACH file is an electronic data file that stores the entry detail records for the ACH transactions. Each ACH detail record corresponds to an ACH transaction for the business 30.” (*Id.*, [0043]). Smith explains “a single ACH file holds one or more electronic transactions.” (*Id.*, [0045]). Thus, Smith’s business computer uploads a single ACH detail record associated with each individual transaction to the TPPP. (Ex. 1003, ¶ 119). As explained for element 2, this ACH detail record, together

with the transaction data file, forms the “enriched data record.” (*Id.*, ¶¶ 119, 77-80). The ACH transaction detail record comprises various fields (*i.e.*, “attributes”) that are extracted from the underlying ACH transaction information (*i.e.*, “document”) in the process of generating the ACH detail record and transaction data file (*i.e.*, “enriched data record”). (Ex. 1004, [0047]).

Smith also teaches gathering a plurality of additional information pertaining to the transaction 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.” (Ex. 1004, [0052]). POSITA would have understood this additional information as comprising “attributes” that the business computer (*i.e.*, “first intermediary server”) extracts from the documents pertaining to the underlying financial transaction stored in the business computer's database. (*Id.*, [0034]; Ex. 1003, ¶ 120).

Second, Smith discloses or would have rendered obvious “combining the plurality of attributes to generate the enriched data record, at the first intermediary server.” (Ex. 1003, ¶ 121). Smith teaches that “the business 30 uploads the ACH transaction detail record...[and] at the same time upload[s] the corresponding transaction data file(s) associated with the ACH transaction detail record.” (Ex. 1004, [0048]). The business computer (*i.e.*, “first intermediary server”) thus combines the attributes of the ACH detail record with the attributes of the transaction data file into a single transmission to generate an “enriched data record” communicated to the TPPP. (Ex. 1003, ¶ 121). If the Board

does not find that uploading “at the same time” teaches “combining” the ACH detail record and transaction data file, POSITA would have found it obvious to do so because combining these two files into one transmission would have simplified and reduced the latency of the information transfer process. (Ex. 1003, ¶ 121).

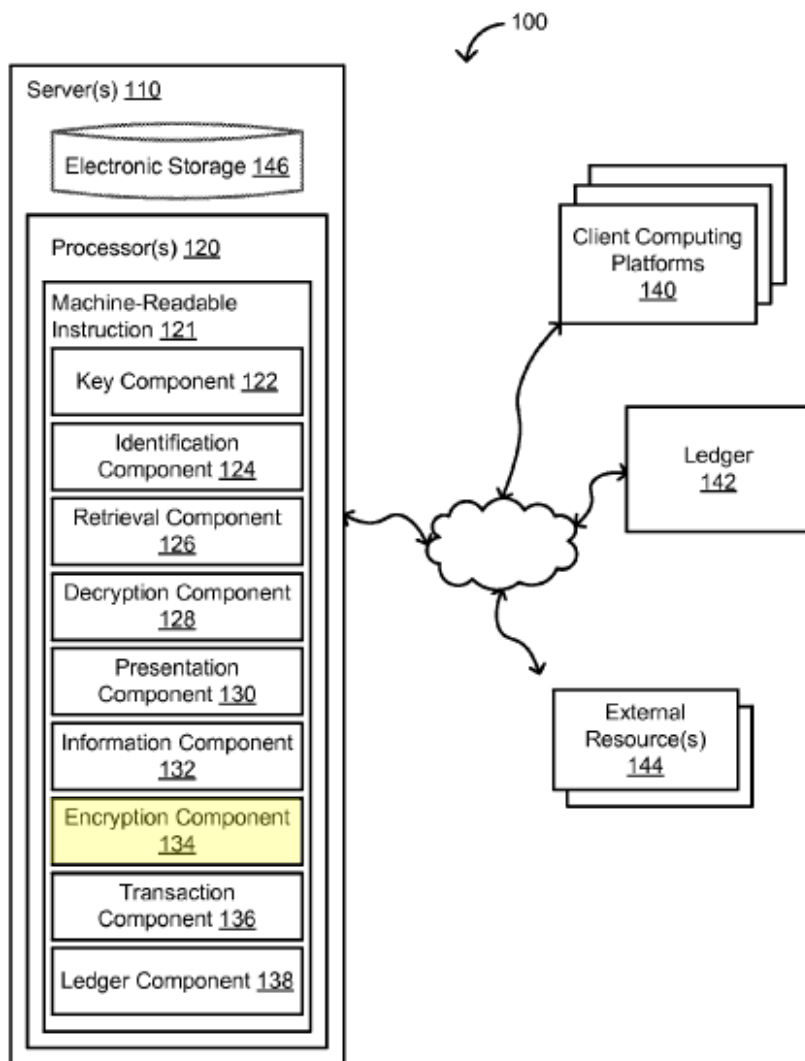
4. Claim 6

Claim 6 depends from claim 1, reciting “generating the enriched data record comprises: extracting a plurality of attributes from the one or more documents, at the first intermediary server; de-identifying the plurality of attributes to obtain a plurality of de-identified attributes, at the first intermediary server; and combining the plurality of de-identified attributes to generate the enriched data record, at the first intermediary server.” The Smith/Seeger combination would have rendered claim 6 obvious.

First, Smith discloses or would have rendered obvious the steps of “extracting” and “combining” as explained for claim 5.

Second, while Smith does not explicitly disclose “de-identifying the plurality of attributes to obtain a plurality of de-identified attributes, at the first intermediary server,” this element would have been obvious in view of Seeger. (Ex. 1003, ¶¶ 124-126). Seeger teaches that the “information transaction that may be held within the distributed ledger” includes encrypted information. (Ex. 1005, 6:1-24). The first encrypted information may be encrypted with “a first public key associated with the first party.” (*Id.*, 6:15-18). Seeger teaches server(s) 110 (*i.e.*, “first intermediary server”) comprise “encryption component 134 [which] may be configured to communicate with key component 122 to

obtain one or more public keys associated with one or more given parties. The one or more public keys obtained may be used to encrypt second information and/or other information intended for the given parties.” (*Id.*, 8:43-48).



(*Id.*, Fig. 2). POSITA would have understood that by encrypting the information payload, the attributes are “de-identified” by the “encryption component” of Seger’s servers. (Ex. 1003, ¶¶ 124-125).

It would have been obvious to POSITA to apply encryption as taught by Seger to

Smith's ACH detail record and transaction data files (*i.e.*, "enriched data record") added to the blockchain such that the attributes are "de-identified." (Ex. 1003, ¶ 126). Smith notes that transaction data is "sensitive information" such that the system "maintains the highest level of compliance and encryption." (Ex. 1004, [0059]). POSITA would have found it obvious to use Seger's teachings to protect Smith's "sensitive information" by ensuring "only authorized parties may read [] the communication and/or data." (Ex. 1005, 1:15-16; Ex. 1003, ¶ 126). As explained for claim 5, Smith discloses or would have rendered obvious combining the ACH detail record and transaction data file into a single transmission. (Ex. 1003, ¶¶ 126, 121). POSITA similarly would have found it obvious in the Smith/Seger combination to send a single transmission with the encrypted data and that would have rendered obvious "combining the plurality of de-identified attributes to generate the enriched data record." (*Id.*).

5. Claim 7

Claim 7 depends from claim 1, reciting "generating the enriched data record comprises: extracting a plurality of attributes from the one or more documents, at the first intermediary server; hashing the plurality of attributes to generate a plurality of respective hashes, at the first intermediary server; and combining the plurality of hashes to generate the enriched data record, at the first intermediary server." The Smith/Seger combination would have rendered claim 7 obvious.

First, Smith discloses or would have rendered obvious the steps of "extracting" and "combining" as explained for claim 5. (Ex. 1003, ¶ 129). *Second*, while Smith does

not explicitly disclose “hashing the plurality of attributes to generate a plurality of respective hashes, at the first intermediary server,” this element would have been obvious in view of Seger. (*Id.*, ¶ 130). As explained for claim 6, Seger discloses encrypting an information payload. (*Id.*, ¶ 131).

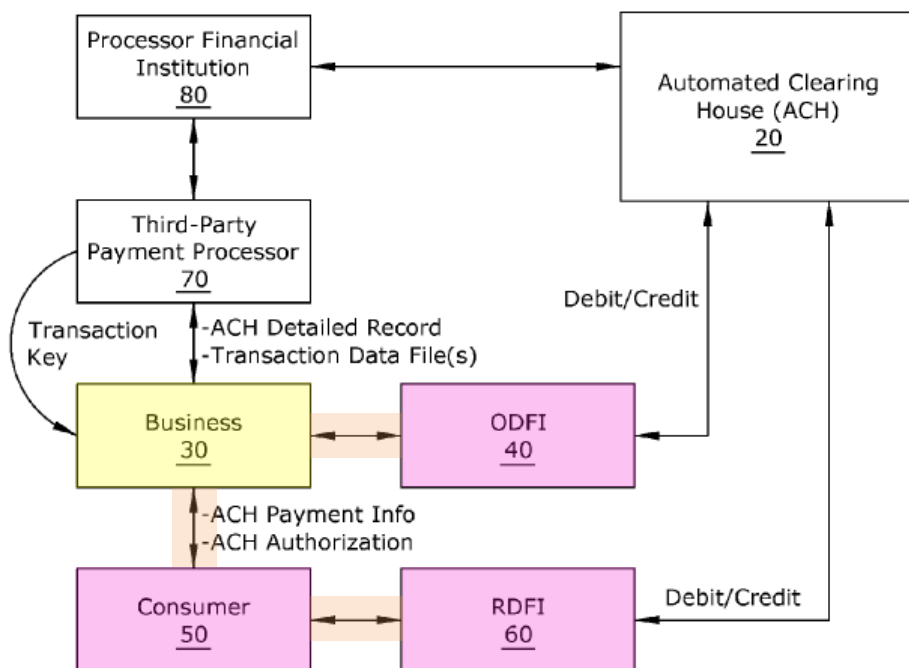
Seger teaches generating “a hash of the first information payload enabling auditing of the information transferred to the first party and stored within the block chain.” (Ex. 1005, 15:44-47). This hash can “verify an integrity of the first information transaction.” (*Id.*, 18:1-2). Accordingly, it would have been obvious to POSITA to hash the plurality of Smith’s attributes to maintain “secure private communication between multiple parties” while providing a means “to verify an integrity” of transaction information. (*Id.*, 1:40-41, 18:1; Ex. 1003, ¶ 131).

6. Claim 8

Claim 8 depends from claim 1, reciting “transmitting one or more first requests, each comprising the token, from the first intermediary server to a second intermediary server in the centralised financial system, via the messaging bus; receiving the one or more first requests at the second intermediary server and transmitting the one or more first requests and the token from the second intermediary server to a second document store; generating one or more first responses, each comprising the token, corresponding to the respective one or more first requests, at the second intermediary server; transmitting the one or more first responses from the second intermediary server to the first intermediary server, via the messaging bus; hashing the one or more first requests

and the one or more first responses at the second intermediary server to generate one or more first request hashes and one or more first response hashes, respectively; adding the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain, from the second intermediary server; and receiving the one or more first responses at the first intermediary server and transmitting the one or more first responses to the first document store.” The Smith/Seeger combination would have rendered claim 8 obvious.

First, Smith teaches the TPPP “communicates the transaction key to the business 30 via the network so the business 30 (or any third-party the business 30 gives the transaction key to ...) can access the ACH detail record and the transaction data files associated with the ACH detail record.” (Ex. 1004, [0041]). Figure 3 shows the business computer (*i.e.*, “first intermediary server”) communicating with computers of other entities (*i.e.*, “second intermediary server”) via a communication network (*i.e.*, “messaging bus”):



(*Id.*, Fig. 3).

POSITA would have understood that by “giv[ing] the transaction key” (*i.e.*, “token”) to other entities on the network (*i.e.*, “second intermediary server”), the business computer (*i.e.*, “first intermediary server”) transmits messages “each comprising the token, from the first intermediary server to a second intermediary server in the centralised financial system.” (Ex. 1003, ¶ 135). As explained for element 3, it would have been obvious for such messages to be communicated via the messaging bus. (Ex. 1003, ¶¶ 135, 98-99).

Smith further teaches that communications through the system may comprise requests and responses. Smith teaches a “request 415 is then sent to a consumer ID and address validation network 140,” and a “response is then supplied to the business device

110 via procedure 435.” (Ex. 1004, [0077]-[0078]).

Smith does not explicitly disclose the transmission of these requests and responses between the first and second intermediary servers, but it would have been obvious to POSITA for the business computer (*i.e.*, “first intermediary server”) and another entity’s computer (*i.e.* “second intermediary server”) to communicate in this manner. (Ex. 1003, ¶ 137). Smith establishes that communicating via requests and responses was well-known. (Ex. 1004, [0077]-[0078]); Ex. 1003, ¶¶ 136-137). POSITA would have understood the consumer communicating in this manner is merely the combination of prior-art elements according to known methods yielding predictable results. (Ex. 1003, ¶ 137).

Accordingly, “transmitting one or more first requests,” “receiving the one or more first requests at the second intermediary server,” “generating one or more first responses ... at the second intermediary server,” “transmitting the one or more first responses from the second intermediary server to the first intermediary server,” and “receiving the one or more first responses at the first intermediary server” would have been obvious to POSITA. (*Id.*, ¶ 138).

Second, it would have been obvious to POSITA to include the token in each request/response. (*Id.*, ¶ 139). Smith teaches that the business computer gives the transaction key (*i.e.*, “token”) to other parties so they “can access the ACH detail record and the transaction data files associated with the ACH detail record.” (Ex. 1004, [0041]). Seger teaches using “transactions [that] may be identified based on the

transaction identifier.” (Ex. 1005, 5:66-67). Seger explains that when a first party sends a request to a second party, the first party may “include a request and/or requirement that Party B use [the transaction identifier] in a second information transaction (e.g., a response to the first information transaction).” (*Id.*, 6:60-65). It would have been obvious to POSITA to include Smith’s transaction key (*i.e.*, “token”) in the request/response to identify the transaction and “enable the intended recipient to provide a response.” (*Id.*, 7:1; Ex. 1003, ¶ 139). The elements of the “one or more first requests, each comprising the token,” and the “one or more first responses each comprising the token corresponding to the respective one or more first requests” would have been obvious to POSITA. (Ex. 1003, ¶ 139).

Third, “transmitting the one or more first requests and the token from the second intermediary server to a second document store” and “transmitting the one or more first responses to the first document store” would have been obvious to POSITA. (*Id.*, ¶ 140). Smith teaches that entities maintain records of their transactions in local storage. (Ex 1004, [0034]). POSITA would have understood that local storage of transaction information is conventional for parties to an electronic funds transfer. (*E.g.*, Ex. 1011, Fig. 4, [0074]). Thus, POSITA would have found it obvious that an entity on Smith’s network communicating with the business computer, such as the consumer’s computer or ODFI computer (*i.e.*, “second intermediary server”), transmits records to local storage (*i.e.*, “second document store”) much like the business computer stores transaction information in a database, such that the other entity may also “store [] information for

later access.” (Ex. 1004, [0034]; Ex. 1003, ¶ 140).

Further, Smith enables “verification” and “proving that a consumer authorized a financial transaction.” (Ex. 1004, [0004]). POSITA would have understood that a means for verifying transaction information is by comparing the transaction information against an entity’s own records. (Ex. 1003, ¶ 141). Seger discloses verification via a similar mechanism where an entity “verif[ies] an integrity of the first information transaction based on the hash of the first information payload” included in the blockchain record. (Ex. 1005, 18:1-3; Ex. 1003, ¶ 141).

POSITA, looking to Seger, would have found it obvious to keep a record of requests and responses to “provide a verifiable record of the various information transactions” through the system. (Ex. 1005, 10:29-30; Ex. 1003, ¶¶ 142, 144-147). POSITA would have further understood that to enact such verification of requests and responses, the Smith/Seger combination includes “transmitting the one or more first requests and the token from the second intermediary server to a second document store” and “transmitting the one or more first responses to the first document store” to “store[] the information for later access” when verifying. (Ex. 1004, [0034]; Ex. 1003, ¶ 142).

Fourth, “hashing the one or more first requests and the one or more first responses at the second intermediary server to generate one or more first request hashes and one or more first response hashes, respectively” would have been obvious to POSITA. (Ex. 1003, ¶ 143). As explained for claim 7, POSITA would have found hashing of information on the system obvious to provide private communications that may still be

verified. (Ex. 1005, 1:40-41, 18:1-3; Ex. 1003, ¶ 144). POSITA would have understood that using hashing to “verify that data has not been altered during transmission or storage” was well-known before the ’413 Patent’s filing date. (*E.g.*, Ex. 1015, 22; Ex. 1024; Ex. 1041, 78, 88; Ex. 1003, ¶ 144). “The originator of the data calculates the hash using the data itself and the hashing algorithm. The originator then ensures that the hash is transmitted with integrity to the intended receiver of the data. ” (Ex. 1015, 22; Ex. 1019, 1). POSITA would have found it obvious to hash one or more responses at the entity on Smith’s network communicating with the business computer so that the business computer can verify the integrity of the response. (Ex. 1003, ¶ 145). POSITA also would have found it obvious to hash one or more requests at the other entity (*i.e.*, “second intermediary server”) so the business computer can ensure its message arrived at the other entity without corruption. (*Id.*).

Fifth, “adding the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain, from the second intermediary server” would have been obvious to POSITA. POSITA would have understood that “[o]ne way to ensure [that the hash is transmitted with integrity] is to publish the hash in a reliable source of public information.” (Ex. 1015, 22; Ex. 1003, ¶ 147). Seger’s “verifiable, and immutable” blockchain is a reliable source of information, published to those on the system. (Ex. 1005, 1:43; Ex. 1003, ¶ 147). Seger teaches verifying data integrity by comparing a hash on the blockchain with an entity’s own hash of the record. (Ex. 1005, 18:1-3; Ex. 1003, ¶ 147). Accordingly, POSITA

would have found it obvious to add the hashes into the blockchain from the other entity on Smith's system (*i.e.*, "second intermediary server") to allow the business computer (*i.e.* "first intermediary server") to compare its data against a reliable source of information, thereby ensuring integrity. (Ex. 1015, 22; Ex. 1003, ¶¶ 146-47).

7. Claim 9

Claim 9 depends from claim 8, reciting "hashing the one or more first responses at the first intermediary server to regenerate the one or more first response hashes; and verifying the one or more first response hashes with the blockchain from the first intermediary server, using the token." The Smith/Seeger combination would have rendered claim 9 obvious.

First, Seeger discloses "verify[ing] an integrity of the first information transaction based on the hash of the first information payload." (Ex. 1005, 18:1-3). Using hashes to verify data integrity was well-known "[w]hen the receiver gets the data an application can generate a hash and compare it to the original one." (Ex. 1015, 22; Ex. 1041, 92; Ex. 1003, ¶ 150). POSITA would have found it obvious for the business computer ("*i.e.*, "first intermediary server") to generate a hash of the "one or more first responses" so the business computer can then verify the information included therein. (Ex. 1003, ¶ 150).

Second, POSITA would have understood that within the Smith/Seeger combination, this verification would have been accomplished "using the token." (Ex. 1003, ¶ 151). As explained for element 3, Smith and Seeger use a "transaction key" and

“transaction identifier,” respectively, to identify transactions. (*Id.*). Seger discloses “verify[ing] an integrity of the first information transaction based on the hash of the first information payload *included in the first information transaction identifier.*” (Ex. 1005, 18:1-4). Accordingly, POSITA would have understood the token of the combination may be used to identify the record of the transaction to which “one or more responses” pertain on the blockchain to accomplish the disclosed verification. (Ex. 1003, ¶ 151).

8. Claim 10

Claim 10 depends from claim 8, reciting “wherein each one of the one or more first requests are: encrypted with a second public key and signed with a first public key at the first intermediary server, before transmission to the second intermediary server; and decrypted with a second private key at the second intermediary server after reception from the first intermediary server; and wherein each one of the one or more first responses are: encrypted with the first public key and signed with the second public key at the second intermediary server, before transmission to the first intermediary server; and decrypted with a first private key at the first intermediary server after reception from the second intermediary server.”

The Smith/Seger combination would have rendered claim 10 obvious. Smith teaches using “the highest level of compliance and encryption within the Payment Card Industry.” (Ex. 1004, [0059]). While Smith does not explicitly disclose the claimed encryption protocol, the claimed steps would have been obvious in view of Seger and

POSITA's knowledge. (Ex. 1003, ¶ 153).

First, Seger teaches use of “one or more forms of public key, or asymmetric, cryptography to facilitate communication.” (Ex. 1005, 4:52-54). An encryption technique where the sending party uses the receiving party's public key to encrypt a message or request before sending, and where the receiving party decrypts the message or request using its private key was well within the knowledge of POSITA. (Ex. 1003, ¶ 154; Ex. 1015 at 19 (“[S]ending party looks up the receiving party's public key and uses it to encipher the data...[R]eceiving party then uses its private key to decipher the data.”); Ex. 1041, 47-48). POSITA would have understood the limitations of “encrypted with a second public key...at the first intermediary server, before transmission to the second intermediary server,” “decrypted with a second private key at the second intermediary server after reception from the first intermediary server,” “encrypted with the first public key at the second intermediary server, before transmission to the first intermediary server,” “decrypted with a first private key at the first intermediary server after reception from the second intermediary server,” as merely implementation of known public key encryption techniques. This generic encryption protocol is reflected in Seger, which teaches using first and second public and private keys to encrypt and decrypt information. (Ex. 1005, 4:61-67, 5:23-30, 7:64-65, Ex. 1003, ¶ 154). Accordingly, POSITA would have found it obvious to apply these well-known public key/asymmetric cryptography taught by Seger into Smith's system to “facilitate secure private communications between” parties on the system. (Ex. 1005, 1:40-41, Ex. 1003,

¶ 154).

Second, Seger describes a party “cryptographically sign[s]” messages on the system. (Ex. 1005, 5:60). Use of public key cryptography to generate digital signatures to authenticate the source of a message was well-known as of the 413 Patent’s filing date. (Ex. 1015, 22-23; Ex. 1041, 88). A sender signs the message with a key associated with that sender. For the Smith/Seger combination, POSITA would have known there are two keys associated with the sender: the sender’s private key or the sender’s public key. (Ex. 1003, ¶ 155).

A conventional digital signature algorithm uses a sender’s private key to sign a message or request; the receiving party uses the sender’s public key to verify the message or request. (*Id.*, ¶ 156). Prior art references show that algorithms using a public key to sign and create a digital signature were known. (Ex. 1003, ¶ 156; *see, e.g.*, Ex. 1016, [0010] (“public key may be used as a signature to verify...identity”); Ex. 1020, 1:22-26 (“communication systems are known that additionally employ digital signing key pairs, such as a signing private key, and a signing public key, to allow the use of digital signatures so that...data may be uniquely and securely signed by an individual”); Ex. 1023, [0340] (“Appropriately signed means signed with the public key”); Ex. 1022, [0114] (“queries can be signed with the public key and verified with the cryptographic signature”); Ex. 1021, [0016] (“[R]equest may also be signed with the public key.”). POSITA would have understood signing with either the sender’s private key or public key were two known options for generating a digital signature. (Ex. 1003, ¶ 157).

POSITA therefore would have found it obvious to sign “one or more first requests” with the first public key and “one or more first responses” with the second public key as a simple design choice between the two known, finite, predictable solutions. (*Id.*).

9. Claim 11

Claim 11 depends from claim 10, reciting “adding the first public key from the first intermediary server into the blockchain and adding the second public key from the second intermediary server into the blockchain.” The Smith/Seeger combination would have rendered claim 11 obvious.

POSITA would have understood that public keys are associated with particular entities on the network, and these keys are shared with others on the system to enable public key/asymmetric cryptography. (Ex. 1015, 20; Ex. 1003, ¶ 159). Typically, parties share this data by “publish[ing] their public keys in a reliable information source.” (Ex. 1015, 20; Ex. 1003, ¶ 159). Seeger’s blockchain is not just “reliable” but “immutable.” Seeger discloses adding information that “may include the first public key” to the blockchain. (Ex. 1005, 2:25-26). It would have been obvious to POSITA that each party would add its public key to the blockchain to publish the keys on an information source that cannot be changed, ensuring integrity of published key information. (Ex. 1003, ¶ 159).

10. Claim 12

Claim 12 depends from claim 1. POSITA would have understood that claim 12 simply recites a reversal of the steps recited in claim 8. (Ex. 1003, ¶ 161). As explained

for claim 8, these elements would have been obvious to POSITA. (*Id.*).

11. Claim 13

Claim 13 depends from claim 12. POSITA would have understood that claim 12 simply recites a reversal of the steps recited in claim 8. The additional steps recited in claim 13 are the same as recited in claim 9, which depends upon claim 8. The Smith/Seeger combination would have rendered claim 13 obvious as explained for claims 9 and 12. (Ex. 1003, ¶ 163).

12. Claim 14

Claim 14 depends from claim 12. POSITA would have understood that claim 12 simply recites a reversal of the steps recited above in claim 8. The additional steps recited in claim 14 are the same as recited in claim 10, which depends from claim 8. The Smith/Seeger combination would have rendered claim 14 obvious as explained for claims 10 and 12. (Ex. 1003, ¶ 165).

13. Claim 15

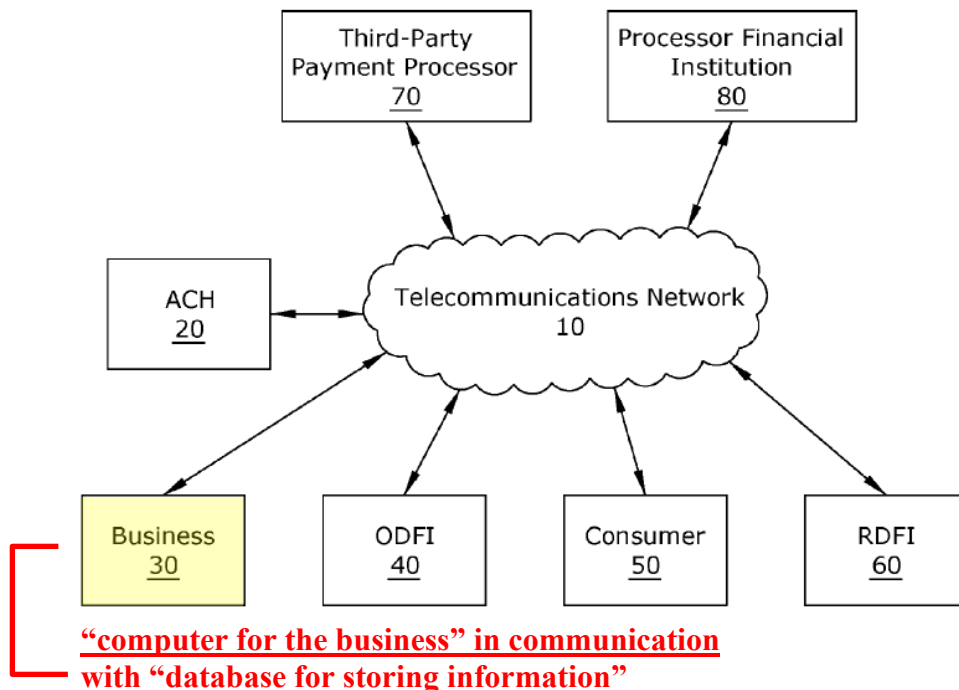
Preamble: A system for processing a financial transaction:

If the preamble is limiting, Smith discloses this element for reasons explained regarding claim 1's preamble. (Ex. 1003, ¶ 166; Ex. 1004, [0004]).

Element 1: a first intermediary server in a centralised financial system, the first intermediary server being operably connected to a network and a first document store;

The Smith/Seeger combination would have rendered this element obvious as explained for claim 1, element 1. (Ex. 1003, ¶¶ 167-168). Smith's "electronic funds

consumer authorization verification system” (*i.e.*, “centralised financial system”) utilizes a “telecommunication network 10 capable of transmitting electronic data and/or electronic funds between a plurality of electronic devices (e.g. computers, mobile devices, etc.).” (Ex. 1004, [0030-0031]).



(*Id.*, Fig. 1). Smith teaches that “a computer for the business 30” is in communication with “a database that stores [] information for later access.” (*Id.*, [0031], [0034]).

POSITA would have understood business computer 30 (*i.e.*, “first intermediary server”) is operably connected to a network and first document store. (Ex. 1003, ¶ 168).

Element 2: a token server operably connected to the network;

The Smith/Seeger combination would have rendered this element obvious as explained for claim 1, element 3. (*Id.*, ¶ 169).

Element 3: a blockchain operably connected to the network, the blockchain being a distributed ledger;

The Smith/Seeger combination would have rendered this element obvious as explained for claim 1, element 2. (*Id.*, ¶ 170).

Element 4: wherein the first intermediary server is configured to: transmit one or more documents pertaining to the financial transaction, to the first document store;

The Smith/Seeger combination would have rendered this element obvious as explained for claim 1, element 1. (*Id.*, ¶ 171).

Element 5: generate an enriched data record from the one or more documents and add the enriched data record into the blockchain;

The Smith/Seeger combination would have rendered this element obvious as explained for claim 1, element 2. (*Id.*, ¶ 172).

Element 6: 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

The Smith/Seeger combination would have rendered this element obvious as explained for claim 1, element 3. (*Id.*, ¶ 173).

Element 7: transmit the token to the first document store;

The Smith/Seeger combination would have rendered this element obvious as explained for claim 1, element 6. (*Id.*, ¶ 174).

Element 8: 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

The Smith/Seeger combination would have rendered this element obvious as explained for claim 1, element 4. (*Id.*, ¶ 175).

Element 9: transmit the token to the first intermediary server, via the messaging bus.

The Smith/Seeger combination would have rendered this element obvious as explained for claim 1, element 5. (*Id.*, ¶ 176).

14. Claim 16

As explained below, the Smith/Seeger combination renders claim 16 obvious for the same reasons as claims 1 and 15. Claim 16 is broader than claims 1 and 15 because it does not recite the token server configured to add the token to the blockchain, which is required in claims 1 and 15.

Preamble: A first intermediary server for use in a centralised financial system to facilitate processing of a financial transaction, operably connected to a network and a first document store, and configured to:

If the preamble is limiting, Smith discloses or renders obvious this element as explained for elements 1 of claims 1 and 15. (Ex. 1003, ¶ 177).

Element 1: transmit one or more documents pertaining to the financial transaction, to the first document store;

The Smith/Seeger combination would have rendered this element obvious as explained for claim 1, element 1. (*Id.*, ¶ 178).

Element 2: generate an enriched data record from the one or more documents and add the enriched data record into a blockchain being a distributed ledger;

The Smith/Seeger combination would have rendered this element obvious as explained for claim 1, element 2. (*Id.*, ¶ 179).

Element 3: request generation of a token corresponding to the financial transaction to identify the one or more documents, to a token server, via a messaging bus in the centralised financial system; and

The Smith/Seeger combination would have rendered this element obvious as explained for claim 1, element 3. (*Id.*, ¶ 180). Even if the Board determines that the Smith/Seeger combination does not disclose “adding the token into the blockchain from the token server,” no such requirement exists in claim 16.

Element 4: transmit the token to the first document store.

The Smith/Seeger combination would have rendered this element obvious as explained for claim 1, element 6. (*Id.*, ¶ 181).

15. Claim 17

Claim 17 depends from claim 16, reciting the first intermediary server is “configured to send a first financial message comprising the token, to a second intermediary server in the centralised financial system, indicative of making a payment to a second user.” The Smith/Seeger combination would have rendered this element obvious as explained for claims 2 and 16. (*Id.*, ¶ 183).

16. Claim 18

Claim 18 depends from claim 16, reciting the first intermediary server is “configured to transmit the token to a first digital device.”

The Smith/Seeger combination would have rendered this claim obvious. (*Id.*, ¶ 185). Smith teaches “[t]he computer for the business 30 [*i.e.*, ‘first intermediary server’)] also communicates with the computer of the [TPPP] 70, the computer for the ODFI 40 and/or the computer for the RDFI via the network [*i.e.*, “first digital device”)].” (Ex. 1004, [0036]). Smith teaches the business 30 “gives the transaction key” to other entities “such as the RDFI or the ODFI.” (*Id.*, [0041]). Smith therefore discloses the business computer (*i.e.*, “first intermediary server”) is configured to transmit the transaction key (*i.e.* “token”) to a computer of another entity on the system (*i.e.*, “first digital device”). (Ex. 1003, ¶ 185).

17. Claim 19

Claim 19 depends from claim 16, reciting the first intermediary server is “configured to: transmit one or more first requests, each comprising the token, to a second intermediary server in the centralised financial system, via the messaging bus; and receive one or more first responses from the second intermediary server and transmit the one or more first responses to the first document store.”

The Smith/Seeger combination would have rendered this claim obvious for the same reasons explained for claims 8 and 16. (*Id.*, ¶ 187).

18. Claim 20

Claim 20 depends from claim 19, reciting “the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.”

The Smith/Seeger combination would have rendered this claim obvious. Seeger teaches “encrypted second information may include and/or be associated with one or both of know your customer (KYC) data, anti-money laundering (AML) data, and/or other financial data.” (Ex. 1005, 8:61-9:4). As the ’413 Patent recognizes, KYC documents are regulatory compliance documents. (Ex. 1001, 1:37-38; Ex. 1003, ¶¶ 40-41). It would have been obvious to POSITA to combine Seeger’s teachings with Smith’s system to allow businesses and banks to share KYC and AML data to facilitate ACH transaction processing. (Ex. 1003, ¶¶ 189-191).

C. Ground 2: Claim 3 Would Have Been Obvious Over The Smith/Seeger Combination In View Of Yago

Claim 3 depends from claim 1, reciting “implementing a smart contract at the token server; and adding the smart contract into the blockchain, from the token server.”

The Smith/Seeger combination teaches transactions involving blockchain, but does not explicitly disclose implementing a “smart contract.” This claim would have been obvious by the Smith/Seeger combination in view of Yago. (*Id.*, ¶¶ 194-201).

First, Yago discloses “implementing a smart contract.” Yago teaches “payment assured contracts” through which a party can “*objectively (and automatically)*, confirm

performance by the seller, by...directly monitoring the CDI network [(i.e., ‘blockchain’)].” (Ex. 1011, [0047]). POSITA would have understood Yago’s payment assured contract is a “smart contract.” (Ex. 1003, ¶ 195; Ex. 1014, [0003] (“Another important area of inquiry is ‘smart contracts’—systems *which automatically* move digital assets according to arbitrary pre-specified rules”); Ex. 1013 (same).

It would have been obvious to POSITA to apply Yago’s “payment assured contracts” to the Smith/Seeger combination. (Ex. 1003, ¶ 196). The motivation to do so would have come directly from Yago itself, which teaches creating “contracts that may be automatically enforced, resulting in reduced fraud and counter-party risk when dealing with all different types of CDFI.” (Ex. 1011, [0006]; Ex. 1003, ¶ 195). Yago, like Smith and Seeger, addresses similar problems relating to the improving verifiability of transactions. (Ex. 1011, [0006] (“[A] method is needed which allows for...payments to be tied to mathematically verifiable events”); Ex. 1005, 1:42-46; Ex. 1004, [0014]; Ex. 1003, ¶ 195]). POSITA would have had a reasonable expectation of success in applying Yago’s “payment assured contract” to the Smith/Seeger combination. (Ex. 1003, ¶¶ 196-197). The idea of blockchain-based smart contracts had been contemplated in the art since blockchain’s beginnings. (Ex. 1012, 29 (“[P]ossibilities for programmable...contracts were baked into the [Bitcoin] protocol at its invention.”); Ex. 1003, ¶¶ 32-34). Applying Yago’s teachings with the Smith/Seeger system would have involved combining well-understood technologies, yielding predictable results. (Ex. 1003, ¶¶ 196-197).

Second, Yago discloses or would have rendered obvious implementing the smart contract “at the token server” and “adding the smart contract into the blockchain, from the token server.” (*Id.*, ¶¶ 198-201). Yago promotes “automated and scalable settlement protocols” including “digital contracts that may be automatically enforced.” (Ex. 1011, [0006]). To do so, Yago discloses a “software/computer/firmware module that creates and applies contract/credit certificates with verifiable and objective terms based on a trade request between two or more parties.” (Ex. 1011, [0007]). Yago’s module is “adapted to monitor crypto-digital instrument networks [(i.e., a blockchain)] to verify performance of the expected terms.” (*Id.*).

Yago explains that “contracts and certificates may be issued on the public ledgers of the CDI systems.” (*Id.*, [0054]). Yago discloses a “transaction system 412 comprising a plurality of modules” configured to transfer the digital certificate or contract to a public ledger, for example by “writ[ing] the first certificate 504 to the public ledger,” and to “monitor the public ledger 406 for the transactions specified in the digital certificate 504 and/or the digital contract 130.” (*Id.*, [0058], [0066], [0068], Fig. 4). After payment is complete, the proof of payment module of transaction system 412 “records the completion of the transaction onto the public ledger.” (*Id.*, [0067]). Proof of payment is recorded on the public ledger “as either a message or a contract.” (*Id.*, [0052], [0054]). Thus, the “payment assured contracts” (i.e., “smart contracts”) are implemented at the transaction system 412 and added to the public ledger (i.e., “blockchain”) by the transaction system 412. (Ex. 1003, ¶ 199).

POSITA would have understood Yago's "transaction system" is like Smith's "token server" because it is a central server unaffiliated with any party to the smart contract. (Ex. 1004, [0040]; Ex. 1011, [0065]; Ex. 1003, ¶ 200). In context of the Smith/Seeger combination, POSITA would have found it obvious that Yago's "payment assured contacts" would be implemented at and added to the blockchain by the token server. (Ex. 1003, ¶ 200).

D. Ground 3: Claim 4 Would Have Been Obvious Over The Smith/Seeger Combination In View Of Kurani-274

The Smith/Seeger combination in view of Kurani-274 would have rendered claim 4 obvious.

First, Smith discloses or would have rendered obvious "transmitting the token from the first intermediary server to a first digital device available with a first user." Smith includes "one or more suitable business devices [] (e.g., computers, mobile devices)" and "each entity type may be associated with any number of suitable computers." (Ex. 1004, [0061]). Accordingly, POSITA would have understood that the business computer (*i.e.*, "first intermediary server") may be associated with additional business devices/computers. (Ex. 1003, ¶ 205). Where the business computer comprises client/server architecture (as taught and motivated by Seeger and explained for claim 1, element 1), POSITA would have understood the business computer's first intermediary server may receive the transaction key (*i.e.*, "token") from the TPPP and then transmit the transaction key to a client device (*i.e.*, "first digital device available

with a first user”) to facilitate further processing such that the business device may communicate the token to the TPPP. (*Id.*).

Second, although Smith does not explicitly disclose “providing the token to a second user, by the first user,” this element would have been obvious from Kurani-274’s teachings. Smith contemplates sharing transaction information between a customer and business, but does not provide details of how it would be performed. (Ex. 1003, ¶¶ 206-210). Like Smith and Seger, Kurani-274 seeks to provide a system for secure financial transactions (Ex. 1007, 1:20-22 (“[P]rinciples of cryptography are used to create, secure, and transfer MBC directly from a first user to a second user.”); Ex. 1004, [0059]; Ex. 1005, 3:6-15). Thus, POSITA looking to improve upon Smith would look to other systems like Kurani-274, which identifies a number of ways for customers and businesses to share important information like the transaction key. (Ex. 1003, ¶ 207). Kurani-274 discloses that during a transaction, the “token may be transmitted” between a customer and business. (Ex. 1007, 6:9-11). Kurani-274 explains that “the token may be transmitted using optical image methods...NFC, wireless, Bluetooth...RFID, hypersonic, Wi-Fi, cellular 3G, 4G, GSM LiFi, etc.” (*Id.*, 6:12-15).

POSITA would have understood that a straightforward, well-known way for owners to pass tokens to the receiving party would be through device-to-device transfer, such as personal computers or smartphones. (Ex. 1003, ¶ 209). POSITA would have further understood from Kurani-274’s disclosure that the token may be sent from a business device (*i.e.*, “first digital device available with a first user”) to a customer

device (*i.e.*, “second digital device of a second user”). (*Id.*).

POSITA also would have understood that servers associated with each device (*i.e.*, “first intermediary” and “second intermediary” servers) would have been involved in transmitting and receiving tokens such that tokens travel from the first intermediary server to the business device, which transmits the token to the customer’s device and thereafter to the second intermediary server associated with the buyer. (*Id.*, ¶ 210).

Third, Smith discloses “providing the token to a second intermediary server in the centralised financial system.” Smith explains that the transaction key is communicated “so the business 30 (or any third-party [to which] the business gives the transaction key...) can access the ACH detail record and the transaction data files associated with the ACH detail record.” (Ex. 1004, [0041]). By teaching that the business computer 30 “gives the transaction key” to other parties, Smith discloses “providing the token to a second intermediary server in the centralised financial system.” (Ex. 1003, ¶ 211).

Fourth, Smith discloses or would have rendered obvious “transmitting the token to a second document store, from the second intermediary server.” (*Id.*). As explained for claim 1, element 1, Smith discloses a first document store associated with the business for storing transaction information. While Smith does not explicitly disclose a corresponding document store associated with the customer, it would have been obvious to POSITA for the customer to maintain such a second document store. (*Id.*, ¶ 212). POSITA would have found this obvious as a well-known means to store locally tokens and other transaction data to “store[] the information for later access” for verification

and recordkeeping. (Ex. 1004, [0034]; Ex. 1003, ¶ 212).

Fifth, Smith/Seeger/Kurani-274 would have rendered obvious “sending a second financial message comprising the token, from the second intermediary server to the first intermediary server, indicative of making a payment to the first user.” Kurani-274 teaches “transmit[ing] a receipt of the transaction” for payments between two entities. (Ex. 1007, 21:19-21). POSITA would have found it obvious for Smith’s method to communicate a message indicative of making payment to the business for transactions involving payment by the customer to provide a receipt of said payment, as Kurani-274 teaches. (Ex. 1003, ¶ 213). POSITA would have had a reasonable expectation of success in doing so because this would involve combining well-understood technologies yielding predictable results. (*Id.*).

V. DISCRETIONARY INSTITUTION

The Board should not exercise its discretion under either §§ 314(a) or 325(d) to deny this Petition.

A. The *Fintiv* Factors Favor Institution

Factor 1 is neutral. There is district-court litigation that is not currently stayed. The district court has not indicated whether it would grant a motion to stay if one were filed.

Factor 2 weighs strongly against discretionary denial. The district court has not

set a scheduling order or trial date. The latest Judicial Caseload Statistics³ report a median time of 38.0 months to trial in the District of Delaware, which projects trial in November 2026—over one year after the Board’s projected deadline for a final written decision.

Factor 3 weighs against discretionary denial. The district-court case is in its early stages. Petitioner (who is defendant in the district-court case) moved to dismiss the amended complaint filed in January 2024. Fact discovery has not begun. Infringement and invalidity contentions have not been served. Claim-construction has not commenced. Even at the time of expected institution, the district-court litigation will be in its infancy.

Factor 4 considers the overlap of issues raised in the petition and in the parallel proceeding. Because infringement contentions have not yet been served in the district-court proceeding, the degree of potential overlap in issues is not yet known, and this factor should not weigh in favor of denial.

Factor 5 weighs against discretionary denial. Although Petitioner is a defendant in the district-court litigation, trial will likely not occur until at least one year after the projected statutory deadline for a final written decision.

Factor 6. Because factors 2, 3, and 5 weigh against discretionary denial and factor

³ <https://www.uscourts.gov/file/78140/download>.

1 is neutral, the balance of factors favors institution, and the Board need not engage in the compelling merits determination. In any event, the merits are compelling because the Challenged Claims recite the combination of conventional and generic elements that were well-known.

B. The *Becton* Factors Favor Institution

Smith, Seger, Kurani, and Yago were not cited during prosecution of the '413 Patent. The arguments made during prosecution and manner in which Petitioner relies on the prior art do not overlap. During prosecution, the Examiner cited “Davis” as teaching all limitations of the independent claims except “transmitting one or more documents pertaining to the financial transaction, from a first intermediary served in a centralized financial system to a first document store,” which the Examiner found was taught by “Morgan.” (Ex. 1002, 305, 317-19). Petitioner’s grounds do not rely on similar arguments or prior art combinations. Therefore, the Board should not exercise its discretion to deny institution under § 325(d). Further, the Office erred in allowing the Challenged Claims. The Examiner did not have the benefit of expert testimony explaining the significance of combining Smith, Seger, Yago, and/or Kurani. Moreover, the Examiner’s reasons for allowance cited eight “closest prior art references of record” but failed to cite Smith, Seger, Yago, and Kurani. (*Id.*, 242-44).

VI. CONCLUSION

Petitioner respectfully requests *inter partes* review of the Challenged Claims.

VII. MANDATORY NOTICES PURSUANT TO 37 C.F.R. § 42.8(a)(1)

Pursuant to 37 C.F.R. § 42.8(a)(1), the mandatory notices identified in 37 C.F.R. § 42.8(b) are provided below as part of this petition.

A. 37 C.F.R. § 42.8(b)(1): Real Parties-In-Interest

The real party-in-interest is JPMorgan Chase Bank, N.A.

B. 37 C.F.R. § 42.8(b)(2): Related Matters

Pursuant to 37 C.F.R. § 42.8(b)(2), Petitioner is aware of the following patent infringement lawsuit involving the '413 Patent: *Identitii Limited v. JPMorgan Chase & Co., et al.*, Case No. 1:23-cv-01095-GBW (U.S. District Court, District of Delaware).

Petitioner is concurrently filing another petition for *inter partes* review of claims 1-20 of the '413 Patent, including challenging the priority date of the '413 Patent.⁴

C. 37 C.F.R. § 42.8(b)(3), (4): Counsel And Service Information

Petitioner provides the following designation of lead and back-up counsel:

Lead Counsel	Back-up Counsel
H. Albert Liou (Reg. No. 71,504) JONES DAY 717 Texas Ave., Suite 3300 Houston, Texas 77002 Telephone: (832) 239-3939 Facsimile: (832) 239-3600 aliou@jonesday.com	Rita J. Yoon (<i>pro hac vice</i> forthcoming) JONES DAY 555 California Street, 26th Fl. San Francisco, CA 94104 Telephone: (415) 875-5816 Facsimile: (415) 875-5700 I. Sasha Mayergoyz (Reg. No. 47,778)

⁴ Petitioner concurrently submits a separate paper explaining why the filing of multiple petitions should not be a basis for discretionary denial under 35 U.S.C. § 314.

	JONES DAY 110 North Wacker Drive, Suite 4800 Chicago, IL 60606 Telephone: (312) 782-3939 Facsimile: (312) 782-8585 smayergoyz@jonesday.com Matthew W. Johnson (Reg. No. 59,108) JONES DAY 500 Grant Street, Suite 4500 Pittsburgh, PA 15219-2514 Telephone: (412) 394-9524 mwjohnson@jonesday.com Marlee R. Hartenstein (Reg. No. 77,851) JONES DAY 500 Grant Street, Suite 4500 Pittsburgh, PA 15219 (412) 394-7257 mhartenstein@jonesday.com Stephen M. Bradley (Reg. No. 81,622) JONES DAY 1221 Peachtree Street NE, Suite 400 Atlanta, GA 30361 (404) 581-8233 sbradley@jonesday.com
--	--

Pursuant to 37 C.F.R. § 42.10(b), a Power of Attorney for Petitioner accompanies this petition. Please address all correspondence to lead and back-up counsel at the addresses above. Petitioner also consents to electronic service by email at the email addresses listed above.

Dated: February 20, 2024

Respectfully Submitted,

/s/ H. Albert Liou

H. Albert Liou (Reg. No. 71,504)

JONES DAY

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a copy of the foregoing petition for *Inter Partes* Review of U.S. Patent No. 10,984,413, including all Exhibits, was served on February 20, 2024 via Express Mail delivery directed to the attorney of record for the patent at the following address:

162809 - Bochner PLLC
1040 Avenue of the Americas, 15th Fl.
New York, NY 10018

An electronic courtesy copy of the foregoing petition and the accompanying declaration of Chien-Chung Shen, Ph.D. was additionally served on litigation counsel for Identitii Limited at the following:

Bunsow De Mory LLP
eday@bdiplaw.com
mbelloli@bdiplaw.com
jtice@bdiplaw.com
mflynobrien@bidplaw.com

Ashby & Geddes
jday@ashbygeddes.com
amayo@ashbygeddes.com

Dated: February 20, 2024

/s/ H. Albert Liou
H. Albert Liou (Reg. No. 71,504)
JONES DAY

CERTIFICATE OF WORD COUNT UNDER 37 C.F.R. § 42.24(a)

I, the undersigned, do hereby certify that the attached petition contains 13,886 words, as measured by the Word Count function of Microsoft Word for Microsoft Office 365. This is less than the limit of 14,000 words as specified by 37 C.F.R. § 42.24(a)(1)(i).

Dated: February 20, 2024

/s/ H. Albert Liou

H. Albert Liou (Reg. No. 71,504)

JONES DAY

APPENDIX OF EXHIBITS

EXHIBIT	TITLE
1001	U.S. Patent No. 10,984,413 (“the ’413 patent”)
1002	File History of the ’413 Patent
1003	Declaration of Dr. Chien-Chung Shen, Ph.D., for Petition #1
1004	U.S. Patent Pub. No. 2015/0081553 (“Smith”)
1005	U.S. Patent No. 9,397,985 (“Seeger”)
1006	Microsoft Computer Dictionary
1007	U.S. Patent No. 11,270,274 (“Kurani-274”)
1008	Everett Rosenfeld, “Forget currency, bitcoin’s tech is the revolution.”
1009	Richards, “The Role of Blockchain Technology in Supply Chain Management” (2013)
1010	Tim Swanson, “Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems.”
1011	U.S. Patent Pub. No. 2015/0206106 (“Yago”)
1012	Swan, “Blockchain: Blueprint for a New Economy” (2015)

1013	Vitalik Buterin, “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,” White Paper (2014)
1014	U.S. Patent Pub. No. 2016/0140653 (“McKenzie”)
1015	IBM, Version 1 Release 13 of z/OS, “Cryptographic Services,” Integrated Cryptographic Service Facility (2011)
1016	U.S. Patent Pub. No. 2006/0015945 (“Fields”)
1017	U.S. Patent Pub. No. 2011/0258123 (“Dawkins”)
1018	U.S. Patent Pub. No. 2013/0212007 (“Mattsson”)
1019	Tiwari et al., “Cryptographic Hash Function: An Elevated View” (2010)
1020	U.S. Patent No. 6,341,164 (“Dilkie”)
1021	U.S. Patent Pub. No. 2010/0223659 (“Ekl”)
1022	U.S. Patent Pub. No. 2013/0080916 (“Lopez”)
1023	U.S. Patent Pub. No. 2003/0200450 (“England”)
1024	<i>Wayback Machine</i> Archive – IBM, Version 1 Release 13 of z/OS “Cryptographic Services,” Integrated Cryptographic Service Facility (2011)
1025	Screenshots – <i>Wayback Machine</i> Archive

1026	<i>Intentionally Omitted</i>
1027	<i>Intentionally Omitted</i>
1028	<i>Intentionally Omitted</i>
1029	<i>Intentionally Omitted</i>
1030	<i>Intentionally Omitted</i>
1031	<i>Intentionally Omitted</i>
1032	<i>Intentionally Omitted</i>
1033	<i>Intentionally Omitted</i>
1034	<i>Intentionally Omitted</i>
1035	<i>Intentionally Omitted</i>
1036	Dr. Chien-Chung Shen <i>Curriculum Vitae</i>
1037	Tannenbaum, “Distributed Systems, Principles and Paradigms” (2007)
1038	Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System” (2008)
1039	Ripple Labs, Inc., “The Ripple Protocol: A Deep Dive for Finance

	Professionals” (2014)
1040	U.S. Patent No. 9,892,460 (“Winkelvoss”)
1041	Stallings, “Cryptography and Network Security Principles and Practices,” 4th Ed. (2006)
1042	U.S. Patent Pub. No. 2009/0249082 (“Mattsson-082”)
1043	U.S. Patent Pub. No. 2013/0212666 (“Mattsson-666”)
1044	U.S. Patent No. 6,173,272 (“Thomas”)
1045	<i>Intentionally Omitted</i>
1046	<i>Intentionally Omitted</i>