# Analiza łańcucha transakcji w sieci Bitcoin

Bartosz Zychal

Promotor: dr inż. Radosław Michalski

12.02.2018

HR EXCELLENCE IN RESEARCH



Politechnika Wrocławska

# Cel pracy

Celem pracy było wykorzystanie technik analizy sieci złożonych do analizy rejestru transakcji w sieci Bitcoin (tzw. Blockchain). W pracy podjęta została próba odpowiedzi na pytanie, jakie własności transakcji można pozyskać wykorzystując analizę sieci złożonych.

# Problem badawczy

Problem badawczym pracy było próbkowanie oraz eksploracja sieci złożonych. Istotnym zagadnieniem było również tempo rozwoju sieci użytej do przeprowadzenia badań, które cały czas rośnie. Wymusza to, obok badania właściwości, badanie trendów zmian w sieci.

# Obiekt badań

Obiektem badań wykorzystanym na potrzeby realizacji pracy była sieć zbudowana na podstawie mechanizmu zawartego w jednej z krypto-walut. Cała sieć jest rzeczywistą siecią złożoną, składającą się z prawie trzystu tysięcy połączeń oraz milionów węzłów, dlatego też jej rozmiar obliguje do zastosowania określonych metod badawczych.

# Zastosowane metody badawcze

Praca opiera się na metodach badawczych stosowanych w badaniu temporalnych sieci złożonych. Metody te charakteryzują się rozszerzeniem klasycznego konceptu sieci złożonej o dodatkowy wymiar, jakim jest czas. Na potrzeby przeprowadzenia badań wybrano sto momentów istnienia sieci Bitcoin, a następnie wykonano szereg analiz.

# Blockchain - rejestr transakcji

## Definicja

Łancuch bloków (ang. Blockchain) jest uporządkowaną strukturą, zwaną jednokierunkową listą składającą się z bloków transakcji. Listę tę charakteryzuje połączenie wsteczne, co oznacza, że blok następny wskazuje na blok poprzedni. Każdy kolejny blok ma przypisaną swoją wysokość w łańcuchu bloków. Wysokość ta ustalana jest na podstawie odległości bloku od pierwszego bloku w łańcuchu. Blok ten, zwany blokiem genezy, stanowi pierwszego *rodzica* oraz wspólnego przodka dla wszystkich bloków w całym łańcuchu. Bloki rozpoznaje się na podstawie unikalnego hash'a, który generowany jest przy użyciu algorytmu kryptograficznego SHA256.

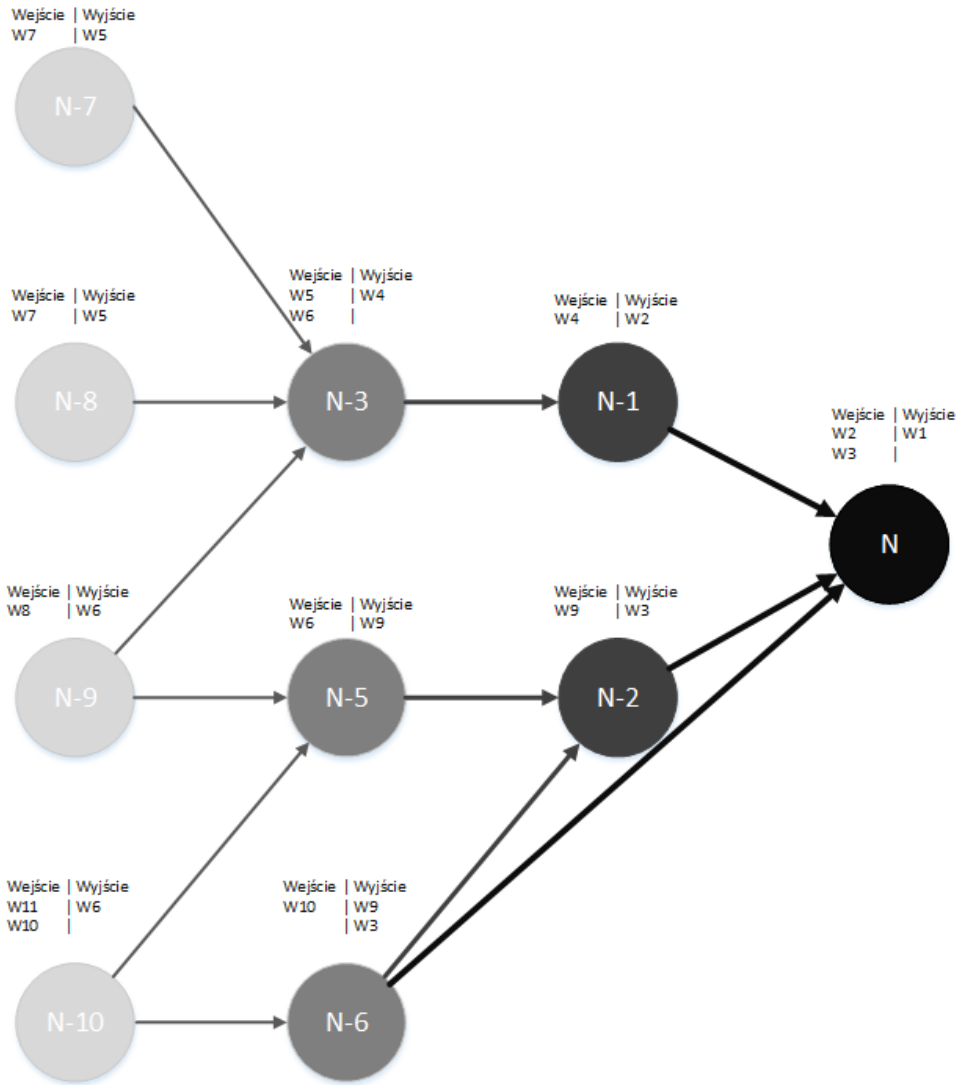
# Blockchain - rejestr transakcji

## Przykładowa zawartość jednego bloku sieci Bitcoin

| | |
|---|---|
| Hash bloku | 00000000000000000a7b47a1e58e456 fd54ae5a30cb92a35ca3e5acee065287 |
| Wysokość bloku | 496201 |
| Rozmiar: | 1071.607 kB |
| Liczba transakcji: | 2032 |
| **Nagłówek bloku** | |
| Wersja: | 0x20000000 |
| Hash poprzedniego bloku: | 00000000000000000c6dd215947b569 fa06de2cb856dec643daf5a7e8efc72e |
| Markle root: | b96da6d09865e36e4862b5a612fb1893 275d889989feb5a7a217503fd84019e3 |
| Czas wykopania: | 2017-11-26 13:51:02 |
| Trudność: | 1,347,001,430,558.57 |
| Transakcje | |

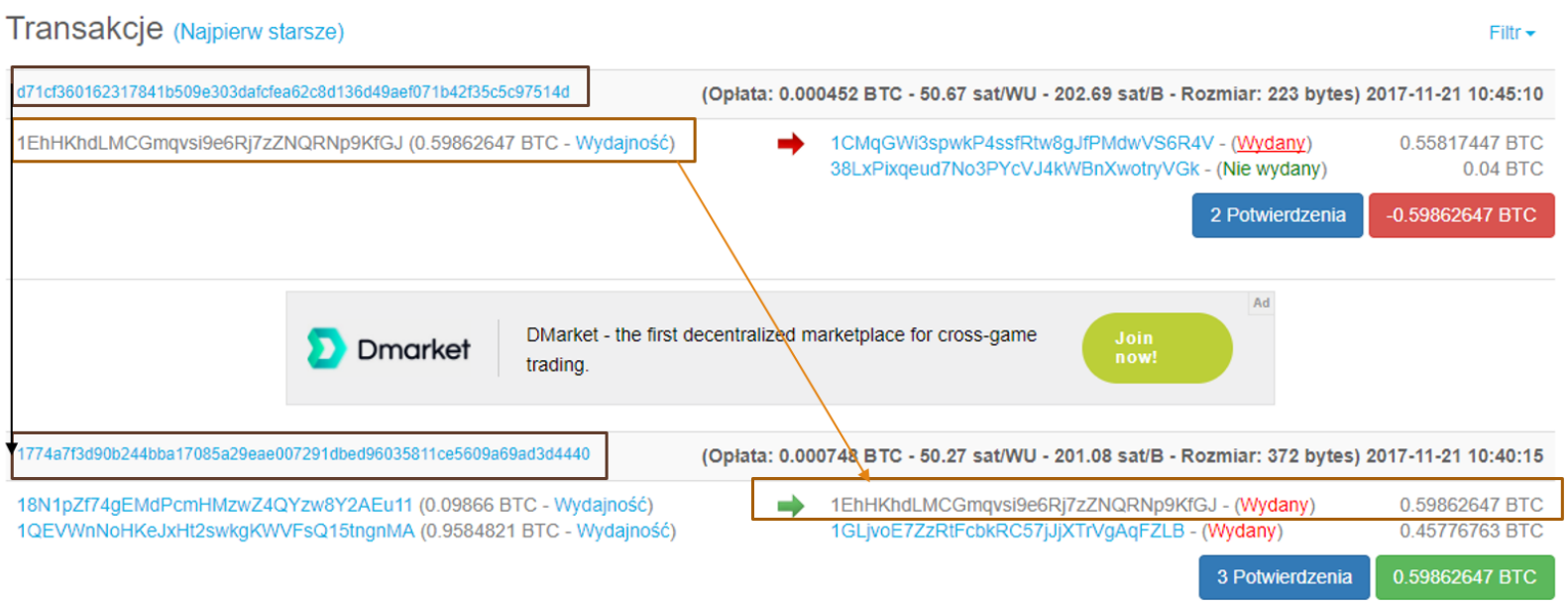
# Sposób budowy sieci

## Model teoretyczny

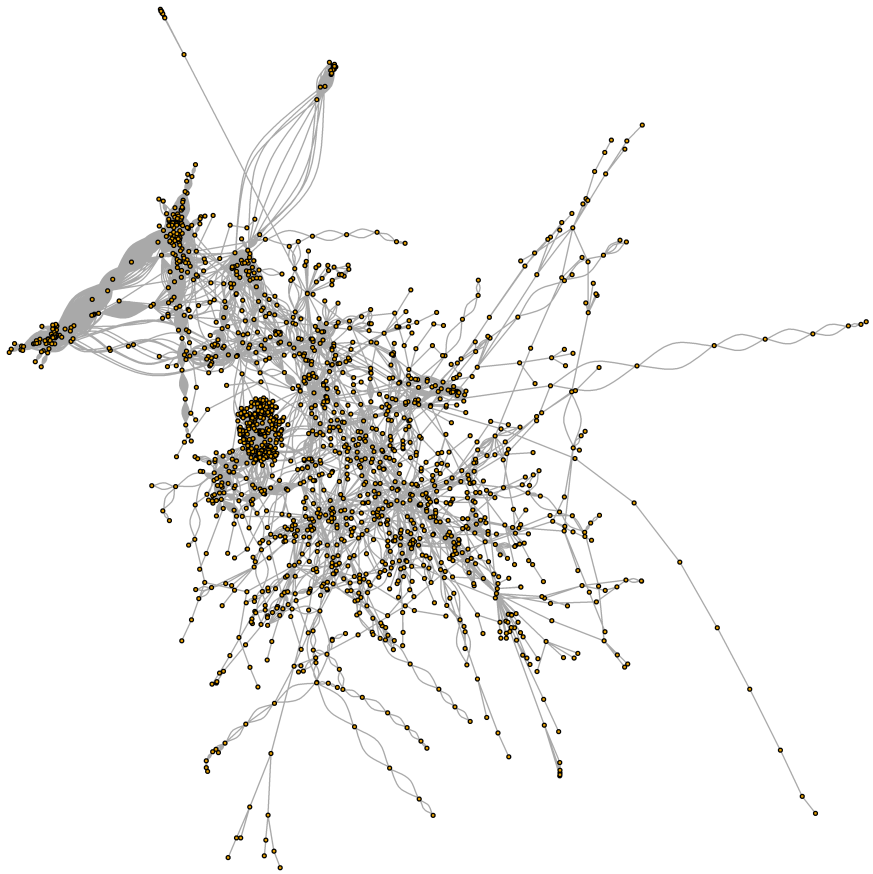


# Sposób budowy sieci

## Praktyczny przykład



# Przykładowa sieć



# Przeprowadzone badania

Przeprowadzono badania podstawowych właściwości sieci:

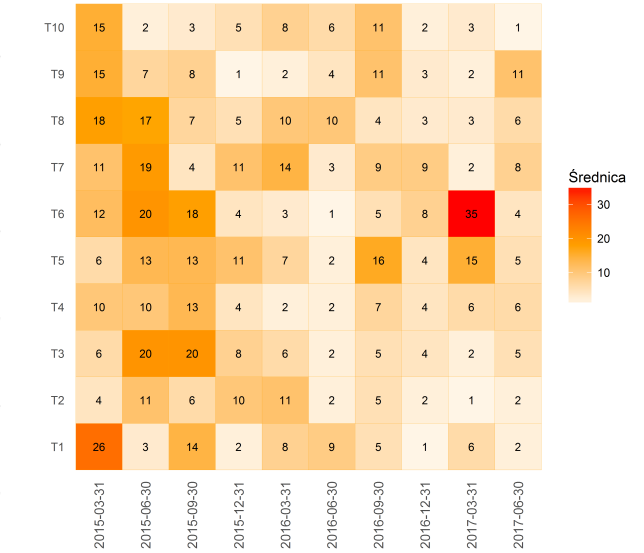
- średnicy,
- średniej długości ścieżek,
- średniego stopienia węzłów,
- średniej centralności węzłów,

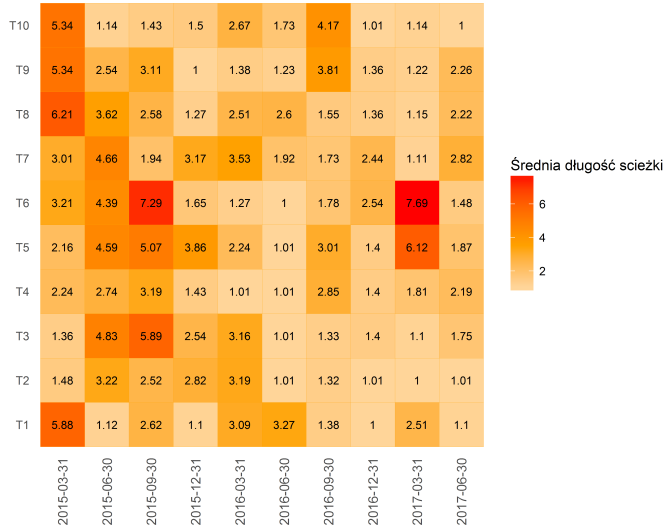
oraz badania wynikające z jej specyfiki:

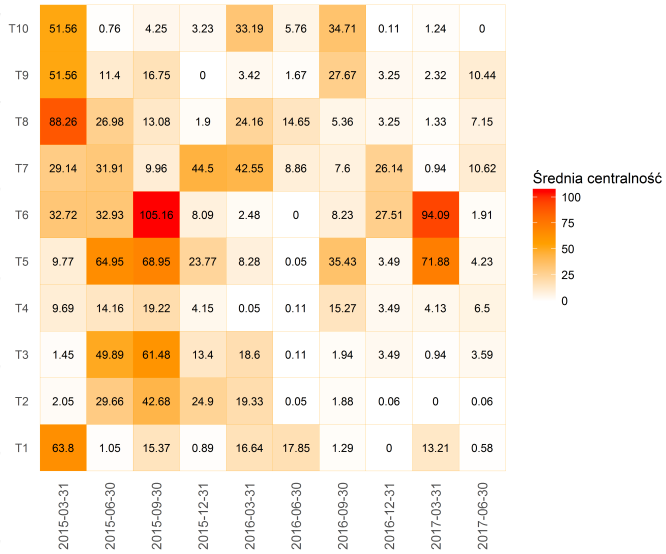
- średnia wartość transakcji,
- liczba bloków potrzebnych do stworzenia próby,
- średnia różnica czasów kolejnych transakcji,
- różnica czasu granicznych transakcji.

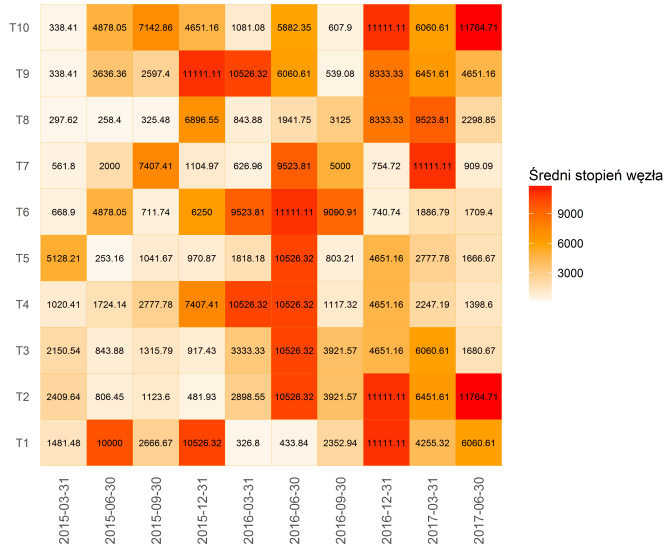
# Wyniki

## Generyczne właściwości sieci



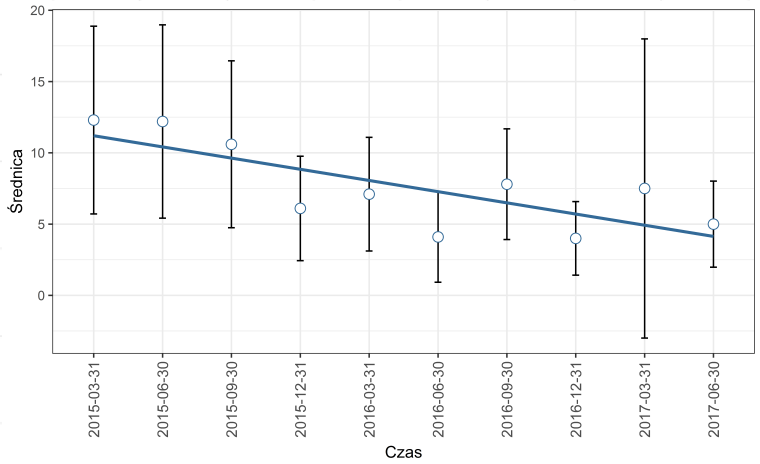



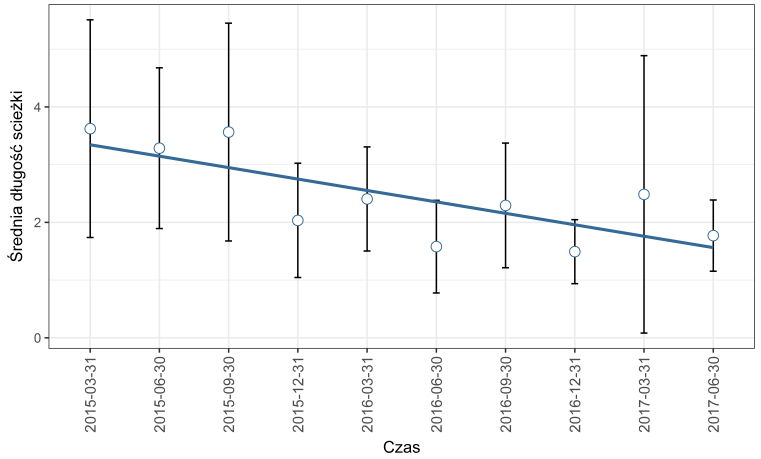



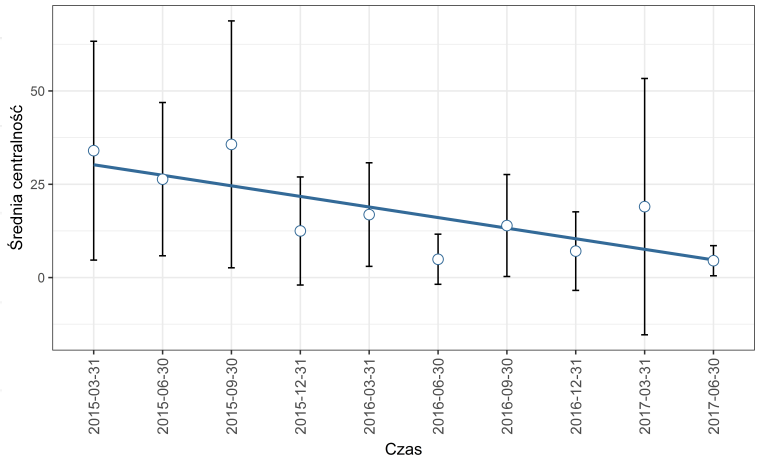



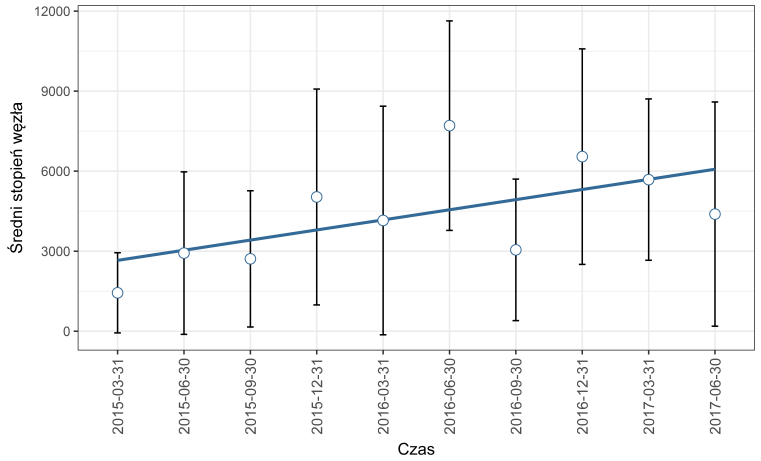
# Trend

## Generyczne właściwości sieci



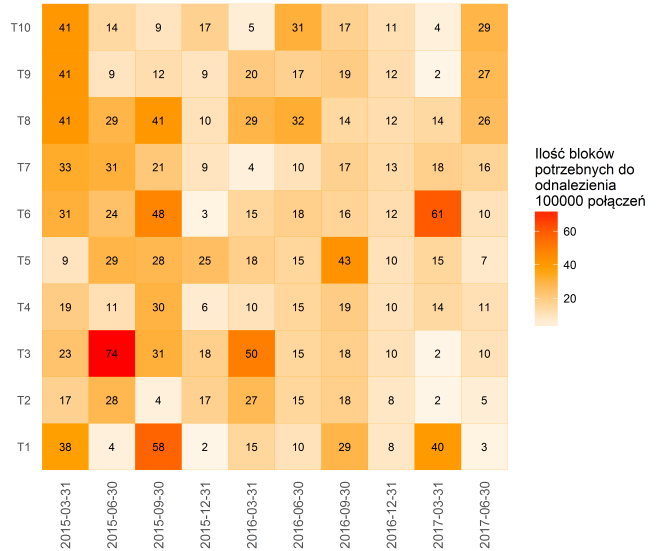



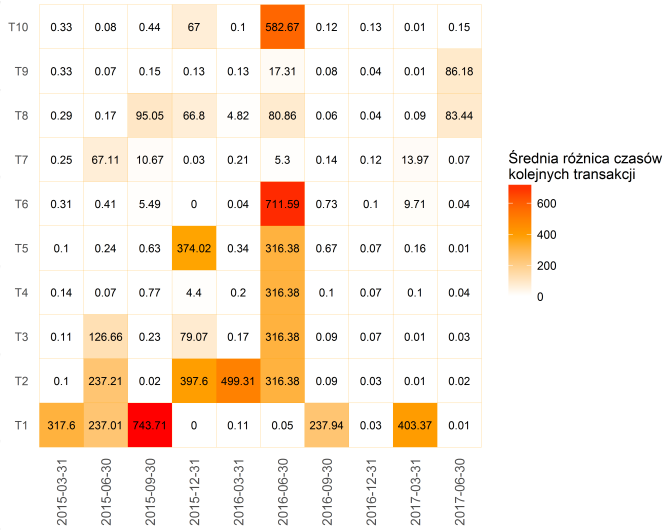



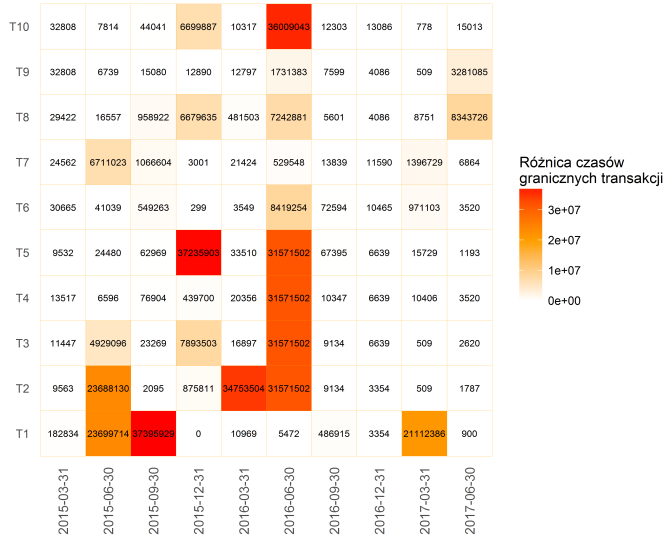



# Wyniki

## Własności sieci wynikające z jej specyfiki

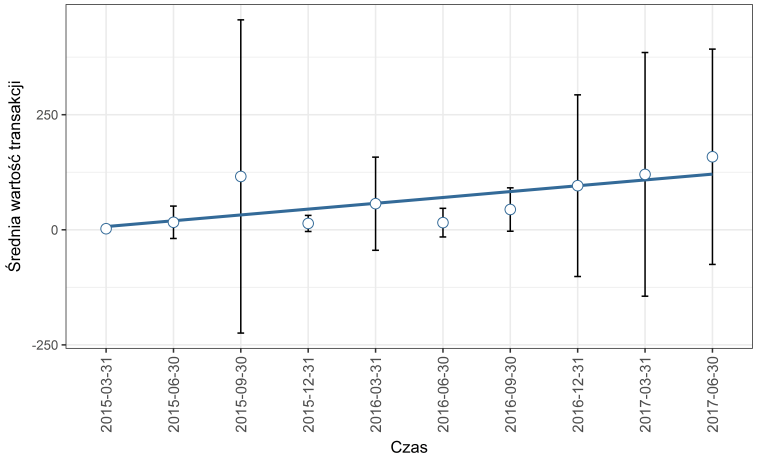



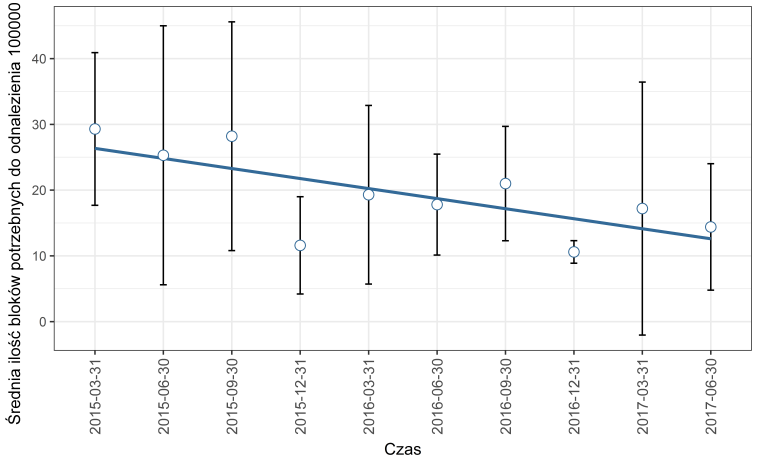



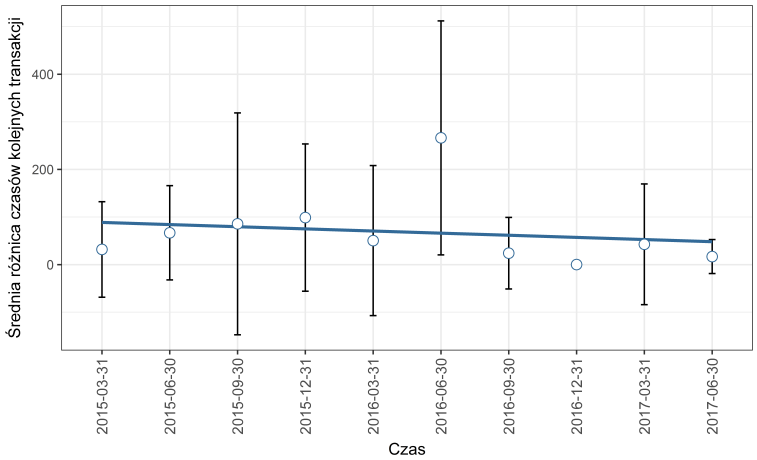



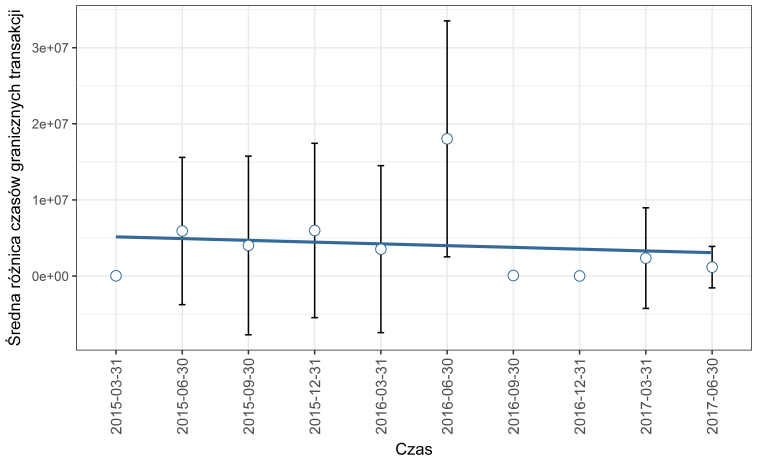
# Trend

## Własności sieci wynikające z jej specyfiki



# Wnioski

A. Sieć Bitcoin jest bardzo złożoną, dynamiczną i szybko rozwijającą się siecią.
B. Gęstość sieci rośnie, co w odniesieniu do jej specyfiki oznacza coraz większą ilość zlecanych transakcji, powstawanie dużej ilości nowych adresów oraz wzrost realizowanych transakcji pomiędzy różnymi uczestnikami sieci.
C. Rosnąca ilość wykonywanych transakcji powoduje spadek istotności pojedynczej transakcji w całej sieci.
D. Właściwości sieci nie są stałe w jednym okresie, a zależeć mogą od aktywności poszczególnych uczestników, dlatego też ilość połączeń pomiędzy transakcjami może być bardzo zróżnicowana.

# Wnioski

E. Wartość większości transakcji nie przekracza 100 bitcoinów, a zazwyczaj są to małe przekazy środków pomiędzy klientami sieci.
F. Badanie ilości bloków potrzebnych do odnalezienia 100 tysięcy połączeń, w powiązaniu z analizą średniej różnicy czasów kolejnych transakcji oraz różnicy czasów transakcji granicznych jednoznacznie wskazuje na zwiększające się tempo rozwoju badanej sieci.
G. Analiza znaczących wartości transakcji pozwoliła na powiązanie okresów z wzmożoną aktywnością giełd.