

Decentralizacja a blockchain

Krzysztof Piech

23. Konferencja pt. „Miasta w Internecie”

Warszawa, 27.06.2019



dr hab. Krzysztof Piech, prof. UŁa



Koordynator
Polski Akcelerator
Technologii Blockchain



Lider Biznesowy
2016-18 Strumień „Blockchain
/ DLT i Waluty Cyfrowe”



Dyrektor
Centrum Technologii
Blockchain UŁa



Członek Zarządu
Polskie Stowarzyszenie
Bitcoin



Prezes
Instytut
Wiedzy i Innowacji



Członek
Polskie Towarzystwo
Ekonomiczne



Struktura prezentacji

1. Znaczenie decentralizacji
2. Bitcoin, blockchain i tokeny: początki i podstawowe pojęcia
3. Zastosowania blockchain w turystyce
4. Wnioski dla regionu

Znaczenie decentralizacji



Rodzaje sieci komputerowych

- „Klasyczny” wykres polskiego inżyniera Barana (sprzed 50 lat).
- Schemat aktualny 50 lat temu, ale nie współcześnie.
- Rozproszone obliczenia (np. Seti@Home) wymagają centralnego komputera.
- Internet jest rozproszony, ale nie wszystkie węzły są sobie równe – sieć zdecentralizowana.
- BitTorrent to sieć P2P (rozproszona).
- TOR czy Bitcoin to sieci zdecentralizowane.

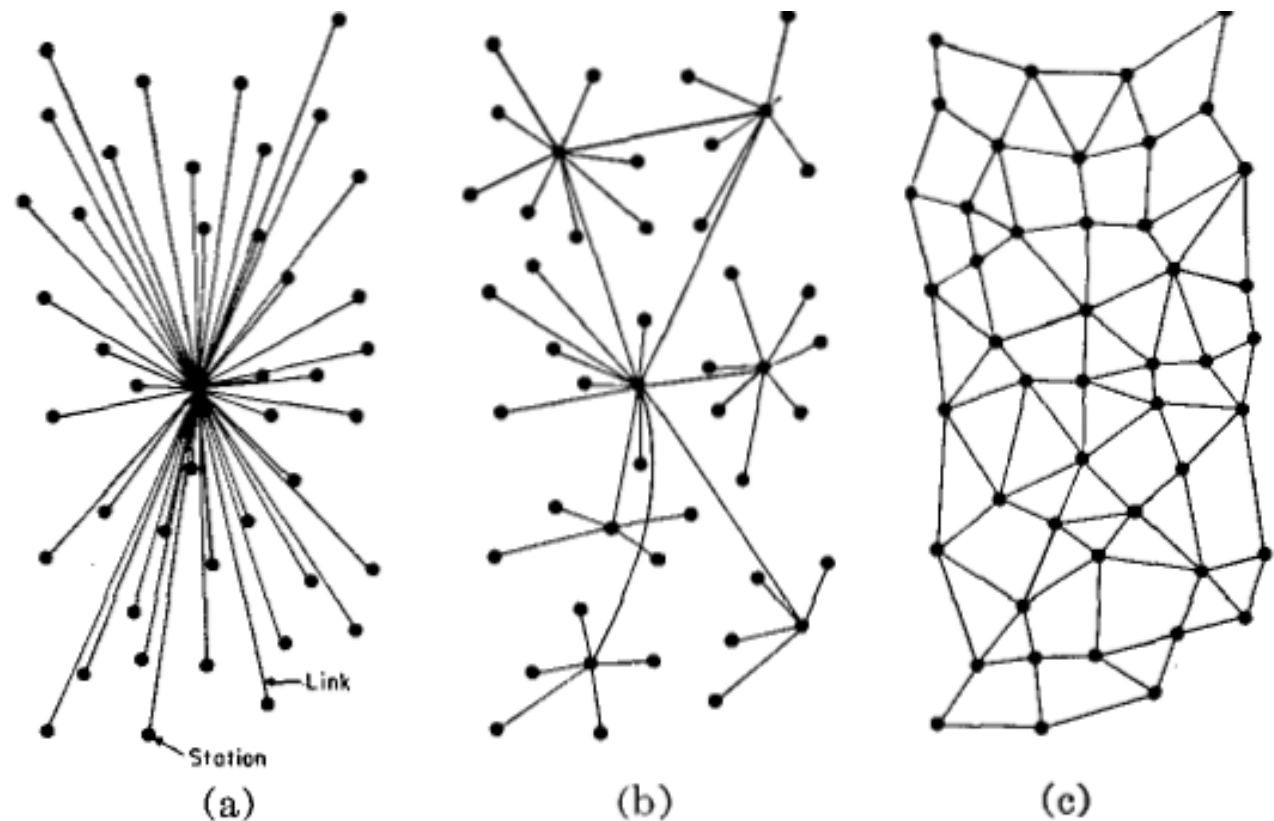


Fig. 1—(a) Centralized. (b) Decentralized. (c) Distributed networks.

Wymiary decentralizacji (wg V. Buterina)

1. Decentralizacja architektoniczna

- Z ilu fizycznych komputerów składa się system?
- Awarię ilu komputerów w danym czasie sieć może tolerować?

2. Decentralizacja polityczna

- Ile osób lub organizacji kontroluje komputery, z których składa się system?

3. Decentralizacja logiczna

- Czy interfejs i struktury danych, które system prezentuje i utrzymuje, wyglądają bardziej jak pojedynczy monolityczny obiekt lub amorficzny rój?
- Heurystyka: jeśli przetnie się system na połowy, włączając w to zarówno dostawców usług, jak i użytkowników, czy obie połowy będą w pełni funkcjonować jako niezależne jednostki?

V. Buterin, The Meaning of Decentralization, 6 lutego 2017 r.,
<https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274>

Decentralizacja - przykłady

- Firmy są scentralizowane politycznie (1 szef), architektonicznie (jedno główne biuro) i logicznie (nie można ich przeciąć na pół).
- Języki są logicznie, politycznie i architektonicznie zdecentralizowane.
- Łańcuchy bloków (blockchain) to sieci:
 - zdecentralizowane politycznie (nikt ich nie kontroluje)
 - zdecentralizowane architektonicznie (brak infrastrukturalnego centralnego punktu awarii), ale są
 - scentralizowane logicznie (istnieje jeden powszechnie uzgodniony stan i system zachowuje się jak pojedynczy komputer).

Dlaczego decentralizacja jest korzystna?

Według Buterina:

- **Odporność na awarie** - zdecentralizowane systemy są mniej narażone na awarię, ponieważ polegają na wielu oddzielnych komponentach, których jednoczesna awaria nie jest prawdopodobna.
- **Odporność na ataki** - zdecentralizowane systemy są droższe w atakowaniu i niszczeniu lub manipulowaniu, ponieważ brakuje im wrażliwych punktów centralnych, które można zaatakować, a koszt ataku na system byłby droższy, niż tenże system.
- **Odporność na zmowę** - uczestnikom zdecentralizowanych systemów znacznie trudniej jest działać w sposób korzystny dla nich kosztem innych uczestników, podczas gdy kierownictwo korporacji i rządy działają w sposób korzystny dla siebie, ale w sposób szkodzący mniej skoordynowanym obywatelom, klientom, pracownikom i ogółowi społeczeństwa.

Osiągnięcie wielowymiarowej decentralizacji nie jest łatwe, nawet w blockchain.

Blockchain – podstawowe cechy

- Rozwiązanie 2 ważnych problemów informatycznych doby internetu:
 - **Niezaprzeczalność zapisu** – wzajemnie „patrzące sobie na ręce” tysiące komputerów weryfikujących stan zapisu
 - Brak możliwości „**podwójnego wydania**” środków, podwójnego sprzedania czegoś, wielokrotnego skopiowania jednostek wartości
- Duże możliwości zapewnienia prywatności, przy jednoczesnych możliwościach śledzenia przepływu wartości (bitcoinów, tokenów)
- Możliwości tworzenia nowych „bytów” (osób „cyfrowych”) – zdecentralizowanych aplikacji (dApp), autonomicznych organizacji (DAO)

An aerial, high-angle view of the New York City skyline, featuring numerous skyscrapers and buildings. The Empire State Building is prominent in the center. The image is slightly faded, serving as a background for the text.

Bitcoin, blockchain i tokeny

Początki i podstawowe pojęcia

Początki

- ✧ Historia technologii blockchain mierze zaczyna się od **bitcoina** (publikacja założeń 2008 r., uruchomienie sieci – styczeń 2009 r.).
- ✧ Wyjątek: Estonia.
 - ❖ Rozwiązanie KSI firmy Guardtime (data powstania: 2007 r.) – kryptografowie z tej firmy byli jednymi z prekursorów rozwiązań używanych w bitcoinie.
 - ❖ To było wtedy dość proste rozwiązanie (w porównaniu do Bitcoina).
 - ❖ Ze względu na brak wbudowanych bodźców ekonomicznych (w tym brak możliwości spekulacji), KSI nie stało się tak popularne jak Bitcoin.

Bitcoin i blockchain

- * Technologia blockchain początkowo nie była znanym pojęciem.
 - ❖ To słowo nawet nie występowało w „białej księdze” bitcoina Satoshiego Nakamoto.
- * Bitcoin początkowo, jak wiele innych nowych technologii, stał się znany wśród fascynatów nowych technologii (geeków), tzw. „antysystemowców” oraz wśród zaawansowanych technologicznie przestępców (SilkRoad).
- * Ze względu na wbudowane bodźce ekonomiczne, stworzone dla ochrony sieci, szybko stał się nie tyle systemem płatności (jak to przewidywał Nakamoto), ale przedmiotem spekulacji.
- * Spektakularne wyniki na spekulacji spowodowane były efektami ubocznymi „ekonomii bitcoina”, tj. sztywna krzywa podaży i elastyczna krzywa popytu, co w efekcie musiało skutkować niestabilnością cenową, a w sytuacji szybkiej adaptacji rozwiązania – wzrostem cen.

Ethereum i smart kontrakty

- Bitcoin jest – z dzisiejszego punktu widzenia – prostym, wolnym oraz drogim w utrzymaniu systemem. Umożliwia jedynie przesyłanie wartości (i zapisywanie dość prostych treści).
- System Ethereum posiada kompletny (*Turing complete*) **język programowania** (Solidity), dzięki któremu możliwe stało się tworzenie programów komputerowych uruchamianych nie na jednym, lokalnym komputerze – ale na ich rozproszonej sieci.
 - Dobrze zaprojektowane inteligentne umowy (smart kontrakty) są bardzo bezpieczne.
 - Powstają zdecentralizowane aplikacje. Dzięki smart kontraktów można też tworzyć autonomiczne, zdecentralizowane organizacje (DAO).
- Kryptowaluty stały się więc czymś więcej, niż tylko systemem płatności czy przedmiotem spekulacji.

Inne blockchainya i tokeny cyfrowe

- * Powstają kolejne blockchainya, w tym również tak zaawansowane, że są w stanie obsługiwać smart kontrakty. Rośnie konkurencja między rozwiązaniami technologicznymi.
 - * Stają się one coraz szybsze, tańsze w utrzymaniu, mają nowe funkcjonalności wygodne dla użytkowników.
- * Można tworzyć tokeny cyfrowe – zamiast oddzielnych kryptowalut na własnej infrastrukturze blockchainowej, którą należy utrzymywać.
- * Tokenów jest już więcej, niż kryptowalut. Niekiedy są zaprojektowane dla poszczególnych projektów, pełniąc w nich pewną użyteczną funkcję (*utility token*) lub łączoną z rolą papierów wartościowych.
 - ❖ Większość z nich się nie upowszechni – jest to normalne w biznesie, w świecie startupów.
 - ❖ Ale te projekty dające większą użyteczność dla klientów mają szansę na sukces.

Zastosowania blockchain

w administracji publicznej



Pierwsze zastosowania – Estonia

- Estonia jako pierwsza na świecie wykorzystwała technologię blockchain w administracji publicznej. Stało się tak dzięki autorskiemu rozwiązaniu, wynalezionemu niezależnie (lecz równolegle) do powstania bitcoina.
- Estonia połączyła infrastrukturę klucza publicznego (Public Key Infrastructure) oraz technologię blockchain. Do połączenia różnych rejestrów stworzono system X-road, który zabezpieczony jest m.in. za pomocą technologii blockchain.
- Estończycy mogą głosować online z dowolnego miejsca, cyfrowo podpisywać dokumenty, bezpiecznie wysyłać dokumenty, składać deklaracje podatkowe, otrzymywać zwroty podatków, dostać cyfrową receptę od lekarza, a część z tych rzeczy odbywa się **zabezpieczając** ww. rejestry przed niepowołanym dostępem za pomocą technologii blockchain.
- Każde niepowołane użycie publicznych baz danych (np. próba fałszerstwa) jest w ciągu sekundy do wykrycia i dzieje się to właśnie dzięki wykorzystaniu **blockchain**.

Inne zastosowania w sektorze publicznym

- Sektor publiczny w wielu krajach na świecie generalnie jest daleko w tyle za zastosowaniami blockchain w biznesie. Wyjątek: Dubaj.
- Na razie, główne prace dotyczyły wprowadzenia ułatwień dla branży firm kryptowalutowych (Malta, Gibraltar, Japonia, niektóre stany) lub dotyczące uregulowania jej funkcjonowania.
- Pomysły:
 - Poczta w Australii.
 - Rejestr ksiąg wieczystych w Gruzji.
 - Cyfrowe waluty narodowe
 - Estonia, Litwa, Wenezuela, Iran; kilka dni temu: Niemcy (CDU-CSU);
 - badania w Banku Anglii, sprzeciw EBC, nieformalny zakaz w Polsce).

Pomysły dot. zastosowania blockchain w samorządach w Polsce

- Polski Akcelerator Technologii Blockchain – pierwszy i jedyny dotąd na świecie, mający wspierać zastosowania blockchain wyłącznie w instytucjach publicznych.
 - Powołany w 2016 r., w 2017 r. rozpoczął działalność, na początku 2018 r. stracił honorowy patronat Ministerstwa Cyfryzacji (projekt dPLN), w końcu 2018 r. – NCBR rozwiązał umowę o dofinansowanie.
 - Rozwijanie projektów dla uczelni wyższych (i szpitali).
 - W zakresie samorządu: wsparcie projektu **iVoting** przewidującego głosowania online w budżetach partycypacyjnych za pomocą technologii blockchain.
- CoperniCoin w UMWWM (Olsztyn).

Wnioski

dla administracji



Wnioski

- Zastosowania technologii blockchain w administracji publicznej są wciąż na wstępnym etapie rozwoju.
 - Stwarza to **ryzyko** (techniczne, rynkowe, regulacyjne), ale i **szanse** (marketing, innowacje, nieprzeciętne zyski).
 - Jednym z częstszych zastosowań blockchain jest wykorzystanie tokenów (cyfrowych „żetonów”) – to najbardziej sprawdzone już (bezpieczne) wykorzystanie technologii blockchain.
 - Inne, ciekawe cechy tej technologii to możliwość eliminacji pośredników (w rezerwacjach, płatnościach).
 - W Polsce rozwijają się wdrożenia „trwałego nośnika” w oparciu o różne rozwiązania blockchainowe (PKO bp, Alior).
- Warto być innowacyjnym, choć nie zawsze się to opłaca.
(Politycznie) opłaca się nie być innowacyjnym, ale nie warto.



Dziękuję za uwagę!

twitter.com/krzysztof_piech

Krzysztof.Piech@lazarski.pl