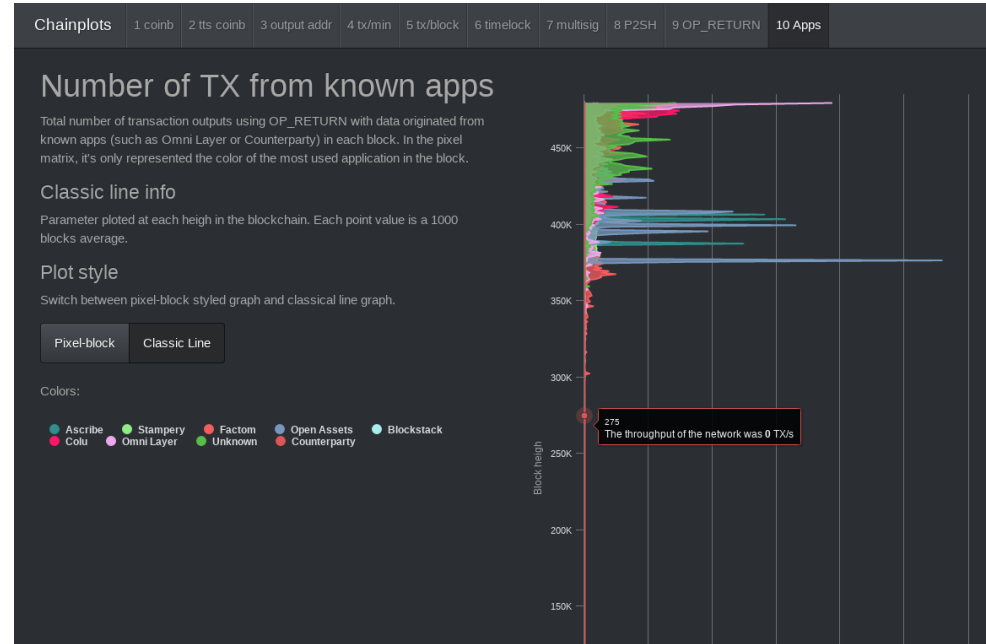


Graphical visualization of blockchain data

- **Fecha:** Enero de 2018
- **Autor:** Federico Laport Rivas
- **Director:** Jordi Herrera Joancomartí
- **Área:** Seguridad en redes y aplicaciones distribuidas

Análisis de parámetros de la blockchain de bitcoin y visualización de los datos en una aplicación web



Blockchain de bitcoin

- Almacena todo el historial de transacciones
- Más de 500k bloques
- Casi 300M de transacciones
- 150 Gbytes
- 9 años de datos

Graphical visualization of blockchain data

Máster en Seguridad de las TIC

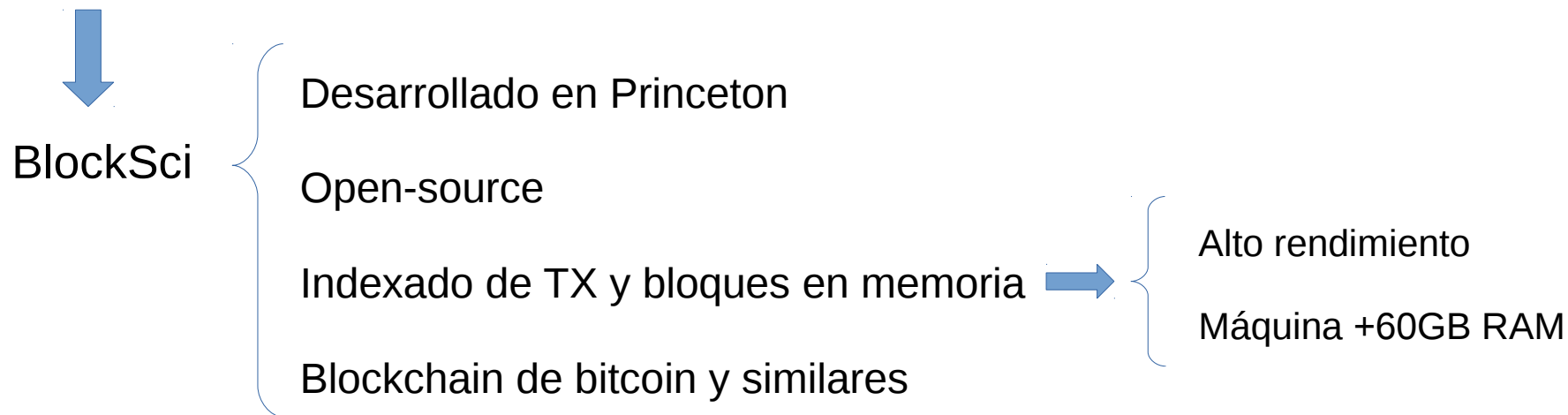
Autor: Federico Laport Rivas

Director: Jordi Herrera Joancomartí



Análisis de la blockchain

Nuevas aplicaciones de análisis



Graphical visualization of blockchain data

Máster en Seguridad de las TIC

Autor: Federico Laport Rivas

Director: Jordi Herrera Joancomartí



Parámetros de análisis propuestos

Relacionados con:

- Gastos de mineros
- Capacidad de la red
- Tipos de outputs
- Aplicaciones sobre blockchain



1. Ratio de gasto de coinbase TX
2. Tiempo hasta el gasto de coinbase TX
3. Número de direcciones en output de coinbase TX

Parámetros de análisis propuestos

Relacionados con:

- Gastos de mineros
- Capacidad de la red
- Tipos de outputs
- Aplicaciones sobre blockchain



4. Throughput de la red bitcoin

5. Número de TX por bloque

(4 y 5 son proporcionales sólo en teoría)

Graphical visualization of blockchain data

Máster en Seguridad de las TIC

Autor: Federico Laport Rivas

Director: Jordi Herrera Joancomartí

Parámetros de análisis propuestos

Relacionados con:

- Gastos de mineros
- Capacidad de la red
- Tipos de outputs
- Aplicaciones sobre blockchain



6. TX con TIMELOCKS

7. TX con MULTISIGNATURE

8. TX Pay-to-script-Hash (P2SH)



+SegWit?

Parámetros de análisis propuestos

Relacionados con:

- Gastos de mineros
- Capacidad de la red
- Tipos de outputs
- Aplicaciones sobre blockchain



9. TX con OP_RETURN

10. Aplicaciones conocidas

Graphical visualization of blockchain data

Máster en Seguridad de las TIC

Autor: Federico Laport Rivas

Director: Jordi Herrera Joancomartí



Visualizaciones propuestas

Para todos los parámetros, dos tipos de visualización:

1. Matriz de píxels:

1 pixel = 1 bloque

Basada en utxo-stats.com

2. Gráfica de línea clásica:

En vertical

Graphical visualization of blockchain data

Máster en Seguridad de las TIC

Autor: Federico Laport Rivas

Director: Jordi Herrera Joancomartí



Visualizaciones propuestas

Para todos los parámetros, dos tipos

1. Matriz de píxels:

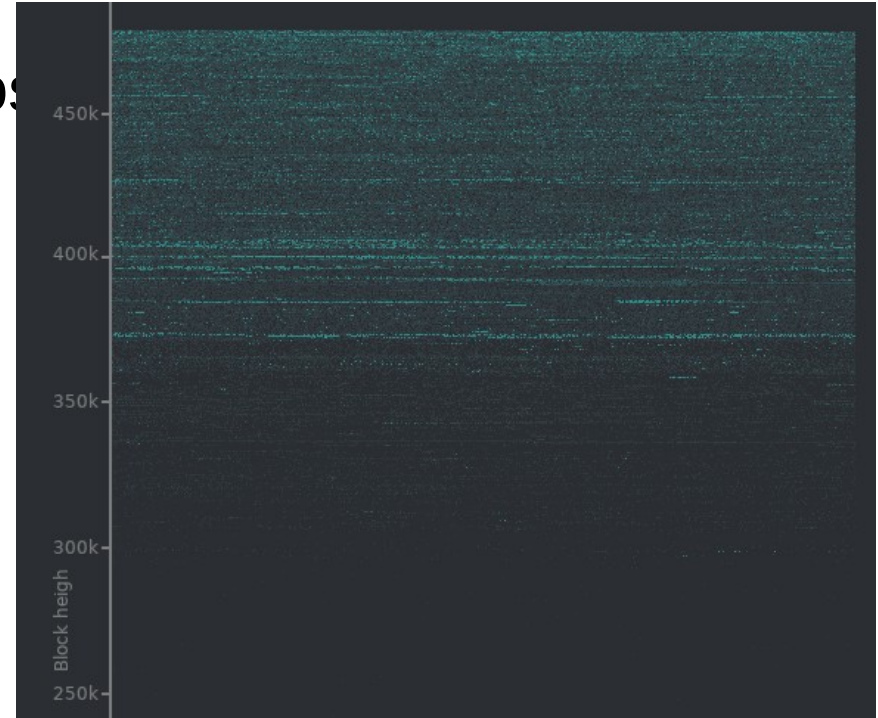


1 pixel = 1 bloque

Basada en utxo-stats.com

2. Gráfica de línea clásica:

En vertical



Visualizaciones propuestas

Para todos los parámetros, dos tipos

1. Matriz de píxels:

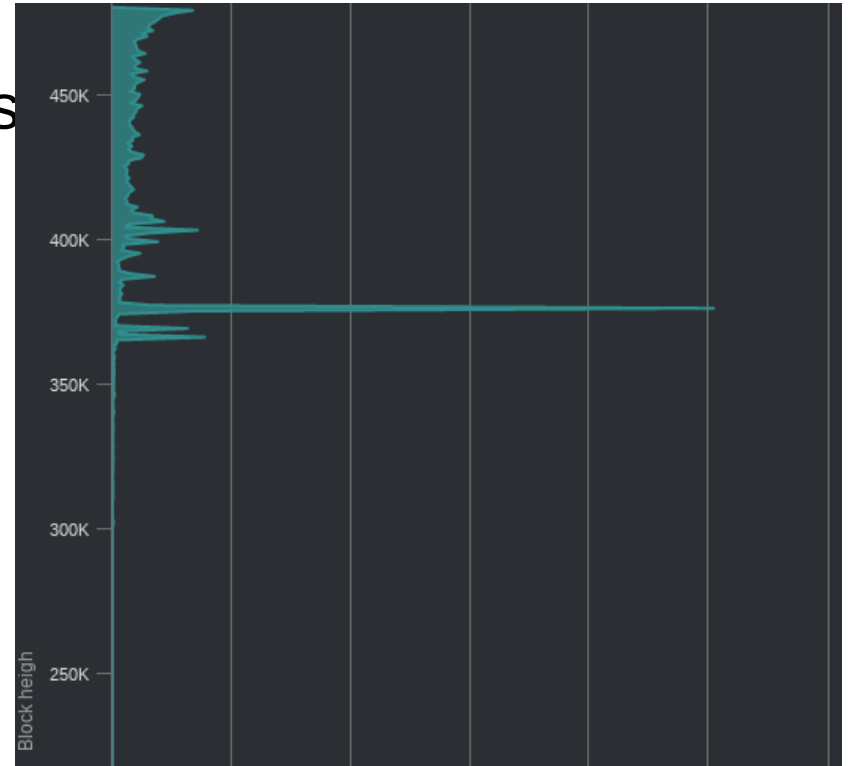
1 pixel = 1 bloque

Basada en utxo-stats.com

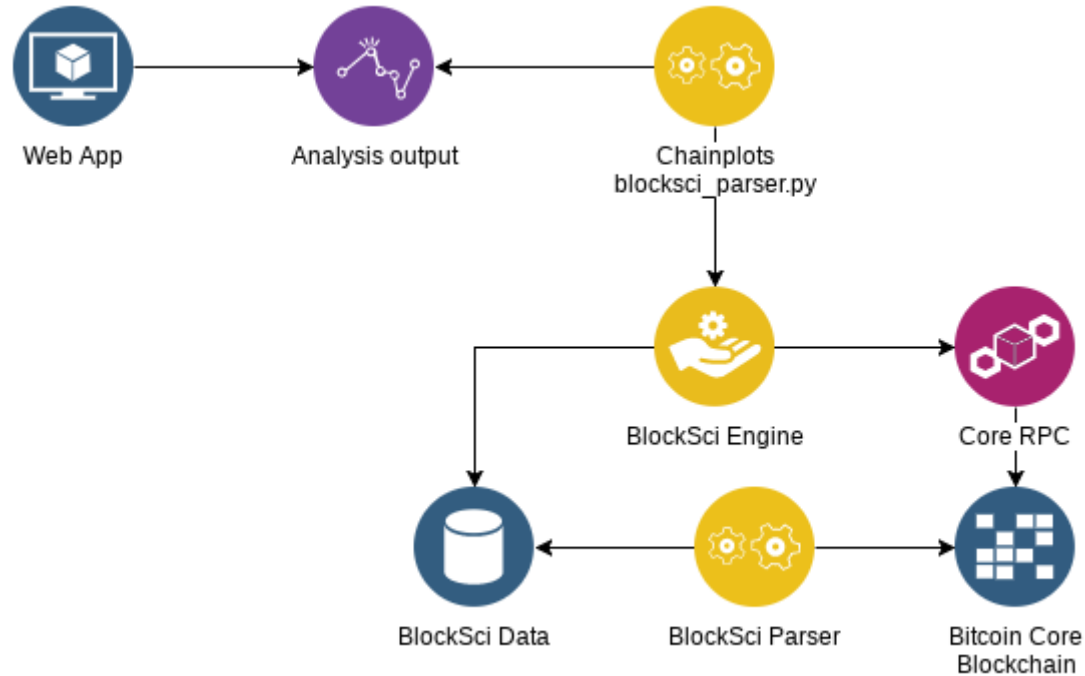
2. Gráfica de línea clásica:



En vertical



Esquema del sistema



Graphical visualization of blockchain data

Máster en Seguridad de las TIC

Autor: Federico Laport Rivas

Director: Jordi Herrera Joancomartí

Scripts de análisis

- Escritos en Python

- Script contra RPC (Semanas) (330 LOC)

```
1 import bitcoin.rpc
```

- Script contra BlockSci (Horas) (230 LOC)

```
1 import blocksci
2 from blocksci import Tx
```

- Script de datos aleatorios

```
1 import random
```

- Script agrupador en miles (gráfica de línea)

```
if i % 1000 == 0:
```

Graphical visualization of blockchain data

Máster en Seguridad de las TIC

Autor: Federico Laport Rivas

Director: Jordi Herrera Joancomartí

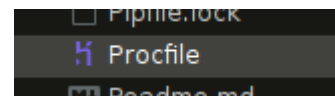


Aplicación web (back-end)

- Escrito en Python (Django Web Framework)



- Funciones: Servir estáticos, Templating páginas, Parámetros a Frontend.
- Configurado para desarrollo o Heroku:
<https://chainplots.herokuapp.com/>



Generando gráficas (front-end)

- Tech stack: JQuery, Bootstrap, Highcharts.js
- Matriz de píxels generada con JavaScript en un canvas HTML
- Gráfica de línea generada con Highcharts.js
- Fichero único (408 LOC): chainplots/static/chainplots.js

Conclusiones y propuestas de futuro

- Algunos gráficos revelan información interesante
- Futuro: Actualización en tiempo real (inviabile BlockSci)
- Futuro: Detección SegWit

Conclusiones y propuestas de futuro

Veámoslo funcionando >>>

Graphical visualization of blockchain data

Máster en Seguridad de las TIC

Autor: Federico Laport Rivas

Director: Jordi Herrera Joancomartí



Muchas gracias

Graphical visualization of blockchain data
Máster en Seguridad de las TIC
Autor: Federico Laport Rivas
Director: Jordi Herrera Joancomartí

