A SURVEY ON MONERO AND ZCASH

PROJECT SUMMARY

Monero and ZCash are two of the most popular cryptocurrencies that prioritize user anonymity and security, as well as privacy. We will be analyzing and assessing these two privacy-focused cryptocurrencies in this project. The survey focuses on a thorough knowledge of how each protocol works and identifies its strengths and weaknesses. We will be examining recent attacks that were addressed at major security conferences and provided an in-depth explanation of the privacy and security properties of these two cryptocurrencies, as well as any potential weaknesses.

We are a team of six and we have divided the work into three parts-

1. Introduction, Working of Monero and ZCash Protocols
2. Recent Attacks and Countermeasures
3. Similarities and Differences, and Conclusion

The work contribution is given in the table below:

| S.No | Student Name | Student ID | Work contribution |
| --- | --- | --- | --- |
| 1 | Alekhya Velicheti | 40222533 | Recent Attacks and Countermeasures |
| 2 | Amukthamalyada Vellanki | 40222749 | Introduction, Working of Monero and ZCash Protocols, and Documentation |
| 3 | Gurumurthy Anagandhula | 40218549 | Similarities, Differences and Conclusion |
| 4 | Lakshmi Vintha | 40221985 | Recent Attacks and Countermeasures |
| 5 | Shankar Teja Yalavarthy | 40225894 | Introduction, Working of Monero and ZCash Protocols, and Documentation |
| 6 | Yashwanth Reddy Bandaru | 40218189 | Similarities, Differences and Conclusion |