

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. IPR2024-00593
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	iv
I. INTRODUCTION	1
II. REQUIREMENTS FOR IPR UNDER 37 C.F.R. § 42.104.....	1
A. Grounds For Standing Under 37 C.F.R. § 42.104(a)	1
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)	2
III. '413 PATENT.....	3
A. Alleged Invention	3
B. Prosecution History	4
C. POSITA	6
IV. THE '413 PATENT IS NOT ENTITLED TO CLAIM PRIORITY TO AU-1'S FILING DATE OF AUGUST 14, 2015	6
A. Challenged Claims	6
B. Nearly 80% Of The '413 Patent Is Absent From AU-1's Disclosures	7
C. Legal Standard And Board Authority	10
D. AU-1 Does Not Provide Written-Description Support For The "Enriched Data Record" Added To The Blockchain From "The First Intermediary Server" As Claimed In The Challenged Claims	11
E. AU-1 Also Does Not Provide Written-Description Support For The "Token" Limitations.....	14
V. THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	15
A. Prior Art.....	15
1. Kennedy	16
2. Kurani-816	19
3. Yago	21
B. Ground 1: Claims 1-2 and 4-20 Are Obvious Over Kennedy In View Of Kurani-816.....	22
1. Claim 1	22

TABLE OF CONTENTS
(continued)

2.	Claim 2	43
3.	Claim 4	46
4.	Claim 5	48
5.	Claim 6	48
6.	Claim 7	49
7.	Claim 8	50
8.	Claim 9	56
9.	Claim 10	57
10.	Claim 11	60
11.	Claim 12	61
12.	Claim 13	61
13.	Claim 14	61
14.	Claim 15	61
15.	Claim 16	65
16.	Claim 17	66
17.	Claim 18	66
18.	Claim 19	67
19.	Claim 20	67
C.	Ground 2: Kennedy And Kurani-816 In View Of Yago Render Obvious Claim 3	68
1.	Claim 3	68
VI.	CONCLUSION	71
VII.	MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(a)(1)	71
A.	37 C.F.R. § 42.8(b)(1): Real Parties-In-Interest	72
B.	37 C.F.R. § 42.8(b)(2): Related Matters	72
C.	37 C.F.R. § 42.8(b)(3), (4): Counsel And Service Information	72
	CERTIFICATE OF SERVICE	74
	CERTIFICATE OF WORD COUNT UNDER 37 C.F.R. § 42.24(a)	75

TABLE OF CONTENTS
(continued)

APPENDIX OF EXHIBITS 76

'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 10,984,413 (“’413 Patent”) (Ex. 1001). This petition challenges the ’413 Patent’s priority date.

The ’413 Patent claims priority to Australian provisional applications filed on August 2015, January 2016, and May 2016. (Exs. 1027-1030). One year after filing the first Australian provisional, Applicant entered the U.S. national phase on August 12, 2016, filing International Application PCT/AU2016/000279. (Ex. 1030). The ’413 Patent issued from this PCT application. ***Nearly 80% of the ’413 Patent is new matter absent from the Australian provisionals.*** (Ex. 1031). The PCT application adds nearly 18,000 words, 255 paragraphs, and 10 new figures not present in the provisional applications. (Ex. 1030). Had the Examiner substantively considered the ’413 Patent’s priority claim, the Examiner would have discovered that the Challenged Claims lack written-description support in the provisional applications. As such, the ’413 Patent’s priority date would have been August 12, 2016—the PCT application’s filing date—and would not have been allowed over the prior art and evidence presented herein.

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

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

The Challenged Claims should be cancelled as unpatentable based on these grounds:

Unpatentability Grounds	Exhibits
<u>Ground 1:</u> Claims 1-2 and 4-20 would have been obvious over U.S. Patent Application 2017/0132626 (“Kennedy”) combined with U.S. Patent 10,719,816 (“Kurani-816”).	1033-1034
<u>Ground 2:</u> Claim 3 would have been obvious over Kennedy and Kurani-816 combined with U.S. Pub. 2015/0206106 (“Yago”).	1011

Section V 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 V explains the relevance of the evidence, as supported by Dr. Chien-Chung Shen’s declaration (Ex. 1026). 37 C.F.R. § 42.104(b)(5).

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

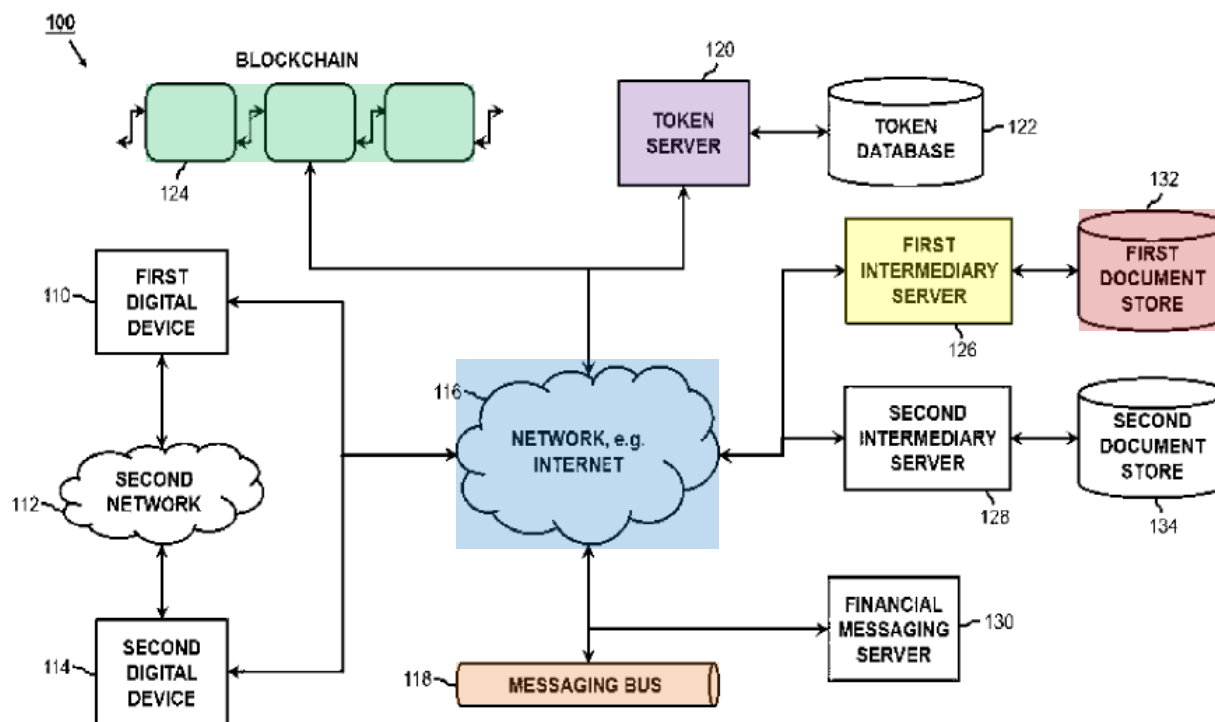
In this proceeding, claims are interpreted to have their plain meaning in view of the specification and file history. *Phillips v. AWH*, 415 F.3d 1303, 1312 (Fed. Cir. 2005). For this proceeding, Petitioner believes no special constructions are necessary to assess whether the Challenged Claims are unpatentable.

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 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 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

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” (e.g., a plurality of attributes from the documents) “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). “[T]he 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”).

¹ Colors added to Figures throughout, unless indicated otherwise.

The '413 Application is a national stage entry of PCT Application PCT/AU2016/000279 filed on August 12, 2016 (“PCT application”).

The '413 Patent claims priority to three Australian provisional applications filed on August 2015 (“AU-1,” Ex. 1027), January 2016 (“AU-2,” Ex. 1028), and May 2016 (“AU-3,” Ex. 1029) (collectively, “Australian provisionals”). As discussed in Section IV, nearly 80% of the '413 Patent is new matter absent from the Australian provisionals. Accordingly, the Challenged Claims are only entitled to claim priority to the PCT application’s filing date.

The PCT application entered the U.S. national stage on February 14, 2018. (Ex. 1002, 497). In a Non-Final Office Action, the Examiner rejected all claims as obvious. (*Id.*, 299-333). Rather than substantively amending the claims, Applicant argued the elements of the independent claims distinguish over the prior art. (*Id.*, 289-293). Responding to rejection of claim 61 (now claim 3)—the only rejection where priority was at issue—Applicant only referred to written-description support in “at least in the PCT application with an international filing date of August 12, 2016.” (*Id.*, 292). ***Applicant did not point to any of the earlier filed Australian provisionals for written-description support.***

The Examiner then issued a Notice of Allowability, noting 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. 1026, ¶ 47).

IV. THE ’413 PATENT IS NOT ENTITLED TO CLAIM PRIORITY TO AU-1’S FILING DATE OF AUGUST 14, 2015

A. Challenged Claims

The Challenged Claims recite numerous limitations not disclosed in the Australian provisionals.² To streamline issues, Petitioner focuses its arguments on three limitations. The Challenged Claims recite a “first intermediary server” that (1) generates an “enriched data record” *and also* (2) adds the “enriched data record” to a blockchain. (Ex. 1001, 59:7-10, 62:11-17, 62:26-38). Claims 1 and 15 further recite a

² Because the prior art grounds raised in this petition predate the filing dates of AU-2 and AU-3, only the ’413 Patent’s priority claim to AU-1 is discussed herein. Petitioner reserves all rights to challenge the 413 Patent’s priority claim to AU-2 and AU-3.

“token server” that adds “the token into the blockchain in association with the enriched data record.” (*Id.*, 59:16-18, 62:21-23). These limitations lack written-description support in at least AU-1. (Ex. 1026, ¶ 49).

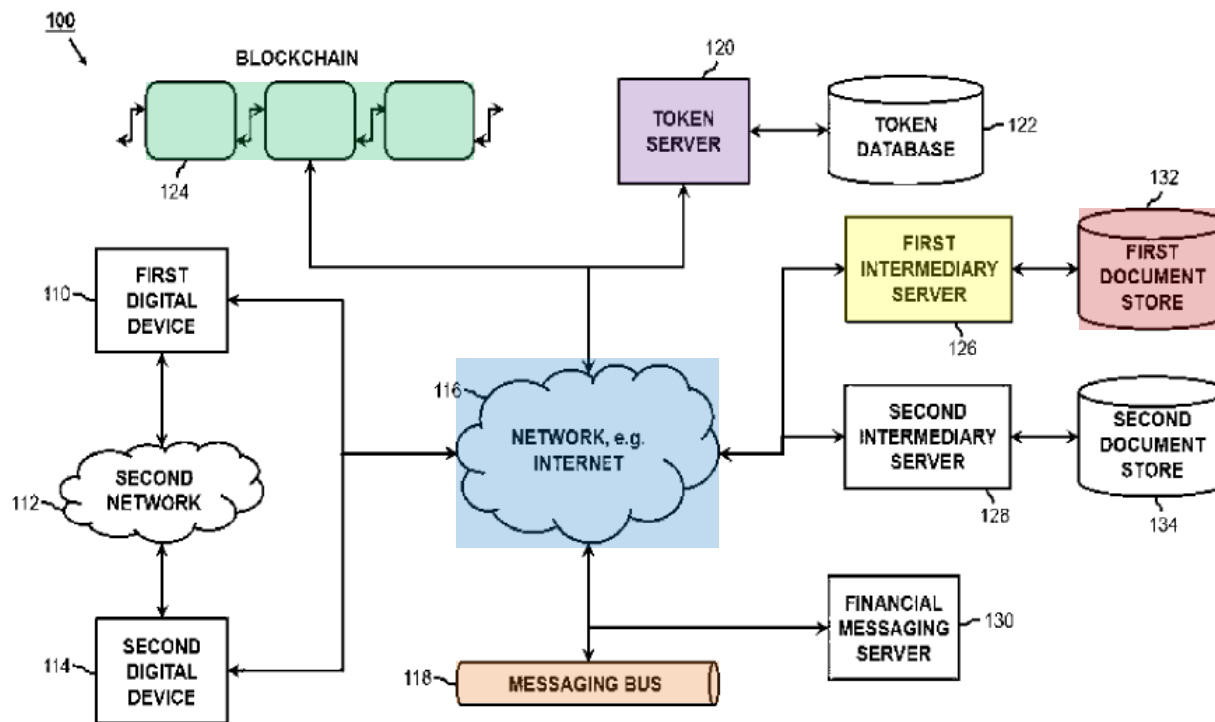
B. Nearly 80% Of The ’413 Patent Is Absent From AU-1’s Disclosures

On August 14, 2015, Applicant filed AU-1 with six rudimentary figures and a skeletal 53-paragraph specification. (Ex. 1027). By contrast, the ’413 Patent has 17 figures and 310 paragraphs. (Ex. 1001). To get from AU-1 to the ’413 Patent, Applicant appended new matter with each intervening application. Exhibit 1031 is an annotated version of the ’413 Patent showing this new matter. (Ex. 1031). In Exhibit 1031, the limited matter that originated from AU-1 is highlighted in yellow.

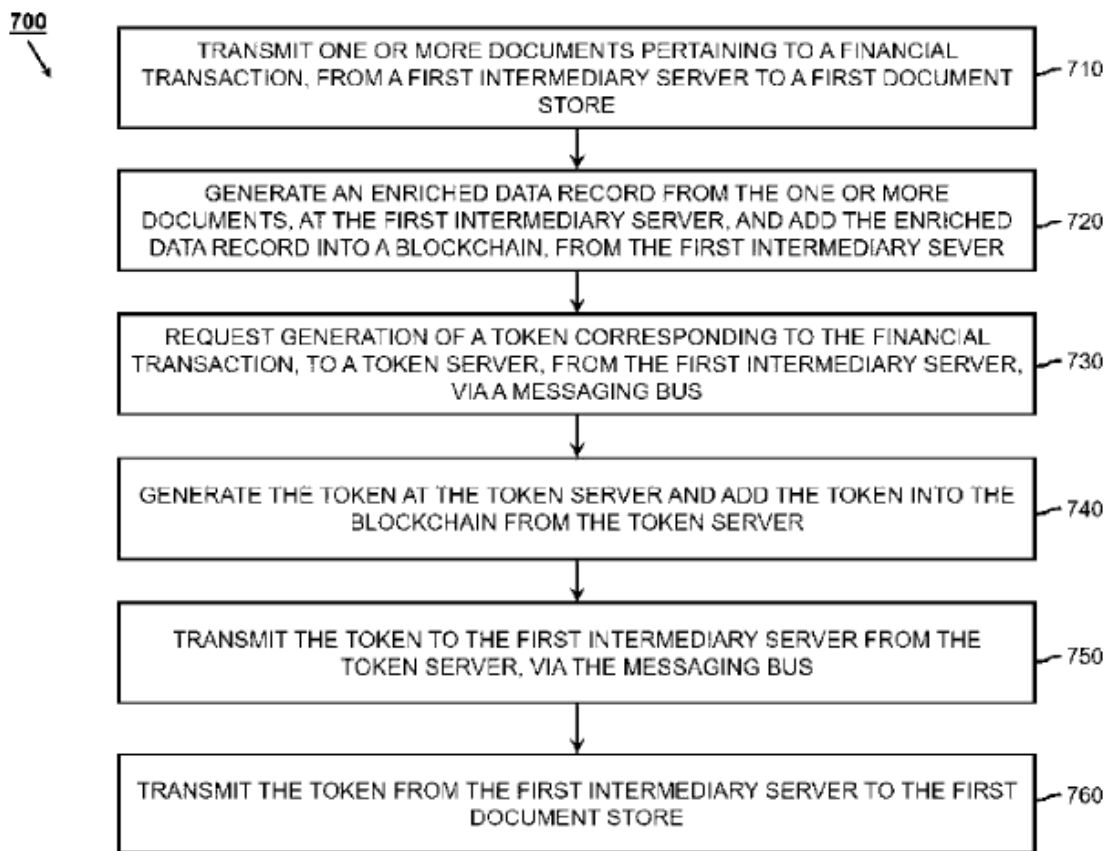
On January 27, 2016, AU-2 added two new figures and 20 additional paragraphs, shown in Ex. 1031 in purple. (*Id.* highlighted in purple). On May 20, 2016, Applicant filed AU-3 adding two new figures, an addition to a pre-existing figure, and corresponding descriptions, shown in orange in Ex. 1031. (Ex. 1031 highlighted in orange; Ex. 1029). These additions correspond to the ’413 Patent’s Figures 15B, 16, and 17 and associated portions of the specification. (Ex. 1031 highlighted in orange).

Finally, Applicant filed its PCT application on August 12, 2016—this application issued in the U.S. as the ’413 Patent. ***The PCT application included seven new figures and nearly 200 new paragraphs of specification.*** (Ex. 1031, portions without highlighting). The PCT’s new matter included Figures 1 and 7 of the ’413 Patent which

mirror the ultimately issued claims. *Figures 1 and 7 of the '413 Patent are wholly absent from AU-1, AU-2, and AU-3:*



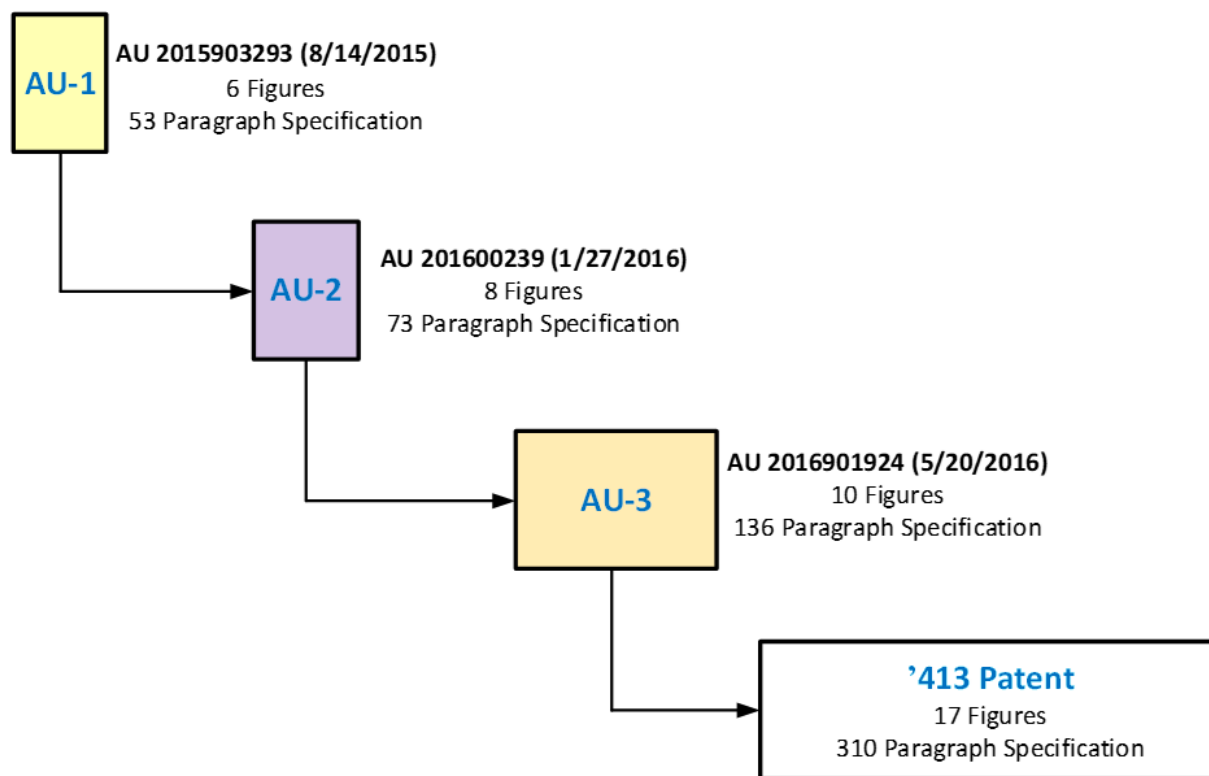
(Ex. 1001, '413 Patent, *Fig. 1* absent from AU-1, AU-2, and AU-3).



(Ex. 1001, '413 Patent, *Fig. 7 absent from AU-1, AU-2, and AU-3*).

The following illustration shows the expanding scope of the applications as filed, and Applicant's injection of new matter into each subsequent application has resulted in claims lacking written-description support.

The Australian Provisionals
Do Not Provide Written Description Support For The '413 Patent



(Ex. 1031).

C. Legal Standard And Board Authority

Claims are entitled to the filing date of a foreign priority application only “if the corresponding foreign application supports the claims in the manner required by section 112, ¶1.” *In re Gosteli*, 872 F.2d 1008, 1010 (Fed. Cir. 1989). To satisfy the written-description requirement, the specification “must describe the invention sufficiently to convey to a [POSITA] that the patentee had possession of the claimed invention at the time of the application, i.e., that the patentee invented what is claimed.” *Lizardtech, v. Earth Res.*, 424 F.3d 1336, 1345 (Fed. Cir. 2005). While “the disclosure as originally

filed does not have to provide *in haec verba* support for the claimed subject matter,” it is required that POSITA, “reading the original disclosure, must immediately discern the limitation at issue in the claims.” *Purdue Pharma v. Faulding*, 230 F.3d 1320, 1323 (Fed. Cir. 2000).

The Board has the authority to analyze Section 112 issues when determining whether the challenged claims are entitled to a certain priority date. *Indivior UK v. Reddy’s Labs.*, 18 F.4th 1323 (Fed. Cir. 2021).

D. AU-1 Does Not Provide Written-Description Support For The “Enriched Data Record” Added To The Blockchain From “The First Intermediary Server” As Claimed In The Challenged Claims

AU-1 is devoid of any disclosure about “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*,” as required by Challenged Claims. (Ex. 1026, ¶ 56). *First*, the term “*enriched data record*” *never appears in AU-1*. Moreover, there is nothing in AU-1 to suggest, much less describe, that “*the first intermediary server*” generates the “enriched data record,” or that it does so from one or more documents. (*Id.*).

In the related district-court litigation, Patent Owner stated that disclosure of “better data” constitutes an “enriched data record.” (Ex. 1045, 9 n.1). Even if this “better data” could disclose an “enriched data record”—which it does not—AU-1 is devoid of any disclosure that the “better data” is: (1) generated at or by “the first

intermediary server,” (2) generated “from the one or more documents pertaining to the financial transaction” as required by the Challenged Claims, *and also* (3) “*add[ed]...into a blockchain...from the first intermediary server.*” (Ex. 1001, 59:5-8, 62:11-16, 62:26-33; Ex. 1026, ¶¶ 56-57). At most, AU-1 states that “the token 221 will include better data 224,” and the token is generated by a “token database 223.” (Ex. 1027, [00042]). These statements bear no relation to the Challenged Claims which require “generating *an enriched data record*”—not a “token”—and doing so “at the first intermediary server”—not at the “token database.” (Ex. 1026, ¶ 57). Given the absence of any such disclosure, POSITA would understand AU-1 does not disclose “generating an enriched data record from the one or more documents, at the first intermediary server.” (*Id.*, ¶¶ 56-57).

Further, AU-1 is silent about the Challenged Claims’ requirement of “adding the enriched data record into a blockchain being a distributed ledger, from the first intermediary server.” AU-1 lacks any disclosure that—explicitly or implicitly—describes or suggests adding an “enriched data record” into a blockchain “*from the first intermediary server.*” (*Id.*, ¶ 58). At most, AU-1 makes a few cursory references to a “blockchain,” noting that embodiments “can be implemented utilizing the ‘Ripple’ framework, protocol and gateway-or more generally any block chain based framework.” (Ex. 1027, [00049]). This passage says nothing about *what information* is added to the blockchain or *from which component* the information is added into the

blockchain. (Ex. 1026, ¶ 58). The passage thus cannot support the claimed step of “adding the enriched data record into a blockchain...from the first intermediary server.” (Ex. 1001, 59:8-10). Similarly, AU-1’s disclosure that *some* data is “fed into a settlement network...operating under the Ripple protocol”—Ex. 1027, [00038]—does not support the claimed requirement that the “first intermediary server” adds an “enriched data record” to the blockchain. (Ex. 1026, ¶ 59). Likewise, AU-1’s statement that “the token database...transmits the tokenised messages as payment data records to a block chain settlement system” (Ex. 1027, [00023], claims 13, 27) cannot support the claims. This passage refers to “tokenized messages”—not the claimed “enriched data record”—and pertains to steps taken by the “token database”—not the claimed “first intermediary server.” (Ex. 1026, ¶ 59).

Applicant’s arguments during prosecution confirm AU-1’s mere mention of “blockchain” cannot disclose “adding the enriched data record into a blockchain...from the first intermediary server.” To overcome a prior-art rejection, Applicant argued that simply because an enriched data record might “be a part of the blockchain...eventually” does not mean it is added from the first intermediary server. (Ex. 1002, 291). In Applicant’s own words: “[T]hat the [first intermediary server] may initiate the blockchain transaction...doesn’t mean the [first intermediary server] adds the enriched data record ...into the blockchain network.” (*Id.*).

Bottom line: Regardless of what Patent Owner tries to assert as supporting an

“enriched data record,” there is nothing in AU-1 that suggests Patent Owner contemplated having an “enriched data record,” both generated and added to the blockchain by the very same server (*i.e.*, “first intermediary server”).

E. AU-1 Also Does Not Provide Written-Description Support For The “Token” Limitations

Applicant materially changed the description of the claimed “token” between AU-1 and the PCT application. AU-1 states that “a *‘token’ is a data record* containing data required to settle a transaction for which the token has been generated.” (Ex. 1029, [0008]). By contrast, the ’413 Patent, based on material added in the PCT application, states that “a ‘token’ *is a pointer to an enriched data record* of a plurality of data required to process a financial transaction.” (Ex. 1001, 28:66-29:1). Based on this divergence between AU-1 and the PCT, POSITA would understand that Applicant did not have possession of “token” as claimed in the ’413 Patent until the PCT application was filed. (Ex. 1026, ¶ 55).

Further, AU-1 does not disclose “adding the token into the blockchain from the token server in association with the enriched data record.” (Ex. 1026, ¶ 60). The Challenged Claims require that two separate servers—“first intermediary server” and “token server”—add two different things—an “enriched data record” and “token,”

respectively—to the “blockchain.”³ AU-1 never discloses or suggests this. (*Id.*). AU-1’s statement that “the token database...transmits the tokenised messages as payment data records to a block chain settlement system” (Ex. 1027, [00023], claims 13, 27) does not describe the claimed “token server,” nor does it suggest adding a “token” associated with an “enriched data record” to the blockchain. (Ex. 1026, ¶60). At most, this statement refers to a “token database” (not a “token server”), and to a “tokenized message” which does not describe either the claimed “token” or the claimed “enriched data record,” much less disclose an “association” between a “token” and an “enriched data record.” (*Id.*; Ex. 1001, 11:27-28 (describing “token server 120” and “token database 122” as distinct components)).

POSITA reading the four corners of AU-1 would not “*immediately discern the limitation[s] at issue* in the claims.” *Purdue*, 230 F.3d at 1323. Accordingly, AU-1 does not provide written-description support for the Challenged Claims. (Ex. 1026, ¶ 61).

V. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Prior Art

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

³ Claim 16 does not recite that the token is added to the blockchain from the token server.

1. Kennedy

Kennedy, entitled “Method And System For Processing Of A Blockchain Transaction In A Transaction Processing Network,” filed on November 5, 2015 and published on May 11, 2017, is prior art under Section 102(a)(2).

Kennedy describes using “blockchain in conjunction with a transaction processing network,” including posting, verification, and transmission of transaction data. (Ex. 1033, [0001]). Kennedy notes “[t]ransaction processing networks, also known as payment networks, involve significant hardware and infrastructure that are specifically configured to quickly process payment transactions from anywhere in the world using a vast, interconnected network.” (*Id.*, [0002]). Kennedy teaches solutions to “increase the security involved in the processing of payment transactions” in conjunction with blockchain. (*Id.*, [0003]).

Kennedy’s Figure 1 depicts a system for validating payment transactions:

100

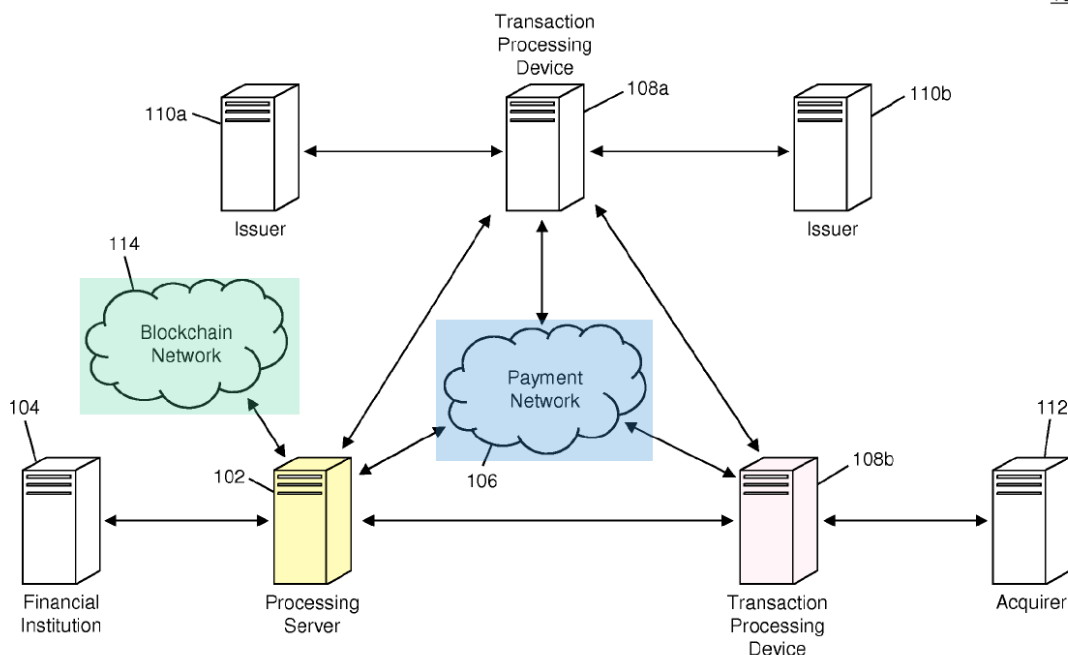


FIG. 1

(*Id.*, Fig. 1).

Kennedy teaches a “financial system 100” centered around “payment network 106” (blue). (*Id.*, [0020]). The “payment networks,” or “transaction processing networks,” transfer “money via the use of cash-substitutes.” (*Id.*, [0017]). “[P]rocessing server 102” (yellow) “assist[s] in the validation of both electronic payment transactions processed using a payment network 106 and blockchain transactions associated with a blockchain network 114” (green). (*Id.*). “[P]rocessing server 102 may be a transaction processing device 108, which may be a computing device associated with the payment network 106 used in the processing of electronic payment transactions.” (*Id.*). The processing server and transaction processing device (pink) “communicate with one or more financial institutions 104, issues 110, acquirers

112, and other entities involved in the processing of electronic payment and blockchain transactions.” (*Id.*, [0021]).

Kennedy’s “transaction messages” “include a plurality of data elements configured to store data as set forth in the associated standard, such as data elements configured to store a primary account number used to fund the payment transaction, a transaction amount, a geographic location, a merchant identifier, an acquirer identifier, an issuer identifier, financial institution data, currency data, point of sale data...” (*Id.*, [0024]).

The processing server performs “enhanced validation using the private blockchain” on transaction messages. (*Id.*). After receiving a transaction message, processing server “generate[s] a data record, which may correspond to a blockchain transaction to be posted to the private blockchain.” (*Id.*, [0026]). This generated data record includes “the message type indicator included in the transaction message as well as one or more of the transaction data values stored in the corresponding data elements in the transaction message.” (*Id.*). “[O]ne or more transaction data values may be hashed, such that the values may be verified via the generated data record.” (*Id.*, [0027]). Processing server then posts the generated data record to the private blockchain for “verif[ication] by one or more nodes included in the associated blockchain network.” (*Id.*, [0026]). The “private blockchain” is “a secure and

confidential, yet publicly accessible, record of processed payment transactions for third party verification.” (*Id.*).

2. Kurani-816

Kurani-816, entitled “Systems And Methods For Math-Based Currency Escrow Transactions,” filed on November 19, 2015 and issued on July 21, 2020, is prior art under Section 102(a)(2).

Kurani-816 describes “escrow systems and methods for transactions involving math-based currency [MBC].” (Ex. 1034, 1:17-19). Kurani-816 explains a “user of MBC can transfer funds to another party by using a private key associated with a certain value of MBC.” (*Id.*, 1:29-31). “The private key may be used to generate a signature for the transaction, and the signature can be verified by verification nodes in the MBC network.” (*Id.*, 1:31-34). Kurani-816 explains that because “more individuals are utilizing MBC in everyday transactions,” “[s]ystems and methods that provide for improved MBC escrow transactions are desired.” (*Id.*, 1:42-52).

Kurani-816 teaches a centralized financial system where “the ownership chain of the asset can be traced and verified through a MBC blockchain or ledger that serves as a record of all MBC transactions.” (*Id.*, Abstract). To verify ownership, Kurani-816 generates a “digital title or a pointer to the digital title is embedded into a MBC transfer from the seller [] to the buyer [].” (*Id.*, 3:15-22). The digital title includes “a unique identifier for the asset, a description of the asset, and ownership information concerning

the asset” and is “embodied as a token or a cryptographic string.” (*Id.*, 6:8-33, 7:3-5).

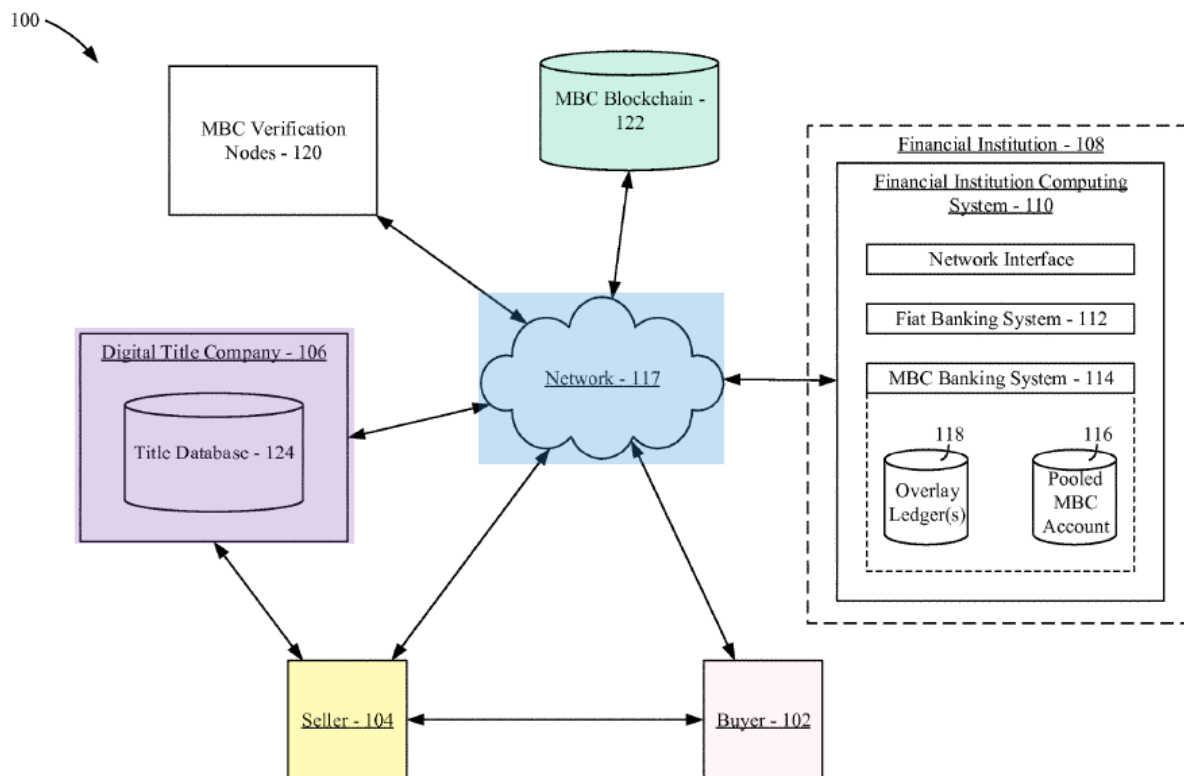


FIG. 1

(*Id.*, Fig. 1).

The “digital title company” (purple) maintains the digital titles and pointers. (*Id.*, 6:8-33.) After receiving a digital title request, the digital title company prompts generation of the digital title/token. (*Id.*, 6:42-45). The digital title request “includes information about the asset subject to the digital title request...for example, a description of the asset, a serial number associated with the asset ... any prior title information.” (*Id.*, 6:45-51).

The digital title may be “inserted into the metadata of the MBC transaction that passes title from the seller [yellow] to the buyer [pink].” (*Id.*, 6:8-33). “MBC blockchain 122” (green) contains “a series of verified transaction blocks” with “a listing of MBC transactions that occurred during the time period corresponding to the block.” (*Id.*, 5:54-59). “Each transaction in the listing of MBC transactions includes information about the transaction...amount of MBC transferred from the sender to the recipient...date and time in which the transaction was verified by the MBC nodes 120, and an additional information field or metadata field that can store additional information related to the transaction.” (*Id.*, 5:59-6:1). Kurani-816 teaches “placing the digital title or a pointer to the digital title [into that] additional information or metadata field” on the blockchain, such that the digital title may be associated with and tracked with the transaction. (*Id.*, 6:1-7).

3. Yago

Yago, entitled “Method For Creating, Issuing, And Redeeming Payment Assured Contracts Based On Mathematically And Objectively Verifiable Criteria,” filed on January 13, 2015 and published on July 23, 2015, is prior art under Sections 102(a)(1)-(a)(2).

Yago “allow[s] parties to transact with the guarantee of settlement upon completion of all elements for that trade.” (Ex. 1011, [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” (“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 4-20 Are Obvious Over Kennedy In View Of Kurani-816

1. Claim 1

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

If the preamble is limiting, Kennedy discloses it. Kennedy’s “payment network” “process[es] the transfer of money for various types of transactions.” (Ex. 1033, [0017], [0020], [0004], Fig. 1; Ex. 1026, ¶ 78).

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;

Kennedy discloses or renders obvious this element. Kennedy’s Figure 1 teaches a financial system 100 centered around payment network 106 (blue), consisting of a “processing server 102” (yellow) (“first intermediary server”) and various other interconnected transaction processing devices and servers:

100

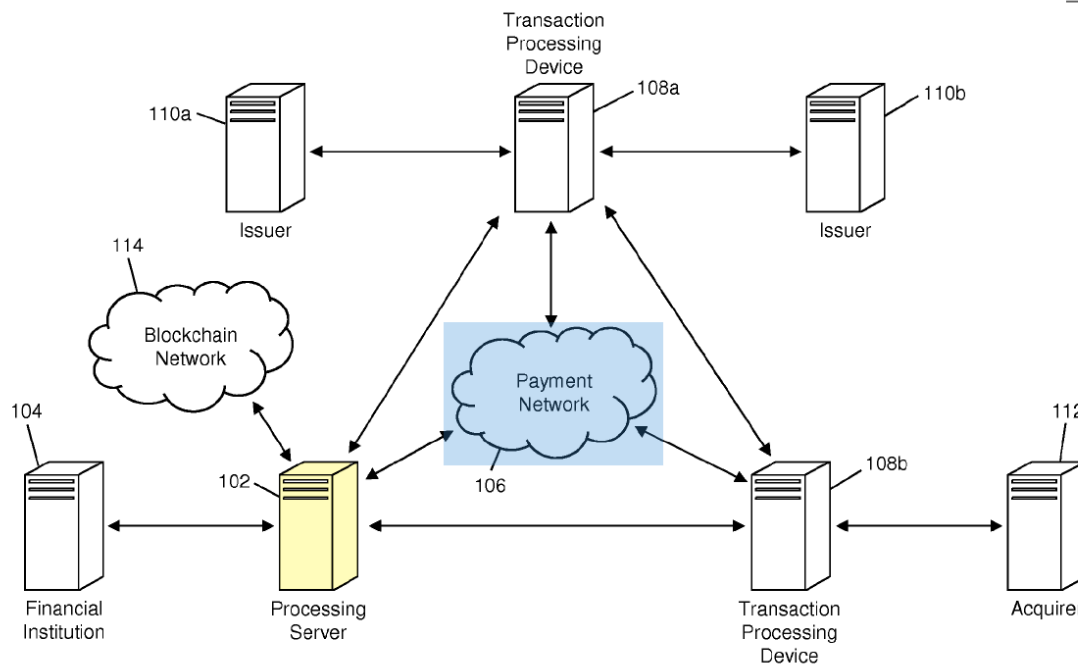


FIG. 1

(Ex. 1033, Fig. 1).

Kennedy explains that payment networks “use a variety of different protocols and procedures in order to process the transfer of money for various types of transactions.” (*Id.*, [0017]). POSITA would have understood the “payment network” connects various servers and components thereby forming the claimed “centralised financial system.” (Ex. 1026, ¶¶ 79-80).

Kennedy teaches “transaction messages” that contain financial transaction data, are “transmitted to the processing server 102 via the payment network 106, and may be formatted based on one or more standards...and include a plurality of data elements including at least data elements configured to store transaction data values for an electronic payment transaction.” (Ex. 1033, [0048], [0026]). The transaction data

values include “transaction amount, transaction time, transaction data, geographic location, primary account number, consumer data, merchant data, issuer data, acquirer data, point of sale data, loyalty data, reward data, offer data, product data, etc.” (*Id.*). Transaction messages include “a message type indicator indicative of an authorization request.” (*Id.*).

POSITA would have understood Kennedy’s transaction messages are the claimed “documents pertaining to the financial transaction” because they are records or a request relating to the transaction containing financial transaction data. (Ex. 1026, ¶¶ 81-82). This aligns with the ’413 Patent’s statement that a “document” may be “a request for processing the financial transaction.” (Ex. 1001, 12:19-20).

Kennedy discloses these transaction messages are transmitted from the “first intermediary server” to a “document store,” as claimed. Kennedy explains “processing server 102” may include “memory 228,” including “any suitable database configuration” or other “storage types.” (Ex. 1033, [0046], [0097]). The memory 228 “store[s] data for use by the processing server 102 in performing the functions.” (*Id.*, [0046], Fig. 2). The processing server’s functions include “applying authentication rules to the transaction data values stored in” a received “transaction message” to calculate authentication and verification scores. (*Id.*, [0030]). Processing server also “generate[s] a data message that includes the blockchain data from the transaction message” and “transmit[s] the transaction message to the payment network 106 for

processing.” (*Id.*, [0051]). POSITA would have understood transaction messages received by “processing server” would be stored to perform these functions and others disclosed in Kennedy, and thus be transmitted from that server to a memory/document store for such short or long-term storage. POSITA would have understood that storing documents and messages was well-known and beneficial at least for recordkeeping and maintaining a local copy of transactions for verification purposes. (Ex. 1026, ¶¶ 83-84).

Kennedy explains a communication module of the processing server “transmit[s] data between modules, engines, databases, memories, and other components of the processing server 102 for use in performing the functions.” (Ex. 1033, [0036]). For a configuration using an external database, POSITA would have understood the communication module would transmit the received transaction message to the external database for storage. For a localized-storage configuration, POSITA would have understood that storing documents would require writing that information to computer memory and/or disk storage. (Ex. 1026, ¶85). Whether the database is stored locally or externally, signals must be propagated to write the transaction messages into memory and/or disk storage. Accordingly, POSITA would have understood and found it obvious that the transaction messages are “transmitted” to the first document store, as claimed. (*Id.*).

Kennedy discloses transmitting one or more documents pertaining to the financial transaction (“transaction messages”), from a first intermediary server (“processing server 102”) in a centralised financial system (“system 100” centralized around “payment network 106”) to a first document store (“memory”). (*Id.*, ¶ 86).

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;

Kennedy discloses or renders obvious this element. Kennedy teaches that processing server “receive[s] the transaction message” and has a “generation module 216” that “generate[s] a data record” from “transaction data values stored in the data elements included in the transaction message.” (Ex. 1033, [0026], [0049]). The “generated data record” (*i.e.*, “enriched data record”) “may correspond to a blockchain transaction to be posted to the private blockchain,” including “message type indicator included in the transaction message as well as one or more of the transaction data values stored in the corresponding data elements in the transaction message.” (Ex. 1033, [0026]). Kennedy teaches that “transaction data values included in the generated data record may be hashed and/or encrypted using one or more suitable hashing and encryption algorithms, respectively.” (Ex. 1033, [0049]). This aligns with the ’413 Patent’s description that an “enriched data record” comprises a combination “of a plurality of attributes from one or more documents” that may be “hashe[d].” (Ex. 1001, 2:36-62, 12:39-64).

Kennedy's Figure 3 shows the "generated data record" is generated at the "processing server" ("first intermediary server") based on "transaction messages" ("one or more documents"):

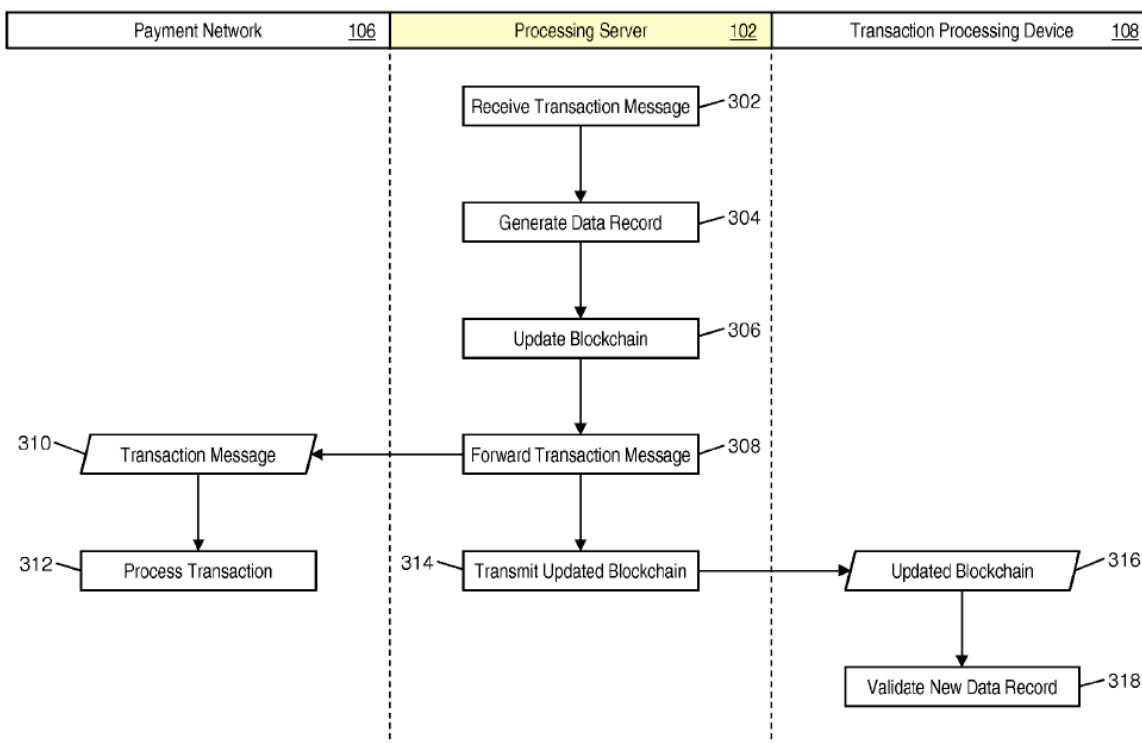


FIG. 3

(Ex. 1033, Fig. 3). The processing server "update[s] a private blockchain by adding the generated data record to the blockchain." (*Id.*, [0050]). POSITA would have understood Kennedy's "private blockchain" to be a "distributed ledger," as claimed. (Ex. 1026, ¶¶ 87-89; Ex. 1033, [0018]).

In Kennedy, "updating of the private blockchain may include the submission of the generated data record to the blockchain network 114 and/or one or more nodes associated therewith for verification and adding to the private blockchain." (Ex. 1033,

[0050]). In Kennedy's Figure 1, the "generated data record" is added to the blockchain from the "processing server":

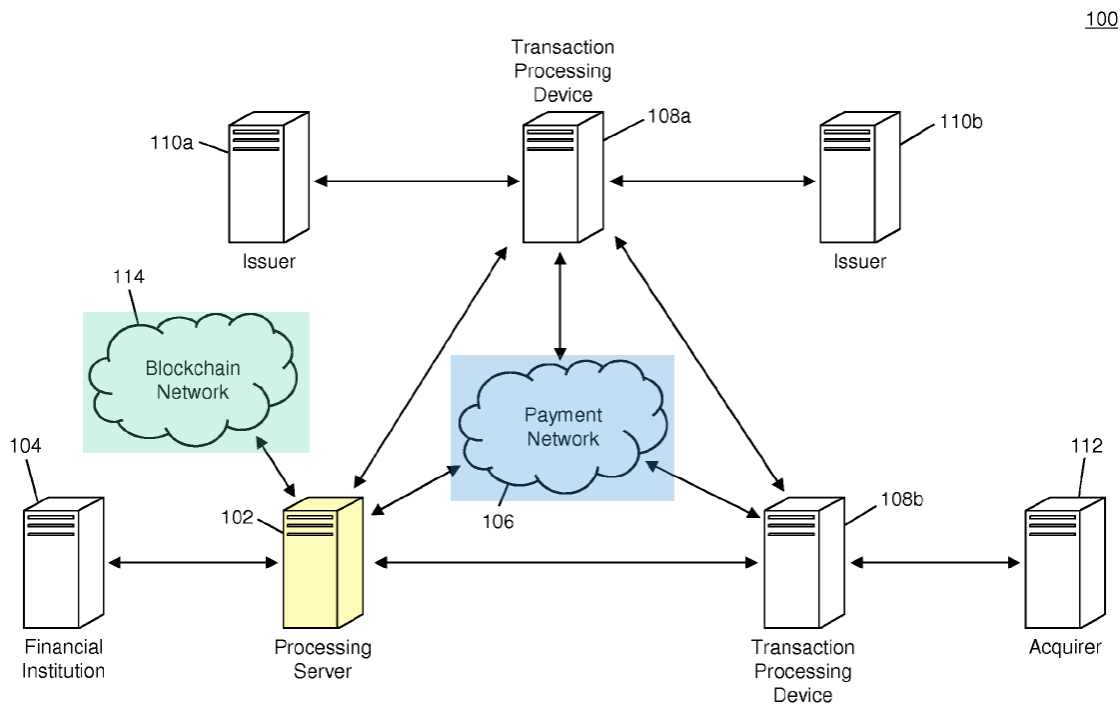


FIG. 1

(*Id.*, [0049-0050], Fig. 1).

Kennedy discloses generating an enriched data record ("generated data record"), from one or more documents ("transaction message"), at the first intermediary server ("processing server 102"), and adding the enriched data record into a blockchain being a distributed ledger ("blockchain" in "blockchain network 114"), from the first intermediary server ("processing server 102"). (Ex. 1026, ¶¶ 90-91).

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;

The Kennedy/Kurani-816 combination renders obvious this element. Kennedy explains the financial transaction is associated with a “transaction identifier,” or “one or more transaction data values suitable for...identifying the new data record corresponding to the electronic payment transaction.” (Ex. 1033, [0052]). Kennedy teaches this “transaction identifier” is included in “the plurality of additional data elements” of the “transaction message, and is further included in the data record generated from the transaction message. (*Id.*, [0071], claims 1&7 (reciting “plurality of additional data elements includes a transaction identifier, and the generated data message further includes the transaction identifier”)). Kennedy also explains the transaction identifier is included in notifications or communications sent between servers and devices within the financial system such that each transaction’s data record is identified and traced using a common variable. (*Id.*, [0052]).

To the extent Kennedy’s “transaction identifier” does not teach the claimed “token,” Kurani-816 clearly discloses this. (Ex. 1026, ¶¶ 92-94). Kurani-816 describes recording and verifying sale transactions, where “the ownership chain of the asset can be traced and verified through a MBC blockchain or ledger that serves as a record of all MBC transactions.” (Ex. 1034, Abstract). Kurani-816 teaches requesting and generating a digital title, where “the digital title or a pointer to the digital title is

embedded into a MBC transfer from the seller [] to the buyer []” so the transaction and associated ownership of the assets is tracked and verified. (*Id.*, 3:15-22). The “digital title” “includes *a unique identifier* for the asset, a description of the asset, and ownership information concerning the asset.” (*Id.*, 7:3-5). Kurani-816 explains the “digital title” may be “embodied as a *token* or a cryptographic string,” where the “*token* or cryptographic string itself [is] inserted into the metadata of the MBC transaction.” (*Id.*, 6:8-33).

POSITA would have understood Kurani-816’s “digital title”—“embodied as a token or a cryptographic string” (*id.*)—corresponds to the claimed “token,” identifying the transaction by serving as a “unique identifier” associated with the asset being purchased and used for recording and tracking title transfers. (Ex. 1026, ¶95; Ex. 1034, 3:15-22, 7:3-5). Likewise, the ’413 Patent describes 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; Ex. 1026, ¶ 95).

POSITA would have understood a well-known way of generating Kurani-816’s “token” or “cryptographic string” is to use the digital-title transaction data as an input to generate an identifying output. (Ex. 1026, ¶ 96). This was conventional in the financial industry even before the filing of AU-1. (*Id.*; *see, e.g.*, Ex. 1017, [0024-0026]; Ex. 1018, [0019]).

For example, one problem facing those seeking to assign a unique token was that of “collision,” where the processes used to generate the tokens or identifiers result in identical keys for more than one transaction. (Ex. 1026, ¶ 97). POSITA would have understood that ensuring uniqueness of the digital title/token would avoid this issue, and would be accomplished via generic data manipulation using transaction data as an input to an algorithm to generate a unique output. (*Id.*). Doing so would mitigate the risk of collision and would have been obvious to POSITA. (*Id.*).

Accordingly, it would have been obvious to POSITA to generate Kurani-816’s digital title/token by formatting or passing the digital title transaction information through an algorithm in a predetermined manner to achieve a “token” that is “unique” and identifies the transaction and asset. (*Id.*, ¶ 98).

POSITA would have found Kurani-816’s “digital title” token to be an improvement on Kennedy’s “transaction identifier,” because it could serve as a pointer to the transaction and also as a unique identifier of an asset and means to transfer title. (*Id.*, ¶99; Ex. 1034, 6:8-33). Kennedy makes clear that an intended use of its system is to transact “product” purchases. (Ex. 1033, [0017]). POSITA seeking to utilize Kennedy’s system for sophisticated transactions and asset sales would have been motivated to implement Kurani-816’s “digital title” token in Kennedy’s system. (Ex. 1026, ¶99). Kennedy recognized sophistication levels of transactions were trending upwards: “transaction processors are often constantly developing new technologies to

further increase the sophistication of these networks, to provide for even more security to protect against fraud and to provide peace of mind to consumers.” (Ex. 1033, [0002]). “[T]he effects of demands known to the design community or present in the marketplace” often demonstrate a motivation to combine prior-art elements from different references.” *KSR v. Teleflex*, 550 U.S. 398, 418 (2007).

Kurani-816’s “digital titles” and pointers are “maintained by the digital title company 106” and associated “digital title company computing system,” which POSITA would have understood to be a “token server.” (Ex. 1034, 6:8-41; Ex. 1026, ¶ 100).

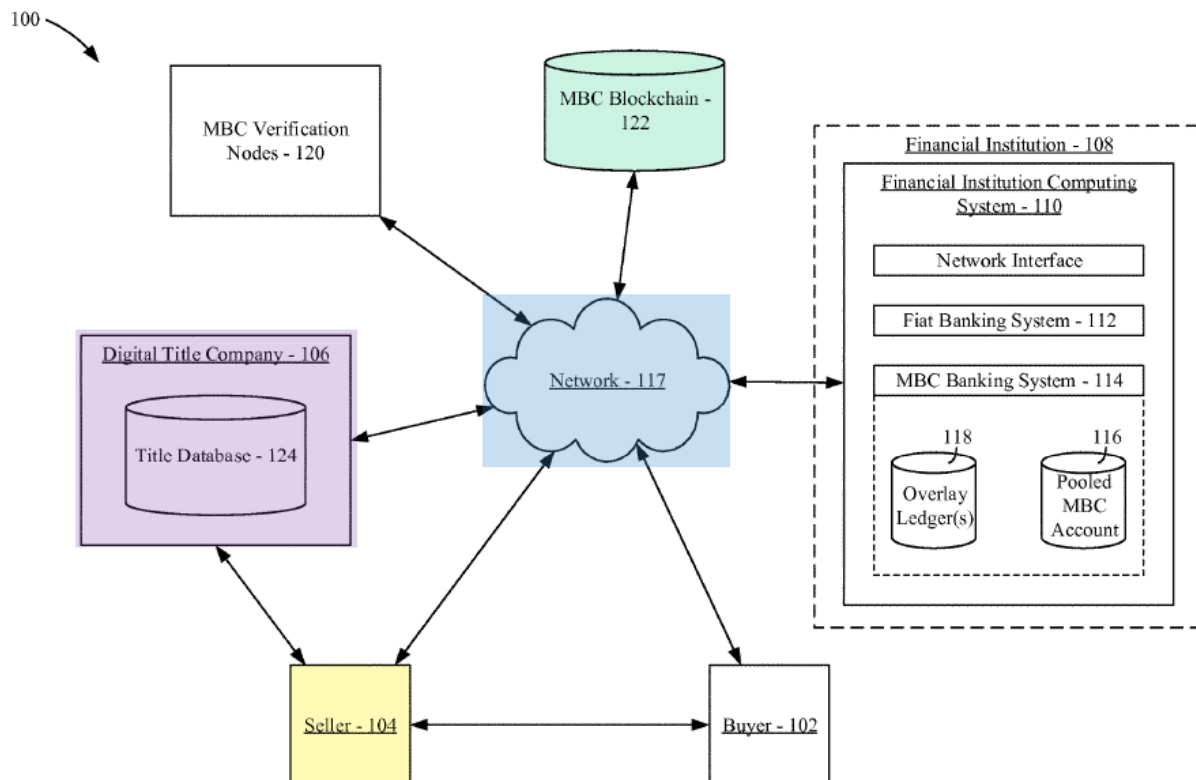


FIG. 1

(Ex. 1034, Fig. 1). Kurani-816's "digital title company" receives a "digital title request" prompting the "digital title company" to generate the digital title/token. (*Id.*, 6:43-45, Fig. 2). Figure 1 shows the seller server transmits a request for digital title generation to digital title company server. (*Id.*). Thus, Kurani-816 teaches that the token generation request originates at, and is transmitted from, a different and separate server from the server responsible for generating tokens. (Ex. 1026, ¶ 101).

Applying Kurani-816's teachings to Kennedy, POSITA would have been motivated to transmit the token generation request from Kennedy's processing server (*i.e.*, "the first intermediary server") so the request for digital title generation is transmitted from a server processing the transaction that is separate from the token generating server. (*Id.*, ¶ 102). POSITA would have found Kurani-816's disclosure of a separate token server advantageous because it provides a neutral and independent location for generating tokens that is not affiliated with any participating buyer, seller, bank, etc. (*Id.*).

For several reasons, POSITA would have been motivated to combine Kennedy's financial system with Kurani-816's token request and generation. (*Id.*, ¶ 103). Both Kennedy and Kurani-816 describe financial transaction verification and authorization systems utilizing blockchain. (Ex. 1026, ¶ 103; Ex. 1033, [0001]; Ex. 1034, Abstract). Both Kennedy and Kurani-816 seek to achieve the same goal: improving systems for blockchain financial transactions. (Ex. 1026, ¶ 104). Kennedy attempts to "increase

the security involved in the processing of payment transactions.” (Ex. 1033, [0003]). Kurani-816 notes “[s]ystems and methods that provide for improved MBC escrow transactions are desired.” (Ex. 1034, 1:51-52, 4:65-5:2).

Kennedy and Kurani-816 teach similar approaches. (Ex. 1026, ¶105). Kennedy describes “validating blockchain transactions using a transaction processing network” comprising interconnected processors and servers, where transaction messages are verified and stored on the blockchain. (Ex. 1033, [0004-0005], [0017]). Kurani-816 describes “facilitating the sale of an asset having digital title” where transaction data is “traced and verified through a MBC blockchain or ledger.” (Ex. 1034, Abstract).

Applying Kurani-816’s teaching of “digital title” generation with Kennedy’s “use of blockchain in conjunction with a transaction processing network” (Ex. 1033, [0001]) is simply the predictable use of prior-art elements according to their established functions. In fact, before AU-1, POSITA would have understood requesting and generating tokens to track transactions was well-known in the art. (Ex. 1026, ¶ 106; Ex. 1046, [0007] (“Non-payment tokens are often used by merchant and acquirer systems to keep track of transactions.”). For example, a token generation system (including “token processing server computer”) that “can be leveraged by external entities” was used with financial transactions to “improve[] protection against the misuse of payment accounts by providing usage controls” and reduce fraud by determining a “token assurance level” for the “token requestor” at the time of

generation. (Ex. 1046, [0034], [0046-0047], [0101]). Kennedy itself contemplates using rudimentary transaction identifiers. (Ex. 1033, [0052], [0071-0072], claims 1&7). Reading Kennedy, POSITA would have been motivated to look to known token generation systems to create a transactional system with increased verification and tracking measures. (Ex. 1026, ¶ 107). As explained above, POSITA would have been motivated to implement Kurani-816's token generation in Kennedy's system to achieve the added benefit of tracing title transfers for more sophisticated transactions, such as high-end asset sales. (*Id.*). Kennedy notes "increas[ing] sophistication" can "provide for even more security to protect against fraud and to provide peace of mind to consumer." (Ex. 1033, [0002], [0017]).

POSITA would have had a reasonable expectation of success in applying Kurani-816's teachings into Kennedy transaction processing system. (Ex. 1026, ¶ 108). Token request and generation by a token server were well-known and understood by POSITA. (*Id.*; Ex. 1046). Combining well-understood technologies of Kennedy and Kurani-816 would yield predictable results. (*Id.*).

Additionally, Kennedy/Kurani-816 renders obvious requesting the generation of a token "via a messaging bus." (*Id.*, ¶¶ 109-11). Kennedy and Kurani-816 describe communication channels that POSITA would understand to be a "messaging bus." Kennedy teaches its "processing server" (*i.e.* "first intermediate server") may include a "communication module" that "utilize[s] various communication methods for

communications within a computing device... [f]or example...*a bus*.” (Ex. 1033, [0036]). Kurani-816 explains its computing system uses “local and remote processing devices that are linked ... *through a communications network*.” (Ex. 1034, 11:61-12:5). Similarly, the ’413 Patent describes the “term ‘bus’...should be construed broadly herein as any system for communicating data.” (Ex. 1001, 33:35-45).

Kennedy’s communication module “communicate[s] between internal components of the processing server 102 and external components of the processing server 102, such as externally connected” devices like Kurani-816’s token server. (Ex. 1033, [0036], [0088-0089], [0098]; Ex. 1026, ¶ 111). Thus, the Kennedy/Kurani-816 combination discloses “requesting...via a messaging bus.” (Ex. 1026, ¶ 111).

The Kennedy/Kurani-816 combination renders obvious requesting generation of a token corresponding to the financial transaction to identify one or more documents (“digital title”/ “token” generation request), to a token server (“digital title company 106”), from first intermediary server (“processing server 102”), via a messaging bus (communication network) in the centralised financial system. (Ex. 1026, ¶112).

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 Kennedy/Kurani-816 combination would have rendered this element obvious. After Kurani-816’s “digital title company” (“token server”) receives the digital title request, “[t]he digital title company computing system creates the digital

title” and “a unique token associated with the digital title.” (Ex. 1034, 6:66-7:18).

Kurani-816 explains the “digital title”—“embodied as a token or a cryptographic string”—is “*inserted into the metadata of the MBC transaction* that passes title from the seller [] to the buyer.” (*Id.*, 6:8-33). Kurani-816 teaches “MBC blockchain” containing “a series of verified transaction blocks” and “a listing of MBC transactions that occurred during the time period corresponding to the block.” (*Id.*, 5:54-59). “Each transaction in the listing of MBC transactions includes information about the transaction, including a sender identity number...a recipient identity number...an amount of MBC transferred from the sender to the recipient, a date and time the transaction was broadcast by the sender, a date and time in which the transaction was verified by the MBC nodes 120, and an additional information field or *metadata field that can store additional information related to the transaction.*” (*Id.*, 5:59-6:1). Kurani-816 teaches “placing the digital title or a pointer to the digital title [into that] additional information or metadata field” of the MBC transaction block. (*Id.*, 6:1-5).

POSITA would have understood that in the Kennedy/Kurani-816 combination, the digital title/token would be added to the blockchain in association with Kennedy’s “generated data record” (“enriched data record”). (Ex. 1026, ¶¶ 113-15). Kennedy’s “generated data record” represents a financial transaction containing various transaction information that is added to the blockchain. (Ex. 1033, [0050], [0062]). The transaction may then be validated by the transaction processing device. (*Id.*,

[0053], [0063]). After the transaction is processed, Kennedy's blockchain is "further updated" to include the generated data record and a validated "new data record." (*Id.*, [0065]). Kurani-816's "digital title" is "written in the MBC blockchain" when the MBC transfer, or transaction, is verified. (Ex. 1034, 9:43-47). POSITA would understand that in the Kennedy/Kurani-816 combination, the digital title—indicative of a processed financial transaction and the "pass[ing of] title from seller [] to buyer"—would be added to the blockchain in association with the "generated data record" containing various information for the financial transaction. (Ex. 1026, ¶ 115).

Additionally, it would have been obvious to POSITA that the token in the Kennedy/Kurani-816 combination is "added into the blockchain from the token server" as claimed. Kurani-816's Figure 1 depicts two-way communication between "digital title company" and tMBC blockchain via the network. (*Id.*, ¶ 116).

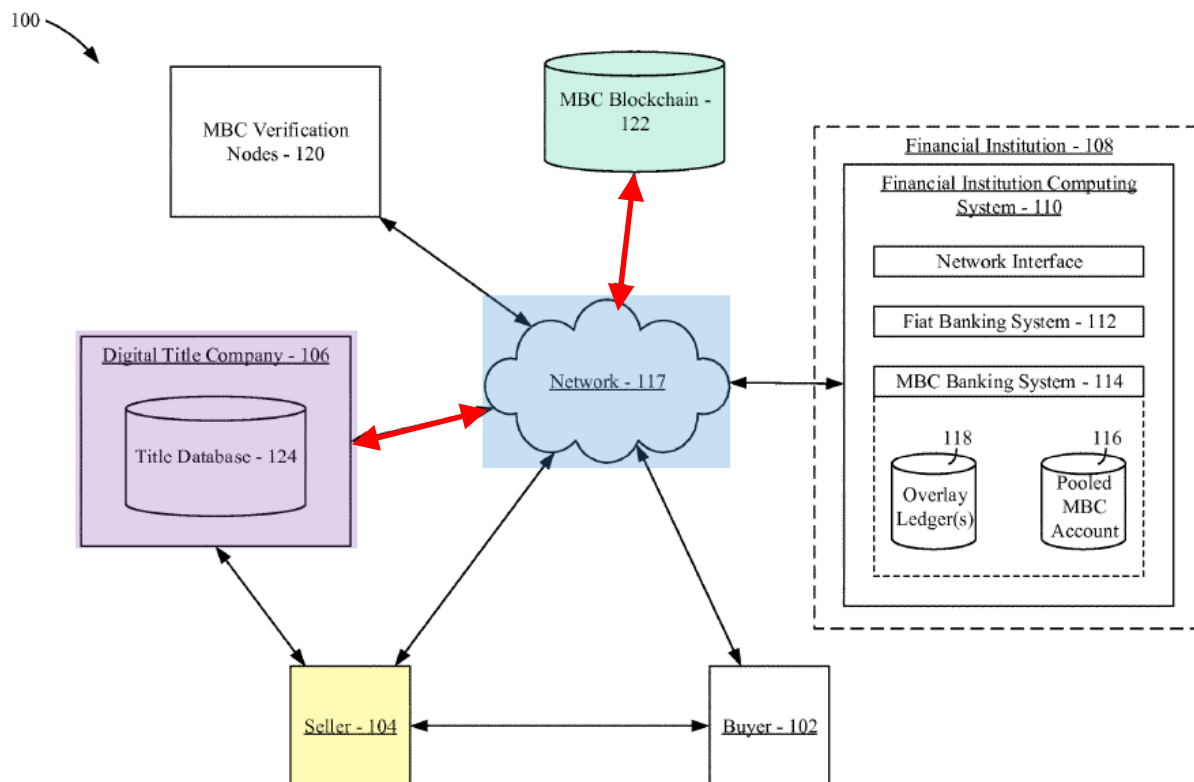


FIG. 1

Kennedy's stated goal is "to protect against fraud and to provide peace of mind to consumers." (Ex. 1033, [0002]). As explained for element 2, use of token servers to reduce misuse and fraud by a token requestor was well-known. (Ex. 1046, [0034], [0046-0047], [0101]). POSITA would recognize that having the system that generated digital title ("token") add the token into the blockchain would ensure integrity of information. Doing so would mitigate risk of token data being corrupted by intermediaries before adding to the blockchain. In the Kennedy/Kurani-816 combination, POSITA would understand digital title/token is added to the blockchain by the token server, for example when the blockchain is "further updated" to include

generated data record and “new data record” reflecting the processed financial transaction. (Ex. 1026, ¶ 117).

For these reasons—including motivations to combine explained for element 3—the Kennedy/Kurani-816 combination renders obvious generating the token (“digital title”/“token”) at the token server (“digital title company 106”) and adding the token into the blockchain (“blockchain” in “blockchain network 114”) from the token server in association with the enriched data record (“generated data record”). (*Id.*, ¶ 118).

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

The Kennedy/Kurani-816 combination discloses this element. Kennedy teaches a “transaction identifier” may be included in the “generated data record” (“enriched data record”) generated by the “processing server” (“first intermediary server”). (Ex. 1033, [0071-0072], claims 1&7). Though Kennedy does not explicitly disclose transmitting a “transaction identifier” or token from a token generation server to the “processing server,” Kurani-816 teaches this element. POSITA would have been motivated to combine Kennedy’s financial system with Kurani-816’s teachings of token request/generation as explained for element 3. (Ex. 1026, ¶ 119).

Kurani-816 teaches that “[t]he digital title request is received by the digital title company computing system *from a title requestor (e.g., the owner of an asset).*” (Ex. 1034, 6:43-45). The “digital title company” then “creates a unique token associated

with the digital title...[which] *may be provided to the verified owner of the asset.*” (*Id.*, 7:7-9). In Figure 1, the “digital title company” transmits the “digital title” token to seller (asset owner). (*Id.*, 6:43-45, 7:7-9).

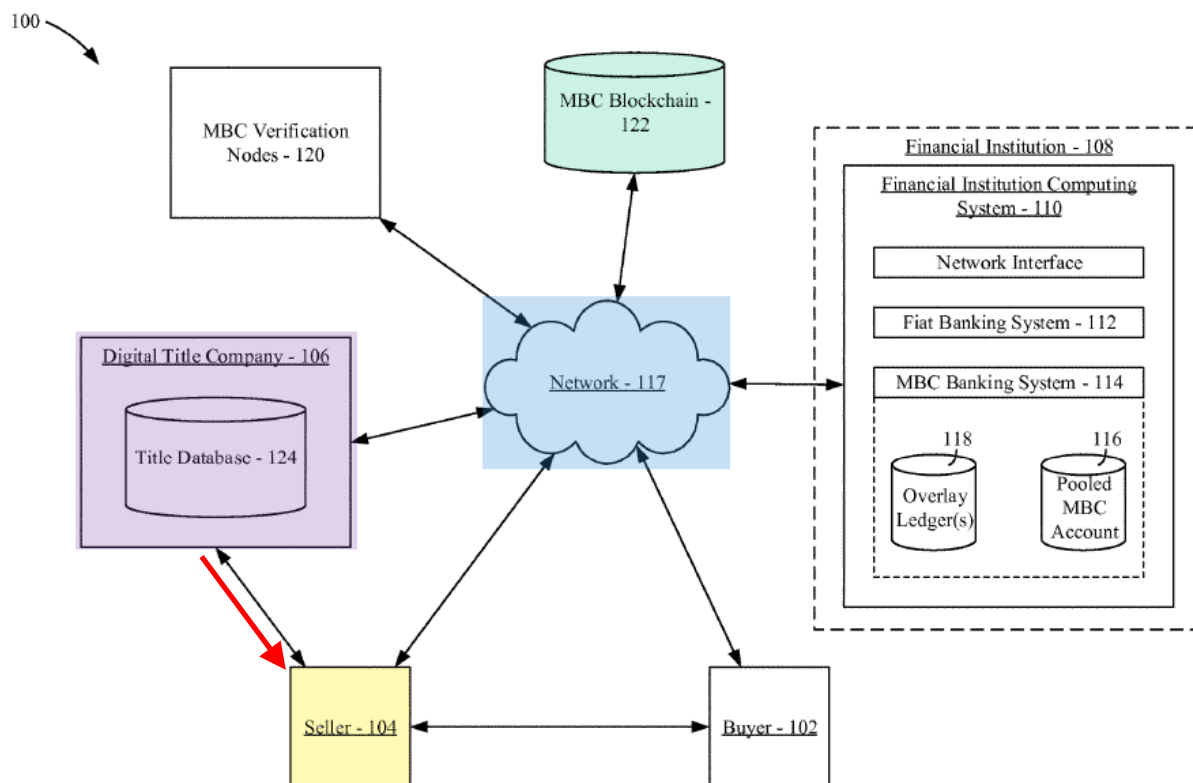


FIG. 1

(*Id.*, Fig. 1). As explained for element 3, POSITA would have understood that within the Kennedy/Kurani-816 combination, Kennedy’s “processing server” sends the token generation requests, so the request for the digital title/token originates from the server processing the transaction and generating the data record. (Ex. 1026, ¶¶ 120-21). Based on Kurani-816’s teachings, POSITA would have been motivated to transmit the token from Kurani-816’s “digital title company” (“token server”) to

Kennedy’s “processing server” (“first intermediary server”), to ensure that the digital title/token is associated and stored with the transaction record and documents. (*Id.*). As explained for Kennedy and Kurani-816’s communication channels for element 3, POSITA would have understood this transmission occurs via a messaging bus. (*Id.*).

The Kennedy/Kurani-816 combination renders obvious transmitting the token (“digital title”/“token”) to the first intermediary server (“processing server”) from the token server (“digital title company”), via the messaging bus (“communication network”). (*Id.*, ¶ 122).

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

The Kennedy/Kurani-816 combination discloses this element. As explained for element 1, Kennedy describes memory for storing transaction data, which POSITA would have understood is a “first document store” for storing transaction messages. (Ex. 1033, [0046]; Ex. 1026, ¶ 123). Kennedy’s transaction identifier is part of “the plurality of additional data elements” of the “transaction message[s]” being stored. (Ex. 1033, [0071-0072]; claims 1&7). Kennedy also teaches the processing server (“first intermediary server”) performs additional processing of the transaction data, including transmitting the data to other parts of the payment network, even after the blockchain has been updated to include the generated data record (“enriched data record”). (*Id.*, [0063-0065]).

From these disclosures, POSITA would have found it obvious to store Kennedy's transaction identifier/token in association with transaction messages in the "first document store" as claimed, to facilitate additional processing performed on transaction data and to maintain a fulsome local record of the transaction to compare against the record stored on the blockchain. (Ex. 1026, ¶ 124). The Kennedy/Kurani-816 combination renders obvious transmitting the token ("digital title"/"token") from the first intermediary server ("processing server") to the first document store ("memory") in association with the one or more documents ("transaction messages"). (*Id.*, ¶ 125).

Claim 1 therefore would have been obvious over the Kennedy/Kurani-816 combination. (*Id.*, ¶ 126).

2. Claim 2

Claim 2 depends from claim 1. (Ex. 1001, 59:24-29). The Kennedy/Kurani-816 combination would have rendered this claim obvious. (*Id.*, ¶¶ 127-28). Kennedy teaches processing financial payments where "each processing server" and "transaction processing device" "communicate with one or more financial institutions 104, issues 110, acquirers 112, and other entities involved in the processing of electronic payment and blockchain transactions." (Ex. 1033, [0021], [0083-0084]).

Kennedy transmits a "notification" from the "processing server" to a "transaction processing device" comprising "one or more transaction data values suitable for use in identifying the new data record corresponding to the electronic payment transaction,

such as a transaction identifier.” (*Id.*, [0052]). Kennedy thus provides transmitting messages from a “processing server” (“first intermediary server”) to another “transaction processing device” (“second intermediary server”) containing transaction identifiers. (Ex. 1026, ¶¶ 128-29).

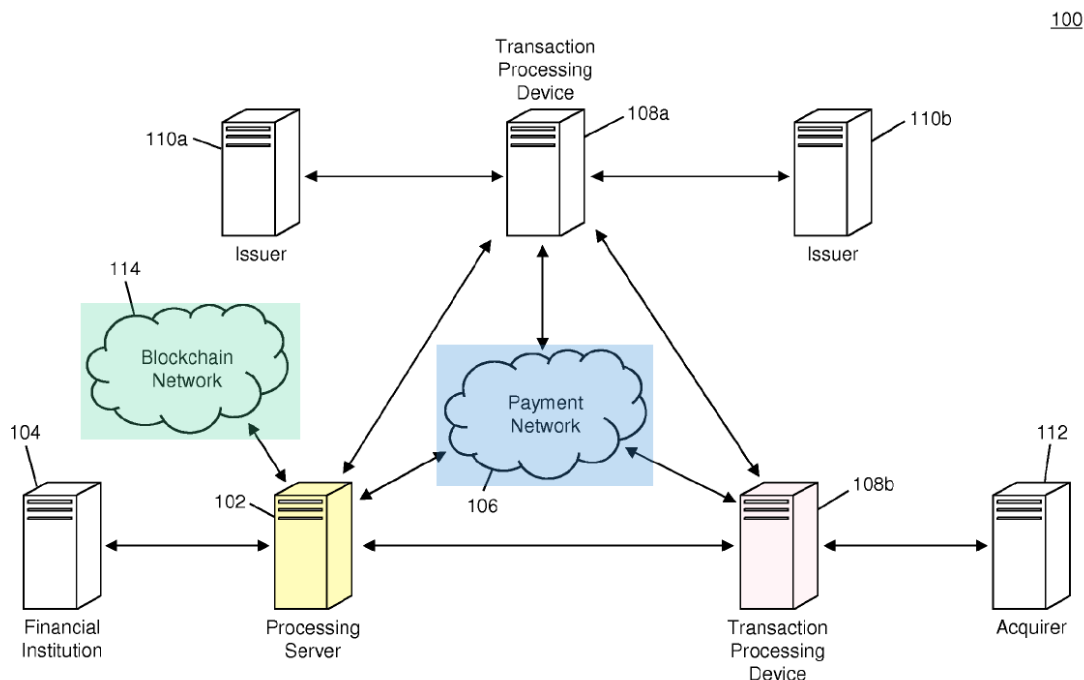


FIG. 1

(Ex. 1033, Fig. 1).

Kurani-816 similarly teaches the “unique token associated with the digital title may be provided to the verified owner of the asset. In such arrangements, to pass ownership of the asset to another party, the owner can pass the token to the receiving party.” (Ex. 1034, 7:8-11). POSITA would have understood that Kurani-816’s receiving party/buyer would have a separate server, as shown in pink above so the digital title/token is passed from a first server (yellow) to a second server (pink), just

like Kennedy. (Ex. 1026, ¶ 130).

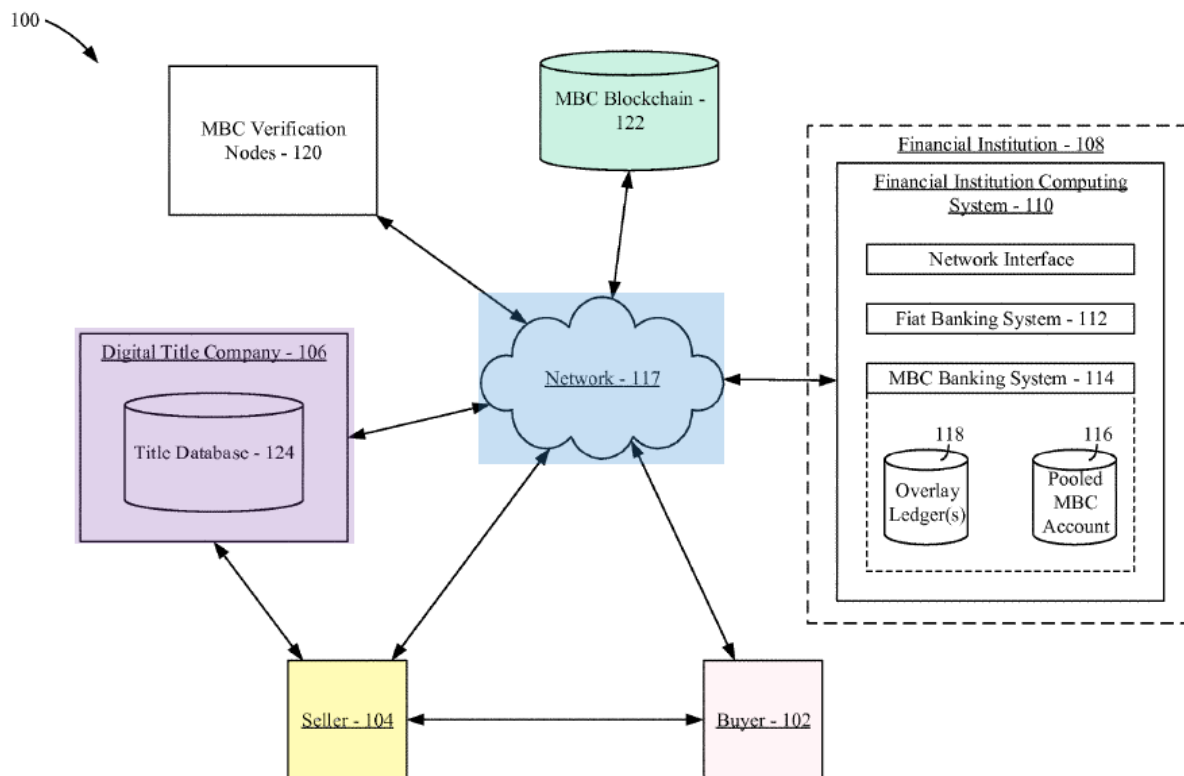


FIG. 1

(Ex. 1034, Fig. 1).

Communication between servers during payment transactions was well-known. POSITA would have been motivated to implement Kurani-816's transmission of digital titles/tokens within Kennedy's payment network so Kennedy's "processing server" transmits the token to the "transaction processing device" of a second user during payment. (Ex. 1026, ¶ 131). Kennedy already discloses transmitting messages including transaction identifiers. POSITA would have been motivated to implement Kurani-816's digital title/token into Kennedy's system to process more sophisticated

transactions. (*Supra* claim 1 elements 3&4; Ex. 1026, ¶ 131). POSITA would have been further motivated to include the token in messages exchanged between users and/or servers to create a common point of identity in each message that ties the exchange back to the transaction. (Ex. 1026, ¶¶ 131-32).

3. Claim 4

Claim 4 depends from claim 1. (Ex. 1001, 59:35-49). The Kennedy/Kurani-816 combination would have rendered this claim obvious. (*Id.*, ¶¶ 133-34). As explained for claim 2, Kennedy and Kurani-816 transmit messages containing transaction identifiers or digital titles/tokens. (Ex. 1033, [0052]; Ex. 1034, 7:8-11). POSITA would have understood a straightforward, well-known way for one party to pass the token to a receiving party is through device-to-device transfer, such as through personal computers. (Ex. 1026, ¶ 134). Kurani-816's "system includes a network interface configured to communicate with customer devices associated with customers via a network." (Ex. 1034, 2:12-14). Kurani-816 teaches that its "processor" receives "from either a buyer device associated with a buyer or a seller device associated with a seller, an indication that the seller agreed to transfer ownership of an asset to a buyer through a transfer of digital title via a math-based currency transaction," "an amount of funds from the buyer," and "an identifier of the math-based currency transaction from the seller device." (*Id.*, 2:18-26).

POSITA would have understood from Kurani-816's teachings that digital

titles/tokens may be sent from the “seller device” (“first digital device available with a first user”) to the “buyer device” (“second digital device” of a “second user”). (Ex. 1026, ¶ 135). POSITA would also have understood that within the Kennedy/Kurani-816 combination, processors associated with each device (“first intermediary server” and “second intermediary server”) would be involved in transmission and receipt of the digital title/token so the token is transmitted: (1) from the “processing server” to the “seller device” (“transmitting the token from the first intermediary server to a first digital device available with a first user”); then (2) from seller to buyer via device-to-device transfer (“providing the token to a second user, by the first user”); and then (3) from the “buyer device” to the “transaction processing device” associated with buyer (“providing the token to a second intermediary server in the centralised financial system, from a second digital device”). (*Id.*).

After the digital title/token is sent to buyer, POSITA would have found it obvious to transmit the token to memory (“second document store”) from the “transaction processing device” (“second intermediary server”) associated with buyer. (*Id.*, ¶ 136). As explained for element 1, Kennedy and Kurani-816 disclose various storage configurations. POSITA would have found it well-known to store tokens and other transaction data locally for verification and record-keeping. (*Id.*).

As explained for claim 2, POSITA would have understood communication between servers during a payment transaction was well-known, as is using a token as a

transaction identifier throughout the course of payment. Thus, POSITA would have been motivated to include the token in any payment messages or transmissions from the second server to the first server (*i.e.*, “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”) to maintain a complete record of the transaction and assist with tracking the chain of title or other financial transfer throughout processing. (*Id.*, ¶¶ 137-38).

4. Claim 5

Claim 5 depends from claim 1. (Ex. 1001, 59:50-56). The Kennedy/Kurani-816 combination would have rendered this claim obvious as explained for claim 1, element 2. (Ex. 1026, ¶¶ 139-41). Kennedy’s “processing server” “generate[s] a data record” from the transaction message, where the “generated data record” includes extracted attributes like “the message type indicator included in the transaction message as well as one or more of the transaction data values stored in the corresponding data elements in the transaction message.” (Ex. 1033, [0026], [0049], Fig. 2).

5. Claim 6

Claim 6 depends from claim 1. (Ex. 1001, 59:57-67).” The Kennedy/Kurani-816 combination would have rendered this claim obvious, as explained for element 2 of claims 1 and 5. Kennedy also teaches “transaction data values included in the generated data record may be hashed and/or encrypted using one or more suitable

hashing and encryption algorithms, respectively.” (Ex. 1033, [0049]). Kennedy teaches that “the primary account number associated with the transaction account used to fund the payment transaction may be hashed such that the payer may be verified using the hashed primary account number, but without the actual primary account number being obtainable via the data record posted to the private blockchain.” (*Id.*). POSITA would have understood hashing and encryption serve to “de-identify” transaction attributes because they remove and/or mask personal transactional information. (Ex. 1026, ¶¶ 142-43).

Kennedy thus discloses extracting “transaction data values” (“extracting a plurality of attributes”) from the “transaction message” (“one or more documents”) at the “processing server” (“first intermediary server”), and “hash[ing] and/or encrypt[ing]” “transaction data values” (“de-identifying the plurality of attributes to obtain a plurality of de-identified attributes”) at the “processing server” to create the “generated data record” (“combining the plurality of de-identified attributes to generate the enriched data record”). (*Id.*, ¶¶ 144-45).

6. Claim 7

Claim 7 depends from claim 1. (Ex. 1001, 60:1-11). The elements of claim 7 are the same as claim 6, except claim 7 recites “hashing” the plurality of attributes instead of “de-identifying” the plurality of attributes. As explained for claim 6, Kennedy teaches hashing transaction data values included in the generated data record.

The Kennedy/Kurani-816 combination would have rendered this claim obvious for the reasons explained for element 2 of claims 1, 5, and 6. (*Id.*, ¶¶ 146-49).

7. Claim 8

Claim 8 depends from claim 1. (Ex. 1001, 60:12-41). The Kennedy/Kurani-816 combination would have rendered this claim obvious. (Ex. 1026, ¶¶ 150-51). Kennedy's Figure 7 shows a communication network where processing of payment transactions is "performed by one or more components of the system 100...such as the processing server 102, financial institution 104, payment network 106, transaction processing device 108, issuer 110, acquirer 112, etc." (Ex. 1033, [0072]).

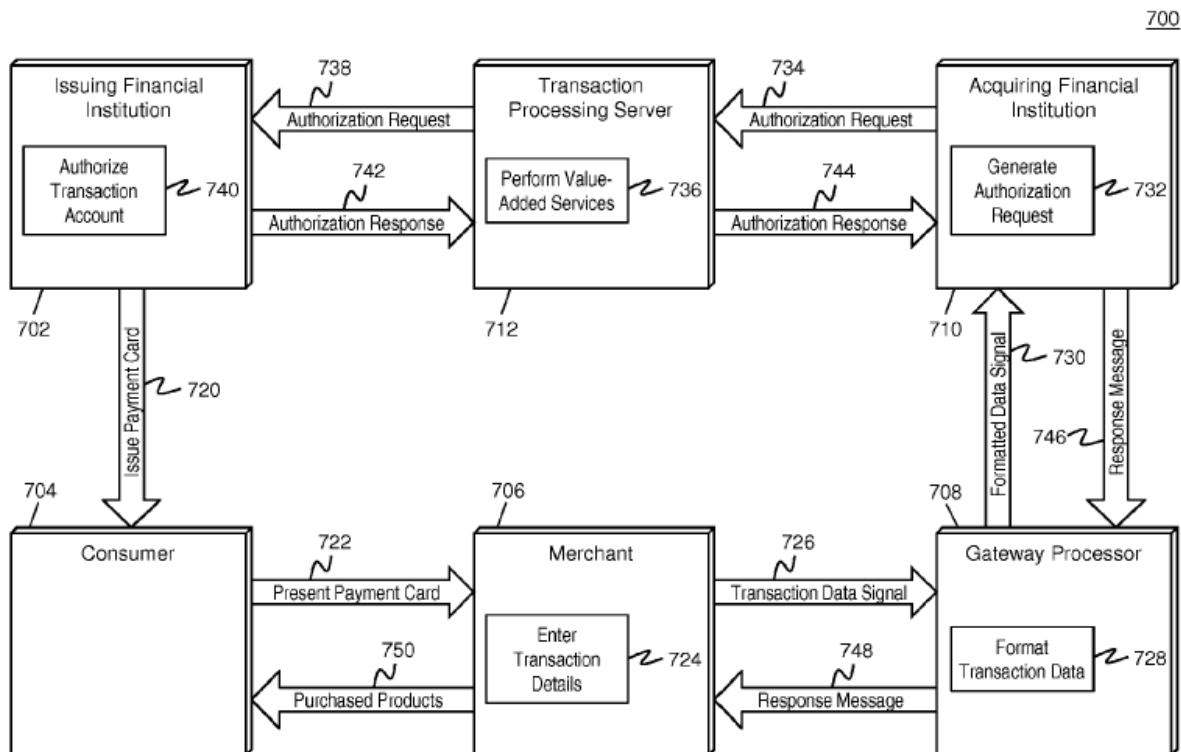


FIG. 7

(*Id.*, Fig. 7).

At steps 732-744, an “acquiring financial institution” communicates via a series of requests/responses with an “issuing financial institution,” which “may be a financial institution...or other suitable type of entity that administers and manages payment accounts and/or payment instruments for use with payment accounts that can be used to fund payment transactions” for consumer. (*Id.*, [0073-0076], Fig. 7). The requests/responses exchanged between each financial institution server involves authorization of the payment transaction, including “approval or denial of the payment transaction” and “other considerations that will be apparent to [POSITA].” (*Id.*, [0083-0084]). Thus, it was well-known for processors and computer components to communicate using requests and responses. (Ex. 1026, ¶ 152). As explained for claim 1, element 3, it would have been obvious to POSITA for such messages to be communicated via the messaging bus. (*Id.*). Accordingly, applying the claimed steps of “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 via the messaging bus,” and “receiving the one or more first responses at the first intermediary server” into Kennedy’s system would have been obvious to POSITA because it would have involved nothing more than combination of prior-art elements according to known methods yielding predictable results.

Further, Kennedy and Kurani-816 teach transmitting messages containing transaction identifiers and digital titles/tokens. (Ex. 1033, [0052]; Ex. 1034, 7:8-11). As explained for claims 2 and 4, POSITA would have understood that messages regarding a particular transaction would include the transaction identifier or digital title/token so each transaction and sale is properly identified throughout the communication flow between servers. (Ex. 1026, ¶ 153). The Kennedy/Kurani-816 combination would have rendered obvious transmitting the token via messages exchanged between the first and second intermediary servers. Accordingly, the elements of the “one or more first requests, each comprising the token,” 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. (*Id.*).

The steps of “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” also would have been obvious to POSITA. (*Id.*, ¶ 154). As explained for element 2 of claims 1 and 4, POSITA would have found it obvious and conventional for entities involved in a centralized financial network to maintain records of their transactions in local storage. (*Id.*). Kennedy and Kurani-816 disclose methods to authenticate, track, and verify transactions. POSITA would have understood that local storage of transaction information is conventional for parties to an electronic funds transfer. (Ex. 1011, Fig. 4, [0074-0075] (disclosing first

and second financial institution store transaction data in a “first private ledger” and “second private ledger” and also add transaction data to a public ledger)). Additionally, POSITA would have understood a well-known way to verify transaction information is to compare that information against an entity’s own records. (Ex. 1026, ¶ 154).

Claim 8 also recites the step of “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.” POSITA would have found this obvious based on their skill and knowledge of the art with Kennedy’s and Kurani-816’s disclosures. Kennedy and Kurani-816 teach financial systems that hash or encrypt various messages and/or transaction information. Kennedy teaches transaction data within the “generated data record” “may be hashed and/or encrypted using one or more suitable hashing and encryption algorithms, respectively.” (Ex. 1033, [0049]). Kurani-816 explains that transactions may be “sign[ed] (e.g., encrypt[ed])...with a private encryption key” during authorization and verification. (Ex. 1034, 5:33-35). These disclosures establish that hashing and encrypting information during transmission were well-known and conventional for protecting transaction information. POSITA would have therefore found it obvious to generate hashes of requests and responses for these same privacy and authentication reasons. (Ex. 1026, ¶ 155).

POSITA would have also found it obvious and advantageous to generate these

hashes for verification purposes. (*Id.*, ¶ 156). Kennedy and Kurani-816 relate to methods for verifying transactions. Kennedy teaches “verify[ing] a blockchain transaction” by using “verification rules” stored in the processing server’s database. (Ex. 1033, [0005]). Kennedy explains that the “private blockchain” is “used as a secure and confidential, yet publicly accessible, record of processed payment transactions for third party verification” and “the data record posted to the blockchain may include transaction data values that may be beneficial for use in additional verification of the associated electronic payment transaction.” (*Id.*, [0026-0027]).

Kennedy explains “one or more transaction data values may be hashed, such that the values may be verified via the generated data record, without the underlying transaction data values being obtainable.” (*Id.*). Similarly, Kurani-816 teaches verification methods, including “MBC verification nodes[], where the transaction is verified and written to the MBC blockchain.” (Ex. 1034, 8:13-15). MBC nodes “verify MBC transactions by verifying information relating to the transaction,” such as “cryptographically verifying the encrypted transaction information.” (*Id.*, 5:5-11, 49-50).

POSITA would have understood from Kennedy’s and Kurani-816’s disclosures that hashing was advantageous for verification. (Ex. 1026, ¶¶ 157-59). POSITA would have understood that hashing for verification was well-known before AU-1. For example, a 2011 IBM publication detailing cryptographic services—nearly four years

before AU-1—shows hashing to “verify that data has not been altered during transmission or storage” was within POSITA’s knowledge. (Ex. 1015, 22, 17-18 (“Cryptography deals with...Hashing...Cryptography is already playing a critical and expanding role in electronic commerce and electronic mail services.”); Ex. 1024, 11 (showing public availability); Ex. 1026, ¶ 159). The IBM publication evidences that POSITA would have known the details of the conventional hash verification process in which “[t]he 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 (“Hash functions were introduced in cryptography to provide message integrity and authentication.”); Ex. 1026, ¶¶ 159-60).

POSITA would have found it obvious to hash one or more responses at the entity on the network communicating with Kennedy’s “processing server”—for example, the “transaction processing device”—so the “processing server” verifies the integrity of the response. (*Id.*, ¶ 161). POSITA also would have found it obvious to hash one or more requests at the “transaction processing device” to ensure when it communicates its response to the “processing server,” the “processing server” confirms its original request arrives without corruption. (*Id.*). Hashing both the request and response at the “transaction processing device” increases system security by allowing parties to verify integrity of information sent and received. POSITA therefore would have found it

obvious to generate hashes of requests and responses at the “transaction processing device” (“second intermediary server”). (*Id.*).

Finally, it would have been obvious to POSITA to “add[] 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,” as claimed. (*Id.*, ¶ 162). Kennedy and Kurani-816 add and update transaction information on the blockchain. POSITA would have found it obvious that verification enabled by hashing information may be accomplished by comparing a hash on the blockchain with an entity’s own hash of the record. (*Id.*). POSITA would have understood “[o]ne way to ensure [that the hash is transmitted with integrity] is to publish the hash in a reliable source of public information.” (*Id.*; Ex. 1015, 22). Accordingly, POSITA would have found it obvious to add the hashes into the “blockchain network” from the “transaction processing device” (“second intermediary server”) to maintain a complete transaction record and allow the “processing server” (“first intermediary server”) to verify integrity of the request delivered to the “transaction processing device” and integrity of the received response. (Ex. 1026, ¶¶ 162-63).

8. Claim 9

Claim 9 depends from claim 8. (Ex. 1001, 60:42-50). The Kennedy/Kurani-816 combination would have rendered this claim obvious. (Ex. 1026, ¶¶ 164-65). As explained for claim 8, Kennedy and Kurani-816 disclose verifying hashed or encrypted

information on a blockchain, and POSITA would have found it obvious to verify the hashed requests and responses on the blockchain. (*Id.*). POSITA would have understood this process to includes regenerating the hash of the “one or more first responses” and to do so “from the first intermediary server” for the entity which receives the response(s) to verify the information included therein. (*Id.*).

POSITA would have further understood that, within the context of the Kennedy/Kurani-816 combination, this response verification would have been accomplished “using the token,” as claimed. As explained for element 3 of claims 1 and 2, Kennedy and Kurani-816 teach using a transaction identifier or digital title/token (“token”) to identify the transaction within the financial system. (*Id.*, ¶ 166). Because the digital title/token is transaction-specific, POSITA would have been motivated to use the token to retrieve the record of the transaction to which the “one or more responses” pertain on the blockchain to accomplish the disclosed verification. (*Id.*, ¶¶ 166-67).

9. Claim 10

Claim 10 depends from claim 8. (Ex. 1001, 60:51-67). The Kennedy/Kurani-816 combination would have rendered this claim obvious. (Ex. 1026, ¶¶ 168-69). Kennedy teaches hashing and encryption “using one or more suitable hashing and encryption algorithms” where “encryption *keys* and algorithms” are stored in the processing server’s memory. (Ex. 1033, [0046], [0049]). While Kennedy does not explicitly disclose the claimed encryption protocol, the claimed steps would have been

obvious in view of Kurani-816 and POSITA's knowledge. (Ex. 1026, ¶ 169).

Kurani-816 discloses public and private key pairs for encrypting information. (Ex. 1034, 3:57-61 (“[T]he financial institution 108 executes an internal transfer of the MBC to a new *private key/public key pair* which are then stored in a database.”); 3:61-65 (“[N]ew *private/public key pair* [] are created as a result of the performance of the transaction.”); 3:65-67, 5:33-37). Encryption techniques 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, were well-known to POSITA. (Ex. 1026, ¶ 170; Ex. 1015, 19 (“The sending party looks up the receiving party's public key and uses it to encipher the data. The receiving party then uses its private key to decipher the data.”))).

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 claiming an implementation of known public-key encryption techniques. This generic encryption protocol is reflected in Kurani-816's teachings of using public and private keys to

encrypt/decrypt information. (Ex. 1034, 3:57-67, 5:33-37; Ex. 1026, ¶ 171).

Accordingly, POSITA would have found it obvious to apply the well-known public key/asymmetric cryptography taught by Kurani-816 into Kennedy's system to facilitate secure private communications. (Ex. 1026, ¶ 172). From the state of the art and Kurani-816's teachings, POSITA would have understood that encryption of information may be accomplished using a plurality of keys (first and second public keys, and first and second private keys) and digital signatures. (Ex. 1026, ¶ 172).

Using public-key cryptography to generate digital signatures to authenticate the message source was well-known before AU-1's filing date. (Ex. 1015, 22-23). To do so, a sender signs the message with a key associated with that sender. In the context of the Kennedy/Kurani-816 combination, two keys associated with the sender—the sender's private key or the sender's public key. (Ex. 1026, ¶ 173). 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.*, ¶ 174). Prior-art references show algorithms using a public key to sign and create a digital signature were well-known. (Ex. 1026, ¶ 174; Ex. 1016, [0010] (“[T]he public key may be used as a signature to verify [] identity.”); Ex. 1020, 1:22-26 (“[C]ommunication 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. 1021, [0016]; Ex. 1022,

[0114] (“[Q]ueries can be signed with the public key and verified with the cryptographic signature.”); Ex. 1023, [0340] (“Appropriately signed means signed with the public key.”)).

POSITA would have understood signing with either the sender’s private or public key were known options for generating a digital signature. (Ex. 1026, ¶ 175). POSITA therefore would have found it obvious to sign the “one or more first requests” with the first public key and the “one or more first responses” with the second public key as a simple design choice between two known, finite, predictable solutions. (Ex. 1026, ¶ 175).

10. Claim 11

Claim 11 depends from claim 10. (Ex. 1001, 61:1-5). The combination of Kennedy/ Kurani-816 would have rendered this claim obvious. As explained for claim 10, Kennedy and Kurani-816 disclose encryption via private/public key pairs, and teach storing and associating these keys with transactions. From these disclosures, POSITA would have understood that public keys associated with particular users or entities could be saved to the blockchain record. (Ex. 1026, ¶¶ 176-77). It would have been obvious to POSITA for each party to add its public key to the blockchain to generate a more robust record for each transaction and allow the transaction to be more easily associated with each party. (*Id.*).

11. Claim 12

Claim 12 depends from claim 1. (Ex. 1001, 61:6-33). The Kennedy/Kurani-816 combination would have rendered this claim obvious. POSITA would have understood that claim 12 simply recites a reversal of the steps in claim 8. (Ex. 1026, ¶¶ 178-79). For the reasons explained for claim 8, these elements would have been obvious to POSITA. (*Id.*).

12. Claim 13

Claim 13 depends from claim 12. (Ex. 1001, 61:34-42). 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 from claim 8. The Kennedy/Kurani-816 combination would have rendered claim 13 obvious for the reasons explained for claims 9 and 12. (*Id.*, ¶¶ 180-81).

13. Claim 14

Claim 14 depends from claim 12. (Ex. 1001, 61:43-59). POSITA would have understood that claim 12 simply recites a reversal of the steps recited in claim 8. The additional steps in claim 14 are the same as recited in claim 10, which depends from claim 8. The Kennedy/Kurani-816 combination would have rendered claim 14 obvious for the reasons explained in claims 10 and 12. (*Id.*, ¶¶ 182-83).

14. Claim 15**Preamble: A system for processing a financial transaction:**

If the preamble is limiting, Kennedy discloses this element for the reasons

explained for claim 1's preamble. (Ex. 1001, 62:1-25; Ex. 1026, ¶ 184; Ex. 1033, [0004], [0017], [0020], Fig. 1).

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 Kennedy/Kurani-816 combination would have rendered this element obvious for the reasons explained for element 1 of claim 1. (Ex. 1026, ¶ 185). Kennedy teaches “system 100 for the validation of electronic payment transactions via assistance of a blockchain network with a transaction processing network.” (Ex. 1033, [0019]). The system includes “processing server 102...[which] may be configured to assist in the validation of both electronic payment transactions processed using a payment network 106 and blockchain transactions associated with a blockchain network.” (*Id.*).

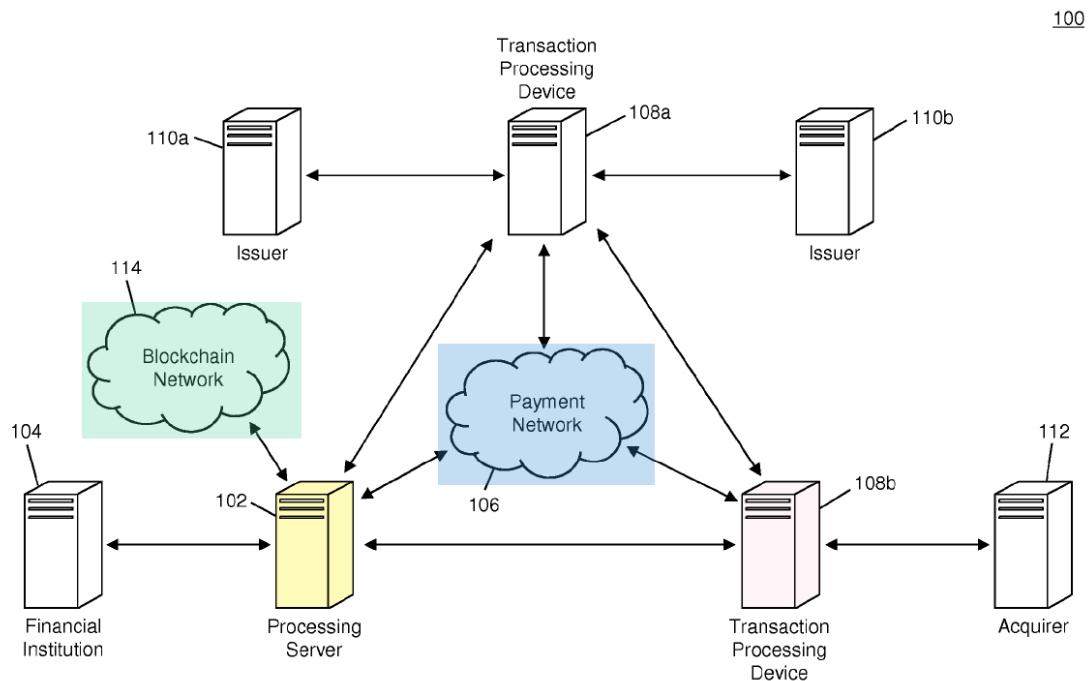


FIG. 1

(Ex. 1033, Fig. 1).

POSITA would have understood the “processing server” (“first intermediary server”) is “operably connected to a network,” as claimed. (Ex. 1026, ¶ 186). As explained for claim 1, element 1, POSITA would have further understood the processing server, which reads and writes to memory, is “operably connected” to the “first document store.”

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

The Kennedy/Kurani-816 combination would have rendered this element obvious for the reasons explained for claim 1, element 3. (*Id.*, ¶ 187; Ex. 1034, Fig. 1 (“digital title company” connected to central payment network)).

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

The Kennedy/Kurani-816 combination would have rendered this element obvious for the reasons explained for claim 1, element 2. (*Id.*, ¶ 188; Ex. 1033, Fig. 1 (“blockchain network” connected to the “payment network” via “processing server”)).

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 Kennedy/Kurani-816 combination would have rendered this element obvious for the reasons explained for claim 1, element 1. (*Id.*, ¶ 189).

Element 5: [wherein the first intermediary server is configured to] generate an enriched data record from the one or more documents and add the enriched data record into the blockchain;

The Kennedy/Kurani-816 combination would have rendered this element obvious for the reasons explained for claim 1, element 2. (*Id.*, ¶ 190).

Element 6: [wherein the first intermediary server is configured to] 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 Kennedy/Kurani-816 combination would have rendered this element obvious for the reasons explained for claim 1, element 3. (*Id.*, ¶ 191).

Element 7: [wherein the first intermediary server is configured to] transmit the token to the first document store;

The Kennedy/Kurani-816 combination would have rendered this element obvious for the reasons explained for claim 1, element 6. (*Id.*, ¶ 192).

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 Kennedy/Kurani-816 combination would have rendered this element obvious for the reasons explained for claim 1, element 4. (*Id.*, ¶ 193).

Element 9: [wherein the token server is configured to] transmit the token to the first intermediary server, via the messaging bus.

The Kennedy/Kurani-816 combination would have rendered this element obvious for the reasons explained for claim 1, element 5. (*Id.*, ¶ 194).

15. Claim 16

The Kennedy/Kurani-816 combination renders claim 16 obvious for the same reasons as for claims 1 and 15. Claim 16 is broader than claims 1 and 15 because it does not recite that the token server adds the token to the blockchain. (*Id.*, ¶ 195; Ex. 1001, 62:26-38).

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, the Kennedy/Kurani-816 combination would have rendered this element obvious for the reasons explained for element 1 of claims 1 and 15. (Ex. 1026, ¶ 196).

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

The Kennedy/Kurani-816 combination would have rendered this element obvious for the reasons explained for claim 1, element 1. (*Id.*, ¶ 197).

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 Kennedy/Kurani-816 combination would have rendered this element obvious for the reasons explained for claim 1, element 2. (*Id.*, ¶ 198).

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 Kennedy/Kurani-816 combination would have rendered this element obvious for the reasons explained for claim 1, element 3. (*Id.*, ¶ 199). Even if the Board determines that the Kennedy/Kurani-816 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 Kennedy/Kurani-816 combination would have rendered this element obvious for the reasons explained for claim 1, element 6. (*Id.*, ¶ 200).

16. 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.” (Ex. 1001, 62:39-43). The Kennedy/Kurani-816 combination would have rendered this element obvious for the reasons explained for claims 2 and 16. (Ex. 1026, ¶ 201).

17. Claim 18

Claim 18 depends from claim 16. (Ex. 1001, 62:44-46). The Kennedy/Kurani-816 combination would have rendered this element obvious for the reasons explained

for claims 2, 4, and 16. (Ex. 1026, ¶ 202).

18. Claim 19

Claim 19 depends from claim 16. (Ex. 1001, 62:47-54). This claim contains a subset of the elements recited in claim 8 regarding steps taken by the first intermediary server. The Kennedy/Kurani-816 renders obvious this claim for the reasons explained for claims 8 and 16. (Ex. 1026, ¶ 203).

19. Claim 20

Claim 20 depends from claim 19. (Ex. 1001, 62:55-58). The Kennedy/Kurani-816 combination would have rendered this element obvious.

POSITA would have understood that “regulatory compliance documents” include documents or messages containing customer identification and authentication information to protect against fraud. (Ex. 1001, 12:31-38; Ex. 1026, ¶¶ 204-05). As explained for claim 8, the Kennedy/Kurani-816 combination discloses that certain institutions and servers communicate via a series of requests and responses. Kennedy explains that the requests/responses may involve processing and authorization of the payment transaction “based on an available credit amount for the transaction account and the transaction amount for the payment transaction, fraud scores provided by the transaction processing server [], and other considerations.” (Ex. 1033, [0083]). During processing, servers “perform value-added services for the payment transaction...specified by the issuing financial institution,” including “fraud scoring,

transaction or account controls, account number mapping....” (*Id.*, [0081]).

POSITA would understand Kennedy’s value-added services protect financial institutions against fraud and involve steps to establish customer identity and qualify that the source of funds are legitimate. (Ex. 1026, ¶ 206). POSITA would have further recognized that KYC processes were commonly used to verify customer identity and reduce fraud. (Ex. 1035, [0008], [0012], [0052] (using “authentication techniques to verify identifying information and perform know-your-customer (KYC) or anti-money laundering (AML) checks” “in accordance with regulatory requirements” by exchanging “data message[s]...to verify a party’s KYC status”)). Kennedy’s request-and-response flow for fraud protection, combined with POSITA’s knowledge of the well-known practice of KYC checks, is consistent with and renders obvious the exchange of KYC or “regulatory compliance” documents. (Ex. 1026, ¶ 206, 41-42).

C. Ground 2: Kennedy And Kurani-816 In View Of Yago Render Obvious Claim 3

1. Claim 3

Claim 3 depends from claim 1. (Ex. 1001, 59:30-34). The Kennedy/Kurani-816 combination in view of Yago would have rendered this element obvious.

As explained for Ground 1, the Kennedy/Kurani-816 combination discloses or would have rendered obvious every element of claim 1. Although neither reference explicitly discloses implementing a smart contract at the token server and adding it to the blockchain, Yago does and would have rendered these additional limitations

obvious. (Ex. 1026, ¶¶ 207-08).

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. 1026, ¶ 209; 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 contract” to the Kennedy/Kurani-816 combination. (Ex. 1026, ¶ 210). The motivation to do so would have been to create “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. 1026, ¶ 210). Like Yago, Kennedy and Kurani-816 seek to address similar problems of security risks and fraud, and a desire to “protect against fraud” and identify potential fraudulent transactions on the blockchain. (Ex. 1026, ¶ 210; Ex. 1033, [0002]; Ex. 1034, 10:9-15). Moreover, Kennedy and Yago are both directed to financial settlement (Ex. 1033, [0024], [0064]; Ex. 1011, [0005]).

POSITA would have had a reasonable expectation of success in applying Yago’s “payment assured contract” to the Kennedy/Kurani-816 combination. (Ex. 1026, ¶ 211). Blockchain-based smart contracts had been contemplated in the art since

blockchain's beginnings. (Ex. 1012, 29 (“[T]he possibilities for programmable...contracts were baked into the [Bitcoin] protocol at its invention.”)). Applying Yago's teachings to Kennedy/Kurani-816's system would have involved combining well-understood technologies yielding predictable results. (Ex. 1026, ¶¶ 211, 34-35).

Moreover, applying Yago's teachings to the Kennedy/Kurani-816 combination discloses or renders obvious implementing the smart contract “at the token server” and “adding the smart contract into the blockchain, from the token server.” (Ex. 1026, ¶ 212). Yago enables “automated and scalable settlement protocols” including “digital contracts that may be automatically enforced.” (Ex. 1011, [0006]). 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.” (*Id.*, [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 “the 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” that transfer the digital certificate or contract to a public ledger 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 transaction system’s proof of payment module “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]). The “payment assured contracts” (“smart contracts”) are implemented at the transaction system and added to the public ledger (“blockchain”) by the transaction system. (Ex. 1026, ¶ 213).

POSITA would have understood that Yago’s “transaction system is like the “digital title company” (“token server”) in the Kennedy/Kurani-816 combination because it is a central server not affiliated with any party to the smart contract. (*Id.*, ¶ 214). In context of the Kennedy/Kurani-816 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. (*Id.*, ¶¶ 214-15).

VI. CONCLUSION

Petitioner respectfully requests *inter partes* review of the Challenged Claims based on the priority challenge and grounds herein.

VII. MANDATORY NOTICES UNDER 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 the '413 Patent based on the earliest possible priority date of August 14, 2015.⁴

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) JONES DAY 110 North Wacker Drive, Suite 4800 Chicago, IL 60606 Telephone: (312) 782-3939 Facsimile: (312) 782-8585 smayergoyz@jonesday.com

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.

	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

A courtesy copy of the foregoing petition and accompanying Exhibits 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 13,541 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	<i>Intentionally Omitted</i>
1004	<i>Intentionally Omitted</i>
1005	U.S. Patent No. 9,397,985 (“Seger”)
1006	<i>Intentionally Omitted</i>
1007	U.S. Patent No. 11,270,274 (“Kurani-274”)
1008	Everett Rosenfeld, “Forget currency, bitcoin’s tech is the revolution” (2014)
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” (2015)
1011	U.S. Patent Pub. No. 2015/0206106 (“Yago”)
1012	Swan, “Blockchain: Blueprint for a New Economy” (2015)

EXHIBIT	TITLE
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-007”)
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)

EXHIBIT	TITLE
1025	Screenshots – <i>Wayback Machine</i> Archive
1026	Declaration of Chien-Chung Shen, Ph.D., for Petition #2
1027	Australian Provisional Application No. 2015903292 (“AU-1”)
1028	Australian Provisional Application No. 2016900239 (“AU-2”)
1029	Australian Provisional Application No. 2016901924 (“AU-3”)
1030	International Application No. PCT/AU2016/000279 (“PCT application”)
1031	Annotated ’413 Patent, highlighted to show matter from AU Provisionals
1032	<i>Intentionally Omitted</i>
1033	U.S. Patent Pub. No. 2017/0132626 (“Kennedy”)
1034	U.S. Patent No. 10,719,816 (“Kurani-816”)
1035	U.S. Patent Pub. No. 2016/0260169 (“Arnold”)
1036	Dr. Chien-Chung Shen <i>Curriculum Vitae</i>

EXHIBIT	TITLE
1037	Tannenbaum et al., “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 (“Winklevoss”)
1041	Stallings, “Cryptography and Network Security Principles and Practices,” 4 th 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	Identitii Opposition to Motion to Dismiss (Dkt. 20), Case No. 23-1095-GBW (D. Del.)
1046	U.S. Patent Pub. No. 2015/0032627 (“Dill”)