

Rafał Boniecki

Uniwersytet Technologiczno-Przyrodniczy w Bydgoszczy  
Wydział Telekomunikacji i Elektrotechniki  
Zakład Systemów Teleinformatycznych  
e-mail: raboni@utp.edu.pl

Józef Rawłuszko

### Możliwości wykorzystania technologii Blockchain w biznesie

**Kody JEL:** L86, G20, D 18, O39

**Słowa kluczowe:** Blockchain, bitcoin, technologia rozproszonych rejestrów

**Streszczenie.** W artykule omówiono zasady działania technologii Blockchain wykorzystanej do stworzenia kryptowaluty bitcoin. Przedstawiono analizę SWOT oraz zarys możliwych dalszych trendów rozwojowych tej technologii rozproszonych rejestrów w biznesie.

#### Wprowadzenie

Bitcoin jest kryptowalutą, która wzbudza w ostatnim czasie wzrastające zainteresowanie nie tylko informatyków i finansistów. Przyczyną tego zainteresowania są wyjątkowe właściwości transakcji realizowanych przy wykorzystaniu bitcoinów (Homa, 2015, Szymankiewicz, 2014). Tę wyjątkowość transakcji bitcoinowych stwarza technologia Blockchain, której koncepcja została opracowana i przedłożona do publicznego użytkowania w styczniu 2009 roku przez Satoshi Nakamoto. Rozpowszechnienie idei wykorzystania bitcoinów w transakcjach biznesowych realizowanych przez internet wywołuje w wielu krajach lawinowy wzrost podmiotów zajmujących się tą tematyką. Szybko też zaczęto dostrzegać, że technologia Blockchain stwarza możliwości szerokiego jej wykorzystania w różnych dziedzinach życia społecznego i gospodarczego.

## 1. Istota technologii BlockChain

W języku polskim nazwa „BlockChain” jest najczęściej tłumaczona jako technologia rozproszonych rejestrów, gdyż w tym przypadku do realizacji transakcji biznesowych i weryfikacji ich poprawności używa się wielopodmiotowego protokołu kryptograficznego. W przeciwieństwie do ksiąg rozliczeniowych w dotychczasowym, tradycyjnym wariacie scentralizowanej księgowości biznesowej, w technologii BlockChain księgi te są rozproszone wśród węzłów sieci, czyli potencjalnie wśród wszystkich użytkowników korzystających z tej technologii.

W sieci realizującej transakcje z użyciem bitcoinów uczestnicy dzielą się na zwykłych użytkowników oraz na „miners” (kopaczy/górników). Rola tych ostatnich polega na weryfikacji i uwierzytelnianiu wszystkich transakcji dokonanych w sieci. Zadanie to sprowadza się w istocie do zadania matematycznego znalezienia niewiadomej  $X$  w funkcji nieodwracalnej, spełniającej nierówność:

$$f(a,x) < c,$$

lub też w innym zapisie:

$$\text{Sha } 256(a,x) < c, \text{ gdzie:}$$

$a$  – jest liczbą kodującą dotychczasową historię transakcji realizowanej w bitcoinach,

$c$  – jest liczbą specjalnie dobranej i uaktualnianej w określonych odstępach czasu,

Sha (256) – jest algorytmem szyfrującym Satoshiego.

Algorytm Satoshiego zapewnia największe jak dotychczas bezpieczeństwo kryptograficzne zapisu pakietu przesyłanej informacji między węzłami sieci (w algorytmie Satoshiego używa się kluczy publicznego i prywatnego o wymiarze  $2^{256}$ ).

Zadaniem „górników” jest odkrycie tej nierówności, które to rozwiązanie można znaleźć jedynie losowo, przeliczając kolejne warianty.

Zwycięzcą wśród „górników” zostaje w danym okresie ten, który znajdzie najszybciej rozwiązanie dla największego łańcucha dokonanych transakcji. Za znalezienie tego rozwiązania (a tym samym weryfikację i uwierzytelnienie wszystkich dotychczasowych dokonanych transakcji) „górnik” otrzymuje nagrodę w postaci nowych bitcoinów (obecnie jest to 12,5 bitcoinów), które może następnie wykorzystywać w dowolny sposób.

## 2. Cechy technologii rozproszonych rejestrów

Przy założeniu, że większość użytkowników występujących w sieci jest uczciwa (a w szczególności większość tzw. górników), technologię rozproszonych rejestrów rozliczeniowych cechuje niezaprzeczalność i niefałszowalność przeprowadzanych

transakcji biznesowych. Wynikają stąd niżej wymienione korzyści stosowanej technologii:

- wzrost cyberbezpieczeństwa sieci internetowej,
- duże ułatwienie dla osób z utrudnionym dostępem do bankowości w wymiarze ogólnosięwiatowym,
- ułatwienie i przyspieszenie płatności w obrocie ogólnosięwiatowym,
- tworzenie globalnej sieci zaufania społeczności internetowej (wyeliminowanie tzw. trzeciej zaufanej strony występującej w tradycyjnym obrocie biznesowym),
- łatwość uzyskania potwierdzenia dokonanych transakcji,
- radykalne ograniczenie możliwości fałszowania dokumentów, a zwłaszcza antydatowania transakcji,
- ochrona danych związanych z pierwszeństwem publikowania/emisji określonych plików.

Jest rzeczą oczywistą, że oprócz zalet w technologii rozproszonych rejestrów można dostrzec i jej mankamenty. Wydaje się ponadto, że technologia ta stwarza duże możliwości rozwojowe, ale również zagrożenia związane z jej stosowaniem.

Kwestie te skrótowo przedstawiono w analizie SWOT w tabeli 1.

### 3. Możliwości wykorzystania technologii Blockchain w innych dziedzinach

W literaturze poświęconej kryptowalucie bitcoin przeważa pogląd, że pomimo trzech „baniek spekulacyjnych”, do jakich doszło od czasu jego stworzenia, technologia ta znajduje się na początkowym, wznoszącym odcinku krzywej Gartnera. Jednocześnie, wyjątkowe właściwości technologii rejestrów rozproszonych nasuwają pomysły na jej zastosowanie w innych dziedzinach gospodarki i życia społecznego.

Można jednoznacznie stwierdzić, że technologia rozproszonych rejestrów wzbudza narastające szybko zainteresowanie głównych światowych firm informatycznych oraz sektora finansowego.

Szacuje się, że nad rozwojem tej technologii pracuje aktualnie w świecie ponad 20 tys. informatyków. W realizację projektów z wykorzystaniem technologii Blockchain włączyły się nie tylko największe koncerny informatyczne (np. Microsoft) i banki, lecz również nowe, specjalnie tworzone w tym celu firmy, np. BlockApps STRATO, Hydrachain, Parity, Dfinity, Raiden.

Jednocześnie łatwo znaleźć w internecie strony i blogi wymiany informacji związanych z nowymi zastosowaniami technologii rozproszonych rejestrów (np. [ameer@blockgeeks.com](mailto:ameer@blockgeeks.com)).

Tabela 1. Analiza SWOT technologii rozproszonych rejestrów

Mocne strony	Słabe strony
<ul style="list-style-type: none"> <li>- niezaprzeczalność transakcji</li> <li>- transparentność dokonywanych operacji</li> <li>- możliwości dokonywania transakcji w skali ogólnoświatowej</li> <li>- wzrost zaufania społecznego do prowadzenia biznesu w skali ogólnoświatowej</li> <li>- wzrost szybkości realizacji transakcji</li> <li>- duży potencjał innowacyjny dla dalszego rozwoju</li> <li>- kolejny etap przenoszenia biznesu w świat cyfrowy (umowy typu „smart contracts”)</li> </ul>	<ul style="list-style-type: none"> <li>- ograniczenie poufności umów handlowych (zaś „biznes lubi dyskrecję”)</li> <li>- łatwość powstawania baniek spekulacyjnych (w kilkuletniej historii bitcoinów wystąpiły już trzy zidentyfikowane bańki spekulacyjne)</li> <li>- radykalny, stały wzrost zapotrzebowania na zasoby systemowe w węzłach kopaczy (przy obliczeniach weryfikacyjnych trzeba pamiętać historię wszystkich transakcji dokonanych w sieci)</li> <li>- brak zabezpieczenia użytkowników przed przypadkowymi błędami np. zapis adresu transakcji</li> <li>- brak jasności sytuacji prawnej i podatkowej uczestników transakcji w sieci BlockChain</li> </ul>
Szanse	Zagrożenia
<ul style="list-style-type: none"> <li>- poszerzenia zastosowań na inne strefy życia społecznego i gospodarczego</li> <li>- tworzenie innych krypto-walut</li> <li>- tworzenie innych sieci w technologii rozproszonych rejestrów</li> <li>- stworzenie współdzielonego rozproszonego rejestru z dostępem użytkownika tylko do swojej części</li> <li>- stworzenie otoczenia prawnego wspierającego rozwój technologii rozproszonych rejestrów</li> </ul>	<ul style="list-style-type: none"> <li>- wzrost wymagań obliczeniowych grozi radykalnym zmniejszeniem zespołów kopaczy (górników), a tym samym wzrasta ryzyko monopolizacji przez grupy o mniejszym zaufaniu publicznym</li> <li>- wraz z radykalnym wzrostem liczby transakcji wzrośnie ryzyko, że kopacze będą pracować „na siebie” pomijając przy weryfikacji niektóre transakcje lub grupy transakcji</li> </ul>

Przykłady istniejących rozwiązań, lub proponowanych propozycji wykorzystania technologii BlockChain:

- projekt stworzenia weryfikacji dostaw i płatności w obrocie międzynarodowym,
- stworzenie kryptowaluty bitcoin i upowszechnienie rozliczeń transakcyjnych w tej walucie na obszarze całego świata,
- stworzenie sieci Ethereum, pełniącej funkcję platformy wykorzystującej technologię rejestrów rozproszonych i umożliwiającej każdemu tworzenie aplikacji do kodyfikowania, decentralizacji i handlu dowolnymi towarami i usługami,
- projekt wykorzystania technologii BlockChain w takich dziedzinach sektora publicznego jak: monitorowanie zanieczyszczeń powietrza, rejestracja pojazdów, rozliczenia mandatów za wykroczenia drogowe, prowadzenie ksiąg wieczystych, ubezpieczenia konsumenckie,
- projekt stworzenia sieci wypożyczania ogólnie dostępnych pojazdów mechanicznych,

- projekty tworzenia własnych kryptowalut przez banki centralne niektórych państw,
- projekty ochrony wrażliwych danych przesyłanych w sieci, np. pozyskiwanych w badaniach medycznych.

## Podsumowanie

Technologia BlockChain (tj. technologia rozproszonych rejestrów) wyróżnia się wieloma istotnymi zaletami ułatwiającymi prowadzenie biznesu w świecie cyfrowym. Pomimo pewnych mankamentów i zagrożeń, jakie może wygenerować, stwarza olbrzymie szanse na dalszy rozwój i szerokie zastosowanie w życiu gospodarczym i społecznym (patrz – powyższa analiza SWOT). Jest ze wszech miar wskazane, by w prace nad rozwojem technologii rozproszonych rejestrów włączyło się jak najszersze grono informatyków, ekonomistów, menadżerów i prawników w Polsce.

## Bibliografia

- Homa, D. (2015). *Sekrety bitcoina i innych kryptowalut. Jak zmienić wirtualne pieniądze w realne zyski*. Gliwice: Helion/OnePress.
- Szymankiewicz, M. (2014). *Bitcoin. Wirtualne waluta internetu*. Gliwice: Helion/OnePress.
- W pracy wykorzystano ponadto informacje z materiałów umieszczonych na blogach dyskusyjnych poświęconych technologii BlockChain, a w szczególności: [ameer@blockgeeks.com](mailto:ameer@blockgeeks.com); [Bitcoinmagazine.com](http://Bitcoinmagazine.com).

## POSSIBILITIES OF MAKING THE MOST OF THE BLOCKCHAIN TECHNOLOGY IN BUSINESS

**Keywords:** BlockChain, bitcoin, distributed ledger technology

**Summary.** The principles of the BlockChain technology used for creating bitcoins were shortly described. The SWOT analysis for this technology and the outlook of further development trends for business applications were presented.

*Translated by Józef Rawłuszko*

## Cytowanie

Boniecki, R., Rawłuszko, J. (2017). Możliwości wykorzystania technologii blockchain w biznesie. *Ekonomiczne Problemy Usług, 1* (126/2), 9–13. DOI: 10.18276/epu.2017.126/2-01.