

Amended complaint for patent infringement filed

15 January 2024 - <u>Identitii (ASX:ID8)</u> ('**Identitii'**, '**the Company**') (ASX:ID8) in keeping with usual process, has filed an amended complaint for patent infringement of U.S. Patent No. 10,984,413 in United States District Court for the District of Delaware. The amended complaint is attached to this announcement.

Consistent with messages in the market release on 4 October 2023, the Company is not able to disclose any further details of the amended complaint claim at this time.

This announcement has been authorised for release to ASX by the Company's CEO.

Ends

About Identitii

Identitii powers the way organisations store, transmit and share sensitive data. Our platform has been designed to help organisations reduce the time and cost required to effectively and scalably manage their data compliance needs through collaborative workflows that connect internal teams, customers, partners and industry bodies while enhancing the protection of that data. We built this for the way data should be.

For more information visit: www.identitii.com

Visit Identitii's interactive Investor Hub: If you have any questions about this announcement or any past Identitii announcements, or would like to see video summaries on important announcements, please visit our investor hub at: https://investorhub.identitii.com/



For more information, please contact:

Identitii

Michael Kotowicz

E: investors@identitii.com

P: +61 416 233 145



PUBLIC 2

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF DELAWARE

IDENTITII LIMITED,)
Plaintiff,)
v.) C.A. No. 23-1095-GBW
JPMORGAN CHASE & CO. and JPMORGAN CHASE BANK, N.A.,) JURY TRIAL DEMANDED)
Defendants.)

FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Identitii Limited ("Plaintiff" or "Identitii"), through its attorneys, for its First Amended Complaint against JPMorgan Chase & Co. and JPMorgan Chase Bank, N.A. (collectively, "JPMC" or "Defendants") alleges as follows:

INTRODUCTION

1. This First Amended Complaint arises from JPMC's unlawful infringement of United States Patent No. 10,984,413 (the "'413 patent") owned by Identitii. The '413 patent is attached as Exhibit 1.

THE PARTIES

- 2. Identitii is an Australian public company with its principal place of business located at 388 George Street, Sydney, NSW, Australia 2000. Identitii is the sole owner by assignment of all rights, title and interest in the '413 patent, including the right to recover for past, present and future infringement and damages.
- 3. On information and belief, Defendant JPMorgan Chase & Co. is a corporation organized and existing under the law of the State of Delaware. JPMorgan Chase & Co. is registered

to do business in the state of Delaware and this judicial district. JP Morgan Chase & Co. may be served via its registered agent, The Corporation Trust Company, located at 1209 Orange St., Wilmington, Delaware 19801. JPMorgan Chase & Co. is one of the largest banking institutions in the United States and conducts business in the state of Delaware and this judicial district.

4. On information and belief, Defendant JPMorgan Chase Bank, N.A. is a national bank whose main office is located in Columbus, Ohio, as designated in its Articles of Association with offices in this judicial district. On information and belief, JPMorgan Chase Bank, N.A. is a wholly owned subsidiary of Defendant JPMorgan Chase & Co.

JURISDICTION AND VENUE

- 5. This action arises under the patent laws of the United States, Title 35 of the United States Code. Subject matter jurisdiction is proper in this Court pursuant to 28 U.S.C. §§ 1331 and 1338(a).
- 6. This Court has personal jurisdiction over Defendants in this action because each has committed and continues to commit acts within this District giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over each would not offend traditional notions of fair play and substantial justice. Defendants directly and through subsidiaries or intermediaries, have committed and continue to commit acts of infringement in this District, by among other things, making, using, offering to sell and selling the Accused Instrumentalities, including the Oynx products and services, including "Liink by J.P. Morgan."
- 7. Venue is proper in this Court under 28 U.S.C. §§ 1391 and 1400(b). JPMorgan Chase & Co. resides in this District. JPMorgan Chase & Co. has chosen to incorporate in the state of Delaware, thereby receiving the benefits offered to Delaware corporations.
 - 8. On information and belief, venue is likewise proper for JPMorgan Chase Bank, N.A.,

as it has regular and established places of business in the District. JPMorgan Chase Bank, N.A. has multiple branches throughout this District, including branches in Greenville, Delaware, Newark, Delaware, Middletown, Delaware, and Wilmington, Delaware, including its branch located at 201 N Walnut St., Wilmington, DE 19801.

9. On information and belief, JPMC has committed acts of infringement in this District, including by making, using, selling and offering for sale the Accused Instrumentalities. *See*https://www.jpmorgan.com/onyx/; https://www.jpmorgan.com/onyx/terms of use.htm.

FACTUAL ALLEGATIONS

- 10. Identitii was founded under the name "Sparro" in 2014 and rebranded as Identitii in 2016.
- 11. As explained to JPMC back in June 2016, Identitii is a start-up company focused on helping banks meet their compliance requirements by, among other things, enriching payments with additional information and using tracking tokens and distributed ledger technology (i.e., blockchain) to create a novel payment platform/architecture that solves the challenge of reconciliation of payments. Exhibit 20 at 1. Identitii's mission is to make payments safer for financial institutions, which led to Identitii's inventions, including the use of a token contained within the payment message to create a link to a blockchain based information layer that is interoperable with existing legacy systems. The information layer has multiple features such as, for example, enabling documents to be attached to a payment, enabling access by banks along the transaction chain, enabling secondary identifiers to be attached to a payment to better enable compliance checks and reduce false positives and to create an auditable record of all actors present to the payment and all compliance checks completed in relation to a transaction without exposing the underlying information. Exhibit 20 at 2.

This new architecture, with its enriched data records, helps financial institutions meet compliance requirements as explained in more detail below.

- 12. On August 14, 2015, Identitii filed Australian provisional application 2015903292 (the "Australian Provisional"). The '413 patent claims priority to the Australian Provisional. *See* Exhibit 1.
- 13. JPMC is no stranger to Identitii. Shortly after the filing of the Australian Provisional, JPMC was interested in learning about Identitii's technology. Identitii confidentially provided JPMC information about Identitii's technology, including through a series of slide decks provided by Identitii to JPMC in September 2015, December 2015, June 2016, and July 2016, as well as oral communications. Exhibits 2-5, 22. Identitii explained to JPMC that Identitii's technology was patent pending. Disclosures of at least certain of these materials extended to Naveen Mallela and Elizabeth Polanco Aquino of JPMC.
- 14. On August 12, 2016, Identitii filed PCT Application No. PCT/AU2016/00279, which led to the '413 patent.
- 15. JPMC subsequently began filing patent applications including provisional application 62/414,398 and application 15/797,602 ("'602 application"), naming Mallela and Aquino as inventors. During prosecution of JPMC's '602 application, the pending claims were rejected over Identitii's U.S. Pub. No. 2018/0247302, which is the U.S. Patent Office's publication of Identitii's application that issued as the '413 patent.
- 16. JPMC also filed provisional application 62/523,429 and application 16/015,709 with Aquino as a named inventor.
 - 17. Identitii's '413 patent issued on April 20, 2021. Exhibit 1.

- 18. Shortly thereafter, in September 2021, Identitii approached JPMC's Umar Farooq to discuss JPMC's infringement of the '413 patent.¹ A slide deck was provided. Exhibit 6. JPMC responded to Identitii's charge of infringement by denying infringement, but never articulated any basis for its position.
- 19. In April 2022, Identitii's CEO John Rayment called JPMC's Umar Farooq to discuss JPMC's need to take a license due to its infringement of the '413 patent. JPMC declined any interest in a license, yet never provided any reason why it believed it was not liable.
- 20. Left with no other option, Identitii was forced to file this suit to protect its intellectual property and remedy JPMC's willful infringement.

BACKGROUND OF THE '413 PATENT

21. At the time of the invention of the '413 patent, existing technology and infrastructure for executing financial transactions between banks and other institutions suffered from numerous problems. For example, the Society for Worldwide Interbank Financial Telecommunications (SWIFT)² was (and still is) the main network for executing financial transactions between banks around the globe. SWIFT provides one of the largest worldwide financial messaging systems for financial institutions to send and receive information to support global payment orders. SWIFT's key characteristics are standardized messaging and a relatively secure network. Exhibit 7 at 22. SWIFT, however, is a legacy payment processing technology and architecture that suffers from numerous drawbacks and inefficiencies, especially in light of the ongoing regulatory developments around Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF). *Id.* at 23. In addition, at the time

¹ Mr. Farooq's bio indicates that he works for JPMorgan Chase & Co. and that he is "CEO, Oynx by JP Morgan," which, on information and belief, is a division of JPMorgan Chase Bank, N.A. Exhibit 21.

² Other existing networks include Automated Clearing House (ACH) and Real Time Gross Settlement (RTGS.) Exhibit 1, '413 patent, 26:49.

of the invention, the SWIFT protocol only supported the transmission of fixed-width messages with limited information. Exhibit 1, '413 patent, 26:1-2.

- 22. As explained in the '413 patent, it is difficult to keep track of the plurality of data during a financial transaction and it is even more difficult to ensure that integrity of the plurality of data is maintained either during or after the financial transaction has been completed or to confirm that the data existed at a certain point in the financial transaction process. Exhibit 1, '413 patent, 1:39-43. In addition, at the time of the invention, systems like SWIFT supported only one-way transmission of the plurality of data in any given financial transaction such that if it is later discovered that there are deficiencies in the plurality of data being transmitted, there was no support in the network architecture for confirming or requesting additional data for the transaction as the transaction is being processed. Exhibit 1, '413 patent, 1:44-51. Thus, because of the lack of secure storage and transmission in conventional payment rails, financial transactions cannot be effectuated efficiently and may fail. *Id.* This is an increasing concern, as payment regulations and requirements are now oft changing to become more complex and sophisticated in view of, for example, money laundering and terrorism financing concerns.
- 23. The drawbacks and inefficiencies of SWIFT and other comparable messaging systems relate primarily to an outdated architecture which was developed in the 1970s. SWIFT serves "the financial services sector as [the] proprietary communications platform" and "forms a core part of the financial services infrastructure." *The Society for Worldwide Interbank Financial Communications* (SWIFT), Susan V. Scott and Markos Zachariadis, 1st edition, 2013, at p. 1. It has been described as the "internet for financial services" and the "transport network for a large number of major payment and securities infrastructures." *Id.* SWIFT "is responsible for providing the network, standards, products and services that allow member institutions to connect and exchange financial information."

Id. at p. 2.

- 24. SWIFT's messaging format at the time of the invention and today—MT103—"limits the amount of information that can be sent to banks, given the original messaging systems were not designed to cater to much larger bandwidths needed for richer underlying data sets." Exhibit 7 at 23. Identitii explained this drawback of SWIFT to JPMC when it explained its invention to JPMC. Exhibit 4 at 3; Exhibit 20 at 3 of presentation.
- 25. The lack of supporting information regarding payments sent through SWIFT causes problems with the entire infrastructure. Exhibit 1, '413 patent, 21:57-22:9. Many transactions and transfers go through numerous banks prior to reconciliation as demonstrated below:

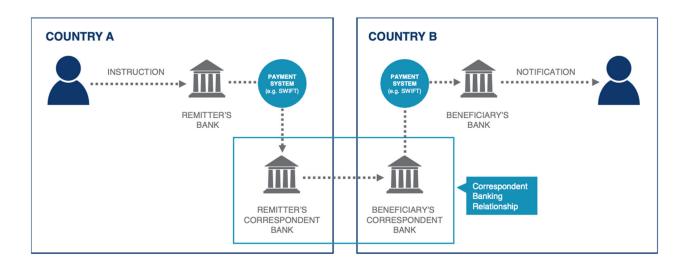


Exhibit 7 at 5.

26. The conventional payment processing infrastructure used the SWIFT messaging system, architecture and format to process transactions like the one depicted above. A fundamental problem with this architecture is that many transactions like the one depicted above cannot be cleared using SWIFT alone and are extremely labor intensive. *See*, *e.g.*, Exhibit 7 at 18; Exhibit 1, '413 patent 1:25-51; 21:25-22:24. Banks are required to comply with numerous regulations such as Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) regulations. *See*, *e.g.*, Exhibit 7 at 4.

Given SWIFT's legacy architecture and conventional messaging structure, compliance with these regulations is often not possible. *Id.* Financial institutions must implement Know Your Customer (KYC) processes and conduct further diligence regarding transactions like the one above to clear and settle a transaction. Systems and architectures like SWIFT do not provide a mechanism for doing this. *Id.* Rather, the various financial institutions must request additional information and communicate directly with each other—often outside of SWIFT—in order to facilitate the processing of the payment transactions, making it difficult for banks to conduct risk-based analysis of individual payments. Exhibit 7 at 22-23.

27. The following describes certain issues with the SWIFT architecture (Exhibit 7 at 23):

Notwithstanding the widespread adoption of messaging systems such as SWIFT, we see a number of limitations associated with the current global payments infrastructure, especially in light of ongoing regulatory developments around AML/CTF:

- 1. Limited information capture: while the industry is embracing the ISO20022 XML messaging standard, SWIFT's current 'MT' messaging format (e.g. MT103) limits the amount of information that can be sent between banks, given the original messaging system was not designed to cater to much larger bandwidths needed for richer underlying data sets.
- 2. Lack of interoperability between banks' backend systems: the lack of standardisation in banks' back-end operating systems means that the much richer data set required to comply with increasing AML regulations cannot be effectively shared between banks.
- 3. Parties are difficult to identify: other than the remitter and beneficiary's own banks (i.e. the banks that have the direct, onboarded relationships), other banks along the correspondent banking value chain may not know the true identity of the transacting parties, including any ultimate benefifcial owners. However, they are still required to comply with KYC, CTF and AML regulations.

- 4. No straight-through-processing (STP): pretransaction checks require manual review of information against a bank's own data sets (e.g. sanction and PEP lists), inhibiting the ability to conduct straight-through-processing (STP). These manual processes result in considerable time delays for international money transfers.
- 5. Capacity for information to be altered/ incorrect/missing: payments can still be processed when information contained within the payment instruction is missing, incorrect or even altered. The ability to forge SWIFT messages saw Bangladesh's central bank hacked for USD 81 million in early 2016.¹¹
- 6. Time-limited information capture: SWIFT only stores messages for a period of 180 days. Given banks are required by regulators to store transaction data for a period of up to five years, they must rely on their own data storage and retrieval systems.

In the next part of this report we will examine the emerging role of blockchain technology in the global payments system.

- 28. In addition to the drawbacks with respect to SWIFT, financial institutions also faced significant challenges with respect to receivables matching and reconciliation, resulting from disconnects between a payment and the invoice/remittance information because, for example, while invoices may often by emailed or posted to a customer, the invoice numbers are not always included in the return payment and using the invoice amount alone is not reliable as a reconciliation key. These disconnects lead to significant inefficiency.
- 29. At the time of the invention, the inventors envisioned using blockchain technology with global payment systems. Exhibit 1; Exhibit 7 at 24-26, 33-35. Blockchain is a type of distributed

ledger database that records and maintains a constantly growing list of transactions into sequential blocks. The transactions using blockchain are encrypted and stored in linked blocks, creating a cryptographic audit trail that cannot be changed or deleted. As a result, those with access to the network have access to a shared, single source of truth. *Id*; Exhibit 1, '413 patent, 12:65-13:8; 25:14-46; Figure 15.

- 30. In addition, industry analysts back in November 2016 after the filing date of the '413 patent, saw huge potential in the immediate-term use of blockchain to run alongside and hence modernize legacy payment and messaging infrastructure, overlaying existing systems with a rich information layer—including specifically, Identitii's inventive solution that was patent pending at the time. Exhibit 7 at 26, 33-35. "By attaching more detailed information to each transaction or payment instruction (e.g., legal entity information, ultimate beneficiary owner) blockchain technology could help reduce the current high false positive rates (currently 99.9%) for suspicious transactions, helping banks to conduct KYC checks at the transaction level (i.e., know your transaction.)" *Id.*; Exhibit 1, '413 patent, 12:19-38; 15:57-16:3. Finally, "the distributed ledger would also act as an effective means of recordkeeping for audit purposes, given the data is both irrefutable and immutable." *Id.*
- 31. Identitii explained these same drawbacks with SWIFT and other architectures to JPMC:

identitii is helping financial institutions to address information challenges caused by ageing legacy payment & bank systems

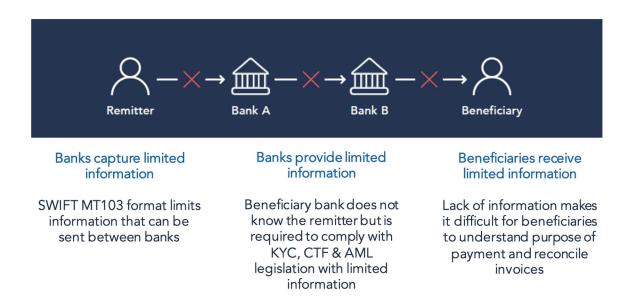


Exhibit 4 at 3. Exhibit 20 at page 3 of the presentation.

- 32. Identitii reimagined an architecture to eliminate these problems as described in the '413 patent's specification and as claimed in, for example, claim 15. The revamped architecture uses a tracking token to provide a robust information layer over existing payment systems like SWIFT to enrich payments with supporting information that is accessible at each step of the payment process, enabling banks to clear transactions more quickly and reliably with greater security because the use of blockchain allows for certainty of data that can be viewed at any point in time during the transaction and is verifiably linked to the underlying participants in the transaction. The token likewise provides for access to information in the blockchain regardless of the legacy system being used, making this "interoperability" a unique feature of the '413 patent as well. Exhibit 1, '413 patent, 25:1-13. Finally, the use of a token enables better straight through processing of financial transactions by reducing exceptions and false positives.
 - 33. The innovative architecture covered by claim 15 is depicted, among other places, in

Fig. 14, industry publications, and Identitii's presentations to JPMC:

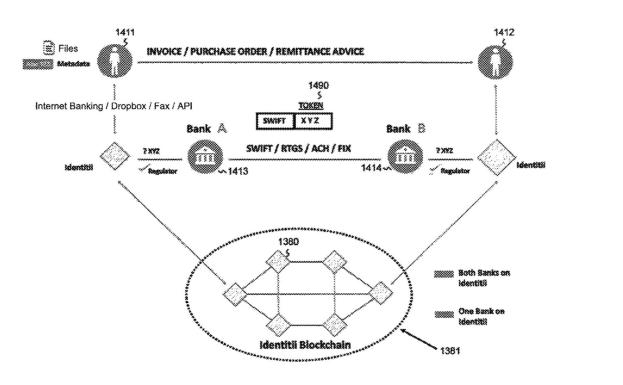


Exhibit 1, '413 patent, Fig. 14.

FIGURE 15: IDENTITII TOKENS

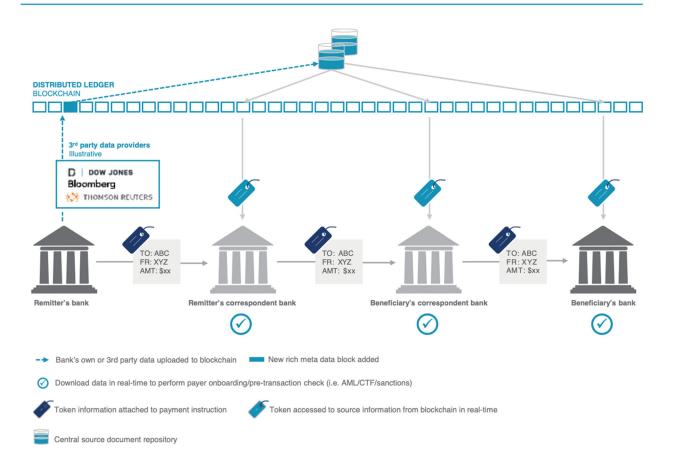


Exhibit 7 at 34.

identitii's receivables product provides a low touch solution requiring limited change to workflow

Illustrative workflow

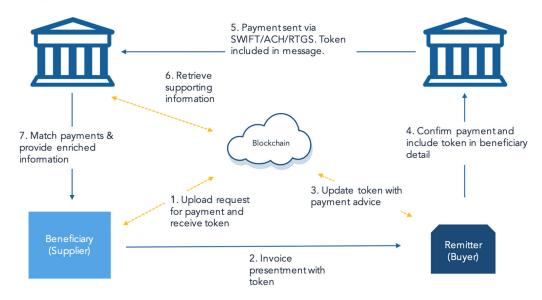


Exhibit 4 at 9.

34. In accordance with the claimed invention, Identitii invented a system that generates an enriched data record from documents regarding a financial transaction and that enriched data record is inserted on a blockchain. Exhibit 1, '413 patent, claim 15. The additional information is used to enrich payments with more information given the inability of existing payment systems such as SWIFT to communicate enriched information. *Id.* at 26:34-38. The system also generates a token associated with the enriched data record and that token is stored in the blockchain in association with the enriched data record. *Id.* at 13:9-14. The token provides a pointer to the enriched data record in the blockchain and can be used to retrieve the enriched data record at, for example, the time of an audit. *Id.* at 2:12-15; 16:1-3; 22:45-57; 22:61-67; 23:19-29; 23:66-24:2; 28:66-29:7. The purpose of storing the token only in the blockchain is to both de-identify the information in the blockchain (which is critical for banks) and enable use of existing SWIFT/ACH/RTGS or new messaging systems to send the payment information in tokenized format. *Id.* at 26:46-50. The system leverages blockchain

and tokenization technology to create an unconventional architecture that is a departure from prior architectures like SWIFT. Now banks can use the tokens and enriched data records by directly accessing the blockchain which is centralized as opposed to having to contact numerous other banks about a transaction depending on the number of financial institutions that are involved. The financial institutions involved in the financial transaction may communicate in real-time and ensure, for example, that the payer, the beneficiary and all the parameters corresponding to the financial transaction are validated. *Id.* at 31:46-50.

35. Identitii's unconventional architecture created numerous technological advances and benefits as explained in the '413 patent (*see*, *e.g.*, Exhibit 1, '413 patent, 31:36-57), industry publications and as Identitii explained to JPMC:

REAL-TIME KYC

The protocol envisaged would have the ability for feeds from third party data providers to be accessed as changes occurred, so that the correspondent/ beneficiary bank is also able to gain access to the most up-to-date data, such as changes to a remitting company's ultimate beneficial owner or even data about a fellow bank further down the payment chain.

STRAIGHT THROUGH PROCESSING

In the fully integrated version of identitii's technology, integration with a bank's systems would mean that downloaded data can be fed directly into a bank's compliance engines, including KYC/customer due diligence, fraud monitoring, sanctions screening and AML systems. Such solutions are very compelling for the banks as they offer straight through processing, doing away with much of the manual collection and review of documentation that is currently required at each stage along the global payment transaction process to satisfy compliance obligations.

The reduced time and cost that straight through processing offers can reduce the operating costs of banks, and provide peace of mind as knowing the nature of the transaction will allow banks to maintain and re-establish their correspondent bank relationships, opening up more revenue opportunities.

Exhibit 7 at 35.

END USER BENEFITS

Access to a rich dataset opens up the payment system to further commercial advantages for endusers (i.e. customers, for example, can experience real-time tracking of payments and easier matching of invoices to payments).

FUTURE AGENCY MODEL?

As richer information is built up in robust and centralised repositories and as KYC/CTF regulation becomes more sophisticated, we believe that we may move to the point where any KYC, sanctions & CTF checks performed by other parties along a global payment process would be accepted bona fide by the legal and regulatory requirements in different jurisdictions where the banks are domiciled or operating, thereby reducing the duplicative compliance processes that are commonplace today.

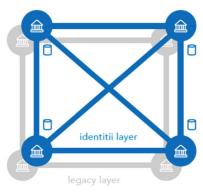
Currently, over 11,000 financial institutions use SWIFT, one of the most popular payment messaging systems for international payments. identitii has focused on ways to enhance the relatively stable and robust nature of such existing financial markets infrastructure. The payload of the rich data remains on the distributed ledger and centralised repositories such that the legacy infrastructure is not overloaded. We believe that by overlaying a richer data layer onto proven systems like SWIFT through their token technology, this will allow for much greater adoption and likelihood of becoming a global standard. At the same time, the intra-operability of their technology means that it can also be used in conjunction with emergent cross-border payments systems being developed by players such as Ripple.

FIGURE 11: ILLUSTRATIVE REMITTANCE PROCESS

COUNTRY A COUNTRY B COUNTRY A COUNTRY B COUNTRY B COUNTRY A COUNTRY B COUNTRY A COUNTRY B COUNTRY A COUNTRY B One payment instruction shared between all 'nodes', serving as a single source of truth Share of information (including direction of information sharing) No share of information

Exhibit 7 at 25.

identitii's patent pending tokens use a private blockchain to create a single source of truth for banks



Exchange of trusted information

Allows banks to share compliance checks without sharing underlying data

Interoperability between legacy systems and blockchain

API driven architecture allows for simple integration

Irrefutable and immutable

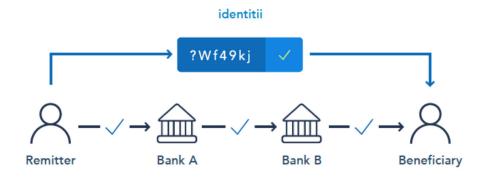
The identitii blockchain creates a record of AML & CTF checking that is tamperproof

Decentralised and resilient

The identitii blockchain is resilient by not requiring a centralised store of information

Exhibit 4 at 3.

identitii has developed a token that links legacy systems to provide the "who, what and why" for every transaction



identitii's tokens allow customer to attach documents to payments

Reducing operational costs from manual document handling

identitii's tokens allow banks to retrieve enriched information about payments

Reducing risk of fines for noncompliance and eliminating headcount due to reduction of manual investigations identitii's tokens connect the payment with the purpose

Increasing revenue from new products including receivables reconciliation & financing

Exhibit 4 at 4.3

identitii's tokens can enrich payments with information to solve multiple issues for banks

Problem		Solution	
1.	Correspondent banks have limited information about payment & must other banks to be KYC, AML & CTF compliant	1.	Attach risk rating to payment & auditable log of compliance checks completed on customer & payment, without exposing information
2.	Inability to attach purpose of payment documentation to payment results in manual investigation and processes	2.	Attach purpose of payment documentation directly to a payment for clearance by an operator
3.	Different payment messaging formats limit compatibility and straight through processing	3.	Attach multiple payment formats to MT103 message

Exhibit 4 at 15.

36. The '413 patent identifies the problems with legacy architectures and the benefits of Identitii's claimed solutions. *See*, *e.g.*, Exhibit 1, Figs. 8, 11, 13; 1:27-54, 24:36-25:13, 26:1-33; 28:31-39; 28:44-60; 31:38-57.

37. The industry recognized Identitii's novel architecture. SWIFT itself acknowledged the innovative architecture as Identitii won the 2016 SWIFT Innotribe⁴ Compliance Challenge based on its new patented architecture. Exhibit 7 at 33; Exhibit 8; Exhibit 9. Just after winning the SWIFT Innotribe award, Identitii demonstrated its new architecture to JPMC, including setting up and settling transactions using the system. Identitii's novel architecture also led to it being named as one of

³ As stated in the specification, the inventions of the '413 patent apply to processing financial transactions between different financial institutions and/or different branches of the same financial institution. Exhibit 1, '413 patent, 10:58-65; 31:38-45; 24:36-41; 24:60-63; 26:1-6.

⁴ Innotribe is SWIFT's innovation arm: https://www.swift.com/about-us/innovate-swift/innotribe.

KPMG's 2016 Fintech100 Emerging Stars. Exhibit 7 at 33.

- 38. The Patent Office found that Identitii's claimed architecture was novel over, among other things, the disclosures of the Bitcoin whitepaper, which is the original thesis paper written in 2008 that set forth the structure of the Bitcoin network—a blockchain based payment system that has achieved great notoriety. Exhibit 1 at References Cited, Other Publications.
- 39. JPMC, which uses Identitii's patented technology, has expressly recognized the novel architecture by advertising Oynx/Liink, the infringing services it offers. For example, on its website, JPMC states "Formed in 2020, Oynx has pioneered the world's first bank-led blockchain platform for the exchange of value. information and digital assets." https://www.jpmorgan.com/onyx/index.htm. JPMC also states on its website: "Onyx by J.P. Morgan is at the forefront of a major shift in the financial services industry. We are the first global bank to offer a blockchain-based platform for wholesale payments transactions, helping to re-architect the that information moving around the world." way money, and assets are https://www.jpmorgan.com/onyx/about. JPMC says this is "Transforming the future of banking." *Id.* JPMC makes numerous other similar statements on the same page:
 - "Who we are . . . Oynx has pioneered the world's first block-chain based platform for wholesale payment transactions, helping to transform the way that money, information and assets are moving around the world."
 - "We are innovators who have cultivated a deep understanding of institutional banking and technology to create <u>reliable infrastructure</u> and services for the world's most pressing problems – starting . . . payments and information sharing within banking."

• "Why blockchain innovation . . . We use technology to large institutions, corporations and fintechs who are interested in leveraging innovative technology solutions to help solve real-world business problems at scale. We have re-architected the infrastructure of value transfer, using intelligent, real-time networks to help unlock the potential of distributed ledger technology."

See id.

- 40. In a video on JPMC's website concerning the infringing Liink platform, JPMC states that the architecture of the platform "enables seamless and secure information exchange for account validation, fraud prevention, and even faster payment processing." *See* video at https://www.jpmorgan.com/onyx/liink.
- 41. In another video on JPMC's website, Onyx: Unleash the Power of Tokenization, JPMC asks "Why Tokenize?" and answers its question: "You get the advantages of speed, security, and ease of transfer intended to improve upon legacy processes and systems." Exhibit 22. In the video, JPMC also touts that the Onyx platform is "built on our blockchain infrastructure, network and managed services, so you don't have to." https://www.jpmorgan.com/onyx/onyx-digital-assets. *Id*.
- 42. JPMC has also touted its use of Identitii's patented architecture on television. Speaking to Bloomberg live from the Singapore Fintech Festival in 2023, Umar Farooq, JPMC's head of the infringing Onyx and Liink platforms stated: "I think the kernel of our thinking is that if you think about how infrastructure has evolved in financial markets, you have securities as one infrastructure, you have money as a different infrastructure, you have commodities as a third infrastructure, the list just goes on. And I think block-chain tech actually gives us the opportunity to rewrite the infrastructure potentially as a consolidated one with consolidated data structures like tokenization and I think that can unlock potential and how markets work, how money moves, and

frankly create a ton of value for customers, whether they are bank customers or otherwise, and so I think this can really rewrite how financial markets will work in the future." Exhibit 14 (video from Bloomberg); see also Exhibit 15.

- 43. All of the foregoing statements by JPMC (1) evidence the novelty of Identitii's patented architecture; (2) acknowledge that Identitii's patented architecture is a departure from convention; and (3) confirm that Identitii's patented architecture is a technological solution to multiple problems with computer-based execution of financial transactions. Numerous industry publications have confirmed the foregoing as well in papers and articles since 2020. Exhibits 10-13. JPMC thus recognizes the advancement in technology achieved by Identitii's patented architecture.
- 44. JPMC has made numerous statements to the Patent Office—in connection with its own patent applications with priority dates after the '413 patent—about the patentability of block-chain based technologies used to execute and secure financial transactions. Exhibits 16-17. Each of these arguments resulted in issued patents. Exhibits 18-19.
- 45. In light of the foregoing, and the relevant timeline (depicted below), Identitii was the first to develop a blockchain based, tokenized payment architecture that JPMC is now using and acknowledges is revolutionary.

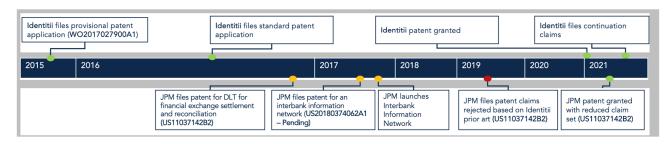


Exhibit 6 at 3.

FIRST COUNT

(INFRINGEMENT OF U.S. PATENT NO. 10,984,413)

46. Identitii incorporates by reference the foregoing paragraphs as if fully set forth herein.

- 47. Identitii owns by assignment, all rights, title and interest, including the right to recover damages for past, present and future infringement, in U.S. Patent No. 10,984,413 titled "Computer Implemented Method for Processing a Financial Transaction and a System Therefor." The '413 patent is valid, enforceable, and was duly and legally issued by the United States Patent and Trademark Office on April 20, 2021.
- 48. On information and belief, Defendants—i.e., JPMorgan Chase & Co. and JPMorgan Chase Bank, N.A., both individually and collectively—have directly infringed and continue to directly infringe one or more claims of the '413 patent, including at least claim 15 of the '413 patent in this District and elsewhere in the United States by, among other things, making, using, selling, offering for sale, and/or importing into the United States instrumentalities and services that embody the inventions claimed in at least claim 15 of the '413 patent (the "Accused Instrumentalities") in violation of 35 U.S.C. § 271(a). The Accused Instrumentalities, include, but are not limited to, Defendants' Onyx products and services (e.g., Liink), as well as all reasonably similar products and/or services. For example, on information and belief, JPMorgan Chase Bank, N.A. makes, assembles, implements, deploys, hosts, uses, operates, offers for sale, sells and controls the network architecture and services of its including, Onyx products and services, e.g., Liink. https://www.jpmorgan.com/onyx/terms of use.htm.
- 49. As another example, JPMorgan Chase & Co. offers for sale the Accused Instrumentalities in the United States, including via advertisements and offers on the Onyx website.

Copyright © 2023 JPMorgan Chase & Co. All rights reserved.

See, e.g., https://www.jpmorgan.com/onyx/liink;

https://www.jpmorgan.com/onyx/terms of use.htm.

Copyright Notices

Any works of authorship contained in this Website, including but not limited to all site design, text, and images, are owned, except as otherwise expressly stated, by JPMorgan Chase & Co. or one of its subsidiaries. Except as otherwise expressly stated herein, they may not be copied, transmitted, displayed, performed, distributed (for compensation or otherwise), licensed, altered, framed, stored for subsequent use, or otherwise used in whole or in part in any manner without prior written consent, except to the extent permitted by the Copyright Act of 1976 (17 U.S.C. § 107), as amended, and then, only with notices of the owner's proprietary rights. You may download or export records of Communications made via the Website that you are a party to.

See, e.g., https://www.jpmorgan.com/onyx/terms of use.htm.

50. JPMorgan Chase & Co. and JPMorgan Chase Bank, N.A., individually and collectively, market and offer for sale the Accused Instrumentalities in the United States.

J.P. Morgan, JPMorgan, JPMorgan Chase and Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its subsidiaries worldwide (collectively, "JPMC"). Products or services may be marketed and/or provided by commercial banks such as JPMorgan Chase Bank, N.A., securities or other non-banking affiliates or other JPMC entities. JPMC contact persons may be employees or officers of any of the foregoing entities and the terms "J.P. Morgan", "JPMorgan", "JPMorgan Chase" and "Chase" if and as used herein include as applicable all such employees or officers and/or entities irrespective of marketing name(s) used. Nothing in this material is a solicitation by JPMC of any product or service which would be unlawful under applicable laws or regulations.

https://www.jpmorgan.com/onyx/documents/Confirm-Accelerate-transactions-processing-with-global-account-validation.pdf.

51. JPMC's Onyx Liink, for example, is a "peer-to-peer network for secure, privacy-preserving information exchange." The image below is excerpted from JPMC's website.

LIINK

Unleash the power of the world's first bank-led, peer-to-peer network for secure, privacy-preserving information exchange.

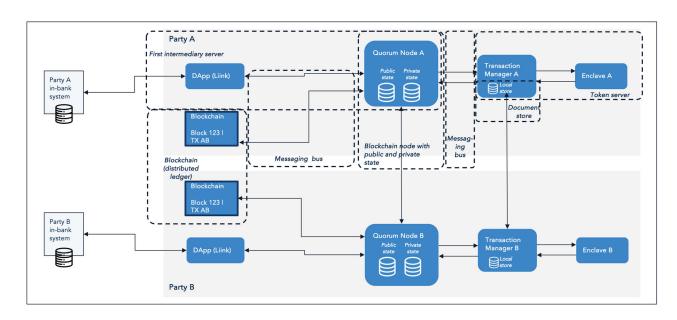
See, e.g., https://www.jpmorgan.com/onyx/liink.htm

52. JPMC has stated that Liink provides JPMC's customers "access to a blockchain network [and] hosting infrastructure." *See*, *e.g.*, *id.* JPMC has also stated that the Liink blockchain network is "a permissioned blockchain based on the Quorum protocol in use by JPMorgan Chase to process payments." *See*, *e.g.*,

https://www.jpmorgan.com/content/dam/jpm/cib/complex/content/technology/publications/qkd-research-prototype-project-5-1.pdf. According to JPMC, it developed and launched one of the largest blockchain networks of banks in the world, allowing entities to share data using blockchain nodes. *See, e.g.*, https://www.youtube.com/watch?v=_0GvIhEybIQ. According to JPMC, Liink is "a secure, private, permissioned, blockchain-based network." *See, e.g.*,

https://www.jpmorgan.com/onyx/content-hub/confirm-for-financial-institutions.htm.

53. JPMC's Liink architecture is illustrated below. Particularly, each of the items in the "Party A" and "Party B" boxes (e.g., the blue boxes) are part of JMPC's Liink architecture (e.g., "DApp," "Quorum Nodes," "Transaction Managers," "Enclaves," and "Blockchains.") JMPC makes, assembles, implements, deploys, hosts, uses, operates, offers for sale, sells and controls this network architecture. As illustrated below, the Accused Instrumentalities are, on information and belief, communicatively connected to a party's internal system, such as a bank's in-bank system.



54. On information and belief, as illustrated above, one using the Liink system (e.g., JPMC or a third party bank), accesses/uses the JPMC network architecture and functionality of the Accused Instrumentalities which include a DApp (e.g., Liink DApp), a node, (e.g., a Quorum node), a transaction manager, an enclave, and a blockchain. These components of the Accused Instrumentalities are shown, for example, in Quorum's Transaction Processing documentation⁵:

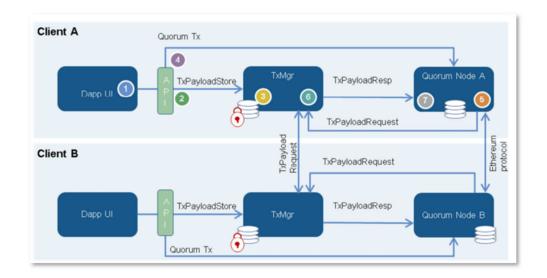
⁵ Available at https://github.com/ConsenSys/quorum/wiki/Transaction-Processing/9637df4934995acbd81948e28501fcd5f9b7df83 (last visited January 11, 2024).

Party A 9.TxPayloadRequest 3&10.En/decryption 2.TxPayloadStore request 1.Private Tx AB Dapp Enclave A Manager A 6.Tx Hash 4&11.Tx Response 8.Block w/ Tx AB locol 12.TxPayloadResp (Tx Payload) Ε Party B 7.Ethere 5.TxPayle Ethereur 9.TxPayloadRequest 10.En/decryption request Quorum Node B Transaction Enclave B Manager B 11.Tx Response xL mn 12.TxPayloadResp 8.Block w/ Tx AB (Tx Payload)

Below is a description of how Private Transactions are processed in Quorum:

- 55. The image above was generated and/or circulated by JPMC.
- 56. The components of the Accused Instrumentalities are further shown, for example, by Quorum's Whitepaper:⁶

⁶ Available at https://www.blocksg.com/single-post/2017/12/27/quorum-whitepaper (last visited January 11, 2024).



- 57. These components are also shown in documentation from an interview with Mr. Umar Farooq describing JPMC's IIN network.⁷ On information and belief, JPMC's IIN network is a prior name for Liink. *See, e.g.*, https://www.businesswire.com/news/home/20201027006268/en/J.P.-Morgan-Adds-New-Features-to-Newly-Branded-Liink%E2%84%A0.
- 58. As discussed above, on information and belief, JPMorgan Chase Bank, N.A. makes, assembles, implements, deploys, hosts, uses, operates, offers for sale, sells and controls its Onyx network infrastructure including the infrastructure of JPMC's Liink products and services. Further, on information and belief, JPMorgan Chase & Co. and JPMorgan Chase Bank, N.A. individually and collectively, make, use, offer for sale and sell the Accused Instrumentalities in the United States.
- 59. The Accused Instrumentalities meet every limitation of one or more claims of the '413 patent, including, e.g., claim 15 of the '413 patent, which recites:

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

- a first intermediary server in a centralised financial system, the first intermediary server being operably connected to a network and a first document store;
- a token server operably connected to the network;

⁷ Available at https://medium.com/@AzamShaghaghi/future-payments-the-blockchain-enabled-network-by-j-p-morgan-2a86ce2cab0d (last visited January 11, 2024).

a messaging bus in the centralised financial system, the messaging bus being operably connected to the network; and

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

wherein the first intermediary server is configured to:

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

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

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

transmit the token to the first document store;

wherein the token server is configured to:

generate the token and add the token into the blockchain in association with the enriched data record; and

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

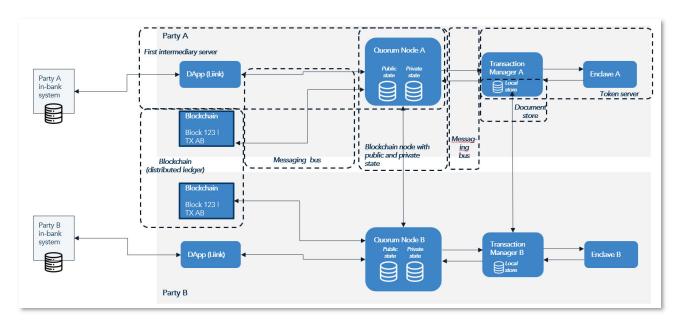
60. To the extent the preamble is limiting, the Accused Instrumentalities are a system for processing a financial transaction. As an example, the Accused Instrumentalities are used to validate transaction information for processing a transfer of funds, as shown in the image below. The image of this paragraph is an excerpt from JPMC's website. JPMC maintains this website and the information displayed thereon in the ordinary course of its business.

Confirm by Liink

Validate account information prior to payment initiation easily, quickly and securely

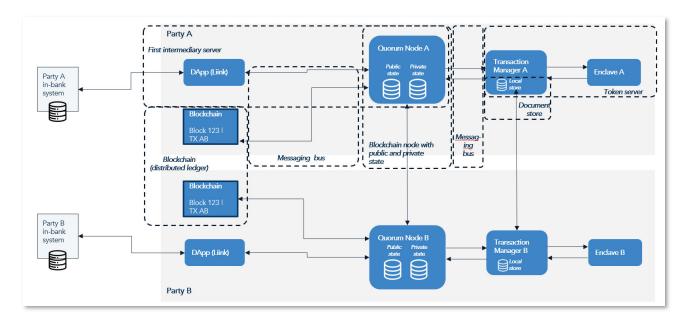
See, e.g., https://www.jpmorgan.com/onyx/confirm.htm; see also https://www.jpmorgan.com/onyx/check-match.htm; https://www.jpmorgan.com/onyx/route-logic.htm

61. The Accused Instrumentalities include a first intermediary server in a centralized financial system, the first intermediary server being operably connected to a network and a first document store. For example, the Accused Instrumentalities include a node for an entity such as a bank that is a participant in the network of the Accused Instrumentalities. As an example, JPMC maintains a Quorum node. A Quorum node is a blockchain node. A Quorum node associated with Liink is associated with a bank. The Accused Instrumentalities include "DApp (Liink)." The Accused Instrumentalities include at least one "Quorum Node." DApp (Liink) and a "Quorum Node" constitute a first intermediary server.



- 62. JPMC's documents further show the first intermediary server. *See, e.g.*, US Pub. No. 2018/0374062, at ¶ 5, Claim 1, Fig. 3 (describing and illustrating a "bank node" coupled to an inbank system).
- 63. The first intermediary server is operably connected to a network and a first document store. For example, the first intermediary server described above is connected to JPMC's Liink-

related network and, via the network, a document store (e.g., a database for storing documents pertaining to the transaction). On information and belief, the Accused Instrumentalities connect to and share bank private database information which contains, e.g., transactional and/or customer information. Link includes a "transaction manager." Such information is stored in a document store, such as, e.g., a "local store" of a transaction manager of the Accused Instrumentalities.



- 64. The Accused Instrumentalities include a token server operably connected to the network. As discussed in more detail below, the Accused Instrumentalities generate a token. That token is generated by a token server (e.g., an enclave and/or a transaction manager as illustrated above). As illustrated above, both the enclave and transaction manager are connected to the network to communicate with other portions of the Accused Instrumentalities' system.
- 65. The Accused Instrumentalities include a messaging bus in the centralized financial system, the messaging bus being operably connected to the network. For example, the components of the Accused Instrumentalities are communicatively coupled to the network to transfer messages (e.g., information associated with the transaction). For example, the first intermediary server (e.g., the node) is coupled to the network via a messaging bus.

66. The Accused Instrumentalities include a blockchain operably connected to the network, such as the blockchain shown above. A blockchain is a distributed ledger. The blockchain of the Accused Instrumentalities is a distributed ledger.

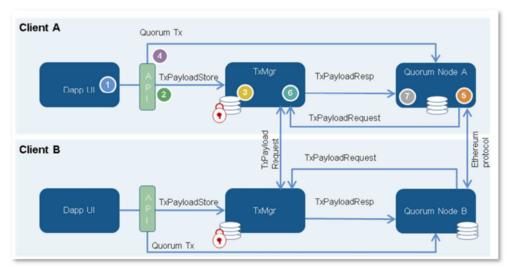


Network Infrastructure

Build applications using a secure technology stack providing access to a blockchain network, hosting infrastructure, tools and integrations to quickly bring use cases to life

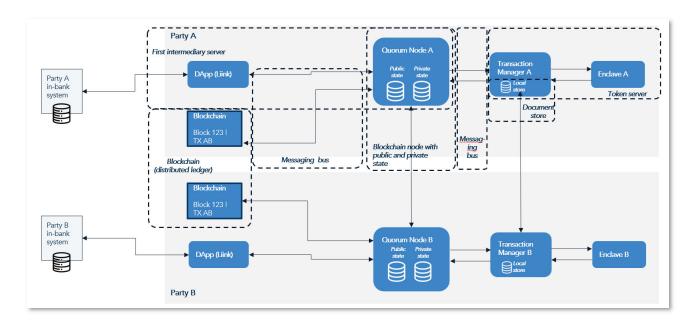
See, e.g., https://www.jpmorgan.com/onyx/liink; see also US Pub. No 2018/0374062 at ¶¶ 30-33.

- 67. The first intermediary server is configured to transmit one or more documents pertaining to the financial transaction, to the first document store. As an example, Liink's DApp, together with a Liink Quorum node associated with an entity such as a bank is configured to transmit documents required for the transaction (e.g., "transactional, customer and PI [i.e., personal information] data") to the document store (e.g., the document store of the transaction manager). *See*, e.g., JPMC's US Pub. No. 2018/0374062, at, ¶33, Fig. 3. For example, the one or more documents may include details of the transaction as well as information to validate the financial transaction. *See*, e.g., https://www.jpmorgan.com/onyx/confirm.htm; see also https://www.jpmorgan.com/onyx/check-match.htm; https://www.jpmorgan.com/onyx/route-logic.htm. As an example, the documents are sent from the Liink Quorum node to the Liink transaction manager to facilitate managing a transaction.
- 68. The first intermediary server is configured to generate an enriched data record from the one or more documents. As an example, the accused first intermediary server generates a transaction payload:

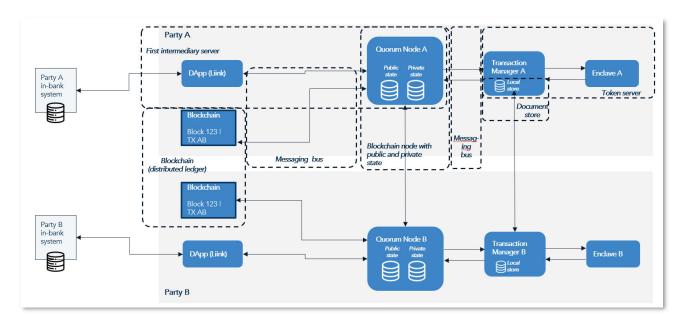


https://www.blocksg.com/single-post/2017/12/27/quorum-whitepape

- 69. On information and belief, DApp and node generate an enriched data record using the information from the one or more documents discussed above for storage in the blockchain. On information and belief, the enriched data is information extracted or otherwise gathered or obtained from the documents. Additionally or alternatively, the data of the documents is encrypted (e.g., hashed) to create the enriched data record. *See, e.g.*, JPMC's US Pub. No. 2018/0374062 at Figs. 7, 8 (showing a "payment message" including payment and personal information, which is encrypted). The information from the one or more documents must be hashed or otherwise encrypted to be placed on the blockchain.
- 70. The first intermediary server is configured to add the enriched data record into the blockchain. For example, the Liink DApp and node (e.g., Quorum node) of the Accused Instrumentalities adds the enriched data record to the blockchain (e.g., the private state of the Quorum blockchain).



71. The accused 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. As an example, the Liink's DApp and node is configured to request an enclave and/or transaction manager of the Accused Instrumentalities to generate a token to identify the one or more documents of the transaction via the messaging bus.

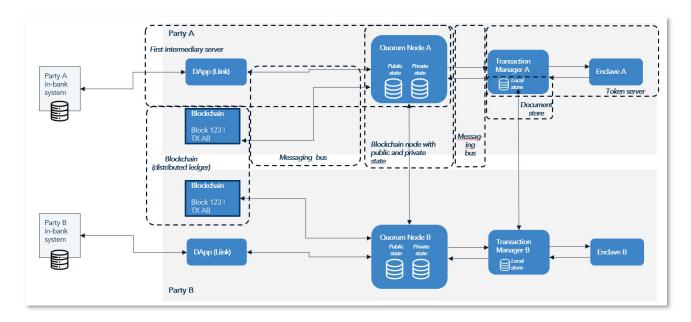


72. As an example, the token may be a hash derived from the enriched data record to identify the one or more documents. As one example, the token may be an ID, such as a messaging ID that points to or otherwise identifies the one or more documents. *See also, e.g.*, US Pub. No 2018/0374062 at Figs. 7 and 8 (showing a token "1234567XYZ" associated with the payment message):



- 73. The accused first intermediary server is configured to transmit the token to the first document store (e.g., the local store of the Transaction Manager). As an example, after receiving the token in response to the request, the node transmits the token to the first document store for storage.
- 74. The accused token server is configured to generate the token and add the token into the blockchain in association with the enriched data record. For example, the enclave and/or transaction manager adds the token described above to the blockchain of the Accused Instrumentalities (e.g., the Quorum blockchain).
- 75. The accused token server is configured to transmit the token to the first intermediary server, via the messaging bus. As an example, the accused token server transmits the token to the

DApp and the node. The accused token server and node are communicatively coupled via the messaging bus, and the messaging bus is thus used in the token transfer.



76. In addition and/or in the alternative to its direct infringement, JPMC has also infringed and continues to infringe the claims of the '413 patent by, among other things, actively inducing others to use the Accused Instrumentalities. JPMC's users, customers, consumers, agents, and other third parties who use the Accused Instrumentalities in accordance with JPMC's instructions infringe the claims of the '413 patent, in violation of 35 U.S.C. § 271(a). JPMC intentionally instructs its customers to infringe through support information such as websites, videos, demonstrations, support information and other published information. For example, JPMC's website touts the benefits of the Accused Instrumentalities and instructs and encourages JPMC's customers to use, manage, and control the infringing components and functionalities of the Accused Instrumentalities. See, e.g., https://www.jpmorgan.com/onyx/content-hub/confirm-for-financial-institutions.htm (touting the benefits of Liink to customers and encouraging them to use Liink to "securely access and share data" using the Onyx infrastructure, including Liink); see also https://www.jpmorgan.com/onyx/liink.htm (encouraging customers to, use Liink to inter alia, "Access a ready-made network of participants.");

see also https://www.jpmorgan.com/onyx/confirm.htm; https://www.jpmorgan.com/onyx/checkmatch.htm; https://www.jpmorgan.com/onyx/route-logic.htm. JPMC has a team to provide answers to customers and potential customers and instruct them regarding the use and operation of its Onyx offerings including, Liink. See https://www.jpmorgan.com/onyx/contact.htm; e.g., https://www.jpmorgan.com/onyx/documents/Confirm-Accelerate-transactions-processing-withglobal-account-validation.pdf. As demonstrated above, the components of the infringing system (e.g., first intermediary server, token server, messaging bus, blockchain) reside with and are supplied by JPMC and customers use the system and the various components when using the infringing Oynx/Liink system. When third party users use the Oynx/Liink system, they are using those constituent components (e.g., first intermediary server, token server, messaging bus, blockchain) as part of processing a transaction.

- 77. Thus, JPMC actively instructs and directs its customers to infringe and actively encourages infringement by its customers. JPMC is thereby liable for infringement of the '413 patent under 35 U.S.C. § 271(b).
- 78. JPMC has had knowledge of the '413 patent since at least September 2021 when Identitii notified JPMC of its infringement of the '413 patent. Despite this knowledge, JPMC has continued to engage in activities to encourage and assist its customers in the use of the Accused Instrumentalities. Thus, on information and belief, JPMC (1) had actual knowledge of the patent; (2) knowingly induced its customers to infringe the patent; and (3) had specific intent to induce the patent infringement.
- 79. Additionally or alternatively, JPMC is liable as a contributory infringer of the '413 patent under 35 U.S.C. § 271(c) by having offered to sell, sold and imported and continuing to offer to sell, sell, and import into the United States the Accused Instrumentalities and reasonably similar

products, to be especially made or adapted for use in an infringement of the '413 patent. The JPMC Onyx platform includes the material components for use in practicing the '413 patent and are especially made and are not staple articles of commerce suitable for non-infringing use.

- 80. As a result of JPMC's infringement of the '413 patent, Identitii has suffered monetary damages (past, present and future) and is entitled to no less than a reasonable royalty for JPMC's use of the claimed inventions of the '413 patent, together with interest and costs as determined by the Court. Identitii will continue to suffer damages in the future.
- 81. On information and belief, despite having knowledge of the '413 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '413 patent, JPMC has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement such that JPMC's infringement of the '413 patent is willful. JPMC's infringing activities relative to the '413 patent have been, and continue to be, willful, wanton, malicious, deliberate, consciously wrongful, and an egregious case of misconduct beyond typical infringement such that Identitii is entitled to enhanced damages under 35 U.S.C. § 284 up to three times the amount found or assessed.
- 82. JPMC's acts of direct and indirect infringement have caused and continue to cause damages to Identitii. Identitii is entitled to damages in accordance with 35 U.S.C. §§ 271, 281, and 284 sustained as a result of JPMC's wrongful acts in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Identitii prays for judgment and seeks relief against JPMC as follows:

- A. For judgment that JPMC has infringed one or more claims of the '413 patent, directly, and/or indirectly by way of inducement or contributory infringement;
- B. For judgment awarding Identitii damages adequate to compensate it for JPMC's

infringement of the '413 patent, including all pre-judgment and post-judgment interest as well as an award for mandatory future royalties for continuing infringement;

- C. For judgment that JPMC has willfully infringed one or more claims of the '413 patent;
- D. For judgment awarding enhanced damages pursuant to 35 U.S.C. § 284;
- E. For judgment awarding attorneys' fees pursuant to 35 U.S.C. § 285 or otherwise permitted by law;
- F. For judgment awarding costs of suit; and
- G. For judgment awarding Identitii such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure Identitii hereby demands a trial by jury of this action.

ASHBY & GEDDES

/s/ Andrew C. Mayo

Of Counsel:

M. Elizabeth Day
Marc Belloli
Jerry D. Tice II
Michael E. Flynn-O'Brien
BUNSOW DE MORY LLP
701 El Camino Real
Redwood City, CA 94063
(650) 351-7248
eday@bdiplaw.com
mbelloli@bdiplaw.com
jtice@bdiplaw.com
mflynnobrien@bidplaw.com

Dated: January 12, 2024

John G. Day (#2403 Andrew C. Mayo (#5207) 500 Delaware Avenue, 8th Floor P.O. Box 1150 Wilmington, DE 19899 (302) 654-1888 jday@ashbygeddes.com amayo@ashbygeddes.com

Attorneys for Plaintiff