10 lat Bitcoina
i planowane zmiany w nim

DIGITAL MONEY & BLOCKCHAIN FORUM

• TECHNOLOGY • BUSINESS • PAYMENT • COMMERCE • SECURITY • LAW • COMPLIANCE •

Rafał Kiełbus

Warszawa 16-05-2019

About: Rafał Kiełbus

Bitcoin.pl

POLSKIE STOWARZYSZENIE BITCOIN

Od papierowej do cyfrowej Polski

SEJM RZECZYPOSPOLITEJ POLSKIEJ

IZBA GOSPODARCZA BLOCKCHAIN I NOWYCH TECHNOLOGII

AKCELERATOR .tech

KNF KOMISJA NADZORU FINANSOWEGO

SZKOŁA GŁÓWNA HANDLOWA W WARSZAWIE

SGH Szkoła Główna Handlowa w Warszawie

ASBIRO Alternatywna Szkoła Biznesu i Rozwoju Osobowego im. Ludwiga von Misesa

foldit Solve Puzzles for Science

FP IT Management

Rafał prostuje Bitcoina

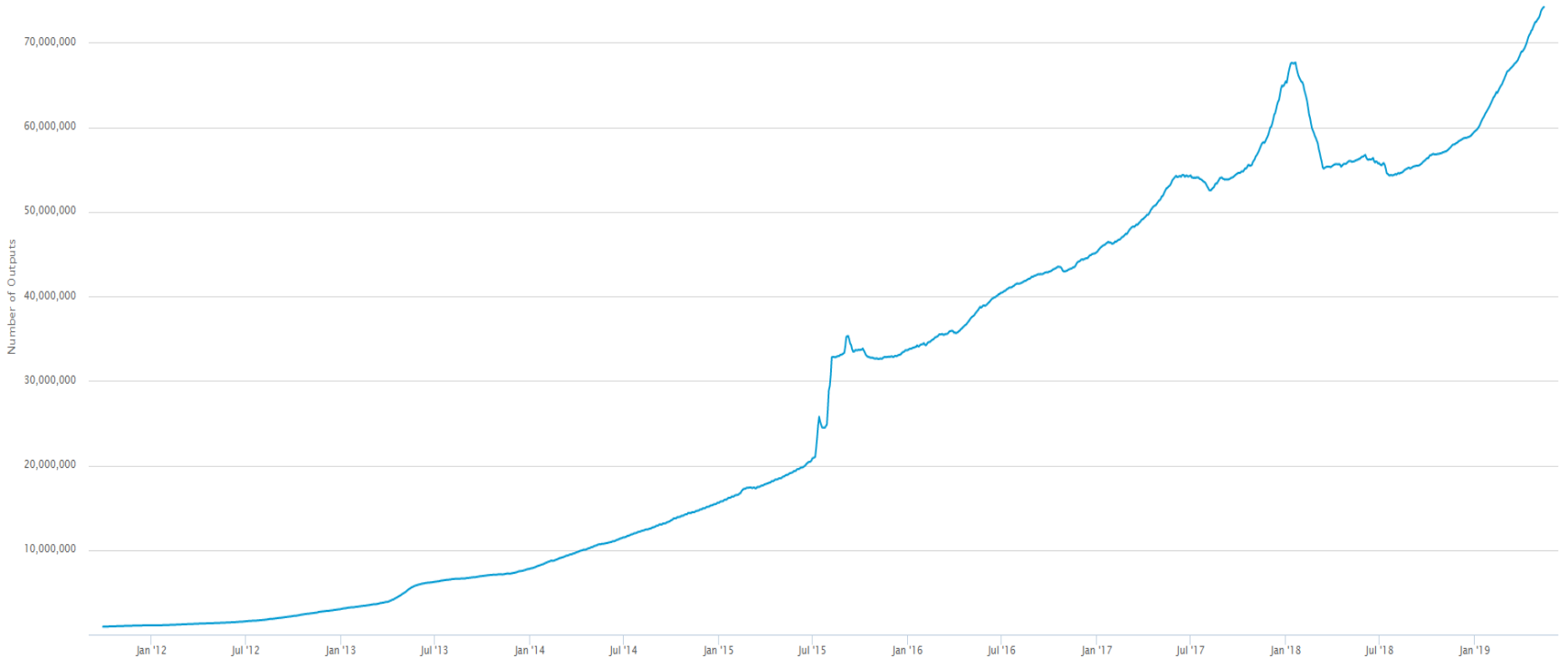
Walka o przepustowość

- W tradycyjnym systemie finansowym transakcja to: kto, komu, ile
- W sieci Bitcoin jedna transakcja może zawierać wiele „kto” oraz wiele „komu, ile” w dowolnych proporcjach

Ile może Bitcoin?

- „Standardowa” transakcja (1 wejście, 2 wyjścia) ważyła około 266 bajtów, co przy limicie 1MB i bloku co 10 minut daje ok 6 transakcji na sekundę
- W przypadku, gdy wysyłamy do wielu odbiorców w krótkim czasie (np. 10 minut) łączenie transakcji w jedną niesie znaczny wzrost przepustowości

Ilość niewydanych wyjść w czasie



Problemy techniczne

- Wprowadzenie limitu wielkości bloku i opłat transakcyjnych jako zabezpieczenie przed „spamem” sieci
- Możliwość modyfikacji transakcji w celu zmiany jej identyfikatora („transaction mallebility”)
- „Blockchain trilemma” - bezpiecznego i otwartego (rozproszonego) systemu nie można pogodzić z dużą szybkością

Trylemat blockchain

Zmiany wpływające na wydajność

- Kwiecień 2011, 0.3.21
  - wprowadzenie komendy „sendmany”
- Marzec 2012, 0.6.0
  - wprowadzenie „kompresji” kluczy publicznych (65→33 bajty)
- Maj 2012, 0.6.1
  - wprowadzenie adresów typu „multisig”
- Luty 2013, 0.8.0
  - wyłączenie domyślnego „txindex”,
  - wprowadzenie filtrów Blooma (natywna obsługa SPV)

Kolejne zmiany...

- Grudzień 2013, 0.8.6
  - podniesienie domyślnej, maksymalnej wielkości bloku do 350kb
- Marzec 2014, 0.9.0
  - wprowadzenie OP_RETURN jako metodę zapisu danych do blockchain,
  - 750kb jako domyślna wielkość bloku,
  - monitorowanie i raportowanie „zmutowanych” transakcji
- Luty 2015, 0.10.0
  - Podpisy transakcji przy pomocy Libsecp256k1 zamiast OpenSSL
- Lipiec 2015, 0.11.0
  - Wprowadzono możliwość kasowania starych bloków („pruning”)

I jeszcze kilka...

- Październik 2015, 0.10.3
  - Wprowadzenie kontroli kodowanie podpisów ECDSA pod kątem wymogu „low-s”
- Listopad 2015, 0.11.2
  - Wprowadzenie transakcji zablokowanych w czasie (OP_CHECKLOCKTIMEVERIFY, CLTV)
- Luty 2016, 0.12.0
  - Wprowadzenie transakcji RBF („replace-by-fee”)
- Kwiecień 2016, 0.12.1
  - Wprowadzenie możliwości rozgałęziania skryptu wydania w zależności od czasu wykonania transakcji (OP_CHECKSEQUENCEVERIFY, CSV)

I najnowsze

- Sierpień 2016, 0.13.0
  - Przesyłanie bloków jako nagłówki + lista transakcji
  - Wprowadzenie kodu oddzielonych podpisów (Segregated Witness, SegWit)
  - Łączenie transakcji oczekujących w łańcuchy, obliczanie opłat dla całego łańcucha (Child-Pay-For-Parrent, CPFP)
- Wrzesień 2017, 0.15.0
  - Usunięcie możliwości wykonywania darmowych transakcji
  - Aktywacja SegWit w sieci
- Luty 2018, 0.16.0
  - Pełna obsługa adresów SegWit
  - Lightning Network startuje w marcu jako „beta”
- Październik 2018, 0.17.0
  - Wprowadzenie obsługi częściowo podpisanych transakcji (Partially Signed Bitcoin Transactions, PSBT)

Przyszłość

- Podpisy Schnorra
  - Możliwość łączenia wielu podpisów w jeden
  - Efektywne przy 3+ wejściach w transakcji
- Łańcuchy boczne
  - Możliwość wykonywania dowolnej ilości transakcji poza łańcuchem głównym
  - Możliwość wykonywania transakcji niemożliwych w sieci głównej – Rootstock działa jak Ethereum zasilane BTC

Dziękuję :)