STUDIA I ARTYKUŁY

BARTŁOMIEJ KLINGER[1]
JACEK SZCZEPAŃSKI[2]

BLOCKCHAIN - HISTORIA, CECHY I GŁÓWNE OBSZARY ZASTOSOWAŃ

STRESZCZENIE:

Technologia blockchain jest uznawana za jedną z przełomowych technologii informatycznych naszych czasów. Ponad 8 letnia już historia tej technologii łączy się nierozerwalnie z historią cyfrowej waluty Bitcoin, stworzonej przez tajemniczego Satoshi Nakamoto. Od czasu, gdy pierwsi użytkownicy podłączyli się do sieci Bitcoin, nastąpiła ewolucja w postrzeganiu samej technologii blockchain jako technologii bazowej, dającej się zastosować nie tylko do tworzenia innych niż Bitcoin kryptowalut. Istotne było także pojawienie się niezależnej od Bitcoin sieci blockchain nazwanej Ethereum, zaprojektowanej przez 19 letniego Vitalika Buterina, która zaoferowała nowe możliwości funkcjonalne - inteligentne kontrakty. Blockchain jaki znamy dzisiaj bardzo intensywnie i skutecznie wykorzystuje znane koncepty kryptograficzne takie jak jednokierunkowe funkcje haszujące, kryptografię asymetryczną czy znakowanie czasem. Mechanizmy konsensusu zawieranego automatycznie przez uczestników sieci blockchain eliminują potrzebę zaufanej trzeciej strony przy przetwarzaniu transakcji, a inteligentne kontrakty poszerzyły obszar zastosowań technologii blockchain daleko poza transfer kryptowalut. Przedsiębiorstwa i instytucje na całym świecie dostrzegły innowacyjny potencjał wynikający z unikalnych cech technologii blockchain i dzisiaj są już na etapie usprawniania swoich procesów z wykorzystaniem tej technologii. Przytoczone przykłady zastosowań realnie wpływają także na poprawę jakości życia zwykłych ludzi.

[1] CEO i lider zespołu Positiverse, doświadczony menedżer i kierownik projektów informatycznych. Od ponad 15 lat realizuje projekty konsultingowe, wytwórcze, wdrożeniowe i utrzymaniowe o zasięgu ogólnokrajowym oraz europejskim. Entuzjasta technologii blockchain oraz nowoczesnych rozwiązań z obszaru biometrii i kryptografii.
[2] CTO Postiverse, doświadczony architekt rozwiązań IT i praktyk Agile z bardzo silnymi kompetencjami z inżynierii oprogramowania. Realizował różnorodne projekty dla sektora finansów, telekomunikacji, branży ubezpieczeniowej i wielu instytucji publicznych. Entuzjasta nowoczesnych rozwiązań i trendów IT w szczególności technologii blockchain.

SŁOWA KLUCZOWE:

Technologia blockchain, funkcja haszująca, kryptografia asymetryczna, znakowanie czasem, mechanizm konsensusu, inteligentne kontrakty, zastosowania blockchain, łańcuch dostaw, identyfikacja, potwierdzanie autentyczności, zarządzanie tożsamością, prawa własności, FinTech, crowdfunding, głosowanie elektroniczne

***

1. GENEZA

Historia powstania technologii blockchain łączy się nierozerwalnie z historią cyfrowej waluty znanej jako Bitcoin oraz z postacią jej twórcy, tajemniczego Satoshi Nakamoto. Aż trudno uwierzyć, że prawdziwa tożsamość wynalazcy jednej z najbardziej rewolucyjnych technologii naszych czasów pozostaje ciągle nieznana, pomimo że osoba ta (lub osoby) ukryta pod pseudonimem, aktywnie współuczestniczyła przez ponad 2 lata przy rozwijaniu kodu źródłowego oprogramowania Bitcoin.

Trudno stwierdzić dokładnie od kiedy tajemniczy Satoshi Nakamoto pracował nad koncepcją i rozwiązaniami technicznymi Bitcoin. Pojawia się na ten temat wiele spekulacji i domysłów, a sam Nakamoto w jednym ze swoich postów[3], publikowanych na grupie dyskusyjnej dotyczącej kryptografii sugeruje, że już w 2007 roku opracowywał elementy rozwiązania. Zdarzeniem, które jest uznawane za zapowiedź powstania sieci Bitcoin było zarejestrowanie 18 sierpnia 2008 r. domeny internetowej bitcoin.org. Rejestracja odbyła się co prawda poprzez serwis anonymousspeech.com umożliwiający anonimową rejestrację domen, ale powszechnie uznaje się, że pierwszym właścicielem domeny był sam Satoshi. Kluczowym momentem w historii Bitcoin, który pokazał światu technologię blockchain było opublikowanie 31 października 2008 roku przez Nakamoto dokumentu (tzw. white paper) pod tytułem: "Bitcoin: A Peer-to-Peer Electronic Cash System"[4].

Kolejne wydarzenia potoczyły się dość szybko. Po zarejestrowaniu 9 listopada 2008 r. projektu o nazwie Bitcoin w serwisie SourceForge.net[5], już 3 stycznia 2009 r. inicjalny blok

[3] http://satoshi.nakamotoinstitute.org/emails/cryptography/15/ [dostęp: 28.05.2017].
[4] https://bitcoin.org/bitcoin.pdf [dostęp: 28.05.2017].
[5] SourceForge.net to darmowy system zarządzania i kontroli projektów Open Source, pozwalający m.in. na przechowywanie i wersjonowanie kodu źródłowego tych projektów oraz udostępnianie tego kodu każdemu zainteresowanemu.

Bitcoin (tzw. Genesis Block) został wygenerowany ("wykopany"). Następnie 9 stycznia wydana została pierwsza stabilnie działająca wersja oprogramowania Bitcoin oznaczona jako 0.1, a 12 stycznia wykonana została pierwsza transakcja przesłania kryptowaluty: 10 Bitcoinów (Satoshi wysłał je do Hala Finneya - znanego aktywisty w środowisku kryptografów). Tak rozpoczęła się ponad 8-letnia już historia Bitcoin i samej technologii blockchain, która jest rozpoznawana jako rewolucja na miarę uruchomienia globalnej sieci Internet. Do dzisiaj wokół sieci Bitcoin wydarzyło się wiele i przytaczanie wszystkich tych zdarzeń, nierzadko niewyobrażalnych z dzisiejszej perspektywy (jak choćby zapłacenie 10000 Bitcoinów za jedną pizzę), przekracza ramy niniejszego artykułu. Jest to jednak historia na tyle ciekawa, że bez wątpienia warto się z nią choćby ogólnie zapoznać.

Istotne do odnotowania są także zdarzenia związane z ewolucją postrzegania samej technologii blockchain jako technologii bazowej, dającej się zastosować nie tylko do tworzenia innych niż Bitcoin kryptowalut. Jednym z takich zdarzeń było bez wątpienia pojawienie się zupełnie nowej, niezależnej od Bitcoin sieci blockchain nazwanej Ethereum. Tym razem twórca jest znany. Jest nim 23 letni dzisiaj Vitalik Buterin, który w wieku 6 lat wyemigrował z rodziną z Rosji do Kanady, gdzie jako utalentowany matematyk i programista osiągał znaczne sukcesy już jako nastolatek (np. brązowy medal na Międzynarodowej Olimpiadzie Informatycznej w 2012 r.[6]).

Vitalik swoją przygodę z kryptowalutami rozpoczął już w 2011 roku, kiedy to pierwszy raz zetknął się z Bitcoinem. Uczestnicząc od tamtego czasu aktywnie w społeczności rozwijającej oprogramowanie Bitcoin, pisząc artykuły o Bitcoin oraz współtworząc jedno z pierwszych czasopism poświęconych tematyce kryptowalut (Bitcoin Magazine) stał się ekspertem w dziedzinie kryptowalut i technologii blockchain. W 2013 roku mając 19 lat porzucił studia i zaczął podróżować po świecie, biorąc udział w tworzeniu otwartego oprogramowania (open source) związanego z kryptowalutami. Efektem tych podróży i projektów był pomysł na zupełnie nowy rodzaj sieci blockchain opisany przez Buterina pod koniec 2013 roku[7]. Na podstawie opisanej koncepcji 23 stycznia 2014 roku Vitalik ogłosił uruchomienie projektu Ethereum i rozpoczęło się tworzenie oprogramowania nowej sieci blockchain, która miała oferować nowe możliwości funkcjonalne niedostępne w Bitcoinie. Główną rewolucją funkcjonalną w Ethereum była możliwość "programowania" w blockchain,

[6] http://www.ioi2012.org/competition/results-2/ [dostęp: 28.05.2017]

[7] http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf [dostęp: 28.05.2017]

czyli możliwość użycia aplikacji/skryptów, wykonujących praktycznie dowolne obliczenia czy przechowujących dane, nazwanych "inteligentnymi kontraktami" ("smart contracts"), które po dołączeniu do blockchain pozostawały niezmienne i przez cały czas działały tak, jak je pierwotnie zaprogramowano. W zamyśle Vitalika sieć Ethereum miała stać się nie tylko rejestrem zapisującym transakcje kryptowalutowe, ale także "światowym komputerem" - platformą pozwalającą na tworzenie rozproszonych aplikacji korzystających z dobrodziejstw technologii blockchain, na której byłyby osadzone. Ostatecznie sieć Ethereum została uruchomiona 30 lipca 2015 r. i od tamtej pory jest rozwijana jako drugi co do wielkości, otwarty blockchain, którego obszar zastosowań wyszedł daleko poza transfer kryptowalut.

2. ISTOTA

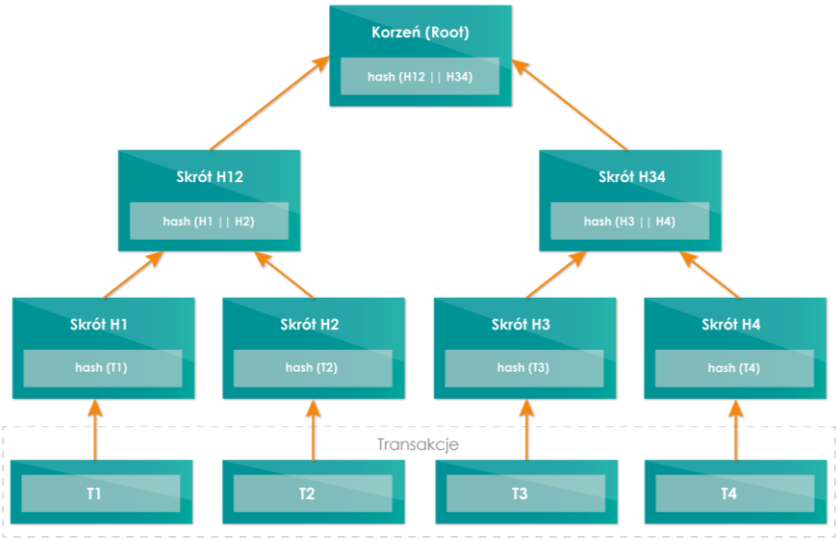
Bez wątpienia zarówno Bitcoin, jak i Ethereum są pierwowzorami dla innych rozwiązań, które obecnie intensywnie się rozwijają i dalej ewoluują. Poznanie podstawowych mechanizmów działania obu tych sieci pozwala zrozumieć także pozostałe współczesne rozwiązania określane jako technologie blockchain czy szerzej technologie rozproszonych rejestrów.

2.1. Blockchain bardzo intensywnie i skutecznie wykorzystuje znane koncepty kryptograficzne. Pierwszym z nich jest tworzenie unikalnych i jednoznacznych "odcisków" danych za pomocą jednokierunkowych funkcji skrótu (tzw. funkcji haszujących). Są to funkcje znane i wykorzystywane w informatyce już od ponad 27 lat[8], a ich działanie polega na wyliczaniu krótkiej sygnatury (tzw. "skrót", ang. "hash") dla podanych danych wejściowych. Mając na wejściu dowolny dokument, zdjęcie czy inne informacje w postaci cyfrowej, a nawet całe ogromne zbiory danych, możemy za pomocą funkcji haszującej wyliczyć "skrót" tych danych, który będzie:

- odporny na kolizje - dwa różne zestawy danych nie dadzą tego samego skrótu i nie ma praktycznej możliwości wygenerowania zestawu danych o takim samym skrócie jak wskazany zestaw danych;
- jednokierunkowy, nieodwracalny - nie da się odtworzyć oryginalnej wiadomości znając jej skrót.

[8] Pierwsze wykorzystywane przez wiele lat algorytmy funkcji skrótu z rodziny "MD" pojawiły się już w 1989 r., a ich twórcą był Ronald Rivest (https://en.wikipedia.org/wiki/Ron_Rivest)

Obie te cechy skrótów danych wyliczonych za pomocą funkcji haszujących są w praktyce wykorzystywane do szybkiej identyfikacji danych cyfrowych i weryfikacji integralności tych danych. Chodzi o to, aby nawet najmniejsza zmiana w danych źródłowych, choćby zmiana jednego tylko bitu, powodowała, że wyliczony hash różni się od skrótu danych źródłowych. Ten podstawowy mechanizm kryptograficzny działający na pojedynczej porcji danych może być wykorzystywany wielokrokowo do zapewniania integralności całych zestawów danych, dla których skróty poszczególnych składowych zestawu są wyliczane niezależnie, a następnie obliczając hierarchicznie skróty skrótów uzyskujemy na końcu jeden hash identyfikujący cały zestaw danych. Właśnie takie podejście jest wykorzystywane w blockchain, gdzie poszczególne transakcje są hashowane oddzielnie, a cały zestaw transakcji zapakowany w dany blok jest odwzorowany za pomocą drzewa skrótów (wynalezione w 1979 roku przez Ralpha Merkle[9]) pozwalającego zidentyfikować nie tylko podmianę danych w pojedynczej transakcji, ale także jakąkolwiek próbę wymiany całej transakcji na inną. Schemat powstawania drzewa skrótów najlepiej zobrazować na diagramie:



2.2. Drugim ważnym składnikiem technologii blockchain jest kryptografia asymetryczna pozwalająca zabezpieczyć wymianę informacji, czy wręcz zaszyfrować informacje wymieniane między dwiema stronami, bez konieczności uzgadniania przez te strony jednego wspólnego klucza zabezpieczającego. Kryptografia asymetryczna jest wykorzystywana przez każdego z nas, gdy otwieramy zabezpieczoną przez SSL stronę internetową (HTTPS), czy też podpisujemy cyfrowo pocztę lub dokumenty

[9] https://pl.wikipedia.org/wiki/Drzewo_hash [dostęp: 28.05.2017]

elektroniczne. Certyfikaty i podpisy cyfrowe bazujące na tym rodzaju kryptografii są dzisiaj powszechnie używane i można bez najmniejszego problemu znaleźć dowolnie szczegółowe informacje na ich temat. Warto poznać różnice między tymi powszechnie znanymi nam rozwiązaniami, a wykorzystaniem mechanizmu kryptografii asymetrycznej w ramach technologii blockchain. Przede wszystkim kryptografia asymetryczna w blockchain jest wykorzystywana przy każdej transakcji, jest to podstawa funkcjonowania blockchain. Każdy uczestnik sieci blockchain wchodząc w interakcję z innymi uczestnikami sieci posługuje się za każdym razem swoim kluczem prywatnym do podpisywania wysyłanych przez siebie transakcji oraz kluczami publicznymi adresatów tych transakcji. Ponadto w publicznych sieciach blockchain takich jak Bitcoin czy Ethereum nie ma "certyfikacji kluczy" użytkowników sieci, każdy może wygenerować sobie swoją parę kluczy i od razu stać się pełnoprawnym uczestnikiem wymiany dóbr w ramach wybranej sieci blockchain.

2.3. Trzecim elementem ze świata kryptografii zaadaptowanym przez technologię blockchain jest znakowanie czasem. Czas w sieci blockchain jest synchronizowany między uczestnikami sieci (węzłami), zarówno transakcje, jak i same bloki są znakowane czasem. Dzięki temu wszystkie obiekty i zdarzenia w blockchain są bardzo precyzyjnie umieszczone na zsynchronizowanej osi czasu i razem tworzą wiarygodną, ułożoną chronologicznie historię.

2.4. Kolejnymi filarami zapewniającym unikalne cechy funkcjonalne blockchain są mechanizmy konsensusu i inteligentne kontrakty (smart contracts).

Mechanizm konsensusu to w dużym skrócie mechanizm zatwierdzania transakcji i dołączania nowych bloków do łańcucha, wykonywany przez oprogramowanie węzłów sieci blockchain. W tradycyjnych rozwiązaniach, aby potwierdzić zajście pewnych zdarzeń (zatwierdzić transakcje) konieczne jest ustanowienie zaufanej trzeciej strony, która gromadzi wszelkie dane pozwalające jej rozstrzygać, która wersja zdarzeń przedstawiona przez uczestników danego procesu zostanie uznana za obowiązującą. W blockchain potrzeba takiej zaufanej trzeciej strony została wyeliminowana i zastąpiona uzgodnieniem dokonywanym automatycznie pomiędzy węzłami sieci, nazywanym właśnie konsensusem. Spotykamy dwa główne typy mechanizmów konsensusu. Pierwszy to tzw. "konsensus Nakamoto" polegający na przeprowadzeniu dla każdego nowego bloku pewnego rodzaju loterii i wyborze węzła-lidera, który będzie mógł zaproponować nowy blok przeznaczony do dołączenia do łańcucha, a po zatwierdzeniu tego bloku przez inne węzły uzyskać wynagrodzenie za dodanie tego bloku.

Najbardziej znaną implementacją konsensusu tego typu jest tzw. "dowód pracy" (proof-of-work) wykorzystywany w Bitcoin czy Ethereum. Drugi typ konsensusu bazuje na klasycznym algorytmie bizantyjskich generałów wykorzystywanym w sieciach rozproszonych i polega na wykonywaniu przez węzły sieci rund głosowań w celu uzyskania konsensusu[10]. Konsensus tego typu wykorzystywany jest bardzo często w zamkniętych sieciach blockchain, nie stosujących zachęt ekonomicznych dla węzłów dołączających się do sieci.

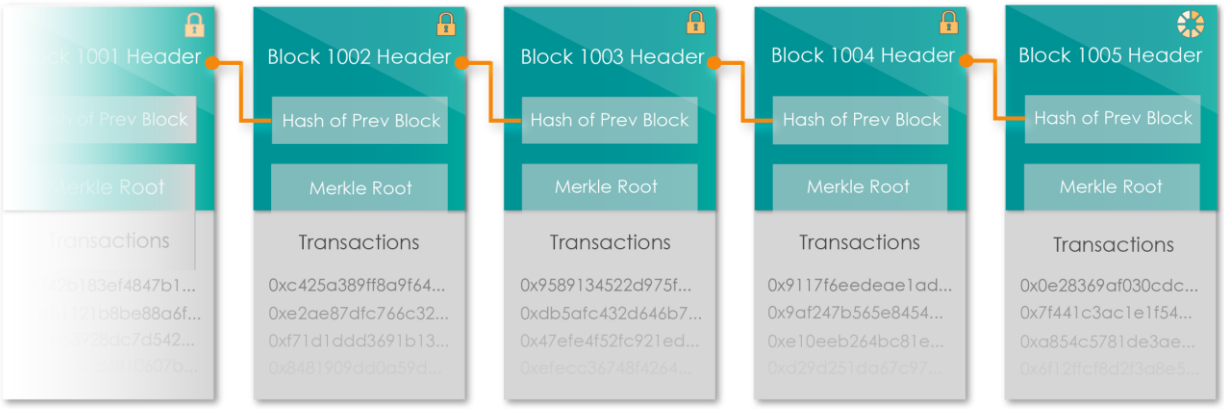
Inteligentne kontrakty, najczęściej określane ich oryginalną angielską nazwą "smart contracts", zostały koncepcyjne opisane już ponad 20 lat temu przez kryptografa Nicka Szabo[11].

Realizację koncepcji opracowanej przez Szabo możemy odnaleźć w bardzo ograniczonej formie już w sieci Bitcoin, jednak dopiero Vitalik Buterin wdrożył w pełni ten koncept w sieci Ethereum, której funkcjonalną esencją są właśnie inteligentne kontrakty. Te wyspecjalizowane programy, rezydujące w sieci blockchain jako autonomiczni agenci, odpowiadają za wykonywanie podczas przetwarzania transakcji dodatkowych operacji zapisanych w ich kodzie programistycznym. Dzięki inteligentnym kontraktom sieć blockchain uzyskuje dodatkowe możliwości funkcjonalne, pozwalające na dużo bardziej skomplikowane przetwarzanie niż tylko transfer podstawowej kryptowaluty danej sieci. Smart contract może zarówno definiować zupełnie nowe, nieznane wcześniej kryptowaluty o praktycznie dowolnych funkcjonalnościach, ale może także stać się nośnikiem czy składnicą niefinansowych walorów cyfrowych oraz cyfrowej reprezentacji wartości materialnych. Taka elastyczna funkcjonalność sieci blockchain uzyskana dzięki inteligentnym kontraktom jest dzisiaj wielką obietnicą zupełnie nowych, prawdziwie innowacyjnych rozwiązań budowanych w oparciu o blockchain.

Zarówno mechanizmy konsensusu, jak i inteligentne kontrakty są to zagadnienia na tyle obszerne i zarazem interesujące, że bez wątpienia zasługują na oddzielne i bardziej wnikliwe opracowania, które znajdą się w kolejnych numerach kwartalnika „Człowiek w Cyberprzestrzeni".

2.5. Łącząc opisane do tej pory składowe: funkcje haszujące, drzewa skrótów, kryptografię asymetryczną, znakowanie czasem, mechanizm konsensusu i inteligentne kontrakty w jedną całość otrzymujemy technologię blockchain jaką znamy obecnie.

[10] https://pl.wikipedia.org/wiki/Problem_bizantyjskich_genera%C5%82%C3%B3w [dostęp: 28.05.2017]
[11] https://en.wikipedia.org/wiki/Nick_Szabo [dostęp: 28.05.2017]



Przed zagłębieniem się w konkretne przypadki użycia blockchain istotne jest, aby uświadomić sobie, że systemy oparte o tą technologię tworzą niezmienne, znakowane czasem wpisy w rozproszonej bazie danych dla każdej kiedykolwiek wykonanej, pojedynczej transakcji. Dzięki temu każda transakcja i odpowiadający jej rekord danych są łatwo i jednoznacznie identyfikowalne. Ta rozproszona baza danych nie ma wyróżnionego węzła centralnego, ani żadnego "super administratora", dzięki czemu blockchain nie posiada pojedynczego punktu awarii. Dodatkowo mechanizm konsensusu i nieustannie prowadzona przez węzły weryfikacja zapisów zabezpiecza system transakcyjny przed podwójnym użyciem tego samego tokena/kryptowaluty/waloru (double-spent[12]), dzięki czemu przeciwdziała oszustwom, nadużyciom oraz innym rodzajom manipulacji na danych transakcji.

Wychodząc od cech technologii blockchain i próbując zweryfikować, czy ta technologia ma szansę wpłynąć na poprawę jakości życia zwykłych ludzi, warto przyjrzeć się wybranym, realizowanym obecnie na świecie, projektom.

3. BLOCKCHAIN I ŁAŃCUCH DOSTAW TOWARÓW

Naturalnym użyciem tej technologii wydaje się być rejestrowanie różnych faktów i zdarzeń jako transakcji w blockchain. Większość z nas używa w codziennym funkcjonowaniu GPS (Global Positioning System) jako użytecznego sposobu nawigacji[13]. Przy założeniu, że dane o położeniu byłyby umieszczane w blockchain, otrzymalibyśmy niezaprzeczalny zapis naszej trasy. Nikt, od momentu zapisu, nie byłby w stanie zmodyfikować udostępnionego śladu geolokalizacji. Dzięki naturalnemu dla blockchain znakowaniu czasem otrzymujemy trasę

[12] https://en.wikipedia.org/wiki/Double-spending [dostęp: 28.05.2017]
[13] http://www.gps.gov/ [dostęp: 28.05.2017]

obiektu skorelowaną z czasem, w jakim odbywały się zapisy w punktach kontrolnych. Jeżeli tylko jesteśmy w stanie „oznakować" interesujący nas obiekt w sposób jednoznaczny, to otrzymujemy narzędzie do pewnego i wiarygodnego śledzenia przemieszczeń towarów. Śledzenie pochodzenia i przemieszczania w całym łańcuchu dostaw ma znaczącą rolę przy elementach o wysokiej wartości, takich jak towary luksusowe, farmaceutyki, kosmetyki czy elektronika. Za każdym razem, gdy element fizyczny zmienia położenie w czasie (np. poprzez zmianę kolejnych dostawców), token cyfrowy jest przenoszony równolegle tak, że prawdziwy łańcuch dostaw jest precyzyjnie odzwierciedlany przez łańcuch transakcji na poziomie blockchain. Pozwala to w znacznym stopniu ograniczyć nadużycia podczas procesów dystrybucyjnych oraz reagować praktycznie natychmiast po wykrytej anomalii.

Niezaprzeczalne śledzenie pochodzenia i trasy dla towarów to dopiero pierwszy i w miarę oczywisty przypadek użycia. Dla wielu towarów, takich jak żywność czy farmaceutyki, ważniejsze od samej trasy są warunki, w jakich były przewożone i nierzadko także wszelkie opóźnienia w trakcie transportu. Tutaj z pomocą przychodzi nam IoT[14] (Internet of Things). Dzięki czujnikom potrafiącym komunikować się z siecią Internet, a tym samym z blockchain, możemy dodatkowo mierzyć i rejestrować chociażby takie parametry jak temperatura czy wilgotność powietrza podczas transportu i takie pomiary również umieszczać wraz z lokalizacją punktów kontrolnych jako transakcje blockchain[15]. Zapisy mogą odbywać się autonomicznie, a zapisane wartości są niemodyfikowalne, co przy transparentności odczytu danych daje skuteczne narzędzie weryfikacji dla odbiorcy towaru i de facto klienta końcowego. Już dziś istnieją systemy działające w oparciu o opisany wyżej model, gdzie klient otrzymuje aplikację mobilną, dzięki której skanując kod kreskowy towaru w sklepie jest w stanie zweryfikować jego pochodzenie i prześledzić przebytą trasę oraz warunki, w jakich ten towar był transportowany. Stosując takie podejście dostawcy są w stanie zarówno zagwarantować wysoką jakość towaru, jak i przedstawić odbiorcy wiarygodne dowody zachowania wysokich standardów jakości w całym łańcuchu dostaw, a tym samym otrzymać odpowiednio wyższe wynagrodzenie za dostarczony towar. Dla przykładu, ryby dostarczane z Indonezji z konkretnych łowisk rybackich do ekskluzywnych angielskich restauracji uzyskują cenę kilkunastokrotnie wyższą właśnie dzięki udokumentowaniu w blockchain zarówno tego skąd dokładnie pochodzą, jak i samej trasy ich dostaw[16].

[14] https://en.wikipedia.org/wiki/Internet_of_things [dostęp: 28.05.2017]
[15] http://blulog.eu/pl/ [dostęp: 28.05.2017]
[16] https://www.provenance.org/tracking_tuna_on_the_blockchain [dostęp: 28.05.2017]

4. IDENTYFIKOWANIE I AUTENTYCZNOŚĆ DÓBR

Potwierdzona autentyczność towarów jest cechą, na której zależy wielu kontrahentom. Dobrym przykładem jest potwierdzanie pochodzenia w kontekście towarów luksusowych np. diamentów. Poznanie pochodzenia kamienia może powstrzymać oszustwa ubezpieczeniowe oraz odsiać prawdziwe diamenty od syntetycznych lub tych "krwawych", czy też pochodzących z obszarów objętych konfliktami zbrojnymi. Fałszowane świadectwa papierowe sprawiają, że pochodzenie diamentów jest bardzo trudne do zweryfikowania. W 2015 roku powstała inicjatywa stworzenia globalnego rejestru diamentów w oparciu o zapisy w blockchain. Wykorzystuje się ponad 40 własności kamieni, w tym kolor i przejrzystość, aby utworzyć identyfikator każdego diamentu. Informacje te stają się świadectwem chroniącym pochodzenie klejnotów, od kopalni do pierścionka. Firma Everledger dokonała digitalizacji ponad miliona diamentów i współpracuje z wieloma firmami, w tym np. z Barclays[17].

Nietrudno sobie wyobrazić, że potwierdzenie takiej cechy jak autentyczność staje się ważna nie tylko w odniesieniu do towarów rzadkich i wartościowych, ale dotyka praktycznie całego świata dóbr cyfrowych[18].

Wymiana tych dóbr, szczególnie w postaci cyfrowej, dzięki coraz silniej zintegrowanym systemom, staje się łatwa, powszechna i praktycznie niczym nieskrępowana, ale także narażona na manipulacje, fałszerstwa i cyberataki. W wielu sytuacjach istotną rolę odgrywa właśnie potwierdzenie autentyczności danych i dokumentów elektronicznych. Trend z wykorzystaniem niezaprzeczalnego potwierdzenia w blockchain widać nawet u takich gigantów informatycznych jak Microsoft. Niedawno firma wprowadziła dodatek do pakietu MS Office, który wykorzystuje sieci blockchain (Bitcoin oraz Ethereum) do zapisania identyfikatora dokumentu będącego jednokierunkowym skrótem tego dokumentu[19]. Identyfikator ten zapisany w blockchain pozwala odbiorcy tego dokumentu zweryfikować czy dokument jest autentyczny.

Łatwość użycia i pewność zapisów powodują, że coraz więcej państwowych rejestrów i systemów obiegu dokumentów sięga po rozwiązania oparte o blockchain. Znamiennym przykładem jest nowa strategia dla Dubaju, która zakłada, że do 2020 roku wszystkie działania

[17] http://www.wired.co.uk/article/blockchain-conflict-diamonds-everledger [dostęp: 28.05.2017]
[18] https://stampery.com/ [dostęp: 28.05.2017]
[19] https://www.microsoft.com/reallifecode/2017/04/10/stampery-blockchain-add-microsoft-office/ [dostęp: 28.05.2017]

w ramach administracji państwowej rezygnują z używania papieru na rzecz dokumentów elektronicznych weryfikowanych w ramach sieci blockchain[20].

Władze Zjednoczonych Emiratów Arabskich są przekonane, że taka modernizacja da nie tylko realne oszczędności kosztów funkcjonowania administracji państwowej, ale przede wszystkim pozwoli na dużo efektywniejszą obsługę spraw obywateli i lepszy dostęp do usług publicznych.

5. BLOCKCHAIN W PRODUKCJI I DYSTRYBUCJI W ENERGETYCE

Nowe inicjatywy energetyczne, takie jak produkcja energii domowej i społeczna energia słoneczna, uzupełniają luki w dostawach energii elektrycznej na całym świecie. Coraz częściej słyszymy o tym, że pod względem energetycznym gospodarstwa domowe powinny stać się realnymi prosumentami, a nie tylko konsumentami, jak to ma obecnie miejsce. Prosument łączy w sobie zarówno konsumpcję energii, jak i jej produkcję. Przykładem są chociażby panele słoneczne połączone z Internetem za pomocą technologii oferowanych przez nowo powstałe firmy takie jak Filament, umożliwiające podłączenie do sieci Internet tradycyjnych urządzeń elektronicznych[21]. Dzięki wykorzystaniu czujników IoT tworzone są anonimowe certyfikaty energii i mogą one zostać sprzedane każdemu, kto chce skorzystać z energii słonecznej w ramach sieci energetycznej[22].

Oczywiście firmy energetyczne widzą również korzyści dla siebie, gdyż będą dzięki temu mogły w znacznym stopniu zoptymalizować przepływy w sieci energetycznej, a tym samym zminimalizować straty energetyczne podczas przesyłu energii.

6. ZARZĄDZANIE CYFROWĄ TOŻSAMOŚCIĄ

Dotychczas wymienione przykłady zastosowań systemów opartych o blockchain miały wspólną cechę w postaci anonimowości użytkowników. Weryfikacja autentyczności towarów, jego przemieszczenia czy przesyłu energii nie wymusza podania tożsamości użytkownika. Skoro jednak umiemy tworzyć jednoznaczne cyfrowe identyfikatory dla otaczających nas

[20] http://gulfnews.com/news/uae/government/dubai-launches-blockchain-strategy-to-become-paperless-by-2020-1.1907790 [dostęp: 28.05.2017]
[21] https://filament.com/ [dostęp: 28.05.2017]
[22] https://solarcoin.org/en/front-page/ [dostęp: 28.05.2017]

rzeczy, to co stoi na przeszkodzie, żeby spróbować jednoznacznie określić tożsamość osoby i zapisać ją do blockchain?

Prawdziwa identyfikacja powinna być łatwo dostępna dla tych, którzy tego potrzebują, a publicznie dystrybuowana baza jaką jest blockchain może w tym pomóc. Tożsamość to w wielu przypadkach potwierdzone informacje o tym kim jesteś i co inni wiedzą o Tobie (co w wielu przypadkach jest bardziej uczciwe niż to, co powiesz o sobie sam). Wychodząc z takiego założenia powstają już systemy, które umożliwiają utworzenie potwierdzenia swojej tożsamości w cyberprzestrzeni, ale bez przechowywania swoich danych na serwerach zaufanej trzeciej strony (np. banku). Wykorzystując informacje, które jesteśmy w stanie potwierdzić oraz dokumenty, które posiadamy system utworzy odpowiednie wpisy w blockchain[23] [24].

7. POTWIERDZENIE PRAW WŁASNOŚCI

Technologia blockchain umożliwia także potwierdzenie, że dana rzecz lub dobro należy niezaprzeczalnie do konkretnej osoby i przechowuje te informacje w sposób trwały i niezmienny. Daje to olbrzymie możliwości w dziedzinie różnorodnych rejestrów praw własności. Na przykład w celu potwierdzenia autorstwa wszelkiego rodzaju dokumentów (papierowych, fotograficznych lub nagrań audio/wideo) można wykorzystać tzw. dowody istnienia (proof-of-existence[25]).

Ta prosta metoda pozwala każdemu na przechowywanie kryptograficznego skrótu dowolnego dokumentu w blockchain, co potwierdza, że dane dobro cyfrowe istniało w momencie, gdy dany blok został dodany do łańcucha. Nazwisko autora lub jego jednoznaczny identyfikator tożsamości wstawiony do dokumentu będzie oznaczał silne powiązanie danego dobra i osoby właściciela. Jeśli nikt nie udowodni posiadania lub znajomości tego konkretnego dobra (pliku czy dzieła) sprzed daty zapisanej w transakcji w blockchain, autor powinien mieć możliwość dochodzenia swoich praw na podstawie tych zapisów. W USA znane są już precedensy, gdzie jako dowód sądowy został uznany wpis transakcji w blockchain[26]. Otwiera to pole działań w temacie notarialnych potwierdzeń dokumentów oraz aktów własności (np. gruntów).

[23] https://shocard.com/ [dostęp: 28.05.2017]
[24] https://www.sovrin.org/ [dostęp: 28.05.2017]
[25] https://proofofexistence.com/ [dostęp: 28.05.2017]
[26] https://www.blockcrushr.com/vermont-state-legislature-will-begin-accept-blockchain-evidence-admissible-court [dostęp: 28.05.2017]

8. ZABEZPIECZENIE DANYCH MEDYCZNYCH

Zabezpieczenie zarówno własności, jak autentyczności jest jeszcze bardziej krytyczne i pożądane, gdy w grę wchodzą dane wrażliwe - np. dane medyczne (protokoły z testów, wyniki badań, formularze na udzielenie zgody itp.)[27]. Jeśli podczas procesu ktoś ma wątpliwości co do autentyczności danych, z którymi się styka, może sprawdzić, czy jego informacje są autentyczne, wykorzystując do tego skróty danych oryginalnych zapisane w blockchain.

9. BLOCKCHAIN I ROZWIĄZANIA FINANSOWE

Wiele kwestii, takich jak wysoki koszt transferu, ograniczone metody dystrybucji pieniędzy, ograniczone możliwości promocji własnej marki, ograniczone sposoby radzenia sobie z pieniędzmi itp. wpłynęło na to, że blockchain mógł szczególnie wyraźnie zaprezentować swoje mocne strony w obszarze rozwiązań FinTech. Nawet tradycyjne instytucje finansowe dostrzegły ogromny potencjał technologii blockchain w zakresie innowacji w usługach finansowych. Przelewy i wymiana walut są chyba najbardziej rozwiniętymi obszarami zastosowań blockchain, bo wykorzystują podstawowe mechanizmy tej technologii. Dziesiątki dużych instytucji finansowych, w tym wiele największych banków na świecie, już zainicjowały prace badawcze i koncepcyjne mające na celu zbadanie realnego potencjału blockchain[28] np. w temacie szybkich przelewów międzybankowych. Blockchain umożliwia pewną i bezpieczną wymianę bezpośrednią walorów finansowych między dwoma użytkownikami sieci ("peer-to-peer") i jest to jego ogromna przewaga nad tradycyjnymi rozwiązaniami, które nie mogą się obejść bez zaufanej trzeciej strony do rozliczania transakcji. Poprzez wyeliminowanie pośredników blockchain może umożliwić tanie i błyskawiczne przekazy transgraniczne, a tym samym zwiększyć siłę wydatkową obrotu pieniężnego. Pożyczki w systemie alternatywnych kryptowalut należą do bardzo rozpowszechnionego dzisiaj trendu.

10. CROWDFUNDING I WYNAGRADZANIE TWÓRCÓW

[27] https://www.wired.com/2017/02/moving-patient-data-messy-blockchain-help/ [dostęp: 28.05.2017]
[28] http://socialracemedia.com/jpmorgan-tests-blockchain-for-loan-streamlining/ [dostęp: 28.05.2017]
https://www.credit-suisse.com/pl/en/about-us/media/news/articles/media-releases/2016/09/en/blockchain-demonstration-shows-potential-loan-market-improvements.html [dostęp: 28.05.2017]
http://www.reuters.com/article/us-banks-blockchain-idUSKCN0RF24M20150915 [dostęp: 28.05.2017]

Specyficznym i ciekawym przypadkiem wymiany bezpośredniej w oparciu o sieć blockchain są systemy tworzenia treści np. blogów lub książek, gdzie każdy uczestnik takiego procesu uzyskuje odpowiednie udziały/granty w postaci kryptowaluty (tokena), w zależności od wkładu w tworzoną publikację. Udziały te następnie przekładają się bezpośrednio na procent zysków, jakie dana publikacja wygeneruje w dedykowanym do tego systemie e-learning'owym. Im lepszy materiał powstał, tym więcej osób go czyta i tym większe "wynagrodzenie" jest przekazywane automatycznie przez smart-contract na rzecz autorów. W Stanach Zjednoczonych model taki został wprowadzony na kilku uczelniach wyższych. Czytanie jest darmowe, a autor zbiera punkty, które potem przekładają się na elementy zaliczeń przedmiotów oraz dodatkowych bonusów w ramach działania uczelni. Oczywiście istnieją też komercyjne zastosowania tego modelu, gdzie czytający płaci kryptowalutą za możliwość zapoznania się z przygotowaną przez autorów publikacją.

11. ELEKTRONICZNE GŁOSOWANIE (E-VOTING)

Temat głosowań elektronicznych, szczególnie przez Internet, dla wielu ludzi jest tematem zamkniętym nawet na dyskusję. Waga takiego systemu jest na tyle znacząca, że ludzie nie chcą powierzyć w całości możliwości głosowania systemowi informatycznemu. Istniejące elektroniczne systemy głosowania cierpią z powodu poważnych wad projektowych. Wykorzystanie scentralizowanych ośrodków przeprowadzania głosowań oznacza, że istnieje jeden dostawca, który kontroluje bazę danych i wyjścia systemowe oraz dostarcza narzędzia monitorujące ten system. Brak otwartej, niezależnej weryfikacji danych wejściowych utrudnia takiemu scentralizowanemu systemowi zdobycie wiarygodności, wymaganej przez wyborców i organizatorów wyborów. Blockchain może działać jako bezpieczna, niezaprzeczalna baza danych do rejestrowania głosów i wyników audytu w wiarygodny i pewny sposób. Zarówno w sferze głosowań publicznych[29], jak i korporacyjnych[30] z wykorzystaniem blockchain, na całym świecie widać wzmożone działania badawcze i projektowe oraz znaczące inwestycje. W obszarze elektronicznych wyborów publicznych przełomowy okazał się sukces Estonii, która jako pierwszy kraj na świecie wprowadziła możliwość głosowania przez Internet z

[29] http://www.zdnet.com/article/australia-post-details-plan-to-use-blockchain-for-voting/ http://e-vox.org/balta-installs-e-voxnarada/ [dostęp: 28.05.2017]

[30] https://bitcoinmagazine.com/articles/russia-s-national-settlement-depository-successfully-tests-blockchain-based-e-voting-system-1464198071/ [dostęp: 28.05.2017] http://bravenewcoin.com/news/new-blockchain-e-voting-service-complements-abu-dhabi-economic-vision/ [dostęp: 28.05.2017]

wykorzystaniem systemu opartego na blockchain[31]. Jak pokazuje przykład estoński, dzięki wykorzystaniu blockchain system głosowań staje się bardziej odporny na fałszerstwa, bardziej transparentny i o wiele bardziej dostępny, czym poszerza możliwości realnego udziału wyborców w akcie wyborczym.

12. PODSUMOWANIE

Przytoczone w artykule przypadki użycia technologii blockchain, które realnie wpływają na zwiększenie efektywności funkcjonowania przedsiębiorstw oraz poprawę jakości życia zwykłych ludzi, to jedynie niewielki wycinek możliwości jakie daje blockchain. Coraz lepsze rozumienie tej technologii i jej innowacyjnego potencjału powoduje, że praktycznych zastosowań będzie coraz więcej. Blockchain jest typem technologii zwanej często „enabler" lub „changer", co oznacza, że wiele trudnych lub wręcz nierozwiązywalnych dotąd problemów staje się realnie prostych.

Warto także zauważyć, że blockchain wprowadza bardzo ważny, nowy aspekt do sieci Internet - bezpośrednie relacje ekonomiczne między członkami sieci. Dodając do tego zdolność potwierdzenia autentyczności fizycznych bądź cyfrowych dóbr oraz tożsamości osób, otrzymujemy zupełnie nowe, nieznane dotychczas narzędzie – „Internet of Value".

***

BLOCKCHAIN - THE STORY, CHARACTERISTICS AND MAIN USE CASES

The blockchain technology is named as one of the most disruptive information technologies of our times. The 8-year-old story of this technology is linked to the story of the Bitcoin digital currency, created by mysterious Satoshi Nakamoto. Since the first users joined the Bitcoin network in 2009, blockchain has evolved as a base technology, which is now applicable not only to new cryptocurrencies. An important fact was also an introduction of the Bitcoin-independent Ethereum blockchain, designed by 19-year-old Vitalik Buterin, which offered new functional capabilities - smart contracts. Blockchain very intensively and effectively uses well-known cryptographic concepts such as hash functions, asymmetric

[31] http://business.nasdaq.com/marketinsite/2017/Is-Blockchain-the-Answer-to-E-voting-Nasdaq-Believes-So.html [dostęp: 28.05.2017]

cryptography and timestamping. Automated consensus mechanisms eliminate the need for trusted third parties to process transaction and smart contracts have expanded the scope of blockchain applications far beyond cryptocurrencies. Companies and institutions around the world have recognized the innovative potential of the unique features of blockchain and are now at the stage of streamlining their processes with this technology. These applications of the blockchain technology affect also the quality of ordinary people's life.

KEYWORDS:

Blockchain technology, hash function, asymmetric cryptography, timestamping, consensus mechanism, smart contracts, blockchain applications, supply chain, identification, authentication, identity management, property rights, FinTech, crowdfunding, electronic voting

BIBLIOGRAFIA

http://satoshi.nakamotoinstitute.org/emails/cryptography/15/

https://bitcoin.org/bitcoin.pdf

http://www.ioi2012.org/competition/results-2/

http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

https://pl.wikipedia.org/wiki/Drzewo_hash

https://pl.wikipedia.org/wiki/Problem_bizantyjskich_genera%C5%82%C3%B3w

https://en.wikipedia.org/wiki/Nick_Szabo

https://en.wikipedia.org/wiki/Double-spending

https://en.wikipedia.org/wiki/Internet_of_things

https://www.provenance.org/tracking_tuna_on_the_blockchain

http://www.wired.co.uk/article/blockchain-conflict-diamonds-everledger

https://www.microsoft.com/reallifecode/2017/04/10/stampery-blockchain-add-microsoft-office/

http://gulfnews.com/news/uae/government/dubai-launches-blockchain-strategy-to-become-paperless-by-2020-1.1907790

https://www.blockcrushr.com/vermont-state-legislature-will-begin-accept-blockchain-evidence-admissible-court

https://www.wired.com/2017/02/moving-patient-data-messy-blockchain-help/

http://socialracemedia.com/jpmorgan-tests-blockchain-for-loan-streamlining/

https://www.credit-suisse.com/pl/en/about-us/media/news/articles/media-releases/2016/09/en/blockchain-demonstration-shows-potential-loan-market-improvements.html

http://www.reuters.com/article/us-banks-blockchain-idUSKCN0RF24M20150915

http://www.zdnet.com/article/australia-post-details-plan-to-use-blockchain-for-voting/

http://e-vox.org/balta-installs-e-voxnarada/

https://bitcoinmagazine.com/articles/russia-s-national-settlement-depository-successfully-tests-blockchain-based-e-voting-system-1464198071/

http://bravenewcoin.com/news/new-blockchain-e-voting-service-complements-abu-dhabi-economic-vision/

http://business.nasdaq.com/marketinsite/2017/Is-Blockchain-the-Answer-to-E-voting-Nasdaq-Believes-So.html