Technologia blockchain – możliwości zastosowania

Eduard Vaskovskyi

Student Szkoły Głównej Handlowej w Warszawie

listopad 2018

ALTERUM
Ośrodek Badań i Analiz Systemu Finansowego

❖ Spis treści

Rozdział III

Wstęp

Tematem niniejszej pracy jest technologia blockchain w kontekście potencjalnego wykorzystania w sektorze usług finansowych i innych dziedzinach. Wraz z rozwojem innowacyjności działanie technologii wykracza poza zwykle dokonywanie płatności za pomocą kryptowalut. Pojawiają się pierwsze praktyczne zastosowania technologii rozproszonych rejestrów. Banki centralne, rządy niektórych państw i największe instytucje finansowe analizują możliwe zastosowania technologii oraz jej wpływ na gospodarkę światową.

Podstawę do napisania pracy stanowiły publikacje, określające algorytmy stosowanych technologii informatycznych i kryptograficznych, raporty instytucji finansowych na temat możliwych zastosowań blockchain w sferze finansów. Literatura specjalistyczna jest ograniczona z uwagi na nowatorstwo i ciągłą postępowość technologii, większość literatury jest dostępna w języku angielskim. Warto zauważyć, że ze względu na spekulacje cenowe kryptowalut możliwości technologii często są przeszacowane, nie odzwierciedlają realnej wartości, nie obejmują zagrożeń i niedoskonałości zdecentralizowanego systemu.

Pierwszym podejściem opartym na blockchain był bitcoin, dlatego w pracy szczególną uwagę zwrócono na działanie tego systemu, który jest najbardziej znanym przykładem realizacji płatności bez pomocy pośredników oraz centralnych komputerów. Przyjmuje się, że nazwa „bitcoin" w znaczeniu waluty pisana jest małą literą, natomiast „Bitcoin" jako cały system transakcji w sieci – dużą. Ponieważ ostatnio w świecie finansów zrobiło się głośno na temat „magii" systemu blockchain, w pracy zostanie opisana metoda kryjąca się za magią. Na przykładzie Bitcoin zostanie pokazane historia i przyczyny powstania nowego narzędzia.

Przedmiotem pracy jest działanie technologii rozproszonego rejestru, która wykorzystuje bardzo zaawansowane narzędzia kryptograficzne, komputerowe oraz matematyczne w połączeniu z koncepcjami finansowymi.

Celem pracy jest rzetelne opisanie działania technologii blockchain. Zagadnienia poruszone w pracy dotyczą możliwości zastosowania zdecentralizowanego systemu w sferze bankowości i innych.

W pierwszym rozdziale wytłumaczone zostanie podłoże działania systemu, stosowane funkcje, za pomocą których możliwe jest przeprowadzenie transakcji między dwoma podmiotami bez udziału zaufanej trzeciej strony. Rozdział jest poświęcony analizie procesu przekazywania wirtualnej waluty za pomocą stosowanych narzędzi kryptograficznych oraz matematycznych, które zapewniają bezpieczeństwo i zaufanie między podmiotami. W rozdziale również pokazane zostaną niezbędne komponenty technologii, pochodzenie adresów w sieci, narzędzia szyfrowania informacji, wykorzystanie par kluczy do weryfikowania podpisów cyfrowych oraz będzie przedstawiony cykl życia transakcji Bitcoin.

Drugi rozdział pracy przedstawi stosowane narzędzia technologii blockchain, które wykraczają poza dokonanie płatności za pomocą kryptowalut, na przykład, możliwość zastosowania technologii przez rządy państw, stworzenie zdecentralizowanej uniwersalnej bazy danych w celu zmniejszenia kosztów operacyjnych i zawarcie inteligentnych umów *(smart contracts)* za pomocą blockchain. Zwrócono też szczególną uwagę na blockchain jako publiczną bazę danych wszystkich transakcji, które zostały kiedykolwiek wykonane i stanowią dowód na ich istnienie w sieci. Przedstawione zostaną również techniczne różnice pomiędzy blockchain prywatnym a publicznym, możliwe zastosowania, jak działają uprawnienia i w jakich przypadkach należy używać systemu łańcucha bloków.

Ostatni rozdział dotyczyć będzie potencjalnych zastosowań technologii, przedstawione będą platformy blockchain, aby zwrócić uwagę na różnice techniczne i możliwe implementacje. Analizie zostaną poddane działania powoływanych konsorcjów, mające na celu poszukiwanie rozwiązań wykorzystania technologii w sektorze usług finansowych, regulacji prawnych i rozwijanie tematu rozproszonego rejestru równolegle w wielu dziedzinach. Zostaną omówione również główne zalety i zagrożenia dla sektora usług finansowych

Ze względu na innowacyjność technologii najlepsze pomysły zastosowania technologii są w trakcie badań. Mimo tego, że nadal zostaje wiele pytań bez odpowiedzi, nie ulega wątpliwości, że nowe czasy wymagają nowego podejścia. Obecne procesy zmierzają w kierunku automatyzacji, gdzie rola pośrednika maleje. Banki, które będą w stanie zmienić dotychczasowe praktyki będą w stanie wykorzystać potencjał technologii do własnego rozwoju.

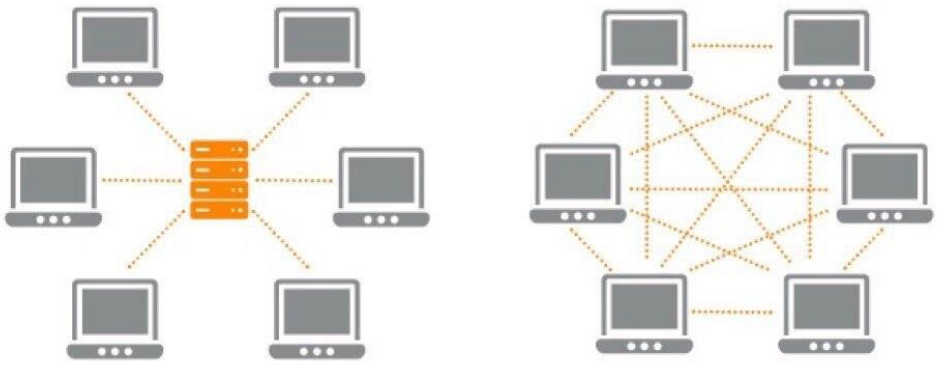
❖ ROZDZIAŁ I. Architektura blockchain na przykładzie Bitcoin'a

Systemy blockchain mogą wydawać się skomplikowane; jednak można je łatwo zrozumieć, badając indywidualnie każdy komponent technologii. Na wysokim poziomie, blockchain wykorzystuje dobrze znane mechanizmy informatyczne (połączone listy, rozproszone sieci), a także proste rozwiązania kryptograficzne (technologię hash, podpisy cyfrowe, klucze publiczne/prywatne) połączone np. z koncepcjami finansowymi (takimi jak księgi rachunkowe).

Bitcoin pozostaje najbardziej godnym uwagi systemem transferu środków, opartym na technologii blockchain, dlatego jest sens zacząć wprowadzenie do technologii poprzez zrozumienie jak łańcuch bloków działa na przykładzie kryptowaluty bitcoin, który jest również rozumiany jako system elektronicznego pieniądza funkcjonujący w ramach modelu płatności *peer-to-peer*, który łączy dwie strony transakcji bez udziału instytucji finansowych[1]. Cały system dokonywania płatności za pomocą kryptowaluty bitcoin oraz wszystkie techniczne aspekty działania i stworzenia zostały udostępnione w 2008 r. przez osobę o pseudonimie Satoshi Nakamoto. Przyczyny powstania tego typu systemu tłumaczono jako brak zaufania do instytucji finansowych, jak i związane z ich działalnością koszty transakcyjne. Dlatego stworzono *Elektroniczny system płatności oparty na dowodach kryptografii zamiast na zaufaniu, umożliwiając dowolnym dwóm podmiotom, wyrażającym taką chęć, realizacje transakcji bezpośrednio pomiędzy sobą bez potrzeby uczestnictwa dodatkowego, zaufanego podmiotu. Transakcje których wycofanie jest obliczeniowo niepraktyczne będą bronić sprzedawców przed oszustwami, zaś wprowadzenie rutynowych mechanizmów depozytowych z łatwością chroniłoby kupujących*[2].

[1] K. Perez, M. Urbaniak, Bitcoin – wirtualny eksperyment czy waluta przyszłości?, „Ruch Prawniczy, Ekonomiczny i Socjalistyczny", Rok LXXV – zeszyt 4 - 2013, s. 164.
[2] S. Nakamoto, 2009, „Bitcoin: A Peer-to-Peer Electronic Cash System", tłum. http://bitcoin.pl/o-bitcoinie/manifest-satoshi-nakamoto, data dostępu: 15.10.2017.

Rysunek 1. System, oparty na obsługiwaniu sieci za pomocą serwerów oraz „peer-to-peer" system



Obsługiwanie za pomocą serwerów Peer-to-peer

Źródło: https://www.wowza.com/uploads/images/Server-based-vs-P2P-network.jpg (data dostępu: 11.10.2017).

Bitcoin – to tylko jedno z możliwych zastosowań technologii blockchain, w której system może być wykorzystywany do obsługi różnorodnych transakcji (handel, waluty, akcje, udziały). Nadal trwają pracę nad wdrożeniem łańcucha bloków jako księgi rachunkowej w bankowości, systemie uwierzytelniania dokumentów, podpisu cyfrowego w administracji państwowej i zapisu notarialnego. Wszystkie te transakcje mogą odbywać się poza funkcjonującym od lat systemem – bez udziału instytucji zaufania publicznego, bezpośrednio pomiędzy stronami transakcji.

Dla zapewnienia zaufania użytkowników wykorzystuje się dwa mechanizmy kryptograficzne:

- cyfrowe podpisy na bazie klucza publicznego, pozwalające na uwierzytelnianie transakcji pomiędzy węzłami w sieci;
- funkcja skrótu (hash), która dokonuje dowód wykonanej pracy (*proof-of-work*) w sieci Bitcoin, czyli problem obliczeniowy, który swoim rozwiązaniem potwierdza, że została wykonana praca do jego rozwiązania.

Rola pośredników w świecie elektronicznych płatności polega na rozwiązaniu problemu wielokrotnego wydania tej samej wartości, odejmując odpowiednią kwotę z konta użytkownika po przeprowadzeniu transakcji. Dla tego, żeby cyfrowe dobra w sieci Bitcoin nie były w stanie w sposób niegraniczony powielać się, wykorzystywana jest kryptografia klucza publicznego oraz otwarty rejestr transakcji, zapisywany w tak zwanym łańcuchu bloków *(block chain).*

1.1 Kryptograficzne podłoże blockchain – funkcja Hash

Ważnym elementem technologii blockchain jest użycie kryptograficznych funkcji mieszania dla wielu operacji, takich jak mieszanie zawartości bloku. *Hashing* to metoda obliczania stosunkowo unikatowego formatu o stałym rozmiarze (nazywanego *message digest,* lub streszczeniem wiadomości) dla danych wejściowych o prawie dowolnym rozmiarze (np. plik, tekst lub obraz). Nawet najmniejsza zmiana danych wejściowych (na przykład pojedynczego bitu) spowoduje całkowite rozłączenie wyniku końcowego. Rysunek 2 pokazuje proste przykłady. Algorytmy skrótu są zaprojektowane w taki sposób, aby były jednokierunkowe (znane jako *preimage resistance*): obliczenie dowolnego wejścia, które odwzorowuje dowolne z góry określone wyjście, jest niewykonalne obliczeniowo. Jeśli pożądane są konkretne dane końcowe (wyjście), wiele danych wejściowych musi zostać wypróbowanych poprzez przepuszczenie ich przez funkcję mieszającą, dopóki nie zostanie znalezione wejście, które daje pożądany wynik. Algorytmy skrótu są również zaprojektowane tak, aby były odporne na kolizje (znane jako *second preimage resistance*): obliczenie dwóch lub więcej wejść, które wytwarzają ten sam wynik, jest niewykonalne obliczeniowo.

Rysunek 2. Przykład mieszania danych wejściowych za pomocą algorytmu SHA-256

Dane wejściowe	Wartości mieszane SHA-256
1	0x6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
2	0xd4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
Cześć!	0xdffd6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f

Źródło: opracowanie własne za pomocą SHA-256 generator

Algorytm hash, który jest stosowany w technologii blockchain - to algorytm *Secure Hash Algorithm* (SHA) o rozmiarze wyjściowym 256 bitów (SHA-256). Wiele komputerów obsługuje ten algorytm w oprogramowaniu, co przyspiesza obliczanie. Ten algorytm ma wyjście 32 (8-bitowe) znaków (pokazane wyżej, na Rysunku 2, jako 64-znakowy łańcuch szesnastkowy), co oznacza, że istnieje $2^{256} \approx 10^{77}$ możliwych wartości. Algorytm dla SHA-256, jak również innych, jest określony w Federal Information Processing Standard (FIPS) 180-4[3].

Ponieważ istnieje bardzo duża liczba możliwych wartości wejściowych i skończona liczba możliwych wartości podsumowania wyjściowego, możliwe jest wystąpienie kolizji, gdzie hash (x) = hash (y), (tj. mieszanie dwóch różnych wejść daje takie same wyniki wartości). Jednak jest bardzo mało prawdopodobne, aby takie dane wejściowe x i y, które wytworzyłyby ten sam wynik, były ważne w kontekście systemu blockchain (w tym przypadku oba są poprawnymi transakcjami blockchain), a także byłyby obliczane poprawnie obok siebie jednocześnie.

Zastosowany algorytm skrótu (SHA-256) jest odporny na kolizje, ponieważ aby znaleźć ten sam wynik w SHA-256, trzeba byłoby wykonać algorytm średnio około 2^{128} razy. Technologie blockchain pobierają listę transakcji i tworzą skrót "unikalnego znaku" (niepowtarzalna cyfrowa wartość) tej listy. Każda osoba z taką samą listą transakcji może wygenerować dokładnie ten sam „unikalny ciąg znaków". Jeśli zmieni się pojedyncza wartość w transakcji na liście, zmieni się treść tego bloku, dzięki czemu można łatwo wykryć nawet niewielkie zmiany jednego bitu.

[3] https://www.nist.gov/publications/secure-hash-standard - strona NIST *(National Institute of Standards and Technology)* - zawiera specyfikacje FIPS dla wszystkich algorytmów hash zatwierdzonych przez NIST, data dostępu: 12.03.2018.

1.2 Kryptografia z kluczem asymetrycznym

Podstawową technologią wykorzystywaną w technologiach blockchain jest kryptografia asymetryczno-kluczowa[4] (określana również jako kryptografia klucza publicznego/prywatnego). Kryptografia z kluczem asymetrycznym używa pary kluczy: klucz publiczny i klucz prywatny, które są matematycznie ze sobą powiązane. Klucz publiczny może zostać upubliczniony bez zmniejszania bezpieczeństwa procesu, ale klucz prywatny musi pozostać tajny, jeśli dane mają zachować ochronę kryptograficzną. Mimo że istnieje związek między tymi dwoma kluczami, klucz prywatny nie może być skutecznie określony na podstawie znajomości klucza publicznego.

Asymetryczna kryptografia kluczy używa różnych kluczy z pary kluczy do określonych funkcji, w zależności od tego, która usługa ma być świadczona. Na przykład przy cyfrowym podpisywaniu danych algorytm kryptograficzny wykorzystuje klucz prywatny do podpisania. Podpis można następnie zweryfikować za pomocą odpowiedniego klucza publicznego.

Wykorzystanie kryptografii klucza asymetrycznego w systemach blockchain wykorzystuje, że:

- Klucze prywatne służą do cyfrowego podpisywania transakcji.
- Klucze publiczne są używane do wyprowadzania adresów, umożliwiając podejście pseudonimiczne typu jeden do wielu (jedna para kluczy publicznych może generować wiele adresów, w niektórych przypadkach wiele par kluczy publicznych jest używanych do tworzenia wielu adresów).
- Klucze publiczne służą do weryfikowania podpisów generowanych za pomocą kluczy prywatnych.
- Kryptografia z kluczem asymetrycznym zapewnia możliwość sprawdzenia, czy użytkownik przekazujący wartość innemu użytkownikowi posiada klucz prywatny, który jest w stanie podpisać otrzymywanie wartości.

[4] Publikacja FIPS 186-4 Digital Signature Standard określa wspólny algorytm dla cyfrowego podpisu stosowanego w technologii blockchain: *Elliptic Curve Digital Signature Algorithm (ECDSA).*

1.3 Podpisy cyfrowe

W celu likwidowania pośrednika twórcy systemu wykorzystali kryptografię klucza publicznego oraz otwarty rejestr transakcji, który jest zapisywany w tak zwanym łańcuchu bloków. Rysunek 3 przedstawia proces bezpiecznego podpisu cyfrowego i weryfikacji.

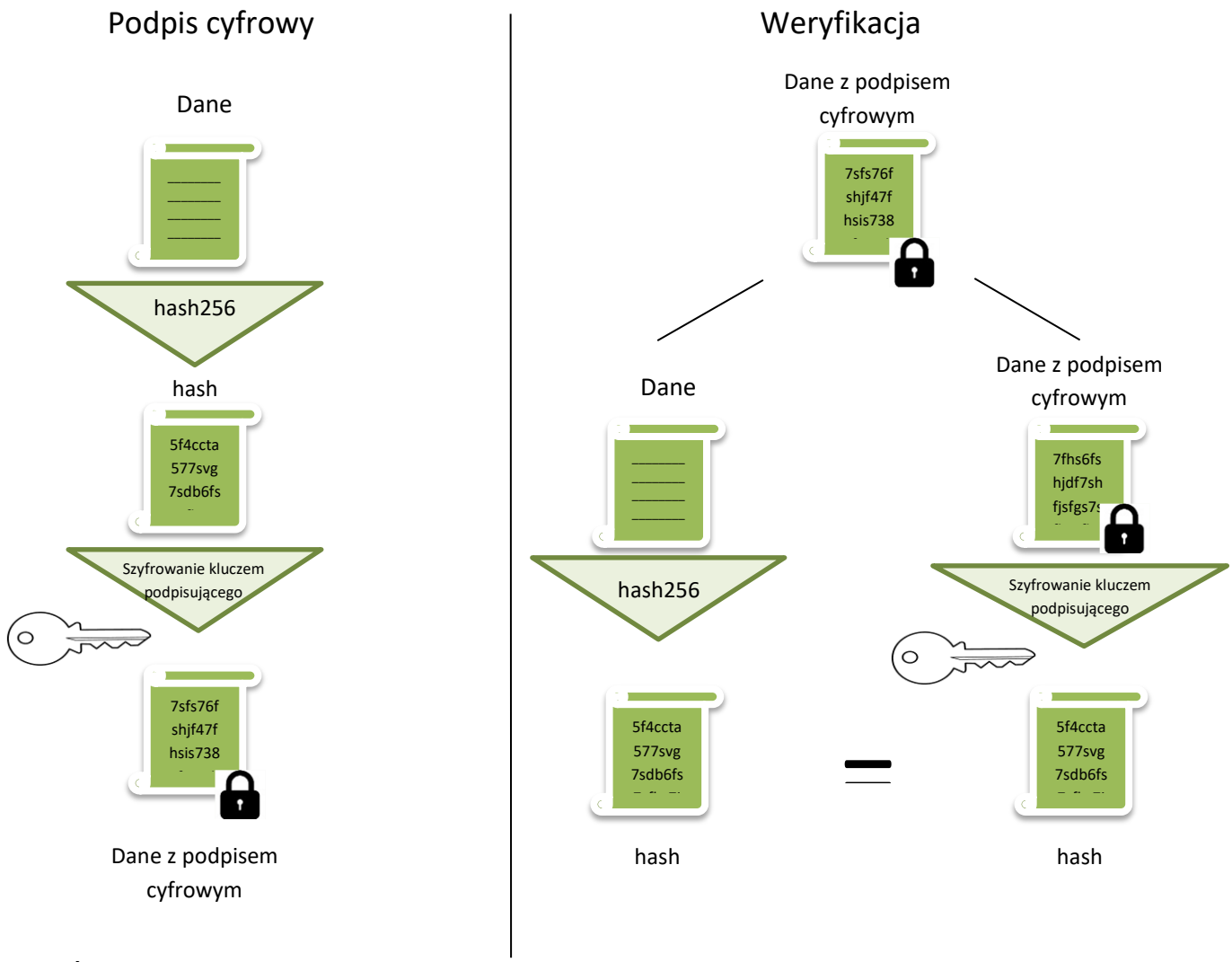
Każda informacja, która mieści się w bloku musi być zaszyfrowana za pomocą pary kluczy (publicznego i prywatnego). Z kolei podpisy cyfrowe są źródłem kryptografii klucza publicznego, która wykorzystuje parę kluczy do zapewniania integralności i pochodzenia komunikatu, innymi słowy sprawdza autentyczność informacji.

Komunikat jest dołączony do prywatnego klucza, znanego tylko przez nadawcę, który jest przechowywany w tajemnicy, służy do sprawdzenia wiarygodności wysyłanych wiadomości oraz odczytywania przez odbiorcę zaszyfrowanych treści; każdy z dostępem do klucza publicznego, powiązanego z nadawcą może następnie uwierzytelnić komunikat. Podpis ten jest unikalny dla każdego zestawu danych i zawiera informacje o nadawcy, treści i czasie zdarzenia *(timestamp)*. W uproszczeniu, działa to jako praktycznie unikalna pieczęć woskowa, która służy do uwierzytelniania nadawcy, udziela wiarygodności treści i zapobiega niezaprzeczalności.

Dla realizacji powyższego potrzebne są trzy algorytmy:

- Algorytm generowania kluczy, który jednocześnie generuje prywatny klucz podpisu i publiczny klucz weryfikacji. Para jest generowana tak, że istnieje związek matematyczny pomiędzy nimi, a klucz prywatny nie może pochodzić z klucza publicznego.
- Algorytm podpisywania, który miesza komunikat i wiąże prywatny klucz strony wysyłającej do wiadomości.
- Algorytm weryfikacji podpisu, który używa klucza publicznego, żeby zaakceptować odpowiedni klucz prywatny, aby podpisać skrót *(digest)*.

Rysunek 3. Proces bezpiecznego podpisu cyfrowego oraz weryfikacji

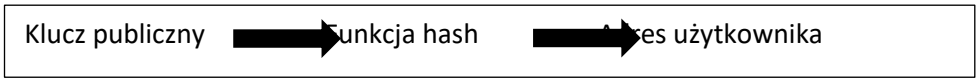


Źródło: opracowanie własne na podstawie: Credit Suisse, *Report Blockchain,* Europe/United Kingdom.

Ten proces jest używany od końca lat 70. w celu określenia integralności i autentyczności komunikatu i umożliwienia niezaprzeczalności jego źródła. Tożsamość i własność bitcoin zarządzana jest za pomocą znajomości prywatnego klucza; w tym sensie bitcoin jest instrumentem na okaziciela, w którym znajomość klucza prywatnego jest synonimem kontroli nad zawartością sparowanego adresu publicznego.

1.4 Adresy i pochodzenie adresów

Adres użytkownika jest krótkim, alfanumerycznym ciągiem pochodzącym z klucza publicznego użytkownika za pomocą funkcji mieszania (hash), wraz z dodatkowymi danymi (używanymi do wykrywania błędów). Adresy są używane do wysyłania i odbierania zasobów cyfrowych. Większość systemów blockchain używa adresów jako "do" i "z" punktów końcowych w transakcji. Adresy są krótsze niż klucze publiczne i nie są tajne. System wygenerowania adresów pobiera klucz publiczny, hashuje go i przekształca hash na tekst:



Użytkownicy mogą generować dowolną liczbę par kluczy (prywatny/publiczny), a więc adresów według potrzeb, co pozwala na różny stopień pseudoanonimowości. Adresy funkcjonują jako publiczna "tożsamość" w systemie blockchain dla użytkownika, a często adres jest konwertowany na kod QR[5] dla łatwiejszego użycia.

Kiedy blockchain dystrybuuje zasoby cyfrowe, robi to przez przypisanie ich do adresu. Aby wydać ten cyfrowy zasób, użytkownik musi udowodnić posiadanie odpowiedniego klucza prywatnego adresu. Podpisując cyfrowo transakcję za pomocą klucza prywatnego, transakcję można zweryfikować za pomocą klucza publicznego.

1.5 Transakcje

Transakcja w systemie blockchain jest to rejestracja transferu aktywów (waluty cyfrowej, jednostek towaru itp.) między stronami. Wynikiem tego będzie zapis na rachunku bieżącym za każde zdeponowanie lub wypłatę pieniędzy. Rysunek 4 pokazuje hipotetyczny przykład transakcji. Każdy blok w łańcuchu bloków zawiera wiele transakcji. Pojedyncza transakcja zwykle wymaga co najmniej następujących pól informacyjnych, ale może zawierać więcej:

- Kwota - całkowita kwota cyfrowego zasobu (np. kryptowalut) do przesłania.

[5] Kod QR, QR Code (ang. *Quick Response*, QR: szybka odpowiedź) – alfanumeryczny, dwuwymiarowy, matrycowy, kwadratowy kod graficzny, http://www.qrcode.com/en/about/ data dostępu: 22.03.2018.

- Wejścia (w tym przypadku rozumiane jako nadawca) - lista cyfrowych zasobów do przesłania (ich całkowita wartość jest równa kwocie). Należy pamiętać, że każdy zasób cyfrowy jest jednoznacznie identyfikowany i może mieć różne wartości z innych zasobów. Jednak zasobów nie można dodawać ani usuwać z istniejących zasobów cyfrowych. Zamiast tego zasoby cyfrowe można podzielić na wiele nowych zasobów cyfrowych (każdy z mniejszą wartością) lub połączyć w celu utworzenia mniejszej ilości nowych zasobów cyfrowych (każdy o odpowiednio większej wartości).
- Wyjścia (odbiorca) - konta, które będą odbiorcami zasobów cyfrowych. Każde wyjście określa wartość, która ma zostać przekazana nowemu właścicielowi, tożsamość nowego właściciela (właścicieli) i zestaw warunków, które muszą spełnić nowi właściciele, aby otrzymać tą wartość. Jeśli udostępnione zasoby cyfrowe są większe niż wymagane, dodatkowe środki są zwracane do nadawcy (jest to mechanizm "wprowadzania zmian").
- Identyfikator transakcji/hash - unikalny identyfikator każdej transakcji. Niektóre łańcuchy bloków używają identyfikatora, a inne pobierają skrót (hash) danej transakcji jako unikalny identyfikator.

Rysunek 4. Przykład transakcji

	Wejście (Nadawca)	Wyście (Odbiorca)	Kwota	Razem
Identyfikator transakcji: 0xa3b5c1	Konto A	Konto B	0.0537	
		Konto C	2.7000	
				2.7537

Źródło: opracowanie własne

Ważne jest ustalenie ważności transakcji. Tylko dlatego, że ktoś twierdzi, że transakcja miała miejsce, nie oznacza, że tak naprawdę się stało. Transakcje są podpisywane i można je zweryfikować za pomocą par kluczy publicznych/prywatnych w dowolnym momencie

Użytkownicy sieci Bitcoin wykorzystują wirtualną walutę bitcoin do wykonania transakcji. Aby móc przesłać odpowiednią ilość bitcoinów, użytkownik musi posiadać

wirtualny portfel, który służy do przechowywania wirtualnej waluty – jest to pojedynczy plik, który zawiera wszystkie BTC, posiadane przez użytkownika[6]. W celu posiadania takiego portfela trzeba zainstalować darmowe oprogramowanie lub skorzystać z usług portali internetowych, które oferują przechowywanie środków (mogą to być portfele w postaci aplikacji mobilnej, portfele offline lub przeglądarkowe).

Portfel także może przechowywać klucze prywatne, klucze publiczne i powiązane adresy. Oprogramowanie do portfela może również obliczyć całkowitą liczbę zasobów, które może posiadać użytkownik.

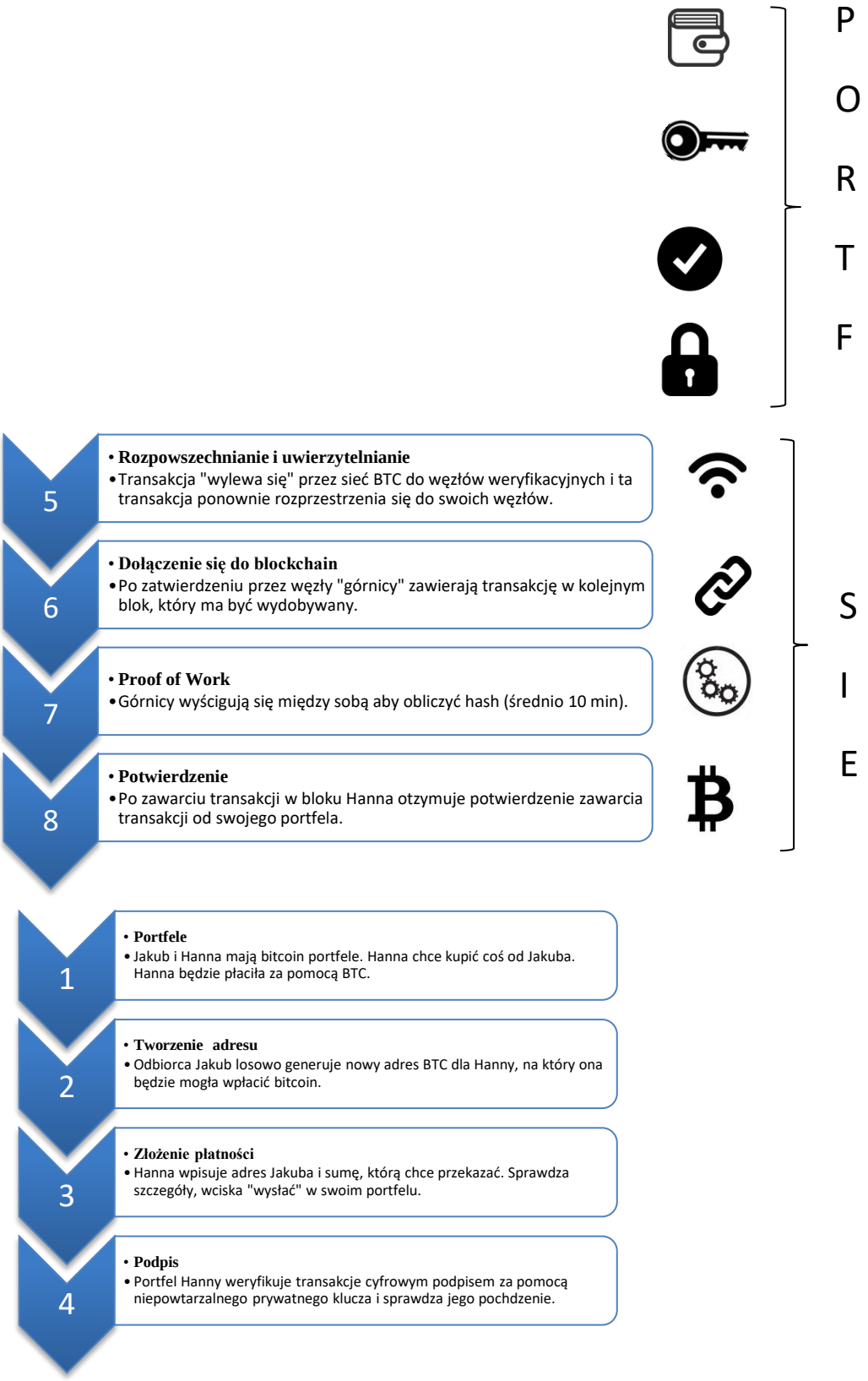
Większość użytkowników systemu blockchain nie zapisuje ręcznie swoich kluczy prywatnych, a raczej używa do tego oprogramowanie powszechnie nazywane portfelem, gdzie bezpiecznie je przechowuje.

Klucz prywatny jest zwykle generowany przy użyciu bezpiecznej funkcji losowej, co oznacza, że jego odtworzenie jest trudne, jeśli nie niemożliwe. Jeśli użytkownik utraci klucz prywatny, to wszelkie zasoby powiązane z tym kluczem zostaną utracone. Jeśli klucz prywatny zostanie skradziony, atakujący będzie miał pełny dostęp do wszystkich zasobów kontrolowanych przez ten klucz prywatny. Bezpieczeństwo prywatnych kluczy jest tak ważne, że wielu użytkowników używa specjalnego bezpiecznego sprzętu do przechowywania.

Przechowywanie klucza prywatnego jest niezwykle ważnym aspektem technologii blockchain. Kiedy pojawiają się informacje o kradzieży cyfrowych jednostek prawie na pewno oznacza to, że znaleziono klucze prywatne i wykorzystano je do podpisania transakcji wysłania pieniędzy na nowe konto, a nie, że system został naruszony. Warto też zauważyć, że ponieważ dane w systemie blockchain nie mogą być ogólnie zmieniane, to gdy przestępca kradnie klucz prywatny i publicznie przenosi powiązane środki na inne konto, nie można już tego cofnąć.

Portfel przechowuje listę transakcji, rezerwę kluczy, które mogą być wykorzystane do otrzymywania i wysyłania funduszy, preferencje klienta oraz numer wersji używanego oprogramowania. Na rysunku 5 przedstawiono cykl życia transakcji Bitcoin i opisano, jak się odbywa cały proces transakcji a także strony, zaangażowane w proces.

[6] Zob. P. Lis Markiewicz, S. Nowak, Bitcoin. Przyszłość inwestowania, Wydawnictwo Naukowe PWN, Warszawa 2015.


P
O
R
T
F
S
I
E
5
• Rozpowszechnianie i uwierzytelnianie
• Transakcja "wylewa się" przez sieć BTC do węzłów weryfikacyjnych i ta transakcja ponownie rozprzestrzenia się do swoich węzłów.
6
• Dołączenie się do blockchain
• Po zatwierdzeniu przez węzły "górnicy" zawierają transakcję w kolejnym blok, który ma być wydobywany.
7
• Proof of Work
• Górnicy wyścigują się między sobą aby obliczyć hash (średnio 10 min).
8
• Potwierdzenie
• Po zawarciu transakcji w bloku Hanna otzymuje potwierdzenie zawarcia transakcji od swojego portfela.
1
• Portfele
• Jakub i Hanna mają bitcoin portfele. Hanna chce kupić coś od Jakuba. Hanna będzie płaciła za pomocą BTC.
2
• Tworzenie adresu
• Odbiorca Jakub losowo generuje nowy adres BTC dla Hanny, na który ona będzie mogła wpłacić bitcoin.
3
• Złożenie płatności
• Hanna wpisuje adres Jakuba i sumę, którą chce przekazać. Sprawdza szczegóły, wciska "wysłać" w swoim portfelu.
4
• Podpis
• Portfel Hanny weryfikuje transakcje cyfrowym podpisem za pomocą niepowtarzalnego prywatnego klucza i sprawdza jego pochdzenie.

Rysunek 5. Cykl życia transakcji Bitcoin

Źródło: opracowanie własne na podstawie: Credit Suisse, *Report Blockchain,* Europe/United Kingdom.

Załóżmy, że Hanna chce przekazać jeden bitcoin Jakubowi: wygeneruje losowy 256-bitowy klucz prywatny; to jest po prostu losowa liczba. Przeprowadzana jest transformacja krzywej eliptycznej *(Elliptic Curve Digital Signature Algorithm (ECDSA)*, która generuje klucz publiczny, z którego klucz prywatny jest niezidentyfikowany. Na ogół, Hanna używa oprogramowania "portfel z bitcoin", który jest bezpłatny i powszechnie dostępny do pobrania, aby wygenerować te kody identyfikacyjne.

Po pomyślnym wygenerowaniu i przy założeniu, że Hanna ma bitcoiny do wydania (otrzymała więcej niż wydała), ona ponownie wysyła podpisany komunikat w formacie bazującym się na regułach na adres Bitcoin Jakuba (także wygenerowany przy użyciu oprogramowania portfela i powiązanego z kluczem prywatnym), określając ilość BTC, którą chce przekazać. Hanna wysyła klucz publiczny Jakubowi, co pozwala na niezaprzeczalność i potwierdzenie autentyczności transakcji.

Ani Hanna, ani Jakub nie mogą samodzielnie potwierdzić lub dokonać transakcji. Podobnie jak gotówka, cyfrowe żetony mogą zostać sfałszowane, natomiast, w przeciwieństwie do gotówki, są podatne na podwójne wydatki. Tradycyjnie centralna strona trzecia wystąpiłaby między Hanną a Jakubem w celu potwierdzenia, uwierzytelnienia i administrowania transferem. Jednak w przypadku transakcji cyfrowej, bitcoin przekazuje władzę poprzez stosunkowo prostą strukturę bodźców umożliwiających potwierdzenie transakcji Hanny i Jakuba przez innych uczestników sieci dzięki porozumieniu „graczy" w sieci Bitcoin, które udowodniają swoją wiarygodność poprzez wyświetlanie mocy obliczeniowej.

Jako sieć peer-to-peer, bitcoin jest wspierany przez samego siebie. Peer jest znany jako "węzeł", co oznacza każdy komputer podłączony do sieci Bitcoin. Istnieją dwa typy węzłów: lekkie węzły, takie jak Hanna i Jakub, łączące się za pośrednictwem klientów portfela i pełne węzły, które uruchamiają oprogramowanie rdzeniowe Bitcoin.

Pełne węzły są w posiadaniu całego blockchain (obecnie 165 GB[7]) i są szczególnie integralne dla systemu, ponieważ nie tylko wykonują zadanie weryfikacji i propagowania transakcji, takich jak węzły lekkie, ale również wykonują bardziej wymagające obliczenia weryfikacyjne i aktualizacyjne wspólnej księgi transakcji, czyli blockchain.

Po przekazaniu przez Hannę 1 BTC Jakubowi transakcja została podpisana z jej kluczem prywatnym i zatwierdzona przez użytkownika Jakuba. Ważna transakcja (około 400 bajtów danych) jest transmitowana do wszystkich węzłów (zarówno lekkich, jak i pełnych), z którymi jest połączone oprogramowanie portfela Jakuba. Każdy „peer" otrzymujący transakcję przeprowadza serię 20 sprawdzianów - w tym potwierdza autentyczność transakcji, przesłanej przez wirtualny portfel Hanny, sprawdzając, czy jej klucz publiczny pasuje do podpisu i sprawdza osiąganie konsensusu, który ma na celu ustalenie przez wszystkich akceptujących, czy transakcja zostanie zatwierdzona i dodana do bloku. Sprawdza, czy Hanna otrzymała więcej bitcoinów niż wydała, a zatem ma wystarczająco środków do wykonania transakcji do Jakuba. Jeśli transakcja zostanie uznana za ważną, węzeł ponownie przekazuje transakcję do wszystkich węzłów w sieci (peer), z którymi jest połączony. Proces ten jest znany jako „powódź", gdyż bardzo szybko nowa ważna transakcja przemieszcza się w ekspansywnie rozwijającej się fali po całej sieci.

Pełne węzły nie tylko utrzymują w posiadaniu pełną, kompletną i aktualną wersję blockchain, ale również niezależnie sprawdzają i dodają do niego kolejne bloki. Proces ten jest znany jako górnictwo *(mining)* i polega na uruchamianiu intensywnego obliczeniowo oprogramowania do rozwiązywania złożonych problemów matematycznych. Trudność tego problemu - znana jako "dowód pracy" *(proof of work)* - jest korygowana tak, że jest ona rozwiązana mniej więcej co 10 minut.

Wracając znowu do transakcji z Jakubem, po zweryfikowaniu przez wystarczająco dużo lekkich węzłów propagowanych przez większość sieci, transakcja jest agregowana z innymi ważnymi transakcjami, które zostały wykonane od czasu tworzenia ostatniego bloku. Przy obecnych obrotach było to około 1500 transakcji w ciągu około 9 minut.

[7] https://blockchain.info/charts/blocks-size data dostępu: 20.04.2018.

W skutku pojawi się ostateczny hash, w wyniku którego powstaje wynik mieszania wszystkich transakcji, które miały miejsce od ostatniego bloku. Te wyniki poszczególnych transakcji dostarczają niezaprzeczalnych dowodów na każdą transakcję, która się pojawiła, a przychodzi do niej poprzez powiązanie każdej z nich poprzez łączenie danych, a następnie powiązanie wyniku z inną parą i ponowne zawijanie. Ten wyczerpujący się proces jest powtarzany, dopóki wszystkie dane transakcji nie zostaną zawarte w jednym ostatecznym skrócie i nie będą miały pary, z którą mają się połączyć.

❖ ROZDZIAŁ II. Narzędzia blockchain

Potencjalne zastosowanie blockchain wykracza poza zwykle płatności lub stworzenie kryptowalut. W rzeczywistości technologia ma potencjał zmienić sposób oddziaływania na mienie intelektualne, rynki kapitałowe, ubezpieczenia, opiekę zdrowotną, rząd i wiele innych sektorów, między innymi zmienić tradycyjną bankowość.

Technologia jest postrzegana jako olbrzymia szansa i jednocześnie wielkie zagrożenie. Z jednej strony blockchain zmniejsza koszty operacyjne, transakcje stają się bardziej przejrzyste i bezpieczniejsze, z innej – eliminuje pośredników, między innymi banki i zmniejsza ilość pracowników poprzez skomputeryzowanie.

Jedno z najbardziej skutecznych narzędzi blockchain – umowy inteligentne, które są w pełni samoistne i mogą być zrealizowane między dwoma podmiotami bez uczestnictwa strony trzeciej. Ideą jest zawarcie umowy w sposób wolny od konfliktów, jednocześnie unikając pracy pośrednika i redukując koszty, związane z uczestnictwem zaufanej strony trzeciej podczas zawarcia umowy.

Blockchain jest zazwyczaj klasyfikowany na podstawie modelu uprawnień, który określa, kto może uzyskać do niego dostęp. Jeśli ktokolwiek może czytać i pisać do blockchain, to jest to łańcuch bloków publiczny *(permissionless)*. Jeśli tylko poszczególni użytkownicy mogą czytać i zapisywać do niego, jest on prywatny *(permissioned)*. Mówiąc prościej, prywatny blockchain jest podobny do kontrolowanego Intranetu korporacyjnego, podczas gdy publiczny blockchain jest podobny do Internetu, w którym każdy może uczestniczyć.

2.1 Publiczny blockchain

Publiczny blockchain jest zdecentralizowaną platformą bez władzy centralnej i jest otwarty na uczęstnictwo bez specjalnych uprawnień. Publiczny blockchain często wykorzystuje metod consensusu, który wymaga więcej wysiłku w celu przeciwdziałania złym użytkownikom łatwego obalenia systemu. Takimi metodami konsensusu są dowody pracy *(proof of work)* i dowody na metody stawek *(proof of stake)*. Przyczyną, dzięki której publiczny blockchain pracuje jest wynagrodzenie za uczestnictwo w tym procesie.

Podejmując decyzje, czy użyć publiczny blockchain należy rozważyć, czy zastosowanie wymaga następujących cech:

- Dane podawane publicznie - z uwagi na to, że publiczny łańcuch bloków pozwala każdemu kontrolować i wnosić wkład do blockchain, dane są ogólnie udostępnione. Zatem należy rozważyć kwestie czy dane mogą być dostępne dla wszystkich.
- Pełna historia transakcji - dzięki otwartemu charakterowi danych dla tych systemów każdy może śledzić transfer aktywów między kontami. Począwszy od utworzenia zasobów, do każdej trwającej transakcji.
- Fałszywe próby transmisji danych - ponieważ każdy mógł wnieść swój wkład do blockchain, niektórzy mogli przesyłać fałszywe dane do systemu, naśladując dane z prawidłowych źródeł. Zatem jest ważne badanie czy istnieje sposób aby zapewnić, że blockchain będzie gromadził tylko dane z renomowanych źródeł.
- Niezmienność danych - wiele aplikacji korzysta z funkcji "CRUD" *(create, read, delete, update)* - (tworzenie, odczytywanie, aktualizacja, usuwanie) danych. W blockchain jest tylko "CR" *(create, read*) - (tworzenie, czytanie). Istnieją metody, które można wykorzystać do "wycofywania" starszych danych, jeśli zostanie znaleziona nowsza wersja, ale nie ma procesu usuwania oryginalnych danych.
- Transakcyjna przepustowość - obecnie transakcje na blokach nie są przeprowadzane w tym samym tempie, co inne rozwiązania (np. Bloki do blockchain nie są dodawane wystarczająco szybko), więc może wystąpić pewne spowolnienie w oczekiwaniu na wysłanie danych.

Niektóre zastosowania publicznego blockchain:

- Zaufany znacznik czasu:

zaufane oznaczanie dat jest sposobem na udowodnienie, że pewne informacje istniały w danym momencie[8]. Korzystanie z blockchain pozwala stronie udowodnić, że miał dostęp do danych w sposób, który nie może być odrzucony. Na przykład, jeśli dana osoba chciała udowodnić, że posiada plik, może zaszyfrować plik i zapisać ten plik jako adnotację do transakcji. Następnie, jeśli kiedykolwiek będzie musiał udowodnić posiadanie pliku, zostanie to zapisane publicznie w całym blockchain.

Inne przypadki wykorzystania sygnatur czasowych w łańcuchu blokowym obejmują udowodnienie, że zadanie zostało wykonane w określonym terminie, co udowodniło posiadanie zdjęcia, potwierdzenie podpisania umowy lub udowodnienie wystąpienia zdarzenia.

- Przemysł energetyczny:

inne zastosowanie blockchain jest rejestracja autonomicznych transakcji typu machine-to-machine dotyczących zużycia energii elektrycznej. Wykorzystałoby to możliwości platformy cyfrowej i zmieniające się modele biznesowe do śledzenia transakcji na inteligentnej sieci. Jednym z ważniejszych przykładów zastosowania w przemyśle energetycznym dla blockchain są certyfikaty rejestracyjne. Istnieją różne elektrownie wytwarzające energię i tworzące certyfikaty potwierdzające ilość energii wyprodukowanej w celu późniejszej wymiany. Obecnie istnieją dwa problemy, takie jak wydawanie certyfikatów emisji, a także potrzeba sprostania wyzwaniom regulacyjnym i zapewnienie bardziej jednolitego dostępu dla wszystkich na rynku. Blockchain może skutecznie śledzić emitowanie i wydawanie tych certyfikatów energetycznych.

Innym przykładem wykorzystania blockchain w przemyśle energetycznym jest handel nadwyżką energii odnawialnej. Budynki mogą być połączone z urządzeniami mierzącymi zużycie energii i zapisującymi je do blockchain, umożliwiając sprzedaż i kupowanie nadmiaru energii na rynku.

[8] B. Gipp, N, Meuschke, A. Gernandt, "Decentralized Trusted Timestamping using the Crypto Currency Bitcoin," in Proceedings of the iConference 2015, Newport Beach, California, 2015, data dostępu: 20.04.2018.

2.2 Prywatny blockchain

Publiczny blockchain jest pierwotną koncepcją łańcucha bloków Bitcoin, w którym każdy może czytać i zapisywać na blockchain, a księga jest rozproszona/publiczna. Organizacje, które chcą współpracować, ale nie ufają sobie w pełni, mogą ustanowić prywatny blockchain i zaprosić partnerów biznesowych do rejestrowania swoich transakcji we wspólnej rozproszonej księdze rachunkowej. Prywatny blockchain może mieć taką samą identyfikacje zasobów, które przechodzą przez blockchain, a także spełniać te same funkcje rozproszonego, bezpiecznego systemu przechowywania danych, jak i publiczny łańcuch blockchain. Organizacje te mogą określić mechanizm konsensusu, który ma być stosowany, w zależności od tego, jak bardzo sobie nawzajem ufają.

Prywatny blockchain można skonfigurować tak, że każdy może je odczytać, ale tylko wybrane członkowie mogą rejestrować transakcje na nich. Tego typu blockchain zapewni pełny wgląd w wewnętrzne interakcje organizacji przez każdego, kto ma interes, ale ogół społeczeństwa nie będzie w stanie ingerować się w dane. Można również skonfigurować łańcuch bloków, aby każdy mógł rejestrować transakcje na blockchain, ale tylko wybrani członkowie mogą czytać dane.

Choć prywatny blockchain jest często uważany za lepszy od obecnych systemów, niektóre cechy konstrukcyjne muszą być traktowane ostrożnie, aby zapewnić bezpieczeństwo. Na przykład podczas korzystania z bazy danych można uzyskać szczegółową ilość uprawnień, na przykład zezwalając określonym użytkownikom na wykonywanie określonych zapytań lub zezwalając tylko określonym użytkownikom na zapisywanie danych w określonych tabelach. Aplikacje korzystające z blockchain potrzebują rozważenia czy uprawnienia obsługiwane przez blockchain są wystarczająco szczegółowe, aby umożliwić utworzenie wystarczającej liczby ról w systemie (uprawnienia pozwalają na bardziej tradycyjne role, takie jak administrator, użytkownik, weryfikator, audytor itp.).

Dotyczy to również sposobu administrowania uprawnieniami. Kiedy użytkownik otrzyma dostęp zapisu do blockchain, istnieje potrzeba wyjaśnienia kwestii cofnięcia tego uprawnienia. Większość implementacji blockchain jest niezmienna, co może skomplikować nadanie dostępów do sieci blockchain.

Zaufanie jest kolejną kwestią krytyczną przy podejmowaniu decyzji o zbudowaniu aplikacji w systemie blockchain. W ramach dozwolonego systemu łańcucha bloków metoda konsensusu jest zwykle mniej intensywna obliczeniowo - w związku z tym użytkownicy mogą działać złośliwie. Zaufanie nie musi jednak obejmować wszystkich użytkowników. Możliwe jest, aby opiekun łańcucha wyznaczył ograniczony zestaw węzłów górniczych. Jeśli są one godne zaufania, nie jest konieczne, aby cała populacja użytkowników była godna zaufania, ponieważ górnicy będą egzekwować reguły blockchain.

Innym ważnym aspektem jest posiadanie konstrukcji z widocznym zabezpieczeniem. Jeśli złośliwy węzeł górniczy próbował zmienić blok, może na przykład dokonać transakcji, by dać sobie pieniądze, zatem niezbędnym jest przeanalizowanie możliwości wykrycia takich przypadków.

Niezmienność jest ważna i jest jedną z podstawowych zasad blockchain. Ogólnie rzecz biorąc, złośliwe transakcje, które wchodzą do łańcucha blockchain, nie mogą zostać cofnięte, nawet jeśli zostaną zidentyfikowane. Aby to zrobić, konieczne jest przepisanie opublikowanych bloków, które zasadniczo powodują blokowanie i wymagają zatwierdzenia większości węzłów górniczych. W systemie z uprawnieniami może to być łatwiejsze, ponieważ węzły wyszukiwania są na ogół zaufanym zestawem, który ma specjalną relację. Jest to o wiele trudniejsze, ale technicznie możliwe, jak np. w systemie publicznego blockchain, na którym jest zbudowany bitcoin.

Niektóre przykłady zastosowania prywatnego blockchain:

- Bankowość:

załóżmy, że wiele banków chce zachować prywatną, rozproszoną księgę dostępną tylko dla uczestniczących banków. Dałoby to możliwość rejestrowania transakcji z każdego banku w sposób widoczny dla uczestników, ale nie dla opinii publicznej. Jednakże, aby zrobić to jako prywatny blockchain (aby uniknąć konieczności używania kosztownego algorytmu dowodu pracy), każdy bank na zmianę podpisuje bloki w ramach rozproszonego algorytmu konsensusu.

Jest kilka interesujących rozważań przy korzystaniu z prywatnego blockchain z kilkoma uczestnikami, takimi jak zdolność przezwyciężenia jego niezmienności. W przypadku wystąpienia poważnej katastrofy lub wyjątkowej sytuacji banki mogłyby skoordynować

wycofanie transakcji z blockchain i napisać inną transakcję. Ponadto transakcje nie będą anonimowe, ponieważ do dołączenia potrzebny będzie identyfikator bankowy.

- Łańcuch dostaw:

rejestracja transferu dóbr fizycznych od producenta, do terminalu wysyłkowego, na statek, do pociągu towarowego, do ciężarówki dostawczej i do sklepu jest atrakcyjnym zastosowaniem technologii blockchain. Blockchain może odegrać kluczową rolę w zaufaniu i przejrzystości z klientami końcowymi. Technologia może również służyć do monitorowania działań dostawców. Dostawcy mogą rejestrować wyprodukowany produkt (taki jak liczba widżetów X w określonym dniu) w sposób, który mogą zweryfikować inni użytkownicy łańcucha bloków. Dzięki systemowi blockchain magazyny mogą efektywnie zarządzać logistyką, unikając nadmiernego magazynowania.

- Ubezpieczenia i opieka zdrowotna:

w czasie, gdy ktoś odwiedza placówkę medyczną, mnóstwo transakcji odbywa się za kulisami. Transakcje administracyjne od pielęgniarek, lekarzy, personelu medycznego, firm ubezpieczeniowych i aptek mogą być zapisywane na blockchain. Transakcje (takie jak sprawdzanie świadczeń, kwalifikacji, zasięgu i dostępnej podaży leków) można odczytać z blockchain. Obecnie zapisy tych transakcji znajdują się w różnych systemach, dzieląc się wynikami po zakończeniu (często ręcznego) procesu.

2.3 Zaufane rozproszone księgi

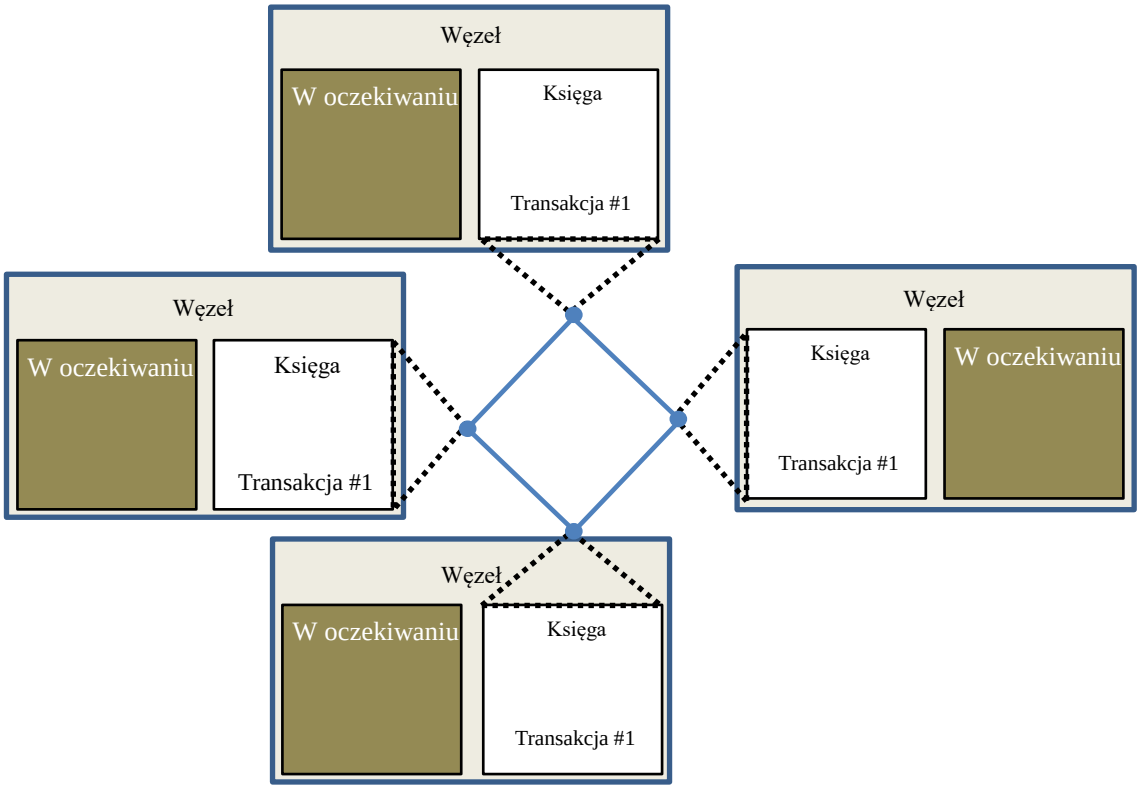
Księga jest zbiorem transakcji. Na przestrzeni dziejów do śledzenia wymiany towarów i usług wykorzystywano księgi rachunkowe i papierowe. Niedawno księgi zapisano cyfrowo, często w dużych bazach danych, których właścicielem i operatorem są wyłącznie scentralizowane "zaufane" strony trzecie w imieniu społeczności użytkowników (tj. Strona trzecia jest właścicielem księgi głównej). Scentralizowane księgi mogą mieć braki, takie jak:

- Mogą zostać zgubione lub zniszczone; użytkownik musi ufać, że właściciel prawidłowo tworzy kopię zapasową systemu.
- Transakcje mogą nie być ważne; użytkownik musi ufać, że właściciel sprawdza każdą otrzymaną transakcję.
- Lista transakcji może nie być kompletna; użytkownik musi ufać, że właściciel zawiera wszystkie ważne transakcje, które zostały odebrane.

- Dane transakcji mogły zostać zmienione; użytkownik musi ufać, że właściciel nie zmienia poprzednich transakcji.

Oczywiście w najlepszym interesie każdej scentralizowanej księgi jest tworzenie kopii zapasowych danych, sprawdzanie poprawności transakcji, uwzględnianie wszystkich ważnych transakcji i niemodyfikowanie historii. Księga wprowadzona za pomocą łańcucha bloków może złagodzić te problemy za pomocą rozproszonego mechanizmu konsensusu. Jednym z aspektów jest to, że księga blockchain będzie kopiowana i dystrybuowana do każdego węzła w systemie. Rysunek 6 przedstawia prostą sieć z czterema węzłami, z których każdy ma kopię księgi transakcji.

Rysunek 6. Sieć węzłów



Źródło: opracowanie własne na podstawie: Computer Security Resource Center, Blockchain Technology Overview, U.S. Department of Commerce, 2018.

Dalej nowe transakcje są przesyłane do węzła, które następnie sygnalizują resztę sieci o nadejściu nowej transakcji, która czeka w oczekiwaniu na potwierdzenie, żeby dołączyć się do księgi. Ostatecznie węzeł zawrze tę nową transakcję w ramach bloku i uzupełni system. Ten nowy blok zostanie rozłożony w systemie, a wszystkie księgi zostaną zaktualizowane, aby uwzględnić nową transakcję. Za każdym razem, gdy nowi użytkownicy dołączą do systemu, otrzymują pełną kopię blockchain, co utrudnia utratę lub zniszczenie księgi głównej. Wszystkie transakcje są przechowywane w blokach w ramach całego blockchain.

2.4 *Smart contracts*

Umowy inteligentne (ang. *smart contracts*) to kolejny postęp technologii blockchain, który pozwala na przejście z protokołu transakcji finansowych do narzędzia, które automatycznie będzie wdrażać warunki umów, minimalizując ryzyko błędu i manipulacji.

Umowa inteligentna jest to umowa lub zestaw zasad regulujących transakcje biznesowe[9]. Transakcja jest przechowywana w pojedynczym bloku całego blockchain i wykonywana automatycznie w ramach transakcji. Celem *smart contracts* jest zapewnienie bezpieczeństwa lepszego od tradycyjnych umów przy jednoczesnym obniżeniu kosztów i opóźnień, które występują w umowach tradycyjnych.

Mówiąc bardziej technicznie są to linie kodu, do napisania którego wykorzystuje się język Solidity (język programowania, porównywalny do języka Java Script). Ten kod następnie jest przekształcany w kod bajtowy i podłączany do bloku w sieci blockchain jako inteligentna umowa. Każda umowa posiada własny adres blokowy, w wyniku czego w czasie porozumienia się z kimś utworzy się umowa w ramach bloku, a jej adres będzie dostępny dla wszystkich zainteresowanych stron. Aby transakcja zrealizowała się strony muszą wypełnić określone zobowiązania.

Przyszłe transakcje wysyłane do blockchain mogą następnie wysyłać dane do publicznych metod oferowanych przez inteligentną umowę. Umowa realizuje odpowiednią metodę z danymi dostarczonymi przez użytkownika w celu wykonania usługi. Kod znajdujący się na blockchain jest niezmienny i dlatego może być używany (między innymi)

[9] M. Gupta, Blockchain, John Wiley & Sons, Inc., 2017, s. 17.

jako zaufana strona trzecia do transakcji finansowych, które są bardziej skomplikowane niż zwykłe wysyłanie środków między kontami. Inteligentna umowa może wykonywać obliczenia, przechowywać informacje i automatycznie wysyłać środki na inne konta. To niekoniecznie musi pełnić funkcję finansową. Na przykład istnieją inteligentne kontrakty, które publicznie generują wiarygodne liczby losowe[10].

W praktyce wszystkie węzły wyszukiwania jednocześnie wykonują kod inteligentnego kontraktu podczas wydobywania nowych bloków. Zatem inteligentne wykonanie umowy może być droższe niż proste transfery funduszy w innych kryptowalutach opartych na blockchain. Często użytkownik wystawiający transakcję na inteligentną umowę będzie musiał zapłacić za koszt wykonania kodu oprócz normalnych opłat transakcyjnych. Istnieje ograniczenie, ile czasu realizacji może zostać wykorzystane przez połączenie z inteligentnym kontraktem. Jeśli ten limit zostanie przekroczony, wykonywanie zostanie zatrzymane, a transakcja zostanie odrzucona. Mechanizm ten nie tylko wynagradza górników za wykonanie inteligentnego kodu kontraktowego, ale także uniemożliwia szkodliwym użytkownikom wdrażanie, a następnie uzyskiwanie dostępu do inteligentnych kontraktów, które będą wykonywać odmowę usługi w węzłach wyszukiwania przez zużywanie wszystkich zasobów (np. Za pomocą nieskończonych pętli).

Na przykład, *smart contract* może zawierać warunki, przy których nastąpi transfer obligacji korporacyjnych albo warunki ubezpieczenia podróżnego, które będą mogły spełnić się w momencie, na przykład, opóźnienia lotu więcej niż o 6 godzin.

2.5 Obecne obszary zastosowań

Obecnie blockchain może być wykorzystywany do obsługi różnorodnych transakcji (handel, waluty, akcje, udziały, rynek energii elektrycznej), ale trwają prace nad wykorzystywaniem łańcucha bloków, jako księgi rachunkowej w bankowości, systemie uwierzytelniania dokumentów, podpisu cyfrowego w administracji państwowej i zapisu notarialnego.

[10] P. Mell, J. Kelsey, J. Shook, "Cryptocurrency Smart Contracts for Distributed Consensus of Public Randomness." October 7, 2017. https://doi.org/10.1007/978-3-319-69084-1_31, data dostępu: 20.04.2018.

Wszystkie te transakcje mogą odbywać się poza funkcjonującym od lat systemem – bez udziału instytucji zaufania publicznego, bezpośrednio pomiędzy stronami transakcji.

Najbardziej rozpowszechniony sposób używania blockchain – przez rządy, głównie służy do zastępowania tradycyjnych metod rejestracji własności, potwierdzenia tożsamości, wypłaty świadczeń lub tworzenia publicznych baz danych na bazie blockchain. Wdrożenie technologii ma na celu zmniejszenie oszustw, zwiększenie przejrzystości systemu oraz przyniesienie znacznych oszczędności czasu i kosztów.

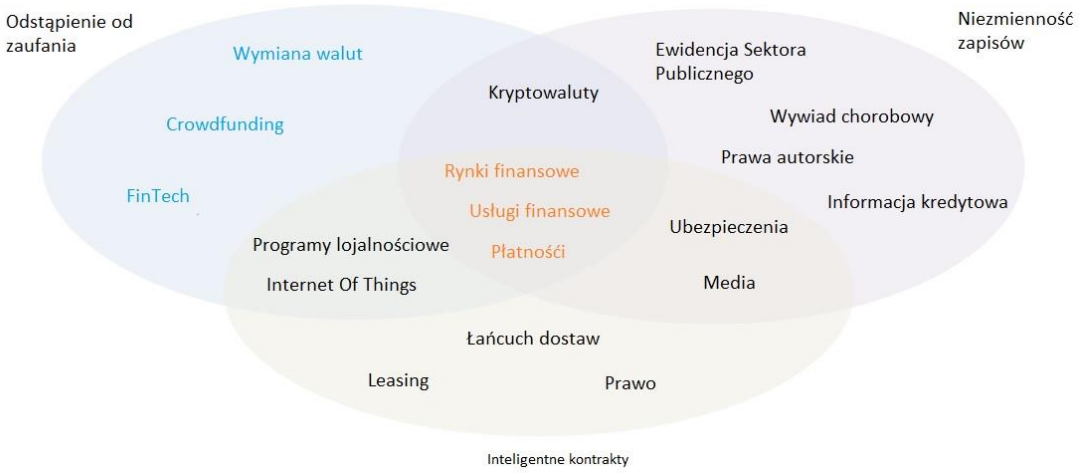
Niektóre przykłady zastosowań technologii przez rządy państw:

- Gruzja - blockchain jest używany do rejestracji tytułów własności gruntów.
- Wielka Brytania - rząd rozpoczął wykorzystanie technologii w Departamencie Pracy i Emerytur, dzięki czemu wnioskodawcy mogą otrzymywać i wypłacać świadczenia, korzystając z aplikacji mobilnej, a wszystkie transakcje są rejestrowane. System ten powinien zmniejszyć oszustwa, związane z wypłatami świadczeń opieki społecznej i ma pomóc w rejestrowaniu aktywów.
- Singapur – obecnie Singapurski Bank Centralny wykorzystuje blockchain w obszarze płatności międzybankowych. Wynikiem używania technologii są skrócenie czasu transakcji, zwiększenie przejrzystości i odporności systemu oraz obniżenie kosztów długoterminowego przechowywania danych.
- Delaware, Stany Zjednoczone – blockchain jest wykorzystywany do przechowywania umów i innych danych korporacyjnych. Zapewnia to większe bezpieczeństwo i umożliwia automatyczny dostęp do dokumentów akcjonariuszom, inwestorom i pracownikom. Główną zaletą w tym przypadku jest oszczędność kosztów fizycznego przechowywania dokumentów.
- Polska – projekt „Od papierowej do cyfrowej Polski”[11], wdrażanie e-usług, takich jak e-Faktura, e-Paragon, e-Świadczenie, e-Zdrowie. Celem oferowanych usług elektronicznych jest obniżenie kosztów administracji, uproszenie opłaty i księgowania składek na ubezpieczenia społeczne oraz poprawa efektywności procesów administracyjnych poprzez automatyzacje procesów.

[11] Ministerstwo Cyfryzacji, „Od papierowej do cyfrowej Polski”, 2017, https://www.gov.pl/cyfryzacja/od-papierowej-do-cyfrowej-polski?inheritRedirect=true, data dostępu: 14.10.2017.

Nadal trwa okres testów i zaczynają działać nowe projekty, aby znaleźć zastosowanie technologii w nowych obszarach. Rysunek 7 przedstawia branże, w których bloki rejestrów pełnią funkcje notariusza (np. zarządzanie prawami autorskimi), tworzą rejestr danych (jak w przypadku ewidencji sektora publicznego), umożliwiają natychmiastowe transakcje peer-to-peer (kryptowaluty, wymiana walut i płatności), smart contracts (łańcuch dostaw i leasing).

Rysunek 7. Potencjalne korzyści i obszary wdrożenia blockchain



Źródło: opracowanie własne na podstawie: Credit Suisse, *Report Blockchain,* Europe/United Kingdom.

Zdecentralizowana uniwersalna baza danych może być wykorzystywana w różne interesujące sposoby. Obecnie banki tworzą bazy danych i rejestrują ich dyrektywy, co jest dość drogie. Jednak przy użyciu blockchain bazy danych mogą być uniwersalne i używane przez wiele instytucji, przynosząc o wiele większą wydajność i pomagając porozumieniu różnych systemów. Blockchain obniża koszty i otwiera możliwości dla ludzi i firm, które nie mają bardzo wysokich kapitałów, tak, aby zamiast tworzenia nowej infrastruktury można by było dołączyć się do już istniejącej.

Estoński bank LHV eksperymentuje z blockchain, wydając kwotę 100 000 EUR wierzytelności "zabezpieczonych kryptograficznie" wobec banku. Wykorzystuje kolorowe monety - protokół open source do tworzenia zasobów cyfrowych, oparte na Bitcoin blockchain, aby utworzyć to, co nazywa się *Cryptographic Universal Blockchain Added Receivables (CUBER)*[12], jest rodzajem certyfikatu depozytowego, który może być wykorzystywany jako podstawa do innowacyjnych produktów finansowych. Bank planuje także umożliwić swoim klientom bezpłatne wypłaty w walucie przy pomocy blockchain. Celem LHV jest kierowanie innowacyjnością finansową dla mniejszych developerów oprogramowania i sugeruje, że startupy i firmy, które zajmują się wymianą kryptowalut mogą korzystać z jej platformy. Jest to dobry przykład w praktyce banku tworzącego bardziej wydajną platformę i umożliwiającą szerszy, bardziej otwarty dostęp. To, co wcześniej nie było praktyczne ze względu na koszty technologii, teraz staje się bardziej dostępne z pojawieniem się sieci elektronicznych oraz szerokiego udziału klientów detalicznych i instytucji finansowych, co w wyniku ma wpływ na dotychczasowe modele biznesowe w branży finansowej. Blockchain otwiera nowe możliwości w rozwiązywaniu problemów, kiedy zamiast jednego podmiotu istnieje sposób rozwiązywania problemów grupą podmiotów jednocześnie. Innymi słowy, początkowe wprowadzenie blockchain będzie miało na celu poprawę efektywności, ale z biegiem czasu wszechobecność mogłaby stworzyć nową strukturę, aby łatwiej łączyć kontrahentów w innowacyjnych konfiguracjach sieciowych, a nie bardziej scentralizowanych modelach, obecnie stosowanych.

Jednym z przykładów wykorzystania blockchain w obszarze, w którym istnieje wyraźne połączenie między światem fizycznym i finansowym, jest firma Kynetix, która powołała konsorcjum graczy z całego cyklu handlu towarami, w tym giełdami, bankami inwestycyjnymi, izbami rozliczeniowymi, firmami magazynowymi i brokerami, aby zbadać zastosowanie blockchain na rynkach fizycznych. W ramach prac badawczo-rozwojowych w przestrzeni firma Kynetix ogłosiła, że pomyślnie przeniosła tytuł na pojedynczą partię pieprzu na blockchain, oparty na bitcoin przy użyciu Sentinel, swojej platformy do zarządzania zapasami i fizycznej dostawy, która tworzy elektroniczną rejestrację tytułu, własności i magazynowania towarów.

[12] A. Chepel, "Pro-bitcoin Estonian bank creates a wallet based on Colored Coins", Coinfox, 08 June 2015, http://www.coinfox.info/news/2169-cuber, data dostępu: 15.10.2017.

Uważa się, że potencjał blockchain w płatnościach jest wysoki, a firmy takie jak „Ripple" przyciągnęły wiele uwagi w przestrzeni płatności. Blockchain pozwala każdemu uczestniczącemu w transakcji zobaczyć cały cykl życia transakcji i zaangażowanie wszystkich osób, biorących w niej udział. „Smart contracts" mogą być wykorzystane w celu zwiększenia przejrzystości i kontrolowania terminów płatności i zmniejszania ryzyka. Wprowadzenie blockchain do systemów płatności umożliwia ich realizację w skali międzynarodowej poprawiając ich jakość, szybkość realizacji, dzięki czemu proces jest bardziej przejrzysty i ciągły.

Blockchain tworzy nowe możliwości transformacyjne. Po pierwsze, fakt, że możemy „przyłączyć" zachowanie do pieniędzy, co otwiera możliwości dla nowych instrumentów na rynkach kapitałowych, chociaż ten aspekt innowacji nie jest jeszcze rozwinięty i nie pozwala dołączyć się do środowiska produkcyjnego. Drugi obszar potencjalnego zastosowania blockchain w stosunkowo krótkim czasie dotyczy rozliczeń na rynkach kapitałowych.

Zalety wykorzystania blockchain w obszarze rynków kapitałowych to:

- Natychmiastowa realizacja i zakończenie transakcji.
- Obniżenie kosztów transakcji.
- Poprawa terminowości.
- Wyeliminowanie pośrednich etapów w procesie.

Centralni kontrahenci zostali wprowadzeni w celu zmniejszenia ryzyka kontrahenta, ale w przypadku blockchain użytkownik ma zabezpieczenie i natychmiastowe rozliczenie, czyli ryzyko kontrahenta znika.

Pierwszy dowód konceptu transakcji Nasdaq został symbolicznie zarejestrowany w Sylwestra 2015 roku przez Chain.com, firmę deweloperską typu blockchain, która pomaga Nasdaq w budowie platformy Linq opartą na wykazie rozproszonym. Pierwszy projekt bazujący się na blockchain, które firma Nasdaq próbowała wprowadzić na rynek - efektywne, elektroniczne usługi związane z wydawaniem, transferem i zarządzaniem prywatnymi papierami wartościowymi.

Drugi przykład, który stosuje narzędzia blockchain – Deutsche Bank. Zdaniem analityków blockchain ma największy potencjał na rynkach kapitałowych i ma najwięcej możliwości w obszarze papierów wartościowych. Deutsche Bank dokonał wewnętrznego eksperymentu za pomocą blockchain, stosując go do zarządzania cyklem życia obligacji korporacyjnych, aby zrozumieć możliwości technologii, a także aspekty prawne i regulacyjne. Wynikiem tego projektu było uznanie technologii blockchain zdolnej jako do wykonania tych funkcji.

❖ ROZDZIAŁ III. Potencjalne zastosowania i kontrowersje blockchain

Dzisiaj blockchain głównie używany jest do cyfrowych rozwiązań gotówkowych. W tej sekcji przedstawiono wybór platform blockchain, aby podkreślić różnice techniczne i stosowane podejścia, a także niektóre kontrowersje w używaniu łańcucha bloków, wokół którego ostatnio pojawiło się dużo hałasu w świecie finansów. Przedstawione zostaną wady technologii i potencjalne zastosowania.

3.1 Kryptowaluty

Liczne aplikacje technologii blockchain są zorientowane przede wszystkim na przenoszenie waluty z jednego konta na drugie. W tej sekcji opisano kilka przykładów takich aplikacji blockchain:

- Bitcoin:

Bitcoin to cyfrowy system gotówkowy, o którym wcześniej mówiono jako o pionierze w korzystaniu z blockchain. Nowe bloki są tworzone mniej więcej raz na 10 minut przy użyciu funkcji mieszania SHA-256, aby je połączyć. Jest to dowód na system pracy, w którym węzły wyszukiwania muszą znaleźć element, który będzie zawierany w swoim bloku tak, aby wartość mieszania bloku była mniejsza niż pewna z góry określona wartość trudności. Trudność jest korygowana w górę lub w dół, aby osiągnąć 10-minutowy cel tworzenia bloku. Na początku historii Bitcoin, poszczególne komputery mogły kopać i publikować bloki; obecnie Bitcoin wymaga wyspecjalizowanego sprzętu, dużych centrów danych lub wielu osób pracujących razem w polu wydobywczym *(mining pool)*, aby wygrać konkurs na publikowanie bloków.

W przypadku Bitcoin opłaty za transakcje są technicznie opcjonalne, ponieważ węzły wydobywcze otrzymują większość swoich funduszy poprzez publikację bloków. Opłata ta ma być niewielką opłatą za każdą transakcję, ale może i stała się duża ze względu na znaczne zaległości oczekujących transakcji. Płacenie wyższej opłaty za transakcję może nadać transakcji większy priorytet przy dodawaniu do blockchain. Początkowo węzły wydobywcze otrzymywały 50 bitcoinów dla każdego bloku i tylko połowę tego po pewnej liczbie bloków.

Na przykład nagroda za wydobycie bloku wyniosła 12,5 bitcoinów w lipcu 2016 r. Zgodnie z protokołem Bitcoin ta nagroda zmniejszy się o połowę co 210 000 bloków (około czterech lat) i spadnie do zera po wyprodukowaniu 21 milionów bitcoinów. Wydobywanie bitcoinów będzie kontynuowane w tym momencie, ale nagroda będzie w całości pochodzić z opłat transakcyjnych[13].

Warto zauważyć, że każda transakcja w sieci Bitcoin zawiera kod napisany w języku zwanym Script. Ten kod reprezentuje prosty program, który określa transakcję. Nie zawiera pętli *(loops)* i jest bardzo ograniczony pod względem funkcjonalności (tj. nie posiada kompletności Turinga)[14]. Transakcje bitcoinowe wykorzystują dziś tylko niewielką część dostępnych funkcji skryptu. W praktyce większość transakcji Bitcoin wykorzystuje jeden z niewielu szablonów kodu do przepływu funduszy między stronami.

- Litecoin:

Litecoin jest inspirowany i jest bardzo podobny do Bitcoin, ale ma na celu zapewnić szybsze czasy potwierdzenia. Litecoin wdrożył SegWit[15], dzieląc transakcje na dwa segmenty i ukrywając zwiększony rozmiar bloku[16]. Sygnatura "świadka" *(witness)* jest oddzielona od drzewa MerkleTree. Inną różnicą między Bitcoinem i Litecoinem jest to, że Litecoin używa algorytmu Scrypt do mieszania zamiast SHA-256. Algorytm Scrypt jest trudniejszy do rozwiązania niż SHA-256, ponieważ wykorzystuje więcej pamięci, co utrudnia tworzenie

[13] J. Donnelly, "What is the 'Halving'? A Primer to Bitcoin's Big Mining Change," CoinDesk, June 12, 2016. https://www.coindesk.com/making-sense-bitcoins- halving/ data dostępu: 27.03.2018.

[14] Kompletny system Turinga (system komputerowy, język programowania itp.) Może być użyty do dowolnego algorytmu, niezależnie od złożoności, aby znaleźć rozwiązanie.

[15] SegWit (skrót od *Segregated Witness*) to uaktualnienie protokołu, które zmienia sposób przechowywania danych.

[16] A. Hertig, "Litecoin's SegWit Activation: Why it Matters and What's Next," CoinDesk, April 26, 2017. https://www.coindesk.com/litecoins-segwit-activation- why-it-matters-and-whats-next/ data dostępu: 27.03.2018.

niestandardowych układów scalonych specyficznych dla aplikacji (ASIC). Istnieje większa maksymalna liczba monet, które można wydobyć (84 miliony litecoinów). Litecoin jest uzupełnieniem Bitcoin, o wyższych wolumenach transakcji i nie jest przeznaczony do jego zastąpienia[17].

- Ethereum:

Ethereum to platforma typu blockchain, która koncentruje się na dostarczaniu inteligentnych kontraktów. Inteligentne kontrakty to programy, które istnieją na blockchain, do których mają dostęp użytkownicy Ethereum. Mogą zarówno otrzymywać, jak i wysyłać fundusze podczas wykonywania dowolnych obliczeń. Właściwie zaprojektowana umowa może działać jako zaufana strona trzecia w transakcjach finansowych, ponieważ jej kod jest zarówno publiczny, jak i niezmienny. Językiem programowania transakcji Ethereum zawiera kompletność Turinga *(Turing completeness)*. Węzły wydobywcze otrzymują fundusze za pośrednictwem górnictwa i opłat transakcyjnych.

Ethereum ma również koncepcję o nazwie "gaz" używane do zasilania obliczeń transakcyjnych (na ogół około 1/100 000 z Eteru). Każda transakcja zużywa gaz podczas wykonywania zlecenia, a inicjator danej transakcji musi zapłacić wystarczającą ilość gazu lub wykonanie transakcji zostaje przerwane. Istnieje maksymalny limit gazu na jeden inteligentny kontrakt (obecnie trzy miliony gazu), aby zapobiec kosztownym obliczeniowo programom przedkładanym do węzłów wydobywczych Ethereum. Dzieje się tak dlatego, że wszystkie węzły wyszukiwania muszą wykonywać transakcje równolegle[18].

Złożenie transakcji do umowy Ethereum powoduje, że program jest uruchamiany równolegle na komputerach węzłów górniczych. Rezultat umowy jest przechowywany na blockchain przez użytkownika, który publikuje następny blok.

[17] Litecoin Project. https://litecoin.org/ data dostępu: 27.03.2018.
[18] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger” data dostępu: 27.03.2018.

- Dash:

Dash jest kryptowalutą zbudowaną w celu zapewnienia szybszych transakcji. Korzysta z sieci "masternodu" i może dokonywać transakcji w ciągu czterech sekund[19]. Dash używa deterministycznego porządkowania dla masternodów za pomocą hasha i dowodu pracy dla każdego bloku. Co ciekawe, stanie się masternodą wymaga zabezpieczenia 1000 Dash, co czyni bardzo drogim (prawie niemożliwym) kontrolowanie ponad 50 procent sieci. Wymóg zabezpieczenia dla masternodów ma na celu złagodzenie problemów niezaufanych węzłów w sieci typu peer-to-peer.

Dash używa innego algorytmu mieszania niż większość, x11. Obejmuje to użycie wszystkich 11 algorytmów uczestnika SHA-3 (w tym BLAKE, JH, Keccak i Skein), przy czym każdy skrót jest przekazywany do następnego algorytmu w łańcuchu. Rozumowanie jest takie, że użycie wielu algorytmów utrudnia tworzenie ASIC, który jest przeznaczony do rozwiązywania tych skrótów w sprzęcie.

- Ripple:

Ripple to nazwa zarówno kryptowaluty, jak i sieci płatniczej, w której jest przesyłana. Celem Ripple jest budowanie podejścia Bitcoin i łączenie różnych systemów płatności. Ma stałą podaż 100 miliardów XRP, z czego połowa przeznaczona jest do obiegu. Klienci Ripple nie muszą pobierać całego blockchain, co ułatwia klientom dołączanie w ciągu kilku sekund. Dodatkowo, nie ma nagrody górniczej za uruchomienie serwera, ponieważ każda transakcja kosztuje niewielką ilość Ripple, podobną do gazu Ethereum. Dlatego nie ma węzłów wydobywczych ani pul wydobywczych *(mining pools)*; zamiast tego zniszczona jest około jedna tysięczna centa z każdej transakcji[20]. Ripple nie został zaprojektowany z wyraźnymi celami anonimowości, ale posiada funkcje zapewniające prywatność, takie jak korzystanie z płatności proxy.

[19] "What Is Dash?", WeUseCoins. https://www.weusecoins.com/what-is-dash/ data dostępu: 27.03.2018.

[20] A. Brown, "10 things you need to know about Ripple," CoinDesk, May 17, 2013. https://www.coindesk.com/10-things-you-need-to-know-about-ripple/ data dostępu: 27.03.2018.

3.2 Hyperledger

Hyperledger to grupa projektów mających na celu tworzenie otwartych ksiąg rozproszonych o otwartych źródłach[21]. Projekt Hyperledger jest obsługiwany i hostowany przez Linux Foundation. Mimo że hostowane przez Linux Foundation, każdy projekt został opracowany i wniesiony przez różne źródła. W ramach projektu Hyperledger jest kilka projektów, z których każdy zapewnia platformę blockchain do rozwiązywania konkretnych problemów.

Cele:

- spowodowanie, by technologia blockchain przeniknęła przemysł na wszelkie możliwe sposoby (cross-industry);
- przeniesienie rozwiązań blockchain na grunt komercyjny.

Członkowie:

- 10020 firm i instytucji - liderzy w dziedzinie finansów, bankowości, Internetu przedmiotów, łańcucha dostaw, produkcji i technologii.

Obszary zainteresowań:

- Definiowanie usług finansowych dla zastosowania blockchain i prowadzenie różnego rodzaju proof-of-concept w zakresie finansów;
- Ujednolicenie odmiennych procesów w zakresie opieki zdrowotnej, zwiększenie przepływu danych i płynności, zmniejszenie kosztów i poprawa świadczeń dla pacjenta.

[21] "Hyperledger Business Blockchain Technologies", The Linux Foundation. https://www.hyperledger.org/projects data dostępu: 27.03.2018.

Projekty:

- Hyperledger Fabric:

efekt pierwszego Hackathonu; implementacja technologii blockchain, która ma służyć jako podstawa do rozwijania aplikacji i rozwiązań blockchain. Oferuje on architekturę modułową i wykorzystuje technologię pojemnościową do organizacji inteligentnych umów zwanych „chaincode". Został stworzony przez IBM i DAH.

- Hyperledger Sawtooth:

jest to modułowa rozproszona księga, wykorzystująca dowód upływającego czasu jako protokół konsensusu. W dowodzie upływającego czasu każdy uczestnik żąda "czasu oczekiwania" od sprzętowej enklawy (zaufanej i bezpiecznej funkcji dostępnej na niektórych urządzeniach), która losowo rozkłada czas oczekiwania. Niezależnie od tego, który uczestnik otrzymał najkrótszy czas, tworzy następny blok w łańcuchu. Korzystanie z oprogramowania Sawtooth firmy Hyperledger jest ściśle powiązane ze sprzętem obsługującym funkcję enklawy sprzętowej. Hyperledger Sawtooth został początkowo wniesiony przez firmę Intel.

- Hyperledger Iroha:

działa to jako usługa Identity / Know Your Customer (KYC) przy użyciu technologii blockchain, która umożliwia instytucjom udostępnianie danych i zarządzanie tożsamością. Hyperledger Iroha był początkowo współtworzony przez Soramitsu, Hitachi, NTT Data i Colu.

- Hyperledger Burrow

Hyperledger Burrow jest platformą blockchain z uprawnieniami umożliwiającymi inteligentne zawieszenie umów. Akceptuje kod inteligentnych kontraktów opartych na Ethereum. Hyperledger Burrow został pierwotnie przekazany przez Monax i sponsorowany przez firmę Intel.

- Hyperledger Indy:

jest to niezależna platforma tożsamości zapewniająca pochodzenie transakcji powierniczych i odpowiedzialności. Obsługuje kontrolowane przez użytkownika wymiany sprawdzalnych roszczeń dotyczących identyfikacji informacji, a także modeli unieważnień.

Obsługuje następujące ważne funkcje prywatności:

- zdecentralizowane identyfikatory (DID),
- wskaźniki do źródeł poza księgi rachunkowej, aby żadne dane osobowe nie były zapisywane w księdze rachunkowej,

Kod Indy został wniesiony do Projektu Hyperledger przez Fundację Sovrin.

3.3 Konsorcja R3CEV oraz Multichain

Konsorcjum to organizacja zrzeszająca kilku podmiotów na określony czas w konkretnym celu. Ważne znaczenie w badaniu, szukaniu sposobów wdrożenia technologii blockchain mają konsorcja i rady blockchain. Większość z nich powstała w okolicach połowy 2016 r. Konsorcja te mają swoje siedziby głównie w USA i Wielkiej Brytanii, ale także w Japonii, Chinach, Kanadzie, Luksemburgu czy Dubaju. Największe z nich (Hyperledger i ISITC) zgromadziły 100 członków, a łączna liczba instytucji zaangażowanych w konsorcja to ok. 550.

Główne obszary zainteresowań konsorcjów to przede wszystkim upowszechnianie wiedzy na temat tej nowej technologii, odkrywanie jej możliwych zastosowań i wdrażanie w różnych dziedzinach gospodarki (początkowo poprzez projekty pilotażowe, umożliwiające zdobycie wiedzy na potrzeby późniejszych pełnych wdrożeń).

Obszary działań konsorcjów:

- współpraca w sektorze finansów;
- poprawa opieki zdrowotnej i świadczeń medycznych;
- poprawa sprawności funkcjonowania i oszczędności dla administracji i rządu;
- poprawa logistyki transportu i łańcucha dostaw;
- rozwój blockchain w rachunkowości;
- rozwój blockchain w przemyśle farmaceutycznym;
- edukowanie instytucji i firm zainteresowanych blockchain;
- pomoc we wdrażaniu blockchain w konkretnych projektach;
- oferowanie platform edukacyjnych, ułatwiających zrozumienie blockchain i wdrażanie projektów.

Kilka konsorcjów zawiązało się w celu standaryzacji blockchain i technologii rozproszonych rejestrów, a także opracowania regulacji prawnych, sprzyjających rozwiązaniom opartym na blockchain. Ponadto każde z powstałych konsorcjów zdaje się być płaszczyzną wymiany doświadczeń i know-how dla projektów badawczych, dzięki współpracy ekspertów w dziedzinie blockchain i naukowców z uczelni, co skutkuje komercjalizacją rozwiązań blockchain. Konsorcjum pozwala na zdobycie obszerniejszej wiedzy w zakresie blockchain i umożliwia rozwijanie tematu rozproszonego rejestru równolegle w wielu dziedzinach. Konsorcja same w sobie nie dają przewagi konkurencyjnej, dlatego większość ich członków angażuje się w kilka różnych inicjatyw równolegle. W Polsce wykorzystano istniejący już schemat współpracy administracji i biznesu wypracowany w rządowym programie „Od papierowej do cyfrowej Polski" w postaci tzw. strumieni. Stąd – decyzją Minister Cyfryzacji Anny Streżyńskiej – powołano Strumień „Blockchain/DLT i waluty cyfrowe".

Konsorcjum R3CEV powstało 15.09.2015 r. z inicjatywy jego lidera – R3 (2014 r.) – innowacyjnej firmy koncentrującej się na budowaniu i wzmacnianiu nowej generacji globalnej technologii usług finansowych. Członkowie założyciele: Barclays, BBVA, Commonwealth Bank of Australia, Credit Suisse, Goldman Sachs, J.P. Morgan, Royal Bank of Scotland, State Street, and UBS. Jest to jedno z największych konsorcjów blockchain – 7016 instytucji finansowych i największych na świecie firm technologicznych.

Cel:

- wdrożenie technologii blockchain w największych światowych bankach i instytucjach finansowych.

Obszary zainteresowań:

- projektowanie i dostarczanie zaawansowanych technologii rozproszonych rejestrów na światowe rynki finansowe;
- współpraca z instytucjami partnerskimi w zakresie badań, eksperymentów i projektowania;
- informowanie i gromadzenie użytkowników nowej technologii w procesie projektowania i produkcji od samego początku.

3 filary działalności wspierane przez badania cross-stream:

1. Finansowy rozwój rejestru – rozwijanie podstawowej architektury odniesienia, by podbudować finansowy rozwój rejestru.
2. Centrum badawcze – rozmieszczanie bezpiecznych laboratoriów, które, współpracując ze sobą, będą testować jakość technologii blockchain.
3. Rozwój produktu – wdrażanie kolejnych wypracowanych i pilotażowych rozwiązań, w celu identyfikacji i projektowania aplikacji komercyjnych.

Projekty:

1. Prezentacja szablonów inteligentnych kontraktów Barclays w londyńskim Barclays Akcelerator Demo Day At The O2 w 18.04.2016. Był to pierwszy publiczny pokaz platformy rozproszonego rejestru Corda18 za pomocą prototypu.
2. Concord - platforma, która częściowo jest repliką Bitcoin, Ethereum i innych sieci opartych na blockchain. Ma zmienione najważniejsze funkcje i koncepcje tak, by mogła być stosowana w środowisku bankowym.
3. „Crypto 2.0" Inteligentne zastosowanie technologii kryptograficznej i protokołów opartych na rozproszonym rejestrze na globalnych rynkach finansowych.
4. „Exchances" - innowacyjne rozwiązania egzekucyjne, które pozwalają zdefiniować na nowo doświadczenia handlowe dla istniejących i rozwijających się klas aktywów.
5. „Ventures" - ukierunkowanie inwestycji początkowego stadium w spółkach opartych na przyszłościowym myśleniu, które stawiają sobie za cel kształtowanie nowej generacji usług finansowych.

MultiChain to otwarta platforma blockchain, która pozwala każdemu skonfigurować i wdrożyć prywatny, półprywatny lub publiczny blockchain. MultiChain jest rozwidleniem Bitcoin, ale z wieloma modyfikacjami. Użytkownicy mogą określić, czy blockchain ma być powiązany z kryptowalutą, jak również metodę consensus. W domyślnej konfiguracji MultiChain to prywatny, oparty na uprawnieniach blockchain, wykorzystujący consensus typu round-robin. Oznacza to, że pierwsza osoba, która skonfigurowała blockchain, działa jako administrator i początkowy węzeł; wszyscy dodatkowi użytkownicy muszą skierować swoich klientów MultiChain do tego pierwszego węzła, a administrator musi nadać im uprawnienia.

Strumienie MultiChain[22] są unikalną cechą; są one opisane jako "wspólne niezmienne bazy danych szeregów czasowych w kluczach i wartościach", które są przechowywane w łańcuchu bloków.

3.4 Szanse i ograniczenia

Ideą technologii blockchain jest eliminowanie pośredników, jakimi są instytucje finansowe, i to, czy banki będą potrafiły dostosować się do nowego modelu biznesowego, będzie zależało czy technologia stanie się wielkim zagrożeniem lub szansą do rozwoju i pozyskiwania nowych klientów.

Główne zalety, które blockchain może przynieść np. w sektorze bankowym:

1. Dokumentowanie

W kontekście instytucji finansowych blockchain może być narzędziem ustalenia zaufania, w sytuacji, kiedy takie jest wymagalne, na przykład, weryfikacja tożsamości i zdolności kredytowej klienta za pomocą połączenia historii transakcji z blockchain.

2. Koszt

Transakcje peer-to-peer, które mogą zaoszczędzić bankom ok. 20 miliardów dolarów biurowych kosztów[23]. W wyniku mniejszych kosztów, banki mogą zaoferować szerszy dostęp do usług finansowych oraz rynków kapitałowych poprzez udostępnianie produktów za pomocą aplikacji mobilnych.

3. Szybkość

Obecnie funkcjonujące procesy bankowości korespondencyjnej są dość wolne i drogie, a sieć pośredników bardzo złożona, blockchain natomiast może uprościć i zautomatyzować ten proces. Przejście do natychmiastowych transakcji uwolniłoby znaczną część kapitału, przebywające w tranzycie podczas takich transakcji.

[22] G. Greenspan, “Introducing MultiChain Streams,” MultiChain, September 15, 2016. http://www.multichain.com/blog/2016/09/introducing-multichain-streams/ data dostępu: 28.04.2018.
[23] “The Fintech 2.0 Paper: rebooting financial services”, Santander, 2015.

4. Zarządzanie ryzykiem

Technologia blockchain może zmniejszyć kilka rodzajów ryzyka finansowego. Pierwszym jest ryzyko rozliczeniowe, czyli niepomyślna transakcja przez usterkę w procesie rozliczeniowym. Drugim jest ryzyko kontrahenta – niewywiązanie się przez kontrahenta z obowiązania. Najbardziej znaczącym jest ryzyko systemowe – łączna suma wszystkich zaległych kontrahentów w systemie. Natychmiastowe transakcje za pomocą blockchain mogą w całości wyeliminować wyżej wymienione formy ryzyka.

5. Open source

Obecne systemy, działające w sektorze usług finansowych utknęły się w technologicznym progresie i potrzebują zmian. Jako technologia typu *open source*, blockchain może stale rozwijać się i wprowadzać innowacje, opierając się na innych użytkowników, z którymi powiązana jest sieć.

Te zalety potwierdzają, że wdrożenie systemu blockchain znacznie obniża koszty, eliminuje ryzyka, podwyższa szybkość transakcji i niesie ze sobą wysoką wartość innowacji.

Zdolność do adaptacji ma potencjał zmienić nie tylko model biznesowy banków, a również sektor papierów wartościowych, księgowości, kapitału wysokiego ryzyka, zarządzania ryzykiem przedsiębiorstw i innych filarów branży.

Technologia blockchain ma wiele korzyści dla całego społeczeństwa, jednak są obszary, w których tradycyjne systemy są niezbędne. Niektóre powody, dla których wciąż jest sensowność zdecentralizowanych systemów:

1. Ochrona klienta

Blockchain działa jako system rozliczeniowy typu *push*. Oznacza to, że jednostka posiada uprawnienia nad zasobem, który chce zweryfikować za pomocą zdecentralizowanego systemu. Mogą to być kryptowaluty, uwierzytelnienia certyfikatów, tytuły gruntów itp. Problem polega na tym, że w momencie, kiedy transakcja już zrealizowała się i została zweryfikowana w systemie, jedynym możliwym sposobem zwrotu transakcji jest przypadek, kiedy strony zgadzają się na jej odwrócenie. W przypadku systemu scentralizowanego, jak na przykład bank, istnieje procedura umożliwiająca rozstrzyganie sporów po zakończeniu transakcji.

2. Rozliczanie w blockchain jest powolne

Wszyscy uczestnicy sieci muszą potwierdzić, że transakcja jest ważna, co w przypadku jednego pośrednika – banku jest znacznie szybciej.

3. Atak 50%+

Aby transakcja w sieci została uznana jako ważna połowa obliczeniowej mocy całego systemu musi to potwierdzić. Atak 50%+ polega na zmianie zaistniałej transakcji przez sztuczne utworzenie bloku na tej samej wysokości z transakcją, która ma innego adresata, i uczynieniem alternatywnej drogi dominującą w łańcuchu[24]. Całkowita moc sieci jest ogromna, dlatego posiadanie ponad połowy mocy obliczeniowej wymaga ogromnej ilości pieniędzy.

4. Rosnący rozmiar bloków

Z każdym nowym blokiem rośnie blockchain. Problem polega na tym, że każdy uczestnik sieci przechowuje w bloku cała historię wszystkich transakcji w celu uczestnictwa. Każda transakcja zajmuje kilku bajtów, natomiast całkowity rozmiar wszystkich bloków obecnie wynosi ok. 165 GB[25]. Przy czym, wykorzystanie blockchain nadal wzrasta.

Istnieje tendencja do nadmiernego hałasu i nadużywania najbardziej rodzącej się technologii. Wynika to z faktu, że technologia jest stosunkowo nowa i nie jest dobrze rozumiana, a jej możliwości są otoczone błędnymi przekonaniami. Dalej zostaną przedstawione niektóre z ograniczeń i błędnych koncepcji technologii blockchain:

a) Kontrola blockchain

Częstym błędnym przekonaniem jest to, że publiczne łańcuchy bloków to systemy bez kontroli i własności. Przy zaletach technologii często pojawia się pogląd, że nikt nie kontroluje blockchain, jednak, gdy żaden użytkownik, rząd ani kraj nie kontroluje blockchain, wciąż istnieje grupa głównych programistów, którzy są odpowiedzialni za rozwój systemu. Twórcy ci mogą działać w interesie społeczności, ale nadal utrzymują pewien poziom kontroli.

[24] P. Lis Markiewicz, S. Nowak, … op. cit., s. 75.
[25] www.blockchain.info/charts/blocks-size, data dostępu: 20.04.2018.

Na przykład, w 2013 r. grupa deweloperów stworzyli nową wersję oprogramowania Bitcoin, który wprowadził lukę i tymczasowo podzielił łańcuch bloków na dwie różnie sieci o różnych zasadach. Twórcy musieli zdecydować czy zachować nową wersję (która nie została jeszcze przyjęta przez wszystkich), czy przywrócić starą wersję[26]. Każdy wybór spowodowałby odrzucenie jednego łańcucha - a transakcje pieniężne niektórych osób stałyby nieważne.

Twórcy dokonali wyboru, powrócili do starej wersji oprogramowania i pomyślnie kontrolowali postępy blockchain Bitcoin. Ten przykład był niezamierzoną zmianą w oprogramowaniu i implementacji łańcucha blokowego *(fork)*; programiści mogą jednak celowo budować zaufanie nowych klientów, a przy odpowiedniej adaptacji z bazy użytkowników można utworzyć udany fork. Te zmiany w oprogramowaniu blockchain są często omawiane z dużą dokładnością i mają długi okres adaptacji, zanim zostaną wprowadzone jako obowiązkowe, aby kontynuować rejestrację transakcji na nowym "głównym" forku.

Wyrażenie "nikt nie kontroluje blockchain" byłoby lepiej określone jako "nikt nie kontroluje z kim i kiedy można wykonać transakcje, w ramach zasad systemu blockchain."

b) Złośliwi użytkownicy

Podczas gdy system blockchain może egzekwować reguły transakcji i specyfikacje, nie może wymuszać kodeksu postępowania. Jest to problematyczne w publicznych systemach blockchain, ponieważ użytkownicy są anonimowi i nie ma mapowania typu jeden-do-jednego między węzłami blockchain a użytkownikami systemu. Publiczny łańcuch bloków zapewniają zachętę (np. kryptowalutę) do motywowania użytkowników do uczciwego działania; jednak niektórzy mogą działać złośliwie, jeśli zapewnia to większe zachęty. Największym problemem dla złośliwych użytkowników jest uzyskanie wystarczającej mocy (np. Udziału w systemie, mocy obliczeniowej itp.), Aby spowodować szkody.

[26] Narayanan A., "Analyzing the 2013 Bitcoin fork: centralized decision-making saved the day," MultiChain, July 28, 2015. https://freedom-to- tinker.com/2015/07/28/analyzing-the-2013-bitcoin-fork-centralized-decision-making-saved-the-day, data dostępu: 29.03.2018.

Po utworzeniu wystarczająco dużej, złośliwej zmowy działania złośliwego kopania mogą obejmować:

- Ignorowanie transakcji od określonych użytkowników, węzłów, a nawet całych krajów.
- Stworzenie zmienionego, alternatywnego łańcucha w tajemnicy, a następnie przesłanie go, gdy alternatywny łańcuch będzie dłuższy niż prawdziwy łańcuch. Uczciwe węzły przestawią się na łańcuch, który ma najwięcej "pracy" (zgodnie z protokołem blockchain). Może to zaatakować pojęcie "niezmienności" w systemie blockchain.
- Odmowy przekazywania bloków innym węzłom, co zasadniczo zakłóca dystrybucję informacji.

c) Użycie zasobów

Technologia Blockchain reprezentuje światową sieć wartości, w której każda transakcja jest weryfikowana, a cały blockchain jest zsynchronizowany z wieloma użytkownikami. W przypadku systemów blockchain wykorzystujących dowód pracy, oznacza to, że duża liczba użytkowników traci czas na przetwarzania informacji i zużywa dużo energii elektrycznej.

Łańcuchy bloków są często porównywane z bazami danych, ale ilość danych, które mogą być przechowywane w systemie blockchain jest mocno ograniczona. Przy czym informacja jest ogólnodostępna, zatem bloki nie mogą spełniać funkcji nośnika pamięci. Aby szybko obliczyć hasze transakcji i rozdzielić transakcje pomiędzy wszystkich w sieci, transakcje muszą być stosunkowo niewielkie. Duże ilości danych są zwykle przechowywane "poza łańcuchem", z "wskaźnikami / referencjami" lub hasłami danych przechowywanych w samym bloku blockchain.

d) Przenoszenie ciężaru przechowywania danych uwierzytelniających na użytkowników

Ponieważ blockchain nie jest scentralizowanym systemem, nie ma wewnętrznego centralnego miejsca do zarządzania kluczami użytkowników. Użytkownicy muszą zarządzać własnymi kluczami prywatnymi, co oznacza, że w przypadku zagubienia, wszystko związane z tym kluczem prywatnym zostanie utracone (zasoby cyfrowe itd.). Nie ma opcji "zapomniałem hasła" lub "odzyskaj moje konto" dla systemów blockchain. Chociaż można wdrożyć scentralizowane rozwiązania do zarządzania, stwarzają one te same problemy, co obecne systemy: centralne punkty awarii.

e) Infrastruktura prywatnych/publicznych kluczy i tożsamość

Fakt, że technologia blockchain zawiera infrastrukturę klucza publicznego/prywatnego, nie oznacza, że również wewnętrznie wspiera tożsamość. Tak nie jest, ponieważ nie ma relacji jeden-do-jednego z parami kluczy prywatnych do użytkowników (użytkownik może mieć wiele kluczy prywatnych), ani nie istnieje relacja jeden-do-jednego między adresami blockchain a kluczami publicznymi (wiele adresów można uzyskać z jednego klucza publicznego). Węzły w łańcuchu Bitcoin walidują transakcje, zanim zostaną dodane do bloku, a następnie są włączane do blockchain. Jeden etap tej weryfikacji wymaga, aby użytkownik, który zainicjował transakcję, podpisał transakcję kluczem prywatnym. Węzły blockchain weryfikują podpis, aby udowodnić, że użytkownik faktycznie jest właścicielem przekazywanej wartości Bitcoin.

Podpisy cyfrowe są często wykorzystywane do udowodnienia tożsamości w świecie cyberbezpieczeństwa, co może prowadzić do nieporozumień dotyczących potencjalnego zastosowania blockchain do zarządzania tożsamością. Proces weryfikacji podpisu transakcji blockchain łączy transakcje z właścicielami kluczy prywatnych, ale nie zapewnia możliwości powiązania rzeczywistych tożsamości z tymi właścicielami.

W niektórych przypadkach możliwe jest łączenie tożsamości w świecie rzeczywistym z kluczami prywatnymi, ale połączenia te są wykonywane za pośrednictwem procesów zewnętrznych, a nie bezpośrednio wspieranych przez blockchain. Na przykład organ ścigania może zażądać zapisów z giełdy, które łączyłyby transakcje z konkretnymi osobami. Innym przykładem jest osoba publikująca adres online dla darowizn.

Chociaż możliwe jest stosowanie blockchain w ramach zarządzania tożsamością, które wymagają rozproszonego komponentu księgi, ważne jest, aby zrozumieć, że typowe implementacje łańcucha bloków nie są zaprojektowane jako osobne systemy zarządzania tożsamością, ale więcej do posiadania bezpiecznych tożsamości cyfrowych niż po prostu wdrożenie blockchain.

Podsumowując, technologia blockchain ma wiele zalet, ale również jest kontrowersyjna. To od banków zależy, czy będą w stanie zmienić się i przystosować się do nowych technologii, testując blockchain i wykorzystać technologię jako ścieżkę do rozwoju oraz pozyskiwania nowych rozwiązań w sferze usług finansowych.

Zakończenie

W opracowaniu została zaprezentowana technologia blockchain oraz jej zastosowania. Rozpoczęto od typowych zastosowań w postaci transakcji *peer-to-peer* bez udziału pośredników, bezpośrednio pomiędzy dwoma podmiotami z wykorzystaniem szyfrowania, dzięki czemu uczestnicy nie muszą podlegać identyfikowaniu z uwagi na fakt, że transakcje kierowane są do konkretnych użytkowników. Potwierdzenie transakcji odbywa się z udziałem wszystkich węzłów sieci za pomocą publicznej historii transakcji, której zmiana jest obliczeniowo niemożliwa, jeżeli węzły posiadają większość mocy obliczeniowej systemu.

Blockchain to znacząca nowa droga do rozwoju technologicznego, umożliwiająca bezpieczne transakcje bez potrzeby posiadania centralnego organu. Od czasów powstania kryptowaluty bitcoin, rośnie liczba innych kryptowalut, opartych na technologii łańcucha bloków, co ważniejsze, powstają nowe zastosowania, wykraczające poza dziedzinę transferu środków.

Wykorzystanie blockchain jest wciąż na wczesnym etapie, ale jest oparte na szeroko rozumianych i rozsądnych zasadach kryptograficznych. Idąc dalej, jest prawdopodobne, że blockchain będzie kolejnym narzędziem, które może być użyte do rozwiązania nowych problemów, dlatego w niniejszym opracowaniu zwrócono szczególną uwagę na narzędzia blockchain, które otwierają nowe możliwości zastosowania technologii, oprócz systemu transakcji.

Blockchain ma również duży potencjał do przechowywania i rejestrowania zapisów danych łańcucha dostaw. Technologia może rejestrować każdy krok w życiu produktu, od momentu utworzenia go w fabryce, po jego wysłaniu, a następnie dostarczeniu do sklepu, a na końcu do momentu zakupu przez konsumenta.

Mogą istnieć nawet nowe branże, takie jak notariusze cyfrowi, którzy mogą udowodnić, że dana osoba ma dostęp do konkretnej informacji, zapisując jej skrót do łańcucha bloków. Istnieje wiele potencjalnych zastosowań i możliwości dla technologii blockchain.

Z uwagi na fakt, że technologia blockchain jest bardzo młoda, świat dopiero zaczyna poznawać korzyści systemu. Obecnie technologia jest używana w niektórych administracjach państwowych w celu rejestracji własności, potwierdzenia tożsamości, wypłaty świadczeń lub

tworzenia publicznych baz danych przeprowadzonych transakcji na bazie blockchain, co ma na celu zmniejszenie oszustw i zwiększenie przejrzystości systemu. Sektor prywatny, w tym banki nadal testują technologię, tworzą pilotażowe projekty blockchain, szukają możliwości wdrożenia technologii, aby nie tracić pozycji zaufanego pośrednika.

Technologia ma potencjał konkurencyjny z funkcjonującym od lat scentralizowanym systemem zaufania publicznego i organizacjami finansowymi. Prawdopodobnie skutki nadchodzących zmian i nowych rozwiązań odczują banki. Mogą one być zmuszone do dostosowania lub nawet całkowitej zmiany swoich praktyk i modeli biznesowych.

❖ Bibliografia

1. Perez K., Urbaniak M., Bitcoin – wirtualny eksperyment czy waluta przyszłości?, „Ruch Prawniczy, Ekonomiczny i Socjalistyczny", Rok LXXV – zeszyt 4 - 2013, s. 164.
2. Lis Markiewicz P., Nowak S., Bitcoin. Przyszłość inwestowania, Wydawnictwo Naukowe PWN, Warszawa 2015
3. Mougayar W., The business blockchain, John Wiley & Sons, Inc., Hoboken, New Jersey, 2016
4. Tapscott D., Tapscott A., "Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World", Portfolio, 2016
5. Gupta M., *Blockchain*, John Wiley & Sons, Inc., 2017
6. Nakamoto S., 2009, "Bitcoin: A Peer-to-Peer Electronic Cash System", tłum. http://bitcoin.pl/o-bitcoinie/manifest-satoshi-nakamoto, (data dostępu: 15.10.2017)
7. Credit Suisse, Report Blockchain, Europe/United Kingdom, 2016 http://www.the-blockchain.com/docs/Credit-Suisse-Blockchain-Trust-Disrupter.pdf (data dostępu: 12.10.2017)
8. Credit Suisse, Report Blockchain, Europe/United Kingdom, 2017 http://www.the-blockchain.com/docs/Credit-Suisse-Blockchain-Trust-Disrupter.pdf (data dostępu: 20.04.2018)
9. www.blockchain.info/charts/blocks-size (data dostępu: 20.04.2018)
10. Chepel A., "Pro-bitcoin Estonian bank creates a wallet based on Colored Coins", Coinfox, 08 June 2015, http://www.coinfox.info/news/2169-cuber (data dostępu: 15.10.2017)

11. Desjardins J., "The Power of Smart Contracts on the Blockchain", http://www.visualcapitalist.com/smart-contracts-blockchain/ (data dostępu: 14.10.2017)
12. Korpała F., „Czym jest Smart Contract?", 2017, https://bithub.pl/artykuly/czym-smart-contract/ (data dostępu: 14.10.2017)
13. Jajesniak E., „Blockchain jako rewolucja technologiczna i jej zastosowania przez rządy krajów", 2016, https://www.lazarski.pl/pl/wydzialy-i-jednostki/instytuty/wydzial-ekonomii-i-zarzadzania/centrum-technologii-blockchain/blockchain-jako-rewolucja-technologiczna-i-jej-zastosowanie-przez-rzady-krajow/ (data dostępu: 12.10.2017)
14. Ministerstwo Cyfryzacji, „Od papierowej do cyfrowej Polski", 2017, https://www.gov.pl/cyfryzacja/od-papierowej-do-cyfrowej-polski?inheritRedirect=true (data dostępu: 14.10.2017)
15. Santander, The Fintech 2.0 Paper: rebooting financial services, Santander InnoVentures,https://www.finextra.com/finextradownloads/newsdocs/the%20fintech%202%200%20paper.pdf (data dostępu: 13.10.2017)
16. Garstka M., Piech K., „Konsorcja i Rady Blockchain na Świecie", 2017 https://www.gov.pl/cyfryzacja/strumien-blockchain/dlt-i-waluty-cyfrowe (data dostępu: 18.10.2017)
17. NIST (National Institute of Standards and Technology) - https://www.nist.gov/publications/secure-hash-standard (data dostępu: 12.03.2018)
18. http://www.qrcode.com/en/about/ (data dostępu: 22.03.2018)
19. Computer Security Resource Center, Blockchain Technology Overview, U.S. Department of Commerce, 201 https://csrc.nist.gov/publications/detail/nistir/8202/draft (data dostępu: 22.03.2018)
20. Hertig A., "Litecoin's SegWit Activation: Why it Matters and What's Next," CoinDesk, April 26. 2017. https://www.coindesk.com/litecoins-segwit-activation-why-it-matters-and-whats-next/ (data dostępu: 27.03.2018)
21. Litecoin Project. https://litecoin.org/ (data dostępu: 27.03.2018)
22. Wood G., "Ethereum: A Secure Decentralised Generalised Transaction Ledger" (data dostępu: 27.03.2018)

23. “What Is Dash?”, WeUseCoins. https://www.weusecoins.com/what-is-dash/ (data dostępu: 27.03.2018)
24. Brown A. “10 things you need to know about Ripple,” CoinDesk, May 17, 2013. https://www.coindesk.com/10-things-you-need-to-know-about-ripple/ (data dostępu: 27.03.2018)
25. “Hyperledger Business Blockchain Technologies”, The Linux Foundation. https://www.hyperledger.org/projects (data dostępu: 27.03.2018)
26. Greenspan G., “Introducing MultiChain Streams,” MultiChain, September 15, 2016. http://www.multichain.com/blog/2016/09/introducing-multichain-streams/ (data dostępu: 28.04.2018)
27. Narayanan A., “Analyzing the 2013 Bitcoin fork: centralized decision-making saved the day,” MultiChain, July 28, 2015. https://freedom-to-tinker.com/2015/07/28/analyzing-the-2013-bitcoin-fork-centralized-decision- making-saved-the-day (data dostępu: 29.03.2018)
28. Donnelly, J., “What is the 'Halving'? A Primer to Bitcoin's Big Mining Change,” CoinDesk, June 12, 2016. https://www.coindesk.com/making-sense-bitcoins- halving/ (data dostępu: 27.03.2018)
29. Gipp B., Meuschke N., Gernandt A., “Decentralized Trusted Timestamping using the Crypto Currency Bitcoin,” in Proceedings of the iConference 2015, Newport Beach, California, 2015, (data dostępu: 20.04.2018)
30. Mell P., Kelsey J., Shook J., “Cryptocurrency Smart Contracts for Distributed Consensus of Public Randomness.” October 7, 2017. https://doi.org/10.1007/978-3-319-69084-1_31, (data dostępu: 20.04.2018)

Streszczenie

Tematem niniejszej pracy jest technologia blockchain oraz sposoby potencjalnego zastosowania w różnych dziedzinach, w tym bankowości. Dodatkowo biorąc pod uwagę nowatorstwo i złożoność tematyki przedstawiono zagadnienia stosowanych technologii informatycznych i kryptograficznych. Jednocześnie uwzględniając duży rozgłos w świecie finansów poruszone zostały kwestie dotyczące bezpieczeństwa, problemów i jakie są ograniczenia implementacji blockchain.

Praca składa się z trzech części. W pierwszej z nich przedstawiono zarys teoretyczny opisujący działanie technologii, komponenty, na których opiera się blockchain, wykorzystywane mechanizmy informatyczne i kryptograficzne. Nacisk został położony na działanie systemu na przykładzie kryptowaluty bitcoin, który jest najbardziej znanym przykładem realizacji płatności w ramach systemu łańcucha bloków. Przedstawione zostały funkcje podpisu i uwierzytelniania transakcji za pomocą par kluczy prywatnych/publicznych, a także proces bezpiecznego cyfrowego podpisu i weryfikacji. Wytłumaczono również tworzenie i pochodzenie adresów, używanych do wysyłania i odbierania zasobów cyfrowych na przykładzie całego cyklu życia transakcji Bitcoin.

Druga część poświęcona jest narzędziom technologii, wykraczającym poza zwykle płatności czy stworzenie kryptowalut. Wprowadzone zostały rozróżnienia pomiędzy publicznym a prywatnym blockchain, opisano ich cechy, wady, które należy wziąć pod uwagę przed podejmowaniem decyzji o wdrożenie technologii, możliwości konfiguracji oraz przedstawiono niektóre zastosowania i problemy, które rozwiązuje blockchain. Zagadnienie to jest bardzo istotne, ponieważ wybór typu łańcucha bloków ma znaczny wpływ na bezpieczeństwo oraz potencjalne korzyści, które może przynieść takie rozwiązanie. Następnie szczegółowo przeanalizowano, jak działają zaufane rozproszone księgi w systemie blockchain, kto jest uczestnikiem całego procesu, jak się odbywa sprawdzanie poprawności transakcji oraz mechanizm tworzenia kopii zapasowych danych. Następnie opisano kolejny postęp technologii blockchain - umowy inteligentne (ang. smart contracts), które pozwalają na przejście z protokołu transakcji finansowych do narzędzia, które automatycznie będzie wdrażać warunki umów, minimalizując ryzyko błędu i manipulacji. Na zakończenie rozdziału przedstawiono wstępne implementacje zastosowań, np. do obsługi różnorodnych transakcji

(handel, waluty, akcje, udziały, rynek energii elektrycznej), używania technologii przez niektóre rządy do wypłaty świadczeń, potwierdzenia tożsamości oraz tworzenie publicznych baz danych na bazie blockchain.

W ostatniej, trzeciej części przedstawiono potencjał technologii do zmiany sposobu oddziaływania na mienie intelektualne, rynki kapitałowe, ubezpieczenie, opiekę zdrowotną, rząd i wiele innych sektorów, między innymi potencjał zmienić tradycyjną bankowość. Przedstawiono również platformy blockchain, aby podkreślić różnice techniczne i stosowane podejścia. Pierwszą opisaną platformą są kryptowaluty, które są zorientowane głównie na przenoszenie wartości. Pokazano techniczne różnice, stosowane funkcje kryptograficzne oraz metody wydobywania. Drugą platformą są stworzone projekty przez powołane stowarzyszenia i konsorcja, które mają na celu tworzenie projektów, z których każdy zapewnia platformę blockchain do rozwiązywania konkretnych problemów. Przedstawiono obszary działań takich projektów, uczestnicy, cele i sposoby wdrożenia technologii blockchain. Szczególną uwagę zwrócono na szanse i ograniczenia technologii. Przedstawiono korzyści wykorzystywania blockchain w sektorze bankowym, takie jak zmniejszenie kosztów, zabezpieczenie przed ryzykiem, zwiększenie szybkości transakcji i wysoka wartość innowacji. Jednocześnie pokazane zostały ograniczenia technologii i błędne koncepcje, przeanalizowano problemy i obszary, w których tradycyjne systemy są niezbędne.

Słowa kluczowe

bankowość, blockchain, bitcoin, łańcuch bloków, hash, finanse, transakcja, smart contracts

ALTERUM Ośrodek Badań i Analiz Systemu Finansowego
ul. Solec 38 lok .104
00-394 Warszawa
mm@alterum.pl