

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. – Not Yet Assigned
U.S. Patent No. 10,984,413

**DECLARATION OF CHIEN-CHUNG SHEN, PH.D.
REGARDING U.S. PATENT NO. 10,984,413**

I declare that all statements made in this Declaration of my own knowledge are true, that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Date: February 20, 2024

By:



Chien-Chung Shen, Ph.D.

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	PROFESSIONAL BACKGROUND.....	4
III.	RELEVANT LEGAL STANDARDS	6
IV.	TECHNOLOGY BACKGROUND.....	11
	A. Distributed Systems And Blockchain	11
	B. Tokens	16
	C. Smart Contracts	17
	D. Cryptography	18
	E. Know-Your-Customer (“KYC”)	20
V.	THE ’413 PATENT	21
	A. Description Of The Alleged Invention.....	21
	B. Person Of Ordinary Skill In The Art.....	23
VI.	THE CHALLENGED CLAIMS ARE NOT SUPPORTED BY THE FIRST AUSTRALIAN PROVISIONAL APPLICATION.....	24
	A. The Challenged Claims	24
	F. The Provisional Applications	25
	B. AU-1 Does Not Provide Written-Description Support For The Challenged Claims	27
VII.	THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	32
	A. Overview Of The Prior Art	32
	1. Kennedy.....	32
	2. Kurani-816.....	36
	3. Yago 39	
	B. Ground 1: Claims 1-2 And 4-20 Are Obvious Over Kennedy In View Of Kurani-816.....	40
	1. Claim 1	40
	2. Claim 2	66
	3. Claim 4	70

4.	Claim 5	73
5.	Claim 6	73
6.	Claim 7	75
7.	Claim 8	76
8.	Claim 9	85
9.	Claim 10	86
10.	Claim 11	90
11.	Claim 12	91
12.	Claim 13	92
13.	Claim 14	92
14.	Claim 15	93
15.	Claim 16	97
16.	Claim 17	98
17.	Claim 18	99
18.	Claim 19	99
19.	Claim 20	99
C.	Ground 2: Kennedy And Kurani-816 In Further View Of Yago Render Obvious Claim 3	101
1.	Claim 3	101
VIII.	CONCLUSION.....	105

I. INTRODUCTION

1. I have made this declaration at the request of JPMorgan Chase Bank, N.A. (“Petitioner”) in the matter of the *Inter Partes* Reviews of U.S. Patent No. 10,984,413 (“the ’413 Patent”). This declaration supports the second of the two petitions filed concurrently by Petitioner with respect to the ’413 Patent.

2. I am being compensated for my work in this matter at the standard hourly rate for my consulting services. In no way does my compensation in this matter depend on the outcome of this proceeding.

3. In preparing this Declaration, I considered all materials cited in the body of this Declaration, which includes but is not limited to the following:

- The ’413 Patent (Ex. 1001)
- File History of the ’413 Patent (Ex. 1002)
- U.S. Patent No. 9,397,985 (“Seeger”) (Ex. 1005)
- U.S. Patent No. 11,270,274 (“Kurani-274”) (Ex. 1007)
- Everett Rosenfeld, “Forget currency, bitcoin’s tech is the revolution” (2014) (Ex. 1008)
- Richards, “The Role of Blockchain Technology in Supply Chain Management” (2013) (Ex. 1009)
- Tim Swanson, “Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems” (2015) (Ex.

1010)

- U.S. Patent Pub. No. 2015/0206106 (“Yago”) (Ex. 1011)
- Melanie Swan, “Blockchain, Blueprint For A New Economy” (2015) (Ex. 1012)
- Vitalik Buterin, “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,” White Paper (2014) (Ex. 1013)
- U.S. Patent Pub. No. 2016/0140653 (“McKenzie”) (Ex. 1014)
- IBM, Version 1 Release 13 of z/OS, “Cryptographic Services,” Integrated Cryptographic Service Facility (2011) (Ex. 1015)
- U.S. Patent Pub. No. 2006/0015945 (“Fields”) (Ex. 1016)
- U.S. Patent Pub. No. 2011/0258123 (“Dawkins”) (Ex. 1017)
- U.S. Patent Pub. No. 2013/0212007 (“Mattson-007”) (Ex. 1018)
- Tiwari et al., “Cryptographic Hash Function: An Elevated View” (2010) (Ex. 1019)
- U.S. Patent No. 6,341,164 (“Dilkie”) (Ex. 1020)
- U.S. Patent Pub. No. 2010/0223659 (“Ekl”) (Ex. 1021)
- U.S. Patent Pub. No. 2013/0080916 (“Lopez”) (Ex. 1022)
- U.S. Patent Pub. No. 2003/0200450 (“England”) (Ex. 1023)

- Wayback Machine Archive – IBM, Version 1 Release 13 of z/OS “Cryptographic Services,” Integrated Cryptographic Service Facility (2011) (Ex. 1024)
- Screenshots of Wayback Machine Archive (Ex. 1025)
- Australian Provisional Application No. 2015903292 (“AU-1”) (Ex. 1027)
- Australian Provisional Application No. 2016900239 (“AU-2”) (Ex. 1028)
- Australian Provisional Application No. 2016901924 (“AU-3”) (Ex. 1029)
- International Application No. PCT/AU2016/000279 (“PCT”) (Ex. 1030)
- Annotated ’413 Patent, highlighted to show matter from AU Provisionals (Ex. 1031)
- U.S. Patent Pub. No. 2017/0132626 (“Kennedy”) (Ex. 1033)
- U.S. Patent No. 10,719,816 (“Kurani-816”) (Ex. 1034)
- U.S. Patent Pub. No. 2016/0260169 (“Arnold”) (Ex. 1035)
- Tannenbaum et al., “Distributed Systems, Principles and Paradigms” (2007) (Ex. 1037)

- Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System” (2008) (Ex. 1038)
- Ripple Labs, Inc., “The Ripple Protocol: A Deep Dive for Finance Professionals” (2014) (Ex. 1039)
- U.S. Patent No. 9,892,460 (“Winklevoss”) (Ex. 1040)
- William Stallings, “Cryptography and Network Security, Principles and Practice” (2005) (Ex. 1041)
- U.S. Patent Pub. No. 2009/0249082 (“Mattsson-082”) (Ex. 1042)
- U.S. Patent Pub. No. 2013/0212666 (“Mattsson-666”) (Ex. 1043)
- U.S. Patent No. 6,173,272 (“Thomas”) (Ex. 1044)
- Identitii Opposition to Motion to Dismiss (Ex. 1045)
- U.S. Patent Pub. No. 2015/0032627 (“Dill”) (Ex. 1046).

II. PROFESSIONAL BACKGROUND

4. I received my B.S. and M.S. degrees in Computer Science from the National Chiao Tung University in Taiwan in 1982 and 1984, respectively, and my Ph.D. in Computer Science from the University of California, Los Angeles (UCLA) in 1992.

5. I am currently a Professor of Computer and Information Science at the University of Delaware, where I have been teaching and conducting research in the

Department of Computer and Information Sciences since 1998. I have taught undergraduate and graduate-level courses in Computer Science, Business Telecommunication Networks, Computer Networks, Distributed Computing, Distributed Ledger Technology (Blockchain), and Software-Defined and Virtualized Networks.

6. From 1993 to 1998, I was a Research Scientist at Bellcore, Applied Research, where I was responsible for the researching and prototyping of fault-tolerant, distributed network control and management systems for DARPA ATDNet (ATM and SONET) and DARPA MONET (WDM) projects. From 1992 to 1993, I was a Technical Consultant at AT&T, Bell Laboratories, focusing on system architecture design, software development, and performance evaluation for network monitoring systems.

7. I am a member of both the Association for Computing Machinery and the Institute of Electrical and Electronics Engineers. I have received numerous honors for my work, including the U.S. National Science Foundation CAREER Award.

8. I have authored or co-authored approximately 200 journal articles, book chapters, online publications, conference publications, and poster publications. In my research, I have studied and authored publications relating to computer science, distributed computing, computing networks, blockchain, Bitcoin, smart contracts, cyber security, cryptography, authentication, data processing, and wireless communications,

among others. I am also a named inventor on one U.S. Patent directed to wavelength-division multiplexed communication networks.

9. I have served as a conference chair, lecturer, invited speaker, or panelist on computer science topics many times over the last 30 years, including at universities, the International Conference on Computer Communications and Networks, the Institute of Electrical and Electronics Engineers, the International Congress on Blockchain and Applications, the National Science Foundation, the National Institute of Standards and Technology, and the U.S. Army Research Laboratory.

10. A more detailed description of my professional qualifications, including a listing of my specialties, expertise, and professional activities, is contained in my curriculum vitae, a copy of which is included at Exhibit 1036.

III. RELEVANT LEGAL STANDARDS

11. I have been asked to provide my opinions as to whether claims of the '413 Patent are anticipated by the prior art or would have been obvious to a person having ordinary skill in the art ("POSITA") at the time of the alleged invention, in view of the prior art. My opinions are set forth in this declaration.

12. I am a professor and scientist by education and profession. The opinions expressed by me in this Declaration are based in part upon the application of my computer science knowledge and experience to the evaluation of certain prior art with respect to the '413 Patent. I am neither an attorney nor a patent agent. Therefore, I have

requested attorneys from Jones Day, who represent Petitioner, to provide me with guidance as to the applicable patent law in this matter. The paragraphs below express my understanding of how I must apply current legal principles related to patentability.

13. I understand that in determining whether a patent claim is anticipated or obvious in view of the prior art in an IPR proceeding, the Patent Trial and Appeal Board (PTAB) gives claims their ordinary and customary meaning, or the meaning that the term would have to a POSITA at the time of the invention in view of the intrinsic record. I understand that the claim language, specification, and prosecution history are relevant in determining the meaning of a claim term. I understand that the prosecution history of a patent provides the record of the examination of a patent application before the U.S. Patent and Trademark Office (PTO). The prosecution history provides evidence of how the patent examiner and the inventors understood the patent application and the claims and can therefore be instructive on how to interpret the claims. I understand that extrinsic evidence may also be used in understanding the meaning of a claim term. Extrinsic evidence includes dictionaries, treatises, expert testimony, and prior art. But I understand that in construing claims, one should look first to the intrinsic evidence before looking at extrinsic evidence.

14. I understand that there are at least two circumstances wherein the words in a patent claim may differ from and not be given their plain and ordinary meaning. One circumstance occurs when an applicant acts as his or her own lexicographer by setting

forth clearly a definition of a claim term that may differ from the plain and ordinary meaning that the term would otherwise possess. Another circumstance occurs when the applicant includes or provides an intentional disclaimer or disavowal of the claim scope. I understand that an applicant may act as his or her own lexicographer, or may disclaim or disavow claim scope, in either the specification or in the prosecution history of the patent. I understand also that the applicant may act as lexicographer, or disclaim or disavow claim scope, by making amendments to the claims during prosecution, or by making assertions to the PTO about differences between the claimed inventions and the prior art.

15. I understand that a claim is unpatentable under 35 U.S.C. § 102 (i.e., “anticipated”) if each and every element and limitation of the claim is found either expressly or inherently in a single prior art reference.

16. I understand that a claim is unpatentable under 35 U.S.C. § 103 (i.e., “rendered obvious”) if the claimed subject matter as a whole would have been obvious to a person of ordinary skill in the art at the time of the alleged invention. I also understand that an obviousness analysis takes into account the scope and content of the prior art, the differences between the claimed subject matter and the prior art, and the level of ordinary skill in the art at the time of the invention.

17. In determining the scope and content of the prior art, I understand that a reference is considered appropriate prior art if that reference falls within the field of the

inventor's endeavor. In addition, a reference is considered prior art if that reference is reasonably pertinent to the particular problem with which the inventor was involved. A reference is reasonably pertinent if it would have commended itself logically to an inventor's attention in considering his or her problem. A reference supports use as prior art in an obviousness analysis if that reference relates to the same problem as that of the claimed invention.

18. To assess the differences between the prior art and the claimed subject matter, I understand that 35 U.S.C. § 103 requires that the claimed invention be considered as a whole. I also understand that a finding of obviousness requires more than merely demonstrating that each claim element was known in the prior art. Obviousness requires showing that a person of ordinary skill in the art would have been motivated to combine the teachings of the prior art to achieve the claimed invention and would have had a reasonable expectation of success in doing so.

19. I understand that the Supreme Court has recognized several rationales for combining references or modifying a reference to show the obviousness of the claimed subject matter. Some of these rationales include: combining prior art elements according to known methods to yield predictable results; simple substitution of one known element for another to obtain predictable results; a predictable use of prior art elements according to their established functions; applying a known technique to a known device (method or product) ready for improvement to yield predictable results; choosing from a finite

number of identified, predictable solutions, with a reasonable expectation of success; and some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

20. I understand that in order to rely on the filing date of an earlier application (i.e., “claim priority to” the earlier application), the earlier application must include a disclosure that complies with the written description requirement of 35 U.S.C. § 112. I understand that a patent satisfies the written description requirement if it conveys to a person of ordinary skill in the art that the inventor had possession of the full scope of the claimed invention. I understand that this description may be satisfied by any combination of the words, structures, figures, diagrams, formulas, etc., contained in the original patent application. I also understand that the full scope of a claim or of a particular claim limitation need not be disclosed word-by-word in the original application if, as of the effective filing date, a person of ordinary skill in the art would have understood that the inventor possessed the full scope of the claim. I understand that for there to be written-description support, a POSITA, in reading the disclosure, must immediately discern the limitation at issue in the claims.

21. I understand that patent claims are entitled to the filing date of a foreign priority application under 35 U.S.C. § 119 only if the corresponding foreign application

supports the claims in a manner that complies with the written description requirement of 35 U.S.C. § 112.

IV. TECHNOLOGY BACKGROUND

22. In this section, I describe the state of the art with respect to a number of technology areas relevant to the subject matter of the '413 Patent. As of the relevant time frame, which I have been asked to assume is the August 14, 2015 time frame (the filing date of Australian Provisional Application No. 2016901924, the earliest application to which I understand the '413 Patent claims priority),¹ a POSITA would have been aware of concepts and developments in the areas of distributed systems, payments networks, cryptography, and blockchain that are relevant to the '413 Patent. These are described below.

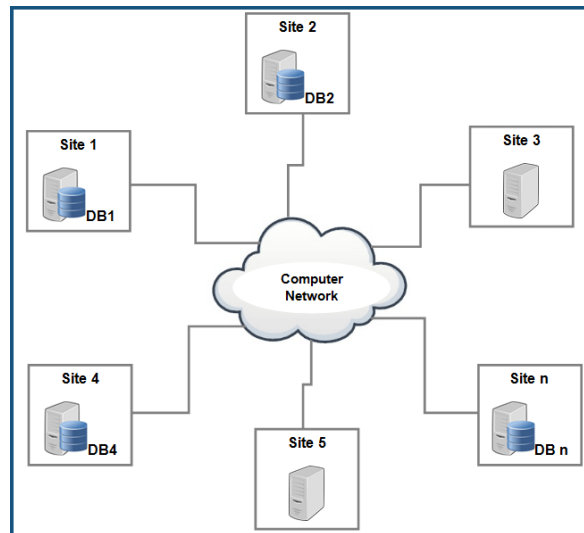
A. Distributed Systems And Blockchain

23. Distributed systems have been utilized in the art for decades. Generally, a “distributed system” is a “collection of independent computers that appears to its users as a single coherent system.” (Ex. 1037, 21). Thus, a basic distributed system “consists

¹ As I discuss below, it is my opinion that the claims of the '413 Patent are not supported by the Australian provisional filed on this date. This does not change my opinion about the state of the art in the relevant time period.

of components (i.e., computers) that are autonomous” and collaborate so “users (be they people or programs) think they are dealing with a single system.” (Ex. 1037, 21). “How to establish this collaboration lies at the heart of developing distributed systems.” (Ex. 1037, 21).

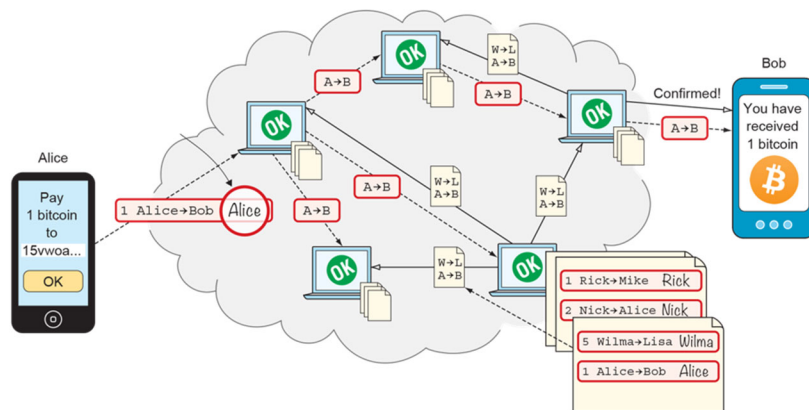
24. The World Wide Web (WWW) is the most famous distributed system invented in 1989, which comprises millions of interconnected web servers and client computers distributed across the globe. The figure below depicts an example:



25. A later example of a fully distributed, peer-to-peer system is Bitcoin, which utilizes blockchain technology in the field of digital currency. (Ex. 1038). Exhibit 1038 is a true and correct copy of the Nakamoto Bitcoin White Paper retrieved from <https://web.archive.org/web/20100704213649/https://bitcoin.org/bitcoin.pdf>, showing the paper was available online at least as early as July 4, 2010 (Ex. 1025), though those skilled in the art know that this paper was first published in October 2008. (*E.g.*,

<https://www.forbes.com/sites/peterizzo/2023/10/31/15-facts-about-the-satoshi-white-paper-on-bitcoins-15th-birthday/?sh=701039b44821>).

26. Blockchain is a decentralized distributed ledger that facilitates the process of recording transactions and tracking assets in a network. Bitcoin operates a decentralized system where transactions are recorded on a public ledger called the blockchain. When someone initiates a transaction, it is broadcasted to the network and verified by miners, who compete to solve complex mathematical puzzles to validate and add new blocks of transactions to the blockchain through a process called mining. Below is a high-level visual of Bitcoin where miners (nodes with “OK”) validate transactions and maintain replicas of the blockchain distributed ledger (denoted as “folders”).



27. Skilled artisans recognized the benefits of blockchain at least as early as the Bitcoin paper in 2008. The Bitcoin system involves digital math-based assets, or “digital assets based upon a computer generated mathematical and/or cryptographic protocol that may, among other things, be exchanged for value and/or be used to buy

and sell goods or pay for services.” (Ex. 1040, 10:34-38). As described, for example, in U.S. Patent No. 9,892,460, those of skill in the art were well aware that digital math-based asset systems “may use [] decentralized electronic ledger system[s], which may be maintained by a plurality of physically remote computer systems.” (Ex. 1040, 10:59-61). “The ledger may be a decentralized public transaction ledger,” such as a blockchain, “which can be distributed to users in the network, e.g., via a peer-to-peer sharing.” (Ex. 1040, 10:64-66).

28. Blockchain rapidly gained popularity after the publication of the Bitcoin paper, and soon those skilled in the art began to foresee applications of blockchain to technologies outside of cryptocurrency. “Commonly cited applications include using on-blockchain digital assets to represent custom currencies and financial instruments (‘colored coins’), the ownership of an underlying physical device (‘smart property’), non-fungible assets such as domain names (‘Namecoin’) as well as more advanced applications such as decentralized exchange, financial derivatives, peer-to-peer gambling and on-blockchain identity and reputation systems.” (Ex. 1011, 1, 10-11).

29. One well-known application of blockchain is as a ledger to record financial transactions. (Ex. 1008, 2 (“[P]roponents [of blockchain] say it is the most secure record-keeping technology ever devised.”); Ex. 1009, 1 (“Blockchain... provides a secure and transparent platform for recording and verifying transactions. ...The immutable nature of blockchain ensures that every transaction and movement of goods

can be recorded and tracked in real-time.”); Ex. 1010, 29-37 (describing a number of companies using permissioned distributed ledgers for record-keeping). Exhibit 1010 is a true and correct copy of the report archived and retrieved from <https://web.archive.org/web/20150412002203/https://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf>, showing the report was available online at least as early as April 12, 2015. (Ex. 1025).

30. In addition, U.S. Patent No. 9,397,985 to Seger et al. identifies a blockchain as a means to provide a “verifiable, and immutable record[.]” (Ex. 1005, 1:43-44). Seger explains its “distributed ledger may provide a verifiable record of all of the information exchanges [between parties,] including various information transactions including encrypted information.” (Ex. 1005, 10:20-26).

31. Further, prior to the August 14, 2015 timeframe, systems like Ripple had already been developed using blockchain to assist banks with real-time settlement of cross border payments. (Ex. 1001, 24:21-23, 25:44-46.) “Ripple is a universal protocol founded in 2012 to power the cheapest and fastest payment system for value transfer with a global, post-Internet architecture... enabl[ing] users to exchange money (including fiat currencies, digital currencies, gold, and other items of value) across national boundaries. ... On a high level, one can think of Ripple as a neutral, open-source ledger that connects financial institutions and networks, and on which developers can build innovative payment applications.” (Ex. 1039, 4-5). Ripple was well-known

in the prior art (Ex. 1007, 1:33), and is acknowledged in the '413 Patent as pre-existing. Ex. 1001, 27:56-58 (“Embodiments of the invention can be implemented utilizing the ‘Ripple’ framework, protocol and gateway-or more generally any blockchain based framework.”)).

B. Tokens

32. It was known to use (fixed length) tokens or transaction identifiers, that are generated, for example, as a UUID (universally unique identifier) or as a hash of the transaction data, to uniquely identify or locate each transaction stored in the system.

33. As of the August 14, 2015 timeframe, a POSITA would have been familiar with the use of tokens as an identifier of information. (Ex. 1042, [0005] (“Tokenization is the act of replacing the original data field with reference or pointer to the actual data field.”)). The POSITA would have appreciated that numerous techniques for generating tokens existed in the art. For example, static or dynamic lookup tables could be used to map an input value to a particular token (Ex. 1043, [0020], [0022]). Hashing was another well-known technique for generating a token. (Ex. 1044, 12:1-11). Within the realm of financial transactions, tokens were a well-known means to prevent unauthorized access to payment or other sensitive communication information (E.g., Ex. 1043, [0005]; Ex. 1007, 6:24-33; Ex. 1017, [0027]; Ex. 1018, [0006], [0019]) and to provide unique identification of transaction data. (Ex. 1042, [0103] (“The tokenization enables you to store a reference pointer anywhere within your network or database

systems and can be used to reduce the cost of securing data fields.”)). In fact, tokenization of transaction information in electronic payments was known in the art at least as early as 2001. (Ex. 1044, 11:16-22, 11:45-53).

C. Smart Contracts

34. As of the August 14, 2015 timeframe, the POSITA would have been aware of the benefits and tools that distributed ledger systems provide. One such tool is a “smart contract.” (Ex. 1011, [0047] (describing “payment assured contracts” where a party can “objectively (and automatically), confirm performance by the seller, by [] directly monitoring the CDI network [(i.e., ‘blockchain’)].”); Ex. 1014 (defining smart contracts as “systems which automatically move digital assets according to arbitrary pre-specified rules.”); Ex. 1013, 1 (“Another important area of inquiry is ‘smart contracts’ – systems which automatically move digital assets according to arbitrary pre-specified rules”)). Exhibit 1013 is a true and correct copy of the White Paper retrieved from <https://web.archive.org/web/20140723210954/https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf>, showing the paper was available online at least as early as July 23, 2014. (Ex. 1025). The idea of blockchain-based smart contracts had been known in the art since blockchain’s beginnings. (Ex. 1012, 29 (“the possibilities for programmable ... contracts were baked into the [Bitcoin] protocol at its invention.”)).

35. As of the August 14, 2015 timeframe, the POSITA would have been aware of hundreds of use-cases for “smart contracts,” including many in financial transaction

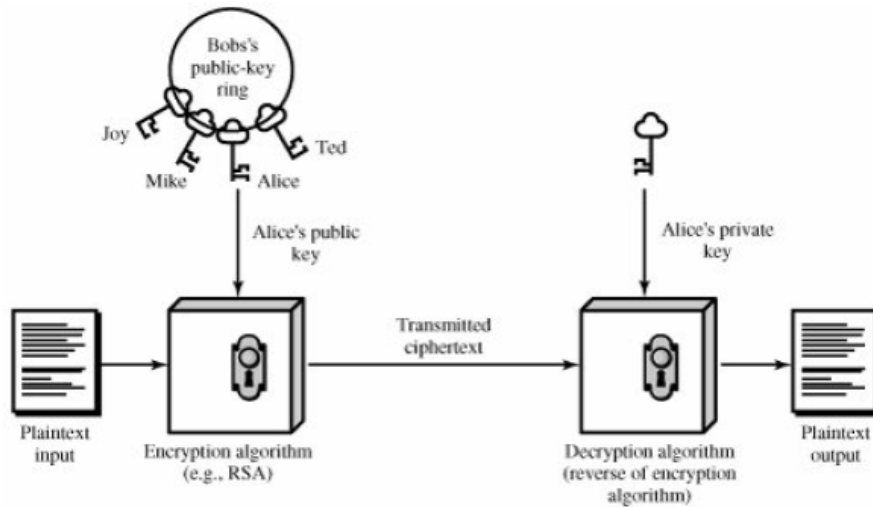
space, such as in cross border settlements, central or derivative clearing, mortgages, the managing of escrow accounts, guaranteed lending, and more. (Ex. 1010, 16-17).

D. Cryptography

36. As of the August 14, 2015 timeframe, cryptographic tools, such as hashing and digital signatures, are core well-known components of digital currencies, secure networks, and verification methods. These techniques have been taught in textbooks for decades, and those skilled in the art would have been well aware of the encryption methods described below prior to the filing of the '413 Patent. (Ex. 1041).

37. There are two general types of cryptographic algorithms: symmetric and asymmetric. “Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the same key.” (Ex. 1041, 10). This encryption method, “also referred to as conventional encryption or single-key encryption, was the only type of encryption in use prior to the development of public-key encryption in the 1970s.” (Ex. 1041, 10).

38. Asymmetric or public-key algorithms use two keys that are mathematically related. One key is used for encryption while a different, related key is used for decryption. (Ex. 1041, 46). The general steps are represented in the below excerpt from a 2006 textbook:



(Ex. 1041, 47).

39. Essentially, “[e]ach user generates a pair of keys to be used for the encryption and decryption of messages.” (Ex. 1041, 47). “Each user places one of the two keys in a public register or other accessible file,” while “the companion key is kept private.” Shown in the example above, if Bob wishes to transmit a confidential message to Alice, Bob encrypts the message using Alice’s public key. When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows her private key. (Ex. 1041, 46-47). It was also well-known that public-key encryption can be used for authentication .

40. Additional conventional cryptographic techniques for message authentication are message authentication codes (MAC) and secure hash functions. (Ex. 1041, 76). A MAC is an algorithm that requires the use of a secret key. It “takes a variable length message and a secret key as input and produces an authentication code.

A recipient in possession of the secret key can generate an authentication code to verify the integrity of the message.” (Ex. 1041, 76). A “hash function maps a variable-length message into a fixed length hash value, or message digest.” (Ex. 1041, 77). The purpose of a hash function “is to produce a ‘fingerprint’ of a file, message, or other block of data.” (Ex. 1041, 93). Hashing is a well-known cryptographic technique that has been utilized by those skilled in the art for decades.

E. Know-Your-Customer (“KYC”)

41. As of the August 14, 2015 timeframe, a POSITA would have also been aware of and understood the benefits of value-added services that protect financial institutions against fraud, including know-your-customer (“KYC”) and anti-money laundering (“AML”) checks. It was well-known to those skilled in the art that KYC and AML checks are important processes that guard against financial crimes. In fact, in the United States, there are regulations requiring that certain financial institutions “use reasonable diligence, in regard to the opening and maintenance of every account, to know (and retain) the essential facts concerning every customer and concerning the authority of each person acting on behalf of such customer.” FINRA Rule 2090 (2012).

42. Indeed, KYC processes have been used to verify customer identity and reduce fraud well before the ’413 Patent. (Ex. 1035, [0008], [0012], [0052] (disclosing “us[ing] 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”); Ex. 1005, 8:61-9:4 (disclosing a financial system that can associate encrypted information “with one or both of know your customer (KYC) data, anti-money laundering (AML) data, and/or other financial data”). A POSITA would have been familiar with implementing these types of KYC checks on a blockchain network. (Ex. 1005).

V. THE ’413 PATENT

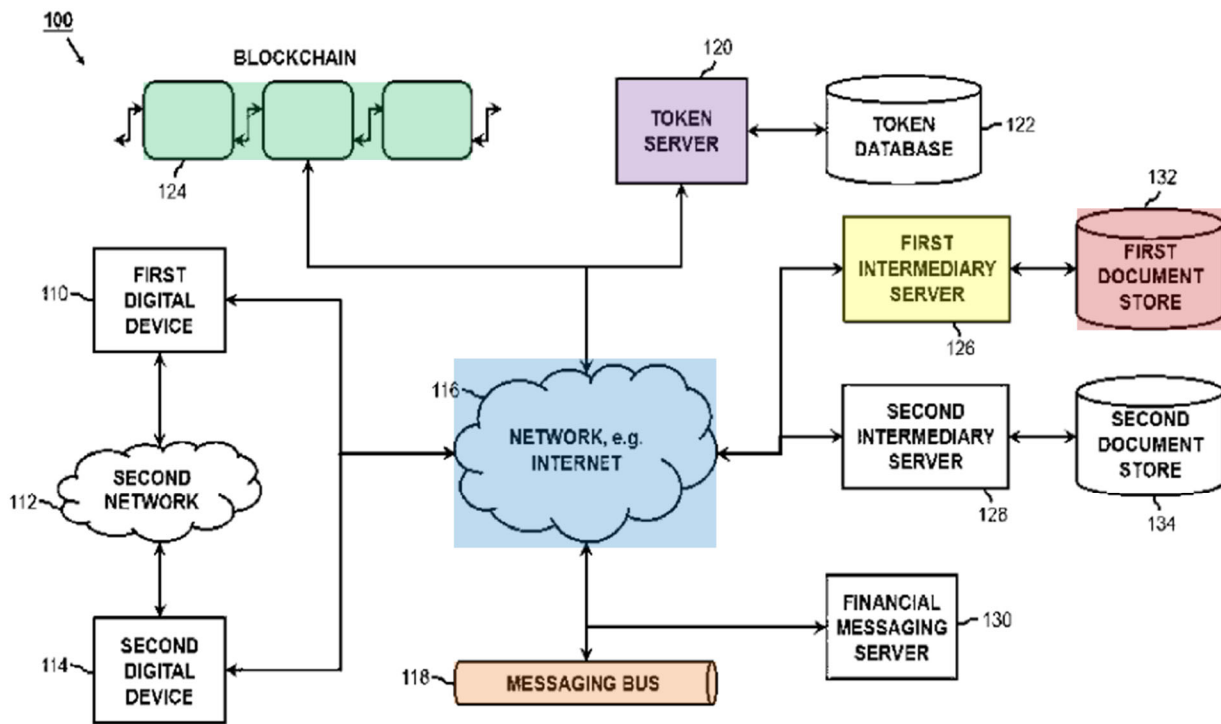
A. Description Of The Alleged Invention

43. The ’413 Patent takes conventional financial transactions and records them on a generic blockchain. The patent explains that “any financial transaction includes a plurality of data associated with the financial transaction.” (Ex. 1001, 1:30-38). The ’413 Patent purportedly addresses problems with “keep[ing] track of the plurality of data during the financial transaction,” and states that if there are “deficiencies in the plurality of data transmitted, time consuming checking and querying operations and correspondence often ensues before the financial transaction can be effected.” (Ex. 1001, 1:39-51).

44. The ’413 Patent purports to provide methods and systems that do not suffer from these issues by using a “token” and an “enriched data record” stored on a generic “blockchain.” (Ex. 1001, Abstract). The ’413 Patent acknowledges that the claimed “token” and “enriched data record” were well-known elements in conventional financial

systems. (Ex. 1001, 27:16-19; 29:1-7; 36:26-28). The 413 Patent also acknowledges it merely applies these well-known elements to *“any blockchain based framework.”*² (Ex. 1001, 24:21-23).

45. Figure 1 of the '413 Patent shows a system for processing a financial transaction where a “first intermediary server 126 (yellow) is connected with a token server 120 (purple) and a blockchain 124 (green) over a network 116 (blue):



(Ex. 1001, Fig. 1).

² Emphasis added unless noted otherwise.

46. The “first intermediary server” transmits “one or more documents pertaining to [a] financial transaction” to the “first document store.” (Ex. 1001, 18:20-23). An “enriched data record is generated from the one or more documents, at the first intermediary server.” (Ex. 1001, 18:31-32). The “enriched data record is added into the blockchain 124, from the first intermediary server.” (Ex. 1001, 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.” (Ex. 1001, 18:63-65). “[T]he token is added into the blockchain.” (Ex. 1001, 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.” (Ex. 1001, 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.” (Ex. 1001, 2:14-15, 28:66-29:3).

B. Person Of Ordinary Skill In The Art

47. It is my opinion that a person of ordinary skill in the art (“POSITA”) at the time of the ’413 Patent would have (i) 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.

VI. THE CHALLENGED CLAIMS ARE NOT SUPPORTED BY THE FIRST AUSTRALIAN PROVISIONAL APPLICATION

48. I understand that PCT Application No. PCT/AU2016/000279 filed on August 12, 2016 (“PCT application,” Ex. 1030) led to the ’413 Patent. I understand that the ’413 Patent claims priority to three Australian provisional applications filed on August 14, 2015 (“AU-1,” Ex. 1027), January 27, 2016 (“AU-2,” Ex. 1028), and May 2016 (“AU-3,” Ex. 1029) (collectively “Australian provisionals”). I have been asked to opine on whether the Challenged Claims are supported by AU-1. As I discuss below, it is my opinion that AU-1 lacks written-description support for the Challenged Claims.

A. The Challenged Claims

49. It is my opinion that the Challenged Claims recite certain limitations that are not disclosed in the first Australian provisional, AU-1. For example, the Challenged Claims recite a “first intermediary server” that generates an enriched data record and 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 that the “token server” adds “the token into the blockchain in association with the enriched data record.” (Ex. 1001, 59:16-18, 62:21-23). It is my opinion that these limitations have no written-description support in the first Australian provisional application.

F. The Provisional Applications

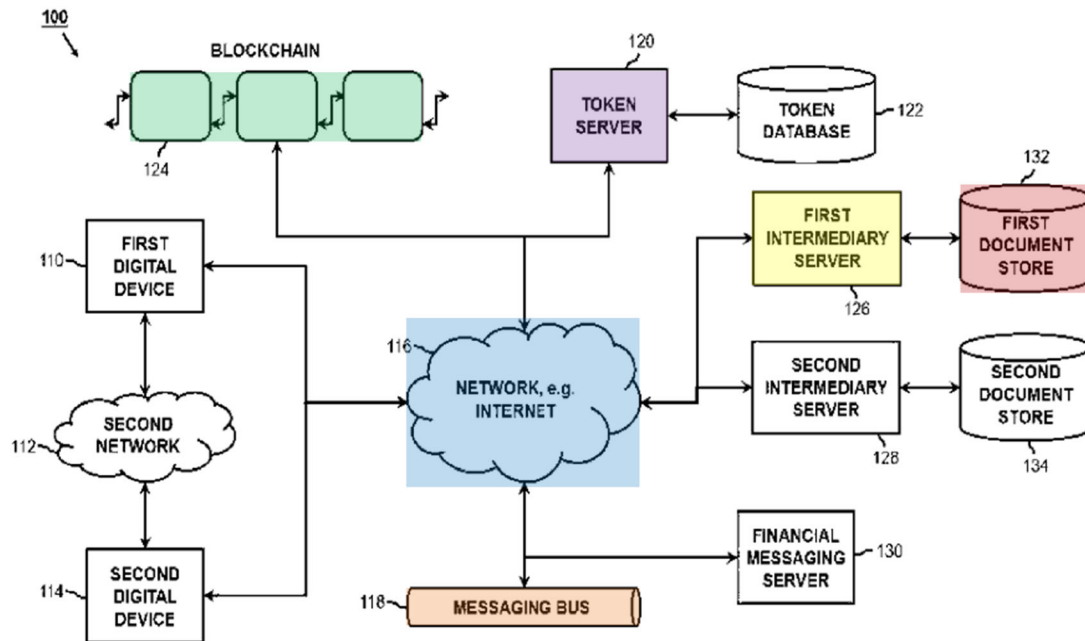
50. Patent Owner filed AU-1 with 6 figures and a 53-paragraph specification. (Ex. 1027). By contrast, the '413 Patent has 17 figures and 310 paragraphs. (Ex. 1002, 147-232). Between AU-1 and the '413 Patent, Patent Owner added new matter with each subsequent application. To illustrate, Ex. 1031 is a copy of the '413 Patent with highlights indicating material disclosed in the provisional applications. Language and figures that are not highlighted indicate material that was not included in any provisional application. Yellow highlights indicate disclosure present in AU-1; purple indicates disclosure added in AU-2; orange indicates disclosure added in AU-3.

51. I understand that Patent Owner filed AU-2 on January 27, 2016. AU-2 has two new figures and 20 additional specification paragraphs that are not included in AU-1. (Ex. 1031, purple highlights).

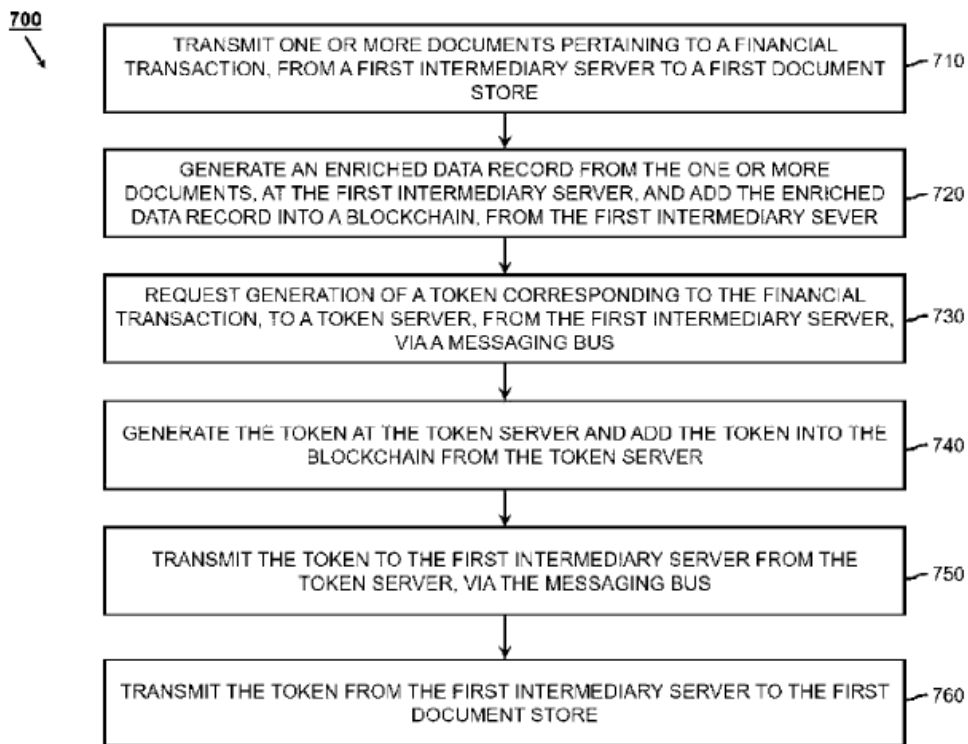
52. I understand that Patent Owner filed AU-3 on May 20, 2016. That application includes two new figures, an addition to a pre-existing figure, and corresponding descriptions for these figures. (Ex. 1029). The additions in AU-3 correspond to Figures 15B, 16, and 17 in the '413 Patent and associated portions of the specification. (Ex. 1031 (portions highlighted orange)).

53. Finally, Patent Owner filed the PCT application that led to the '413 Patent on August 12, 2016. The PCT application included 7 new figures and nearly 200 new paragraphs of specification. (Ex. 1031 (portions without highlighting)). The PCT

application's new matter included Figures 1 and 7 of the '413 Patent, reproduced below, which in my opinion most closely mirror the claims:



(Ex. 1001, Fig. 1).



(Ex. 1001, Fig. 7).

54. In my opinion, the Challenged Claims lack written-description support in AU-1.

B. AU-1 Does Not Provide Written-Description Support For The Challenged Claims

55. First, it is my opinion that Patent Owner 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]). But 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). The description of “token” in AU-1 refers to a “data record,” where the description of “token” in the ’413 Patent refers to a “*pointer to* an enriched data record,” which has a different meaning. Given this difference between AU-1 and the PCT application, it is my opinion that a POSITA would understand that the Patent Owner did not have possession of “token” as claimed in the ’413 Patent until filing the PCT application in August 2016.

56. Second, AU-1 does not disclose “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,” required by the Challenged Claims. The term “enriched data record” never appears in AU-1. And it is my opinion that there is nothing in AU-1 to suggest or describe that “the first intermediary server” generates such a data record or that it does so from the one or more documents.

57. I understand that Patent Owner has indicated in filings from a related litigation that it believes the disclosure of “better data” constitutes an “enriched data record.” (Ex. 1045, 9 (n.1)). But even if this “better data” could disclose an “enriched data record,” it is my opinion that the above-mentioned limitation is unsupported because there is no disclosure that this “better data” is: (1) generated at or by “the first intermediary server,” and (2) generated “from the one or more documents pertaining to

the financial transaction.” (Ex. 1001 59:5-8, 62:11-16, 62:26-33). 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]). It is my opinion that these statements do not relate 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.” Therefore, it is my opinion that the POSITA would understand AU-1 does not disclose the claim 1 limitation of “generating an enriched data record from the one or more documents, at the first intermediary server,” and the claims 15 and 16 limitation of the “first intermediary server... configured to: ... generate an enriched data record from the one or more documents.”

58. AU-1 is also silent about the Challenged Claims requirement of “adding the enriched data record into a blockchain being a distributed ledger from the first intermediary server.” It is my opinion that 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.*” AU-1 makes some 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]). But this passage says nothing about *what information* is added to the blockchain or *which component* adds information on the blockchain. The passage thus cannot support the claim 1 step of “adding the enriched data record into a

blockchain ... from the first intermediary server” and the claim 15 and 16 limitations of the “first intermediary server... configured to: ... add the enriched data record into [a/the] blockchain.” (Ex. 1001, 59:8-9, 62:11-16, 62:26-33).

59. It is also my opinion that 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 claims’ requirement that the “first intermediary server” adds an “enriched data record” to the blockchain. 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) also provides no support. It is my opinion that 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.”

60. Third, it is my opinion that AU-1 does not disclose “adding the token into the blockchain from the token server in association with the enriched data record.” The Challenged Claims require two separate servers (the “first intermediary server” and “token server”) to add two different things (an “enriched data record” and a “token,”

respectively) to the “blockchain.”³ It is my opinion that AU-1 never discloses or suggests this. 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.” It also does not explain or suggest adding a “token” associated with an “enriched data record” to the blockchain. 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,” and does not describe an “association” between a “token” and an “enriched data record.” (Ex. 1001, 11:27-28 (describing “token server 120” and “token database 122” as distinct components)).

61. It is thus my opinion that a POSITA reading AU-1 would not immediately discern the limitations at issue in the claims. For the foregoing reasons, AU-1 does not provide written description support for the limitations required by the Challenged Claims.

³ As discussed below, Claim 16 does not contain a requirement that the token is added to the blockchain from the token server and is therefore broader than Claim 1 and 15 in this aspect.

VII. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Overview Of The Prior Art

1. Kennedy

62. U.S. Patent Publication 2017/0132626 (“Kennedy,” Ex. 1033), entitled “Method And System For Processing Of A Blockchain Transaction In A Transaction Processing Network,” was filed on November 5, 2015 and published on May 11, 2017.

63. Kennedy relates generally “to the use of a blockchain in conjunction with a transaction processing network,” and specifically to the posting and verification of transaction data in a blockchain using the transaction processing network. (Ex. 1033, [0001]). Kennedy notes that “[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.” (Ex. 1033, [0002]). And while these networks are “often highly sophisticated,” transaction processors are always “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]). Thus, Kennedy seeks to provide a technical solution “to further increase the security involved in the processing of payment transactions,” where the payment transaction network may be used in conjunction with a blockchain network for verification and increased processing of transactions. (Ex. 1033, [0003]).

64. Figure 1 of Kennedy depicts a system architecture for validating electronic payment transactions via blockchain and transaction processing networks:

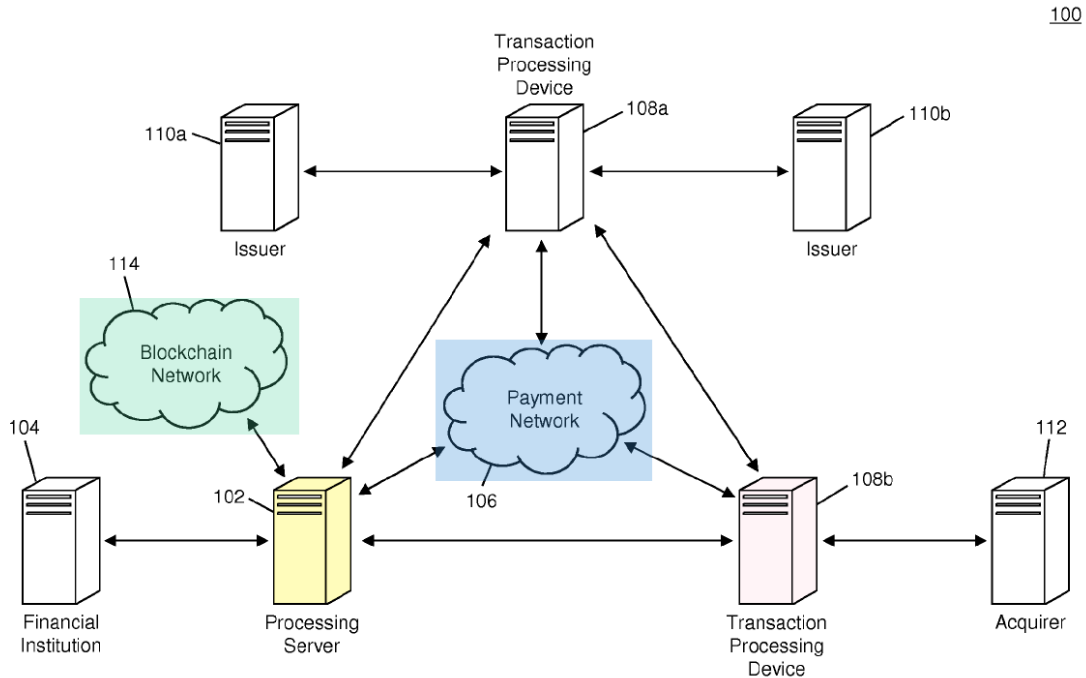


FIG. 1

65. As shown above, Kennedy teaches a financial system 100 centered around payment network 106 (blue). (Ex. 1033, [0020]). Kennedy explains that “payment networks,” or “transaction processing networks,” are “system[s] or network[s] used for the transfer of money via the use of cash-substitutes.” (Ex. 1033, [0017]). “Transactions that may be performed via a payment network may include product or service purchases, credit purchases, debit transactions, fund transfers, account withdrawals, etc.” (Ex. 1033, [0017]).

66. Within the financial system is processing server 102 (yellow), 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 114” (green). (Ex. 1033, [0017]). “In some instances, the processing 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 using traditional methods.” (Ex. 1033, [0017]). “As illustrated in FIG. 1, each processing server 102 and transaction processing device 108 [pink] may be configured to 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]).

67. In one example method, Kennedy teaches that “an acquirer 112 associated with a merchant involved in the payment transaction may submit a transaction message to the payment network 106 via a transaction processing device 108.” (Ex. 1033, [0024]). Transaction messages “may 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, and other data associated with the payment transaction that may be useful in the processing thereof.”

(Ex. 1033, [0024]). The transaction message may be forwarded to processing server 102 “for enhanced validation using the private blockchain.” (Ex. 1033, [0024]).

68. After receipt of the transaction message, processing server 102 “may be configured to generate a data record, which may correspond to a blockchain transaction to be posted to the private blockchain.” (Ex. 1033, [0026]). This generated data record “may include 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]). “In some cases, 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.” (Ex. 1033, [0027]). Processing server 102 then posts the generated data record to the private blockchain so that it “may be subsequently verified by one or more nodes included in the associated blockchain network 114.” (Ex. 1033, [0026]).

69. The posted record “may then be a part of the blockchain, which may thus be independently verifiable by any entity configured to access the blockchain, such as the acquirer 112 and/or issuer 110 involved in the electronic payment transaction, a third party financial institution 104, a consumer or merchant involved in the electronic payment transaction, etc.” Kennedy explains that “[t]he private blockchain [is thus] used as a secure and confidential, yet publicly accessible, record of processed payment transactions for third party verification.” (Ex. 1033, [0026]).

2. Kurani-816

70. U.S. Patent No. 10,719,816 (“Kurani-816,” Ex. 1034), entitled “Systems And Methods For Math-Based Currency Escrow Transactions,” was filed on November 19, 2015 and issued on July 21, 2020.

71. Kurani-816 relates generally to “escrow systems and methods for transactions involving math-based currency [MBC].” (Ex. 1034, 1:17-19). Kurani-816 explains that a “user of MBC can transfer funds to another party by using a private key associated with a certain value of MBC.” (Ex. 1034, 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, thereby completing the transaction.” (Ex. 1034, 1:31-34). Kurani-816 notes that “more and more individuals are utilizing MBC in everyday transactions,” and as such, “[s]ystems and methods that provide for improved MBC escrow transactions are desired.” (Ex. 1034, 1:42-52).

72. Kurani-816 thus discloses a centralized financial system for recording and verifying math-based currency (“MBC”) asset 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). In order to verify ownership of the assets being transferred, Kurani-816 teaches the generation of 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 [].” (Ex. 1034, 3:15-22). The digital title may

“include[] a unique identifier for the asset, a description of the asset, and ownership information concerning the asset” and may be “embodied as a token or a cryptographic string.” (Ex. 1034, 6:8-33, 7:3-5).

73. Kurani-816’s digital titles and pointers are “maintained by the digital title company 106” (purple, below). (Ex. 1034, 6:8-33).

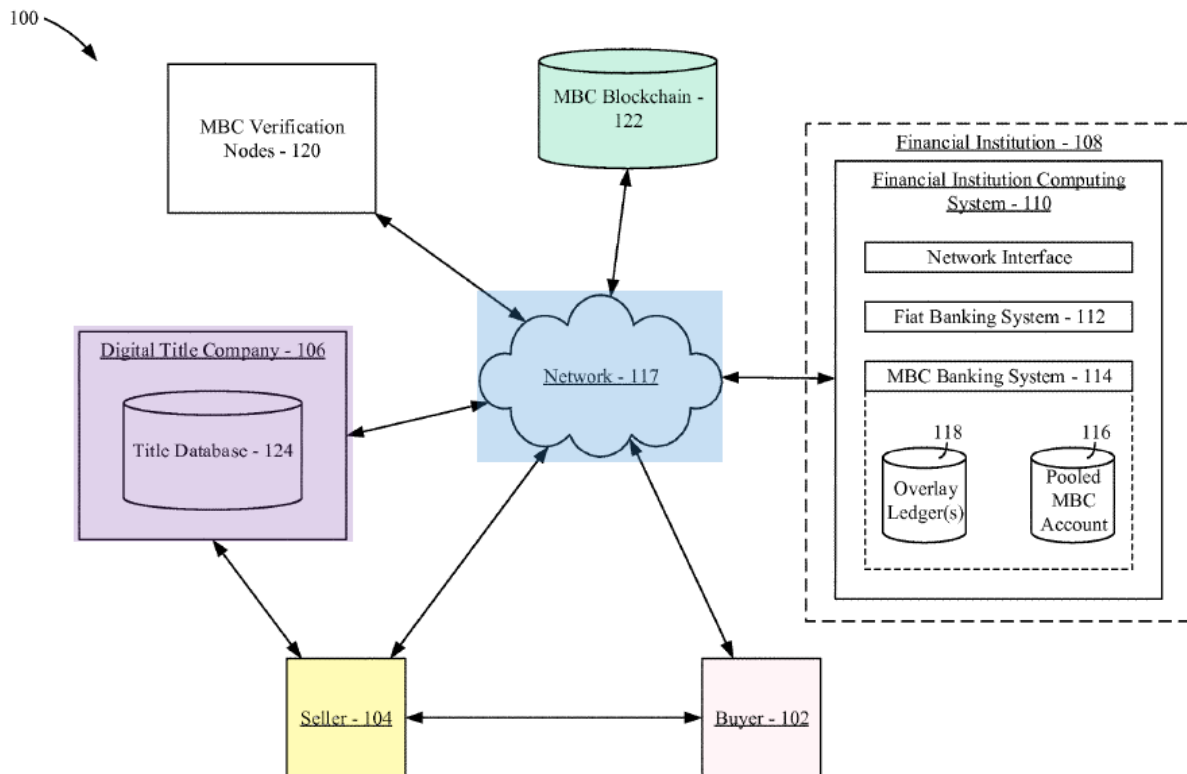


FIG. 1

74. Kurani-816 explains that the digital title company 106 receives a digital title request, which prompts the digital title company to generate the digital title/token. (Ex. 1034, 6:42-45). “The digital title request is received by the digital title company

computing system from a title requestor (e.g., the owner of an asset),” represented in yellow. (Ex. 1034, 6:43-45). 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, a picture of the asset, any prior title information (e.g., proof of ownership, paper title documents, deeds, etc.) and the like.” (Ex. 1034, 6:45-51).

75. The digital title may then be “inserted into the metadata of the MBC transaction that passes title from the seller [yellow] to the buyer [pink].” (Ex. 1034, 6:8-33). Specifically, Kurani-816 discloses a “MBC blockchain 122” (green) that contains “a series of verified transaction blocks” with “a listing of MBC transactions that occurred during the time period corresponding to the block.” (Ex. 1034, 5:54-59). Kurani-816 explains that “[e]ach transaction in the listing of MBC transactions includes information about the transaction, including a sender identity number (e.g., the sender address), a recipient identity number (e.g., the recipient address), 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.” (Ex. 1034, 5:59-6:1). Kurani-816 discloses “placing the digital title or a pointer to the digital title [into that] additional information

or metadata field” of the MBC transaction block on the blockchain, such that the digital title may be associated with and tracked alongside the transaction. (Ex. 1034, 6:1-7).

3. Yago

76. U.S. Patent Application Publication No. 2015/0206106 (“Yago,” Ex. 1011), entitled “Method For Creating, Issuing, And Redeeming Payment Assured Contracts Based On Mathematically And Objectively Verifiable Criteria,” was filed on January 13, 2015 and published on July 23, 2015.

77. Yago’s system “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.” (Ex. 1011, [0046]). Yago adds the contract to a “CDI network” (i.e., “a blockchain”). (Ex. 1011, [0054], [0042], [0013]). A “payment issuer will be able to objectively (and automatically), confirm performance by the seller.” (Ex. 1011, [0047]).

B. Ground 1: Claims 1-2 And 4-20 Are Obvious Over Kennedy In View Of Kurani-816

1. Claim 1

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

78. I have been asked to assume the preamble is a limitation of claim 1. Under that assumption, it is my opinion that Kennedy discloses the preamble. Kennedy describes computer-implemented “systems and methods for validating blockchain transactions using a transaction processing network.” (Ex. 1033, [0004], [0020], Fig. 1). Kennedy’s “transaction processing network” may “process the transfer of money for various types of transactions,” including “product or service purchases, credit purchases, debit transactions, fund transfers....” (Ex. 1033, [0017]).

- b) 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;**

79. It is my opinion that 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) (*i.e.*, “first intermediary server”) and a variety of other interconnected transaction processing devices and servers:

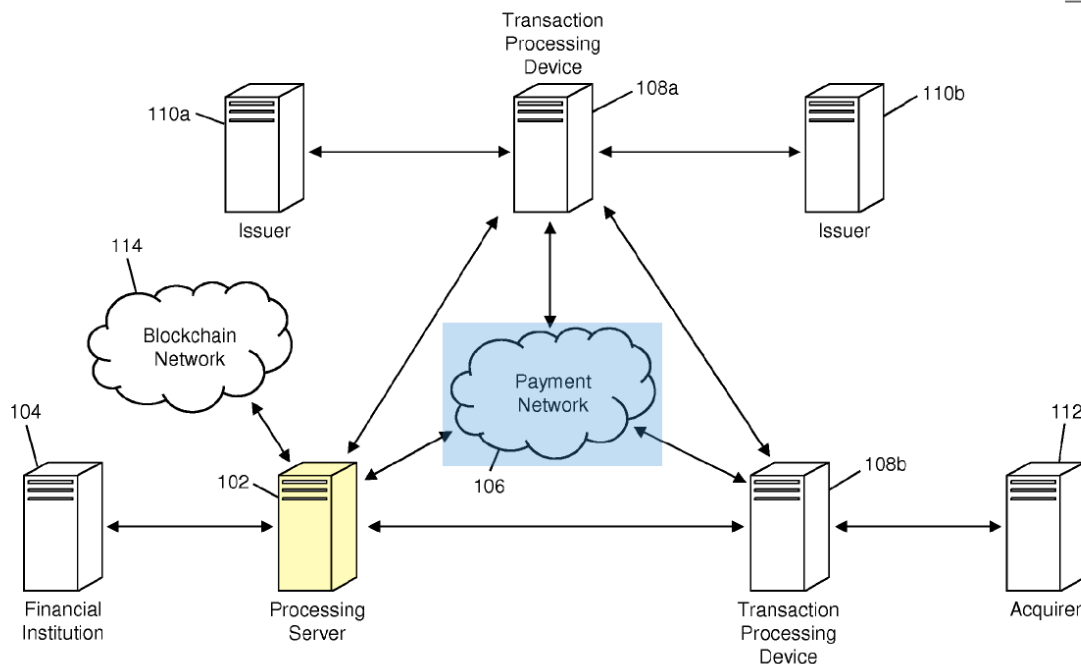


FIG. 1

80. Kennedy explains that the “[p]ayment networks, also referred to herein as transaction processing networks, may use a variety of different protocols and procedures in order to process the transfer of money for various types of transactions. (Ex. 1033, [0017]). The POSITA would have understood that the “payment network” connects these various servers and components, thereby forming the claimed “centralised financial system.”

81. Within Kennedy’s system, “transaction messages” containing financial transaction data are transmitted and exchanged by the “processing server 102.” (Ex. 1033, [0048]). Kennedy explains that “transaction message[s] may be electronically 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 message may also include “a message type indicator indicative of an authorization request.” (Ex. 1033, [0048]). 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.” (Ex. 1033, [0048]).

82. The POSITA would have understood that Kennedy’s transaction messages are the claimed “documents pertaining to the financial transaction because they are records or requests relating to the transaction that contain financial transaction data. 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). The ’413 Patent also states the documents may comprise data such as “account numbers,” “Business Identifier Codes (BIC) of the financial institutions,” “amount of currency to be transferred,” and “type of currency etc.” (Ex. 1001, 12:24-30).

83. It is my opinion that Kennedy further discloses or suggests that these transaction messages are transmitted from a “first intermediary server” to a “document store,” as claimed. Kennedy explains that the “processing server 102” may include “memory 228,” Kennedy explains that the “processing server 102” may include

“memory 228,” which may be “any suitable type of memory,” including “any suitable database configuration” or other “[s]uitable configurations and storage types.” (Ex. 1033, [0046], [0097]). The memory 228 may be “configured to store data for use by the processing server 102 in performing the functions discussed [in Kennedy].” (Ex. 1033, [0046], Fig. 2). The functions of processing server 102 include “applying authentication rules to the transaction data values stored in” a received “transaction message” to calculate authentication and verification scores. (Ex. 1033, [0030]). The processing server 102 also “generate[s] a data message that includes the blockchain data from the transaction message.” The processing server 102 also “transmit[s] the transaction message to the payment network 106 for processing.” (Ex. 1033, [0051]).

84. The POSITA would have understood that transaction messages received by “processing server 102” 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. As Kennedy explains, “processing server 102 may also include a communication module 204. The communication module 204 *may be configured to transmit* data between modules, engines, databases, memories, and other components of the processing server 102 for use in performing the functions discussed herein. (Ex. 1033, [0036]). The POSITA would have understood that storing documents and messages was well-known in the art and would have been beneficial at

least for record-keeping and maintaining a local copy of the transactions for verification purposes.

85. As Kennedy explains, a communication module 204 of processing server 102 “transmit[s] data between modules, engines, databases, memories, and other components of the processing server 102 for use in performing the functions discussed herein. (Ex. 1033, [0036]). For a storage configuration utilizing an external database for storage, the POSITA would have understood that the communication module 204 would have transmitted the received transaction message to the external database to be stored. For a localized storage configuration, the POSITA would also have understood that storing documents would have required writing that information to computer memory and/or disk storage. Whether the database is stored locally, or externally, signals must be propagated in order to write the transaction messages into memory and/or disk storage. Accordingly, it is my opinion that the POSITA would have understood and found it obvious that the transaction messages are “transmitted” to the first document store, as claimed.

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

- c) **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;**

87. It is my opinion that Kennedy discloses or renders obvious this element. Kennedy teaches that “processing server 102” “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]). Kennedy explains that the “generated data record” (*i.e.*, “enriched data record”) “may correspond to a blockchain transaction to be posted to the private blockchain” and “include 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]). Kennedy further 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).

88. Kennedy’s Figure 3 shows that the “generated data record” (*i.e.*, “enriched data record”) is generated at the “processing server 102” (*i.e.*, “first intermediary server”) based from the “transaction messages” (*i.e.*, “one or more documents”):

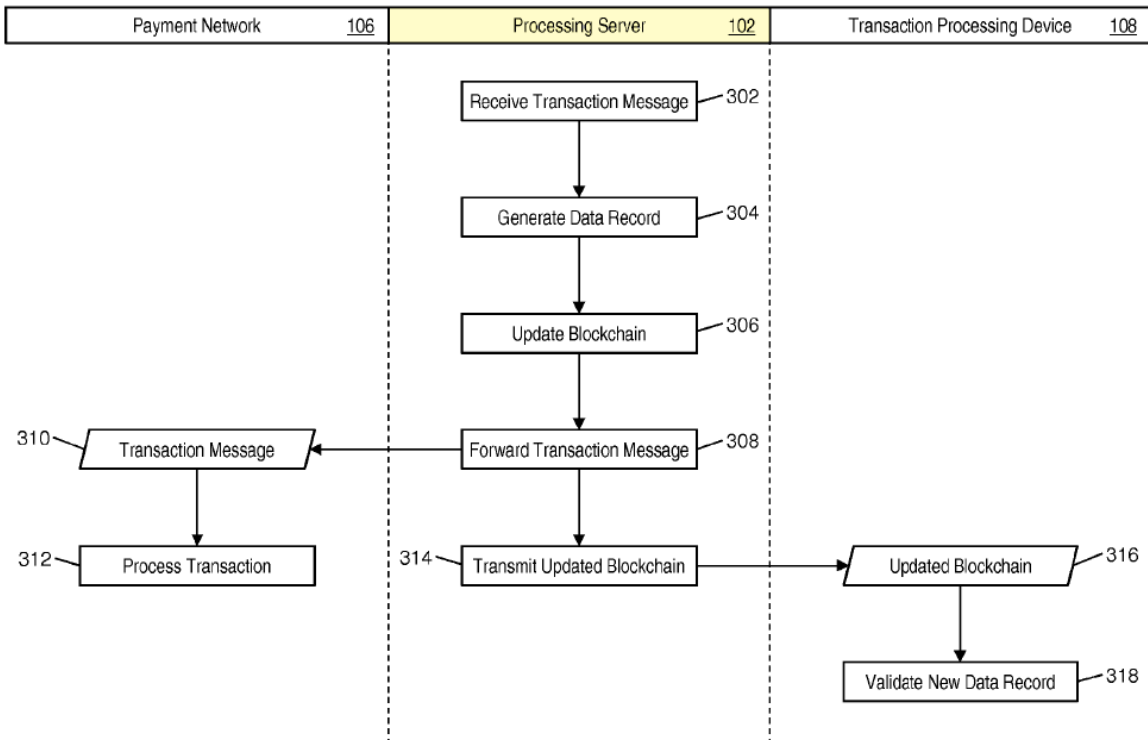


FIG. 3

(Ex. 1033, Fig. 3).

89. The “processing server 102” then “update[s] a private blockchain by adding the generated data record to the blockchain.” (Ex. 1033, [0050]). Kennedy defines “blockchain” as “[a] public ledger of all transactions of a blockchain-based currency” that “may be a ledger of transactions in chronological order, or may be presented in any other order that may be suitable for use by the blockchain network.”

(Ex. 1033, [0018]). The POSITA would have understood this to disclose a “distributed ledger,” as claimed.

90. Kennedy explains that “the private blockchain may be associated with a blockchain network 114 [green], where the 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]). As shown in Figure 1 below, the “generated data record” is added to the blockchain from the “processing server 102” (*i.e.*, “first intermediary server”):

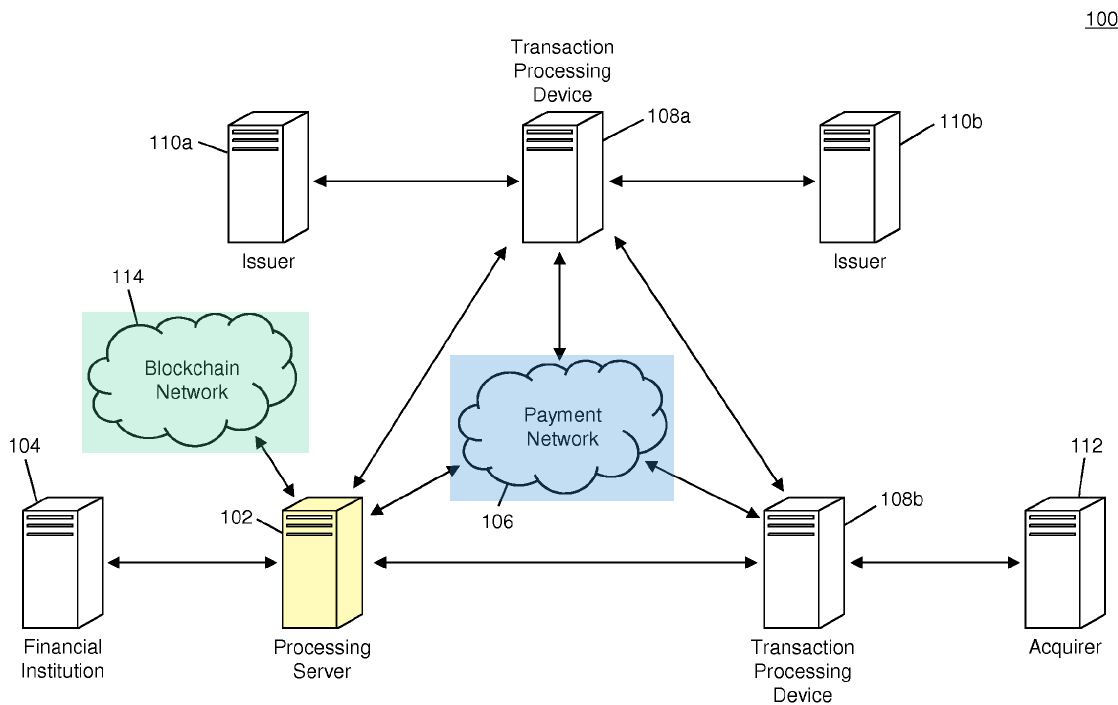


FIG. 1

(Ex. 1033, [0049]-[0050], Fig. 1).

91. Thus, it is my opinion that Kennedy discloses generating an enriched data record (*i.e.*, “generated data record”), from the one or more documents (*i.e.*, “transaction message”), at the first intermediary server (*i.e.*, “processing server 102”), and adding the enriched data record into a blockchain being a distributed ledger (*i.e.*, “blockchain” in “blockchain network 114”), from the first intermediary server (*i.e.*, “processing server 102”).

d) 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;

92. Kennedy, in combination with Kurani-816, renders obvious this element. Kennedy explains that the financial transaction is associated with a “transaction identifier,” or “one or more transaction data values suitable for use in identifying the new data record corresponding to the electronic payment transaction.” (Ex. 1033, [0052]). Kennedy teaches that this “transaction identifier” is included in “the plurality of additional data elements” of the “transaction message,” and is further included in the data record that is generated from the transaction message. (Ex. 1033, [0071], claims 1 and 7 (reciting “the plurality of additional data elements includes a transaction identifier, and the generated data message further includes the transaction identifier”)). Kennedy also explains that the transaction identifier may be included in notifications or

communications sent between servers and devices within the financial system so that the data record of each transaction is identified and traced using a common variable. (Ex. 1033, [0052]).

93. To the extent that Kennedy’s “transaction identifier” does not teach the claimed “token,” Kurani-816 clearly discloses requesting the generation of, and generating, the claimed token.

94. Kurani-816 describes systems and methods for recording and verifying math-based currency (“MBC”) transactions. (Ex. 1034, Abstract). Kurani-816 provides examples dealing with the sale of an asset, 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). In these transactions, Kurani-816 teaches the generation of 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 that the transaction and associated ownership of the asset(s) are tracked and verified. (Ex. 1034, 3:15-22). The “digital title” may “include[] *a unique identifier* for the asset, a description of the asset, and ownership information concerning the asset.” (Ex. 1034, 7:3-5). Kurani-816 explains that 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 that passes title from the seller [] to the buyer [].” (Ex. 1034, 6:8-33).

95. The POSITA would have, therefore, understood that Kurani-816's "digital title" qualifies as the claimed "token" in the '413 Patent. The POSITA would have understood that Kurani-816's "digital title," that can "embodied as a token or a cryptographic string" (Ex. 1034, 6:8-33), corresponds to the claimed "token," and identifies the transaction because it serves as a "unique identifier" associated with the asset being purchased that can be used to record and track title transfers. (Ex. 1034, 3:15-22, 7:3-5). This aligns with the '413 Patent's statement that a "token is a pointer to an enriched data record of a plurality of data required to process a financial transaction and wherein the plurality of data is rendered, formatted or passed through an algorithm in a predetermined manner." (Ex. 1001, 28:66-29:3).

96. The POSITA would have understood that 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. Before August 2015, this means of generating an identifier was conventional and well-practiced in the financial world. (*E.g.*, Ex. 1017, [0024]-[0026]; Ex. 1018, [0019]).

97. For example, one problem facing those seeking to assign a unique token is "collision." This refers to a problem where the processes used to generate the tokens or identifiers in a system result in identical keys for more than one transaction. The POSITA would have understood that ensuring the uniqueness of the digital title/token can avoid this issue, and that this may be accomplished via generic data manipulation

processes that use transaction data as an input to an algorithm in order to generate a unique output. Doing so would have mitigated the risk of collision and would have been obvious to a POSITA. Skilled artisans would have understood that this process can be supplemented by using a unique random value known as a ‘salt’ in addition to the transaction data as an input to an algorithm (such as a well-vetted and secure cryptographic hash function like SHA-256, or SHA-3). This would reduce the chance of collision even further.

98. Accordingly, it would have been obvious to the 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, in order to achieve a “token” that is “unique” and capable of identifying the transaction and asset.

99. The POSITA would have also found Kurani-816’s “digital title” token to be an improvement on Kennedy’s “transaction identifier,” because it could serve not only as a pointer to the transaction but also as a unique identifier of an asset and means to transfer title. (Ex. 1034, 6:8-33). Kennedy makes clear that an intended use of its system is to transact “product” purchases. “Transactions that may be performed via a payment network may include product or service purchases, credit purchases, debit transactions, fund transfers, account withdrawals, etc.” (Ex. 1033, [0017]). Thus, the 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 the

combination. In fact, Kennedy itself recognizes that 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]).

100. Kurani-816’s “digital titles” and pointers are “maintained by the digital title company 106” (purple, below) and its associated “digital title company computing system,” which the POSITA would have understood serves the role of a “token server.” (Ex. 1034, 6:8-41).

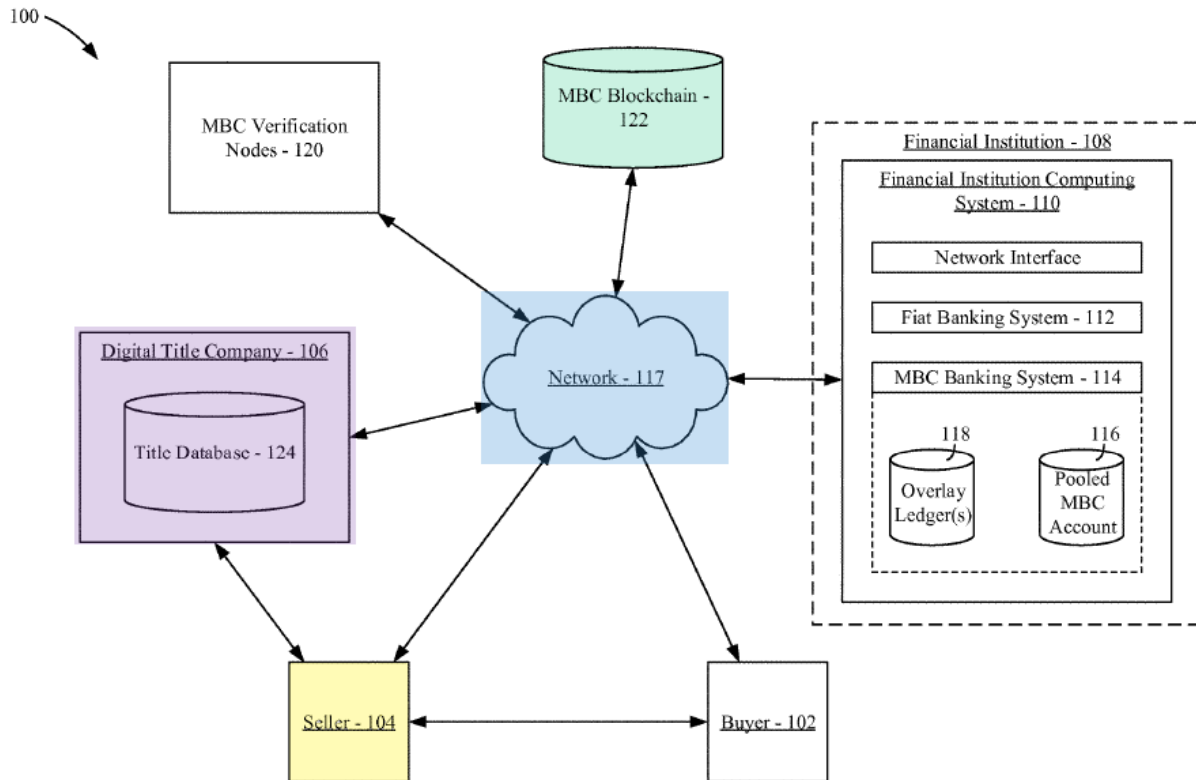


FIG. 1

(Ex. 1034, Fig. 1).

101. Consistent with the claims of the '413 Patent, the “digital title company 106” receives a “digital title request,” which prompts the “digital title company” to generate the digital title/token. As Kurani-816 explains: “The digital title request is received by the digital title company computing system from a title requestor (e.g., the owner of an asset),” represented in yellow. (Ex. 1034, 6:43-45, Figs. 1-2). 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, a picture

of the asset, any prior title information (e.g., proof of ownership, paper title documents, deeds, etc.) and the like.” (Ex. 1034, 6:45-51).

102. As shown above in Kurani-816’s Figure 1, the request for a digital title generation is transmitted from the seller server 104 (yellow) to the digital title company server 106 (purple). (Ex. 1034, 6:43-45, Figs. 1-2). 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. The POSITA applying Kurani-816’s teachings to Kennedy’s system would have thus been motivated to transmit the token generation request from Kennedy’s processing server (*i.e.*, “from the first intermediary server”) such that the request for digital title generation is transmitted from a server processing the transaction that is separate from the token generating server. The POSITA would have found Kurani-816’s disclosure of a separate token server advantageous so as to provide a neutral and location-independent solution for generating tokens that is not affiliated with any participating buyer, seller, bank, etc.

103. For several reasons, the POSITA would have been motivated to combine Kennedy’s financial system with Kurani-816’s token request and generation. Both Kennedy and Kurani-816 describe financial transaction verification and authorization systems utilizing blockchain. Kennedy “relates to the use of a blockchain in conjunction with a transaction processing network, specifically the posting of transaction message data in a blockchain verified using a transaction processing network.” (Ex. 1033,

[0001]). Kurani-816 describes “facilitating the sale of an asset having digital title through two separate math-based currency (‘MBC’) 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).

104. Both Kennedy and Kurani-816 seek to achieve the same goal: improving the systems and methods involved in blockchain-based financial transactions. Kennedy attempts “to further increase the security involved in the processing of payment transactions using a transaction processing network.” (Ex. 1033, [0003]). Kurani-816 notes that “[s]ystems and methods that provide for improved MBC escrow transactions are desired,” and describes “MBC verification nodes 120 and the MBC blockchain 122,” where “[t]he MBC nodes 120 verify all MBC transactions and maintain a distributed ledger (i.e., the MBC blockchain 122) of all the verified MBC transactions.” (Ex. 1034, 1:51-52, 4:65-5:2).

105. Further, Kennedy and Kurani-816 teach similar approaches. Kennedy teaches “systems and methods for validating blockchain transactions using a transaction processing network” made up of interconnected processors and servers, where transaction messages associated with financial transactions and asset sales are verified and stored on the blockchain. (Ex. 1033, [0004]-[0005], [0017]). Kurani-816 similarly teaches “[s]ystems and methods for facilitating the sale of an asset having digital title,”

where transaction data can be “traced and verified through a MBC blockchain or ledger.” (Ex. 1034, Abstract).

106. Moreover, 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 nothing more than the obvious use of prior-art elements according to their established functions. In fact, by the time of the ’413 Patent, the POSITA would have understood that requesting the generation of, and thereafter generating, tokens to track transactions was well-known and commonplace in the art. (Ex. 1046, [0007] (“Non-payment tokens are often used by merchant and acquirer systems to keep track of transactions.”). In one example, a token generation system (including a “token processing server computer”) that “can be leveraged by external entities” was used in connection with financial transactions to “improve[] protection against the misuse of payment accounts by providing usage controls” and to reduce fraud by determining a “token assurance level” for the “token requestor” at the time of generation.) (Ex. 1046, [0034], [0046-0047], [0101]).

107. Further, Kennedy itself already contemplates the use of basic transaction identifiers. (Ex. 1033, [0052], [0071]-[0072], claims 1 and 7). The POSITA reading Kennedy would have been motivated to look to known token generation systems to create a transactional system with increased verification and tracking measures. As explained above, the 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 during more sophisticated transactions, such as property or other high-end asset sales. As Kennedy notes, "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 consumer." (Ex. 1033, [0002], [0017]).

108. The POSITA also would have had a reasonable expectation of success in applying Kurani-816's teachings to Kennedy's transaction processing system. Token request and generation by a token server was well-known and understood by a POSITA in the relevant time period. (Ex. 1046). Thus, combining Kennedy and Kurani-816 merely involves the combination of well-understood and predictable technologies that would have led to obvious results.

109. Additionally, the combination of Kennedy and Kurani-816 renders obvious requesting the generation of a token "via a messaging bus." Indeed, both Kennedy and Kurani-816 describe communication channels that a POSITA would have understood to be a "messaging bus." For example, Kennedy teaches that its "processing server 102" may include a "communication module 204" "configured to transmit data between modules, engines, databases, memories, and other components of the processing server 102." (Ex. 1033, [0036]). According to Kennedy, the "communication module 204 may be comprised of one or more communication types and utilize various

communication methods for communications within a computing device... [f]or example, ... *a bus*.” (Ex. 1033, [0036]).

110. Similarly, Kurani-816 explains that “[t]hose skilled in the art will appreciate that [its] network computing environments may encompass many types of computers [and] processor systems” and may be “practiced in distributed computing environments where tasks are performed by local and remote processing devices that are linked ... *through a communications network*.” (Ex. 1034, 11:61-12:5).

111. These descriptions in Kennedy and Kurani-816 align with the ’413 Patent’s statement that the “term ‘bus’ ... should be construed broadly herein as any system for communicating data.” (Ex. 1001, 33:35-45). A POSITA would have understood that Kennedy’s “communication module 204” may be configured “to communicate 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]).

112. Accordingly, it is my opinion that the combination of Kennedy and Kurani-816 renders obvious requesting generation of a token corresponding to the financial transaction to identify the one or more documents (*i.e.*, “digital title”/ “token” generation request), to a token server (*i.e.*, “digital title company 106”), from the first intermediary server (*i.e.*, “processing server 102”), via a messaging bus (*i.e.*, communication network) in the centralised financial system.

e) **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;**

113. It is my opinion that Kennedy, in combination with Kurani-816, renders obvious this element. After Kurani-816's "digital title company" (*i.e.*, "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, at 6:66-7:18).

114. Kurani-816 further explains that the "digital title," "embodied as a token or a cryptographic string," may then be "*inserted into the metadata of the MBC transaction* that passes title from the seller [] to the buyer." (Ex. 1034, 6:8-33). Specifically, Kurani-816 teaches a "MBC blockchain 122," or "a chronological and public ledger of all MBC transactions that have been executed," containing "a series of verified transaction blocks" with "a listing of MBC transactions that occurred during the time period corresponding to the block." (Ex. 1034, 5:54-59). "Each transaction in the listing of MBC transactions includes information about the transaction, including a sender identity number (e.g., the sender address), a recipient identity number (e.g., the recipient address), 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.*" (Ex.

1034, 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 on the blockchain, “such as the op_return field, the nSequence field, or another metadata field of a Bitcoin transaction.” (Ex. 1034, 6:1-7).

115. The 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.” Kennedy teaches that its “generated data record” representing a financial transaction contains various transaction information and is added to the blockchain in blockchain network 114. (Ex. 1033, [0050] [0062]). The transaction may then be validated by the transaction processing device 108. (Ex. 1033, [0053], [0063]). After the transaction has been processed, Kennedy’s blockchain is then “further updated” to include the generated data record and a “new data record,” which is validated. (Ex. 1033, [0065]). Kurani-816’s “digital title” is “written in the MBC blockchain 122” when the MBC transfer, or transaction, is verified. (Ex. 1034, 9:43-47). The POSITA thus would have understood 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 transaction information for the financial transaction.

116. Additionally, it would have been obvious to a POSITA that the token in the Kennedy/Kurani-816 combination be “added into the blockchain from the token server” as claimed. Figure 1 of Kurani-816 depicts two-way communication between “digital title company 106” (purple) and the MBC blockchain 122 (green) via network 117 (blue):

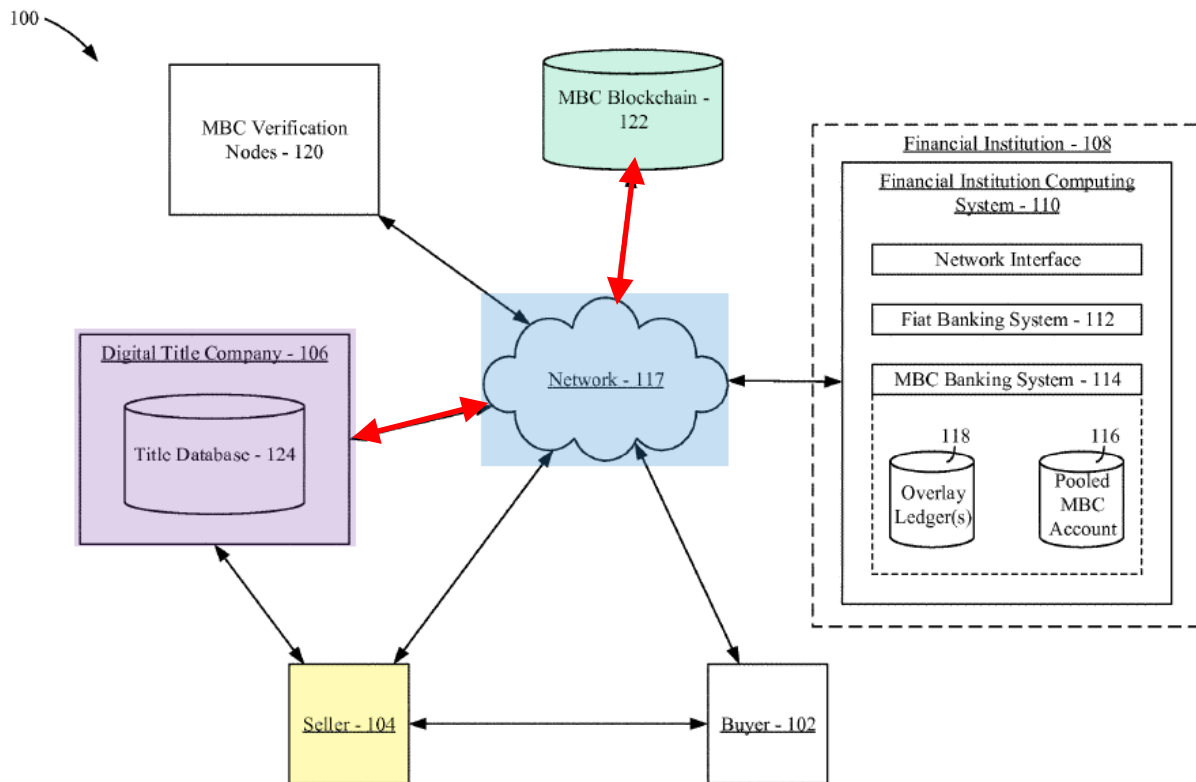


FIG. 1

117. One of Kennedy’s stated goals for transaction processing networks is “to protect against fraud and to provide peace of mind to consumers.” (Ex. 1033, [0002]). As explained above for claim element 2, it was well-known to use token servers to

reduce misuse and fraud by a token requestor. (Ex. 1046, [0034], [0046-0047], [0101]). The POSITA would have recognized that having the system that generated the token add the token into the blockchain would ensure integrity of the information. Doing so would mitigate the risk of token data being corrupted by intermediaries before it is added to the blockchain. In the Kennedy/Kurani-816 combination, the POSITA would have understood the digital title/token to be added to the blockchain by the token server, such as for example, when the blockchain “further updated” to include the generated data record (previously added) and the “new data record” reflecting the processed financial transaction.

118. Thus, for the reasons stated above, it is my opinion that the combination of Kennedy and Kurani-816 renders obvious generating the token (*i.e.*, “digital title”/“token”) at the token server (*i.e.*, “digital title company 106”) and adding the token into the blockchain (*i.e.*, “blockchain” in “blockchain network 114”) from the token server in association with the enriched data record (*i.e.*, “generated data record”).

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

119. It is my opinion that Kennedy, in combination with Kurani-816, renders obvious this element. As discussed above, Kennedy teaches that a “transaction identifier” may be included in the “generated data record” (*i.e.*, “enriched data record”) generated by the “processing server 102” (*i.e.*, “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 102,” Kurani-816 teaches this element, and the POSITA would have been motivated to combine Kennedy’s financial system with Kurani-816’s token request and generation methods for the reasons I explained above for element 3.

120. 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). Then “the digital title company computing system creates a unique token associated with the digital title... [which] *may be provided to the verified owner of the asset.*” (Ex. 1034, 7:7-9). As Kurani-816’s Figure 1 shows, the “digital title company” (purple) transmits the “digital title” token to the owner of the asset, represented by “seller 104” server (yellow) below:

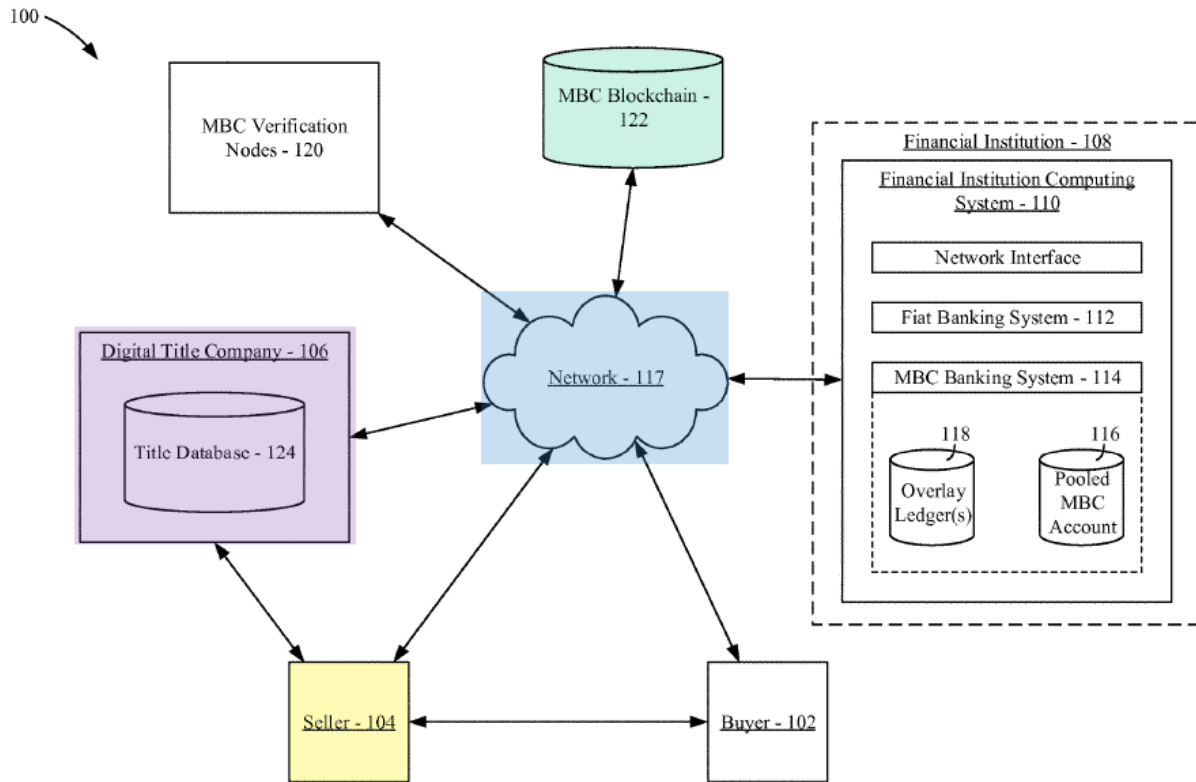


FIG. 1

121. Kurani-816 thus discloses that the digital title/token is transmitted from the token server to the first intermediary server that sent the token generation request. (Ex. 1034, 6:43-45, 7:7-9). As explained for element 3, the POSITA would have understood that within the Kennedy-Kurani-816 combination, Kennedy’s “processing server 102” sends the token generation requests, such that the request for the digital title/token originates from the server processing the transaction and generating the data record. Based on Kurani-816’s teachings, the POSITA would have been motivated to transmit the token from Kurani-816’s “digital title company computing system” (*i.e.*, “token

server”) to Kennedy’s “processing server 102” (*i.e.*, “first intermediary server”), to ensure that the digital title/token is associated and stored locally with the transaction record and documents. For the reasons already explained regarding Kennedy’s communication module and Kurani-816’s communications network for element 3, the POSITA would have understood that this transmission occurs via a messaging bus.

122. Accordingly, it is my opinion that the combination of Kennedy and Kurani-816 renders obvious transmitting the token (*i.e.*, “digital title”/“token”) to the first intermediary server (*i.e.*, “processing server 102”) from the token server (*i.e.*, “digital title company 106”), via the messaging bus (*i.e.*, communication network).

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

123. It is my opinion that Kennedy, in combination with Kurani-816, renders obvious this element. As explained for element 1, Kennedy discloses memory configured to store transaction data, which the POSITA would have understood to be a “first document store” capable of storing transaction messages. (Ex. 1033, [0046]). Kennedy’s transaction identifier may be included in “the plurality of additional data elements” of the “transaction message[s]” being stored. (Ex. 1033, [0071]-[0072]; claims 1 and 7). Kennedy also discloses that the processing server 102 may perform additional processing of the transaction data, including transmitting the transaction data

to other parts of the payment network, even after the blockchain has been updated to include the generated data record. (Ex. 1033, [0063-65]).

124. From these disclosures, the POSITA would have found it obvious to store the digital title/token in association with the transaction messages in the “first document store,” as claimed, to facilitate the additional processing performed on the transaction data and to maintain a useful local record of the transaction that can be compared against the record stored on the blockchain.

125. Thus, the combination of Kennedy and Kurani-816 renders obvious transmitting the token (*i.e.*, “digital title”/“token”) from the first intermediary server (*i.e.*, “processing server 102”) to the first document store (*i.e.*, “memory”) in association with the one or more documents (*i.e.*, “transaction messages”).

126. It is my opinion that claim 1 would have been obvious over the combination of Kennedy and Kurani-816.

2. Claim 2

127. Claim 2 depends from claim 1, reciting “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.”

128. It is my opinion that Kennedy, in combination with Kurani-816, renders obvious this claim. Kennedy teaches systems and methods to process financial

payments, such as to a merchant for the purchase of goods. (Ex. 1033, [0083]-[0084]). Kennedy also explains that “[t]he processing server 102 may be configured to communicate with a financial institution 104,” which “may be an entity involved in the conducting and processing of payment transactions, such as a participant (e.g., payer or payee), an account holder, gateway processor, etc... [E]ach processing server 102 and transaction processing device 108 may be configured to 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]).

129. As shown in the figure below, Kennedy teaches transmitting a “notification” from the “processing server 102” (yellow) to a “transaction processing device 108” (pink) 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.” (Ex. 1033, [0052]). Kennedy thus provides transmitting messages from a “processing server” (*i.e.*, “first intermediary server”) to another “transaction processing device” (*i.e.*, “second intermediary server”) that contains a transaction identifier.

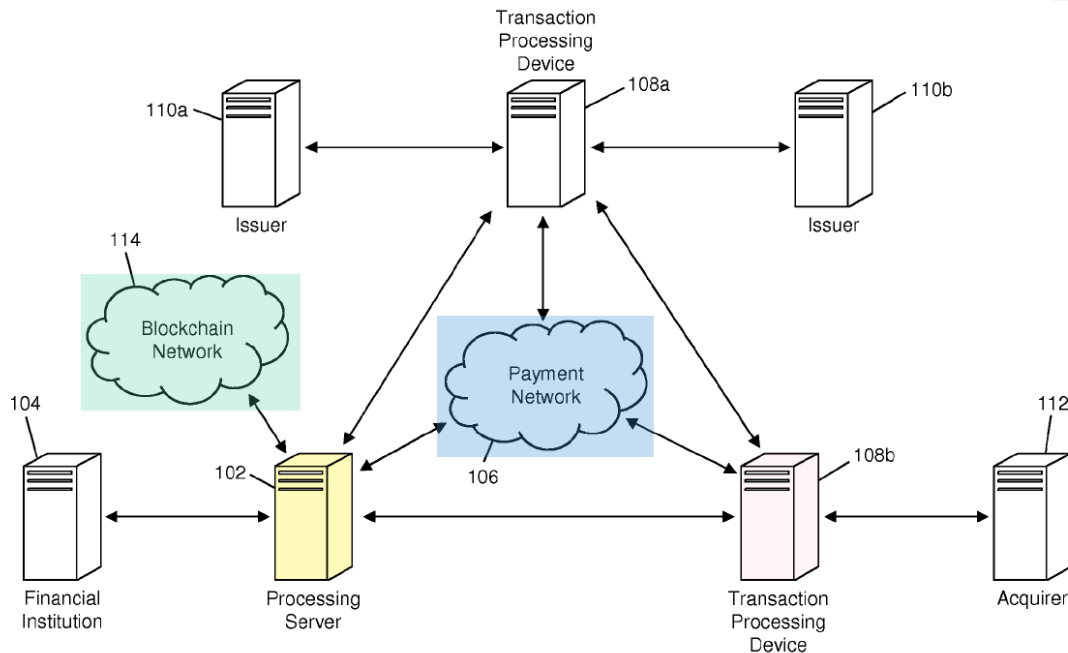


FIG. 1

130. Kurani-816 similarly teaches that 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). The POSITA would have understood that Kurani-816’s receiving party/buyer would have a separate server, as shown by the separate pink block in Kurani-816’s Figure 1, such that the digital title/token is passed from a first server of the system (yellow) to a second server (pink), just like Kennedy.

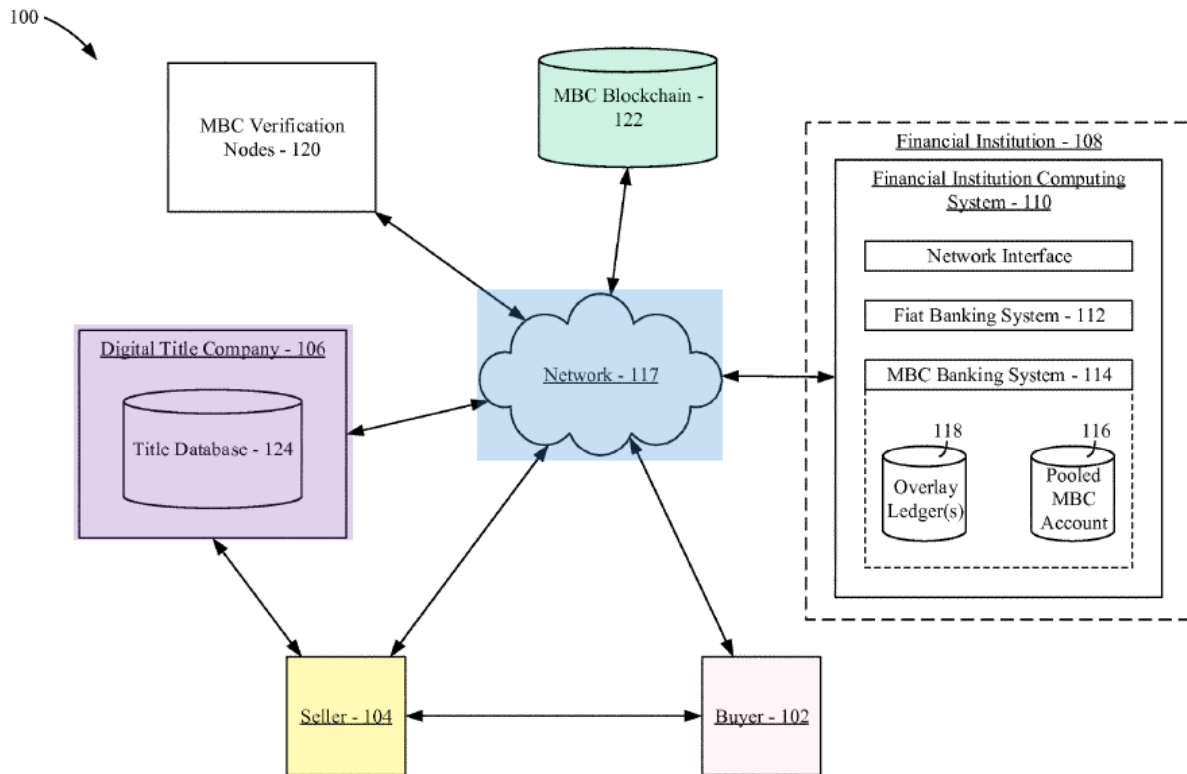


FIG. 1

131. As shown above, communications between servers during a payment transaction were well known, and the POSITA would have been motivated to implement Kurani-816's transmission of digital titles/tokens within Kennedy's payment network such that the Kennedy's "processing server" transmits the token to the "transaction processing device" of a second user during payment. Indeed, Kennedy already discloses transmitting messages that include transaction identifiers, and the POSITA would have been motivated to implement Kurani-816's digital title/token into Kennedy's system in order to process more sophisticated transactions and asset sales, as I discuss above in

elements 3 and 4. The POSITA would have been further motivated to include the token in messages exchanged between users and/or servers to create a common identity in each message that ties the exchange back to the transaction.

132. It is my opinion that claim 2 would have been obvious over the combination of Kennedy and Kurani-816.

3. Claim 4

133. Claim 4 depends from claim 1, further reciting “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.”

134. It is my opinion that Kennedy in combination with Kurani-816 renders obvious this claim. As explained for claim 2, Kennedy and Kurani-816 teach transmitting messages containing transaction identifiers or digital titles/tokens. (Ex. 1033, [0052]; Ex. 1034, 7:8-11). The POSITA would have understood that a straightforward and well-known way for one party to pass the token to a receiving party is through a device-to-device transfer, such as through personal computers or other

devices. As Kurani-816 recognizes, its “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 is configured to receive, 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” and “configured to receive an amount of funds from the buyer, and to receive an identifier of the math-based currency transaction from the seller device.” (Ex. 1034, 2:18-26).

135. The POSITA would have understood from Kurani-816’s teachings that the digital titles/tokens may be sent from the “seller device” (*i.e.*, “first digital device available with a first user”) to the “buyer device” (*i.e.*, “second digital device” of a “second user”). It would have also been understood by the POSITA that within the Kennedy-Kurani-816 combination, processors associated with each device (*i.e.*, “first intermediary server” and “second intermediary server,” respectively) would be involved in the transmission and receipt of the digital title/token such that the token is transmitted: (1) from the “processing server 102” to the “seller device” (*i.e.*, “transmitting the token from the first intermediary server to a first digital device available with a first user”); then (2) from the seller to the buyer via device-to-device transfer (*i.e.*, “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 the buyer (*i.e.*, “providing the token to

a second intermediary server in the centralised financial system, from a second digital device”).

136. Additionally, after the digital title/token is sent to the buyer, the POSITA would have found it obvious to transmit the token to memory (*i.e.*, a “second document store”) from the “transaction processing device” (*i.e.*, “second intermediary server”) associated with the buyer. For the same reasons explained above for element 1, both Kennedy and Kurani-816 disclose various memory and storage configurations and the POSITA would have found it well-known and conventional to store tokens and other transaction data locally for verification and record-keeping purposes, as I discuss above in element 1.

137. Finally, as explained for claim 2, the POSITA would have further understood that communication between servers during a payment transaction were well known, as is using a token as a transaction identifier throughout the course of payment. Thus, the 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”) in order to maintain a complete record of the transaction and assist with tracking the chain of title or other financial transfer throughout processing.

138. It is my opinion that claim 4 would have been obvious over the combination of Kennedy and Kurani-816.

4. Claim 5

139. Claim 5 depends from claim 1, reciting “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.”

140. It is my opinion that Kennedy, in combination with Kurani-816, renders obvious this claim for the reasons provided explained for element 2 of claim 1. Kennedy teaches its “processing server” “generate[s] a data record” from the transaction message, where the “generated data record” may include 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).

141. It is my opinion that claim 5 would have been obvious over the combination of Kennedy and Kurani-816.

5. Claim 6

142. Claim 6 depends from claim 1, further reciting “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.”

143. It is my opinion that Kennedy, in combination with Kurani-816, renders obvious this claim in part for the reasons explained for element 2 of claim 1 and claim 5. In addition, Kennedy teaches that the “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]). For example, 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.” (Ex. 1033, [0027]). The POSITA would have understood that hashing and encryption serves to “de-identify” the transaction attributes, as claimed, because these hashing and encryption measures remove and/or mask personal transactional information for privacy reasons.

144. Kennedy thus discloses extracting “transaction data values” (*i.e.*, “extracting a plurality of attributes”) from the “transaction message” (*i.e.*, “one or more documents”) at the “processing server 102” (*i.e.*, “first intermediary server”), and “hash[ing] and/or encrypt[ing]” the “transaction data values” (*i.e.*, “de-identifying the

plurality of attributes to obtain a plurality of de-identified attributes”) at the “processing server 102” (*i.e.*, “first intermediary server”) to create the “generated data record” (*i.e.*, “combining the plurality of de-identified attributes to generate the enriched data record”).

145. It is my opinion that claim 6 would have been obvious over the combination of Kennedy and Kurani-816.

6. Claim 7

146. Claim 7 depends from claim 1, reciting “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.”

147. 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 “hash[ing]” transaction data values included in the generated data record. (Ex. 1033, [0049]). A POSITA would have understood that hashing is a valuable tool for de-identification because it provides irreversible transformation, consistency, determinism, and security.

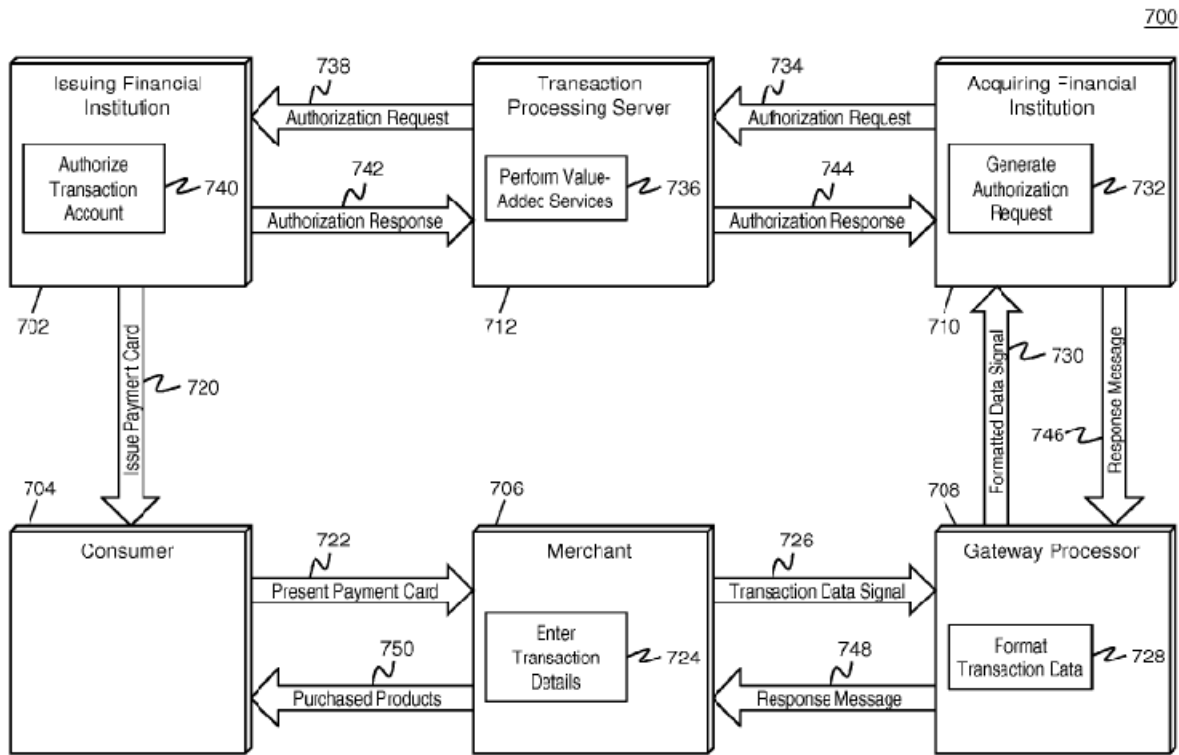
148. Kennedy in combination with Kurani-816 renders obvious this claim for the reasons explained for element 2 of claim 1 and claims 5 and 6.

149. It is my opinion that claim 7 would have been obvious over the combination of Kennedy and Kurani-816.

7. Claim 8

150. Claim 8 depends from claim 1, further reciting “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.”

151. Kennedy, in combination with Kurani-816, renders obvious this claim. Kennedy teaches a comprehensive communication network where “each processing server 102 and transaction processing device 108 may be configured to communicate with one or more financial institutions 104, issue[r]s 110, acquirers 112, and other entities involved in the processing of electronic payment and blockchain transactions.” (Ex. 1033, [0021]). Kennedy’s Figure 7 shows that processing of payment transactions with a merchant “may be performed by one or more components of the system 100 discussed above, such as the processing server 102, financial institution 104, payment network 106, transaction processing device 108, issuer 110, acquirer 112, etc.” (Ex. 1033, [0072]).



152. At steps 732-744, an “acquiring financial institution 710,” which “may manage transaction accounts for merchants 706” communicates via a series of requests/responses with an “issuing financial institution 702,” which “may be a financial institution, such as a bank, 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 704. (Ex. 1033, [0073]-[0076], Fig. 7). The requests/responses exchanged between each of the financial institution servers involve authorization of the payment transaction, including “approval or denial of the payment transaction” “and other considerations that will be apparent to persons having

skill in the relevant art.” (Ex. 1033, [0083]-[0084]). Thus, it was well-known in the art for processors and computer components to communicate using requests and responses following the client-server interaction paradigm. As explained for element 3 of claim 1, it would have been obvious to the POSITA for such messages to be communicated via the messaging bus. Accordingly, incorporating 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 the POSITA, as this involves nothing more than the combination of prior-art elements according to known methods to yield obvious results.

153. 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, the POSITA would have understood that messages regarding a particular transaction would include the transaction identifier or digital title/token such that each transaction and sale is properly identified throughout the communication flow between servers. As described above, the combination of Kennedy and Kurani-816 renders 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,” and the “one or more first responses each comprising the token corresponding to the respective one or more first requests” would have been obvious to the POSITA.

154. 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 the POSITA. As explained for element 2 of claim 1 and claim 4, the POSITA would have found it obvious and conventional for entities involved in the centralized financial network to maintain records of their transactions in local storage. Both Kennedy and Kurani-816 disclose methods to authenticate, track, and verify transactions (either with a merchant or with respect to an asset transfer between users). And the POSITA would understand that local storage of transaction information is conventional for parties to an electronic funds transfer. (*E.g.*, Ex. 1011, Fig. 4, [0074]-[0075] (disclosing that a first and second financial institution on a network store transaction data in a “first private ledger” and “second private ledger” in addition to adding transaction data to a public ledger)). Additionally, as explained below, the POSITA would have understood that a well-known and standard way to verify transaction information is to compare that information against an entity’s own records.

155. 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.” The POSITA would have found this step obvious based on their skill level and knowledge of the art with the disclosures of Kennedy and Kurani-816. Both Kennedy and Kurani-816 teach financial systems that hash or encrypt various messages and/or transaction information for verification purposes. As described above, Kennedy teaches that 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 MBC transactions may be “sign[ed] (e.g., encrypt[ed]) ... with a private encryption key” during the authorization and verification process. (Ex. 1034, 5:33-35). These disclosures establish that hashing and encrypting information during transmission were well-known to the POSITA, and were a conventional way to protect transaction information. The POSITA would have, therefore, found it obvious to generate hashes of the requests and responses and digitally sign transactions for these same privacy, integrity, and authentication reasons.

156. The POSITA would have also found it obvious and advantageous to generate these hashes for verification purposes. Kennedy and Kurani-816 relate to methods for verifying transactions. Kennedy provides methods for “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 may [] be 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.” (Ex. 1033, [0026]-[0027]).

157. Kennedy further explains that these transaction data values may be hashed for verification purposes: “[O]ne 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. For example, 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.” (Ex. 1033, [0027]).

158. 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). “The MBC nodes 120 verify MBC transactions by verifying information relating to the transaction, such as by verifying the signatures of the MBC transactions,” and “cryptographically verifying the encrypted transaction information.” (Ex. 1034, 5:5-11, 49-50).

159. The POSITA would have understood from Kennedy's and Kurani-816's disclosures that it would have been advantageous to utilize hashing for verification purposes. The POSITA would have understood that using hashing for data integrity verification was well-known. There is extensive documentation of this concept in the art, including a 2011 IBM publication documenting cryptographic services, which shows that the use of hashing to "verify that data has not been altered during transmission or storage" was already well known and within the knowledge of those skilled in the art. (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.")). A POSITA would have recognized IBM as a significant player in the field of cryptography and computer security. The POSITA also would have known that IBM maintains a publicly available library featuring documentation related to its offered products and services. Thus, a POSITA seeking to implement a cryptographic system would have looked to IBM's library to understand industry standards and would have accessed the publication described above. (Ex. 1024, 11 (highlight indicating link to publication)).

160. This publication evidences that those of skill in the art would have known the details of this 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.”)).

161. The POSITA would have thus found it obvious to hash one or more responses at the entity on Kennedy’s network communicating with the “processing server” (*i.e.*, “first intermediary server”)—for example, Kennedy’s “transaction processing device” (*i.e.*, second intermediary server)—so that the “processing server” may verify the integrity of the response. The POSITA also would have found it obvious to hash the one or more *requests* at Kennedy’s “transaction processing device” (*i.e.*, second intermediary server”). This would ensure that when the “transaction processing device” communicates its response to the “processing server,” the “processing server” can also ensure that its original request arrives without being corrupted. Hashing both the request and the response at the second intermediary server, therefore, increases the security of the system allowing parties to verify the integrity of information both sent and received. The POSITA, therefore, would have found it obvious to generate hashes of the requests and responses at the “transaction processing device” (*i.e.*, “second intermediary server”) for these reasons.

162. Finally, it would have been obvious to the 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. As I discuss above in claim 1, both Kennedy and Kurani-816 teach methods of adding and updating

transaction information on the blockchain. The POSITA would have found it obvious that the verification enabled by hashing information described above may be accomplished by comparing a hash on the blockchain with an entity's own hash of the record. And the POSITA would have understood that "[o]ne way to ensure [that the hash is transmitted with integrity] is to publish the hash in a reliable source of public information." (Ex. 1015, 22). Accordingly, the POSITA would have found it obvious to add the hashes into the blockchain of "blockchain network 114" from the "transaction processing device" (*i.e.*, "second intermediary server") in order to maintain a complete transaction record and to allow the "processing server 102" (*i.e.*, "first intermediary server") to verify the integrity of the request as delivered to the "transaction processing device" (*i.e.*, "second intermediary server") and the integrity of the received response.

163. It is my opinion that claim 8 would have been obvious over the combination of Kennedy and Kurani-816.

8. Claim 9

164. Claim 9 depends from claim 8, further reciting "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."

165. It is my opinion that Kennedy, in combination with Kurani-816, renders obvious this claim. As explained for claim 8, Kennedy and Kurani-816 disclose

transaction verification, including verifying hashed or encrypted information on a blockchain, and the POSITA would have found it obvious and conventional to verify the hashed requests and responses on the blockchain. The POSITA would have understood this process to include regenerating the hash of the “one or more first responses” and to do so “from the first intermediary server” in order for the entity that receives the response(s) to verify the information included therein.

166. The POSITA would have further understood that, within the context of the Kennedy and Kurani-816 combination, this response verification would have been accomplished “using the token,” as claimed. As explained for element 3 of claim 1 and claim 2, Kennedy and Kurani-816 include the use of a transaction identifier or digital title/token (*i.e.*, “token”) to identify the transaction or asset transfer within the financial system. Because the digital title/token is transaction-specific, the 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, in order to accomplish the disclosed verification.

167. It is my opinion that claim 9 would have been obvious over the combination of Kennedy and Kurani-816.

9. Claim 10

168. Claim 10 depends from claim 8, reciting “wherein each one of the one or more first requests are: encrypted with a second public key and signed with a first public

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

169. It is my opinion that the Kennedy/Kurani-816 combination renders obvious this claim. As I discussed above, 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 the POSITA’s knowledge.

170. For example, Kurani-816 discloses using public and private key pairs to encrypt information. (Ex. 1034, 3:57-61 (“[T]he customer transfers various information for the MBC (including the private keys) and the 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 (“[C]ustomers initiate a transaction to the financial institution 108 and the new *private/public key pair* which are created as a result of the performance of the transaction are stored in the database.”); 3:65-67 (describing “pooled MBC

account 116 (i.e., a database of *private key/public key pairs*”); 5:33-37). And 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 within the knowledge of a POSITA. (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.”)).

171. The POSITA would have understood the claim 10 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 generally in Kurani-816, which teaches using public and private keys to encrypt and decrypt information. (Ex. 1034, 3:57-67, 5:33-37).

172. The POSITA would have found it obvious to apply the well-known public key/asymmetric cryptography taught by Kurani-816 to Kennedy’s system to facilitate secure private communications between the parties. From the state of the art and Kurani-816’s teachings, the POSITA would have understood that encryption of

information may be accomplished using a plurality of keys (specifically a first public key, a second public key, a first private key, and a second private key) and digital signatures.

173. It was well-known to use public key cryptography to generate digital signatures to authenticate the source of a message. (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, there are two keys associated with the sender—the sender’s private key or the sender’s public key.

174. A conventional digital signature algorithm uses a sender’s private key to sign a message or request, and the receiving party uses the sender’s public key to verify the message or request. Prior art references show that algorithms using a public key to sign and create a digital signature had also been disclosed and were known in the art. (Ex. 1016, [0010] (“the public key may be used as a signature to verify [] identity”); Ex. 1020, 1:22-26 (“communication systems are known that additionally employ digital signing key pairs, such as a signing private key, and a signing public key, to allow the use of digital signatures so that ... data may be uniquely and securely signed by an individual”); Ex. 1021, [0016] (“The request may also be signed with the public key”); Ex. 1022, [0114] (“queries can be signed with the public key and verified with the cryptographic signature”); Ex. 1023, [0340] (“Appropriately signed means signed with the public key”)).

175. The POSITA would have understood signing with either the sender's private key or public key were two known options for generating a digital signature. The 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 the two known, finite, predictable solutions.

10. Claim 11

176. Claim 11 depends from claim 10, reciting "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."

177. Kennedy, combined with Kurani-816, renders obvious this claim. As explained for claim 10, Kennedy and Kurani-816 disclose verification via private/public key pairs, and teach various methods for storing and associating these keys with the transaction. From these disclosures, the POSITA would have understood that public keys associated with particular users or entities would be saved to a transaction to the blockchain record. It would have been obvious to the 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.

11. Claim 12

178. Claim 12 depends from claim 1, reciting “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.”

179. Kennedy, combined with Kurani-816, renders obvious this claim. The POSITA would have understood that this claim recites an obvious reversal of the steps in claim 8 (*i.e.*, the second intermediary server sends a request, and the first intermediary

server sends a response). For the reasons explained for claim 8, these elements would have been obvious to the POSITA.

12. Claim 13

180. Claim 13 depends from claim 12, reciting “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.”

181. As I explained for claim 12, the POSITA would have understood that claim 12 recites a duplication of the steps in claim 8, except the flow of information is reversed. The additional steps recited in claim 13 are the same as recited in claim 9, which depends from claim 8. Kennedy, combined with Kurani-816, renders obvious claim 13 for the reasons explained for claims 9 and 12.

13. Claim 14

182. Claim 14 depends from claim 12, reciting “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.”

183. As I explained for claim 12, the POSITA would have understood claim 12 simply recites a reversal of the steps recited above in claim 8. The additional steps recited in claim 14 are the same as the steps recited in claim 10, which depends upon claim 8. Kennedy, combined with Kurani-816, discloses or renders obvious claim 14 for the reasons explained claims 10 and 12.

14. Claim 15

a) Preamble: A system for processing a financial transaction:

184. I have been asked to assume the preamble is a limitation of claim 15. Under that assumption, it is my opinion that Kennedy discloses the preamble for the reasons explained for claim 1’s preamble. Kennedy discloses “systems and methods for validating blockchain transactions using a transaction processing network.” (Ex. 1033, [0004], [0020], Fig. 1). Kennedy’s “blockchain transactions” in are financial, including “product or service purchases, credit purchases, debit transactions, fund transfers, account withdrawals, etc.” (Ex. 1033, [0017]). Kennedy discloses the preamble.

- b) 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;**

185. The Kennedy/Kurani-816 combination renders obvious this element for the reasons explained for element 1 of claim 1. 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, shown below, includes “processing server 102..., [which] may be configured to assist in the validation of both electronic payment transactions processed using a payment network 106 [blue] and blockchain transactions associated with a blockchain network 114.” (Ex. 1033, [0019]).

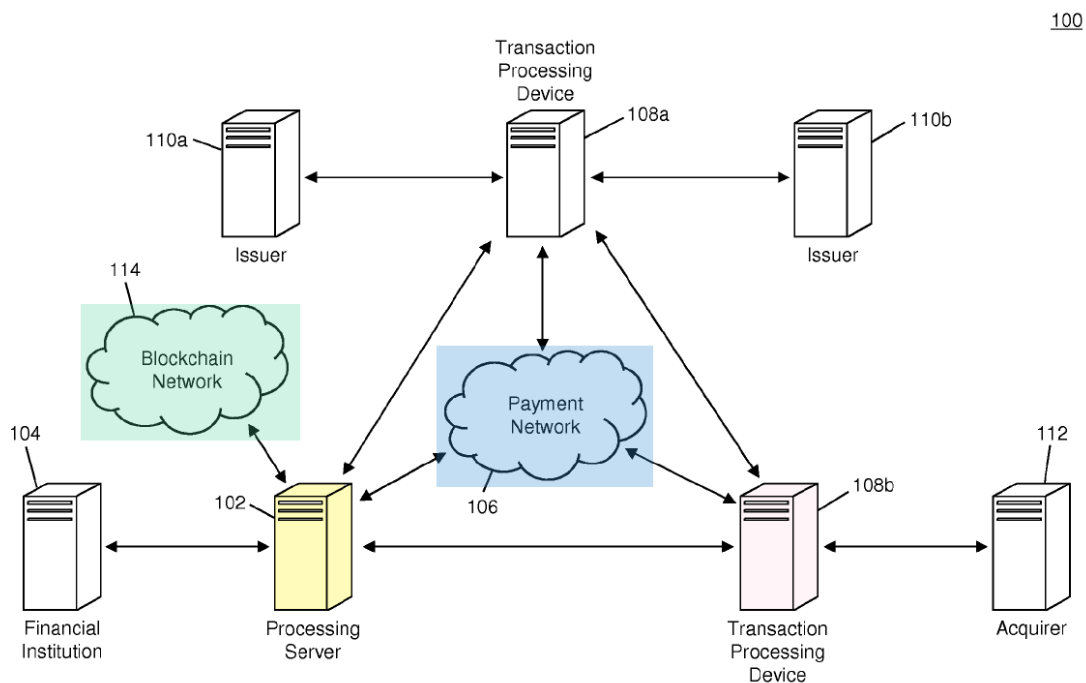


FIG. 1

186. The POSITA would have understood that the “processing server” (*i.e.*, “first intermediary server”) is “operably connected to a network,” as claimed. As explained for element 1 of claim 1, the POSITA would have further understood that the processing server, which is capable of reading and writing to memory, is “operably connected” to the “first document store.”

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

187. The Kennedy/Kurani-816 combination renders obvious this element for the reasons explained for element 3 of claim 1. (Ex. 1034, Fig. 1 (depicting Digital Title Company 106 operably connected to a central payment network)).

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

188. The Kennedy/Kurani-816 combination renders obvious this element for the reasons explained for element 2 of claim 1. (Ex. 1033, Fig. 1 (depicting Blockchain Network 114 operably connected to the Payment Network 106 via the processing server)).

e) 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;

189. The Kennedy/Kurani-816 combination renders obvious this element for the reasons explained for element 1 of claim 1.

- f) 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;**

190. The Kennedy/Kurani-816 combination renders obvious this element for the reasons explained for element 2 of claim 1.

- g) 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**

191. The Kennedy/Kurani-816 combination renders obvious this element for the reasons explained for element 3 of claim 1.

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

192. The Kennedy/Kurani-816 combination renders obvious this element for the reasons explained for element 6 of claim 1.

- i) 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**

193. The Kennedy/Kurani-816 combination renders obvious this element for the reasons explained for element 4 of claim 1.

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

194. The Kennedy/Kurani-816 combination renders obvious this element for the reasons explained for element 5 of claim 1. It is my opinion that claim 15 would have been obvious over the Kennedy/Kurani-816 combination.

15. Claim 16

195. As I explain below, the combination of Kennedy and Kurani-816 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 is configured to add the token to the blockchain, which is required in claims 1 and 15.

- a) **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:**

196. I have been asked to assume the preamble is a limitation of claim 16. Under that assumption, it is my opinion that the Kennedy/Kurani-816 combination renders it obvious for the reasons explained for element 1 of claims 1 and 15.

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

197. The Kennedy/Kurani-816 combination renders obvious this element for the reasons explained for element 1 of claim 1.

- c) **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;**

198. The Kennedy/Kurani-816 combination renders obvious this element for the reasons explained for element 2 of claim 1.

- d) **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**

199. The Kennedy/Kurani-816 combination renders obvious this element for the reasons explained for element 3 of claim 1.

- e) **Element 4: transmit the token to the first document store.**

200. The Kennedy/Kurani-816 combination renders obvious this element for the reasons explained for element 6 of claim 1. It is my opinion that claim 16 would have been obvious over the Kennedy/Kurani-816 combination.

16. Claim 17

201. Claim 17 depends from claim 16, reciting the first intermediary server is “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.” The Kennedy/Kurani-816 combination discloses or renders obvious this claim for the reasons explained for claims 2 and 16.

17. Claim 18

202. Claim 18 depends from claim 16, reciting the first intermediary server is “further configured to transmit the token to a first digital device.” The Kennedy/Kurani-816 combination discloses or renders obvious this claim for the reasons explained for claims 2, 4, and 16.

18. Claim 19

203. Claim 19 depends from claim 16, reciting the first intermediary server is “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.” This claim contains a subset of the elements recited in claim 8 regarding steps taken by the first intermediary server. The Kennedy/Kurani-816 combination discloses or renders obvious this claim for the reasons explained for claims 8 and 16.

19. Claim 20

204. Claim 20 depends from claim 19, reciting “the one or more first responses comprise one or more second regulatory compliance documents pertaining to a second user.” It is my opinion that the Kennedy/Kurani-816 combination discloses or renders obvious this claim.

205. The POSITA would have understood that “regulatory compliance documents” include documents or messages containing customer identification and authentication information for the purpose of protecting against fraud. (Ex. 1001, 12:31-38). As explained for claim 8, the Kennedy/Kurani-816 combination discloses that certain institutions and servers communicate with one another via a series of requests and responses. Kennedy explains that the requests and responses exchanged between the servers 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 that will be apparent to persons having skill in the relevant art.” (Ex. 1033, [0083]). During processing, the servers may “perform value-added services for the payment transaction... specified by the issuing financial institution.” (Ex. 1033, [0081]). “Value-added services” include “fraud scoring, transaction or account controls, account number mapping....” (Ex. 1033, [0081]).

206. The POSITA would understand that Kennedy’s value-added services, including “fraud scoring,” protect financial institutions against fraud and involve steps to establish customer identity and qualify that the source of funds are legitimate. The POSITA would have further recognized that KYC processes were commonly used to verify customer identity and reduce fraud. (Ex. 1035, [0008], [0012], [0052] (disclosing “us[ing] 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 the POSITA’s knowledge of the practice of performing KYC checks, is consistent with and renders obvious the exchange of KYC or “regulatory compliance” documents.

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

1. Claim 3

207. Claim 3 depends from claim 1, reciting “implementing a smart contract at the token server; and adding the smart contract into the blockchain, from the token server.” It is my opinion that the Kennedy/Kurani-816 combination in view of Yago renders obvious this claim.

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

209. Yago discloses “implementing a smart contract,” as claimed. 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]). The POSITA would have

understood that Yago’s contract is a “smart contract.” (Ex. 1013, 1 (“Another important area of inquiry is ‘smart contracts’ – systems which automatically move digital assets according to arbitrary pre-specified rules”); Ex. 1014 (defining smart contracts as “systems which automatically move digital assets according to arbitrary pre-specified rules.”)).

210. It would have been obvious to the POSITA to apply Yago’s “payment assured contract” to the Kennedy/Kurani-816 combination. Like Yago, both Kennedy and Kurani-816 seek to address similar problems of security risks and fraud. Yago describes “a need for a method that describes automatically issued digital contracts that may be automatically enforced, resulting in reduced fraud and counter-party risk when dealing with all different types of CDFI [Crypto-Digital Financial Instruments].” (Ex. 1011, [0006]). Kennedy identifies a desire to “further increase the sophistication of [transaction processing] networks, to provide for even more security to protect against fraud and to provide peace of mind to consumers.” (Ex. 1033, [0002]). Kurani-816 similarly describes a desire to identify “potential fraudulent transaction[s]” on its MBC blockchain. (Ex. 1034, 10:9-15, 7:33-36). Moreover, Kennedy and Yago both describe systems directed to the settlement of financial transactions. (Ex. 1033, [0024], [0064]; Ex. 1011, [0005] (“[T]here is a need for a monetary system for providing a method of settlement between buyes and sellers of CDFI.”)). Thus, it would have been obvious to the POSITA to apply Yago’s “payment assured contract” to the Kennedy/Kurani-816

combination to improve increase security and reduce fraud in the context of settlement and other processing of financial transactions.

211. The POSITA would have had a reasonable expectation of success when applying Yago's concepts to the Kennedy/Kurani-816 combination. Before August 2015, using smart contracts in blockchain systems was well-known and understood by the POSITA. In fact, the idea of blockchain-based smart contracts had been contemplated in the art since blockchain's beginnings. (Ex. 1012, 29 ("the possibilities for programmable ... contracts were baked into the [Bitcoin] protocol at its invention.")). Thus, applying the teachings of Yago to the Kennedy/Kurani-816 combination would have involved the combination of well-understood technologies that would have led to obvious results.

212. 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." Yago seeks to enable "automated and scalable settlement protocols" including "digital contracts that may be automatically enforced." (Ex. 1011, [0006]). To do so, Yago discloses a "software/computer/firmware module that creates and applies contract/credit certificates with verifiable and objective terms based on a trade request between two or more parties." (Ex. 1011, [0007]). Yago's module is "adapted to monitor crypto-digital

instrument networks [(i.e., a blockchain)] to verify performance of the expected terms.” (Ex. 1011, [0007]).

213. Yago explains that “the contracts and certificates may be issued on the public ledgers of the CDI systems.” (Ex. 1011, [0054]). More specifically, Yago discloses a “transaction system 412 comprising a plurality of modules” configured to transfer the digital certificate or contract to a public ledger, for example, by “writ[ing] the first certificate 504 to the public ledger,” and to “monitor the public ledger 406 for the transactions specified in the digital certificate 504 and/or the digital contract 130.” (Ex. 1011, [0058], [0066], [0068], Fig. 4). After payment has been completed, the proof of payment module of transaction system 412 “records the completion of the transaction onto the public ledger 406.” (Ex. 1011, [0067]). Proof of payment can be recorded on the public ledger “as either a message or a contract.” (Ex. 1011, [0052], [0054]). As such, the “payment assured contracts” (*i.e.*, “smart contracts”) are implemented at the transaction system 412 and added to the public ledger (*i.e.*, “blockchain”) by the transaction system 412.

214. The POSITA would have understood that Yago’s “transaction system” is like the “digital title company 106” (*i.e.*, “token server”) of the Kennedy/Kurani-816 combination because it is a central server not affiliated with any party to the smart contract. (Ex. 1011, [0065]). Accordingly, the POSITA would have found it obvious

that, within the context of the combination described above, Yago's smart contract would have been implemented at, and added to the blockchain by, the token server.

215. It is therefore my opinion that claim 3 would have been obvious over the combination of Kennedy, Kurani-816, and Yago.

VIII. CONCLUSION

216. For the foregoing reasons, it is my opinion that claims 1-20 of the '413 Patent are invalid as obvious over the combinations of references described above.