Summary 1

Joshua Shilts

April 2021

1 Summary

In this article researchers explain and explore known vulnerabilities and mitigation techniques in Block chain. I found this interesting because I hear a lot about how secure block chain is, so reading this showed me that it is more secure but also has know vulnerabilities. One of these vulnerabilities was Public-key and address mismatch. This talked about how a blockchains wallet public key can be truncated and if it is not bound to a specific pair then multiple key can exist for a wallet. This is relevant because I am taking data communication II and we learned about public and private keys and it is awesome that I can apply what I learned to further understand this article.

2 Abstract

Blockchains are not invulnerable. There are known vulnerabilities in various blockchain ecosystem components. This field note describes some vulnerabilities observed in smart contracts and node software, their exploitation, and how to avoid them, with a focus on the Ethereum ecosystem.

References

[1] Nils Amiet. 2021. Blockchain Vulnerabilities in Practice. Digital Threats: Research and Practice 2, 2, Article 8 (April 2021), 7 pages. DOI:https://doi-org.umasslowell.idm.oclc.org/10.1145/3407230