Research Methods
SCS3216

Assignment 01

17000912

Bitcoin: A Peer-to-Peer Electronic Cash System [1]

- Researchers observed the current trust-based online transaction model.
- Studied those models and identified problems within those.
- Suggested mechanisms to overcome each of the problems.
- Hypothesised that attacker can’t break the coin without having more computing power than all the others combined.
- Introduces an experiment to test the above hypothesis.
- Gathered data from the test and analysed to make the conclusion sustaining the hypothesis

Step	
Observations	
Preliminary Study	
Problem Definition	
Theoretical framework	
Hypothesis	
Experimental Design	
Data Gathering	
Data Analysis	
Conclusion	

A Practical De-mixing Algorithm for Bitcoin Mixing Services [2]

- Researchers observed address mixing used for illegal activities.
- Analysed major mixing services and identified variables of those services.
- Hypothesised relationship between variables (fee, delay, max_count) and the output.
- Implemented an algorithm and tested it resulting in 99.14% accuracy.
- Evaluated error cases and reasoned them.
- Concluded that they have implemented a general demixing algorithm with about mentioned accuracy.

Step	
Observations	
Preliminary Study	
Problem Definition	
Theoretical framework	
Hypothesis	
Experimental Design	
Data Gathering	
Data Analysis	
Conclusion	

The Unreasonable Effectiveness of Address Clustering [3]

- Researchers observes that address clustering unintentionally disclose information.
- Studies some related work.
- Identifies address cluster counts and sizes to quantify the levels of address reuse and cluster merging.
- Then they study the formation and structure of address clusters.
- Finally concluded the paper while mentioning future work.

Step	
Observations	
Preliminary Study	
Problem Definition	
Theoretical framework	
Hypothesis	
Experimental Design	
Data Gathering	
Data Analysis	
Conclusion	

Best among the three

A Practical De-mixing Algorithm for Bitcoin Mixing Services

VS Bitcoin: A Peer-to-Peer Electronic Cash System

- Bitcoin paper follows all the steps of the scientific method.
- But it only experiments and proof only one aspect (the attacker fails unless they have more computing power than all the others combined).
- Other features are suggested but not tested and proofed.

VS The Unreasonable Effectiveness of Address Clustering

- Paper observes the problem and find the effective parameters.
- But researchers don’t experiment and prove the hypothesis that they have generated successfully.

Conclusion

- Each paper has found a problem and then suggested solutions.
- And some of these papers are widely known and used in the respective scientific communities.
- But when we consider which paper follows all the steps of scientific properly the **Practical De-mixing Algorithm for Bitcoin Mixing** Services paper surpass the other two.

References

[1] Wright, Craig S. “Bitcoin: A Peer-to-Peer Electronic Cash System.” *SSRN Electronic Journal*, 2008, doi:10.2139/ssrn.3440802.

[2] Hong, Younggee, et al. “A Practical De-Mixing Algorithm for Bitcoin Mixing Services.” *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts - BCC '18*, 2018, doi:10.1145/3205230.3205234.

[3] Harrigan, Martin, and Christoph Fretter. “The Unreasonable Effectiveness of Address Clustering.” *2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, 2016, doi:10.1109/uic-atc-scalcom-cbdcom-iop-smartworld.2016.0071.