MOŻLIWOŚCI WYKORZYSTANIA TECHNOLOGII BLOCKCHAIN

ARTUR ŻUWAŁA

Streszczenie

Technologia blockchain, pierwotnie użyta do stworzenia pierwszej kryptowaluty, bitcoina, rozwija się dynamicznie w ostatnich kilku latach. Jej podstawowym założeniem jest wykorzystanie sieci i algorytmów komputerowych do zapewnienia wiarygodności, oryginalności i czasu przekazu informacji pomiędzy stronami nie mającymi do siebie zaufania. Eliminuje to potrzebę istnienia zaufanej trzeciej strony do autoryzowania transakcji czy zawierania umów. Pozwala na tworzenie inteligentnych kontraktów realizowanych automatycznie po spełnieniu zaprogramowanych warunków, umożliwia każdemu emisję własnej waluty. Artykuł omawia założenia i sposób działania łańcucha bloków na przykładzie bitcoina. Pokazuje zastosowania technologii dotyczące między innymi kryptowalut, przelewów międzynarodowych, pozyskiwania funduszy, śledzenia dostaw, rozproszonych rejestrów.

Słowa kluczowe: blockchain, łańcuch bloków, kryptowaluty, bitcoin, ethereum, funkcje haszujące, inteligentne kontrakty, rozproszone rejestry, oferty ICO

Wprowadzenie

W roku 2017 nastąpił dynamiczny rozwój rynku kryptowalut. Jego wartość w maju 2018 roku wynosiła ponad 300 miliardów dolarów [2]. Gwałtowny wzrost kursu bitcoina, pojawienie się wielu nowych kryptowalut, a także zdarzające się, związane z nimi nieprawidłowości czy oszustwa [13] to najbardziej spektakularne wydarzenia wywołujące publiczną dyskusję i zainteresowanie państwowych regulatorów.

Podstawą działania kryptowalut jest technologia blockchain. Pozwala ona na tworzenie, przechowywanie danych i zarządzanie wiedzą w sieci powiązanych jednostek. Jej istotą jest zapewnienie integralności i oryginalności danych bez udziału jakiegokolwiek centrum autoryzacji w sytuacji, gdy jednostki te nie mają do siebie zaufania. Rolę gwaranta niezmienności zapisanych danych pełnią algorytmy matematyczne, a nie zaufanie do trzeciej strony, państwa czy instytucji.

Dalej idącą innowacją jest wprowadzenie inteligentnych umów (*ang. smart contracts*), które raz stworzone i zapisane w łańcuchu bloków będą realizować się automatycznie, gdy spełnią się określone w nich warunki. Instytucje państwowe i banki z jednej strony odbierają to jako zagrożenie dla własnych interesów, z drugiej same mogą wykorzystać technologię dla usprawnienia swoich działań.

Celem artykułu jest przybliżenie zasad działania technologii blockchain oraz przedstawienie możliwości jej zastosowania. Artykuł skupia się na kwestiach możliwości technicznych i pomija prawne aspekty zastosowania technologii blockchain, kryptowalut czy inteligentnych umów. Obecnie prawo większości krajów, w tym Polski, nie nadąża za zmianami technologicznymi, a odniesienie się do obecnej sytuacji prawnej [8] wykracza poza tematykę artykułu.

1. Zasady działania technologii blockchain

Podstawy działania technologii blockchain wraz z opisem jej zastosowania do stworzenia pierwszej kryptowaluty przedstawił w 2008 roku twórca bądź twórcy bitcoina występujący pod pseudonimem Satoshi Nakamoto. Jego lub ich prawdziwa tożsamość nie jest do dnia dzisiejszego znana. Manifest „Bitcoin: A Peer-to-Peer Electronic Cash System" został opublikowany w Internecie [11].

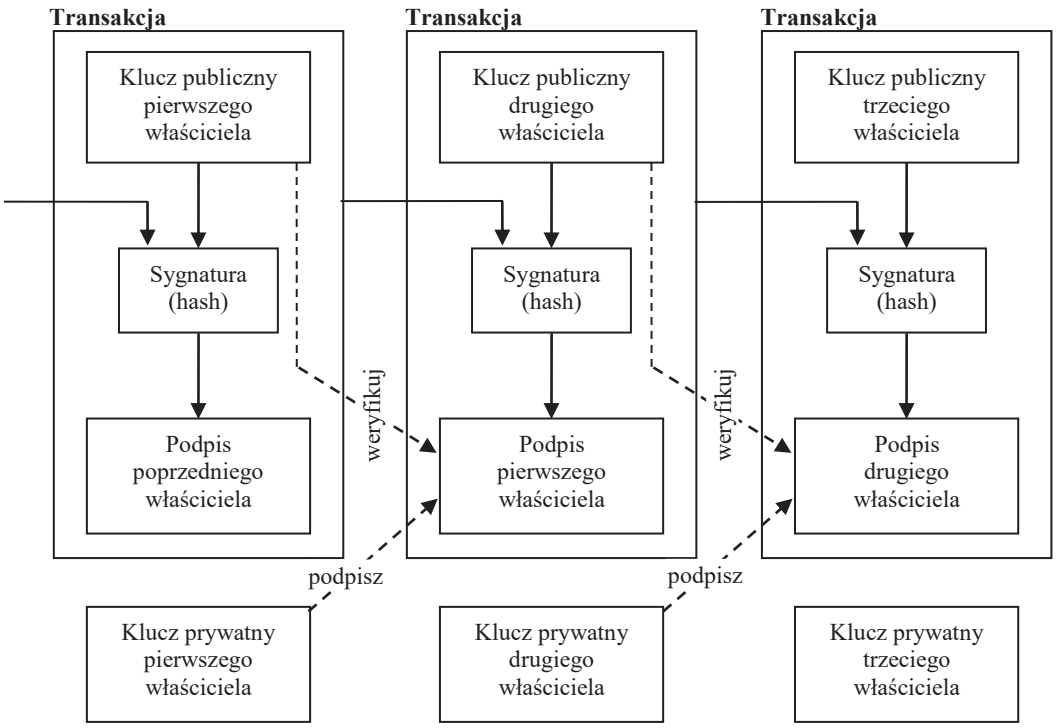
Ideą technologii blockchain zgodnie z jej nazwą jest stworzenie łańcucha powiązanych ze sobą bloków. Pojedynczy blok to zbiór dowolnych dokumentów cyfrowych, powstałych w podobnym czasie i posiadających wspólną sygnaturę cyfrową, tak zwany „hash".

Dla dowolnego dokumentu, zapisanego jako ciąg bitów, hash jest ciągiem znaków o stałej długości, zwykle znacznie krótszym od samego dokumentu i jest praktycznie nieodwracalny. Aby odtworzyć oryginalny dokument należałoby sprawdzić wszystkie potencjalne możliwości. Z drugiej strony dwa różne dokumenty dają różne sygnatury. Zmiana pojedynczego bitu oryginalnego dokumentu powoduje zmianę sygnatury. Powyższe własności pozwalają wykorzystać funkcje haszujące do zapewnienia prostej metody weryfikacji autentyczności pojedynczego dokumentu na podstawie znajomości jego krótkiej sygnatury. Co istotne, taka weryfikacja nie jest złożona obliczeniowo.

Stworzenie bloku z wielu dokumentów z już obliczonymi sygnaturami najczęściej jest realizowane przez ułożenie ich w strukturę drzewiastą i wyliczanie kolejnych sygnatur na każdym poziomie drzewa [10], tylko na podstawie sygnatur podrzędnych gałęzi, a nie pełnych dokumentów. Pozwala to na łatwe dołączanie do bloku kolejnych dokumentów bez potrzeby ponownego wykonywania obliczeń dla wcześniej dołączonych dokumentów. Po zakończeniu dodawania dokumentów do bloku pojedynczy hash pozwala zweryfikować autentyczność wszystkich dokumentów wchodzących w jego skład.

W przypadku bitcoina łańcuch bloków jest wykorzystywany do zapisu kolejnych transakcji. Do zapewnienia identyfikacji właścicieli kryptowaluty, a właściwie ich portfeli, wykorzystuje się powszechnie znane algorytmy szyfrowania niesymetrycznego. Pieniądz elektroniczny jest określony ciągiem wykonanych transakcji. Płatność inicjuje właściciel środków poprzez podpisanie kluczem prywatnym własnego portfela sygnatury poprzedniej transakcji oraz klucza publicznego portfela odbiorcy środków. Pierwszy klucz gwarantuje, że nadawca ma prawo do przesyłanych środków, a drugi, że nikt poza odbiorcą nie będzie w stanie ich odebrać. Schematycznie ciąg transakcji przedstawiono na rysunku 1. Wygląda to analogicznie do przelewu bankowego, ale zamiast numerów kont używane są klucze szyfrujące.

System walutowy będzie działał prawidłowo, jeżeli nie będzie możliwości wielokrotnego wydania tych samych środków. W wypadku pieniądza materialnego następuje jego fizyczne przekazanie. W wypadku przelewu bankowego to bank pełni rolę organu publicznego zaufania i gwarantuje, że nie można dwa razy zapłacić tymi samymi pieniędzmi. W przypadku braku zaufanej jednostki pośredniczącej jedynym sposobem zapewnienia, że płatnik nie wydał wcześniej tych samych środków na inne cele jest posiadanie informacji o wszystkich transakcjach oraz przyjęcie zasady, że ważna jest tylko pierwsza transakcja dotycząca konkretnych środków. Cel ten można zrealizować przez upublicznienie wszelkich transakcji oraz pewność kolejności ich wykonania. Tak jest to właśnie realizowane w przypadku bitcoina.



Rysunek 1. Schemat realizacji transakcji w łańcuchu bloków sieci bitcoin

Źródło: na podstawie [11].

Cały łańcuch bloków zawierających transakcję jest przechowywany przez wiele komputerów tworzących rozproszoną sieć równorzędnych węzłów sieci bitcoin. Żaden z nich nie jest wyróżniony, brakuje centralnego serwera. W tej sieci wszystkie bloki, a więc i transakcje są publicznie dostępne. Nie oznacza to jednak możliwości automatycznej identyfikacji stron tej transakcji. Jawne są publiczne klucze portfeli, co pozwala na weryfikację historii transakcji, ale dopóki nie uda się powiązać portfela z jego właścicielem może on pozostać anonimowy. Wystarczy jednak ujawnienie danych z dowolnej transakcji, aby powiązać portfel z właścicielem na przykład, gdy poda on swoje dane w celu dostawy zamówionego towaru lub rejestracji na giełdzie kryptowalut. Oczywiście każda osoba może posiadać wiele portfeli i używać ich niezależnie.

Każdy z węzłów sieci zbiera nowo rozgłaszane transakcje w blok. Akceptuje je tylko, gdy są prawidłowe i nie doszło do podwójnego wydatkowania w ramach bloku. Po zamknięciu bloku należy nadać mu znacznik czasu. Istotna jest przede wszystkim kolejność bloków, a nie bezwzględny czas ich powstania. Każdy blok posiada znacznik czasu, a ponieważ kolejny blok zawiera skrót poprzednika, to nie jest możliwa zmiana znacznika bloku bez modyfikacji wszystkich powstałych później bloków łańcucha.

W środowisku rozproszonym musi istnieć metoda konsensusu pozwalająca na zatwierdzenie bloku. W przypadku bitcoina zastosowano metodę „dowodu pracy" (proof-of-work), która sprowadza się do rozwiązania złożonego problemu obliczeniowego. Polega na znalezieniu przez węzły sieci wartości, dla której funkcja haszująca zwróci ciąg rozpoczynający się zadaną liczbą zer. Pozwala to na łatwe regulowanie jej złożoności, która rośnie wykładniczo wraz z oczekiwaną liczbą zer. Złożoność jest regulowana automatycznie tak, aby niezależnie od liczby zaangażowanych węzłów i mocy obliczeniowej nowy blok pojawiał się co mniej więcej dziesięć minut.

Każdy aktywny węzeł próbuje znaleźć dowód pracy dla nowego bloku. Jeżeli mu się to uda, rozgłasza to w sieci. Pozostałe węzły weryfikują zarówno poprawność transakcji jak i dowód pracy. Akceptacja bloku następuje poprzez rozpoczęcie pracy nad kolejnym blokiem z włączeniem do niego skrótu właśnie zaakceptowanego bloku. Obowiązuje zasada, że najdłuższy blok jest tym poprawnym. Na wypadek próby ataku na sieć bitcoin lub równoczesnego pojawienia się konkurencyjnych nowych bloków przyjmuje się, że transakcje sprzed sześciu bloków są pewne.

Tworzenie bloków jest pracochłonne – zużywa czas pracy procesorów oraz energię elektryczną. Motywacją do niego jest nagroda dla twórcy bloku w postaci utworzenia nowej monety. Ponadto przewidziano opłaty transakcyjne, w założeniu bardzo małe, które obecnie mają być dodatkowym wynagrodzeniem dla twórców bloków, a po zakończeniu emisji nowych monet ich jedyną gratyfikacją. Proces tworzenia nowych bloków powszechnie nazywany jest kopaniem lub wydobywaniem kryptowalut, zajmujące się tym osoby górnikami, a wykorzystywane przez nich komputery koparkami. Firmy zajmujące się wydobyciem walut na dużą skalę nazywane są kopalniami.

Dokonywanie transakcji bitcoinem nie wymaga uruchamiania węzła sieci. Aby sprawdzić realizację płatności, wystarczy zweryfikować nagłówki najdłuższego bloku oraz gałąź drzewa bloku, w którym transakcja została zapisana ze znacznikiem czasu [11]. W praktyce w Internecie można sprawdzić aktualny stan dowolnego portfela podając jego adres (klucz publiczny). Podobnie przeprowadzanie transakcji wymaga jedynie znajomości adresu portfela odbiorcy i dostępu do własnego portfela lub portfeli (kluczy prywatnych). Dla zwiększenia efektywności sieci transakcje mogą być łączone, czyli można dokonać jednej płatności po części z kilku posiadanych portfeli i jednocześnie wskazać kolejny portfel do wydania reszty.

Bezpieczeństwo systemu opiera się na konieczności akceptacji bloków przez większą część sieci. Większa część jest tu rozumiana jako moc zaangażowanych w obliczenia koparek. Jeżeli większość akceptuje jedynie prawidłowe bloki, czyli nie pozwalające na podwójne wydatkowanie, to potencjalny atak na system polegałby na próbie szybszego wygenerowania dłuższego łańcucha niż łańcuch uczciwy. Nawet, gdyby się to udało atakujący mógłby co najwyżej potwierdzić podwójne wydanie własnych środków, ale nie miałby wpływu na środki innych posiadaczy.

Jeżeli prawdopodobieństwo znalezienia dowodu pracy przez atakującego jest mniejsze niż przez uczciwą część sieci, to z każdym kolejnym krokiem spada ono wykładniczo. Stąd przyjęcie, że wygenerowanie sześciu kolejnych bloków po transakcji upewnia ją. Dla skutecznego ataku pozwalającego na podwójne wydatkowanie środków trzeba by więc przejąć ponad połowę mocy obliczeniowej sieci. To z kolei byłoby nieuzasadnione ekonomicznie, bo dysponujący taką mocą mógłby znacznie więcej zarobić na emisji nowych monet niż na potencjalnym fałszerstwie.

2. Kryptowaluty

Upowszechnienie technologii blockchain nastąpiło wraz ze wzrostem zainteresowania bitcoinem. Stąd pierwszym jej zastosowaniem było tworzenie kryptowalut. Obecnie publicznie dostępnych jest już kilkaset kryptowalut. O ile ogólna idea ich działania jest podobna, to można je podzielić na kilka typów w zależności od szczegółów implementacji. Decydują one o możliwościach wykorzystania i specyficznych cechach poszczególnych walut.

Pojawienie się nowych kryptowalut wynikało z rozwoju technologii, po części z wad i ograniczeń samego bitcoina, chęci zysku oraz łatwości ich tworzenia. Do podstawowych wad bitcoina można zaliczyć brak natychmiastowych transakcji, okresowo wysokie koszty transakcyjne, energochłonność wydobycia i wynikający stąd wpływ na środowisko naturalne oraz podatność na dużą koncentrację wydobycia.

Czas realizacji transakcji w sieci bitcoin wynosi około godziny. Eliminuje go to praktycznie jako walutę do płatności w placówkach handlowych czy usługowych. Nie nadaje się również do mikropłatności w Internecie, gdzie oczekiwane jest natychmiastowe rozliczenie. Pod koniec 2017 roku w czasie hossy na rynku kryptowalut transakcje trwały znacznie dłużej, można je było przyspieszyć deklarując wyższą opłatę transakcyjną. W tym czasie szybka transakcja mogła kosztować nawet kilkadziesiąt złotych.

Wzrost kursu bitcoina spowodował znaczący przyrost chętnych do jego wydobycia. Ponieważ algorytm skaluje trudność tak, aby bloki powstawały równomiernie, to globalny wzrost mocy koparek jest samonakręcającym się mechanizmem. Biorąc pod uwagę dane z maja 2018 roku globalne roczne zapotrzebowanie sieci bitcoin na energię elektryczną wynosi ponad 64 TWh. Wartość tej energii przekracza trzy miliardy dolarów. To podobne zapotrzebowanie jak na przykład Czech. Tylko 41 krajów zużywa rocznie więcej energii elektrycznej [3].

Na podobnej zasadzie jak bitcoin działają inne wzorujące się na nim kryptowaluty pierwszej generacji. Różnią się szczegółami implementacji na przykład częstotliwością pojawiania nowych bloków, szybkością i kosztem transakcji, podatnością algorytmu na stosowanie specjalizowanych układów elektronicznych, podejściem do prywatności użytkowników itp. Przykładami mogą być litecoin (LTC) stawiający na szybkość i niski koszt transakcji czy monero (XMR) stawiające sobie za cel uniemożliwienie śledzenia transakcji konkretnego użytkownika. Założenia monero czynią go w szczególności środkiem płatniczym atrakcyjnym dla przeprowadzających nielegalne operacje.

Wspólną cechą wszystkich kryptowalut jest możliwość pełnienia funkcji pieniądza. W wypadku kryptowalut pierwszej generacji takich jak bitcoin właściwie jest to ich jedyna istotna funkcjonalność. Może być ona realizowana w inny niż tradycyjne sposoby, ale nadal jest to umowny pieniądz, którego wartość wynika z tego, że jest akceptowany oraz istnieją podaż i popyt na niego. Jednak obecnie, biorąc pod uwagę bardzo dużą zmienność kursów kryptowalut w stosunku do tradycyjnych walut, można stwierdzić, że ich głównym zastosowaniem jest spekulacja i w praktyce nie są używane jako środek płatniczy na istotną skalę.

Druga generacja kryptowalut zapewnia szersze wykorzystanie łańcucha bloków. Jej pierwszym przedstawicielem jest stworzony w 2015 roku ethereum. Autor rozwiązania V. Buterin określił sieć ethereum jako rozproszoną platformę inteligentnych kontraktów i aplikacji [1]. Zawartość bloków ethereum nie jest ograniczona jedynie do zapisu historii transakcji. Sieć pozwala na zapis skryptów, które mogą wykonywać dowolne obliczenia, przechowywać dowolne dane i sprawdzać różne warunki.

Skrypty ethereum to programy zapisane w specjalnie stworzonym do tego celu języku Solidity. Inteligentny kontrakt to przeważnie spis warunków określających co ma się wydarzyć, jeżeli zostaną one spełnione. Jeżeli kod kontraktu zostanie zapisany w łańcuchu bloków i zaakceptowany przez wszystkie strony to wykona się on automatycznie po spełnieniu zawartych w nim warunków. Co ważne, zapis w blockchain gwarantuje, że nie da się podmienić raz stworzonego programu. Propozycje stworzenia inteligentnych kontraktów pojawiały się już od dwudziestu lat [15], ale dopiero blockchain pozwolił na ich stosunkowo prostą implementację. Zostaną one omówione w kolejnym punkcie.

Możliwość zapisu dowolnych danych w blokach powoduje, że w wypadku kryptowalut drugiej generacji ich funkcja płatnicza może okazać się tylko cechą uboczną. Ich sieci mogą zostać użyte do zapisu danych o dowolnych aktywach, jak na przykład tradycyjne waluty, akcje, prawa do nieruchomości, certyfikaty posiadania dowolnych dóbr czy energii. Podobnie jak w wypadku bitcoina także ethereum znalazło wielu naśladowców realizujących podobne cele, ale różniących się szczegółami implementacji.

Przykładem kryptowaluty, która ma pełnić głównie funkcję usługową jest ripple (XRP). Celem jej twórców jest stworzenie globalnego protokołu komunikacyjnego dla banków i instytucji finansowych umożliwiającego dokonywanie natychmiastowych płatności międzynarodowych po minimalnych kosztach. Przelewy dotyczą tradycyjnych walut z możliwością ich automatycznej wymiany po najlepszym oferowanym kursie.

Transakcje w sieci RippleNet są zatwierdzane co cztery sekundy. Szybkość działania wynika przede wszystkim z zastosowania algorytmu konsensusu opartym na „dowodzie poprawności" (proof-of-correctness) [14]. Nie wymaga to wykonywania obliczeń, a jedynie uzgodnień pomiędzy węzłami sieci. Nie następuje tu wydobycie nowych monet – liczba ripple jest stała (wszystkie zostały wyemitowane równocześnie). Sieć jest scentralizowana, a kod używanych algorytmów nie jest jawny. Można więc stwierdzić, że jest to prywatny łańcuch bloków jednej organizacji, a nie publiczny.

Założeniem autorów rozwiązania jest konkurowanie z obecnie powszechnie używanym protokołem SWIFT, utrzymywanym przez organizację o takiej samej nazwie[1], będącym w użyciu od 1977 roku, który jest drogi, powolny i nie umożliwia przewalutowania, a ponadto ma niejasne zasady naliczania opłat dla klientów. Ripple ma w założeniach eliminacje wszystkich tych niedogodności. Pojawienie się ripple wymusiło powstanie rozszerzenia protokołu SWIFT poprawiającego niektóre aspekty jego działania. Dokładne porównanie możliwości ripple i modernizacji SWIFT jest dostępne w [18].

W odróżnieniu od innych kryptowalut do sieci RippleNet dołączają nie wszyscy uczestnicy wymiany a jedynie banki i instytucje finansowe. Nadawca i odbiorca przelewu wchodzą w interakcję jedynie ze swoimi bankami i nawet nie muszą wiedzieć w jaki sposób bank realizuje ich zlecenia. W kwietniu 2018 roku na szerszą skalę płatności międzynarodowe w oparciu o blockchain uruchomił Santander Bank dla swoich klientów w Polsce, Wielkiej Brytanii, Hiszpanii i Brazylii [19].

Podobne cele postawili sobie twórcy platformy Stellar używającej kryptowaluty lumen (XLM). Oferuje ona przechowywanie w łańcuchu informacji o dowolnych aktywach z możliwością ich transferu oraz dowolnej wymiany pomiędzy aktywami. Wymiany następują w sposób automatyczny po najlepszym możliwym kursie z możliwością wielokrotnych wymian pośrednich w wypadku braku możliwości bezpośredniej wymiany mniej popularnych aktywów. Sieć Stellar jest otwarta

[1] *SWIFT – Society for Worldwide Interbank Financial Telecommunication.*

i zdecentralizowana, używa własnego protokołu konsensusu [9]. Działa on podobnie do RippleNet, ale każdy może otworzyć własny węzeł sieci oraz zdecydować, które węzły traktuje jako zaufane.

Platforma Stellar jest już wykorzystywana komercyjnie. Usługi finansowe, w tym przelewy międzynarodowe na bazie Stellara, oferują już filipińska firma coins.ph i europejska Tempo. Tempo pozwala na międzynarodowe transfery pieniężne, zarówno online jak i offline poprzez sieć agentów, oferuje dostęp do ponad stu tysięcy punktów wypłat w 55 krajach. Firmy te używają technologii blockchain do stworzenia konkurencyjnych usług finansowych bazujących na tradycyjnych walutach. W tych przypadkach blockchain został użyty jako techniczny środek do osiągnięcia wymaganych własności usług. Natomiast same usługi nie są reklamowane jako bazujące na kryptowalutach, fakt użycia technologii blockchain nie jest w ich wypadku eksponowany.

Istotną cechą odróżniającą wszystkie kryptowaluty od tradycyjnych walut jest brak możliwości sterowania ich ilością na podstawie decyzji rządów czy banków centralnych. To w algorytmie jest już przewidziana liczba dostępnych w danym czasie jednostek i tempo ich przyrostu w czasie. Co więcej są to dane powszechnie dostępne.

3. Inteligentne kontrakty

Inteligentny kontrakt to uzgodnione wzajemne zobowiązania stron zapisane w postaci kodu komputerowego, oparte na założeniu, że gdy wystąpi zdarzenie X, to ma zostać wykonane działanie Y. Zdarzenie X może być wpisem w bazie blockchain np. przelanie kryptowaluty między portfelami użytkowników lub może być upływem jakiegoś terminu. W takich przypadkach wykonanie kontraktu nastąpi automatycznie.

Jeżeli zdarzenie X występuje w świecie fizycznym, np. dostarczenie towaru lub wykonanie usługi, wynik rozegranego meczu itp. to wykonanie kontraktu wymaga zaangażowania osoby trzeciej, która ma wprowadzić odpowiednie dane. Może to być osoba wyznaczona przez strony umowy lub, w niektórych przypadkach, zdecentralizowana usługa działająca w sieci blockchain.

Te cechy inteligentnych kontraktów powodują, że nie należy ich traktować jako zamiennika umów, ale raczej jako techniczny środek ich realizacji. Ponieważ odbywają się one w przestrzeni wirtualnej najlepiej sprawdzą się tam, gdzie całą transakcję można zrealizować w łańcuchu bloków, czyli w sposób niematerialny. Jeśli prawa do materialnych dóbr zostaną zapisane w łańcuch u bloków to wtedy cała transakcja może być zrealizowana poprzez wykonanie kontraktu.

Najważniejszą cechą inteligentnego kontraktu jest zabezpieczenie interesów obu stron transakcji w wypadku, gdyby jedna z nich nie wypełniła swojego zobowiązania. Jeśli kontrahenci dokonują wymiany dóbr, które mogą być reprezentowane cyfrowo to wystarczy, że kontrakt będzie zdefiniowany tak, że strony przekazują je nie sobie, ale do portfela kontraktu. Kontrakt działa tak, że dopiero, gdy obie strony przekażą swoje aktywa w uzgodnionym czasie, to zostaną one przekazane kontrahentom. Jeśli w zadanym czasie jedna ze stron nie wykona zobowiązania, to kontrakt zwróci drugiej stronie jej aktywa.

Jedną z możliwości inteligentnych kontraktów jest emisja tokenów, które mogą reprezentować dowolne aktywa. Emisja tokenów jest o wiele łatwiejsza od stworzenia nowej kryptowaluty, nie wymaga tworzenia nowego łańcucha bloków, a jedynie dopasowania się do standardów sieci w obrębie której są one emitowane. Dla sieci ethereum powstał standard ERC-20, który definiuje wspólne cechy tokenów i ułatwia jednolite zarządzanie nimi. Tak stworzonymi tokenami można natychmiast handlować. Mogą być one traktowane jako kolejne kryptowaluty lub jako udziały w przedsięwzięciach. W maju 2018 roku było ponad 500 rodzajów tokenów w tym standardzie.

Często tokeny są używane jako sposób na publiczne zebranie funduszy. Tak zwane ICO (Initial Coin Offering) zwykle są przeprowadzane przez firmy czy organizacje chcące realizować projekty związane z technologią blockchain. W odróżnieniu od publicznych ofert akcji są one przeprowadzane praktycznie bez nadzoru regulatorów rynku, emitent nie musi spełniać żadnych wymogów formalnych. ICO zwykle trwają krótko i są dostępne globalnie dla wszystkich zainteresowanych. Potencjalnym zyskiem nabywcy jest wzrost wartości tokenów, gdy finansowany projekt odniesie sukces rynkowy. Zwyczajowo przyjęte jest, że plany emitenta przedstawiane są w dokumencie „whitepaper", którego zawartość nie jest jednak standaryzowana. Fundusze mogą być zbierane zarówno na rozwój już działającego projektu jak i w fazie samej koncepcji.

Powyższe cechy ICO powodują, że są to inwestycje obarczone bardzo wysokim ryzykiem, ale równocześnie o potencjalnie bardzo dużej stopie zwrotu. Ryzyko wynika nie tylko z faktu, że finansowany projekt może się nie udać, ale również z braku pewnych wiadomości na temat oferenta. Znaczna część ofert to zwykłe oszustwa – emitenci nie planują realizacji czegokolwiek poza zebraniem funduszy. Wśród projektów rzeczywiście zrealizowanych, które przyniosły zyski rzędu kilkuset tysięcy procent są między innymi samo ethereum – na jego przygotowanie zebrano w 2014 roku 16 milionów dolarów, a także kryptowaluty IOTA, NEO. Wartość funduszy zgromadzonych poprzez ICO wyniosła w 2017 roku ponad 5 miliardów dolarów, a w pierwszym kwartale 2018 roku przekroczyła już 6 miliardów dolarów [6].

4. Blockchain jako rejestr

Łańcucha bloków, w sposób naturalny, pozwala stworzyć rozproszoną księgę główną. Staje się dobrym narzędziem do przechowywania wszelkiego rodzaju rejestrów, w których nie będzie możliwa podmiana raz zapisanych danych. Typowymi przykładami mogą być księgi wieczyste, baza aktów notarialnych, rejestry umów, księgi handlowe, zeznania podatkowe itp.

Korzyści z prowadzenia rejestrów w tej formie to rozproszenie bazy danych, możliwość szybkiego autoryzowanego dostępu do nich oraz możliwość automatyzacji transakcji przy pomocy inteligentnych kontraktów. Łatwym do wyobrażenia przykładem byłaby sprzedaż nieruchomości, w wypadku, gdyby księga wieczysta była zapisywana w łańcuchu bloków, a płatność nastąpiła kryptowalutą lub tokenami reprezentującymi wybraną walutę. W takim wypadku kontrakt mógłby zastąpić notariusza i zabezpieczyć obie strony transakcji.

Kontrakty mogą być również sposobem wynagradzania twórców z tytułu praw autorskich do zasobów dostępnych w sieci. Pobranie materiałów obciążą pobierającego i automatycznie proporcjonalnie wynagradza autorów treści. Taki system ułatwiłby również sprzedaż majątkowych praw autorskich.

Kolejnym zastosowaniem może być potwierdzanie autorstwa i czasu powstania dokumentu. Zapisanie jego sygnatury wraz z identyfikatorem autora w łańcuchu bloków dawałoby dowód istnienia i posiadania go przez dokonującego wpis w danym czasie. Oczywiście może to dotyczyć dowolnych cyfrowych dokumentów w tym zdjęć, filmów, powieści, nagrań muzycznych itp. To mogłoby ułatwić dowodzenia praw autorskich czy pierwszeństwa wniosków patentowych. Podobnie można zabezpieczyć autentyczność danych medycznych.

Blockchain pozwala na wdrożenie systemu współdzielenia zasobów między stronami nie mającymi do siebie pełnego zaufania. Jedne z największych funduszy w ramach ICO (ponad 250 milionów dolarów) zebrali twórcy opartej na łańcuchu bloków sieci Filecoin, która ma służyć do

przechowywania danych na niewykorzystanych powierzchniach dysków. Posiadacze wolnej przestrzeni dyskowej będą wynajmować ją w atrakcyjnych cenach. Użytkownik będzie deklarował, ile danych chce zapisać, a posiadacze wolnej przestrzeni będą licytować stawkę, po której przyjmą dane. Wgrywany plik będzie szyfrowany i dzielony na mniejsze fragmenty rozsyłane do różnych lokalizacji [5].

Śledzenie łańcucha dostaw towarów ma znaczenie dla wielu branż na przykład farmaceutycznej, kosmetycznej, żywności [17], elektroniki. Połączenie wykorzystania czujników IoT z zapisem przemieszczania towarów wraz z oznaczeniem czasu oraz transakcji w sieci blockchain pozwoli na eliminację wielu nadużyć podczas dystrybucji materiałów i towarów. Zastosowanie śledzenia pochodzenia towaru w całym procesie dystrybucji daje możliwość weryfikacji pełnej historii towaru na podstawie numeru jego partii produkcyjnej. Amerykańska sieć Walmart we współpracy z firmą IBM i Uniwersytetem Tsinghua założyły Blockchain Food Safety Alliance, którego celem jest stworzenie systemu do śledzenia chińskiej żywności w całym procesie dystrybucji. Pilotaż obejmuje dostawy mango i wieprzowiny importowanej z Chin do sklepów Walmart w USA [7].

W Polsce bank PKO BP planuje wdrożenie technologii blockchain w celu weryfikacji autentyczności dokumentów bankowych. Każdy dokument zapisany w sieci blockchain (np. potwierdzenie transakcji lub regulamin bankowy) zostanie wystawiony w formie nieodwracalnego skrótu podpisanego kluczem prywatnym banku. Pozwoli to klientowi na zdalne sprawdzenie czy plik, który otrzymał od kontrahenta lub banku, jest prawdziwy i czy nie doszło do próby jego modyfikacji. Początkowo weryfikowane będą taryfy i regulaminy dla klientów. Według przepisów unijnych autentyczności dokumentacji bankowej nie spełniają np. mailingi a blockchain może ją zapewnić. Obniży to koszty komunikacji z klientami [12].

Sama technologia nie stawia wymogu, aby łańcuch bloków był publiczny. Można stworzyć prywatny blockchain czego przykładem jest ripple. Technologię może również wykorzystać administracja państwowa tworząc własne sieci z autoryzowanymi węzłami. Dubaj planuje do 2020 roku wyeliminować papierowe dokumenty i realizować wszystkie rządowe transakcje w sieci blockchain. Ponad sto milionów dokumentów rocznie będzie tworzonych tylko cyfrowo. Ma to zmniejszyć emisję dwutlenku węgla o 114 megaton oraz oszczędzić 25 milionów godzin czasu przetwarzania dokumentów [16].

Krajem, w którym najpełniej jest realizowana wizja cyfrowego społeczeństwa jest Estonia. Wszystkie sprawy urzędowe poza małżeństwem, rozwodem i zakupem nieruchomości można tam zrealizować wirtualnie. Można głosować on-line, w wyborach parlamentarnych w 2015 roku skorzystało z tego ponad 30% wyborców. W Estonii używa się więcej cyfrowych podpisów niż w całej reszcie Unii Europejskiej. Cyfryzacja obejmuje również sektor edukacji oraz służby zdrowia. Lekarz w razie potrzeby ma dostęp do cyfrowej historii pacjenta, w razie wypadku obsługa karetki może na podstawie dokumentu poszkodowanego uzyskać natychmiastowy dostęp do jego danych medycznych. Te dane są zapisywane z użyciem technologii blockchain co zapewnia ich niezmienność [4].

5. Podsumowanie

Technologia blockchain powstała w celu wprowadzenia pierwszej kryptowaluty – bitcoina. Jej pierwsze zastosowania to tworzenie kolejnych kryptowalut. Te pierwszej generacji miały pełnić głównie funkcję środka płatniczego. Nowsze pozwoliły na stworzenie inteligentnych kontraktów, przechowywanie dowolnych informacji, współdzielenie zasobów, dokonywanie transakcji z użyciem tradycyjnych aktywów oraz prowadzenie rozproszonych rejestrów dowolnego typu.

W praktyce żadna z kryptowalut nie stała się walutą używaną do dokonywania transakcji na istotną skalę. Wynika to po części z braku uregulowań prawnych, niskiej świadomości społecznej, dużej zmienności kursów jak i wygody użycia. Obrót nimi ma charakter głownie spekulacyjny. Każda z kryptowalut tworzy własną sieć blockchain, te drugiej generacji oferują często funkcjonalności istotniejsze od funkcji płatniczej. Wycena danej kryptowaluty może w znacznej części wynikać z oceny jej innowacyjności przez inwestorów – kryptowaluta staje się bardziej substytutem udziału w przedsięwzięciu niż środkiem płatniczym.

Technologia blockchain jest już dziś używana do realizacji szybkich i tanich przelewów międzynarodowych, pozyskiwania funduszy na nowe przedsięwzięcia z pominięciem regulatorów rynku, śledzenia dostaw towarów oraz tworzenia rozproszonych rejestrów zarówno publicznych jak i prywatnych.

Bibliografia

[1] Buterin V, *A next-generation smart contract and decentralized application platform*, *https://github.com/ethereum/wiki/wiki/White-Paper*, 2014.
[2] CoinMarketCap, *źródło: https://coinmarketcap.com,* dostęp: [2018.05.30].
[3] Digiconomist.com, *Bitcoin Energy Consumption Index, źródło: https://digiconomist.net /bitcoin-energy-consumption,* dostęp: [2018.05.30].
[4] e-Estonia, *źródło: https://e-estonia.com,* dostęp: [2018.05.30].
[5] *Filecoin: A Decentralized Storage Network,* Filecoin.io, 2018.
[6] Floyd D., *$6.3 Billion: 2018 ICO Funding Has Passed 2017's Total, źródło: https://www.coindesk.com/6-3-billion-2018-ico-funding-already-outpaced-2017/,* dostęp: [2018.05.30].
[7] Galvin D., *IBM and Walmart: Blockchain for Food Safety.* IBM Corporartion, 2017.
[8] Hulicki M., Lustofin P., *Wykorzystanie koncepcji blockchain w realizacji zobowiązań umownych.* [w:] *Człowiek w cyberprzestrzeni (1), s. 28–53*, 2017.
[9] Mazieres D., *The stellar consensus protocol: a federated model for internet-level consensus.* Stellar Development Foundation 2015.
[10] Merkle R. C., *Protocols for public key cryptosystems*. [w:] *Security and Privacy, 1980 IEEE Symposium on*. IEEE, 1980.
[11] Nakamoto S., *Bitcoin: A peer-to-peer electronic cash system*, https://bitcoin.org/bitcoin.pdf, Bitcoin.org, 2008.
[12] PKO BP, *Technologia blockchain ułatwi weryfikację dokumentów bankowych, komunikat prasowy,* 2018.
[13] Prabucki R., *Kryptologia a prawo – wybrane zagadnienia: idea kryptowaluty i jej wpływu na ewolucję oszustw w internecie.* [w:] *Przegląd Nauk Stosowanych Nr 10,* 2016.

[14] Schwartz D., Youngs N., Britto A., *The Ripple protocol consensus algorithm.* Ripple Labs Inc White Paper, 2014.
[15] Szabo N., *Formalizing and securing relationships on public networks*. [w:] *First Monday 2(9)*, http://ojphi.org/ojs/index.php/fm/article/view/548, 1997.
[16] Smart Dubai, źródło: ttps://smartdubai.ae/en/Initiatives/Pages/DubaiBlockchain Strategy.aspx/, dostęp: [2018.05.30].
[17] Tian F. *An agri-food supply chain traceability system for China based on RFID & blockchain technology.* [w:] *Service Systems and Service Management (ICSSSM), 2016 13th International Conference on.* IEEE, 2016.
[18] Treasury Today, *źródło: http://treasurytoday.com/2017/07/ripple-vs-swift-payment-r-evolution-ttpv,* dostęp: [2018.05.30].
[19] Zuckerman M. J., Santander: *We'll Launch Int'l Payment App With Ripple This Spring If No One Beats Us To It, źródło: https://cointelegraph.com/news/santander-well-launch-intl-payment-app-with-ripple-this-spring-if-no-one-beats-us-to-it,* dostęp: [2018.05.30].

POSSIBLE APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

Summary

The blockchain technology, originally used to create the first cryptocurrency, bitcoin, has been growing dynamically in the last few years. Its basic assumption is the use of computer networks and algorithms to ensure the credibility of the originality and the time of information transfer between the parties who have no confidence in each other. This eliminates the need for a trusted third party to authorize transactions or conclude contracts. It allows to create intelligent contracts that are executed automatically after meeting the planned conditions. It allows everyone to issue his own currency. The article discusses the assumptions and operations of the blockchain by an example of bitcoin. It shows the application of technologies concerning, among others, cryptocurrencies, international transfers, fundraising, tracking deliveries, distributed ledger.

Keywords: blockchain, cryptocurrencies, Bitcoin, Ethereum, hash functions, smart contracts, distributed ledger, ICO (initial coin offering)

Publikacja została sfinansowana ze środków przyznanych Wydziałowi Zarządzania Uniwersytetu Ekonomicznego w Krakowie, w ramach dotacji na utrzymanie potencjału badawczego.

Artur Żuwała
Katedra Informatyki
Wydział Zarządzania
Uniwersytet Ekonomiczny w Krakowie
ul. Rakowicka 27, 31-510 Kraków
e-mail: artur.zuwala@uek.krakow.pl