Konferencja:

„Legal regulations of the blockchain technology and digital currencies in the world”

Uczelnia Łazarskiego, 25 maja 2017 r.

Kryptowaluty

wybrane fakty i podstawy rozwiązań technicznych

dr inż. Jacek Wytrębowicz

Instytut Informatyki Politechniki Warszawskiej

Plan

- Czym jest kryptowaluta?
- Bitcoin – najważniejsze fakty
- Inne kryptowaluty
- Poufność i uwierzytelnianie
- Integralność danych
- Rozproszona księga rachunkowa

Kryptowaluta

Instrument płatniczy istniejący jedynie w formie zapisu cyfrowego,
oparty o silne algorytmy kryptograficzne

W założeniach

- niepodlegający regulacjom administracyjnym
- niezależny od banków centralnych
- wartość jest kształtowana wyłącznie poprzez mechanizmy rynkowe

Techniczną podstawą jest *blockchain*

- rozproszony rejestr transakcji
- publicznie znane algorytmy
- zatwierdzone zapisy są niemodyfikowalne
- niemożliwe jest zatwierdzenie sprzecznych zapisów
  (np. dwukrotne wydanie tej samej kwoty)

Zalety kryptowaluty

- niskie koszty transakcji
  - atrakcyjne dla międzynarodowych mikropłatności
- nieodwoływalność płatności
- anonimowość zakupów
  - brak ryzyka kradzieży tożsamości
- nieczułość na presje polityczne
  - brak inflacji

Wady kryptowaluty

- zależność wartości od doniesień medialnych
- ryzyko spirali deflacyjnej (?)
- aktywność hakerów
- ryzyko niestabilności na skutek gier giełdowych
- są zagrożeniem dla banków (?)

Bitcoin (BTC)

Łączna wartość (podaż w obiegu) w USD 33 548 728 731 USD

Źródło: blockchain.info *dostęp 20.05.2017*

- Ile w obiegu ?
  - bitcoinów 33 548 mln USD na 20 maja 2017
  - zł w banknotach i monetach 49 029 mln USD na koniec 1 kw. 2017

- Liczba płatności, dziennie 352 805 maj 2017

- Kantor bitcoinwarszawa.pl 20 maja 2017
  - Sprzedaż 1 BTC = 8 023.31 PLN
  - Skup 1 BTC = 7 088.34 PLN

- Giełda bitmarket.pl 20 maja 2017
  - Średni kurs 1 BTC = 7 560 PLN

- Twórca BTC "Satoshi Nakamoto" 2009

- 1 BTC
  - tys. mBTC, mln μBTC, 100 mln satoshi

- Identyfikator portfela, np.: 1x1a4BoVyN9KoJ8URMfqNwSXpDDEGFFVE
  - na własnym urządzeniu
  - u operatora – hosting portfeli

- Transakcja np.: X przekazuje kwotę Y do Z o czasie T
  - analizowana przez wiele węzłów
  - 10-60 min
  - opłata za transakcję

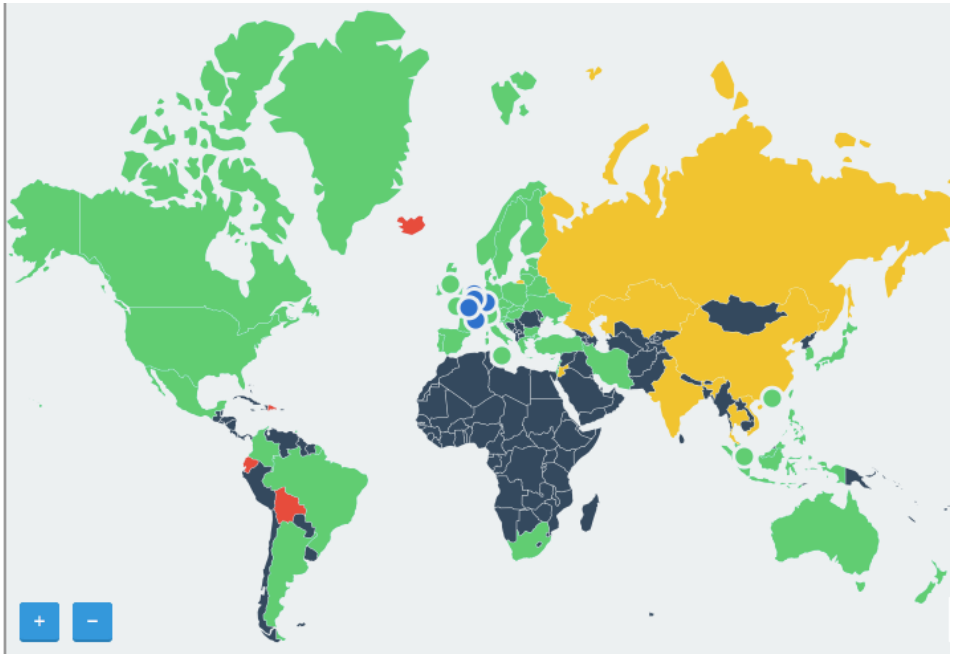
- „Górnictwo”
  - moc obliczeniowa 21 100 000 PetaFLOPS (superkomputer *Sunway TaihuLight* – 93 PetaFLOPS)
    wrzesień 2016
  - granica wydobycia: 21 mln BTC dotychczas wydobyto 16,3 mln

Kto używa BTC

- startupy i małe przedsiębiorstwa
- dostawcy usług i towarów dla komputerowych „geeków”
- kraje
  - rozwijające się
  - z dużą szarą strefą
  - o niskim PKB na mieszkańca

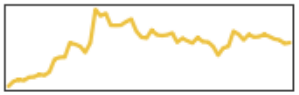
Regulacje prawne

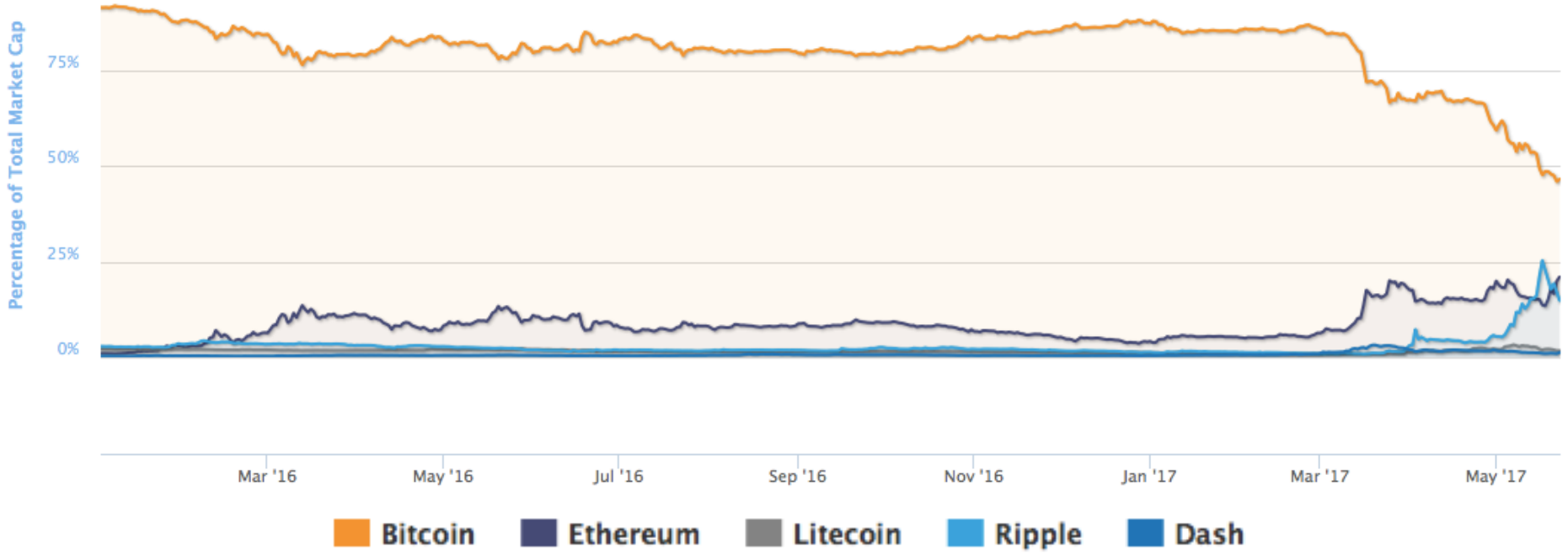
- Różnie w różnych krajach
  - zakaz
  - brak aktów
  - tolerowanie
  - restrykcje – Islandia
  - stabilne regulacje pro – wyspa Moon
- Trwałość determinuje
  - liberalna polityka wielu państw
  - znaczne obroty handlowe



Źródło: bitlegal.io dostęp 20.05.2017

Popularne kryptowaluty coinmarketcap.com 721 Currencies / 112 Assets / 3840 Markets

#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$33,439,322,487	$2046.01	16,343,675 BTC	$1,121,230,000	0.01%	
2	Ethereum	$13,814,871,622	$150.48	91,807,807 ETH	$509,073,000	15.79%	
3	Ripple	$13,047,117,417	$0.338600	38,532,538,149 XRP *	$135,289,000	-6.01%	
4	NEM	$2,231,820,000	$0.247980	8,999,999,999 XEM *	$23,839,200	5.62%	
5	Litecoin	$1,374,535,679	$26.84	51,207,057 LTC	$100,235,000	-2.38%	
6	Dash	$727,558,427	$99.53	7,309,941 DASH	$19,137,400	-3.15%	
7	Bytecoin	$720,372,628	$0.003938	182,919,723,940 BCN	$36,288,500	75.82%	
8	Ethereum Classic	$694,000,593	$7.56	91,842,998 ETC	$39,505,700	-1.03%	
9	Stellar Lumens	$639,402,478	$0.066432	9,624,873,410 XLM *	$59,684,200	25.03%	
10	Monero	$494,716,570	$34.12	14,498,676 XMR	$11,612,300	-1.44%	



23 maja 2017:	46,5%	20,97%	1,75%	14,82%	1,26%

Przykładowe polskie giełdy kryptowalut

- bitstar.pl BTC
- bitbay.net BTC, Litecoin (LTC), Ether i Lisk
- bitmarket.pl BTC, LTC

Polska kryptowaluta

- polcoin (PLC) polcoin.pl od 2014 r.

Poufność i uwierzytelnianie

Cyfrowa reprezentacja danych, np.

Ryszard Kowalski 52 79 73 7a 61 72 64 20 4b 6f 77 61 6c 73 6b 69

liczba 128 bitowa wartości dziesiętnie od 0 do ~3,4 * 10^{38}

Kryptografia symetryczna

1 klucz współdzielony

dł. klucza: 128, 256 bitów

szybka

Kryptografia asymetryczna

2 klucze: prywatny i publiczny

dł. klucza: 1024, 2048 bitów

wolna

Poufność

nadawca → szyfrowanie → deszyfrowanie → odbiorca

klucz publiczny *klucz prywatny*

Uwierzytelnianie

nadawca → szyfrowanie → deszyfrowanie → odbiorca

klucz prywatny *klucz publiczny*

Integralność danych

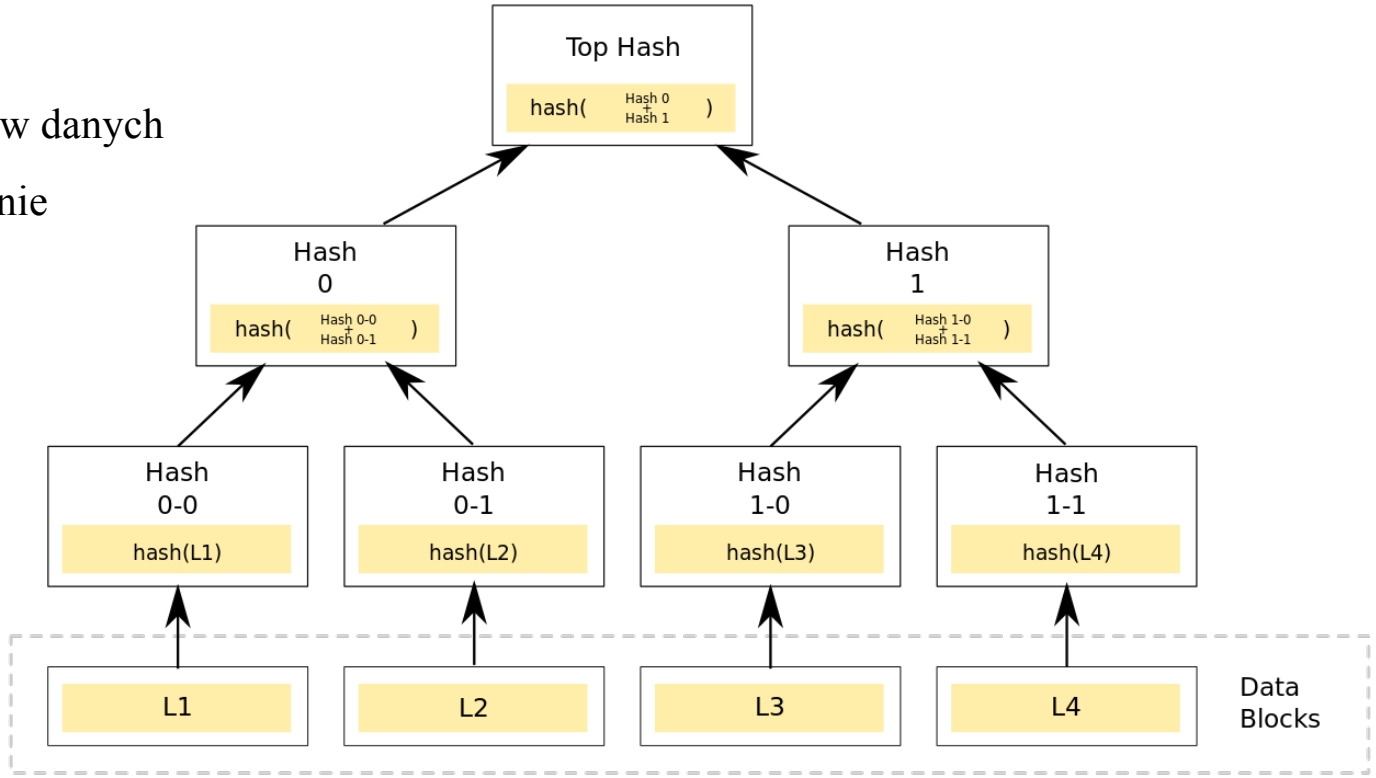
Funkcje skrótu

dowolnej długości łańcuch bitów → liczba stałej długości, np. 128, 256, 512 bitów

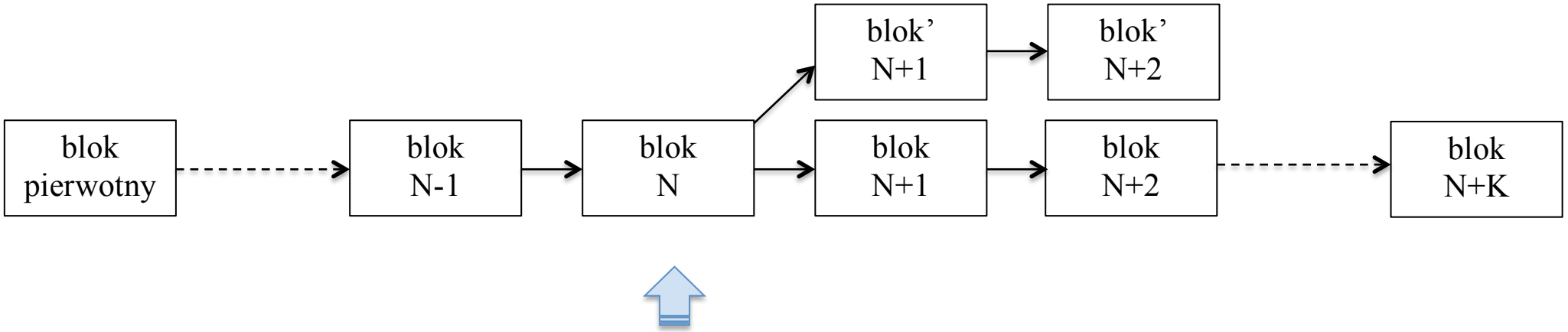
- jest deterministyczna i szybka
- niemożliwe odtworzenie pierwotnego łańcucha na podstawie jego skrótu
- bardzo trudne znalezienie drugiego łańcucha posiadającego taki sam skrót
- zmiana jednego bitu łańcucha powoduje zmianę ponad połowy bitów w skrócie

Drzewo skrótów

- dla dużych zbiorów danych
- szybkie sprawdzanie przynależności



Rozproszona księga rachunkowa



Nagłówek
- skrót bloku N-1
- data
- liczba wypracowywana
- skrót bloku N
- korzeń drzewa skrótów

Ciało
- drzewo skrótów
- transakcja Y
- transakcja X
- …
- transakcja A

Ograniczenia techniczne BTC

- Rosnące zużycie energii elektrycznej
- Rosnące wymaganie na pamięć blockchain zajmuje już ponad 50 GB
  dla tej liczby transakcji co VISA przyrost byłby 3,9 GB/dzień
- Liczba transakcji na sek. = 7 (VISA 20 000)
- Czas na potwierdzenie transakcji od 10 min. do kilku godz.

- Przewidywany wzrost
  - kosztów transakcji
  - oczekiwania na potwierdzenie

Pytania?