

Marcin Zięcina

Wyższa Szkoła Administracji i Biznesu im. E. Kwiatkowskiego w Gdyni, Wydział Zarządzania

Wojciech Sokotowski

Akademia Marynarki Wojennej w Gdyni, Wydział Dowodzenia i Operacji Morskich

# Analiza możliwości wykorzystania wybranych innowacyjnych metod i narzędzi do zarządzania łańcuchem dostaw

## *Selected innovative methods and tools in supply chain management*

Współczesne łańcuchy dostaw podlegają dynamicznym zmianom. Tym zmianom podlegają także narzędzia i metody wykorzystywane do zarządzania nimi. Niejednokrotnie sytuacja jest jednak odwrotna: powstanie nowych rozwiązań w zakresie zarządzania determinuje ewoluowanie tych łańcuchów. Niektóre z rozwiązań mają ogromny potencjał do całkowitej zmiany logiki funkcjonowania transakcji i procesów w tych łańcuchach. Potencjał ten właściwie wykorzystany może prowadzić do kolejnych rozwiązań, takich jak inteligentne umowy (ang. *smart contract*).

Artykuł porusza problematykę zyskujących na popularności innowacyjnych rozwiązań, jakimi są wieże kontroli łańcuchów dostaw oraz łańcuchów bloków (ang. *blockchain*), i ich roli w funkcjonowaniu łańcuchów dostaw.

### **Słowa kluczowe:**

bezpieczeństwo łańcuchów dostaw, wieże kontroli łańcuchów dostaw, *big data*, *blockchain*.

The vast majority of today's supply chains are under very dynamic changes. These changes also apply to the tools and methods used to manage them. However, the situation is often reversed. New management solutions determines the evolution of these chains. Some of these solutions have potential to change the logic of the transactions and processes in these chains. This can lead to further solutions, such as smart contracts.

The article discusses the issue of the growing innovative solutions that are supply chain control towers and the blockchain and their role in the functioning of supply chains.

### **Key words:**

supply chain security, supply chain control towers, big data, blockchain.

## Wprowadzenie

Funkcjonowanie współczesnych łańcuchów dostaw, opartych w głównej mierze o międzynarodowe przepływy surowców, półproduktów, produktów, finansów i informacji, jest szczególnie narażone na różnego rodzaju zagrożenia wynikające nie tylko z powodów naturalnych, ale w równej mierze także z tych powodowanych celową działalnością człowieka. Zagrożenia powodowane czynnikiem ludzkim to obecnie w głównej mierze wynik intensyfikacji działalności terrorystycznej na całym świecie. Jednocześnie zagrożenia w funkcjonowaniu łańcuchów dostaw to zbiór otwarty. Sukcesywnie definiowane są nowe rodzaje zagrożeń i jednocześnie prowadzone są poszukiwania nowych, bardziej efektywnych metod, narzędzi i rozwiązań, minimalizujących, a nawet neutralizujących ich negatywne oddziaływanie. Nie

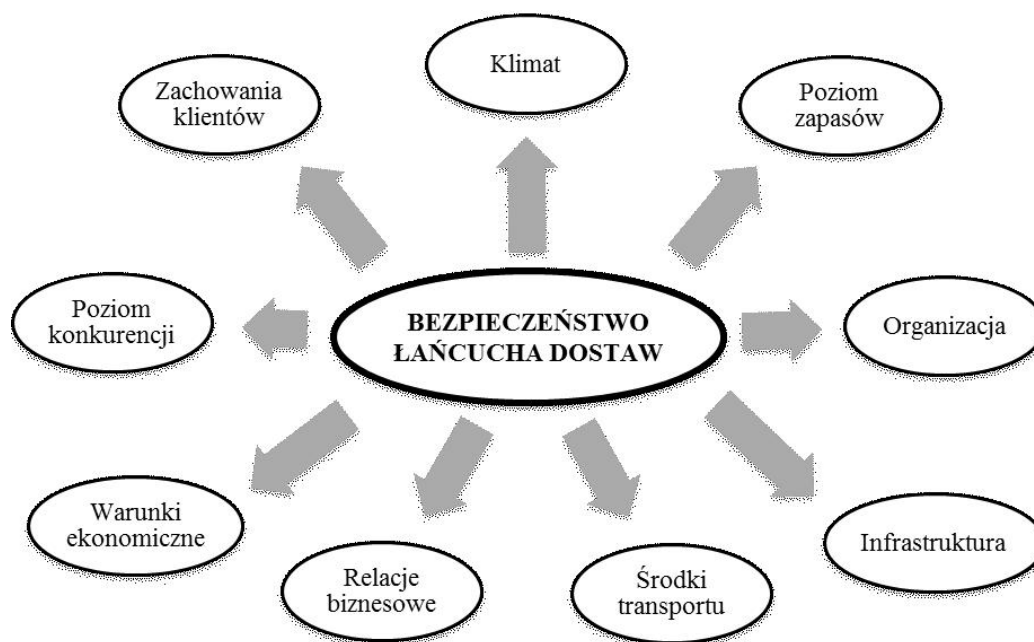
wszystkie z tych zagrożeń determinowane są czynnikami zewnętrznymi. Wielokrotnie to rozwój samych łańcuchów dostaw jest bodźcem warunkującym powstanie nowych sposobów zaburzania stanu bezpieczeństwa.

Pojęcie bezpieczeństwa jest kategorią abstrakcyjną i funkcjonuje jedynie w teorii (Malak, 2007, s. 91–95). W praktycznej działalności podmiotów gospodarczych identyfikuje się go zawsze z przymiotnikiem określającym osobę, obszar lub formę działalności, których dotyczy. Skalę trudności związaną z określeniem bezpieczeństwa w łańcuchu dostaw potęguje fakt, że w dynamicznie zmieniającej się gospodarce obejmuje ono coraz to nowe obszary — nie tylko obszary życia społecznego, gospodarczego, ale także nowe obszary geograficzne.

Jednocześnie wśród największych firm o zasięgu globalnym trwają intensywne wysiłki zmierzające do osiągnięcia przejrzystości łańcucha dostaw (ang. *sup-*

Rysunek 1

Elementy determinujące bezpieczeństwo łańcucha dostaw



Źródło: opracowanie własne na podstawie: Huczek, 2015, s. 122.

ply chain visibility, supply chain transparency). Przejrzystość łańcucha dostaw określana jest jako posiadanie wiedzy (świadomość) oraz sprawowanie kontroli nad istotnymi informacjami związanymi z fizycznymi przepływami produktów w łańcuchu dostaw, włączając w to transport oraz pozostałą działalność logistyczną, jak również posiadanie aktualnej wiedzy w zakresie wyspecyfikowanych zdarzeń zachodzących w łańcuchu dostaw istotnych dla jego prawidłowego funkcjonowania (Heaney, Ball, 2016). Przejrzystość łańcucha dostaw w obecnej rzeczywistości gospodarczej ma jednak ogromne znaczenie nie tylko ze względu na minimalizowanie kosztów, sprawowanie bezpośredniej kontroli nad przepływami informacji, towarów oraz finansów. Przejrzystość ta ma niezwykle istotne znaczenie również dla zapewnienia wiarygodności i reputacji firmy w kategoriach zrównoważonego rozwoju oraz w kategoriach etycznej i społecznej odpowiedzialności nie tylko tzw. biznesu, ale całego łańcucha dostaw (Ethical Business Practices, 2018).

Analiza czynników mających wpływ na bezpieczeństwo łańcucha dostaw pozwala stwierdzić, że są wśród nich zarówno czynniki materialne, takie jak poziom zapasów, infrastruktura, środki transportu, czynniki typowo ekonomiczne, takie jak poziom konkurencji, czynniki społeczne, takie jak zachowania klientów oraz czynniki niematerialne, takie jak relacje biznesowe pozwalające na budowanie strategii łańcucha dostaw. Zapewnienie bezpieczeństwa przy tak wielu zmiennych jest niezwykle trudne, a wręcz

czasami niemożliwe. Niejednokrotnie zagwarantowanie bezpieczeństwa dla jednego z przedmiotowych czynników będzie oznaczało obniżenie bezpieczeństwa dla kolejnego. Zapewnienie jego odpowiedniego poziomu dla wszystkich istotnych elementów wymaga umiejętnego i precyzyjnego zidentyfikowania zagrożeń, zwłaszcza tych o decydującym znaczeniu dla funkcjonowania łańcucha dostaw.

Zestawienie wymagań związanych z zapewnieniem bezpieczeństwa w łańcuchu dostaw oraz jednocześnie zachowaniem jego transparentności nie tylko dla grupy zarządzających przedmiotowym łańcuchem, ale także dla wszystkich jego uczestników, doprowadziło do powstania zapotrzebowania na rozwiązania inne niż dotychczasowe (rys. 1). Jednocześnie takie zdarzenia jak kryzys finansowy, którego szczyt przypadł na lata 2008–2009, znacząco przyspieszyły proces powstania metod i narzędzi dążących m.in. do maksymalnego wyeliminowania niepożądanych ogniw pośrednich (Polski Rynek Finansowy, 2016, s. 7).

## Wieże kontroli łańcuchów dostaw

Efektywna realizacja założeń strategii wspólnych łańcuchów dostaw wymaga posiadania metod, narzędzi, rozwiązań organizacyjnych i funkcjonalnych umożliwiających skuteczne gromadzenie i prze-

Rysunek 2

Czołowi dostawcy i odbiorcy wież kontroli łańcuchów dostaw



Źródło: opracowanie własne na podstawie: Brzeziński, Ocicka, 2016; Lippincott, 2016.

tworzenie informacji w coraz bardziej dynamicznie zmieniającym się zarówno otoczeniu, jak i wnętrzu samego łańcucha dostaw. Skuteczność realizacji zależy więc w coraz większym stopniu od pozyskiwania danych, ich analizy, właściwej interpretacji i kategoryzacji wykonywanych w czasie maksymalnie zbliżonym do rzeczywistego. Zarządzanie parametrami łańcucha dostaw, takimi jak koszty, wielkość zapasów, dystrybucja, zaopatrzenie itp., wymaga wglądu do ich parametrów kluczowych. Osiągnięcie przejrzystości w tym zakresie może zagwarantować efektywne zastosowanie narzędzi do gromadzenia, kategoryzowania i ostatecznego wykorzystania informacji.

Osiągnięcie tej przejrzystości bardzo często polega na tworzeniu i wykorzystywaniu bezpośredniego kontaktu z konsumentem, dostawcą, dystrybutorem, jednym słowem każdym ogniwem zaangażowanym w łańcuch dostaw. Obecny rozwój technologii informatycznych pozwala na tworzenie takich połączeń. Wykorzystywane są do tego różnego rodzaju elektroniczne kanały, w tym takie jak: media społecznościowe (zbieranie informacji o preferencjach klientów oraz ich opinii o produktach — *Twitter, Facebook, Instagram, LinkedIn*), a także systemy wspomagające zarządzanie przedsiębiorstwem (TS — *Transaction Systems*; WMS — *Warehouse Management Systems*; ERP — *Enterprise Resource Planning*; DRP — *Distribution Resources Planning*; MIS — *Management Information Systems*; DSS — *Decision Support Systems*; KMS — *Knowledge Management Systems*).

Jednym z takich rozwiązań są wieże kontroli łańcuchów dostaw. Jest to rodzaj centralnego koncentratora, którego działanie opiera się na wykorzystaniu odpowiedniej technologii i organizacji procesów, służącego do pozyskiwania i gromadzenia danych z łańcucha dostaw w celu zapewnienia jak najwyższej przejrzystości dla podejmowania krótko- i długookresowych decyzji zgodnych z celami strategicznymi przedsiębiorstwa (Capgemini Consulting, 2016). Zasadniczym celem tworzenia tego rodzaju koncentratorów jest przede wszystkim możliwość podejmowania decyzji w czasie rzeczywistym. Wymaga to jednak przedstawienia gromadzonych danych we właściwej formie.

Do niedawna podejmowanie decyzji przez menedżerów zarządzających łańcuchem dostaw wymagało czasochłonnego analizowania danych, przedstawionych najczęściej w postaci długich ciągów liczb lub nawet w postaci opinii konsumentów nagranych na taśmy magnetyczne, wymagających wielogodzinnego ich przesłuchiwania i wyciągania właściwych wniosków (Chui, Fleming, 2016). Wiązało się to często z odwlekaniem decyzji menedżerskich o kolejne dni lub nawet tygodnie, do czasu wypracowania ostatecznej decyzji. Narzędzia informatyczne rozwijane obecnie w ramach wież kontroli pozwalają na podejmowanie decyzji w czasie rzeczywistym, co związane jest m.in. także z formą prezentacji wyników dokonywanych analiz. Dodatkowo narzędzia te rozszerzane są o możliwości przygotowywania symulacji i prognoz

o dużym stopniu prawdopodobieństwa. Pozwala to na generowanie sygnałów wskazujących źródło i rodzaj zmian, analizę ryzyka, rozwój scenariuszy działań, a w efekcie dostarczanie krytycznych danych dla realizacji strategii zarządzania łańcuchem dostaw, podejmowania decyzji i dostosowywania kluczowych wskaźników sukcesu.

Wśród czołowych przedsiębiorstw zarządzających najbardziej konkurencyjnymi łańcuchami dostaw na świecie według rankingu *Gartner Supply Chain Top 25* wieże kontroli posiadają: Unilever, Procter & Gamble, Samsung Electronics, Cisco, Colgate-Palmolive, Coca-Cola, Walmart, Lenovo Group, Kimberly-Clark i Caterpillar. Natomiast wśród głównych dostawców tego rodzaju oprogramowania na świecie w 2016 r. zgodnie z danymi Nucleus Research były: E2open, One Network, Kinaxis, Elementum, Pearl Chain, JDA Software i LLamasoft (rys. 2; Lippincott, 2016).

Wieże kontroli łańcuchów dostaw wykorzystują stosunkowo nową koncepcję, jaką jest *Big Data*. Koncepcja ta w coraz większym stopniu wpływa na funkcjonowanie łańcuchów dostaw.

Idea zbioru danych w koncepcji *Big Data* charakteryzowana jest za pomocą trzech atrybutów — 3V, takich jak (Richey, Morgan, Lindsey-Hall, Adams, 2016):

1. Wysoka dynamika przyrostu (ang. *volume*).
2. Szybki strumieniowy napływ (ang. *velocity*).
3. Duża różnorodność (ang. *variety*).

Atrybuty te podlegają obecnie wielu przemianom definicyjnym, a efekt uzależniony jest przede wszystkim od kontekstu, w jakim *Big Data* rozwija się w danej organizacji.

Istotą *Big Data* jako potencjalnego źródła przewagi konkurencyjnej nowoczesnych przedsiębiorstw i łańcuchów dostaw jest odpowiednie wykorzystanie gromadzonych danych. Możliwość ich rejestrowania, przechowywania, agregowania i analizowania w celu pozyskania potrzebnej wiedzy staje się obecnie ogromnym wyzwaniem dla przedsiębiorstw. Podkreślenie praktycznej roli *Big Data* w łańcuchach dostaw wymaga koncentracji nie tylko w samej bazie danych, lecz także w sposobie pozyskiwania z niej pożądanych informacji. W tym celu stosowane są zaawansowane narzędzia analityczne określane mianem *Big Data Analytics* (BDA). Proces ich wykorzystywania do badania potencjału *Big Data* ma na celu identyfikację informacji (np. ukrytych wzorców, nieznanych dotychczas korelacji itp.) pomocnych w podejmowaniu trafnych decyzji (rys. 3).

Idea funkcjonowania wieży kontroli polega na centralizacji zarządzania informacjami pochodzącymi z systemów informatycznych partnerów współpracujących w łańcuchu dostaw w jednym miejscu. Do integracji różnych systemów jest wykorzystywane odpowiednie oprogramowanie (ang. *middleware software*).

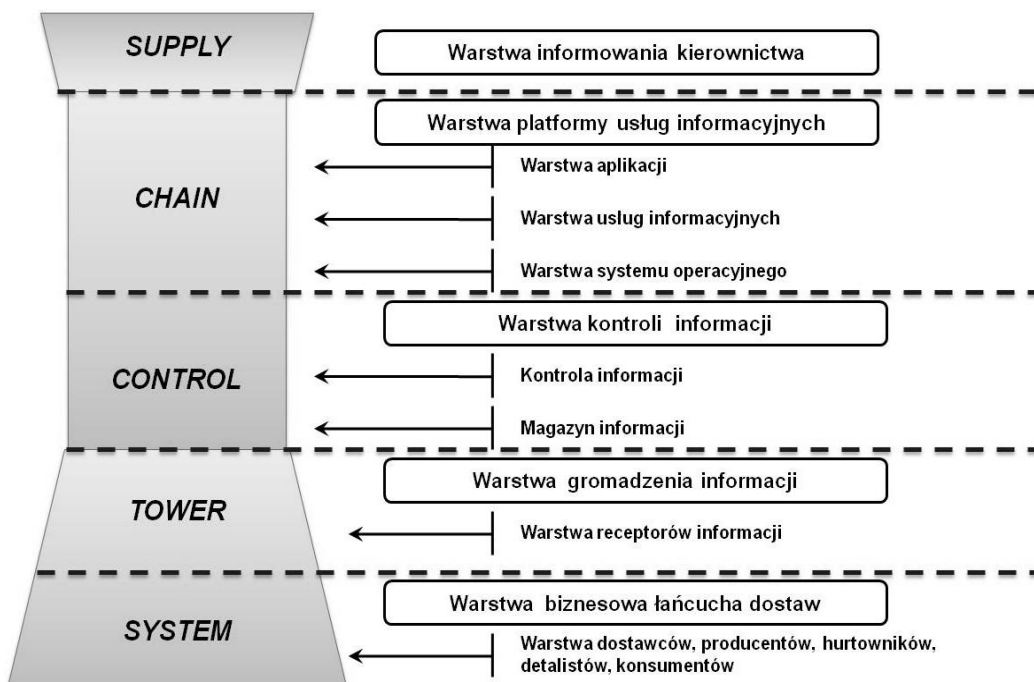
Oprócz technologii wieże kontroli integrują także procesy, które zapewniają przepływ produktów

Rysunek 3

Koncepcja *Big Data* w praktyce



Źródło: opracowanie własne na podstawie: Heaney, Ball, 2016.



Źródło: opracowanie własne na podstawie: Shou-Wen, Ying, Yang-Hua, 2016.

z miejsc ich pochodzenia do ostatecznych konsumentów, niezależnie od złożoności globalnej sieci dostaw. Zyskują one szczególny wymiar w gospodarce cyfrowej, którą charakteryzuje dostęp do coraz większej liczby danych oraz rozwijające się możliwości ich wymiany na platformach *online*, np. w chmurze obliczeniowej. Należy jednak pamiętać, że cyberatak i utrata danych w wyniku celowego zainfekowania urządzeń są przez większość przedsiębiorstw postrzegane jako największe rodzaje ryzyka dla zarządzania łańcuchami dostaw i jednymi z najtrudniej wykrywalnych.

Przykładowa struktura wieży kontroli łańcucha dostaw składa się z pięciu warstw, do których należą (rys. 4; Shou-Wen, T. Ying, G. Yang-Hua, 2016):

1. Warstwa biznesowa łańcucha dostaw jest to podstawowa warstwa leżąca u podstaw każdej wieży kontroli łańcucha dostaw. Warstwę tę stanowią wszyscy uczestnicy łańcucha dostaw (dostawcy, producenci, dystrybutorzy, dostawcy usług logistycznych, detaliści, hurtownicy, konsumenci) oraz zasadnicze aspekty i reguły jego funkcjonowania. Procesy charakterystyczne dla tej warstwy to zakupy materiałowe, transport, magazynowanie, przeładunek, procesy dystrybucji i pakowania oraz przepływ informacji.
2. Warstwa gromadzenia informacji jest „nerwem percepcyjnym” całego systemu i stanowi jednocześnie o jakości całego łańcucha dostaw. W tej warstwie wykorzystywane są technologie charakterystyczne dla Internetu Rzeczy służące gromadzeniu danych, takie jak systemy automatycznej identyfikacji danych (RFID, kody kreskowe, techniki biometryczne, rozpoznawanie obrazu, ścieżki magnetyczne, GPS itp.). Na tym etapie funkcjonowania wieży kontroli łańcucha dostaw tworzone są bazy danych stanowiące podstawę do wypracowania decyzji w kolejnych poziomach.
3. Warstwa kontroli informacji składa się z dwóch części. Pierwsza część określana jest jako magazyn informacji, natomiast druga część to panel kontrolny informacji. Zadaniem pierwszej części jest dostarczanie kompletu informacji wymaganych przez część stanowiącą panel kontrolny. Panel kontrolny powinien posiadać natomiast możliwość rewersyjnego przesyłania informacji do części magazynowej warstwy. Warunkiem koniecznym prawidłowego działania jest oczywiście gromadzenie danych w czasie rzeczywistym. Panel kontrolny informacji podzielony jest na dwa poziomy. Pierwszy z poziomów zawiera algorytmy oraz model logiczny procesów biznesowych łańcucha dostaw w celu dostarczania informacji o ich jakości. Drugi z poziomów kontroluje wewnętrzną jakość opracowanego algorytmu i pozwala na jego bieżące modyfikowanie. Dane pochodzące z tych dwóch poziomów dają pełną informację zwrotną. Z tego powodu warstwa ta nazywana jest „sercem systemu”.
4. Warstwa platformy usług informacyjnych zawiera system operacyjny integrujący wszystkie informa-

cje pochodzące z łańcucha dostaw. Funkcjonujące w tej warstwie aplikacje zdolne są do przetwarzania informacji otrzymanych z różnych systemów w czasie rzeczywistym i zapewniają ich przejrzystość, a następnie umożliwiają wizualizację w formie czytelnej dla potencjalnych odbiorców. Kolejną funkcją tej warstwy jest bieżące monitorowanie informacji pochodzących z łańcucha dostaw. Zastosowane aplikacje pozwalają także na porównywanie wartości danych bieżącej sytuacji z dowolnie wybranym okresem należącym do przeszłości.

5. Warstwa informowania kierownictwa jest ostatnią z warstw w wieży kontroli. Warstwa ta stanowi centrum podejmowania decyzji oraz kontroli menedżerskiej łańcucha dostaw. Jest to centrum monitoringu wszystkich procesów zachodzących w łańcuchu dostaw. Stanowi także ośrodek wczesnego ostrzeżenia oraz pozwala na podejmowanie decyzji strategicznych w czasie rzeczywistym. Oprogramowanie funkcjonujące w ramach tej warstwy posiada także moduły pozwalające na pracę w trybie szkolenia, co umożliwia personelowi wcześniejsze wykrywanie zagrożeń i dostrzeżenie potencjalnych szans.

Oprogramowanie stosowane w poszczególnych warstwach wieży kontroli projektowane jest w taki sposób, aby wykorzystywać wszystkie dostępne źródła informacji istotne dla funkcjonowania łańcucha, włączając w to m.in. aplikacje zbierające automatycznie dane pochodzące z korespondencji mailowej czy też sms-owej.

Wieże kontroli to rozwiązania niezwykle pomocne w zarządzaniu łańcuchem dostaw. Pozwalają na gromadzenie i przetwarzanie informacji w czasie rzeczywistym, dekodowanie sygnałów wskazujących źródła i kategorie zmian, analizowanie ryzyka, prognozowanie i przeprowadzanie symulacji, generowanie scenariuszy ewentualnych działań, a w efekcie dostarczanie krytycznych informacji dla realizacji strategii zarządzania, podejmowania decyzji i doskonalenia kluczowych czynników sukcesu (Supply chain management, 2016).

## Blockchain

Kolejnym z narzędzi, które postrzegane jest przez instytucje i przedsiębiorstwa wdrażające nowe technologie jako to, które zrewolucjonizuje zarządzanie łańcuchem dostaw, jest *blockchain*. Jest to narzędzie stanowiące kolejny etap rozwoju rozproszonych baz danych, które pierwotnie powstało w celu umożliwienia zarządzania kryptowalutą — bitcoin. Z technicznego punktu widzenia *blockchain* jest to łańcuch nierozzerwalnie połączonych cyfrowo bloków (poprzez odpowiednie zapisy w struktu-

rze) zawierających dane na temat realizowanych operacji i jednocześnie jest pewnego rodzaju platformą transakcyjną. Platforma ta jest zdecentralizowana i znajduje się w rozproszonej infrastrukturze sieciowej o architekturze *peer-to-peer* (P2P), jednocześnie funkcjonując w modelu *open-source* bez centralnego miejsca przechowywania danych oraz scentralizowanego oprogramowania zarządzającego procesami, zabezpieczona skomplikowanym narzędziem kryptograficznym (Co to jest łańcuch bloków, 2018). Łańcuch bloków jest jawny i publiczny, a jednocześnie anonimowy. Istnieją jednak łańcuchy bloków, do których dostęp możliwy jest jedynie dla posiadaczy dwóch kluczy kryptograficznych: publicznego oraz prywatnego.

Sposób zapisu danych oraz tworzenia poszczególnych bloków w łańcuchu powoduje, że jest on doskonale zabezpieczony przed cyberatakiem oraz próbą niepowołanego dostępu. Dokonanie takiego ataku na tylko jeden z bloków w łańcuchu wymagałoby wykonania jednoczesnego, symultanicznego ataku na wszystkie bloki tworzące łańcuch, na wszystkie komputery tworzące sieć, na których rozproszony jest *blockchain*, przy jednoczesnym złamaniu narzędzia kryptograficznego, którym jest on zabezpieczony. W chwili obecnej nie istnieje maszyna cyfrowa, której moc obliczeniowa pozwalałaby na dokonanie takiej operacji (Tapscott, Tapscott, 2016, s. 48).

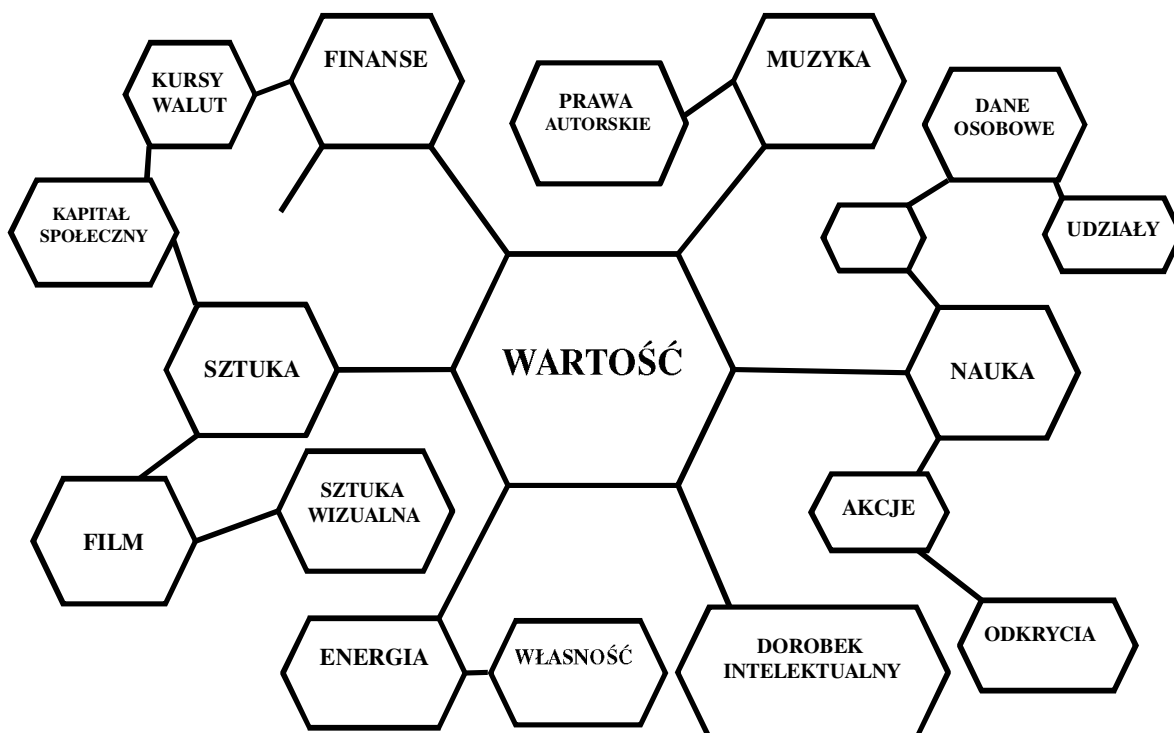
Niepowtarzalny sposób zapisu, przechowywania oraz dostępu do danych generuje zalety tego narzędzia, do których w głównej mierze zalicza się (Blockchain and the Supply Chain, 2018):

1. Zapewnienie przejrzystości i bezpieczeństwa w procesach wymiany danych pomiędzy poszczególnymi uczestnikami łańcucha dostaw.
2. Zapewnienie nieograniczonej dostępności do istotnych informacji dla wszystkich uczestników łańcucha dostaw.
3. Wyeliminowanie ogniw pośrednich weryfikujących dane lub potwierdzających uczestników w operacjach finansowych lub innego rodzaju transakcjach.
4. Wiarygodność przeprowadzanych transakcji wynikającą m.in. z braku możliwości zmiany danych, które zostały już raz zapisane w bloku.
5. Redukcję kosztów związanych z budową i utrzymaniem infrastruktury systemów operacyjnych służących do zarządzania przepływem danych w łańcuchach dostaw.
6. Odporność na różnego rodzaju awarie systemów informatycznych oraz cyberatak.
7. Niezależność od jakiegokolwiek instytucji centralnej.

Jedną z najbardziej istotnych zalet *blockchain* jest możliwość nieograniczonego dostępu do wszystkich informacji i każdej operacji jaka tylko miała miejsce w historii tego łańcucha bloków, dla wszyst-

Rysunek 5

Potencjał *blockchain* w zakresie skutecznego i bezpiecznego przetwarzania oraz przechowywania oryginałów dóbr niematerialnych



Źródło: opracowanie własne na podstawie: Tapscott, Tapscott, 2016, s. 47.

kich zainteresowanych w dowolnym czasie. Daje to ogromne możliwości w porównaniu z obecnym modelem wymiany informacji w łańcuchach dostaw. Łańcuchy dostaw w obecnej formie posiadają strukturę sekwencyjną oraz są systemami pod względem informatycznym wyizolowanymi. Oznacza to, że ogromne ilości danych są kopiowane, wprowadzane do określonych systemów komputerowych i przesyłane zgodnie ze zdefiniowanymi dla nich ścieżkami powiadamiania. Cały ten proces spowalnia jednak łańcuch dostaw działający właśnie w oparciu o transfer danych. Niejednokrotnie w całym procesie uczestniczą dodatkowo pośrednicy (banki, firmy obsługujące kredyty, firmy ubezpieczeniowe, jednostki administracji państwowej), których zadaniem jest weryfikowanie tych danych, uwierzytelnianie stron biorących udział w procesach, zwłaszcza finansowych. Bardzo często zdarza się też, że to właśnie ci pośrednicy generują i organizują całą logikę wszystkich operacji w łańcuchu dostaw, a jednocześnie są źródłem dodatkowych kosztów, co powoduje w pewnych okolicznościach nawet ograniczenia w fizycznych przepływach dóbr i finansów. Wszystkie te elementy powodują utrudnienia w funkcjonowaniu łańcuchów dostaw, do których w głównej

mierze zaliczyć można (Blockchain and the Supply Chain, 2018):

1. Spowolnienie operacji realizowanych w łańcuchu dostaw.
2. Znaczące różnice pomiędzy popytem a podażą.
3. Gromadzenie zbędnych zapasów lub zejście poniżej poziomu zapasu minimalnego.
4. Generowanie wysokich kosztów logistycznych, zwłaszcza w sytuacjach wymagających wykonania szybkiego manewru materiałowego zapasów w łańcuchu dostaw.
5. Podejmowanie decyzji na podstawie zdezaktualizowanych informacji pochodzących zarówno z otoczenia, jak i, wnętrza łańcucha dostaw.

Funkcjonujące w oparciu o chmurę łańcuchy dostaw posiadają również bardzo istotne z ekonomicznego punktu widzenia ograniczenie. Ograniczenie to wynika również ze sposobu przesyłania danych w Internecie. Wszystkie przesyłane w ten sposób informacje to tak naprawdę kopia oryginału, i jeśli w przypadku zwykłej wymiany informacji taki sposób nie stanowi problemu, to jednak w przypadku finansów, papierów wartościowych, utworów, dokumentów potwierdzających prawa autorskie, dokumentów własnościowych, sztuki, muzyki, dorobku intelektualnego

go itp. przesyłanie kopii stanowi bardzo znaczące ograniczenie (rys. 5). Dodatkowym ograniczeniem w przypadku finansów jest problem możliwości wystąpienia tzw. podwójnego wydatkowania tych samych środków (ang. *double-spending*), który został w *blockchain* całkowicie wyeliminowany poprzez odpowiednie operacje weryfikacji danych agregowanych i zamykanych w blokach łańcucha (The Double Spending Problem, 2018).

Analiza możliwości *blockchain* wykazuje również znaczące ograniczenia w zakresie wykorzystania go jako narzędzia do zarządzania łańcuchem dostaw. Pierwszym z nich jest zachowanie poufności danych w ramach tego łańcucha. Przedsiębiorstwa współpracujące w ramach łańcucha dostaw rzadko udostępniają dane do powszechnej wiadomości. Jest to problem określany w literaturze przedmiotu jako: *every-member-can-read-everything* (Notani, 2018). Z uwagi to, że większość firm nie zgadza się, aby dane dotyczące łańcucha dostaw lub istotne informacje handlowe były dostępne nawet dla własnych partnerów w tym łańcuchu, jest to znacząca wada. Cały czas trwają próby pokonania tej przeszkody. Jednym z pomysłów w tym zakresie jest dzielenie łańcucha bloków na tzw. mikrospołeczności (ang. *micro-community blockchain*; Notani, 2018). Prace nad koncepcją podziału łańcucha bloków na mniejsze części wygenerowały dwa podejścia z tym związane:

1. Podejście polegające na łączeniu łańcuchami bloków parami, czyli łańcuchy bloków łączące bezpośrednio dwa współpracujące ze sobą punkty (ang. *pairwise micro-community blockchain*).
2. Podejście polegające na łączeniu łańcuchami dostaw uczestników danej operacji biznesowej (ang. *per-business micro-community blockchain*).

Jednak każde z wymienionych rozwiązań ma istotne ograniczenia, co spowodowało, że prace nad rozwiązaniami zgodnymi z tą koncepcją nie zaowocowały jeszcze stworzeniem praktycznych sposobów.

Kolejnym istotnym ograniczeniem narzędzia, jakim jest *blockchain*, jest jego przepustowość. Liczba transakcji w globalnych łańcuchach dostaw, uwzględniając nie tylko operacje finansowe, ale również liczbę produktów, różne lokalizacje oraz ogromną liczbę partnerów biznesowych, jest znacząca. Technologia, która ma wspierać zarządzanie w takich łańcuchach, powinna sprostać tym wymaganiom i mieć możliwość wykonywania tych operacji niemalże w czasie rzeczywistym. Liczba transakcji wykonywanych na sekundę przez organizację specjalizującą się w operacjach finansowych, jaką jest VISA, w 2015 r. wynosiła ok. 2000 operacji (<https://usa.visa.com>, dostępny 23.04.2018).

Natomiast maksymalna liczba operacji wykonywanych w łańcuchu bloków na sekundę to zaledwie 11 (<https://blockchain.info/pl/>, dostępny 23.04.2018).

Stanowi to najistotniejsze wąskie gardło dla tego narzędzia. W obecnej chwili trwają próby nad wdrożeniem do *blockchain* takich rozwiązań jak skalowanie horyzontalne architektury sieci, które pozwala na osiągnięcie przepustowości łańcucha bloków na poziomie 1000 operacji na sekundę (Blockchain..., <https://www.onenetwork.com/>, dostęp 12.04.2018).

## Wnioski

Analiza innowacyjnych narzędzi do zarządzania łańcuchem dostaw pozwala odnotować, że:

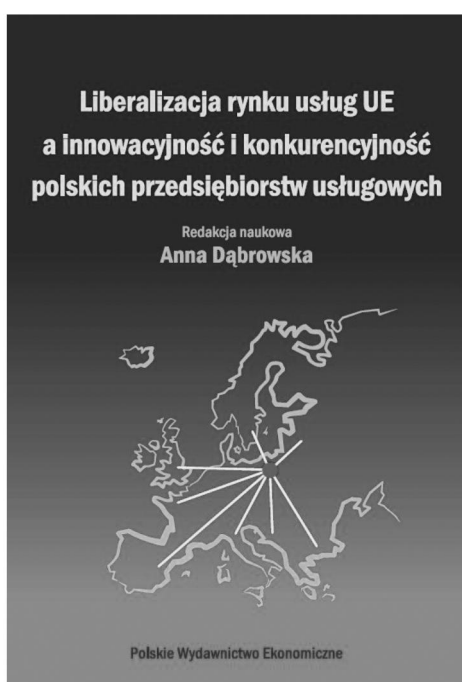
1. Zwiększające się dynamicznie wymagania stawiane przed globalnymi łańcuchami dostaw powodują, że zaprezentowane rozwiązania w zakresie integracji technologicznej, kontroli przepływu informacji, kreowania przejrzystości procesów wydają się mieć fundamentalne znaczenie dla sprawnego ich funkcjonowania.
2. Zintegrowanie informacji w scentralizowanej platformie umożliwia koordynację reakcji współpracujących przedsiębiorstw wobec negatywnych zdarzeń, jakie mogą mieć miejsce. Co więcej, reakcja ta następuje dużo szybciej. Pozwala to też na redukcję niepożądanych skutków powstałych zagrożeń.
3. Dodatkowym atutem wykorzystania tego typu narzędzia jest także możliwość budowania modeli oraz tworzenia symulacji, co pozwala na prognozowanie potencjalnych niebezpieczeństw.
4. Rozwiązania takie mają oczywiście ograniczenia, do których zaliczyć można m.in. nieodzowność przeprowadzenia znacznych inwestycji w zakresie IT, problemy z integracją różnych systemów wykorzystywanych w łańcuchach dostaw, konieczność budowania złożonych narzędzi analitycznych, czy też ryzyko związane z udostępnianiem informacji innym uczestnikom łańcuchów dostaw.
5. *Blockchain* jest narzędziem mającym ogromny potencjał do praktycznie całkowitej zmiany w zarządzaniu łańcuchem dostaw i budowaniu rozwiązań całkowicie zmieniających obecną logikę zarządzania łańcuchem dostaw.

Autorzy zdają sobie sprawę z ograniczeń wykonanej kwerendy i analizy problematyki w zakresie zaprezentowanych rozwiązań. Literatura w tym zakresie jest jeszcze mało dostępna, a procesy, których analiza literatury dotyczy, podlegają ciągłej modyfikacji. Przedsiębiorstwa rozwijające tego rodzaju rozwiązania w ramach własnych łańcuchów bardzo oszczędnie dzielą się obserwacjami z ich wdrażania. Z pewnością jest to jednak interesujący kierunek badań i potencjalny obszar badawczy z zakresu wykorzystania nowoczesnych technologii informatycznych.



## Bibliografia

- Brzeziński J., Ocicka B. (2016). Rola wież kontroli w zarządzaniu globalnym łańcuchem dostaw. W: K. Witkowski, S. Saniuk (red.), *Systemy logistyczne w gospodarowaniu*. Warszawa: Przedsiębiorczość i Zarządzanie (tom XVII, zeszyt 12, część II). Wydawnictwo Społecznej Akademii Nauk. Łódź.
- Ethical Business Practices in Purchasing and Supply Management, The Chartered Institute of Purchasing & Supply*®, <https://www.cips.org>, (dostępny 13.03.2018).
- Huczek, M. (2015). Bezpieczeństwo łańcucha dostaw. Sosnowiec: Zeszyty Naukowe Wyższej Szkoły Humanitas. Zarządzanie.
- Malak, K. (2007). *Bezpieczeństwo jako kategoria i zjawisko społeczne* (91–95). Piotrkowskie Zeszyty Międzynarodowe.
- Richey R.Jr., Morgan T., Lindsey-Hall K., Adams F. (2016). A global exploration of Big Data in the supply chain. *International Journal of Physical Distribution & Logistics Management*, 46 (8).
- Szymański, W. (2012). Niestabilność gospodarcza a szanse przedsiębiorstw. W: Strategiczne zmiany modelu biznesu w warunkach niestabilnego otoczenia. W: R. Sobiecki, J.W. Pietrewicz (red.), *Przedsiębiorstwo a narastająca niestabilność otoczenia*. Warszawa: Oficyna Wydawnicza SGH.
- Szymonik, A., Bielecki, M. (2015). *Bezpieczeństwo systemu logistycznego w nowoczesnym zarządzaniu*. Warszawa: Difin.
- Tapscott, D., Tapscott, A. (2016). *Blockchain revolution. How the technology behind bitcoin is changing money, business and the world*. Canada: Penguin.
- Źródła internetowe:**
- Blockchain and the Supply Chain, Achieving secure, high performance supply chains*, <https://www.onenetwork.com/>, (dostęp 12.04.2018).
- Capgemini Consulting, *Global Supply Chain Control Tower*, <http://www.capgemini.com/resources/global-supplychain-control-towers> (dostęp 16.12.2016).
- Chui M., Fleming T., *Inside P&G's digital revolution*, <http://www.mckinsey.com/industries/consumer-packaged-goods/our-insights/inside-p-and-ampgs-digital-revolution> (dostęp 17.12.2016).
- Co to jest łańcuch bloków (blockchain)? kryptopolonia.info (dostęp 03.03.2018).
- Heaney B., Ball B., *Supply chain visibility and segmentation: Control tower approach*, [www.aberdeen.com](http://www.aberdeen.com) (dostęp 14.12.2016). <https://blockchain.info/pl/>, (dostęp 23.04.2018 r.). <https://usa.visa.com>, (dostęp 23.04.2018 r.).
- Lippincott S., *Control tower value matrix 2016*, <https://nucleusresearch.com> (dostęp 16.12.2016).
- Malak K., *Typologia bezpieczeństwa. Nowe wyzwania*, <http://stosunki-miedzynarodowe.pl/bezpieczenstwo/954-typologia-bezpieczenstwa-nowe-wyzwania> (dostęp 10.12.2016).
- Notani R., *Can Blockchain Revolutionize the Supply Chain?*, [www.onenetwork.com/](http://www.onenetwork.com/) (dostęp 12.04.2018).
- Polski rynek finansowy w obliczu kryzysu finansowego w latach 2008–2009*. Urząd Komisji Nadzoru Finansowego (dostęp 28.12.2016, s. 7).
- Shou-Wen J., Ying T., Yang-Hua G. (2016). Study on Supply Chain Information Control Tower System. *Information Technology Journal*, 12 (24). <http://ansinet.com/itj> (dostęp 10.12.2016).
- Supply chain management in the cloud. How can cloud-based computing make supply chains more competitive?* [https://www.accenture.com/t20150523T022449\\_w\\_us-en\\_acnmedia/Accenture/ConversionAssets/DotCom/Documents/Global/PDF/Dualpub\\_1/Accenture-Supply-Chain-Management-in-the-Cloud.pdf](https://www.accenture.com/t20150523T022449_w_us-en_acnmedia/Accenture/ConversionAssets/DotCom/Documents/Global/PDF/Dualpub_1/Accenture-Supply-Chain-Management-in-the-Cloud.pdf) (dostęp 10.12.2016).
- The Double Spending Problem and Cryptocurrencies. *Banking & Insurance Journal, Social Science Research Network*, <https://ssrn.com/> (dostęp 14.01.2018).



Praca przedstawia aktualne podejście do problematyki powstawania, funkcjonowania i rozwoju firm świadczących usługi na rynku unijnym w kontekście skutków wynikających z implementacji dyrektywy usługowej i najnowszych aktów prawnych związanych z liberalizacją gospodarki Unii Europejskiej. Zawarto w niej wiele cennych myśli, wniosków i propozycji, tworząc dzieło naukowe na wysokim poziomie merytorycznym.

W książce przedstawiono ważne, dotychczas niewystarczająco omówione w literaturze problemy, wsparte zestawieniami liczbowymi, przykładami oraz wynikami obszernych i wielokierunkowych badań pierwotnych i analiz. Zgromadzony materiał badawczy pozwolił na poszerzenie dotychczasowego dorobku na temat liberalizacji rynku usług w UE jako czynnika zwiększania innowacyjności i konkurencyjności polskich podmiotów usługowych, wskazanie mocnych i słabych stron polskich przedsiębiorstw świadczących usługi poza granicami kraju, wpływających na efektywność ich funkcjonowania, a także ocenę zmian w prawie polskim jako skutków wejścia w życie dyrektywy usługowej.

[www.pwe.com.pl](http://www.pwe.com.pl)