Grzegorz Borowik[1]
ORCID: 0000-0003-4148-4817
Zbigniew M. Wawrzyniak[2]
ORCID: 0000-0003-0052-4114
Paweł Cichosz[3]
ORCID: 0000-0002-8049-7410

Technologia blockchain — innowacja i bezpieczeństwo

[1] Dr inż. Grzegorz Borowik — jest naukowcem, doktorem nauk technicznych. Jego aktualne prace koncentrują się na algorytmach maszynowego uczenia, Big Data oraz przetwarzania obrazu. Do 2016 r. był pracownikiem Zakładu Cyberbezpieczeństwa w Instytucie Telekomunikacji Politechniki Warszawskiej. W 2015 r. został laureatem programu stażowo-szkoleniowego „Top 500 Innovators" MNiSW realizowanego na Uniwersytecie Kalifornijskim w Berkeley w Stanach Zjednoczonych, którego celem były szkolenia z obszaru zarządzania biznesowego w nauce i komercjalizacji badań. W 2016 r. odbył staż postdoktorancki w Knowledge Engineering and Discovery Research Institute w Auckland w Nowej Zelandii, gdzie prowadził badania związane z praktycznym zastosowaniem sztucznych sieci neuronowych trzeciej generacji. W latach 2016–2018 zajmował się modelowaniem algorytmów dla bezpiecznych sieci P2P w projekcie Golem, którego celem jest stworzenie zdecentralizowanego superkomputera. W latach 2017–2019 zajmował stanowisko adiunkta w Wyższej Szkole Policji w Szczytnie w Zakładzie Cyberbezpieczeństwa. Aktualnie jest kierownikiem ds. badań i rozwoju w firmie Nethone, gdzie prowadzi projekt z obszaru cyberbezpieczeństwa. Jest autorem podręcznika akademickiego oraz autorem i współautorem ponad stu publikacji w czasopismach naukowych oraz materiałach konferencyjnych. Jego zainteresowania badawcze obejmują inteligencję obliczeniową, techniki maszynowego uczenia, techniki optymalizacji, NLP, Internet rzeczy, kryptografię oraz blockchain. Od wielu lat uczestniczy w projektach B+R, w tym w roli kierownika oraz głównego wykonawcy.
Kontakt z autorem za pośrednictwem redakcji.

[2] Dr inż. Zbigniew M. Wawrzyniak — posiada stopień doktora nauk technicznych w dziedzinie elektroniki nadany przez Wydział Elektroniki i Technik Informacyjnych Politechniki Warszawskiej w 1990 r. Jest adiunktem w Instytucie Systemów Elektronicznych Politechniki Warszawskiej. Jego zainteresowania naukowe koncentrują się na zastosowaniu technik modelowania oraz metod symulacji i prognozowania na podstawie danych obserwacyjnych i sygnałowych — eksperymentalnych, zarządzania i eksploracji statystycznej danych sygnałowych i procesowych, w tym obrazowych i ICT. Jest autorem i współautorem ponad osiemdziesięciu publikacji w monografiach i czasopismach naukowych oraz materiałach konferencyjnych. Posiada bogate doświadczenie w realizacji praktycznych projektów z zakresu modelowania i analizy predykcyjnej danych.
Kontakt z autorem za pośrednictwem redakcji.

[3] Dr inż. Paweł Cichosz — uzyskał stopień doktora nauk technicznych w dziedzinie informatyki na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej w 1998 r. Jest adiunktem w Instytucie Informatyki Politechniki Warszawskiej. Jego zainteresowania naukowe obejmują obszary maszynowego uczenia się, odkrywania wiedzy w danych i sztucznej inteligencji. Posiada bogate doświadczenie w realizacji praktycznych projektów z zakresu analizy danych i modelowania predykcyjnego.
Kontakt z autorem za pośrednictwem redakcji.

Wprowadzenie

Blockchain to jedna z najbardziej rewolucyjnych technologii XXI w., która wciąż rozwija się i której potencjał nie jest jeszcze w pełni zrealizowany. W swej istocie blockchain jest po prostu rozproszoną bazą rekordów. To co czyni go wyjątkowym, to fakt, że nie jest to prywatna baza danych, ale publiczna, tzn. każdy, kto jej używa, ma jej pełną lub częściową kopię. A nowy rekord można dodać tylko za zgodą innych posiadaczy bazy danych. Ponadto dzięki sieci blockchain możliwa jest implementacja kryptowalut i inteligentnych kontraktów.

Ponieważ blockchain jest systemem rozproszonym, który nie jest obsługiwany przez jedną konkretną instytucję, może być traktowany jako rodzaj wspólnej infrastruktury dzielonej między wszystkich uczestników. Oznacza to, że międzyorganizacyjny system zarządzania przepływem pracy oparty na blockchainie ma jedną istotną zaletę — nie istnieje potrzeba posiadania centralnego organu zarządzającego. W związku z tym wykorzystanie systemu opartego na blockchainie jako infrastruktury, ułatwia automatyzację i upraszcza system. Jednak, z drugiej strony, takie rozwiązanie musi stawić czoła wyzwaniom, takim jak nadużycia, niejasne obowiązki lub różne opinie użytkowników.

Istnieją dwa typy technologii blockchain: blockchain publiczny i blockchain prywatny. Do publicznego blockchaina może dołączyć każdy. Bitcoin jest przykładem publicznego blockchaina, w którym każdy, kto chce kupić kryptowalutę, może dołączyć do łańcucha. Blockchain jest otwarty, co oznacza, że wszyscy mogą zobaczyć wszystkie transakcje. Prywatne łańcuchy bloków są administrowane centralnie i wymagają zgody na dołączenie; są przystosowane do użytku w ramach jednej organizacji lub pomiędzy organizacjami partnerskimi. Zarówno publiczne, jak i prywatne rozwiązania są bezpieczne, ponieważ są niezmienne (tj. każdy rekord lub blok jest niezmienny i powiązany z wszystkimi innymi), a także dodawanie nowych bloków wymaga konsensusu wśród użytkowników. Oznacza to, że są one natywnie bezpieczniejsze niż praktycznie każda inna technologia sieciowa.

Mimo że blockchain zyskał na znaczeniu w roku 2009, naukowcy i przedsiębiorcy nie są w stanie nadal zrozumieć jego mechanizmów i w pełni docenić jego potencjału, zwłaszcza z perspektywy technicznych wyzwań i ograniczeń technologii[4]. W artykule[5] można znaleźć siedem wyzwań i ograniczeń technologii blockchain: przepustowość, opóźnienie, rozmiar, bezpieczeństwo, zmarnowane zasoby, użyteczność i wersjonowanie, hardforks i multichains.

[4] R. Beck i in., *Blockchain — The Gateway to Trust — free Cryptographic Transactions*, 24th European Conference on Information Systems (ECIS), Istanbul, Turkey 2016.

[5] M. Swan, *Blockchain. Blueprint for an New Economy*, Sebastopol 2015.

Podstawy technologii

W blockchainie to bloki przechowują cenne informacje. Na przykład bitcoin przechowuje w blokach transakcje, istotę każdej kryptowaluty. Poza tym blok zawiera pewne informacje techniczne, takie jak jego wersja, aktualny znacznik czasu i skrót (ang. *hash*) poprzedniego bloku. W wersji uproszczonej, która zawiera tylko istotne informacje, blok został zilustrowany na rysunku 1.

Rysunek 1

Blok

```
type Block struct {
      timestamp   int64
      data        []byte
      prevBlockHash []byte
      hash        []byte
}
```

Źródło: opracowanie własne

Timestamp jest bieżącym znacznikiem czasu — informacją, kiedy blok został utworzony, *data* jest faktyczną informacją zawartą w bloku, *prevBlockHash* przechowuje wartość funkcji skrótu dla poprzedniego bloku i *hash* jest skrótem dla danego bloku. W opisie protokołu bitcoin pola *timestamp*, *prevBlockHash* i *hash* znajdują się w nagłówku bloku, tworząc oddzielną strukturę danych, natomiast transakcje (*data*) są oddzielną strukturą danych.

Obliczanie skrótu dla bloków jest bardzo ważną integralną cechą blockchaina, która wpływa na jego bezpieczeństwo. Operacja jest trudna obliczeniowo i zajmuje określony czas, nawet na szybkich komputerach. Jest to celowy element architektoniczny, który utrudnia dodawanie nowych bloków i uniemożliwia ich modyfikację po dodaniu do blockchaina.

W swej istocie blockchain to po prostu baza danych o określonej strukturze: jest to uporządkowana lista jednokierunkowa z wskaźnikiem na poprzedni element — blok. Oznacza to, że bloki są przechowywane w kolejności wstawiania i że każdy blok jest połączony z poprzednim. Ta struktura pozwala szybko odczytać najnowszy blok w łańcuchu i (wydajnie) odczytać blok przez jego skrót. Struktura ta może zostać zaimplementowana za pomocą mapy lub w najprostszej wersji dla celów tego artykułu — za pomocą tablicy (rysunek 2). Tablica będzie wtedy przechowywać uporządkowane bloki, a mapa zachowa pary (*hash*, *block*).

Rysunek 2

Blockchain

```
type Blockchain struct {
      blocks []*Block
}
```

Źródło: opracowanie własne

Aby dodać nowy blok, potrzebujemy istniejącego bloku. Tak więc w każdym blockchainie musi istnieć co najmniej jeden blok. Blok, który jest pierwszy w łańcuchu, nazywany jest blokiem genesis.

Rzeczywisty blockchain jest jednak znacznie bardziej złożony, a dodawanie nowych bloków, aby umieścić w nich dane, wymaga wykonania pracy — obliczeń, takie rozwiązanie funkcjonuje na przykład w protokole bitcoina. Następnie nowy blok musi zostać zatwierdzony przez innych uczestników sieci — mechanizm ten określa się konsensusem (ang. *consensus*). Należy jeszcze zaznaczyć, że blockchain jest rozproszoną bazą danych, która nie ma jednego decydenta. Te wszystkie mechanizmy sprawiają, że blockchain jest bezpieczny i spójny. Za wykonaną pracę i akceptację przez inne węzły wypłacana jest nagroda — tak ludzie otrzymują tokeny/kryptowaluty (w zależności od technologii) w ramach wydobycia (ang. *mining*). W blockchainie użytkownicy sieci (ang. *miners*) pracują nad utrzymaniem sieci, dodają do niej nowe bloki i otrzymują nagrodę za swoją pracę. W wyniku ich pracy, blok jest włączany do łańcucha w bezpieczny sposób, co zapewnia stabilność całej bazy danych. Warto zauważyć, że ten, kto ukończył pracę, musi to udowodnić. Potrzeba zabezpieczania transakcji jest związana z problemem podwójnego wydawania (ang. *double spending*), ponieważ w systemie zdecentralizowanym istnieje naturalna możliwość wydania tej samej sumy tokenów dwukrotnie przez jednego kupującego.

W najpopularniejszym rozwiązaniu, przed uzyskaniem pozwolenia na dodanie bloku wykonuje się obliczenia — mechanizm ten nosi nazwę *proof-of-work* (PoW). Wraz z popularyzacją technologii pojawiły się nowe propozycje przeciwdziałające *double spending*, ponieważ największymi wadami metody *proof-of-work* są: duże zużycie energii, zapotrzebowanie na specjalne jednostki obliczeniowe np. ASIC czy GPU, opóźnianie transakcji oraz brak rentowności w dalszej perspektywie utrzymania sieci. Do innych propozycji mechanizmów osiągania konsensusu należy zaliczyć: *proof-of-stake* (PoS), *proof-of-importance* (PoI), *proof-of-capacity* (PoC), *proof-of-space* (PoS).

Algorytmy typu *proof-of-work* muszą spełniać następujące wymaganie: wykonanie pracy jest trudne, ale weryfikacja dowodu wykonania pracy jest łatwa. Wykonanie pracy jest trudne, ponieważ wymaga dużej mocy obliczeniowej. Co więcej, trudność tej pracy reguluje się dynamicznie.

W bitcoinie bloki dodawane są średnio co 10 minut. Celem pracy jest znalezienie skrótu do bloku, który spełnia określone wymagania i to właśnie wyliczony skrót służy jako dowód. Zatem znalezienie dowodu to faktyczna praca. Weryfikacja dowodu może zaś być rozumiana jak podstawienie wyniku wcześniejszych obliczeń do określonego przez protokół równania i porównaniu rezultatu, więc nie zajmuje dużo czasu.

Proces uzyskiwania skrótu dla określonych danych nazywa się hashingiem. Skrót (ang. *hash*) stanowi unikalną reprezentację danych. Funkcja skrótu, czasami nazywana jest funkcją mieszającą, pobiera ona dane o dowolnym rozmiarze i tworzy skróty o stałym rozmiarze. Poniżej przedstawiono kilka kluczowych cech funkcji skrótu:

1. Oryginalne dane nie mogą zostać przywrócone ze skrótu. Zatem mieszanie nie jest szyfrowaniem.
2. Określone dane mogą mieć tylko jeden skrót — skrót jest unikatowy.
3. Zmiana nawet jednego bajtu w danych wejściowych powoduje wygenerowanie zupełnie innego skrótu. Dobrze zaprojektowane funkcje skrótu powinny dać w rezultacie skrót różniący się w przynajmniej 50% dla małej zmiany.

Funkcje skrótu są szeroko stosowane w celu sprawdzenia spójności danych. Niektórzy dostawcy oprogramowania publikują sumy kontrolne dla pakietów oprogramowania, które są wynikiem działania funkcji skrótu.

W blockchainie obliczanie skrótów jest używane w celu zagwarantowania spójności. Dane wejściowe dla algorytmu mieszającego zawierają skrót poprzedniego bloku, co uniemożliwia (jest bardzo trudne) modyfikowanie bloku w łańcuchu — modyfikacja bloku wymusza ponowne przeliczenie jego skrótu i skrótów wszystkich bloków po nim występujących.

Bitcoin używa algorytmu *hashcash*. Jest to algorytm *proof-of-work*, który został oryginalnie opracowany, aby zapobiec generowaniu spamu w postaci niechcianych wiadomości e-mail. Algorytm ten można opisać w następujących krokach:

1. Przygotuj publicznie znane dane (w przypadku wiadomości e-mail — adres e-mail odbiorcy, w przypadku bitcoina — nagłówki bloków).
2. Dodaj licznik do danych (*counter*) — w sensie konkatenacji zbiorów. Licznik rozpoczyna się od 0.
3. Uzyskaj skrót dla (*data*, *counter*).
4. Sprawdź, czy skrót spełnia określone wymagania:
   a) jeśli tak, obliczenia są zakończone,
   b) jeśli nie, zwiększ licznik i powtórz kroki 3 i 4.

A zatem jest to algorytm siłowy (ang. *brute-force*): zwiększenie licznika, następnie obliczenie skrótu, sprawdzenie, zwiększenie licznika, obliczenie skrótu itd. Algorytm jest kosztowny obliczeniowo.

W oryginalnej implementacji programu *hashcash* wymogiem jest, że pierwsze 20 bitów wyniku mieszania musi być zerami. W bitcoinie wymóg jest dostosowywany, ponieważ zgodnie z założeniami, blok musi być generowany co 10 minut, pomimo rosnącej mocy obliczeniowej i coraz większej liczby serwerów/komputerów (*miners*) przyłączających się do sieci.

Blockchain jest przechowywany w bazie danych. W oryginalnym artykule opisującym kryptowalutę bitcoin[6] nie określono konkretnej bazy danych. Bitcoin Core, który został początkowo opublikowany przez Satoshi Nakamoto i jest obecnie referencyjną implementacją bitcoina; używa LevelDB. W tej bazie dane są przechowywane jako pary klucz-wartość. Następnie pary klucz-wartość przechowuje się w segmentach, które z kolei są przeznaczone do grupowania par podobnych — analogicznie do tabel w systemach zarządzania relacyjnymi bazami danych. Bitcoin Core wykorzystuje dwa segmenty do przechowywania danych: *blocks* — przechowują metadane opisujące wszystkie bloki w łańcuchu, *chainstate* — przechowuje stan łańcucha. Ponadto bloki są przechowywane jako oddzielne pliki na dysku. Odbywa się to w celu podniesienia wydajności — odczytywanie pojedynczego bloku nie wymaga załadowania wszystkich z nich do pamięci.

W segmencie *blocks*, pary *key* → *value* to:
1. 'b' + 32-byte block hash → block index record,
2. 'f' + 4-byte file number → file information record,
3. 'l' → 4-byte file number: the last block file number used,
4. 'R' → 1-byte boolean: whether we're in the process of reindexing,
5. 'F' + 1-byte flag name length + flag name string → 1 byte boolean: various flags that can be on or off,
6. 't' + 32-byte transaction hash → transaction index record.

W segmencie chainstate, pary *key* → *value* to:
1. 'c' + 32-byte transaction hash → unspent transaction output record for that transaction,
2. 'B' → 32-byte block hash: the block hash up to which the database represents the unspent transaction outputs.

Utworzenie blockchaina polega na wykonaniu następującej sekwencji:
1. Otwórz plik DB.
2. Sprawdź, czy jest w nim przechowywany blockchain.
3. Jeśli istnieje blockchain:
   a) utwórz nową instancję blockchaina.
   b) ustaw koniec instancji blockchaina na wartość skrótu ostatniego bloku przechowywanego w DB.
4. Jeśli blockchain nie istnieje:
   a) utwórz genesis blok,
   b) zachowaj w DB.
   c) zapisz wartość skrótu genesis blok jako skrót ostatniego bloku.
   d) utwórz nową instancję blockchaina i ustaw koniec instancji blockchaina na wartość skrótu bloku genesis.

[6] S. Nakamoto, *Bitcoin: A Peer-to-peer Electronic Cash System*, 2008, <https://bitcoin.org/bitcoin.pdf>, 17 września 2018 r.

Tak więc struktura blockchaina wygląda jak na rysunku 3.

Rysunek 3

Struktura blockchaina

```
type Blockchain struct {
      tip []byte
      db  *bolt.DB
}
```

Źródło: opracowanie własne

Transakcje są głównym zastosowaniem blockchaina. Celem jest przechowywanie transakcji w bezpieczny i niezawodny sposób, aby po ich utworzeniu nie można było ich modyfikować. W typowych aplikacjach internetowych związanych z płatnościami istnieją bazy danych dla kont i transakcji. Baza kont przechowuje informacje o użytkowniku, w tym jego dane osobowe i saldo, a baza transakcji przechowuje informacje o przelewach. W implementacji bitcoina płatności są realizowane w zupełnie inny sposób. Nie są prowadzone konta, nie są zbierane informacje o saldach, adresach, brakuje monet, nadawców i odbiorców. Występują jedynie transakcje. Ponieważ blockchain jest publiczną i otwartą bazą danych, niepożądane byłoby przechowywanie poufnych informacji o właścicielach portfeli. Monety nie są gromadzone na rachunkach. W strukturze nie ma pola ani atrybutu, który przedstawia saldo konta. Transakcje nie przesyłają pieniędzy w sposób, jaki znamy z realizacji przez systemy bankowe.

Transakcja bitcoina jest kombinacją danych wejściowych i wyjściowych (rysunek 4). Wejścia nowych transakcji odpowiadają wyjściom z poprzedniej transakcji. Spełnione są następujące założenia: istnieją wyjścia, które nie są powiązane z wejściami; w jednej transakcji dane wejściowe mogą odnosić się do danych wyjściowych z wielu transakcji; wejście musi odnosić się do wyjścia. Inaczej mówiąc, transakcje blokują wartości za pomocą skryptu, który może zostać odblokowany tylko przez jednostkę, która je zablokowała.

Rysunek 4

Struktury dla transakcji

```
type Transaction struct {
             id  []byte
             vIn []TXInput
             vOut []TXOutput
}
type TXOutput struct {
             value    int
             scriptPubKey string
}
type TXInput struct {
             txId   []byte
             vOut   int
             scriptSig string
}
```

Źródło: opracowanie własne

Ethereum

Ethereum to zdecentralizowany system kryptowalutowy oparty na blockchainie, jak również platforma do tworzenia rozproszonych aplikacji. W Ethereum możliwe jest implementowanie dowolnych złożonych reguł wymaganych przez system płatności jako inteligentne kontrakty w języku programowania wysokiego poziomu — Solidity. Ponadto Ethereum umożliwia fragmentację tokenów.

Ethereum przechowuje w blockchainie stan globalny. Ten stan jest w istocie zbiorem rachunków, z których każdy ma swój unikalny adres i zapis salda (bilans) w walucie eter. Konto może przechowywać dane i może zawierać powiązany z nimi kod kontraktu[7].

Stan globalny zmienia się według transakcji. Każda transakcja ma adres nadawcy i adres odbiorcy oraz przesyła określoną liczbę eterów pomiędzy tymi adresami. Jeśli konto odbiorcy jest powiązane z kodem umowy, umowa jest realizowana w wyniku transakcji. Transakcja może zawierać dodatkowe dane, dostępne na podstawie umowy. Umowa może wywołać kolejną umowę, która może wywołać jeszcze inną, ale ten łańcuch wykonawczy musi rozpoczynać się od transakcji rozpoczętej przez podmiot zewnętrzny/użytkownika. Umowa nie może wywoływać żadnej usługi zewnętrznej poza Ethereum.

Kontrakty są zawierane przez Ethereum Virtual Machine (dalej jako: EVM)[8]. Każda instrukcja EVM zużywa pewną ilość gazu, która odzwierciedla koszt obliczeniowy przetwarzania instrukcji przez węzły Ethereum. Gaz musi być zakupiony za walutę eter przez użytkownika, który chce zawrzeć umowę. Opłata za gaz jest analogiczna do opłat transakcyjnych w bitcoinach. Cena gazu jest rynkowa: każda transakcja określa maksymalną cenę, którą nadawca jest gotów zapłacić za jednostkę gazową, a „górnicy" (ang. *miners*) mogą priorytetowo traktować transakcje na podstawie tych informacji. Aby oszacować koszt wykonania kontraktu w walucie dolarowej — USD, należy wziąć pod uwagę zarówno aktualną średnią cenę gazu, jak i cenę eteru. Z drugiej strony, aby porównać różne schematy płatności przez wdrożone kontrakty na Ethereum można porównać ich koszt w jednostkach gazowych.

Model obliczeniowy Ethereum jest deterministyczny: wynik każdej transakcji jest zawsze taki sam, gdy jest wykonywany w danym stanie globalnym[9]. Ogranicza to możliwość generowania losowych wartości w Ethereum. Powszechnym rozwiązaniem jest poleganie na przyszłych

[7] N. Atzei, M. Bartoletti, T. Cimoli, *A survey of attacks on Ethereum smart contracts SoK*, „Principles of Security and Trust" 2017, Vol. 10204, s. 164–186.

[8] M. English, S. Auer, J. Domingue, *Block Chain Technologies & The Semantic Web: A Framework for Symbiotic Development*, Computer Science Conference for University of Bonn Students, Bonn, Germany 2016.

[9] I. Konstantinidis i in., *Blockchain for Business Applications: A Systematic Literature Review*, International Conference on Business Information Systems, Springer Cham 2018, s. 384–399.

danych blockchaina jako źródła losowości. Na przykład znacznik czasu lub skrót nagłówka jakiegoś przyszłego bloku może być użyty do wywołania generatora liczb losowych. Kontrakty Ethereum nie mają żadnego mechanizmu do planowania działań, na przykład wywoływania innej umowy lub odczytywania znacznika czasu do wykonania w późniejszym czasie. Dlatego każdy system płatności za pomocą Ethereum będzie opierał się na użytkownikach skłonnych do wykonywania transakcji wymaganych przez protokół programu. W szczególności użytkownicy muszą być *online* podczas wykonywania co najmniej niektórych faz protokołu. Muszą również mieć wystarczającą ilość eterów, aby zapłacić za swoje transakcje, co może być problemem dla protokołów płatności, które wymagają węzłów do podjęcia działań. Jest to szczególnie ważne w protokołach z wieloma uczestnikami, z których każdy może zatrzymać protokół. Na szczęście w inteligentnych kontraktach można wdrożyć mechanizmy realizujące nagradzanie stanowiące zachętę z punktu widzenia ekonomicznego do podejmowania działań.

Zastosowanie

Badania nad zastosowaniem blockchaina koncentrują się w ponad 80% na systemie bitcoin i mniej niż w 20% na innych aplikacjach[10]. Jednak dostępnych jest wiele aplikacji, które wykraczają daleko poza jego pierwszą implementację[11].

Na przykład technologia blockchain może być stosowana jako rynek dla aktywów finansowych, baza łańcucha dostaw odporna na nadużycia[12] lub może tworzyć środowisko dla umów cyfrowych i wymiany danych typu *peer-to-peer*[13]. Blockchain jest adaptowany w wielu branżach i służbach rządowych na całym świecie. W mieście Zug w Szwajcarii używa się go do identyfikacji obywateli. Firmy Maersk i Walmart używają go do śledzenia łańcucha dostaw. TUI Tourism Group chce wykorzystać blockchaina do rezerwacji hotelowych i turystycznych. Ponadto rządy w krajach takich jak Brazylia, Szwecja i Gruzja stosują blockchaina do ewidencji nieruchomości i gruntów. Malta wykorzystuje blockchaina do rejestracji przyznanych dyplomów uniwersyteckich oraz innych certyfikatów edukacyjnych i zawodowych. Firmy, takie jak Gem, Philips i YouBase używają go do opieki zdrowotnej, podczas gdy MIT Media Lab rozwija system opieki medycznej z użyciem blockchaina o nazwie MedRec. Technologia blockcha-

[10] J. Yli-Huumo i in., *Where Is Current Research on Blockchain Technology? A Systematic Review*, "PloS one" 2016, No. 11, Vol. 10, <https://doi.org/10.1371/journal.pone.0163477>, 21 października 2019 r.

[11] R. Beck i in., *Blockchain…*, wyd. cyt.

[12] J. Mattila, *The Blockchain Phenomenon — The Disruptive Potential of Distributed Consensus Architectures*, The Research Institute of the Finnish Economy, 2016, <https://ideas.repec.org/p/rif/wpaper/38.html>, 21 października 2019 r.

[13] M. Swan, *Blockchain…*, wyd. cyt.

in może potencjalnie zrewolucjonizować szerokie spektrum procesów biznesowych[14]. Niektórzy autorzy twierdzą, że ich podejście może zapewnić „automatyczną i niezmienną historię transakcji, bezpośrednią implementację logiki sterowania procesem mediatora" (przy użyciu inteligentnych kontraktów) oraz „ścieżkę audytu dla wspólnych procesów biznesowych"[15]. Crosby i inni[16] rozróżnili aplikacje finansowe i niefinansowe, które potencjalnie mogłyby być adresowane przez blockchain. Ta przełomowa innowacja może nie tylko zmienić charakter interakcji finansowych, ale mieć także zastosowanie w wielu innych obszarach naszego codziennego życia.

Blockchain znajduje różnorodne zastosowania, szczególnie w obszarach, które dotychczas opierają się na udziale strony pośredniczącej w transakcji w celu utrzymania określonego poziomu zaufania. Marcella Atzori sugeruje, że polityka i całe społeczeństwo może zostać zrestrukturyzowane przez blockchain[17]. Wiele istniejących metod oraz funkcji może stracić na atrakcyjności, jeśli ludzie zaczną organizować i chronić społeczeństwo za pomocą zdecentralizowanych platform. W artykule stwierdzono, że „decentralizacja usług rządowych za pośrednictwem blockchainów jest możliwa i pożądana, ponieważ może znacznie zwiększyć funkcjonalność administracji publicznej"[18]. Reorganizacja społeczeństwa ma szczególne znaczenie w krajach słabo rozwiniętych i biednych, gdzie wartość może być lepiej chroniona przy użyciu blockchaina, o ile nie istnieją bariery dostępności do sieci i usług cyfrowych. W krajach Trzeciego Świata właściciele ziemi mają ogromny problem z udokumentowaniem własności, jeśli na przykład lokalny rząd ma na celu wywłaszczenie ludności. Te zagrożenia egzystencjalne można kontrolować przez integrację tytułów ziemi z blockchainem. Dlatego w niektórych krajach rozwijających się próbuje się zaimplementować blockchain jako system rejestracji i zarządzania nieruchomościami. Jednak, jak wskazał Florian Glaser[19], interfejs pomiędzy sferą cyfrową a światem fizycznym może okazać się słabym ogniwem, które niekorzystnie wpłynie na zaufanie cyfrowe w systemie blockchainowym.

Kwestią dyskusyjną wśród naukowców oraz regulatorów prawa jest pytanie, czy kryptowaluty opierające się na blockchainie mogą spełniać funkcje prawdziwych pieniędzy[20]. Pieniądze można zdefiniować jako „wszystko,

[14] I. Weber i in., *Untrusted Business Process Monitoring and Execution Using Blockchain*, Springer, Cham 2016.

[15] Tamże, s. 2.

[16] M. Crosby i in., *Blockchain technology: Beyond bitcoin*, "Applied Innovation Review", No. 2, s. 6–19.

[17] M. Atzori, *Blockchain technology and decentralized governance: Is the state still necessary*?, <https://ssrn.com/abstract=2709713>, 21 października 2019 r.

[18] Tamże, s. 31.

[19] F. Glaser, *Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis*, Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS 2017), Waikoloa Village, Hawaii 2017.

[20] European Central Bank, Virtual Currency Schemes, 2012, <https:// www.ecb.europa.eu/pub/pdf/other/virtualcurrencyscheme s201210en.pdf>, 30 listopada 2016 r.; Federal Bureau of Investigation, *Bitcoin virtual currency: intelligence unique*

co jest ogólnie akceptowane w płatności za towary, usługi lub w spłacie długów”[21]. Wiliam J. Luther oraz Lawrence H. White twierdzą, że kryptowaluty są dzisiaj rzadko używane jako medium wymiany[22]. Florian Glaser, Kai Zimmermann, Martin Haferkorn, Mortiz Weber, Michael Siering zaznaczają jednak, że bitcoin jest wykorzystywany przede wszystkim jako spekulacyjny składnik aktywów[23]. Jednak upowszechnienie kryptowalut może stać się możliwe dzięki innowacyjnemu podejściu przedsiębiorców, którzy przyjmą kryptowaluty jako substytut pieniądza. Dlatego branża finansowa obawia się, że duża część ich obecnej działalności może zostać zastąpiona przez blockchaina. W istocie, jeżeli ludzie płacą dziś kartą kredytową, rozliczenie następuje po kilkudniowej zwłoce. Natomiast korzystając z blockchaina płatność może zostać zrealizowana niemal w czasie rzeczywistym.

Blockchain może przyczynić się do tego, w jaki sposób ludzie będą płacili za towary w świecie rzeczywistym. Na przykład właściciele domów ponoszą znaczne koszty transakcji przy zakupie i obsłudze nieruchomości. Według Goldman Sachs „blockchain może zmniejszyć składki na ubezpieczenie i wygenerować 2–4 miliardy dolarów oszczędności w USA, zmniejszając liczbę błędów oraz obsługę bezpośrednią”[24]. Ta przełomowa innowacja może stworzyć nowe oraz zmienić wiele istniejących modeli biznesowych, a tym samym może mieć poważny wpływ na całe gałęzie przemysłu.

Rozwój technologii blockchain w ostatnich latach spowodował pojawienie się innych koncepcji. Taksonomia zdecentralizowanych systemów zgodności (konsensusowych) i przegląd różnych typów systemów zostały przedstawione przez F. Glasera oraz L. Bezzenbergera w pracy pt. *Beyond Cryptocurrencies — A Taxonomy of Decentralized Consensus Systems*[25]. Nick Szabo wprowadził pojęcie „inteligentnych kontraktów”[26], które łączą protokoły komputerowe z interfejsami użytkownika i mają na celu realizację warunków umowy[27]. Dzięki systemowi blockchain inteligentne kontrakty stają się coraz bardziej popularne, ponieważ można je łatwiej

features present distinct challenges for deterring illicit activity, 2012, <https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf>, 30 listopada 2016 r.

[21] F.S. Mishkin, *The economics of money and financial markets*, Boston 2004.

[22] W.J. Luther, L.H. White, *Can bitcoin become a major currency*?, “Working Paper in Economics” 2014, No. 14–17.

[23] F. Glaser i in., *Bitcoin–asset or currency? Revealing users' hidden intentions*, Proceedings of the 22nd European Conference on Information Systems (ECIS 2014), Tel Aviv 2014.

[24] G. Sachs, *Profiles in Innovation — Blockchain*, <http:// www.the-blockchain.com/docs/Goldman-Sachs-report-Blockchain-Putting-Theory-into-Practice.pdf>, 30 listopada 2016.

[25] F. Glaser, L. Bezzenberger, *Beyond Cryptocurrencies — A Taxonomy of Decentralized Consensus Systems*, materiały z 23rd European Conference on Information Systems (ECIS 2015), Muenster, Germany 2015.

[26] N. Szabo, *Smart contracts: formalizing and securing relationships on public networks*, “First Monday” 1997, Vol. 2, No. 9.

[27] A. Kosbai in., *Hawk: The blockchain model of cryptography and privacy-preserving smart contracts*, *2016 IEEE symposium on security and privacy (SP)*, Vol. 1.

implementować w strukturze blockchaina w porównaniu z technologią dostępną w okresie, kiedy zostały opracowane. Takie innowacyjne podejście może na przykład zastąpić pracę prawników lub banków uczestniczących w umowach dotyczących aktywów według wcześniej określonych warunków[28]. Inteligentne kontrakty można również wykorzystać do kontrolowania własności nieruchomości. Własności te mogą być namacalne (np. domy, samochody) lub niematerialne (np. akcje, prawa dostępu). Wybitnym przykładem technologii blockchain, która implementuje inteligentne kontrakty jest sieć Ethereum, będąca zdecentralizowanym systemem zaproponowanym przez Buterina[29]. Technologia Ethereum pozwala na zawieranie umów z wykorzystaniem kryptografii i zastępowanie stron trzecich (np. notariusza), które były niezbędne do zbudowania zaufania w przeszłości. Blockchain może realizować cały proces transakcji przez automatyczne wykonywanie umów w sposób opłacalny, przejrzysty i bezpieczny[30]. Komponenty architektoniczne technologii blockchain, ich wzajemne oddziaływanie oraz bibliotekę do analizy wpływu na ekosystemy cyfrowe można znaleźć w publikacji F. Glasera — *Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis*[31].

Innym zastosowaniem blockchaina jest tak zwane finansowanie społecznościowe (*crowdfunding*). Kampania crowdfundingowa umożliwia dużej liczbie stron wniesienie funduszy na pewne dobro społeczne. Jeżeli minimalny cel dotacji zostanie osiągnięty przed upływem terminu, wówczas darowizny są przekazane wyznaczonej stronie (przedsiębiorcy), w przeciwnym razie darowizny są zwracane.

Kolejnym zastosowaniem jest ubezpieczenie inwestycji z użyciem instrumentu finansowego swap. Osoba z ryzykownym portfelem inwestycyjnym (np. posiadająca dużą liczbę bitcoinów) może zabezpieczyć się przed ryzykiem poprzez zakup ubezpieczenia (np. przez skuteczne obstawienie za cenę bitcoina z inną osobą). Cena akcji w pewnym przyszłym terminie, określona przez zaufany organ określony w zamówieniu publicznym, ustala, która z dwóch stron otrzyma wypłatę. Umowa prywatna zapewnia poufność zarówno w kontekście szczegółów umowy, tj. progu cenowego, jak i wypłaty.

Technologia blockchain może być wykorzystana w celu ustanowienia dobrowolnych systemów regulacyjnych. Hwyl Labs zaproponował, że blockchain może być wykorzystany do wsparcia zmian klimatycznych. W ramach tego modelu jednostka może zawrzeć umowę inteligentną z inną osobą, organizacją, firmą lub rządem w celu zmniejszenia emisji GHG tego podmiotu. Umowa

[28] J. Fairfield, *Smart contracts, Bitcoin bots, and consumer protection*, "Washington and Lee Law Review Online" 2014, Vol. 71.

[29] V. Buterin, *A next-generation smart contract and decentralized application platform*, <http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf>, 21 października 2019 r.

[30] J. Fairfield, *Smart...*, wyd. cyt.

[31] F. Glaser, *Pervasive...*, wyd. cyt.

określałaby płatność za określony zestaw działań, które zmniejszyłyby GHG (gaz cieplarniany), na przykład przez użycie zielonej energii. Zobowiązania te można śledzić za pomocą czujników w czasie rzeczywistym, np. czujników w silnikach pojazdów, czujników w zakładzie przemysłowym, a następnie weryfikować blockchain, czy osiągnięto odpowiedni poziom. Po pozytywnej weryfikacji zostają wypłacone odpowiednie środki. Indywidualne kontrakty mogłyby zostać połączone w większe zbiory, aby stworzyć zakrojoną na szeroką skalę redukcję emisji gazów cieplarnianych. Obiekty, które są narażone na wysokie koszty redukcji emisji gazów cieplarnianych, mogłyby skutecznie kupić kredyty (z użyciem inteligentnych kontraktów na własny rachunek) w celu ograniczenia emisji gazów cieplarnianych. W efekcie powstałby system handlu GHG, który byłby odporny na oszustwa.

W Stanach Zjednoczonych jednym z ważnych problemów społecznych jest kontrola broni palnej. Obrońcy praw do posiadania broni nie godzą się na rejestrowanie lub śledzenie broni z powodów konstytucyjnych, obawiając się, że jakakolwiek rejestracja będzie krokiem w kierunku naruszającym ich wolność. Zwolennicy kontroli broni wskazują na problem użycia broni w przestępstwach oraz fakt, że legalnie zakupiona broń może zostać wykorzystana przez kogoś, kto ma złe intencje. Do chwili obecnej problem nie został rozwiązany. W modelu blockchaina możliwe byłoby wykorzystanie aplikacji Internetu Rzeczy (IoT) do stworzenia pozarządowej, ale kontrolowanej bazy danych, która rejestrowałaby zakupy i użycie broni jako transakcję na blockchainie, przy założeniu, że broń będzie rejestrowana na blockchainie w czasie produkcji. Przez całe życie broń i każdy punkt w jej historii, każde przeniesienie własności będzie rejestrowane na blockchainie. Transakcja może być prywatna, ale przy użyciu inteligentnych kontraktów może zaistnieć mechanizm, za pomocą którego można skontrolować blockchain, na przykład za pomocą nakazu przeszukania. W ramach transakcji każda ze stron byłaby chroniona przez silny standard szyfrowania, który oferuje blockchain, a rozproszony charakter systemu zapobiegałby oszustwom. Ponadto, ponieważ blockchain istnieje w przestrzeni publicznej, właściciele broni mogliby być pewni, że ich prawa własności będą minimalnie zakłócone. Jeśli broń była wyposażona w blokady biometryczne, można je wykorzystać do dowiedzenia transferu własności.

We wspólnym raporcie Fundacji Policyjnej wraz z firmą CGI z Wielkiej Brytanii[32] możemy przeczytać, że cyfryzacja i nowe technologie, w szczególności blockchain, może usprawnić procesy i połączyć usługi. Zakres technologii i potencjalnych zastosowań dla CJS (*criminal justice system*) jest szeroki. Jednocześnie większe wykorzystanie automatyzacji może poprawić szybkość i jakość wykonywania zadań, takich jak prowadzenie audytów, a w przyszłości może nawet pomóc w rozwiązywaniu problemów, takich jak subiektywne uprzedzenia w procesach decyzyjnych. Technologia blockchain może stanowić wyjątkową okazję do zwiększenia dokładno-

[32] L. Crowhurst, *Reforming justice for the digital age The Police Foundation, in partnership with CGI*, July 2017, <http://www.police-foundation.org.uk/2017/wp-content/uploads/2017/08/pf_cgi_digital_justice.pdf>, 17 września 2018 r.

ści i przejrzystości procesów dzięki bezpiecznym, możliwym do sprawdzenia rozproszonym rekordom. Ten sam raport wyjaśnia, że brytyjski system sprawiedliwości oparty jest w dużej mierze na papierowych rozwiązaniach, archaicznych praktykach i starych systemach informatycznych, które powodują jedynie nieefektywne usługi. Przykładem tego jest, że w całym systemie sądowym w Wielkiej Brytanii tylko połowa posiedzeń ma miejsce w dniu, w którym miały się odbyć, a ręczne procesy powodują niepotrzebne powielanie dokumentów i zwiększenie marginesu błędu.

Słabe punkty technologii

Chociaż blockchain jest obiecującą technologią dla reorganizacji procesów biznesowych oraz wielu zastosowań przemysłowych, wciąż ma wiele słabych punktów pomimo różnej implementacji w wielu istniejących formach.

Eksperci i analitycy ostrzegają również, że technologia nie nadaje się do każdego procesu transakcyjnego. Wdrażanie jest wolniejsze i droższe niż w przypadku tradycyjnych technologii transakcyjnych, takich jak scentralizowana relacyjna baza danych. Autonomiczność blockchaina ma duży wpływ na brak wydajności. Ponieważ nowe bloki wymagają weryfikacji kryptograficznej przed ich dodaniem do blockchaina, może to być nieefektywne dla aplikacji biznesowych, które wymagają szybkiego rozliczenia transakcji. Ze względu na swoją naturę, bloki muszą być serializowane, co oznacza, że tempo aktualizacji jest wolniejsze niż tradycyjnej bazy danych, która może aktualizować dane równolegle.

Największą zaletą blockchaina jest jednokrotny zapis i rozproszenie do węzłów. Można go łatwo rozproszyć w różnych węzłach sieci, ale mimo to każdy rekord zawiera własny skrót, co czyni go niezmiennym. Rozproszona baza oparta na blockchainie może zapewnić bogatszą, bardziej wszechstronną historię transakcji. Nie oznacza to jednak, że dane związane z transakcjami muszą być częścią tego łańcucha. Na przykład, jeśli użytkownicy blockchaina dołączyliby dane multimedialne jako część swoich transakcji, pojemność szybko wzrosłaby — podobnie jak obciążenie sieci. Z powodu dystrybucji wszystkie dane muszą być replikowane do wszystkich węzłów w łańcuchu. Dlatego dla niektórych zadań transakcyjnych lepiej korzystać jest z relacyjnej bazy danych.

Przy tworzeniu prywatnego blockchaina jego architektura jest zagadnieniem kluczowym. Aby osiągnąć konsensus, należy ogłosić i dopisać do blockchaina transakcję. Taka komunikacja musi odbywać się pomiędzy węzłami, z których każdy przechowuje kopię blockchaina i informuje inne węzły o pojawiających się nowych zdarzeniach, tj. ostatnio złożona lub ostatnio potwierdzona transakcja. Użytkownicy blockchaina mogą zarządzać informacji o tym, kto ma uprawnienia do pracy w danym węźle, a także w jaki sposób węzły są połączone. Węzeł z większą liczbą linków szybciej uzyska informacje. Podobnie — węzły mogą mieć możliwość utrzymywania liczby linków, które są aktywne. Węzeł, który ogranicza przekaz informacji lub przekazuje niedokładne informacje, musi być traktowany

szczególnie i obchodzony w transmisji, aby dbać o uczciwość systemu. Prywatny blockchain realizujący np. handel surowcami może wymagać bardziej centralnej pozycji w sieci w celu rozwijania sieci partnerów handlowych. Może także wymagać nowych węzłów do utrzymywania połączenia z jednym z tych centralnych węzłów jako środka bezpieczeństwa, aby upewnić się, czy ich zachowanie jest zgodne z oczekiwaniami.

Innym problemem związanym z bezpieczeństwem w tworzeniu architektury sieci jest przyjęty sposób traktowania węzłów niekomunikatywnych lub nieregularnie aktywnych. Węzły mogą zostać wyłączone także z nieszkodliwych przyczyn, ale sieć musi być przygotowana do normalnego działania — uzyskanie konsensusu we wcześniej zweryfikowanych transakcjach i poprawna weryfikacja nowych transakcji bez węzłów wyłączonych (*offline*). Sieć musi także być w stanie bardzo szybko przywrócić węzły do działania, jeśli staną się aktywne.

Inteligentne kontrakty są jedną z bardziej atrakcyjnych funkcji blockchaina, ponieważ obniżają lub nawet całkowicie redukują koszty administracyjne związane z brakiem zaufania w transakcji. Po spełnieniu określonych warunków umowy, pieniądze, własność lub towary są zwalniane automatycznie, podobnie jak w obrocie handlowym przy arbitrażu z udziałem trzeciej strony, np. banku, instytucji kontrolującej jakość lub osoby zaufania publicznego.

Na przykład firma ubezpieczeniowa może wykorzystywać inteligentne kontrakty do wypłacania roszczeń ze zdarzeń, takich jak huragany, susze czy opóźnienie samolotu. Można jednak mieć wątpliwość, ponieważ wspomniane inteligentne kontrakty nie są zarówno inteligentne, jak również nie są kontraktami w sensie prawnym. Są one tak naprawdę formą automatyzacji i przyspieszenia procesów biznesowych. Aby przeprowadzić automatyzację procesów biznesowych, należy uzgodnić, czym ma być ten proces i jakie zasady mają obowiązywać w tym procesie transakcji, a następnie precyzyjnie zapisać to w postaci wykonywalnego kodu.

Jednak brak dojrzałości języka skryptowego do zapisu reprezentacji kontraktu w języku programowania prowadzić może do błędów lub luk w zabezpieczeniach, które nie zostaną dostrzeżone lub obsłużone. Użytkownicy blockchaina muszą również ustalić między sobą — jako warunki kontraktu — co stanie się w przypadku sporu w wykonywaniu zawartej umowy. Jeśli wydarzy się coś, co nie zostało zapisane w kodzie kontraktu — niezależnie od świadomej lub nieświadomej przyczyny — to musi istnieć sposób naprawienia lub zatrzymania kodu.

Tworzenie nowego procesu biznesowego jako świadome działanie wymaga również ustanowienia porozumienia w sprawie różnych warunków, w tym prawnych. Istnieją przypadki blokowania projektów blockchainowych, ponieważ strony nie osiągnęły porozumienia w sprawie wszystkich warunków, na jakich powinno się prowadzić to działanie (kontrakt transakcyjny). W istocie przełożenie warunków transakcji w różnych aspektach na zapis formalny w języku skryptowym jest kluczowe dla bezpieczeństwa takiej operacji, przy której użycie blockchaina może pomóc, ale nie zastąpi prawidłowej analizy i przygotowania przedsięwzięcia.

Niebezpieczeństwa

Przyjmuje się, że rozpowszechnienie technologii blockchain rozpoczęło się od powstania serwisu *online*, na którym można było kupić narkotyki. Internetowa platforma aukcyjna Silk Road, działająca w sieci TOR, została zamknięta w 2013 r. przez organy ścigania USA. Większość oferowanych przez sprzedawców towarów była nielegalna. Handlowano na niej m.in. narkotykami, co odbywało się za zgodą i wiedzą twórcy platformy. Niedozwolone było natomiast oferowanie przedmiotów i usług, które jednoznacznie szkodziłyby innym ludziom, m.in. dziecięcej pornografii, broni masowego rażenia, kradzionych kart kredytowych. Silk Road była platformą, gdzie po raz pierwszy większość ludzi usłyszała o bitcoinach i kryptowalutach. Po transakcjach wartych ponad miliard dolarów w ciągu nieco ponad dwóch lat Silk Road został zamknięty po śledztwie FBI. Pomimo tego technologia kryjąca się za giełdą narkotyków — technologia blockchain — jest obecnie reklamowana jako najbardziej rewolucyjna od czasu powstania Internetu.

Do wykonania analiz publicznej bazy blockchain potrzebne jest specjalne oprogramowanie, które pozwala przejrzeć informacje, a następnie zinterpretować, które transakcje wydają się być podejrzane. Staje się to coraz trudniejsze, ponieważ użytkownicy przenoszą się do anonimowych systemów kryptowalutowych. W niedawnym raporcie Europolu, unijnej agencji policyjnej, można było przeczytać, że „kryptowaluty takie jak Monero, Ethereum i Zcash zyskują popularność w cyfrowym podziemiu”[33]. Oferując zaawansowane funkcje prywatności, Monero i Zcash ukrywają nadawcę, odbiorcę oraz wartość transakcji, co prawie uniemożliwia prowadzenie śledztwa. Zespół, który stoi za Zcashem, twierdzi, że fakt, że istnieje zwiększona prywatność, nie oznacza, że istnieją dowody na użycie systemu w celach przestępczych. Jednak pomimo dodatkowych zabezpieczeń w kierunku prywatności, czynnikiem ułatwiającym analizę jest moment, kiedy przestępcy próbują wypłacić lub zamienić pieniądze na dolary lub euro, które w regulowanych giełdach można prześledzić.

Phishing jest głównym trendem w działalności przestępców w sieciach blockchainowych, gdzie przestępcy stosują zwykle spreparowany link e-mailowy. Badania wykazały ponad 115 milionów dolarów skradzionej wartości u prawie 17 000 ofiar tylko w blockchainie Ethereum. *Cryptophishing* jest ukierunkowany na potencjalnych inwestorów i powoduje wysyłanie pieniędzy pod zły adres za rzekomą przedsprzedaż tokenów we wstępnej ofercie publicznej (Initial Coin Offering, ICO), a Twitter często rozpowszechnia dezinformację. Zarzuty dotyczące dezinformacji są dosyć powszechne w czasie trwania oferty ICO.

Jak do tej pory nie udało się całkowicie złamać żadnego systemu opartego na blockchainie. Jednak oprogramowanie, które jest budowane na tej

[33] Internet Organised Crime Threat Assessment (IOCTA) 2017, 27 September 2017, s. 11, <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>, 17 września 2018 r.

infrastrukturze ma wiele niedociągnięć. Przykładem jest fundusz venture capital, zwany DAO, który w 2016 r. zebrał ponad 150 milionów dolarów w jeden miesiąc (wówczas największe wydarzenie crowdfundingowe w historii) — a miesiąc później złodzieje wykorzystali lukę w kodzie DAO, aby ukraść ponad 74 miliony dolarów od 11 000 inwestorów. Również w 2016 r. BitFinex stracił z powodu kradzieży 120 000 bitcoinów o wartości 68 milionów dolarów. Raporty wskazały na użycie przez Bitfinex portfela BitGo od dostawcy, który mógł mieć luki w oprogramowaniu.

Jak się szacuje, w sumie około 10% pieniędzy zainwestowanych w ICO na bazie Ethereum trafiło w ręce przestępców. Pomimo teoretycznie bezpiecznych sieci blockchain, technologia ta niekoniecznie jest całkowicie bezpieczna. Biorąc pod uwagę wartość włożoną obecnie w kilka głównych blockchainów, tj. Bitcoin i Ethereum, kod tego oprogramowania musi być idealny. Pomimo że oprogramowanie typu *open source* ułatwia wyszukiwanie luk, jeśli w oprogramowaniu systemu pojawi się błąd, możemy mówić o kradzieży miliardów dolarów, wyłudzonych przez hakerów, jeszcze zanim ludzie dowiedzą się o tym.

Zakończenie

Technologia blockchain umożliwia jednostkom tworzenie sieci wymiany bez fizycznej trzeciej strony transakcji przez zastosowanie nadzoru lub zarządzanie ryzykiem kontrahenta w postaci wirtualnej jako działający algorytm stworzony na podstawie ustaleń transakcyjnych. W związku z tym sieci blockchain są zasadniczo pozbawione zaufania, ponieważ nie wymagają wzajemnej znajomości lub zaufania stron w sieci. Powstanie sieci blockchain umożliwia jednostkom realizację działań, które poprzednio opierały się na kontroli instytucjonalnej: rządowej lub podobnego typu instytucji zaufania publicznego. Blockchain może zastąpić nadzór rządu lub jego agend w obszarach, w których jednostki prowadzące transakcje różnego typu widzą potrzebę uregulowania wspólnych działań, ale nie ufają rządom lub innym instytucjom. W środowisku o niskim poziomie zaufania blockchain realizuje mechanizm, za pomocą którego jednostki mogą współpracować bez ingerencji i interwencji osób trzecich nadzorujących lub kontrolujących. Jednak takie przypadki nie są ograniczone do krajów rozwijających się. Wiele problemów w krajach rozwiniętych może zostać rozwiązanych przez wykorzystanie blockchaina do ustanowienia dobrowolnych, samozachowawczych systemów regulacyjnych. Podobnie w różnych typach kontraktów pomiędzy stronami, które są elementami systemu władzy (centralnej i lokalnej), przedsiębiorczości lub całej sfery specjalizowanych usług.

Technologia blockchain zasadniczo zastępuje wewnętrzne zaufanie między ludźmi lub podmiotami korporacyjnymi za pomocą reguł matematycznych. Niestety mocne zabezpieczenia wymagają dużej mocy obliczeniowej i stają się drogie. Ten kosztowny i powolny proces jest uzasadniony dla globalnej sieci, w której wszyscy uczestnicy mogą potencjalnie być złośliwi. W zamkniętym środowisku korporacyjnym nie ma sensu poświęcać energii i czasu dla

zasadniczo żadnych dodatkowych korzyści. Działając w środowisku komercyjnym, całkowita przejrzystość nie jest zazwyczaj dobra. Na przykład, jeśli technologia blockchain jest wykorzystywana jako część platformy obrotu giełdowego jako mechanizm do natychmiastowego rozliczenia, każdy użytkownik blockchaina może zobaczyć, co robi inny użytkownik, co pozwoliłby na nieuczciwą grę przeciwko drugiemu podmiotowi. W innym przykładzie, jeśli producent wykorzystuje blockchain dla swoich dostawców, umożliwiłoby to jednemu wykonawcy natychmiastową obserwację wszystkich innych podwykonawców zapisanych w blockchainie, co niekoniecznie jest pożądane z przyczyn konkurencyjności i zachowania przewagi w różnych aspektach.

Bibliografia

Literatura

Atzei N., Bartoletti M., Cimoli T., *A survey of attacks on Ethereum smart contracts SoK*, „Principles of Security and Trust" 2017, Vol. 10204.

Beck R. i in., *Blockchain — The Gateway to Trust — free Cryptographic Transactions*, 24th European Conference on Information Systems (ECIS), Istanbul, Turkey, 2016.

Crosby M. i in., *Blockchain technology: Beyond bitcoin*, "Applied Innovation Review" 2016, No. 2.

English M., Auer S., Domingue J., *Block Chain Technologies & The Semantic Web: A Framework for Symbiotic Development*, Computer Science Conference for University of Bonn Students, Bonn, Germany 2016.

Fairfield J., *Smart contracts, Bitcoin bots, and consumer protection*, "Washington and Lee Law Review Online" 2014, Vol. 71.

Glaser F., Bezzenberger L., *Beyond Cryptocurrencies — A Taxonomy of Decentralized Consensus Systems*, Proceedings of the 23rd European Conference on Information Systems (ECIS 2015), Muenster, Germany 2015.

Glaser F., *Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis*, Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS 2017), Waikoloa Village, Hawaii 2017.

Glaser F. i in., *Bitcoin–asset or currency? Revealing users' hidden intentions*, Proceedings of the 22nd European Conference on Information Systems (ECIS 2014), Tel Aviv 2014.

Konstantinidis I. i in., *Blockchain for Business Applications: A Systematic Literature Review*, International Conference on Business Information Systems, Springer Cham 2018.

Kosba A. i in., *Hawk: The blockchain model of cryptography and privacy-preserving smart contracts*, *2016 IEEE symposium on security and privacy (SP)*, Vol. 1.

Luther W.J., White L.H., *Can bitcoin become a major currency*?, "Working Paper in Economics" 2014, No. 14–17.

Mishkin F.S., *The economics of money and financial markets*, Boston 2004.
Swan M., *Blockchain. Blueprint for a New Economy*, Sebastopol 2015.
Szabo N., *Smart contracts: formalizing and securing relationships on public networks*, "First Monday" 1997, Vol. 2, No. 9.
Weber I. i in., *Untrusted Business Process Monitoring and Execution Using Blockchain*, Springer, Cham 2016.

Inne

Atzori M., *Blockchain technology and decentralized governance: Is the state still necessary*?, <https://ssrn.com/abstract=2709713>, 21 października 2019 r.
Buterin V., *A next-generation smart contract and decentralized application platform*, <http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf>, 21 października 2019 r.
Crowhurst L., *Reforming justice for the digital age The Police Foundation, in partnership with CGI*, July 2017, <http://www.police-foundation.org.uk/2017/wp-content/uploads/2017/08/pf_cgi_digital_justice.pdf>, 17 września 2018 r.
European Central Bank, Virtual Currency Schemes, 2012, <https:// www.ecb.europa.eu/pub/pdf/other/virtualcurrencyscheme s201210en.pdf>, 30 listopada 2016 r.
Federal Bureau of Investigation, *Bitcoin virtual currency: intelligence unique features present distinct challenges for deterring illicit activity*, 2012, <https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf>, 30 listopada 2016 r.
Internet Organised Crime Threat Assessment (IOCTA) 2017, 27 September 2017, <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>, 17 września 2018 r.
Mattila J., *The Blockchain Phenomenon — The Disruptive Potential of Distributed Consensus Architectures*, The Research Institute of the Finnish Economy, 2016, <https://ideas.repec.org/p/rif/wpaper/38.html>, 21 października 2019 r.
Nakamoto S., *Bitcoin: A Peer-to-peer Electronic Cash System*, 2008, <https:// bitcoin.org/bitcoin.pdf>, 17 września 2018 r.
Sachs G., *Profiles in Innovation — Blockchain*, <http:// www.the-blockchain.com/docs/Goldman-Sachs-report-Blockchain-Putting-Theory-into-Practice.pdf>, 30 listopada 2016 r.
Yli-Huumo J. i in., *Where Is Current Research on Blockchain Technology? A Systematic Review*, "PloS one" 2016, No. 11, Vol. 10, <https://doi.org/10.1371/journal.pone.0163477>, 21 października 2019 r.

DOI: 10.5604/01.3001.0014.1135
http://dx.doi.org/10.5604/01.3001.0014.1135

Słowa kluczowe: blockchain, smart kontrakt, bezpieczeństwo, innowacja, kryptowaluta, bitcoin, Ethereum, proof-of-work

Streszczenie: Blockchain to jedna z najbardziej rewolucyjnych technologii XXI w., która wciąż rozwija się i której potencjał nie jest jeszcze w pełni zrealizowany. Mimo że blockchain zyskał na znaczeniu w roku 2009, naukowcy i przedsiębiorcy nie są w stanie nadal zrozumieć jego mechanizmów i w pełni docenić jego potencjału, zwłaszcza z perspektywy technicznych wyzwań i ograniczeń technologii. Blockchain znajduje różnorodne zastosowania, szczególnie w obszarach, które dotychczas bazują w transakcji na trzeciej stronie w celu utrzymania określonego poziomu zaufania. Chociaż blockchain jest obiecującą technologią dla reorganizacji procesów biznesowych oraz wielu zastosowań przemysłowych, wciąż ma wiele słabych punktów pomimo różnej implementacji w wielu istniejących formach. Innowacyjnym elementem i jednym z bardziej atrakcyjnych funkcji blockchaina są inteligentne kontrakty, ponieważ obniżają lub nawet całkowicie redukują koszty administracyjne związane z brakiem zaufania w transakcji. Jednak istniejące oprogramowanie, które jest budowane z wykorzystaniem tej infrastruktury, ma wiele niedociągnięć i niestety w połączeniu z brakiem dojrzałości języka skryptowego do zapisu reprezentacji kontraktu w języku programowania prowadzi do błędów lub luk w zabezpieczeniach, które nie zostają dostrzeżone lub obsłużone przez autora skryptu. Jak do tej pory nie udało się całkowicie złamać żadnego systemu opartego na blockchainie. Niemniej jednak phishing jest głównym trendem w działalności przestępców w sieciach blockchainowych. Badania wykazały ponad 115 milionów dolarów skradzionej wartości u prawie 17 000 ofiar tylko w blockchainie Ethereum. Jak szacuje się, w sumie około 10% pieniędzy zainwestowanych w ICO na bazie Ethereum trafiło w ręce przestępców.