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 10
A. Distributed Systems And Blockchain 11
B. Tokens 15
C. Smart Contracts 16
D. Cryptography 17
E. Know-Your-Customer ("KYC") 20
F. Description Of The Alleged Invention 21
G. Person Of Ordinary Skill In The Art 23
V. THE CHALLENGED CLAIMS ARE UNPATENTABLE 24
A. Brief Overview Of The Prior Art 24
1. Smith 24
2. Seger 27
3. Kurani-274 29
4. Yago 30
B. Ground 1: Claims 1-2, And 5-20 Would Have Been Obvious Over Smith In View Of Seger 31
1. Claim 1 31
2. Claim 2 60
3. Claim 5 62
4. Claim 6 65
5. Claim 7 68
6. Claim 8 69
7. Claim 9 78
8. Claim 10 79
9. Claim 11 83
10. Claim 12 84
11. Claim 13 85
12. Claim 14 86
13. Claim 15 87

TABLE OF CONTENTS
(continued)

14. Claim 16 91
15. Claim 17 93
16. Claim 18 93
17. Claim 19 94
18. Claim 20 94

C. Ground 2: Claim 3 Would Have Been Obvious Over Smith And Seger, And Further In View Of Yago. 96

1. Claim 3 96

D. Ground 3: Claim 4 Would Have Been Obvious Over Smith In View Of Seger, And Further In View Of Kurani-274. 100

1. Claim 4 100

VI. 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 first 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)
- The prosecution history of the '413 Patent (Ex. 1002)
- U.S. Patent Pub. No. 2015/0081553 ("Smith") (Ex. 1004)
- U.S. Patent No. 9,397,985 ("Seger") (Ex. 1005)
- Microsoft Computer Dictionary (Ex. 1006)
- U.S. Patent No. 11,270,274 ("Kurani-274") (Ex. 1007)
- Everett Rosenfeld, "Forget currency, bitcoin's tech is the revolution." (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." (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. 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)
- Tannenbaum, "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 Pub. No. 9,892,460 ("Winklevoss") (Ex. 1040)
- William Stallings, Cryptography and Network Security (4th Ed.) ("Stallings") (2006) (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)

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 computer scientist and professor 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 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.

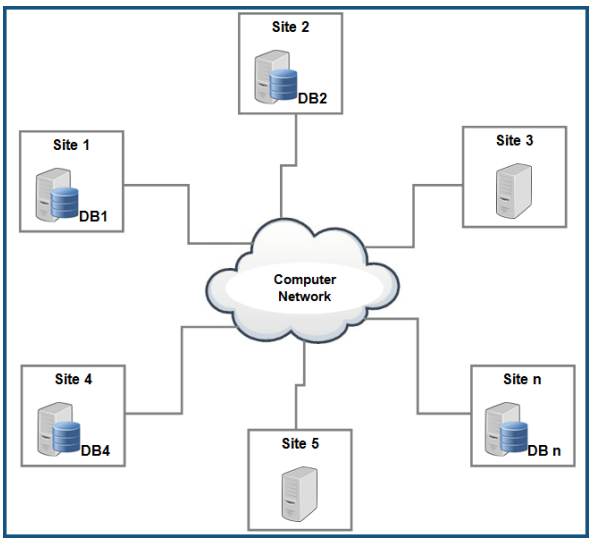
IV. TECHNOLOGY BACKGROUND

21. 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), 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

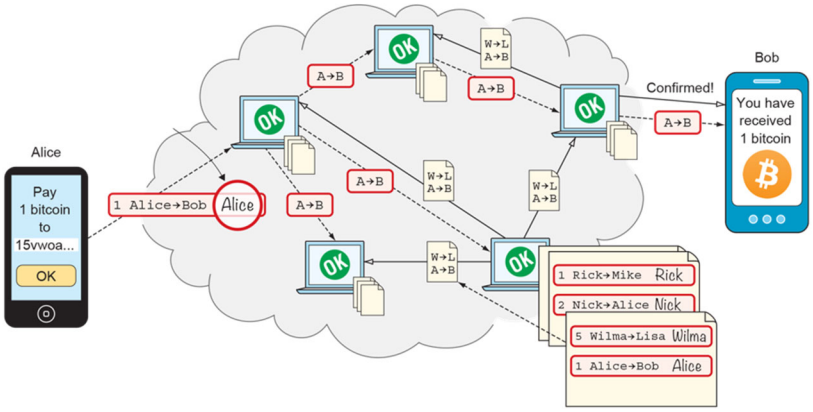
22. Distributed systems have been utilized in the art for decades. Generally, a "distributed system" is a "collection of independent computers that appears to its users as a single coherent system." (Ex. 1037, 21). Thus, a basic distributed system "consists of components (i.e., computers) that are autonomous" 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).

23. 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:



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

25. 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").



26. 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).

27. 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).

28. 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).

29. 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).

30. 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

31. 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 a system.

32. 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 (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

33. 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.")).

34. 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).

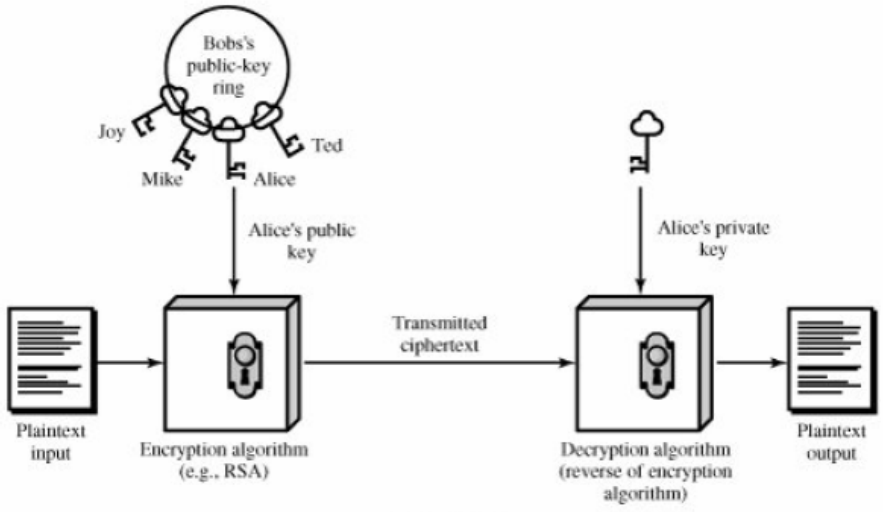
D. Cryptography

35. 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).

36. 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).

37. 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, 261).

38. 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 .

39. 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")

40. 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).

41. 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).

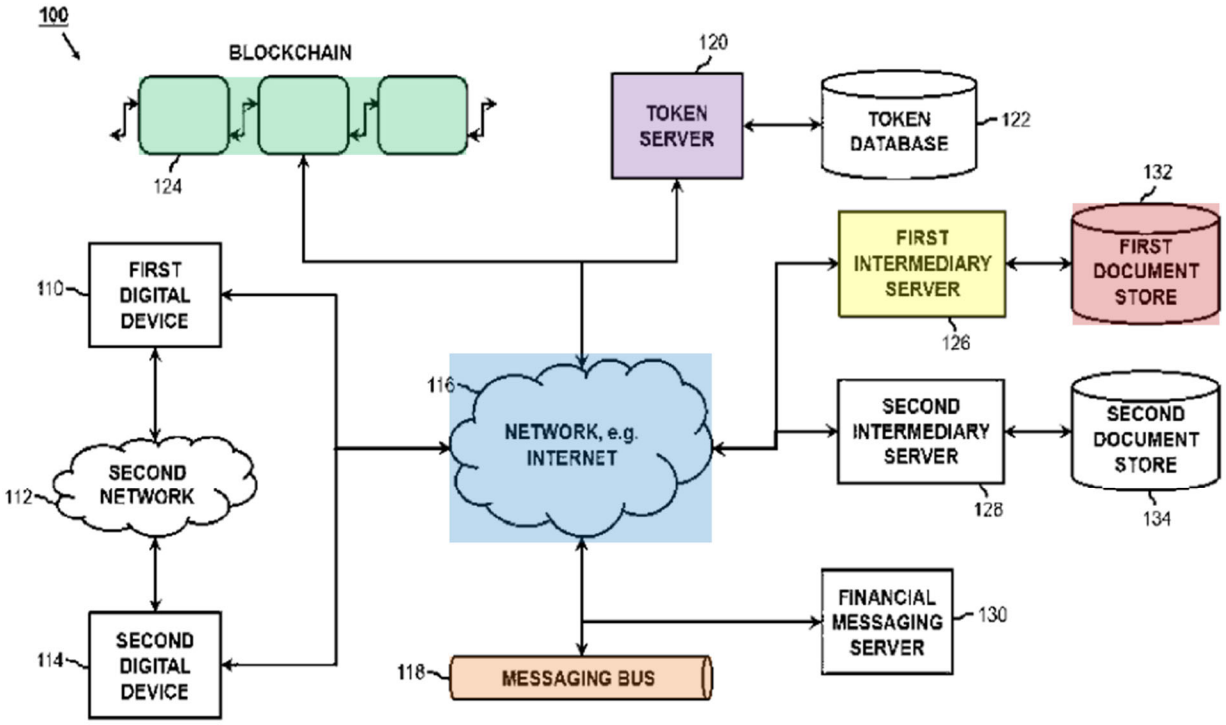
F. Description Of The Alleged Invention

42. 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).

43. 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."*** [1] (Ex. 1001, 24:21-23).

44. 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).

45. The "first intermediary server" transmits "one or more documents pertaining to [a] financial transaction" to the "first document store." (Ex. 1001, 18:20-

[1] Emphasis added unless noted otherwise.

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).

G. Person Of Ordinary Skill In The Art

46. It is my opinion that a person of ordinary skill in the art ("POSITA") at the time of the '413 Patent would have at least a bachelor's degree in computer science, computer engineering, applied mathematics, or equivalent and at least 2 years of experience researching, implementing, programming, or designing computer networks, distributed systems, blockchain technology, applied cryptography, or security. Additional education can supplement practical experience, and vice versa.

V. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Brief Overview Of The Prior Art

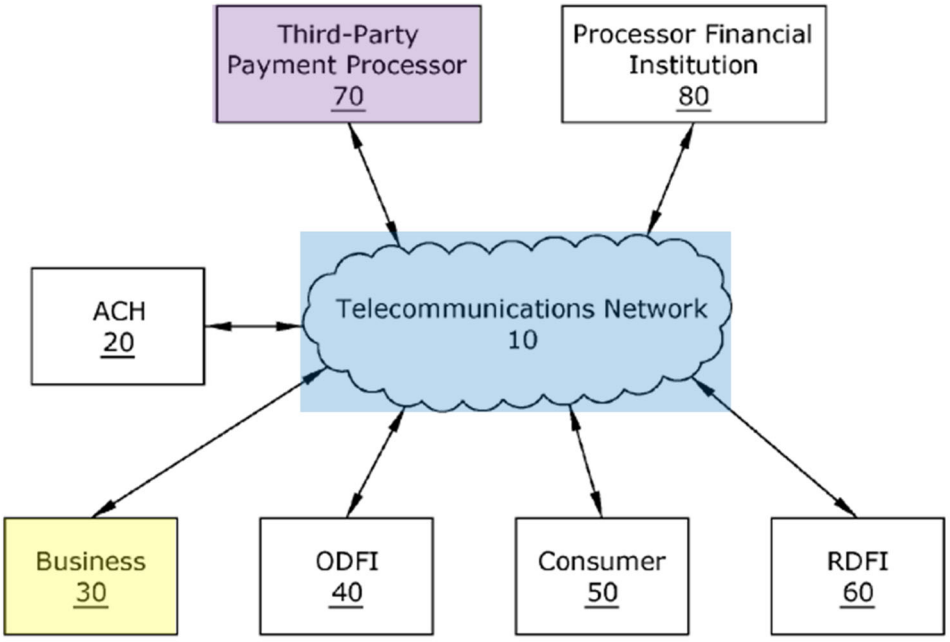
1. Smith

47. Smith (Ex. 1004), entitled "Electronic Funds Transfer Consumer Authorization Verification System," was filed on September 17, 2014 and published on March 19, 2015. (Ex. 1004, cover). I understand that Smith is prior art to the '413 Patent.

48. Smith describes "an electronic funds transfer consumer authorization verification system for efficiently proving that a consumer authorized a financial transaction via an ACH network." (Ex. 1004, [0004]). Smith explains that in traditional ACH (automated clearing house) systems, "the business is unable to attach the consumer's authorization to the ACH transaction thereby inherently creating a risk for the business that the ACH transaction will be returned because the consumer (or another party) disputes that it was authorized." (Ex. 1004, [0013]). Proving such authorization "is time consuming and labor intensive." (Ex. 1004, [0013]). In traditional ACH transactions there is also "no verification system to determine if the business is authorized to do business in the consumer's state thereby exposing the business and the third party processor to unnecessary returns." (Ex. 1004, [0013]). Accordingly, Smith

teaches an "improved … system for efficiently proving that a consumer authorized a financial transaction via an ACH network." (Ex. 1004, [0014]).

49. Smith teaches "accepting by a business 30 an authorization from a consumer 50 to debit and/or credit the consumer's financial account in a specified amount via an ACH network, communicating the ACH detailed record for the ACH transaction along with a transaction data file from the business 30 to a third-party payment processor 70, and communicating to the business 30 a unique transaction key associated with both the ACH detailed record and the transaction data file." (Ex. 1004, [0030]). An example of Smith's system is shown in Figure 1:



(Ex. 1004, Fig. 1).

50. To implement the process described above, Smith discloses that "a plurality of electronic devices" including "devices for each entity" (such as "business 30," "consumer 50," and "third-party payment processor 70") "may communicate via a single telecommunication network 10." (Ex. 1004, [0031]). This network (blue above) allows the business (yellow above) to "send[] one or more transaction data files to the third-party payment processor" (purple above). (Ex. 1004, [0052]). After receiving such data files, "the third-party payment processor 70 then updates its database to include a unique transaction key that is associated with the transaction data file(s) provided by the business 30." (Ex. 1004, [0053]).

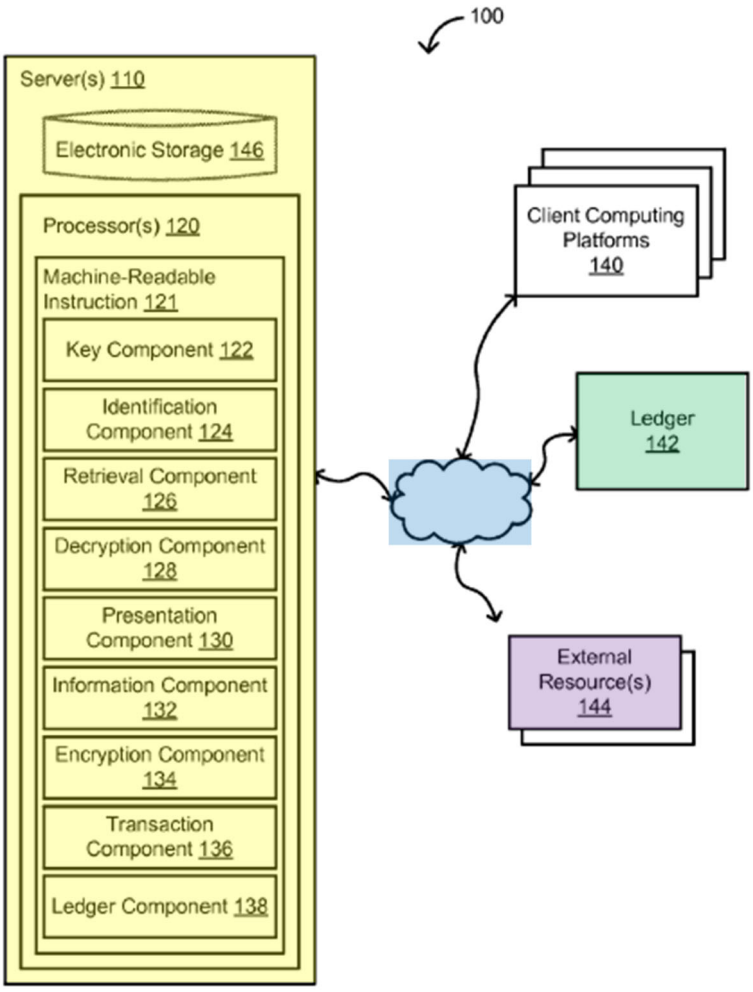
51. In this way, "the business 30 and/or third-party payment processor 70 can easily identify and view the transaction data files associated with the ACH transaction using the transaction key." (Ex. 1004, [0056]). Additionally, "[t]he ACH transaction can then be verified (or not verified) based upon the transaction data files without the business 30 (or the third-party payment processor 70) having to gather and fax the transaction data files." (Ex. 1004, [0056]).

2. Seger

52. Seger (Ex. 1005), entitled "System And Method For Providing A Cryptographic Platform For Exchanging Information," was filed on April 14, 2015. (Ex. 1005, cover). I understand that Seger is prior art to the '413 Patent.

53. Seger provides "a cryptographic platform for exchanging information" that "enables confidential, verifiable, and immutable recording and/or reporting of information transactions." (Ex. 1005, 1:7-8, 1:43-44). Seger notes that "[t]he transmission of an encrypted communication is generally private and not recorded in a log that can be audited after the fact by a third party." (Ex. 1005, 1:19-21). Seger thus provides a system that "enable[s] one or more auditors to audit the information transactions held within [a] distributed ledger." (Ex. 1005, 7:10-12).

54. In Figure 1, Seger shows "one or more servers 110" (yellow) that "communicate with client computing platform(s) 140 according to a client/server architecture." (Ex. 1005, 4:31-33). Seger teaches a distributed ledger (green above) to "provide a verifiable record of various information transactions, including various information payloads that include various encrypted information that is encrypted with various public keys." (Ex. 1005, at 4:22-26). The "information may include and/or be associated with one or more of know your customer (KYC) data; anti-money laundering (AML) data; and/or other financial data." (Ex. 1005, at 6:8-11).



(Ex. 1005, Fig. 1).

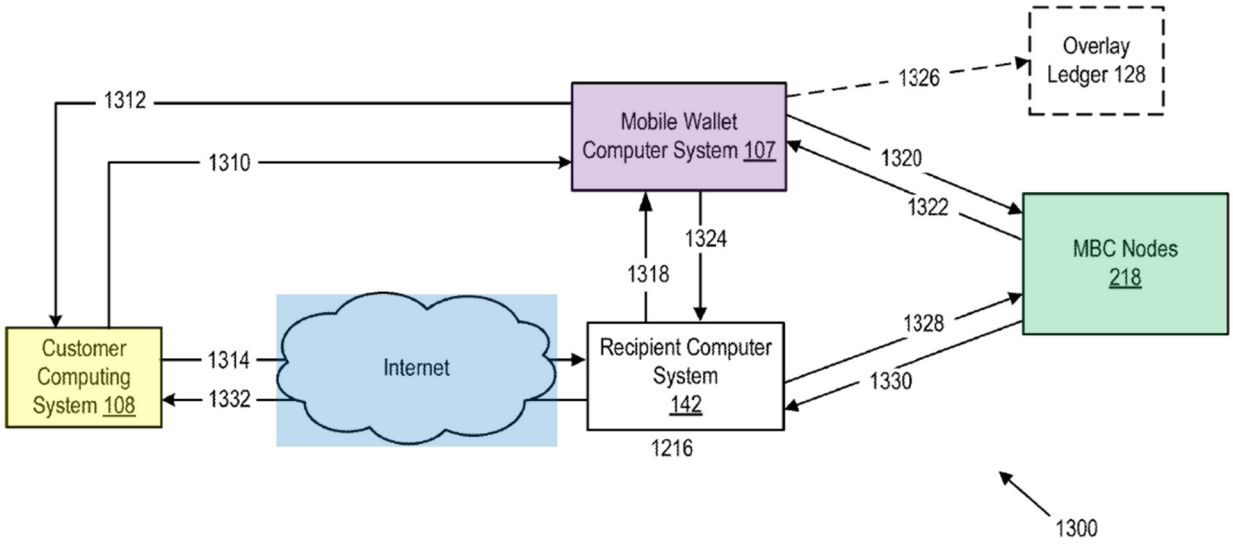
55. Seger explains that "a record of all instances of the distributed ledger (e.g., a ledger chain, a ***blockchain***) may be generated to provide a verifiable record of all instances of the distributed ledger." (Ex. 1005, 10:23-26). Seger thus "enables confidential, verifiable, and immutable recording and/or reporting of information transactions including various encrypted information (e.g., private communications) that may be audited by a third party." (Ex. 1005, 1:43-46).

3. Kurani-274

56. Kurani-274 (Ex. 1007), entitled "Mobile Wallet Using Math Based Currency Systems And Methods" was filed on July 3, 2014. (Ex. 1007, cover). I understand that Kurani-274 is prior art to the '413 Patent.

57. Kurani-274 discloses "banking systems and methods for a mobile wallet system implemented using math-based currency ("MBC")." (Ex. 1007, 2:66-3:1). MBC is "commonly referred to as cryptocurrency" and "allows holders of MBC units to utilize advantageous banking services … in the context of a mobile wallet platform." (Ex. 1007, 1:17-18, 3:2-6). Kurani-274 discloses that a "mobile wallet computer system 107 includes a code/token generator 131" (Ex. 1007, 5:45-46).

58. Kurani-274 describes "code/token generator" that "generates a code that is uniquely associated with the transaction." (Ex. 1007, 6:21-23). In Figure 13, the code/token generator "receiv[es] a message from the customer computing system 108 to generate a token." (Ex. 1007, 21:28-29). The system incorporating the token server (purple) also communicates with MBC Nodes 218 (green) that publish transaction information "in a chain of transactions (i.e., a ***blockchain***)." (Ex. 1007, 17:18-19). This allows transaction verification "via the MBC nodes 218." (Ex. 1007, 21:17-18, 51-52).



(Ex. 1007, Fig. 13).

4. Yago

59. 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. (Ex. 1011, cover). I understand Yago is prior art to the '413 Patent.

60. 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 also adds the contract is to a "CDI network" (i.e., "a

blockchain"). (Ex. 1011, [0054], [0042]). A "payment issuer will be able to objectively (and automatically), confirm performance by the seller, by either directly monitoring the CDI network or receiving a data feed from a trusted third-party." (Ex. 1011, [0047]).

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

1. Claim 1

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

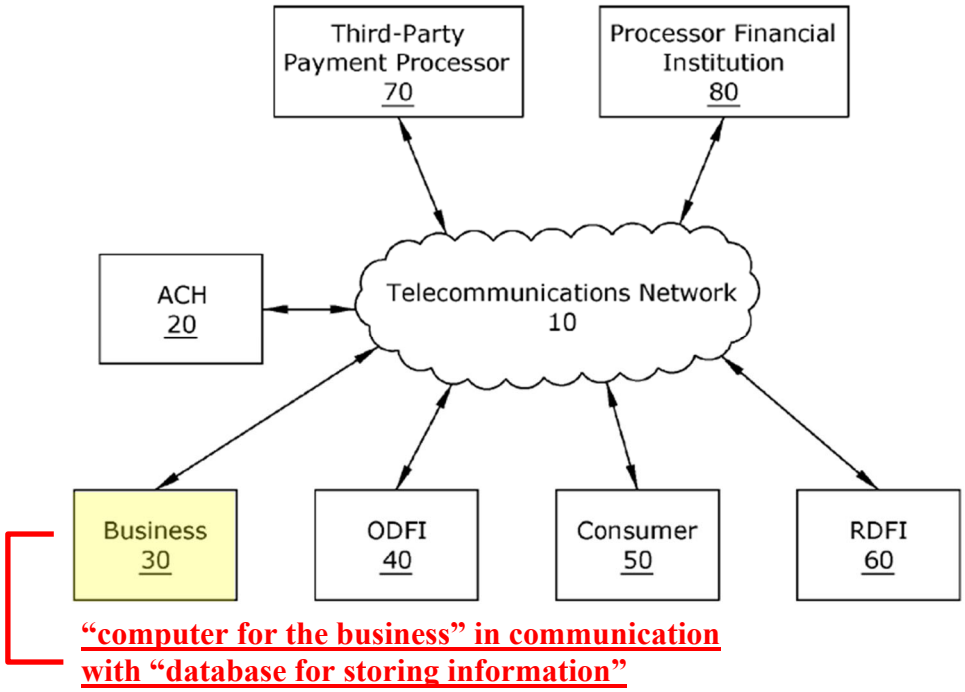
61. I have been asked to assume the preamble of claim 1 is a limitation. It is my opinion that Smith discloses the preamble. Smith describes "an electronic funds transfer consumer authorization verification system for efficiently proving that a consumer authorized a financial transaction via an ACH network." (Ex. 1004, [0004]). Smith thus discloses a method "for processing a financial transaction."

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;

62. It is my opinion that Smith, alone or in combination with Seger, discloses or renders this element obvious.

63. Smith describes an "electronic funds transfer consumer authorization verification system" (*i.e.*, "centralised financial system"). (Ex. 1004, [0030]). Smith's

system includes "a computer for the business 30" (hereinafter, "business computer 30") (*i.e.*, "first intermediary server") connected with other entities and in communication with "a database that stores [] information for later access." (Ex. 1004, [0031], [0034]).



(Ex. 1004, Fig. 1).

64. *First*, Smith discloses a "first intermediary server in a centralised financial system." Smith describes an "electronic funds transfer consumer authorization verification system" (*i.e.*, a "centralised financial system"). (Ex. 1004, [0030]). In Figure 1, Smith shows the business computer 30, "a computer for the consumer 50," "a computer for the automated clearing house 20 (ACH), and a computer for the third-party payment processor (TPPP) 70" that "communicate with one another" "via a single

telecommunication network 10 or multiple telecommunication networks 10 concurrently." (Ex. 1004, [0031]).

65. The POSITA would have considered it obvious for Smith's business computer 30 to be a server. The POSITA further would have understood that a server is "a computer or program that responds to commands from a client." (Ex. 1006 (defining "server")). In a typical client-server paradigm, a server (computer) provides a service or a function that can be requested or accessed by a client (computer) via a communication network.

66. Smith explains the computer for the business 30 ("business computer 30") "is comprised of an electronic device capable of receiving, transmitting and storing electronic data." (Ex. 1004, [0036]). The business computer 30 "receives the authorization for the ACH transaction and other required information from the customer 50" and "provide[s]" to TPPP "one or more transaction data files." (Ex. 1004, [0048], [0047]). Smith teaches that the various devices (e.g., business computer 30) "can be implemented by special-purpose, hardware-based computer systems that perform the specified functions … or combinations of special-purpose hardware and computer instructions." (Ex. 1004, [0084]). This aligns with the '413 Patent's statement that a "computing device" may "take[] the form of the first intermediary server." (Ex. 1001, 16:43-44).

67. The POSITA would have understood that business computer 30 is therefore a server that receives authorization and other information from the consumer and through computer instructions subsequently creates and transmits transaction data files to the TPPP. Here, the business computer is also an "intermediary" between other devices, or a user on the business side and the authorization verification system. Accordingly, the POSITA would have understood Smith's business computer 30 as comprising "a first intermediary server in a centralised financial system."

68. In my opinion, the combination of Smith and Seger further renders obvious to a POSITA that business computer 30 comprises a "first intermediary server." Seger teaches "one or more servers 110" accessing a "system 100 configured for providing a cryptographic platform for exchanging information". (Ex. 1005, 4:7-8, 4:31). Seger explains that servers "communicate with client computing platform(s) 140 according to a client/server architecture." (Ex. 1005, 4:32-34). For example, Seger discloses that system server 301 obtains "information" from a party, and using "one or more processors configured to execute a transaction component," "generate[s]" an "information transaction." (Ex. 1005, 13:38-39, 14:37-38, 14:48-58). System 301 then "provide[s]" the "information transaction" to the distributed ledger 302. (Ex. 1005, 14:58-61).

69. In view of Seger's teachings, it would have been obvious to the POSITA to implement Smith's business computer as a server, using a client/server architecture, to receive information from other entities in Smith's "telecommunications network" and generate transaction information for transmittal and storage on Seger's "distributed ledger" providing various advantages explained below for element 2. Client/server architectures were well-known before the August 14, 2015 timeframe, and the POSITA would have understood that using Seger's teachings with Smith's system would be accomplished by known methods, yielding predictable results with no change in the components' respective functions. Accordingly, the POSITA would have found it obvious, in view of Seger, that Smith's business computer connects to the electronic funds consumer authorization verification system via a "first intermediary server."

70. *Second*, Smith discloses "a first document store." Smith explains that during a financial transaction between a consumer and a business, "[t]he business 30 enters the information received from the consumer 50 into a database that stores the information for later access." (Ex. 1004, [0034]). The "database that stores the information for later access" is the claimed "first document store." This aligns with the '413 Patent's statements that a "document store" "represent[s] databases configured to store a plurality of documents." (Ex. 1001, 11:9-11).

71. *Third*, Smith discloses "one or more documents pertaining to the financial transaction." Smith teaches that information entered into the business computer's database includes financial transaction data such as "the legal name of the consumer 50, state of residency, residential address, amount of the credit or debit, a maximum amount for the credit or debit, a routing number for the financial institution …, a checking/savings account number at the financial institution for the consumer 50 …, copy of driver's license, copy of Social Security card, picture taken of the consumer 50 by the business 30 and the like." (Ex. 1004, [0034]). The business computer 30 (*i.e.*, "first intermediary server") is also "utilized by the business to store … fund transfer information, payment information, purchase information, ACH payment information, ACH authorization" and more. (Ex. 1004, [0036]). Other examples of information provided by the consumer to the business computer in Smith include "a complete ACH authorization agreement signed by the consumer 50, a statement by the consumer 50 authorizing the ACH transaction," and "various other types of documents desirable for verifying a transaction." (Ex. 1004, [0051]). The POSITA would have understood this information provided by the consumer to the business computer constitutes "one or more documents pertaining to the financial transaction."

72. The POSITA would have understood that this information would have been aggregated together as "one or more documents pertaining to the financial

transaction" for entry into the database. It is my opinion that a POSITA would understand "one or more documents" as referring, generally, to records of the transaction that can be retrieved by a user. These need not take on any specific form or be stored in any specific manner to represent "one or more documents" as claimed.

73. *Finally*, Smith discloses "transmitting one or more documents" from the "first intermediary server … to the first document store. The business computer 30 comprises or would have rendered obvious (in view of Seger) "a first intermediary server" that is "capable of receiving, transmitting and storing electronic data." (Ex. 1004 at [0036]. When the consumer "provides various … information required by the business" to execute a transaction (Ex. 1004, [0034]), that information (i.e. "one or more documents") is provided to the business computer 30. By "enter[ing] the information received from the consumer 50 into a database" (Ex. 1004, [0034]), the business computer 30 (i.e., "first intermediary server") transmits the received information (i.e. "one or more documents") to the database (i.e. "first document store") for storage.

74. It is my opinion that the "entering" or "storing" this information into a database, constitutes a transmission of the information. The process of "entering" or "storing" would have required writing that information to computer memory and/or permanent storage like hard disks. Whether the database is stored locally, or externally, signals must be propagated in order to write the transaction information into memory

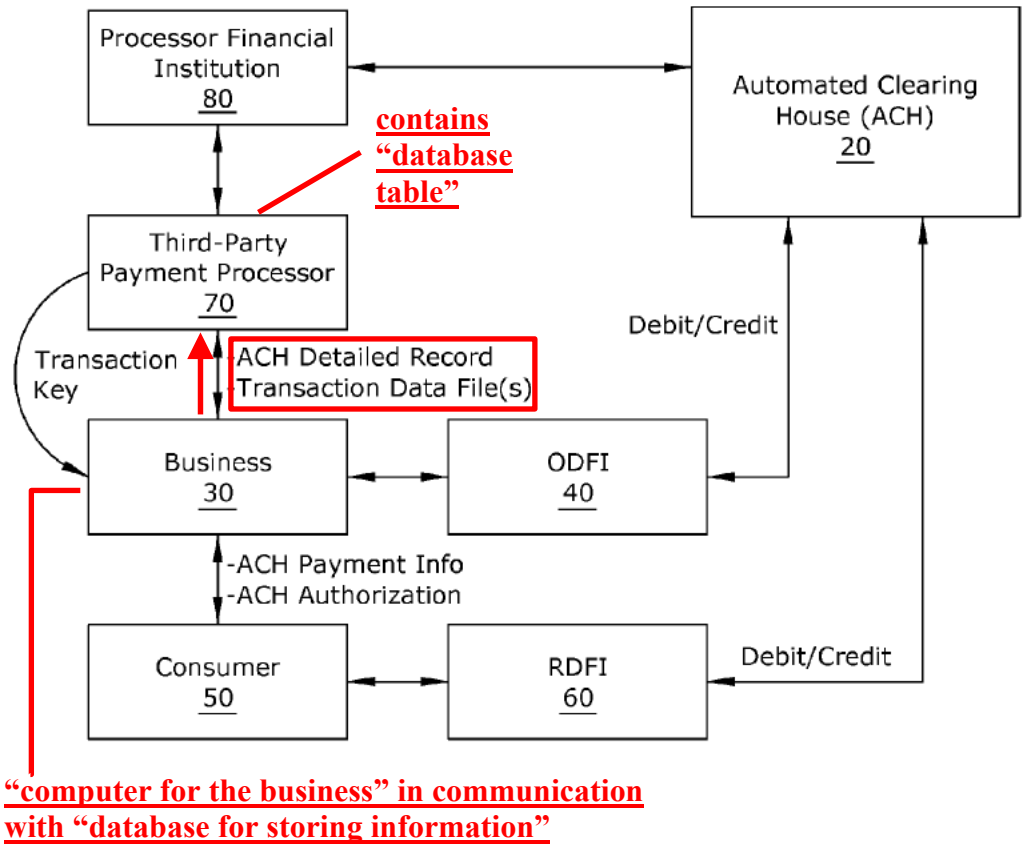
and/or permanent storage like hard disks. Thus, it is my opinion that the POSITA would have understood this as the transaction information being "transmitted" to the first document store as claimed.

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

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;

76. It is my opinion that the combination of Smith and Seger would have rendered this element obvious.

77. *First*, Smith discloses "generating an enriched data record from the one or more documents." Smith teaches "communicating [an] ACH detailed record for the ACH transaction along with a transaction data file from the business 30 to a third-party payment processor 70." (Ex. 1004. at [0030]).



(Ex. 1004, Fig. 2). As explained below, the POSITA would have understood that, individually and/or together, the ACH detail record and its corresponding transaction data file are "an enriched data record" of the financial transaction.

78. The '413 Patent discloses a number of exemplary enriched data records, such as, for example, "a plurality of attributes from the one or more documents." (Ex. 1001, 2:36-62). Both the transaction data file and ACH detail record comprise components of the transaction information that is stored in the business computer's database. (Ex. 1004 at [0034]-[0036], [0046]-[0047], [0051]). Smith teaches that both

the transaction information stored for later access in the business computer's database and the transaction data file may comprise a "copy of the driver's license" and "copy of the Social Security card." (Ex. 1004 at [0034], [0051]). Similarly, the stored transaction information and ACH detail record both include "ACH payment information" and other data such as the "name of the consumer" and the consumer's "account number." (Ex. 1004 at [0034]-[0036], [0046]-[0047]).

79. The POSITA would have understood both the ACH detail record and the transaction data file to be a collection of various "attributes" of the stored transaction information (*i.e.*, "one or more documents") and, as such, is generated by "combin[ing] a plurality of attributes" of the one or more documents. The POSITA would have then understood the ACH detail record and its corresponding transaction data file individually and/or together, to be "an enriched data record" of the underlying financial transaction. This aligns with '413 Patent's statement that "an enriched data record comprises … a plurality of attributes from the one or more documents." (Ex. 1001, 2:36-41).

80. *Second*, Smith discloses "adding the enriched data record into a … ledger." Smith teaches storing "the ACH transaction detail record and the corresponding transaction data files in a database on a computer for the third-party payment processor

70." (Ex. 1004, [0041]). As Smith's Figure 5 shows, this database comprises a table that keeps a record of transactions (*i.e.*, "a ledger"):

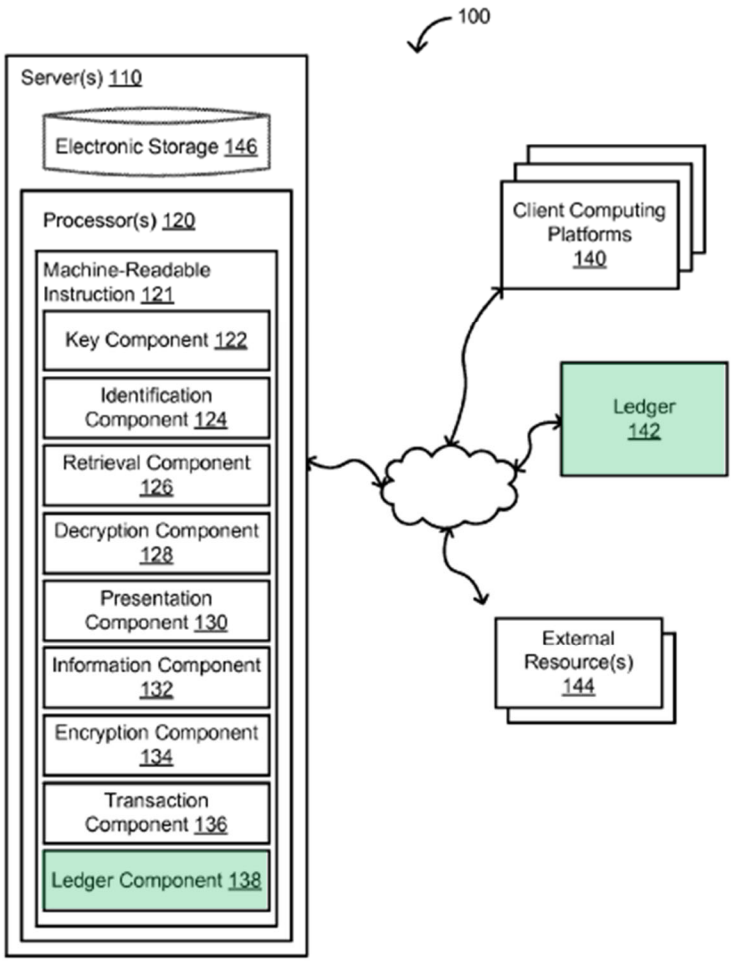
Transaction Key	ACH Transaction Detail Record	Transaction Data File(s)
ABCD1	Detail Record #1	-ACH Authorization File
ABCD2	Detail Record #2	-ACH Authorization File -Drivers License File -Social Security Card File
ABCD3	Detail Record #3	-ACH Authorization File -Business State Licenses File
ABCD4	Detail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

(Ex. 1004, Fig. 5). Figure 5 is a "database table … illustrating the connection of each ACH entry detail record with one or more consumer data files using a common transaction key." (Ex. 1004, [0022]). Smith thus discloses adding "the enriched data record" (outlined in red above) to a ledger.

81. It is my opinion that the POSITA would have understood that using a blockchain ledger is an effective way to achieve Smith's objective of providing a "verification system for efficiently proving that a consumer authorized a financial transaction via an ACH network." (Ex. 1004 at [0014]). Smith already contemplates

the need to verify transactions "based upon the transaction data files" stored in the TPPP's ledger (Ex. 1004, [0056]), but does not teach a mechanism for verifying and ensuring the continued accuracy of that ledger. To fill that gap, the POSITA would have pursued a more all-encompassing verification system and turned to Seger, which, as described below, identifies a blockchain as a means to provide a "verifiable, and immutable record[]." (Ex. 1005, 1:43-44).

82. Seger discloses adding data into a blockchain being a distributed ledger. Seger teaches that transaction information "may be provided to ledger 302 (e.g., the distributed ledger). The [transaction information] provided to ledger 302 may include the second information payload." (Ex. 1005, 14:58-61). In Figure 1, Seger shows that "intermediary servers 110" comprise a "ledger component 128 … configured to provide one or more information transactions to the distributed ledger." (Ex. 1005, 9:43-54):



(Ex. 1005, 9:43-45; Fig. 1). Seger's "distributed ledger may provide a verifiable record of all of the information exchanges including various information transactions including encrypted information," including "a record of all instances of the distributed ledger (*e.g.*, a ledger chain, a blockchain) may be generated to provide a verifiable record of all instances of the distributed ledger." (Ex. 1005, 10:20-26). Seger thus discloses "adding the enriched data record into a blockchain being a distributed ledger."

83. It would have been obvious to a POSITA to apply Seger's blockchain ledger into Smith's system. The combination would have rendered obvious the claim language reciting "adding the enriched data record into a blockchain being a distributed ledger, from the first intermediary server."

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

of the ACH transaction [entities] can easily identify and view" the transaction data. (Ex. 1004, [0041], [0056]). Thus, both Smith and Seger use transaction logs or records to verify transaction integrity. Given these similarities, a POSITA would have had a reason to combine the teachings of Seger with the teachings of Smith.

85. Here, the POSITA would have found it obvious to use a blockchain ledger as taught in Seger because it offers the advantage of providing an "immutable" record, ensuring that transaction data cannot be altered once written. Beyond immutability, the blockchain record confers a number of other advantages over traditional systems including: decentralization, tamper-proof records, increased transparency and trust, global accessibility, and auditability. The POSITA would have been aware of these benefits and found it obvious to pursue them. For example, the POSITA would have been motivated to combine Smith and Seger to include the well-known benefit of a blockchain that allows entities to verify the TPPP's transaction information against an immutable record, thereby enabling quick detection of any data alterations and providing the specific benefit of ensured integrity and accuracy of the system data if the TPPP were compromised.

86. *Second*, before the August 14, 2015 time frame, the POSITA would have understood that using distributed ledgers and blockchain for recordkeeping to be conventional. (Ex. 1008 at 2 ("proponents [of blockchain] say it is the most secure

record-keeping technology ever devised")); Ex. 1009 at 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 at 29-37 (describing a number of companies using permissioned distributed ledgers for record-keeping)). After the publication of the 2008 Bitcoin paper, those skilled in the art realized that blockchain technology's ability to establish trust in a decentralized and transparent manner may have applications beyond digital currency. Before the August 14, 2015 time frame, skilled artisans had already begun exploring these applications, including using blockchain technology in areas such as supply chain management, electronic health records (EHR), real estate management, energy trading, food safety, intellectual property and copyrights, and more. Thus, the application of a blockchain to Smith's system would have been obvious because doing so is nothing more than the predictable use of prior-art elements—Smith's system and using blockchain for recordkeeping—according to their established functions. The POSITA also would have had a reasonable expectation of success in adding blockchain to Smith's system. Seger describes multiple examples of blockchain ledgers that can "provide a verified record" of the system's transactions, including "one or more of the Ripple® Protocol, the 'mining' proof of work protocol implemented by Bitcoin and/or other public consensus protocols." (Ex.

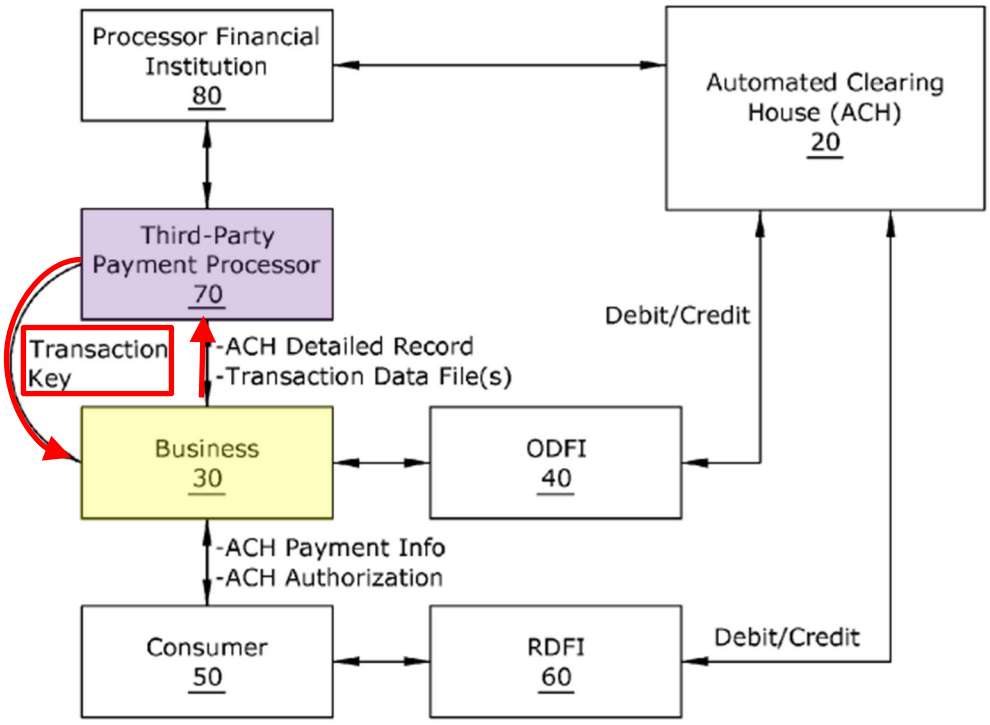
1005, 10:1-4). These examples would have been well-known by a POSITA. Thus, it is my opinion that the combination of Seger and Smith involves the combination of well-understood and predictable technologies that would have led to predictable results.

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

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;

88. It is my opinion that Smith discloses or renders obvious this element.

89. *First*, Smith discloses "a token corresponding to the financial transaction to identify the one or more documents." Smith teaches that the TPPP "determines what the ***unique transaction key*** is for each ACH transaction that corresponds to one or more transaction data files" and generates the "unique transaction key … for each ACH transaction." (Ex. 1004, [0041]).



(Ex. 1004, Fig. 2).

90. Because the "unique transaction key" functions to "associate the ACH transaction entry detail record with one or more transaction data files" (Ex. 1004, [0047]), Smith's "unique transaction key" is a pointer to the ACH transaction entry detail record and transaction data files (*i.e.*, the "enriched data record"). The POSITA would, therefore, have understood the Smith's "transaction key" as the claimed "token." The POSITA would also understand that because Smith's transaction key is a unique key "for each ACH transaction" (Ex. 1004, [0041]) it identifies information relating to the transaction stored by the business computer (*i.e.*, "one or more documents"). (Ex.

1004 at [0034], [0036]). Smith also discloses "[t]he transaction key may be comprised of any format capable of identifying the ACH transaction separately from other ACH transactions" including "letters, numbers, characters" and the like. (Ex. 1004, [0030], [0055]).

91. A POSITA would have understood Smith's "transaction key" as the claimed "token." First, the POSITA would have understood that, as "unique" key for "each ACH transaction" (Ex. 1004, [0041]), Smith's transaction key identifies the information relating to the transaction stored by the business computer (*i.e.*, "one or more documents"). (Ex. 1004, [0034]-[0036]). Further, the POSITA would have understood that by the August 14, 2015 timeframe, it was a well-known technique to generate a unique identifier for a transaction by applying a predetermined algorithm to some or all of the transaction data. (Ex. 1007, 6:28-33 ("the token may incorporate at least a portion of an account number for a source account or the public key of the source account that is associated with the mobile wallet account. The incorporated user account information may include the payment method to be associated with the transaction"); Ex. 1017, [0027] ("tokenization procedures may produce tokens from credit card data"); Ex. 1018, [0006], [0019] ("The payment terminal identifies a set of tokenization parameters based on the identified transaction information, and tokenizes the received payment information based on the set of identified tokenization parameters," "token

refers to a string of characters mapped to an input string of characters in the creation of tokenized data").

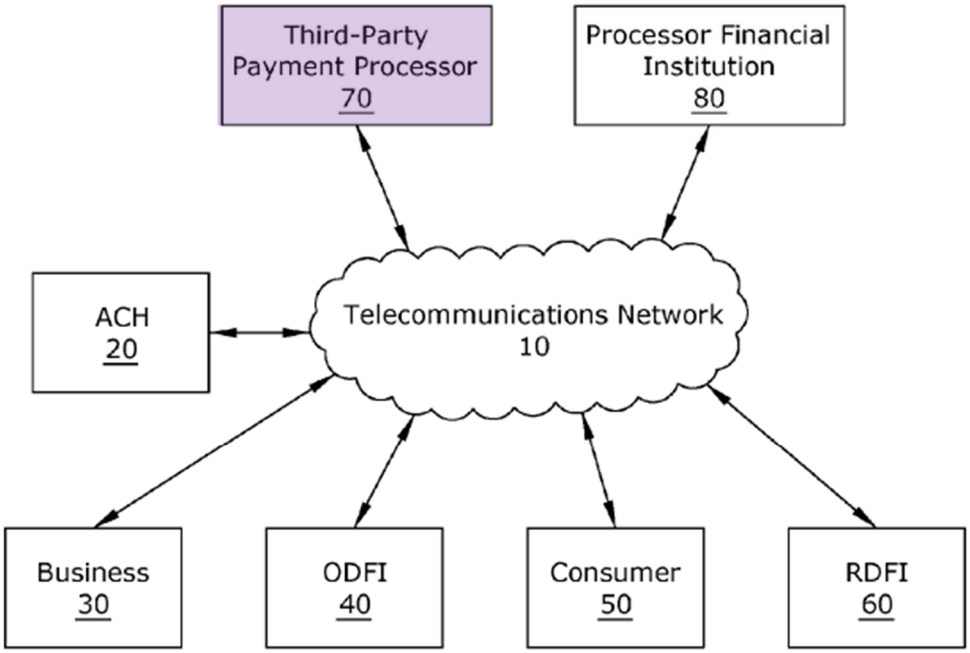
92. The POSITA would have understood that a well-known way to generate this "unique" key "capable of identifying" the transaction would have been to use the transaction data as an input into an algorithm to generate an identifying output in the form of "letters, numbers, and characters" and the like." Thus, Smith's transaction key aligns with the '413 Patent's statement that a "token is a pointer to an enriched data record of a plurality of data 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).). It would have been obvious to the POSITA to generate Smith's transaction key (i.e., "token") by formatting or passing transaction information through an algorithm in a predetermined manner, to effectuate Smith's goal of achieving a transaction key that is "unique" and "capable of identifying" the transaction.

93. One problem facing those seeking to assign a transaction key to a transaction is that of "collision." This refers to a problem where the processes used to generate the transaction keys 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 transaction key 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.

94. Accordingly, it would have been obvious to the POSITA to generate Smith's transaction key (i.e., "token") by formatting or passing transaction information through an algorithm in a predetermined manner, in order to effectuate Smith's goal of achieving a transaction key that is "unique" and "capable of identifying" the transaction..

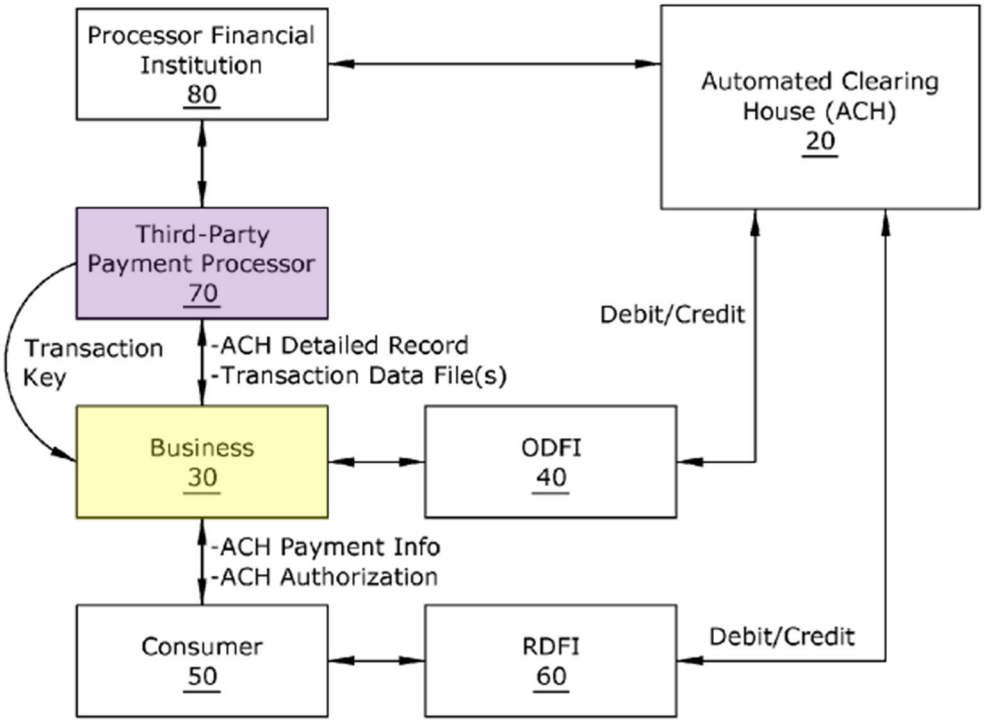
95. *Second*, Smith discloses a "token server." Smith teaches that the "unique transaction key" (i.e., "token") is generated by a "third-party payment processor [TPPP]" (i.e., "token server"). (Ex. 1004, [0041]). Smith's Figure 1 shows that the TPPP "communicates with [other devices] via one or more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



(Ex. 1004, [0031]; Fig. 1). The TPPP comprises computers that communicate with computers associated with other entities of the system via a single, or multiple, telecommunication networks. In operation, and as described in greater detail below, the TPPP performs actions like generating a transaction key in response to communications received from other computers on the network. As described above, a "server" is a computer or program that responds to commands from a client." Accordingly, the POSITA would have understood the TPPP to comprise a "server," and because the TPPP generates a unique transaction key (*i.e*, "a token") for use by other devices (based on the

given ACH transaction of one or more transaction data files), the POSITA would have understood the TPPP to comprise a "token server," specifically.

96. *Third*, it is my opinion that Smith discloses a request for generating tokens sent "to a token server from the first intermediary server." Smith explains that after receiving transaction data record(s) and ACH detail record, the TPPP "updates its database to include a unique transaction key that is associated with the transaction data file(s) provided by the business 30." (Ex. 1004, [0053]). Smith's Figure 2 shows the TPPP "transmits the transaction key to the business 30 for use when the business 30 sends the ACH transaction detail record." (Ex. 1004, [0053]).



(Ex. 1004, Fig. 2). A POSITA would have understood that "request-response" is a basic interaction paradigm used in the client-server architecture that computers use to communicate with one another over a telecommunication network. In a sense, a "request" is simply a message sent between by a "client" object. The receiving object (*i.e.*, a "server") then generates a "response" to the received request and sends this response back to the client. Accordingly, it is my opinion that, in the example of Smith, the transmission of the ACH detailed record and transaction data files from the business computer to the third-party payment processor represents a request for the third-party payment processor to respond. In this interaction, the business computer (*i.e.*, "first intermediary server" for the reasons described above) also acts as a client of the TPPP (*i.e.*, "token server"). The third-party payment processor then responds by generating a transaction key, and transmitting the transaction key back to the business computer.

97. It is therefore my opinion that because the TPPP generates and returns the "unique transaction key" (*i.e.* "token") in response to receiving communications from the business computer 30 (*i.e.*, "first intermediary server"), the POSITA would have understood these communications as the first intermediary server "requesting generation of a token."

98. *Fourth*, Smith discloses or renders obvious requesting "via a messaging bus." Smith teaches communicating data between various computing devices through

telecommunications networks 10. (Ex. 1004, Fig. 1, [0032]). Smith explains that the business computer "provides the transaction data files to the [TPPP] 70 by a secure telecommunication network." (Ex. 1004, [0050]). This aligns with the '413 Patent's statement that "bus" "should be construed broadly herein as any system for communicating data." (Ex. 1001, 33:35-45).

99. Further, a messaging bus is a commonly used term to denote a networked system that provides efficient and scalable information exchange between different services and systems, and to handle large volumes of messages without affecting system performance. The POSITA would have understood the use of a messaging bus to be routine and conventional, and could have easily utilized a messaging bus in Smith's financial system. Thus, Smith discloses or renders obvious "requesting … via a messaging bus."

100. Accordingly, it is my opinion that the combination of Smith and Seger discloses or renders obvious requesting generation of a token (Smith's unique transaction key) corresponding to the financial transaction to identify the one or more documents, to a token server (third-party payment processor), from the first intermediary server (business computer), via a messaging bus in the centralised financial system.

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;

101. It is my opinion that the combination of Smith and Seger would have rendered this obvious.

102. *First*, Smith discloses "generating the token at the token server." Smith teaches that "the third-party payment processor 70" (*i.e.*, "token server") "updates its database to include a unique transaction key" (*i.e.*, "token") that "is associated with the transaction data file(s) provided by the business 30." (Ex. 1004, [0053]).

103. *Second*, Smith discloses "adding the token into" a record, "from the token server, in association with the enriched data record." As shown in Figure 5, Smith teaches a "database table illustrating the usage of a simple transaction key for both an ACH transaction detail record and the transaction data file(s)." (Ex. 1004, [0041]).

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

(Ex. 1004, Fig. 5). Smith teaches that the "third-party payment processor 70 stores the transaction key, the ACH transaction detail record and the corresponding transaction data files in a database." (Ex. 1004, [0041]). The POSITA would have understood that the TPP (*i.e.*, "token server") generates the transaction key (*i.e.* "token," purple above), and then "updates its database to include [the] unique transaction key" (Ex. 1004, [0053]) in association with the records of the transaction (*i.e.*, "enriched data record," yellow above) in a database.

104. Smith thus discloses the entirety of this element with the exception of "the blockchain." However, as explained above for element 2, applying blockchain technology to Smith's authorization verification system would have been obvious to the POSITA. For Smith's transaction key, the POSITA would have recognized that having the TPPP (which generated the key) add the key to the blockchain would help ensure the accuracy and integrity of the transaction key.

105. Data can be corrupted, altered, or otherwise tampered with at a number of different points, including during transmission. Each time data is communicated from one party to another on a system, a malicious entity has a potential opportunity to intercept and tamper with that data. As such, in the combination of Smith and Seger, security and integrity interests would have been best served by the TPPP adding the transaction key to the blockchain, thereby minimizing the number of transmissions

during which the transaction key could be corrupted. Additionally, the TPPP adding the transaction key to the blockchain would have prevented parties to the underlying transaction from obtaining the transaction key data before being added to the immutable ledger. This would have ensured, to all parties on the system, that the record of the transaction key on the blockchain was not affected by any interested parties.

106. The POSITA would have been motivated to do so given Smith's teaching to use transaction keys to resolve "dispute[s] as to the validity of the ACH transaction," including using the key to "easily identify and view the transaction data files." (Ex. 1004, [0056]). Smith further explains the importance of the transaction key: "if no transaction key is provided by the business 30, then the transaction is declined and returned to the business 30." (Ex. 1004, [0057]). Thus, adding the transaction key (i.e., "token") into the blockchain from the TPPP (i.e., "token server") would have been obvious to the POSITA.

107. Accordingly, it is my opinion that the combination of Smith and Seger would have rendered obvious "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."

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

108. It is my opinion that Smith discloses or would have rendered obvious this element.

109. Smith teaches the TPPP "provides the transaction key to the business 30 after receiving the ACH transaction detail record for the business 30 to use with any transaction data files uploaded to the third-party payment processor." (Ex. 1004, [0041]). Figure 1 shows the TPPP communicating with the business computer via a single or multiple "telecommunications network(s)" (*i.e.*, "messaging bus"). (Ex. 1004, Fig. 1). Transmission via the messaging bus would also have been obvious to the POSITA from Smith's teachings as described for element 3.

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

110. It is my opinion that Smith discloses or would have rendered obvious this element.

111. As described above with respect to Element 1, Smith teaches that "business 30 enters the information received from the consumer 50 into a database that stores the information for later access." (Ex. 1004, [0034]). Further, the TPPP "passes back a unique transaction key to the business 30 that is associated with both the ACH

transaction (including the ACH transaction detail record) and the transaction data file(s)." (Ex. 1004, [0058]). The POSITA would have found it obvious for the business computer (*i.e.*, "first intermediary server") to transmit the transaction key (*i.e.*, "token") to the database (*i.e.*, "first document store") in "association with the one or more documents." The POSITA would have been motivated to allow the business computer to store the transaction key "for later access," for example to later send to other entities on the network or to recall transaction information to compare against the TPPP's record. (Ex. 1004, [0034], [0041]). Including the transaction key (*i.e.*, "token") in such communications would allow the receiving entity to easily identify the transaction to which the communication pertains.

2. Claim 2

112. Claim 2 recites:

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

113. It is my opinion that the combination of Smith and Seger would have rendered claim 2 obvious.

114. Smith explains that the transaction key (i.e., "token) is communicated to the business computer (i.e., "first intermediary server") "so the business 30 (or any third-party the business gives the transaction key to such as the RDFI 60 or the ODFI 40) can access the ACH detail record and the transaction data files associated with the ACH detail record." (Ex. 1004, [0041]). By explaining that the business computer "gives the transaction key" to other parties, Smith discloses "sending a first financial message comprising the token from the first intermediary server to a second intermediary server in the centralized financial system" as claimed. (Ex. 1004, [0041]).

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

transaction key (i.e., "token") to the ODFI (i.e., "second intermediary server"), the business computer (i.e., "first intermediary server") informs the ODFI about the ACH transaction, and therefore this message is indicative of a making payment to a second user.

3. Claim 5

116. Claim 5 recites:

> 5. The computer implemented method as claimed in claim 1, wherein the step of generating the enriched data record comprises:
>
> extracting a plurality of attributes from the one or more documents, at the first intermediary server; and
>
> combining the plurality of attributes to generate the enriched data record, at the first intermediary server.

117. It is my opinion that the combination of Smith and Seger would have rendered claim 5 obvious.

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

118. It is my opinion that Smith discloses or would have rendered obvious "extracting a plurality of attributes from the one or more documents, at the first intermediary server." As explained for element 2 of claim 1, Smith describes "transaction data files" and "ACH transaction detail records." (Ex. 1004, Fig. 5). Smith

teaches that the "entry detail record in the ACH batch file includes various fields such as record type code, transaction code, identification of RDFI 60, identification of the ODFI 40, check digit, DFI account number, funds transfer amount, individual identification, individual name …, addenda record indicator and trace number." (Ex. 1004, [0047]).

119. Smith teaches "[t]he ACH file is an electronic data file that stores the entry detail records for the ACH transactions. Each ACH detail record corresponds to an ACH transaction for the business 30." (Ex. 1004, [0043]). Smith explains that "a single ACH file holds one or more electronic transactions." (Ex. 1004, [0045]). Thus, Smith's business computer 30 uploads a single ACH detail record associated with each individual transaction to the TPPP. As explained to element 2, this ACH detail record, together with the transaction data file, forms the "enriched data record." The ACH transaction detail record comprises various fields (*i.e.*, "attributes") that are extracted from the underlying ACH transaction information (*i.e.*, "document") in the process of generating the ACH detail record and transaction data file *(i.e.*, "enriched data record"). (Ex. 1004 at [0047]).

120. Additionally, Smith teaches gathering a plurality of additional information pertaining to the transaction such as "a copy of a state license, a signature of the consumer 50, an ACH authorization by the consumer 50, a copy of an agreement with

the consumer 50, and a copy of a driver's license or other identification for the consumer." (Ex. 1004, [0052]). The POSITA would have understood this additional information as comprising "attributes" that the business computer (i.e., "first intermediary server") extracts from the documents pertaining to the underlying financial transaction stored in the business computer's database. (Ex. 1004, [0034]).

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

121. It is my opinion that Smith discloses or would have rendered obvious "combining the plurality of attributes to generate the enriched data record, at the first intermediary server." Smith teaches that "the business 30 uploads the ACH transaction detail record … [and] at the same time upload[s] the corresponding transaction data file(s) associated with the ACH transaction detail record." (Ex. 1004, [0048]). Thus, the business computer (*i.e.*, "first intermediary server"), by uploading both ACH detail record and the transaction data file "at the same time," combines the attributes of the ACH detail record with the attributes of the transaction data file into a single transmission to generate an "enriched data record" communicated to the TPPP. The POSITA would have found it obvious to combine the two files into one transmission because combining these two files into one transmission would have simplified and reduced the latency of the information transfer process.

4. Claim 6

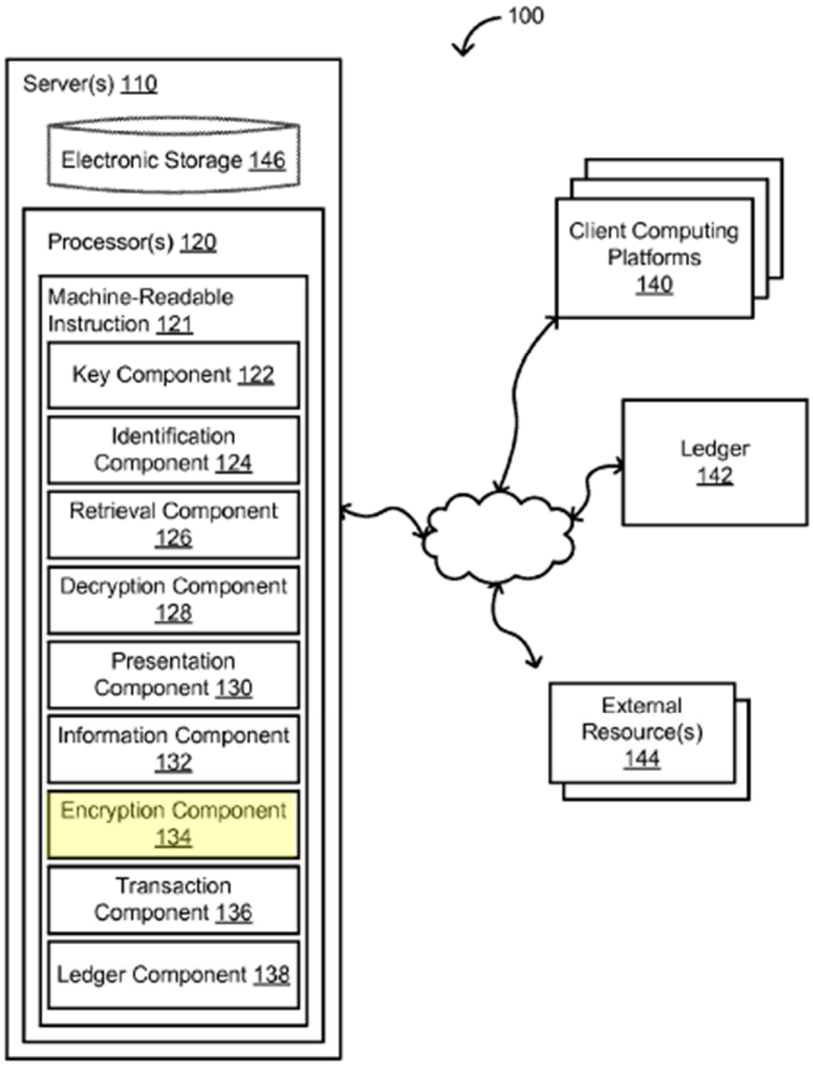
122. Claim 6 recites:

> 6. The computer implemented method as claimed in claim 1, wherein the step of generating the enriched data record comprises:
>
> extracting a plurality of attributes from the one or more documents, at the first intermediary server;
>
> de-identifying the plurality of attributes to obtain a plurality of de-identified attributes, at the first intermediary server; and
>
> combining the plurality of de-identified attributes to generate the enriched data record, at the first intermediary server.

123. In my opinion, the combination of Smith and Seger would have rendered claim 6 obvious. *First*, Smith discloses or would have rendered obvious the steps of "extracting" and "combining" for the reasons described above for claim 5.

124. *Second*, while Smith does not explicitly disclose "de-identifying the plurality of attributes to obtain a plurality of de-identified attributes, at the first intermediary server," this element would have been obvious in view of Seger. Seger teaches that the "information transaction that may be held within the distributed ledger" may include encrypted information. (Ex. 1005, 6:1-24). The first encrypted information may be encrypted with "a first public key associated with the first party." (Ex. 1005 at 6:15-18). Seger teaches that server(s) 100 (*i.e.*, "first intermediary server") comprise

"encryption component 134 [which] may be configured to communicate with key component 122 to obtain one or more public keys associated with one or more given parties. The one or more public keys obtained may be used to encrypt second information and/or other information intended for the given parties." (Ex. 1005, 8:43-48).



(Ex. 1005, Fig. 2). The POSITA would have understood that by encrypting the information payload, the attributes included therein are "de-identified" by the "encryption component" of the Seger server(s).

125. Systems like Smith's, where personally identifiable information (PII) is stored and transmitted via a network often employ some for of data de-identification to protect the privacy and confidentiality of said PII. De-identification can take a number of forms so long as unauthorized parties cannot view the sensitive PII. In some cases de-identification merely involves removing certain identifiers such as name, social security number, etc. However, more sophisticated means of de-identification can include encrypting the data, such that no unauthorized users can view any PII, or hashing the data so as to irreversibly mask the sensitive PII over the network. Accordingly, by encrypting an information payload, Seger teaches de-identifying data, which the POSITA would have found obvious to apply to the system of Smith for the reasons described below.

126. It would have been obvious to the POSITA to apply encryption as taught by Seger to Smith's ACH detail record and transaction data files (i.e., the "enriched data record") added to the blockchain such that the attributes are "de-identified." Smith notes that transaction data is "sensitive information" such that the system "maintains the highest level of compliance and encryption." (Ex. 1004, [0059]). The POSITA would

have found it obvious to apply Seger's teachings to protect Smith's "sensitive information" by ensuring "only authorized parties may read [] the communication and/or data." (Ex. 1005, 1:15-16). As explained for claim 5, Smith discloses or would have rendered obvious combining the ACH detail record and transaction data file into a single transmission. The POSITA similarly would have found it obvious in the Smith/Seger combination to send a single transmission with the encrypted data and would have rendered obvious "combining the plurality of de-identified attributes to generate the enriched data record."

5. Claim 7

127. Claim 7 recites:

> 7. The computer implemented method as claimed in claim 1, wherein the step of generating the enriched data record comprises:
>
> extracting a plurality of attributes from the one or more documents, at the first intermediary server;
>
> hashing the plurality of attributes to generate a plurality of respective hashes, at the first intermediary server; and
>
> combining the plurality of hashes to generate the enriched data record, at the first intermediary server.

128. It is my opinion that the combination of Smith and Seger would have rendered claim 7 obvious.

129. *First*, Smith discloses or would have rendered obvious the steps of "extracting" and "combining" for the reasons described for claim 5.

130. *Second*, although Smith does not explicitly disclose "hashing the plurality of attributes to generate a plurality of respective hashes, at the first intermediary server," it is my opinion that this element would have been obvious in view of Seger.

131. As explained for claim 6, Seger discloses encrypting an information payload. Further, Seger teaches generating "a hash of the first information payload enabling auditing of the information transferred to the first party and stored within the block chain." (Ex. 1005, 15:44-47). Seger explains that this hash can "verify an integrity of the first information transaction." (Ex. 1005, 18:1-2). Accordingly, it would also have been obvious to the POSITA to hash the plurality of Smith's attributes to maintain "secure private communication between multiple parties" while providing a means "to verify an integrity" (Ex. 1005, 1:40-41, 18:1) of the transaction information.

6. Claim 8

132. Claim 8 recites:

> 8. The computer implemented method as claimed in claim 1, further comprising the steps of:
>
> transmitting one or more first requests, each comprising the token, from the first intermediary server to a second intermediary server in the centralised financial system, via the messaging bus;

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

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

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

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

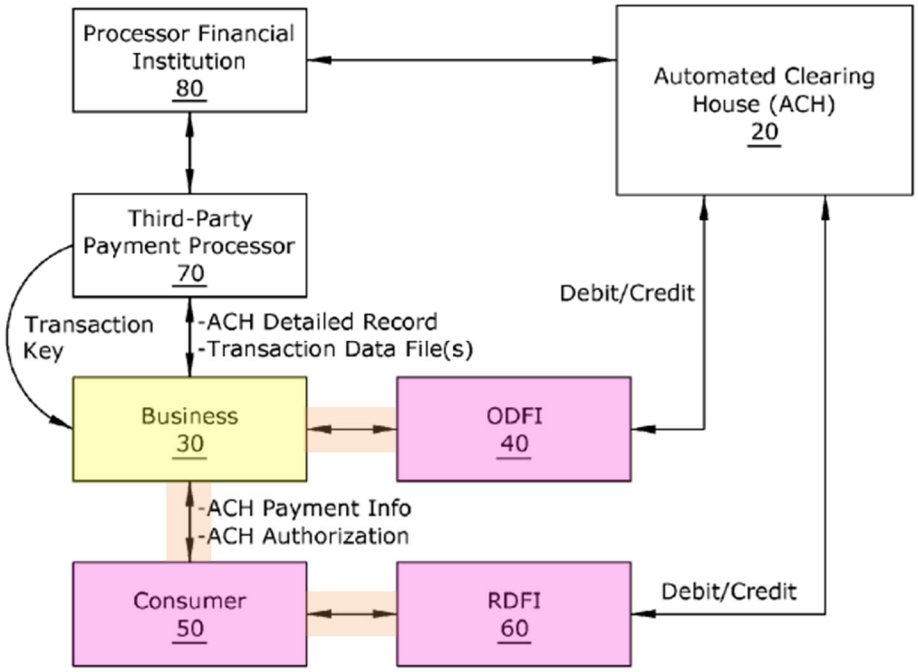
adding the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain, from the second intermediary server; and

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

133. It is my opinion that claim 8 would have been obvious over the combination of Smith and Seger for the reasons described below.

134. *First*, Smith teaches the TPPP "communicates the transaction key to the business 30 via the network so the business 30 (or any third-party the business 30 gives

the transaction key to …) can access the ACH detail record and the transaction data files associated with the ACH detail record." (Ex. 1004, [0041]). Figure 3 shows examples of the business computer (*i.e.*, "first intermediary server") communicating with the computers of other entities (*i.e.*, "second intermediary server") via a communication system (*i.e.*, "messaging bus"):



(Ex. 1004, Fig. 3).

135. The POSITA would have understood that by "giv[ing] the transaction key" (i.e., "token") to other entities on the network (i.e., "second intermediary server"), the business computer (i.e., "first intermediary server") transmits messages "each comprising the token, from the first intermediary server to a second intermediary server

in the centralised financial system." As explained for element 3, it would have been obvious to the POSITA for such messages to be communicated via the messaging bus.

136. Smith further teaches that communications through the system may comprise requests and responses. Smith teaches a "request 415 is then sent to a consumer ID and address validation network 140," and "[a] response is then supplied to the business device 110 via procedure 435." (Ex. 1004, [0077]-[0078]).

137. While Smith does not explicitly disclose the transmission of these requests and response between the first intermediary server and the second intermediary server, it would have been obvious to the POSITA for the business computer (i.e., "first intermediary server") and a computers of another entity (i.e. "second intermediary server") to communicate in this manner. Smith itself establishes that communicating via requests and responses was known in the art. (Ex. 1004, [0077]-[0078]). The POSITA would have understood the business and, for example, the consumer communicating in this manner is merely the combination of prior-art elements. These elements could have been combined according to known methods and would have yielded entirely predictable results.

138. Accordingly, it is my opinion that the 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," and "receiving the one or more first responses at the first intermediary server" would have been obvious to a POSITA.

139. *Second*, it is my opinion that it would have been obvious to the POSITA to include the token in each request and response. Smith teaches that the business computer gives the transaction key (i.e., "token") to other parties so they "can access the ACH detail record and the transaction data files associated with the ACH detail record." (Ex. 1004, [0041]). Seger teaches using "transactions [that] may be identified based on the transaction identifier." (Ex. 1005, 5:66-67). Seger explains that when a first party sends a request to a second party, the first party may "include a request and/or requirement that Party B use [the transaction identifier] in a second information transaction (e.g., a response to the first information transaction)." (Ex. 1005, 6:60-65). It would have been obvious to the POSITA to include Smith's transaction key (i.e, "token") in the request/response to identify the transaction and "enable the intended recipient to provide a response." (Ex. 1005, 7:1). 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.

140. *Third*, 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" would have been obvious to the POSITA. Smith teaches that entities maintain records of their transactions in local storage. (Ex 1004, [0034]). The POSITA would have understood that local storage of transaction information is conventional for parties to an electronic funds transfer. (Ex. 1011, Fig. 4, [0074]-[0075] (disclosing 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)). Thus, the POSITA would have found it obvious that an entity on Smith's network communicating with the business computer, such as the consumer's computer or the ODFI computer (*i.e.*, "second intermediary server"), transmits records to local storage (*i.e.*, "second document store") much like the business computer stores transaction information in a database, such that the other entity may also "store [] information for later access." (Ex. 1004, [0034]).

141. Further, Smith enables "verification" and "proving that a consumer authorized a financial transaction." (Ex. 1004, [0004]). The POSITA would have understood that a means for verifying transaction information is by comparing the transaction information against an entity's own records. Indeed, Seger discloses verification via a similar mechanism where an entity "verif[ies] an integrity of the first

information transaction based on the hash of the first information payload" included in the blockchain record. (Ex. 1005, 18:1-3).

142. For reasons described in greater detail below, the POSITA, looking to Seger, would have found it obvious to keep a record of the requests and responses so as to "provide a verifiable record of the various information transactions" through the system. (Ex. 1005, 10:29-30). The POSITA would have further understood that to enact such verification of the requests and responses, the combination of Smith and Seger includes "transmitting the one or more first requests and the token from the second intermediary server to a second document store" and "transmitting the one or more first responses to the first document store" so as to "store[] the information for later access" when verifying. (Ex. 1004, [0034]).

143. *Fourth*, it is my opinion that 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" would have been obvious to the POSITA.

144. As explained for claim 7, the POSITA would have found the hashing of information on the system obvious to provide secure, private communications that may still be verified. (Ex. 1005, 1:40-41, 18:1-3). 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 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."); Ex. 1041, 78 (a hash function "maps a message of any length into a fixed-length hash value which serves as the authenticator" of a message), 88 ("Because the secret value itself is not sent, an opponent cannot modify an intercepted message and cannot generate a false message."). 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 could have accessed the publication described above. (Ex. 1024, 11 (highlight indicating link to publication)).

145. 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; *see also* Ex. 1019, 1 (“Hash functions were introduced in cryptography to provide message integrity and authentication.”)). The POSITA would have thus found it obvious to hash one or more responses at the entity on Smith’s network communicating with the business computer so that the business computer can verify the integrity of the response. To maximize the business computer’s (*i.e.*, first intermediary server’s) ability to verify the integrity of data moving over the network, the POSITA also would have found it obvious to hash one or more requests at other entity (*i.e.*, second intermediary server). This would ensure that when the other entity communicates its response to the business computer, the business computer can also ensure that its original request arrived 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.

146. *Fifth*, it is my opinion that the step of “adding the one or more first request hashes and the one or more first response hashes to the enriched data record in the blockchain, from the second intermediary server” would have been obvious to the POSITA.

147. 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 at 22). Seger’s “verifiable, and immutable” blockchain is a

realiable source of information, published to those on the system." (Ex. 1005 at 1:43). In fact, Seger teaches that verifying data integrity may be accomplished by comparing a hash on the blockchain with an entity's own hash of the record. (Ex. 1005 at 18:1-3). Accordingly, the POSITA would have found it obvious add the hashes into the blockchain from the other entity on the Smith system (*i.e.*, "second intermediary server") to allow the business computer (*i.e.* "first intermediary server") to compare its data against a reliable source of information, thereby ensuring integrity. (Ex. 1015 at 22).

7. Claim 9

148. Claim 9 recites:

> 9. The computer implemented method as claimed in claim 8, further comprising the steps of:
>
> hashing the one or more first responses at the first intermediary server to regenerate the one or more first response hashes; and
>
> verifying the one or more first response hashes with the blockchain from the first intermediary server, using the token.

149. It is my opinion that the combination of Seger and Smith would have rendered claim 9 obvious.

150. *First*, Seger discloses "verify[ing] an integrity of the first information transaction based on the hash of the first information payload." (Ex. 1005 at 18:1-3).

As explained above, it was well-known that to verify data integrity using hashes, "[w]hen the receiver gets the data an application can generate a hash and compare it to the original one." (Ex. 1015, 22. *See also* Ex. 1041, 92 ("The receiver authenticates that message by recomputing the hash.")). The POSITA therefore would have found it obvious for the business computer ("*i.e.*, "first intermediary server") to generate a hash of the "one or more first responses" such that the business computer can then verify the information included therein.

151. *Second*, the POSITA would have understood that, within the context of the Smith/Seger combination, this verification would have been accomplished "using the token" as claimed. As described for element 3 of claim 1, both Smith and Seger use a token ("transaction key" and "transaction identifier," respectively) to identify transactions on the system. Further, Seger discloses "verify[ing] an integrity of the first information transaction based on the hash of the first information payload ***included in the first information transaction identifier***." (Ex. 1005 at 18:1-4). Accordingly, the POSITA would have understood that the token of the combination may be used to identify the record of the transaction to which "one or more responses" pertain on the blockchain, in order to accomplish the disclosed verification.

8. Claim 10

152. Claim 10 recites:

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

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

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

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

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

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

153. It is my opinion that the combination of Smith and Seger would have rendered claim 10 obvious. Smith teaches using "the highest level of compliance and encryption within the Payment Card Industry." (Ex. 1004, [0059]). While Smith does not explicitly disclose the claimed encryption protocol, the claimed steps would have been obvious in view of Seger and knowledge of a POSITA.

154. *First*, Seger teaches the use of "one or more forms of public key, or asymmetric, cryptography to facilitate communication." (Ex. 1005, 4:52-54). An

encryption technique where the sending party uses the receiving party's public key to encrypt a message or request before sending, and where the receiving party decrypts the message or request using its private key was well within the knowledge of 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."); Ex. 1041, 47-48 ("When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key."). The POSITA would have understood the limitations of "encrypted with a second public key … at the first intermediary server, before transmission to the second intermediary server," "decrypted with a second private key at the second intermediary server after reception from the first intermediary server," "encrypted with the first public key at the second intermediary server, before transmission to the first intermediary server," "decrypted with a first private key at the first intermediary server after reception from the second intermediary server," as merely claiming an implementation of known public key encryption techniques. This generic encryption protocol is reflected in Seger, which teaches using the first and second public and private keys to encrypt and decrypt information. (Ex. 1005, 4:61-67, 5:23-30, 7:64-65). Accordingly, the POSITA would have found it obvious to apply the well-known public key/asymmetric cryptography taught by Seger to Smith's system so as to "facilitate secure private communications

between" the parties on the system. (Ex. 1005 at 1:40-41).

155. *Second*, Seger further describes having a party "cryptographically sign" messages on the system. (Ex. 1005, 5:60). It was well-known to use public key cryptography techniques to generate digital signatures to authenticate the source of a message. (Ex. 1015, 22-23; Ex. 1041, 88). To do so, a sender signs the message with a key associated with that sender. In the context of the combination of Smith and Seger, there are two keys associated with the sender – the sender's private key or the sender's public key.

156. A conventional digital signature algorithm uses a sender's private key to sign a message or request, the receiving party uses the sender's public key to verify the message or request. Prior art references show that algorithms using a public key to sign and create a digital signature had also been disclosed 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. 1023, [0340] ("Appropriately signed means signed with the public key"), Ex. 1022, [0114] ("queries can be signed with the public key and verified with the cryptographic signature"), Ex. 1021, [0016] ("The request may also be signed with the public key.").

157. Accordingly the POSITA would have recognized that signing a message or request with either the sender's private key or public key were two options that had been disclosed in the art to generate a digital signature. It is my opinion that it would not have been inventive for the POSITA to choose signing with the public key from these two options.

9. Claim 11

158. Claim 11 recites:

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

159. It is my opinion that the combination of Smith and Seger would have rendered claim 11 obvious. A POSITA would have understood that public keys are associated with particular entities on the network, and these keys are shared with others on the system to enable public key/asymmetric cryptography. (Ex. 1015 at 4). Typically, parties share this data by "publish[ing] their public keys in a reliable information source." (Ex. 1015 at 4). Seger's blockchain is not just "reliable" but "immutable." Seger even discloses adding information that "may include the first public key" to the blockchain. (Ex. 1005, 2:25-26). It thus would have been obvious to the POSITA for each party to add its public key to the blockchain in order to publish the

keys on an information source that cannot be changed, thereby ensuring the integrity of the published key information.

10. Claim 12

160. Claim 12 recites:

> 12. The computer implemented method as claimed in claim 1, further comprising the steps of:
>
> transmitting one or more second requests, each comprising the token, from a second intermediary server in the centralised financial system to the first intermediary server, via the messaging bus;
>
> receiving the one or more second requests at the first intermediary server and transmitting the one or more second requests from the first intermediary server to the first document store;
>
> generating one or more second responses, each comprising the token, corresponding to the respective one or more second requests, at the first intermediary server;
>
> transmitting the one or more second responses from the first intermediary server to the second intermediary server, via the messaging bus;
>
> hashing the one or more second requests and the one or more second responses at the first intermediary server to generate one or more second request hashes and one or more second response hashes, respectively;
>
> adding the one or more second request hashes and the one or more second

response hashes to the enriched data record in the blockchain, from the first intermediary server; and

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

161. It is my opinion that the combination of Smith and Seger would have rendered claim 12 obvious. The POSITA would have understood that this claim merely sets forth an obvious reversal of the steps recited above in claim 8, (*i.e.*, the second intermediary server sends a request and the first intermediary server sends a response). As such, and for the reasons described above with respect to claim 8, these elements would have been obvious to the POSITA.

11. Claim 13

162. Claim 13 depends from claim 12, reciting "the steps of: hashing the one or more second responses at the second intermediary server to regenerate the one or more second response hashes; and verifying the one or more second response hashes with the blockchain from the second intermediary server, using the token." Claim 13 recites:

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

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

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

163. It is my opinion that the combination of Smith and Seger would have rendered claim 13 obvious. As explained for claim 12, the POSITA would have understood that claim 12 merely sets forth a reversal of the steps recited above in claim 8. The additional steps recited in claim 13 are the same as recited in claim 9, which depends upon claim 8. It is my opinion that the combination of Smith and Seger would have rendered claim 13 obvious for the reasons described for claims 9 and 12.

12. Claim 14

164. Claim 14 recites:

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

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

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

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

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

intermediary server; and

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

165. It is my opinion that the combination of Smith and Seger would have rendered claim 14 obvious. As explained for claim 12, the POSITA would have understood that claim 12 merely sets forth a reversal of the steps recited above in claim 8. The additional steps recited in claim 14 are the same as recited in claim 10, which depends upon claim 8. Therefore, the combination of Smith and Seger would have rendered claim 14 obvious for the reasons described for claims 10 and 12.

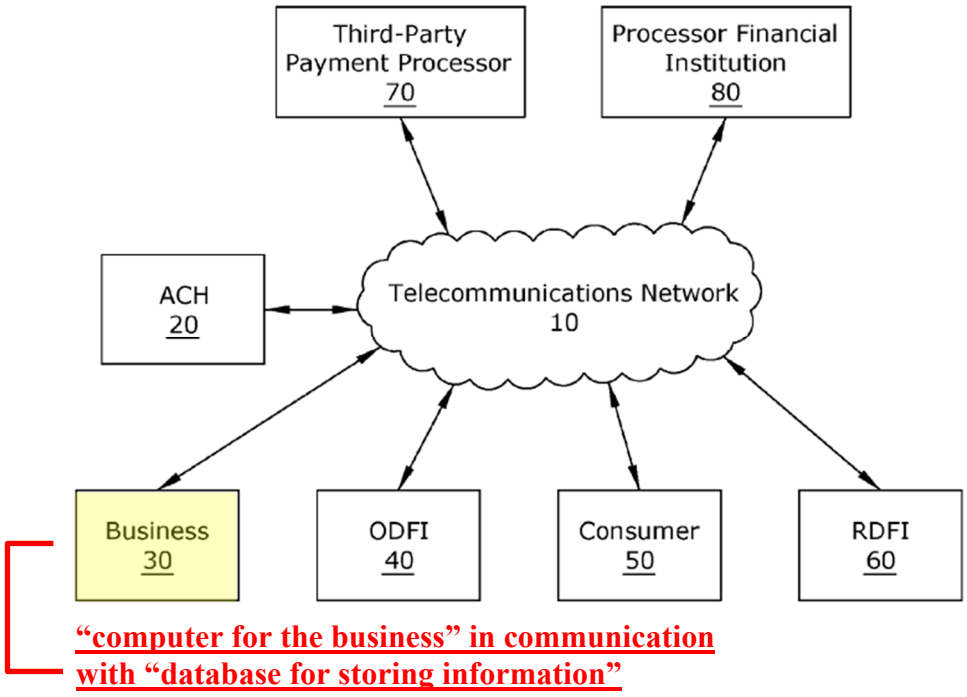
13. Claim 15

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

166. I have been asked to assume the preamble of claim 15 is a limitation. It is my opinion that Smith discloses the preamble for reasons described the preamble of claim 1. (Ex. 1004 at [0004] ("[t]he present invention … relates to an electronic funds transfer consumer authorization verification system for efficiently proving that a consumer authorized a financial transaction via an ACH network.").

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;

167. It is my opinion that the Smith/Seger combination discloses or would have rendered obvious this element for the same reasons explained above for element 1 of claim 1. Smith also teaches that the system "may be utilized upon any telecommunication network 10 capable of transmitting electronic data and/or electronic funds between a plurality of electronic devices (*e.g.*, computers, mobile devices, etc.)." (Ex. 1004, [0031]).



(Ex. 1004, Fig. 1). Smith teaches that "a computer for the business 30" is in communication with "a database that stores [] information for later access." (Ex. 1004, [0031], [0034]).

168. The POSITA would have understood business computer 30 (*i.e.*, "first intermediary server") is "operably connected to a network and a first document store."

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

169. It is my opinion that the combination of Smith and Seger would have rendered this element obvious for the same reasons as explained for element 3 of claim 1.

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

170. It is my opinion that the combination of Smith and Seger would have rendered this element obvious for the same reasons as explained for element 2 of claim 1.

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;

171. It is my opinion that the combination of Smith and Seger would have rendered this element obvious for the same reasons as 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;

172. It is my opinion that the combination of Smith and Seger would have rendered this element obvious for the same reasons as 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

173. It is my opinion that the combination of Smith and Seger would have rendered this element obvious for the same reasons as 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;

174. It is my opinion that the combination of Smith and Seger would have rendered this element obvious for the same reasons as 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

175. It is my opinion that the combination of Smith and Seger would have rendered this element obvious for the same reasons as 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.

176. It is my opinion that the combination of Smith and Seger would have rendered this element obvious for the same reasons as explained for element 5 of claim 1.

14. Claim 16

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:

177. I have been asked to assume the preamble of claim 16 is a limitation. It is my opinion that Smith discloses or renders obvious the preamble for the same reasons as explained for Element 1 of claim 1 and Element 1 of claim 15.

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

178. It is my opinion that the combination of Smith and Seger would have rendered this element obvious for the same reasons as 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;

179. It is my opinion that the combination of Smith and Seger would have rendered this element obvious for the same reasons as 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

180. It is my opinion that the combination of Smith and Seger would have rendered this element obvious for the same reasons as explained for element 3 of claim 1.

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

181. It is my opinion that the combination of Smith and Seger would have rendered this element obvious for the same reasons as explained for element 6 of claim 1.

15. Claim 17

182. Claim 17 recites:

> 17. The first intermediary server as claimed in claim 16, further configured to send a first financial message comprising the token, to a second intermediary server in the centralised financial system, indicative of making a payment to a second user.

183. It is my opinion that the combination of Smith and Seger would have rendered claim 17 obvious for the same reasons as explained for claims 2 and 16.

16. Claim 18

184. Claim 18 recites:

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

185. It is my opinion that the combination of Smith and Seger would have rendered claim 18 obvious. Smith teaches "[t]he computer for the business 30 [(*i.e.*, 'first intermediary server')] also communicates with the computer of the [TPPP] 70, the computer for the ODFI 40 and/or the computer for the RDFI via the network [(*i.e.*, "a first digital device")]." (Ex. 1004, [0036]). Smith also discloses that the business 30 "gives the transaction key" to other entities "such as the RDFI or the ODFI." (Ex. 1004, [0041]). Thus, Smith discloses the business computer (*i.e.*, "first intermediary server")

is configured to transmit the transaction key (*i.e.*, "token") to a computer of another entity on the system (*i.e.*, "a first digital device").

17. Claim 19

186. Claim 19 recites:

> 19. The first intermediary server as claimed in claim 16, further configured to:
>
> transmit one or more first requests, each comprising the token, to a second intermediary server in the centralised financial system, via the messaging bus; and
>
> receive one or more first responses from the second intermediary server and transmit the one or more first responses to the first document store.

187. It is my opinion that the combination of Smith and Seger would have rendered claim 19 obvious for the same reasons explained for claims 8 and 16.

18. Claim 20

188. Claim 20 recites:

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

189. It is my opinion that the combination of Smith and Seger would have rendered claim 20 obvious. Seger teaches "the encrypted second information may

include and/or be associated with one or both of know your customer (KYC) data, anti-money laundering (AML) data, and/or other financial data." (Ex. 1005, 8:61-9:4). As the '413 Patent recognizes, at least KYC documents are a type of regulatory compliance documents. (Ex. 1001, 1:37-38 ("…regulatory compliance documents such as KYC documents."). It would have been obvious to a POSITA to apply the teachings of Seger to Smith's system of Smith to allow the businesses and banks connected to the Smith network to share KYC and AML data.

190. KYC and AML checks are important processes that guard against financial crimes. 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). The POSITA would have understood that for the ACH transactions of Smith, in order to process an ACH transfer, the banks or financial institutions involved would have needed to perform such KYC and AML checks to ensure compliance with relevant regulations and safeguard against financial crimes. Thus, the POSITA would have found it obvious and advantageous to combine Seger's teachings regarding sharing KYC and AML data with Smith's system.

191. The POSITA also would have understood that the computer associated with the Automated Clearing House (ACH) in Smith could have been generic to perform many different financial transactions subject to different regulatory compliance checks. Including KYC, AML, and/or other financial data in the records of transactions of the system would have allowed ACH to invoke a corresponding process to authorize, conduct, and validate the requested financial transaction subject to the given regulatory compliance.

C. Ground 2: Claim 3 Would Have Been Obvious Over Smith And Seger, And Further In View Of Yago.

1. Claim 3

192. Claim 3 recites:

> 3. The computer implemented method as claimed in claim 1, further comprising the steps of:
>
> implementing a smart contract at the token server; and
>
> adding the smart contract into the blockchain, from the token server.

193. It is my opinion that the combination of Smith, Seger, and Yago would have rendered this claim obvious.

194. The combination of Smith and Seger discloses transactions involving a blockchain, but does not explicitly disclose "implementing a smart contract" as claimed. However, this claim would have been obvious in view of Yago.

a) implementing a smart contract at the token server; and

195. *First*, Yago discloses "implementing a smart contract." Yago discloses "payment assured contracts" in which a party can "objectively (and automatically), confirm performance by the seller, by [] directly monitoring the CDI network [(*i.e.*, 'blockchain')]." (Ex. 1011, [0047]). A POSITA would have understood a contract as described in Yago to be 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.")).

196. It would have been obvious to a POSITA to combine Yago's "payment assured contacts" with the Smith/Seger system. The motivation to do so would have come straight from Yago's disclosure which teaches creating "contracts that may be automatically enforced, resulting in reduced fraud and counter-party risk when dealing with all different types of CDFI." (Ex. 1011, [0006]). Like Smith and Seger, Yago is related to improving the verifiability of transactions. (Ex. 1011, [0006] ("[A] method is needed which allows for … payments to be tied to mathematically verifiable events"); Ex. 1005, 1:42-46 ("the cryptographic platform enables confidential, verifiable, and immutable recording and/or reporting of information transactions including various encrypted information (e.g., private communications) that may be audited by a third

party."); Ex. 1004, [0014] ("there is a need for a new and improved electronic funds transfer consumer authorization verification system for efficiently proving that a consumer authorized a financial transaction via an ACH network.")). Thus, the POSITA would have looked to the related teachings of Yago for ways to supplement the verification and authentication measures of the Smith/Seger combination and, as described above, would have applied Yago's "payment assured contract" teachings to the system of Smith/Seger.

197. Additionally, the POSITA would have had a reasonable expectation of success in doing so. By the time of the '413 patent, the use of smart contracts in blockchain systems would have been well-known and understood by a POSITA. In fact, the idea of blockchain-based smart contracts had been contemplated in the art since blockchain's beginnings. (Ex. 1012, 29 ("[T]he possibilities for programmable … contracts were baked into the [Bitcoin] protocol at its invention."). Thus, applying the teachings of Yago with the Smith/Seger system would have merely involved combining well-understood technologies yielding predictable results.

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

198. Yago discloses or would have rendered obvious implementing the smart contract "at the token server" and "adding the smart contract into the blockchain, from the token server. 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]).

199. 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.

200. The POSITA would have understood that the "transaction system" of Yago is like the "token server" of the Smith in that it is a central server not affiliated with any party to the smart contract. (Ex. 1004 at [0040]; Ex. 1011 [0065]). Accordingly, the POSITA would have found it obvious that, within the context of the combination described above, the smart contract would have been implemented at, and added to the blockchain by, the token server.

201. Claim 3 therefore would have been obvious over the combination of Smith, Seger.

D. Ground 3: Claim 4 Would Have Been Obvious Over Smith In View Of Seger, And Further In View Of Kurani-274.

1. Claim 4

202. Claim 4 recites:

> 4. The computer implemented method as claimed in claim 1, further comprising the steps of:
>
> transmitting the token from the first intermediary server to a first digital device available with a first user;
>
> providing the token to a second user, by the first user;
>
> providing the token to a second intermediary server in the centralised financial system, from a second digital device;
>
> transmitting the token to a second document store, from the second

intermediary server; and

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

203. It is my opinion that the combination of Smith, Seger, and Kurani-274 would have rendered this claim obvious.

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

204. Smith discloses or would have rendered obvious "transmitting the token from the first intermediary server to a first digital device available with a first user."

205. Smith's system may comprise "one or more suitable business devices [] (e.g., computers, mobile devices)" and that "each entity type may be associated with any number of suitable computers." (Ex. 1004, [0061]). Accordingly, the POSITA would have understood that the business computer (*i.e.*, first intermediary server) may be associated with additional business devices/computers. In particular, where the business computer comprises client/server architecture (as taught and motivated by Seger and described above with respect to element 1 of claim 1), the POSITA would have understood that the business computer's first intermediary server may receive the transaction key (*i.e.*, "token") from the TPPP and then transmit this may transmit the transaction key to a client device of the business (*i.e.*, "first digital device available with

a first user") to facilitate further processing such that the business device may communicate the token to the TPPP.

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

206. Although Smith does not explicitly disclose "providing the token to a second user, by the first user," this element would have been obvious from the teachings of Kurani-274.

207. Smith contemplates sharing transaction information between a customer and a business, but does not provide details of how it would be performed. Smith/Seger and Kurani-274 seek to provide systems for secure financial transactions. (Ex. 1007, 1:20-22 ("[P]rinciples of cryptography are used to create, secure, and transfer MBC directly from a first user to a second user."); Ex. 1004, [0059] ("This environment maintains the highest level of compliance and encryption"); Ex. 1005, 3:6-15 ("…providing a cryptographic platform for exchanging information…"). Similar to the combination of Smith and Seger, Kurani-274 uses a blockchain to record transaction information. (Ex. 1007, 11:6-8 ("The verification information may be published in a chain of transaction (i.e., a blockchain) that is used for further verifications.")). Thus, a POSITA looking to improve upon Smith's system and provide a means for sharing transaction information between a customer and business would look to other systems

like Kurani-274, which identifies a number of ways for customers and businesses to share important transaction information like the transaction key.

208. Kurani-274 discloses that during a transaction, the "token may be transmitted" between a customer and business. (Ex. 1007, 6:9-11). Kurani-274 explains that "the token may be transmitted using optical image methods …, NFC, wireless, Bluetooth, low energy Bluetooth, RFID, hypersonic, Wi-Fi, cellular 3G, 4G, GSM LiFi, etc." (Ex. 1007, 6:12-15).

209. The POSITA would have understood that a straightforward, well-known way for the owner to pass tokens to the receiving party would be through device-to-device transfer, such through personal computers or smartphones. The POSITA would have further understood from Kurani-274's disclosure that the token may be sent from a business device (i.e., "first digital device available with a first user") to a customer device (i.e., "second digital device of a second user").

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

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

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

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

212. Smith discloses or would have rendered obvious "transmitting the token to a second document store, from the second intermediary server." As explained for element 1 of claim 1, Smith discloses a first document store associated with the business for storing transaction information. While Smith does not explicitly disclose a corresponding document store associated with the customer, it would have been obvious to the POSITA for the customer to maintain such a second document store. The POSITA would have found this obvious as a well-known means to store tokens and other transaction data locally so as to "store[] the information for later access" in verification and record-keeping purposes. (Ex. 1004, [0034]).

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.

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

214. It is therefore my opinion that Claim 4 would have been obvious over the combination of Smith, Seger, and Kurani-274.

VI. CONCLUSION

215. 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.