ISSN 1507-3858
e-ISSN 2450-0003

Monika Sitarska-Buba
Uniwersytet Ekonomiczny we Wrocławiu
e-mail: monika.sitarska-buba@ue.wroc.pl
ORCID: 0000-0002-1848-6972

ARCHITEKTURA SYSTEMÓW *BLOCKCHAIN 2.0*

ARCHITECTURE OF THE BLOCKCHAIN 2.0

DOI: 10.15611/ie.2018.4.10
JEL Classification: C88, M21

Streszczenie: Systemy *blockchain* są technologią umożliwiającą rozproszone przetwarzanie danych między różnorodnymi węzłami w obrębie sieci. Systemy te stanowią przykład technologii rewolucyjnej determinującej zmiany w podejściu do systemu zarządzania oraz systemów ekonomicznych funkcjonujących we współczesnej gospodarce. Osiągnięto to głównie na skutek przeniesienia ciężaru procesu walidacji poprawności transakcji z dotychczasowych jednostek centralnych, takich jak instytucje finansowe, banki czy urzędy, na poziom algorytmów informatycznych zaimplementowanych w danym systemie *Blockchain 2.0.* W artykule zaprezentowano koncepcję architektury systemów *Blockchain 2.0*, zarządzaną przez poszczególne warstwy od aspektów czysto algorytmicznych przez wydajnościowe aż po aspekt biznesowy. Zastosowanie poszczególnych warstw pozwala na coraz bardziej elastyczne zastosowanie systemów *Blockchain 2.0* na gruncie biznesowym.

Słowa kluczowe: *Blockchain 2.0*, technologie rozproszonych rejestrów, inteligentne kontrakty, mechanizm konsensusu.

Summary: Blockchain technology is still new and growing on the market. Different companies work on constant development of new commercial systems based on IT. Decentralized network of nodes connected to one chain is allowed to exchange and authorize transactions without central based authority. The article describes how blockchain systems were growthing within the past 10 years, and how to build business oriented architecture of them. The author describes dependencies between architecture layers of the system to meet business requirements..

Keywords: Blockchain 2.0, technologies of distributed registers, smart contracts, mechanism consensus.

1. Wprowadzenie do technologii *blockchain*

Od kilku lat obserwujemy wzrost zainteresowania technologią *blockchain* oraz jej zastosowaniem na gruncie biznesowym. Wiele koncernów informatycznych inwe-

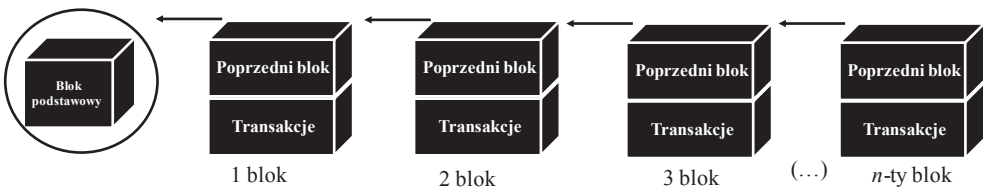
stuje w rozwój autorskich technologii bazujących na zdecentralizowanym i współdzielonym przetwarzaniu transakcji przez pomioty połączone w obrębie jednego łańcucha biznesowego. Powstaje więc pytanie, jakich cech i funkcji powinna dostarczać technologia *blockchain*, aby można było mówić o nowej klasie systemów wspierających zarządzanie przedsiębiorstwem.

Celem artykułu jest omówienie koncepcji systemów *blockchain* oraz wskazanie na podstawowe etapy rozwoju zidentyfikowane w ostatnich dziesięciu latach. W pracy zaprezentowano także koncepcję architektury systemów *Blockchain* 2.0, wskazano poszczególne warstwy składowe oraz powiązania między nimi. Implementacja zdefiniowanej architektury, zdaniem autora, pozwala na zastosowania biznesowe, w których podmioty gospodarcze zarządzają procesami biznesowymi, bazując na rozproszonej księdze głównej transakcji bez konieczności angażowania jednostek centralnych w celach autoryzacji.

Początki systemów *blockchain* są związane z rozwojem kryptowaluty oraz ze zdecentralizowanym przetwarzaniem w chmurze obliczeniowej. Sama koncepcja kryptowaluty po raz pierwszy została opisana przez programistę Wei Daia w 1998 roku, jednak dopiero 10 lat później doczekała się rzeczywistej implementacji jako *bitcoin*. W roku 2008 Satoshi Nakamoto opublikował manifest (manifest Satoshi Nakamoto) opisujący zasady funkcjonowania systemu kryptowaluty *bitcoin* (por. [Bitcoin 2008]).

Autorka Melanie Swan w publikacji pod tytułem *Blockchain* klasyfikuje systemy koncentrujące się jedynie na przetwarzaniu kryptowaluty jako systemy *Blockchain 1.0*, dające początek rozwojowi nowej klasy systemów informatycznych zawierających kryptowalutę, zasady przetwarzania transakcji walutowych (protokoły) oraz sieć połączonych węzłów tworzących wspólny rejestr przetwarzania transakcji (por. [Swam 2015]).

Technologia *Blockchain 1.0*, rozumiana też jako łańcuch bloków, służy do przechowywania i przesyłania informacji o transakcjach walutowych zawartych w Internecie, które gromadzone są w postaci następujących po sobie bloków danych. Każdy z bloków zawiera sekwencję transakcji, które są jawne dla wszystkich uczestników zarejestrowanych w systemie. Każdy blok przechowuje identyczną kopię danych oraz referencję do poprzedniego bloku w łańcuchu, co prezentuje rys. 1.



Rys. 1. Graficzna prezentacja struktury danych *blockchain*

Źródło: opracowanie własne na podstawie [Panda i in. 2018].

Sieć *blockchain* stanowią jednostki rozproszone współpracujące ze sobą w modelu *peer-to-peer*. Każdy uczestnik sieci ma równe prawa w zatwierdzaniu prawidłowości transakcji. Model ten odrzuca tworzenie jednostki centralnej, autoryzującej i uwierzytelniającej procesy przetwarzania w ramach sieci.

Każda transakcja jest szyfrowana asymetrycznie, jest oznaczana jednokierunkową funkcją skrótu (funkcją haszującą), która jest odporna na kolizje oraz nieodwracalna (nie można odtworzyć transakcji, znając tylko jej skrót). Sieć *blockchain* jest rozproszona geograficznie, nie ma jednostki centralnej, nie ma też przyjętej jednej, właściwej strefy czasowej. Wyzwanie to rozwiązano przez numerowanie bloków według kolejności ich dodawania do łańcucha. Przyjmując to założenie, można stwierdzić, że każdy blok ma swój niepowtarzalny znacznik czasu odpowiadający kolejności utworzenia.

Założenia teorii gier znalazły odzwierciedlenie w mechanizmach konsensusu. Według prof. Krzysztofa Piecha konsensus to proces, w ramach którego strony biorące udział w sieci opartej na technologii *blockchain* zgadzają się na przeprowadzenie transakcji zatwierdzanej przez wszystkich uczestników tej sieci. Konsensus gwarantuje integralność danych każdej kopii rejestru i zmniejsza ryzyko przeprowadzenia nieautoryzowanej transakcji [Piech (red.) 2016, s. 8].

Jednym z przykładów algorytmu konsensusu, który jest stosowany w sieci Bitcoin i Etherneum, jest tzw. dowód wykonania pracy (*Proof of Work* − PoW). Konsensus ten wymaga od węzła zatwierdzającego transakcje rozwiązania równania o określonym poziomie trudności, który jest adekwatny do wartości zatwierdzanej transakcji. Rozwiązanie jest wartością losową, więc węzły muszą zaangażować określoną moc obliczeniową, żeby wygenerować wynik. Algorytm reguluje trudność zadań tak, aby zoptymalizować częstotliwość zatwierdzania bloków transakcji lub utrzymać ją na stałym poziomie. Poszczególne węzły otrzymują nagrody za wykonanie pracy, co powoduje, że z ekonomicznego punktu widzenia korzystniejsze jest zatwierdzanie nowych bloków niż modyfikacja transakcji w istniejących.

Innym algorytmem konsensusu, który został zaimplementowany w takich systemach *blockchain,* jak Hyperledger (IBM), Stellar oraz Ripple (Stellar Development Foundation), jest problem bizantyjskich generałów (*Practical Byzantine Fault Tollerance* − PBFT) (por. [Xiwei 2016]). Transakcja jest wysyłana do wszystkich uczestników sieci tak, że każdy węzeł ma swoją replikę danych. Po otrzymaniu transakcji każdy węzeł procesuje ją odpowiednio do swojego stanu wiedzy. Wynik przetwarzania jest następnie przesyłany do pozostałych węzłów tak, aby każdy uczestnik był świadomy transakcji, które są aktualnie przetwarzane. Następnie każdy z uczestników głosuje nad poprawnością transakcji. Konsensus jest osiągany na podstawie większości głosów.

Efekt synergii, wynikający z implementacji zasygnalizowanych technologii, przyczynił się do utworzenia systemów informatycznych o określonych cechach jakościowych, takich jak [Panda i in. 2018]:

1. Niezmienność (*immutability*) i niezaprzeczalność (*non-repudiation*) – ta cecha jest najistotniejsza i najbardziej pożądana, aby utrzymać autonomię transakcji w łańcuchu bloków. Oznacza ona, że transakcja raz wprowadzona do łańcucha bloków nie może zostać zmieniona i każdy węzeł uczestniczący w łańcuchu ma jej kopię. Z czasem, gdy kolejne bloki są dołączane do łańcucha, dokonanie jednoczesnej zmiany we wszystkich węzłach staje się praktycznie niemożliwe. Transakcje są zabezpieczone kryptograficznie, co jeszcze minimalizuje ryzyko dokonania zmiany w łańcuchu.

2. Odporność na fałszerstwa (*forgery resistant*) – technologia *blockchain* uniemożliwia dokonanie zmian w pojedynczym bloku ze względu na zastosowanie *hash* kryptograficznych oraz cyfrowych podpisów sygnujących każdą transakcję. Uważa się, że nawet moce obliczeniowe komputerów kwantowych nie są w stanie dokonać jednoczesnej zmiany (w tym przypadku fałszerstwa) we wszystkich węzłach połączonych w danym łańcuchu bloków. Biorąc tę cechę pod uwagę, można powiedzieć, że praktycznie systemy *blockchain* są odporne na fałszerstwa i inne ataki cyfrowe.

3. Demokracja (*democratic*) – systemy *blockchain* skonstruowane są jako sieci *peer-to-peer*, co oznacza, że każdy uczestnik ma takie same prawa jak wszyscy pozostali.

4. Odporność na podwójne wydatki (*double-spent resistant*) – cecha ta jest łatwa w utrzymaniu w systemach zarządzanych centralnie, gdyż jednostka centralna jest świadoma każdej transakcji. W systemach *blockchain* zapewnienie tej właściwości jest możliwe tylko w sytuacji, kiedy dany blok ma dostęp do wszystkich transakcji wykonanych w obrębie danego systemu aż do węzła podstawowego (*genesis node*) w celu walidacji poprawności transakcji.

5. Konsystencja księgi głównej (*cosistent state of the ledger*) – cecha ta zakłada niezmienność transakcji w obrębie księgi głównej. Jest na osiągana w systemach *blockchain* przez wybór odpowiedniego dla danego systemu biznesowego mechanizmu konsensusu.

6. Odporny na usterki (*resilient*) – usterka pojedynczego węzła nie powinna wpłynąć na konsystencję całego łańcucha bloków. Transakcje zawarte w obrębię pojedynczych bloków pozostają niezmienne w przypadku utraty połączenia sieciowego przez pojedyncze węzły lub awarii spowodowanych przez utratę pakietu danych w trakcie transmisji.

7. Gotowość do audytu (*auditable*) – wszystkie transakcje, bieżące i historyczne, są przechowywane w niezmienionej postaci w łańcuchach bloków. Cecha ta umożliwia przeprowadzenie kontroli takiej księgi głównej przez jednostki zewnętrzne w celu potwierdzenia prawidłowości transakcji.

Transakcja jest elementarną składową systemu *blockchain*. Proces dodania nowej transakcji do pojedynczego bloku i uznania jej w obrębie systemu za prawidłową jest wieloetapowy. Warto zwrócić uwagę na najistotniejsze kroki, które zapewniają, że cechy jakościowe systemu są spełnione.

Nowa transakcja jest transmitowana w sieci bloków, co oznacza, że każdy węzeł otrzymuje informacje o dodaniu nowego wpisu w tym samym czasie po to, aby potwierdzić lub odrzucić jego prawidłowość i autentyczność. Poszczególne węzły mogą grupować transakcje w celu budowania nowego bloku i propagować nowy blok transakcji.

Decyzja o dodaniu nowego bloku powinna być podejmowana autonomicznie przez każdy z węzłów zarejestrowanych w systemie na podstawie przyjętego konsensusu. Jeśli konsensus zostanie osiągnięty, nowy blok zostaje dodany do bieżącego łańcucha. Nowo dodany blok będzie przechowywać skrót (*hash*) poprzedniego bloku, co pozwala na zachowanie struktury danych w systemie.

2. Architektura systemów *Blockchain 2.0*

Omówione w poprzednim rozdziale cechy jakościowe systemów *blockchain* przyczyniły się do powszechnego przekonania, że systemy te są godne zaufania na tyle, aby rozszerzać ich podstawową funkcjonalność (zarządzanie kryptowalutami) o inne obszary zastosowań, w których następuje zarzadzanie dobrami materialnymi lub niematerialnymi stanowiącymi podstawę wolnego rynku. W tabeli 1 zaprezentowano przykłady możliwych rodzajów transakcji, które mogą zostać zaimplementowane w technologii *blockchain*.

Tabela 1. Przykłady towarów materialnych, niematerialnych i usług będących przedmiotem obrotu w systemach *blockchain*

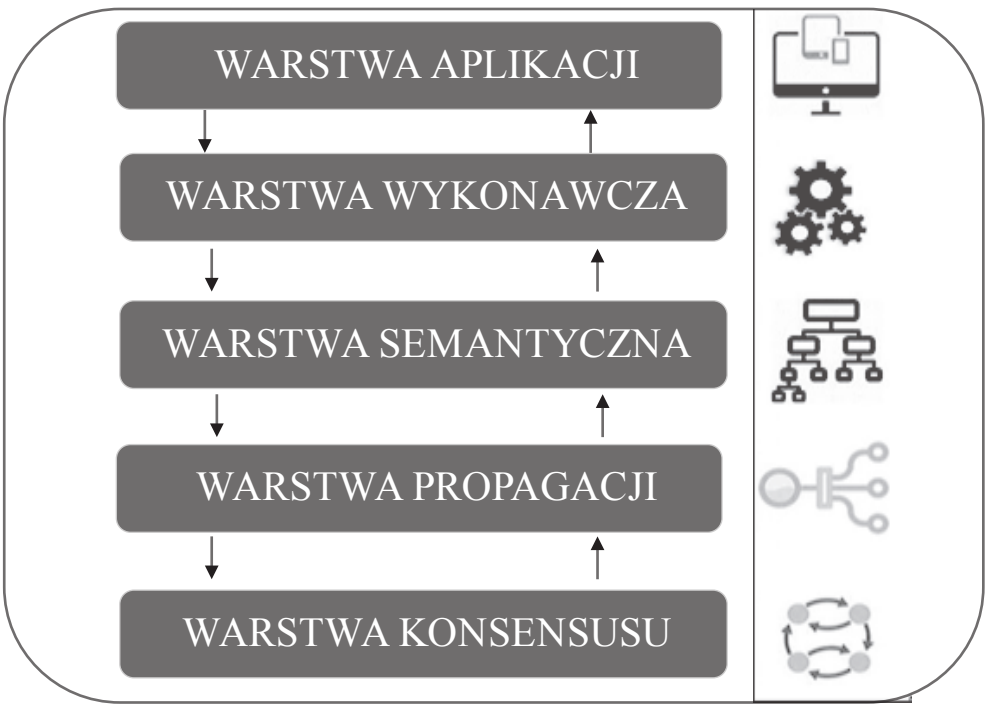
Rodzaj towaru lub usługi będący przedmiotem transakcji	Przykłady
Transakcje wielostronne	transakcje powiernicze, umowy wiązane, arbitraż zewnętrzny, transakcje podpisu wielostronnego
Transakcje finansowe	akcje, *crowdfunding*, obligacje, fundusze inwestycyjne, instrumenty pochodne, renty, emerytury
Dane dotyczące rejestrów publicznych np. sądy, urzędy statystyczne, urzędy miejskie	tytuły ziemi i własności, rejestracje pojazdów, zezwolenia na prowadzenie działalności, akty małżeństwa, akty zgonu
Dokumenty identyfikacyjne	prawa jazdy, dowody osobiste, paszporty, rejestracje wyborców
Dane dotyczące rejestrów prywatnych np. banki, notariusz	pożyczki, kontrakty, zakłady, podpisy, testamenty, depozyty
Zaświadczenia	dowód ubezpieczenia, dowód własności, dokumenty poświadczone notarialnie
Dobra materialne	domy, pokoje hotelowe, samochody do wynajęcia, dostęp do samochodów
Dobra niematerialne	patenty, znaki towarowe, prawa autorskie, zastrzeżenia, nazwy domen

Źródło: opracowanie własne na podstawie [Swam 2015].

Rozszerzenie przedmiotu transakcji poza kryptowaluty stanowi krok milowy w rozwoju tej klasy systemów i przyczyniło się do powstania *Blockchain 2.0*, który przez cześć autorów jest utożsamiany z technologiami rozproszonych rejestrów (*Distributed Ledger Technology* − DLT). Dane w DLT są przechowywane w postaci ciągłej, bez podziału na bloki, ponadto konsensus może być osiągnięty między ograniczoną liczbą uczestników − tzw. walidatorów, którym przyznawane jest większe zaufanie niż pozostałym członkom sieci [Piech (red.) 2016, s. 14]. Można postawić tezę, że dopiero systemy *Blockchain 2.0* znajdują zastosowanie w świecie biznesowym, w którym przedmiotem transakcji nie jest wirtualna waluta, lecz tradycyjne dobra zbywalne będące w realnym obrocie rynkowym.

Jeśli podejdziemy do technologii *blockchain* jak do klasy systemów informatycznych, należy się zastanowić nad ich elementami składowymi oraz wzajemnymi relacjami.

Autorzy Dhameja, Sekhar oraz Singhal zaproponowali architekturę systemów *Blockchain 2.0*, która składa się pięciu warstw (*leyers*) zaprezentowanych na rys. 2 (por. [Panda i in. 2018]). Każda z warstw odgrywa inną rolę i jest odpowiedzialna za egzekucję określonej funkcjonalności determinującej system *Blockchain 2.0* jako całość.



Rys. 2. Warstwy systemu *Blockchain 2.0*

Źródło: opracowanie własne na podstawie [Panda i in. 2018].

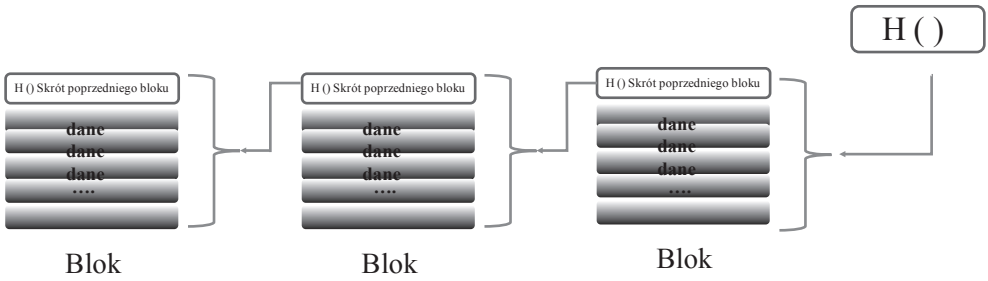
Warstwa aplikacji w systemach *blockchain* jest odpowiedzialna za komunikację z użytkownikami, dostarczając im określonych funkcjonalności oraz usług informatycznych definiowanych na poziomie biznesowym.

Rozwój aplikacji, których środowiskiem backendowym jest *blockchain*, wymaga, podobnie jak w klasycznych rozwiązaniach, kompetencji i środowiska programistycznego (*development framework*). W związku z faktem, że ideą systemów *blockchain* jest praca w środowisku rozproszonym, sugerowaną technologią implementacyjną są aplikacje hostowane na serwerach webowych, gdzie wymagane jest programowanie funkcji na poziomie serwera oraz API odpowiedzialnego za komunikację z użytkownikami. Dla użytkownika systemu *Blockchain 2.0* warstwa aplikacji stanowi warstwę biznesową, w której możliwe jest procesowanie transakcji z zachowaniem wszystkich zasad i technologii dostępnych w obrębie danej sieci.

Warstwa wykonawcza jest odpowiedzialna za egzekucję instrukcji, które są wywoływane przez warstwę aplikacyjną na poziomie każdego bloku w łańcuchu. Instrukcje stanowią pojedyncze skrypty, algorytmy lub programy, takie jak *smart contracts*. Każdy blok w łańcuchu w celu zatwierdzenia transakcji musi wykonać ten sam zbiór instrukcji niezależnie. Deterministyczne wykonanie określonej instrukcji na tym samym zbiorze danych wejściowych oraz przy tych samych warunkach ograniczających zawsze dostarcza ten sam set danych wyjściowych we wszystkich blokach łańcucha. Cecha ta pozwala na zachowanie spójności danych w systemie rozproszonych rejestrów.

Warstwa semantyczna definiuje strukturę logiczną danego łańcucha bloków. Każda transakcja prawidłowa lub nie jest przetwarzana na poziomie warstwy wykonawczej, ale dopiero na poziomie warstwy semantycznej następuje jej walidacja i w konsekwencji zatwierdzenie lub odrzucenie. Warstwa ta jest odpowiedzialna za definiowanie zasad systemowych, modeli danych oraz ich struktury. Jedną z popularnych struktur danych implementowaną w systemach *blockchain* są drzewa skrótów zdefiniowane w latach 70. ubiegłego wieku, co uczynił Ralph Merkle [Klinger i in. 2017, s. 15]. Struktura danych w drzewie skrótów polega na haszowaniu pary elementów, najczęściej na poziomie liści, a następnie następuje ponowne haszowanie wyników i przekazanie ich do kolejnego w hierarchii węzła aż do węzła generycznego (*markle root*) [Panda i in. 2018]. Przepływ danych następuje od korzeni drzewa do jego węzła generycznego. Struktura ta jest odporna na wprowadzenie nieautoryzowanych transakcji, gdyż praktycznie niemożliwe jest wprowadzenie jednoczesnej zmiany na każdym poziomie drzewa. Przykładem implementacji struktury drzewa skrótów jest *bitcoin*.

Inną strukturą danych stosowaną w systemach *blockchain* są funkcje skrótów (*hash pointers*) szyfrujące transakcje danego bloku. Każdy blok przechowuje swoją funkcję skrótu oraz pamięta funkcję skrótu swojego poprzednika aż do bloku generycznego [Drescher 2017].



Rys. 3. Struktura danych oparta na funkcjach skrótu

Źródło: opracowanie własne na podstawie [Panda i in. 2018].

W warstwie semantycznej poza strukturą danych definiowane są także zasady walidowania transakcji w systemie. To na tym poziomie projektanci systemu implementują inteligentne kontakty (*smart contracts*), które są autonomicznymi algorytmami lub miniprogramami wykonującymi w trakcie realizacji transakcji dodatkowe operacje zapisane w ich kodzie [Klinger i in. 2017, s. 17]. Szerokie zastosowanie inteligentnych kontraktów pozwala na tworzenie nowych dóbr wirtualnych stanowiących wartość biznesową w określonym systemie *blockchain*. Funkcja ta otwiera szeroki wachlarz implementacyjny, który nie jest już tylko ograniczony do wirtualnej waluty.

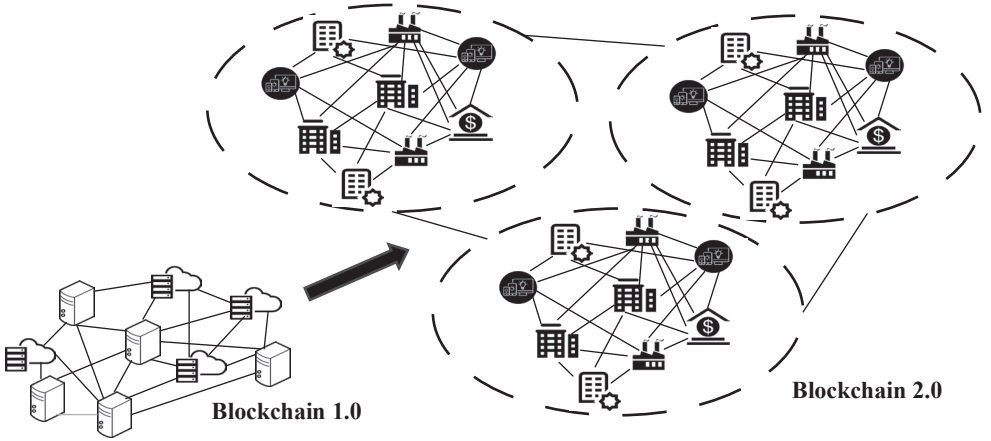
Warstwa propagacji jest odpowiedzialna za definicję komunikacji oraz synchronizację w obrębie sieci *blockchain*. Z założenia sieć *blockchain* jest siecią *peer-to-peer*, w której każdy z węzłów jest autonomiczny i nie ma jednostki centralnej zatwierdzającej transakcje. Projektując warstwę propagacji, należy więc zapewnić widoczność wszystkich węzłów wchodzących w skład łańcucha oraz zasady dodawania nowych węzłów tak, aby stały się równorzędnymi członkami sieci. Po zapewnieniu widoczności poszczególnych węzłów kolejnym aspektem jest ustalenie zasad synchronizacji bloków oraz transakcji między członkami łańcucha z zachowaniem ustalonych zasad akceptacji transakcji (konsensusu danej sieci *blockchain*). W przypadku sieci Bitcoin węzły po wygenerowaniu nowego bloku natychmiast podejmują próbę jego walidacji w całej sieci. Jeśli blok ten przejdzie poprawną walidację na poziomie warstwy konsensusu, to następuje jego synchronizacja w obrębie całej sieci. W takim przypadku kluczowe, z punktu widzenia danego węzła, stają się jego lokalne uwarunkowania, takie jak moc obliczeniowa czy przepustowość lokalnej sieci, które w realny sposób mogą opóźnić synchronizację nowego bloku. Jeśli więc techniczne uwarunkowania wpływają na rolę danego węzła, można zadać pytanie, czy rzeczywiście na poziomie biznesowym możemy mówić o przetwarzaniu *peer-to-peer*, skoro lepsze technicznie węzły są w stanie realnie wytworzyć większą ilość dóbr (np. kryptowaluty) będących przedmiotem obrotu danego systemu.

Definiując warstwę propagacyjną, można wyobrazić sobie inne scenariusze propagacyjne zdefiniowane w obrębie danej sieci *blockchain*, które, jeśli jest potrzeba, mogą adresować ograniczenia techniczne pojedynczych węzłów. Na przykład synchronizacja bloków może następować w określonym czasie, żeby zminimalizować zależności od bieżącej przepustowości sieci oraz mocy obliczeniowej. Można też przyjąć zasadę, że to bloki będą synchronizowane, a nie pojedyncze transakcje. Scenariuszy może być wiele, co otwiera wiele możliwości implementacyjnych i biznesowych. Jedyną niepodważalną zasadą powinno być przetwarzanie *peer-to-peer*.

Warstwa konsensusu jest najważniejszą i bazową warstwą z punktu widzenia założeń biznesowych systemów *blockchain*. Na tym poziomie definiowany jest konsensus, na podstawie którego zatwierdzane są transakcje lub bloki w obrębie całej sieci. Podstawowym zadaniem każdej sieci *blockchain* jest osiągniecie zgodności wszystkich węzłów co do jednej właściwej wersji zbioru rejestrów księgi głównej (*consistent state of the ledger*). Każdy z systemów *blokchain* może implementować i realizować inny algorytm konsensusu, jednak co do założenia wynik jego działania ma za zadanie zatwierdzić jedną, wspólną w obrębie sieci wersję rejestru bez udziału trzeciej arbitralnej strony. Bezpieczeństwo, jednoznaczność oraz siła danej sieci są mierzone efektywnością algorytmu konsensusu. W publicznych sieciach, takich jak *Bitcoin* czy *Ethereum*, wykorzystywany jest mechanizm konsensusu oparty na dowodzie pracy (PoW), kiedy nowy blok jest dodany dopiero po sprawdzeniu, czy zawiera on wszystkie transakcje, oraz po wykonaniu określonego zadania obliczeniowego. Dopiero po spełnieniu obu warunków sieć jest rozszerzona o nowy blok.

Warto nadmienić, że w warstwie konsensusu będą także definiowane tzw. inteligentne kontrakty (*smart contracts*), stanowiące skompilowany kod programistyczny zintegrowany z kodem całego rejestru i rozporoszony w obrębie wszystkich węzłów sieci. Oznacza to, że implementując inteligentne kontrakty w danym systemie blochchain, można odwzorować zasady biznesowe oraz procesy, które definiują sposób dokonywania i przebieg transakcji (por. [Piech (red.) 2016, s. 13; Bartoletti 2017]).

Stwarza to zupełnie nowe możliwości zastosowań biznesowych, podnosząc systemy *Blockchain 2.0* do klasy systemów wspierających zarządzanie. Współdzielona księga główna, zasady biznesowe odwzorowane w inteligentnych kontraktach, odpowiedni poziom bezpieczeństwa oraz zaufanie stron transakcji umożliwia budowanie współdzielonych między różnymi podmiotami gospodarczymi procesów biznesowych (por. [Prusty 2018]), a co za tym idzie − przeniesienie idei węzła z pojedynczej jednostki obliczeniowej na pojedynczy podmiot gospodarczy. Rysunek 4 prezentuje transformację sieci *Blockchain 1.0*, którą stanowią pojedyncze węzły obliczeniowe wykorzystywane do tworzenia nowych jednostek kryptowaluty w kierunku tworzenia sieci podmiotów gospodarczych realizujących współdzielone procesy biznesowe (sieci *Blockchain 2.0*).



Rys. 4. Kierunek transformacji systemów *blockchain*

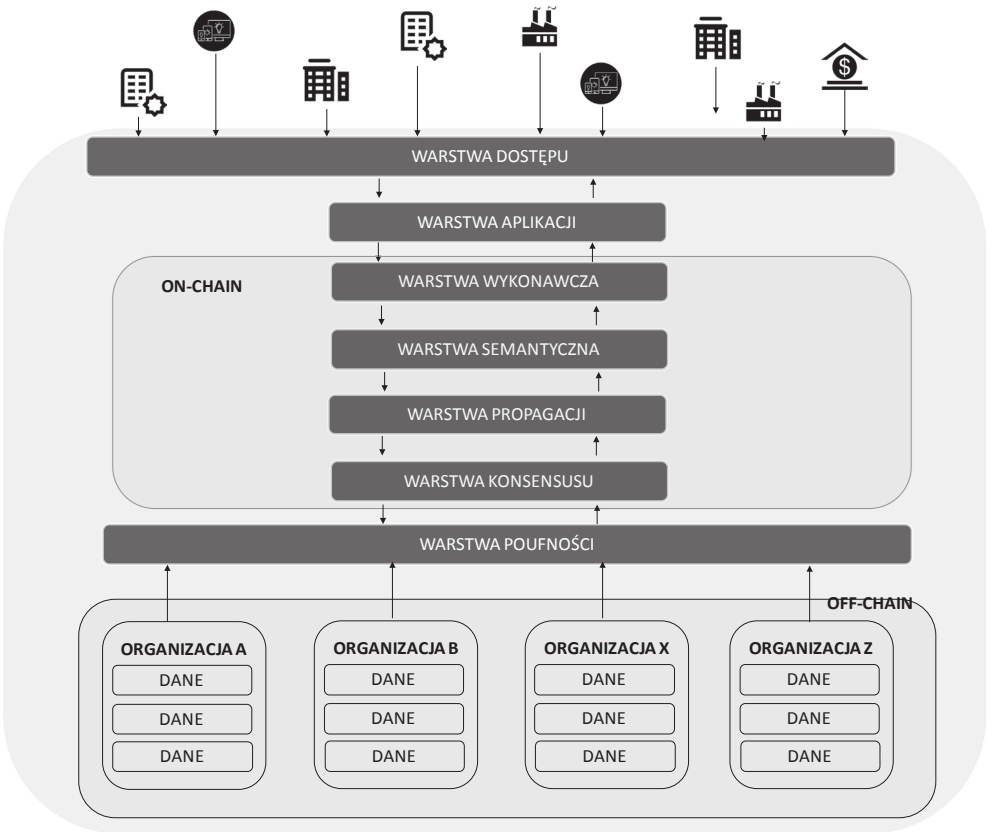
Źródło: opracowanie własne.

Aby w pełni można było zaimplementować technologię *Blockchain 2.0* na gruncie współdzielonych procesów biznesowych, należy rozważyć dwa dodatkowe aspekty wpływające na architekturę.

Po pierwsze – dostęp do sieci. Systemy *Blockchain 2.0* są przykładami prywatnych sieci łączących jednostki, które wewnętrznie decydują o podmiotach mogących do danej sieci dołączyć. W przeciwieństwie do sieci publicznych, które są charakterystyczne dla obrotu kryptowalutami, prywatne sieci *blockchain* tworzą współdzieloną księgę główną transakcji dystrybuowaną wśród węzłów sieci, które są z góry określone i predefiniowane przez realizowane procesy biznesowe. Systemy *Blockchain 2.0* są raczej dedykowane sieciom przedsiębiorstw lub społeczności, które już realizują wspólne procesy biznesowe, niż szeroko rozumianej społeczności internetowej. Na poziomie architektury warstwę tę można nazwać warstwą dostępu (*permission layer*).

Drugim aspektem, istotnym dla implementacji systemów *Blockchain 2.0* w jednostkach gospodarczych, jest możliwość decydowania o rodzaju danych, które będą przetwarzane w systemie. Wiele firm, mając dane poufne, zwłaszcza dotyczące danych osobowych, ze względu na obowiązujące w Europie przepisy nie może danych tych udostępniać podmiotom zewnętrznym. Dlatego istotne jest zdefiniowanie zakresu transakcji przetwarzanych w obrębie sieci (*on-chain*) oraz wyodrębnienie tych danych, które będą przetwarzane poza siecią (*off-chain*) (por. [Xiwei 2017]).

Rysunek 5 prezentuje wzbogaconą architekturę systemów *Blockchain 2.0*.



Rys. 5. Architektura systemów *Blockchain 2.0*

Źródło: opracowanie własne.

Warstwa dostępu definiowana jest przez uczestników sieci i jej zadaniem jest ustalenie zasad dotyczących przyjmowania nowych członków. Jej implementacja może być jedynie na gruncie biznesowm odwzorowana w tradycyjnych kontraktach podpisywanych między poszczególnymi firmami. Automatyczną realizację warstwy dostępu można zaimplementować na poziomie inteligentnych kontraktów. Ich kod wzbogacony o zasady dostępu podmiotów do danego łańcucha można rozstrzygać przez odpowiednie modyfikacje mechanizmu konsensusu przeniesionego na grunt zarządzania dostępem.

Warstwa poufności ma za zadanie automatyczne definiowanie zakresu transakcji przetwarzanych w obrębie łańcucha. Założenie to daje duże możliwości implementacyjne na gruncie biznesowym, gdyż pozostawia uczestnikom sieci decyzje o rodzaju transakcji będącej przedmiotem przetwarzania wewnątrz sieci (*on-chain*).

Podstawowe przesłanki do rozgraniczenia warstw przetwarzania w systemach *blockchain* stanowią ograniczenia techniczne, takie jak moc obliczeniowa danej jednostki, przepustowość lokalnej sieci oraz przestrzeń dyskowa potrzebna do przechowywania kopii całego rejestru na poziomie pojedynczego węzła. Multiplikacja transakcji między wszystkimi węzłami powoduje wykładniczy przyrost danych, które muszą być przechowywane lokalnie i powielane w obrębie łańcucha w momencie zatwierdzenia nowej transakcji, co skutecznie wydłuża czas przetwarzania pojedynczej transakcji. Stąd też idea definiowania metadanych i przechowywania ich bezpośrednio w systemie *blockchain* (*on-chain*) oraz przechowywanie prywatnych danych poza systemem (*off-chain*). Zasadę tę można transponować na grunt zasad biznesowych i definiować metadane biznesowe, czyli takie dane, które uczestnicy sieci uznają za przedmiot transakcji. Natomiast pozostałe typy transakcji można przechowywać w systemach prywatnych, niebędących elementami architektury systemu *blockchain*.

3. Zakończenie

Twórcy technologii *blockchain* wykorzystują znane koncepty technologiczne, takie jak przetwarzanie rozproszone *peer-to-peer*, kryptografia oraz teoria gier (por. [Badr 2018]). Każdy z tych konceptów ma zastosowanie w IT od wielu lat, jednak połączenie ich w celu budowania rozproszonych sieci biznesowych przechowujących i przetwarzających transakcje biznesowe stanowi istotny krok w rewolucji technologicznej, której jesteśmy świadkami.

Wielu cytowanych w niniejszym artykule autorów wskazuje, że systemy *Blockchain 2.0* stanowią przykład technologii rewolucyjnej determinującej zmiany w podejściu do systemu zarządzania oraz systemów ekonomicznych funkcjonujących we współczesnej gospodarce (por. [Hofmann 2018]). Autonomiczna i niezależna od zewnętrznych instytucji autoryzacja transakcji następuje wewnątrz systemu *blockchain*. Algorytm, któremu jest przyznany odpowiedni poziom zaufania biznesowego, może zastąpić jednostki centralne (takie jak instytucje finansowe, banki czy urzędy) w procesie walidacji poprawności transakcji gospodarczych. Jednak aby osiągnąć ten cel, konieczne jest prezentowanie spójnych i implementowanych systemów, które można odpowiednio skalować i wdrażać w sieciach biznesowych.

W artykule zaprezentowana została koncepcja architektury systemów *Blockchain 2.0*, zarządzana przez poszczególne warstwy: od aspektów czysto algorytmicznych przez wydajnościowe aż po aspekt biznesowy. Ciągle jeszcze systemy *blokchain* są w fazie rozwoju, w której problemy stanowią czas przetwarzania transakcji oraz wydajność, wysokie koszty utrzymania, uwzględniające koszty przechowywania danych czy poziom dostępności do danych. Rozwiązanie tych problemów jest głównym kierunkiem badawczym wielu globalnych firm, widzących w systemach *blockchain* zastosowanie komercyjne.

W dalszych pracach badawczych autor chciałby się skoncentrować na procesie projektowania systemów *Blockchain 2.0* uwzględniających omówione aspekty architektoniczne.

Literatura

Badr B., 2018, *Blockchain by Example*, Packt Publishing, ISBN 9781788475686.

Bartoletti M., Po mpianu L., 2017, *An empirical analysis of smart contracts: platforms, applications, and design patterns*, Lecture Notes in Computer Science, https://www.researchgate.net/publication/315454656_An_Empirical_Analysis_of_Smart_Contracts_Platforms_Applications_and_Design_Patterns, dostęp: 11.11.2018.

Bitcoin, 2008, https://bitcoin.pl/manifest-satoshi-nakamoto/, dostęp: 15.11.2018.

Deloitte, 2017, https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Reports/pl_Blockchain-technology-and-its-potential-in-taxes-2017-PL.PDF, dostęp: 17.09.2018.

Drescher D., 2017, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, Apress, ISBN 9781484226049.

Hofmann E.U.M., Bosia N., 2018, *Supply Chain Finance and Blockchain Technology*, Springer. ISBN 978-3-319-62371-9.

Klinger B., Szczepański J., 2017, *Blockchain − historia, cechy i główne obszary zastosowań*, http://czasopisma.uksw.edu.pl/index.php/cwc/article/view/1858/1682, dostęp: 17.09.2018.

Panda P.S., Singhal B., Dhameja G.,2018, *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions*, Apress, ISBN 9781484234440.

Prusty N., 2018, *Blockchain for Enterprise*, Packt Publishing, ISBN: 9781788479745.

Piech K. (red.), 2016, *Leksykon pojęć na temat technologii Blockchain i kryptowalut*, https://www.gov.pl/documents/31305/0/leksykon_pojec_na_temat_technologii_blockchain_i_kryptowalut.pdf/77392774-1180-79ab-4dd5-089ffab37602, dostęp: 15.11.2018.

Santos M., Moura E., 2019, *Hands-On IoT Solutions with Blockchain*, Packt Publishing Ltd., ISBN 9781789132243.

Schwöbel Ch., Bensberg F., Gerth Ch., Potenziale von, *Blockchain 2.0 in der Energiewirtschaft − Analyse einer Applikation für einen lokalen Energiemarkt auf Basis von Smart Contracts*, https://www.researchgate.net/publication/329894290_Potenziale_von_Blockchain_20_in_der_Energiewirtschaft_-_Analyse_einer_Applikation_fur_einen_lokalen_Energiemarkt_auf_Basis_von_Smart_Contracts, dostęp: 12.12.2018.

Swam M., 2015, *Blockchain*, O'Reilly Media, Inc., ISBN 9781491920497.

Xiwei Xu, Pautasso C., Zhu L., Gramoli V., Ponomarev A., Chen Sh., 2016, *The Blockchain as a Software Connector*, https://ieeexplore.ieee.org/abstract/document/7516828, dostęp: 12.12.2018.

Xiwei Xu, Weber I., Staples M, Zhu L., Bosch J., Bass L., Pautasso C., Rimba P., 2017, *A Taxonomy of Blockchain-Based Systems for Architecture Design*, https://ieeexplore.ieee.org/document/7930224, dostęp: 12.12.2018.