[IIC3272] Proyecto II Criptomonedas 2020-1

Consensus from Trust

Camilo Berríos - Felipe Gómez - Saúl Langarica - Pablo Rojas

Introducción

- Método para decidir la veracidad de un mensaje en una red informática.
- Un nodo recibe mensajes de varios nodos diferentes y comprueba su veracidad si todos son idénticos.

Consensus from trust

- No utiliza proof of work
- Un nodo se suscribe a un nodo en el cual confía y recibe sus mensajes para luego propagarlos a los demás nodos.

¿Cómo funciona el algoritmo?

- Se crea un grafo con **n** nodos
  - Cada nodo puede o no estar conectado a otro (p)
  - Cada nodo puede o no recibir el mensaje (pp)
  - Cada nodo puede o no ser malicioso (ppp)
- Se realizarán transacciones entre nodos y se transmitirán por la red
- Los nodos llegan a consenso: igual lista de transacciones

Nodos maliciosos

- Tres posibles comportamientos:
  a. Nodo muerto
  b. Solo transmite el primer mensaje
  c. Alterna entre **a** y **b**

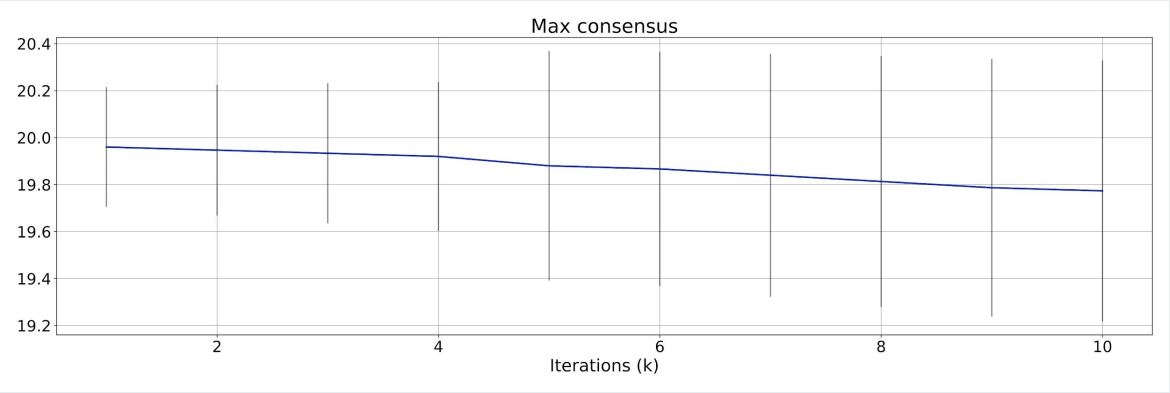
Experimentos

Se realizaron las siguientes simulaciones:

- Simulación con los parámetros iniciales del enunciado.
- Varían los parámetros:
  - **n** 10 hasta 100 paso 10
  - **k** 10 hasta 100 paso 10
  - **p** 0.1 hasta 1, paso 0.05 (conectividad)
  - **pp** 0.1 hasta 1, paso 0.05 (probabilidad de recibir primer mensaje)
  - **ppp** 0.1 hasta 1, paso 0.05 (porcentaje nodos maliciosos)
- Se reportará n, #consensos y %consenso más grande

Simulación Inicial

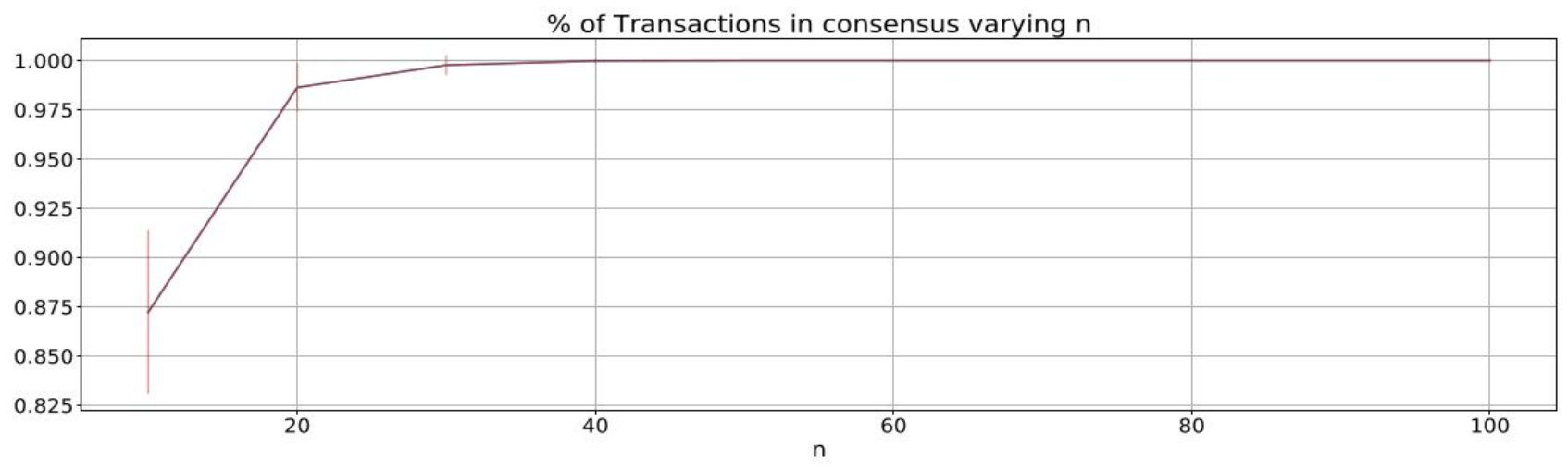
Se utilizaron los parámetros iniciales del enunciado.



Parámetro	Valor
n	20
k	10
% p	0.4
% pp	0.2
% ppp	0.1

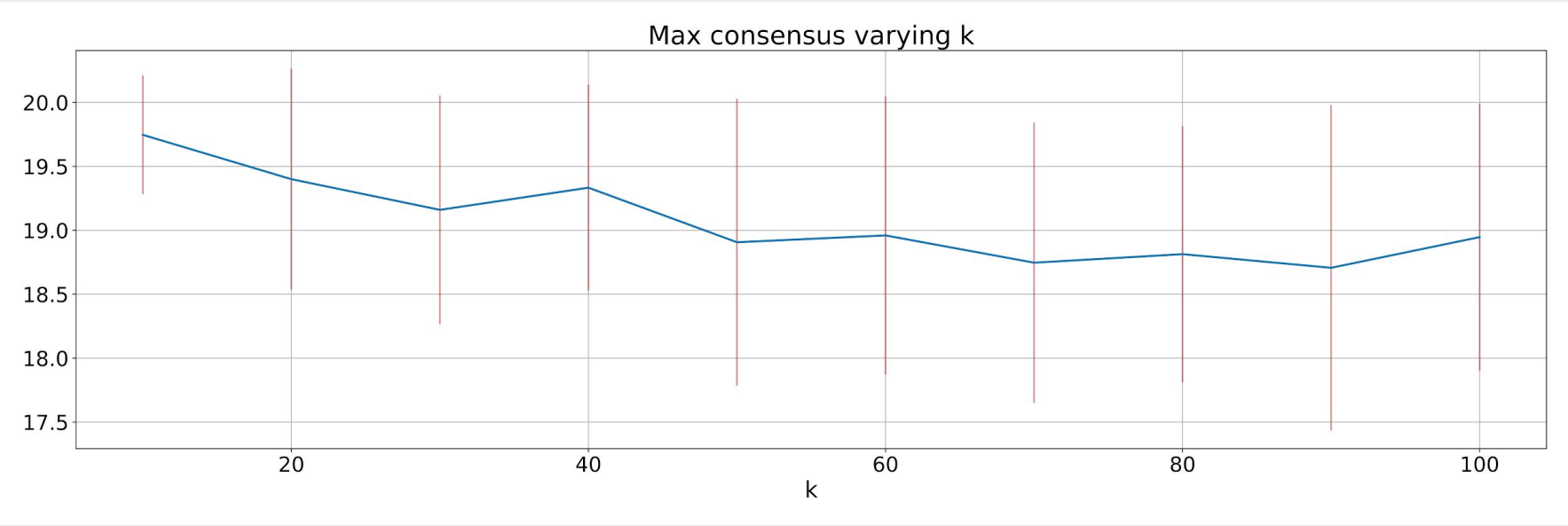
Simulación variando n

Se varían la cantidad de nodos de 10 a 100, 75 simulaciones por cada uno.



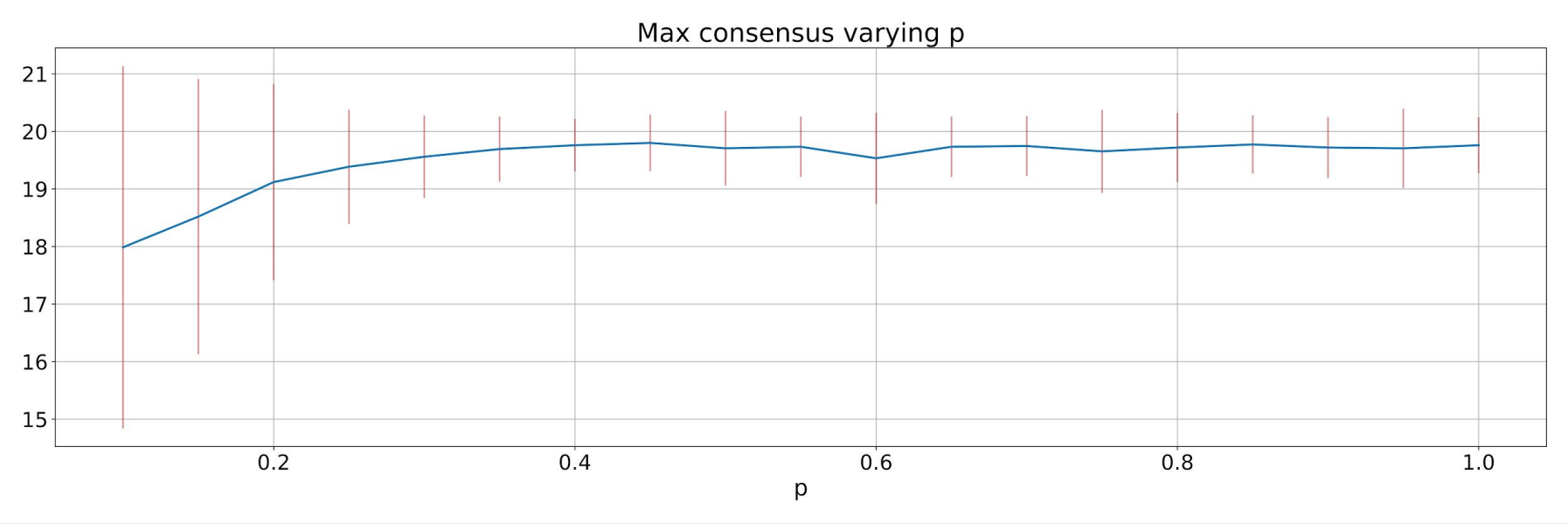
Simulación variando k

Se varían la cantidad de iteraciones de 10 a 100, 75 simulaciones por cada uno.



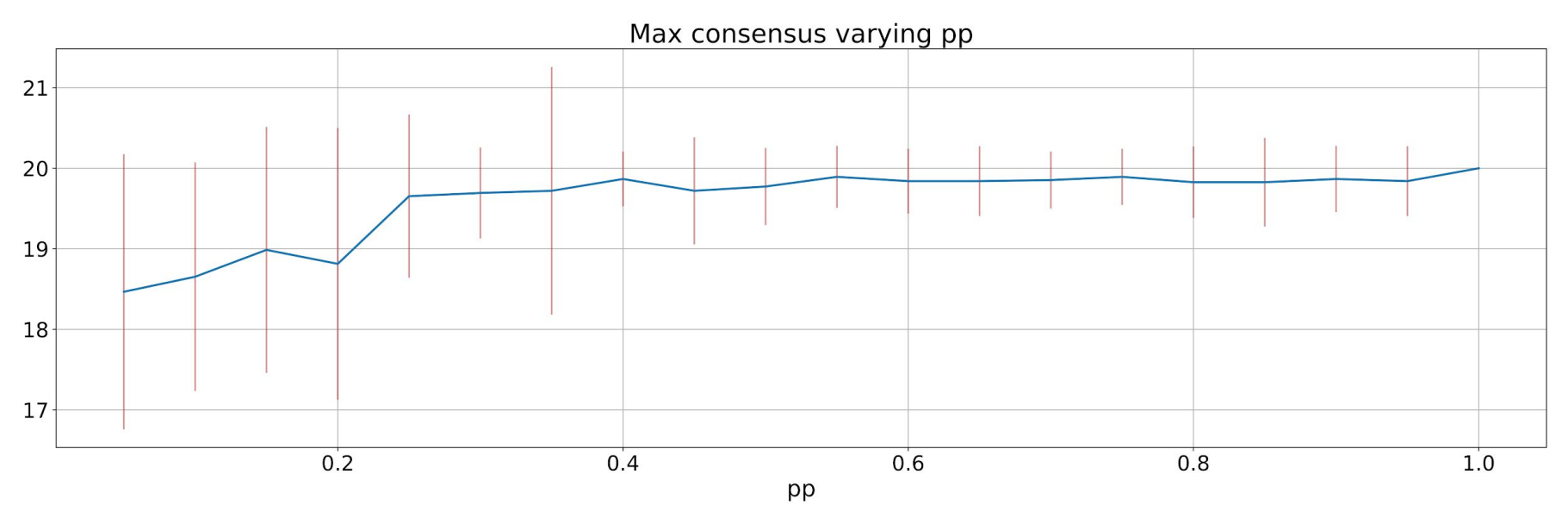
Simulación variando p

Se varían la tasa de conectividad, de 0.1 a 1.



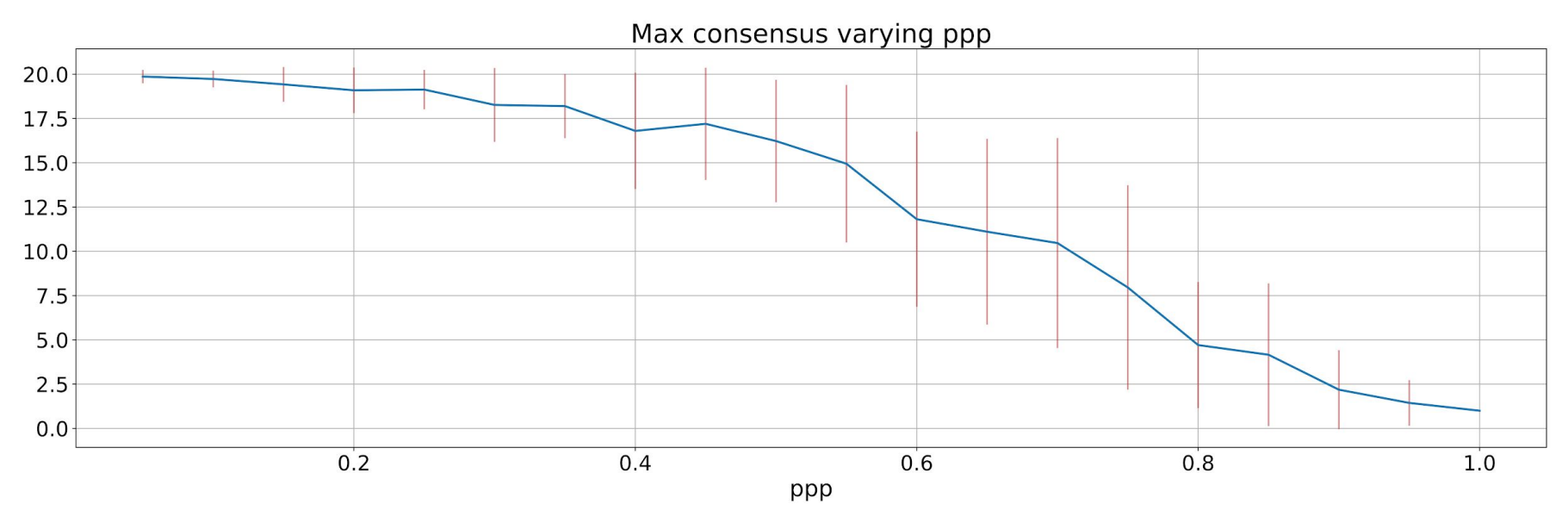
Simulación variando pp

Se varían la probabilidad de recibir el mensaje directamente, de 0.05 a 1.

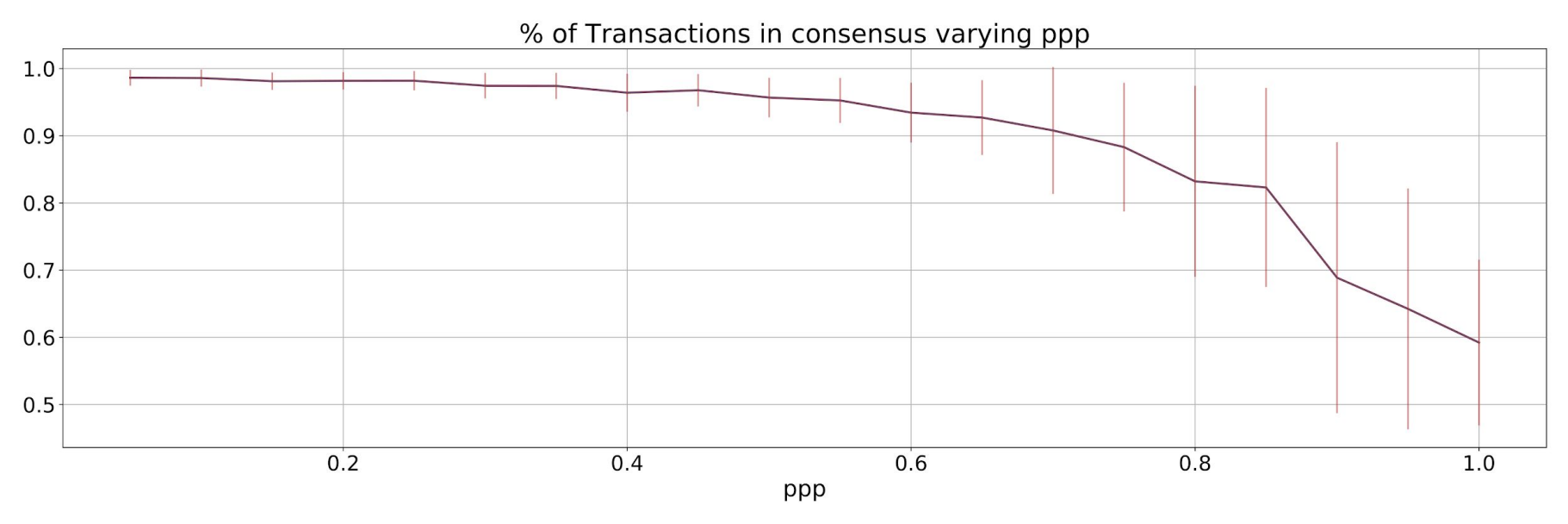


Simulación variando ppp

Se varía la cantidad de nodos maliciosos. De 0.05 a 1.

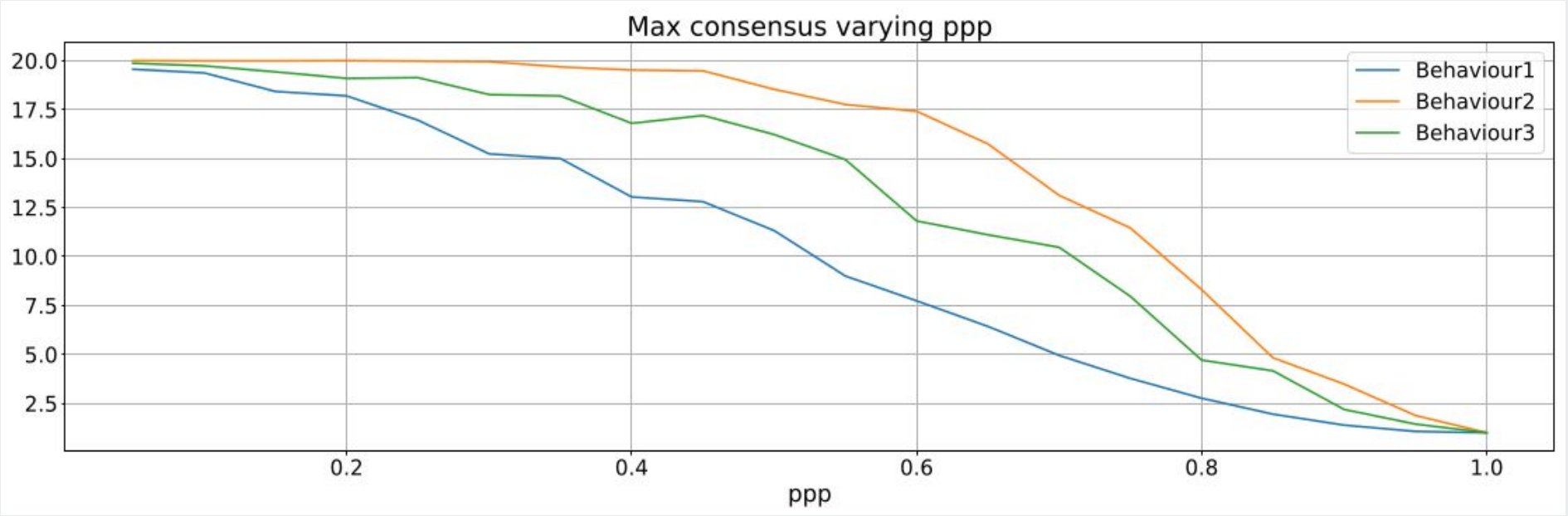


Simulación variando ppp



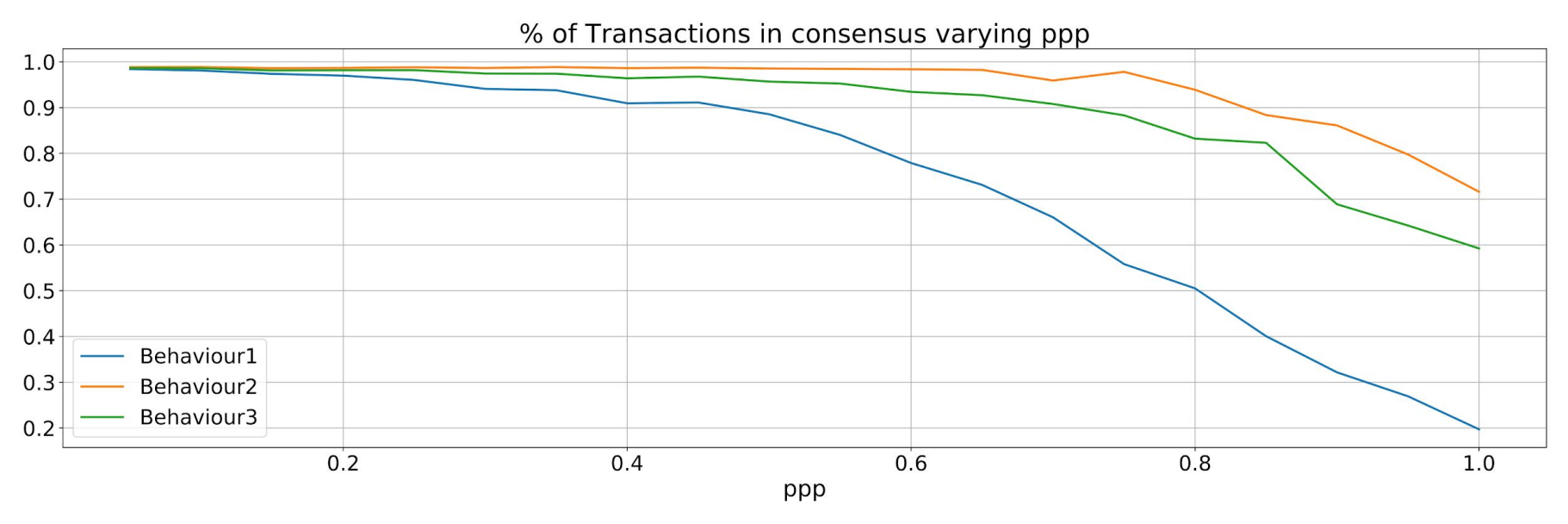
Simulación de comportamiento

Se cambia el comportamiento de los nodos maliciosos.



Simulación de comportamiento

Se cambia el comportamiento de los nodos maliciosos.



Conclusiones

- Se necesita una red grande.
- Una red muy conectada.
- Un mínimo de centralización.
- Por eso no se usa en bitcoin.

[IIC3272] Proyecto II Criptomonedas 2020-1

Fin de la presentación

Camilo Berríos - Felipe Gómez - Saúl Langarica - Pablo Rojas