



Detecting Ransomware Payments

Harry Smith



Goal

Use records of **Bitcoin** transactions
to detect **Ransomware** payments

The background image shows a person from behind, sitting at a desk with several laptops. The laptop screens display a red background with white binary code (0s and 1s) and the word "RANSOMWARE" in large, bold, white capital letters. A large, semi-transparent red text graphic is overlaid on the image, reading "\$7.5 billion" in a serif font, with "from the US economy in 2019" in a smaller, white sans-serif font below it.

\$7.5 billion

from the US economy in 2019



67%

of victims pay

Data

From study at University of Texas, Dallas by Akcora et al.

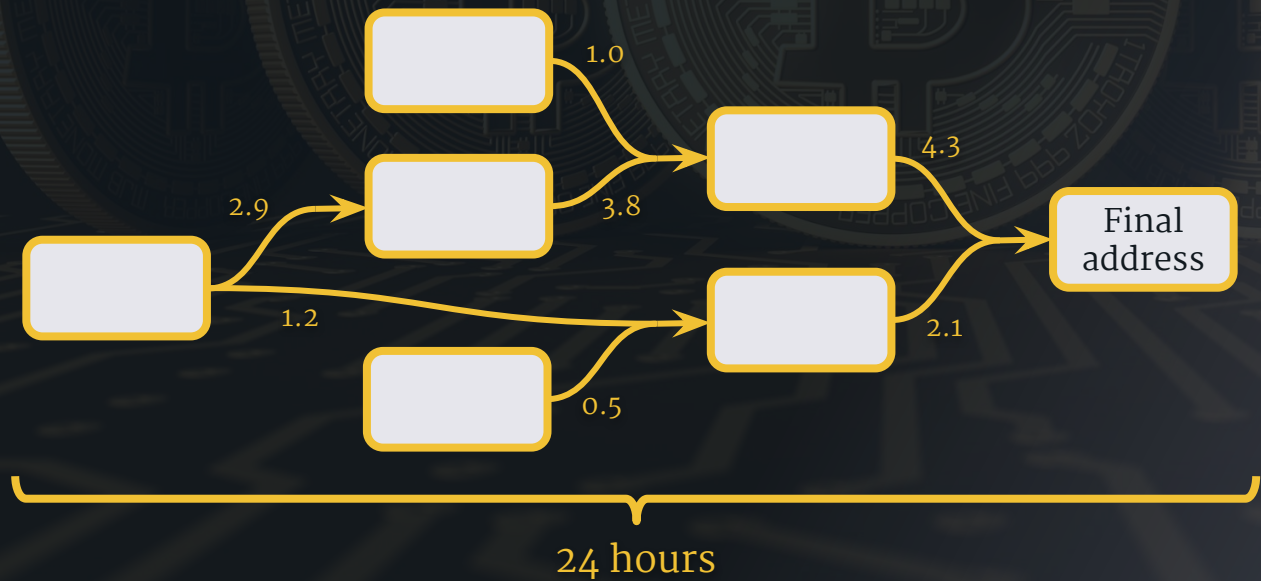
- ❖ Jan 2009 – Dec 2018
- ❖ All **bitcoin addresses** which receive ≥ 0.3 bitcoin in each 24 hour period
- ❖ Labels only include reported **Ransomware** addresses

Data

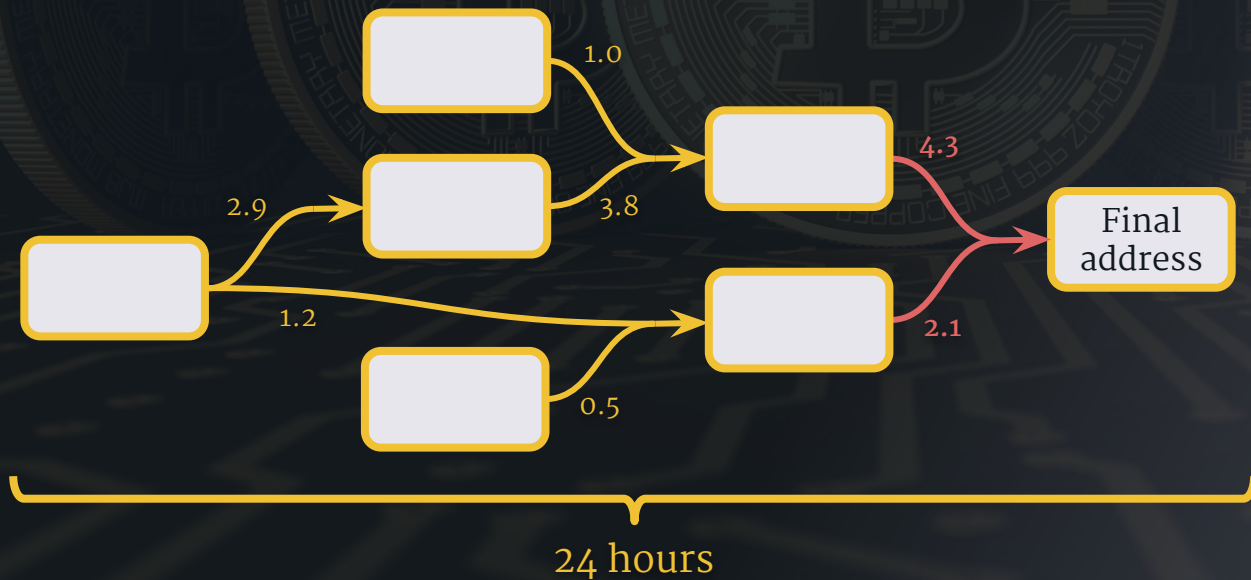
The background of the slide is a dark, textured surface. It features five Bitcoin coins arranged in a slightly overlapping row across the top half. The coins are dark with a lighter, embossed design. Below the coins, the entire background is covered with a faint, glowing circuit board or PCB pattern, which adds a technological and digital feel to the overall aesthetic.

Final
address

Data

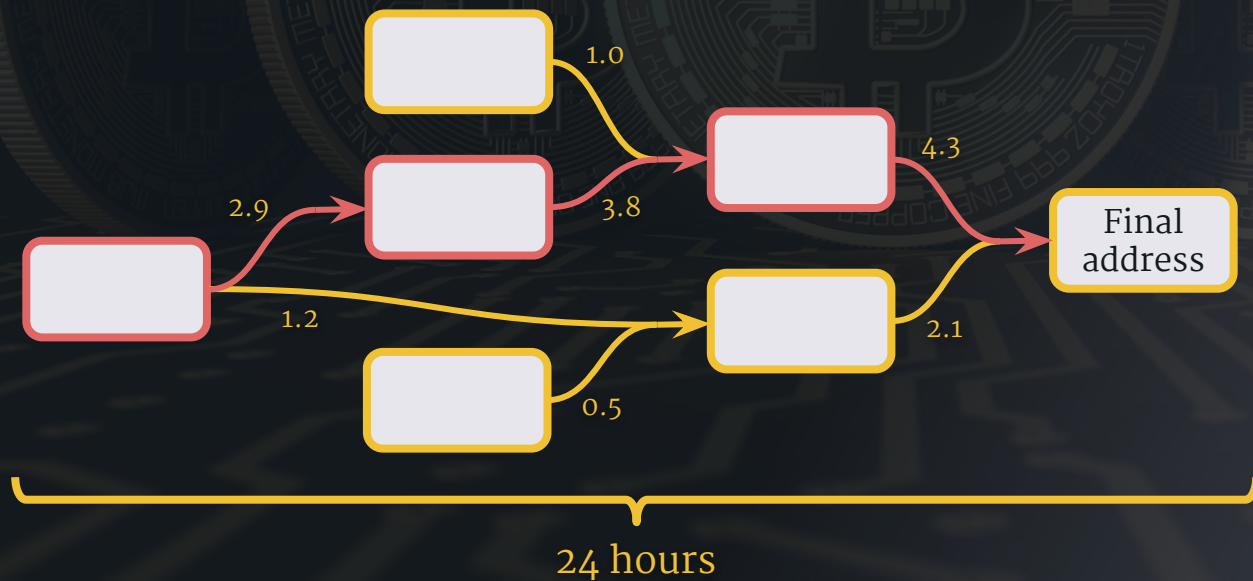


Data



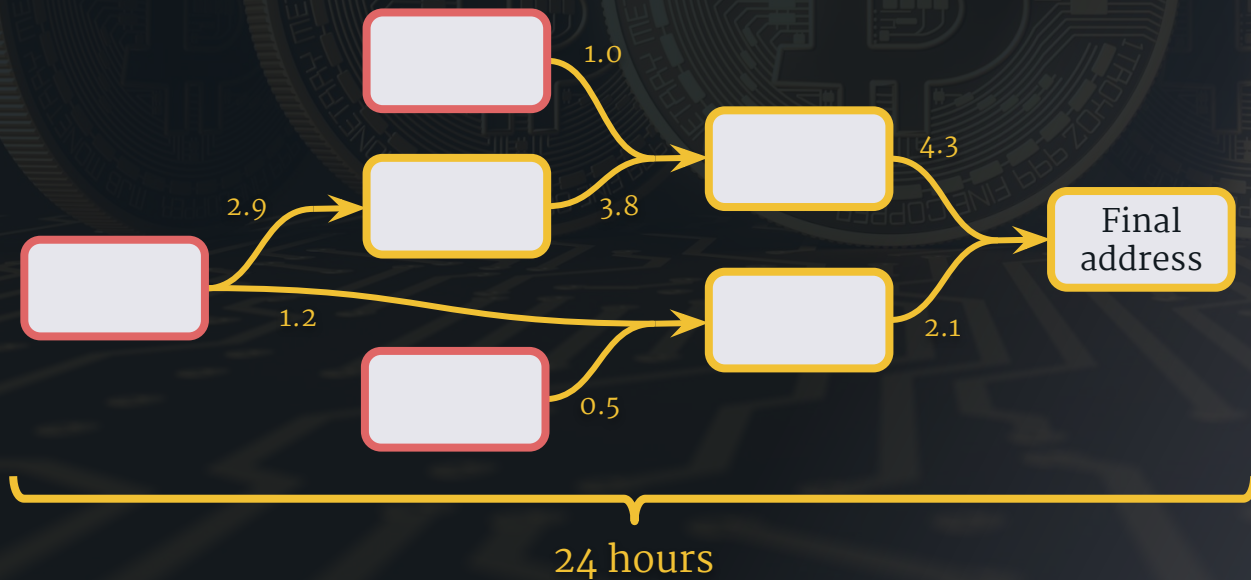
Feature	Row data
Income	6.4

Data



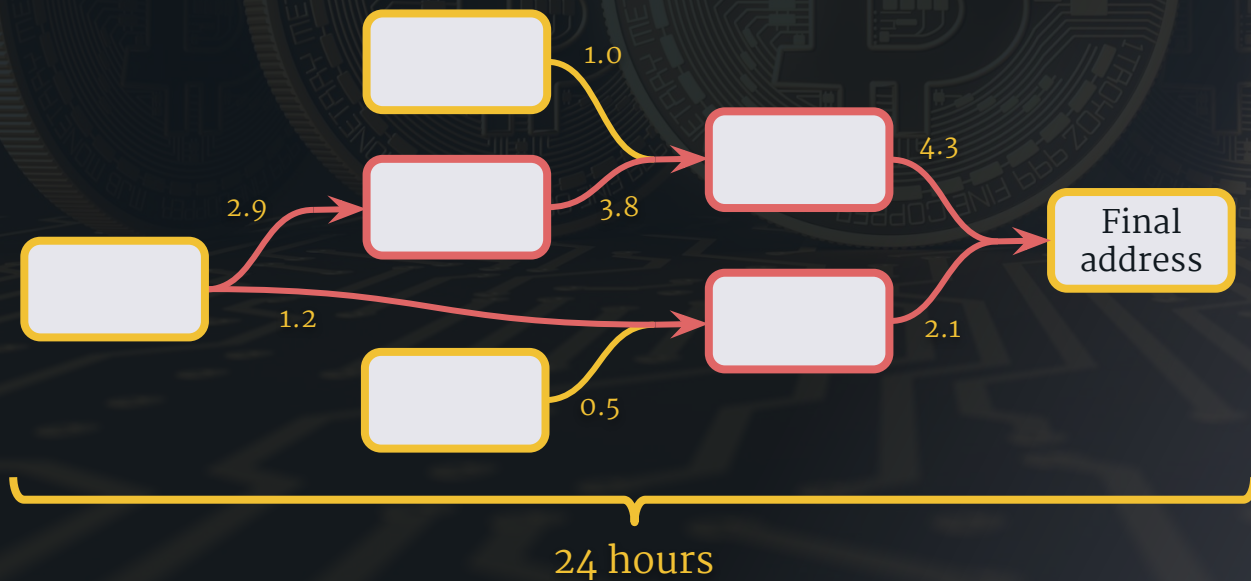
Feature	Row data
Income	6.4
Length	3

Data



Feature	Row data
Income	6.4
Length	3
Count	3

Data



Feature	Row data
Income	6.4
Length	3
Count	3
Loop	1

Modelling

Round 1

- ❖ Uploaded data onto Spark cluster on AWS
- ❖ Modelling done with PySpark
- ❖ Final model was a Gradient Boosted Tree Classifier:

Accuracy = 66.7%

Recall = 34.5%

Frequency of Attacks

First Wave

■ CryptoLocker

■ CryptoWall

(more loops, higher length)

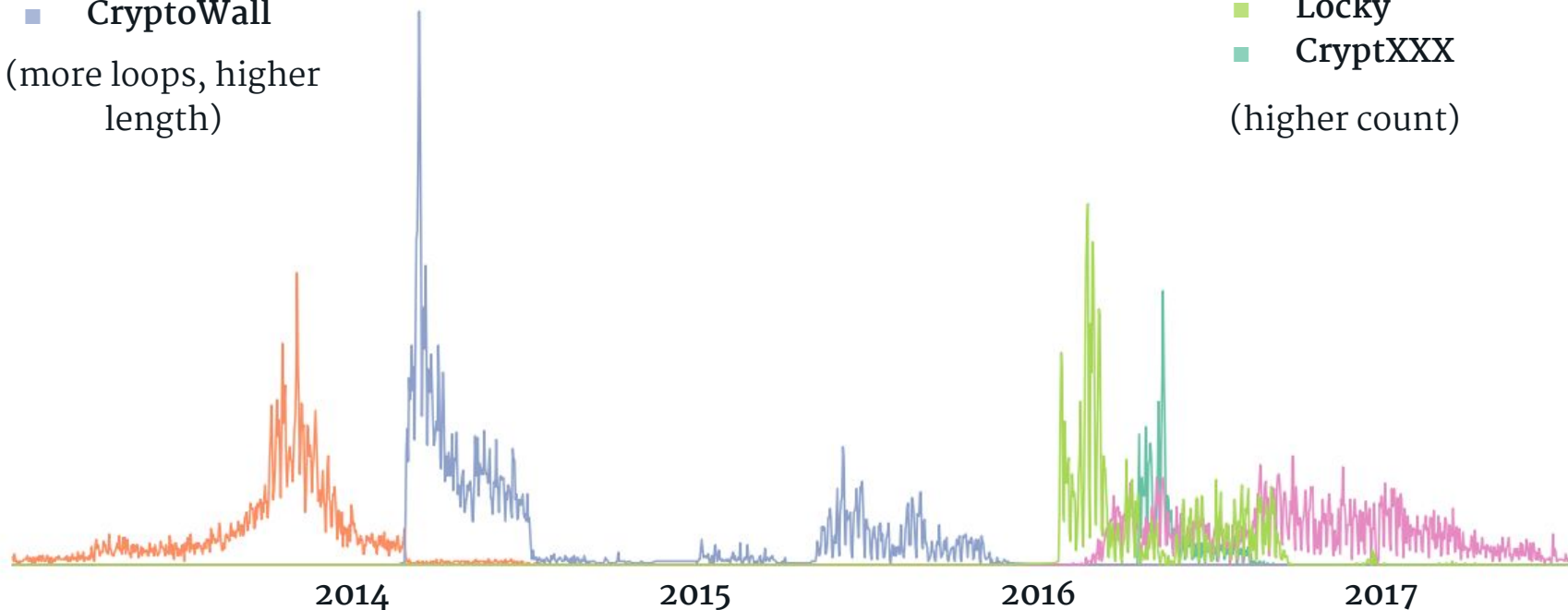
Second Wave

■ Cerber

■ Locky

■ CryptXXX

(higher count)



Modelling

Round 2

Modelled with scikit-learn, Random Forest Classifier

- First Wave:
- ◆ Accuracy = 71.7%
 - ◆ Recall = 59.4%
 - ◆ 30 false positives for each true positive

Modelling

Round 2

Modelled with scikit-learn, Random Forest Classifier

- Second Wave:
- ❖ Accuracy = 66.3%
 - ❖ Recall = 83.4%
 - ❖ 15 false positives for each true positive

Conclusion

- ❖ **Ransomware** has exhibited different patterns of behaviour over time
- ❖ Ability to detect **Ransomware** payments is greatly improved by targeting groups with similar behaviour



Thank you for watching

Harry Smith
hsmith14680@gmail.com
Linkedin: hsmith14680
Github: hsmith24