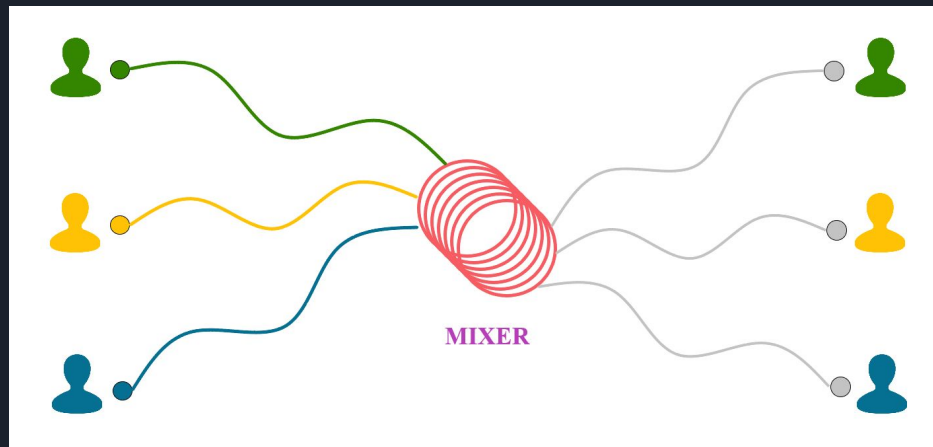


Mixing based privacy mechanisms are insufficient

Mixing what?

There are two main components in mixing based privacy mechanisms.

1. Unlinking senders and receivers
2. Masking the transaction amount



Pic credit: Devashish Tomar



Linking the unlinkable transactions

- Anonymity set is limited in size
- Churning can help
- Analytics companies have access to more data than normal users
- Every transaction that gets de-anonymized reduces anonymity of others
- Bad actors can poison the anonymity set
- A big enough network of nodes can collect extra information over time

Attack on Wasabi




Samourai Wallet
@SamouraiWallet



PSA

There exists an entity operating as a de-anonymizing “hot wallet” present within transactions by Wasabi since June 1, 2019. This entity has been clustered very easily due to flagrant address reuse, and downright bizarre behavior. This impacts ALL users since June.

<https://twitter.com/SamouraiWallet/status/1153253164298227713>



FloodXMR: Low-cost transaction flooding attack with Monero's bulletproof protocol

“An attacker can take advantage of Monero's Bulletproof protocol, which reduces transaction fees, to flood the network with his own transactions and, consequently, remove mixins from transaction inputs. Assuming an attack timeframe of 12 months, our findings show that an attacker can trace up to 47.63% of the transaction inputs at a cost of just 1,746.53 USD. Moreover, we show also that more than 90% of the inputs are affected by our tracing algorithm.”

<https://eprint.iacr.org/2019/455.pdf>

Mixing based
privacy
mechanisms are
awesome but
don't blindly trust
them.



Thank You!

Reach out to me

Email: hi@mudit.blog

Twitter: [Mudit_Gupta](https://twitter.com/Mudit_Gupta)

Github: [maxsam4](https://github.com/maxsam4)



POLYMAT^H
THE SECURITIES TOKEN PLATFORM

Presentation by Mudit Gupta

YOU FOUND A STAR

Speaker Track



dropparty.tech



<https://mudit.blog/>