

Monero and ZCash. In this project, you will need to:

PART 1• Describe in detail how these protocols work. Differences and similarities.

PART 2• Recent attacks: review papers published in the last two years (at least) at major security conferences: IEEE S&P, ACM CCS, NDSS, etc.

PART 1

Name	Assigned task
Samson	Describe in detail how Zcash protocol works
Eunice	Describe in detail how Monero protocol works
Olivia	Introduction, Differences and Similarities between Zcash and Monero, Conclusion

PART 2

Name	Assigned Task
Benjamin	Recent Attack on Zcash
Roseline	Recent Attack on Zcash
Fredrick	Recent Attack on Zcash
Emmanuel: Analysis of transactional flooding against Monero	Recent Attack on Monero
Oreoluwa: Anonymity Attack on Monero	Recent Attack on Monero
Dami: Monero Ring attack recreating Zero Mixin Transaction	Recent Attack on Monero

Effect	
--------	--

<https://medium.com/vauld/zcash-vs-monero-which-is-the-superior-privacy-coin-2b144d59d6b2>

<https://www.gemini.com/cryptopedia/what-is-zcash-blockchain-protocol>

<https://z.cash>

https://zcash.readthedocs.io/en/latest/rtd_pages/basics.html

https://zcash.readthedocs.io/en/latest/rtd_pages/protocol.html

Abstract

Introduction

Zcash

Monero

Differences & Similarities

Attacks

Conclusion