Matt Odell @matt_odell

24 Aug • 19 tweets • matt_odell/status/1297977489424371714

1/ One way to attack coinjoin users is through a sybil attack.

A sybil attack in this context is when an attacker attempts to flood coinjoin rounds with their own transactions. This can allow them to track their target user(s) through process of elimination.

2/ If an attacker has knowledge of other users' transactions they can also leverage that to make their attack more effective.

Both samourai & wasabi attempt to make this type of attack expensive by incorporating a coinjoin fee.

3/ The purpose of this coinjoin fee is that it makes a sybil attack prohibitively expensive at scale as long as there is substantial liquidity from other sources. Since the fee is paid to them, it naturally doesn't do anything to prevent them from doing a sybil attack themselves.

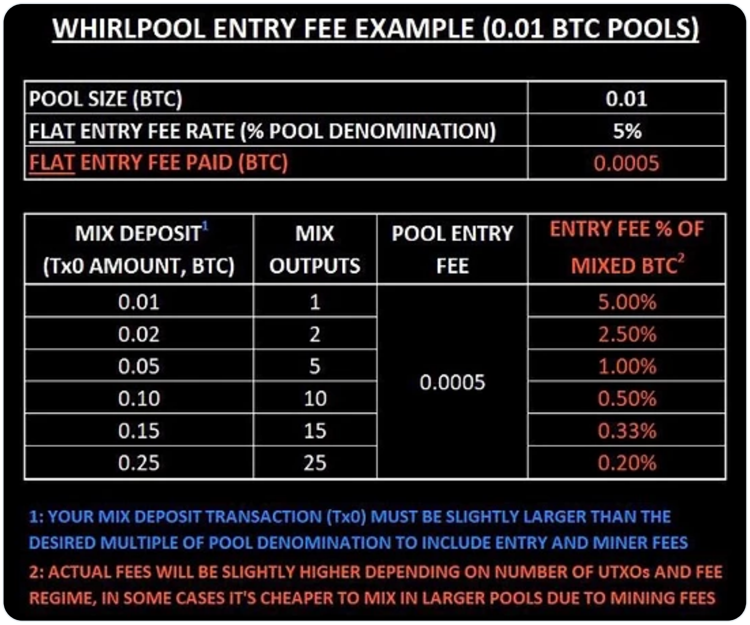
4/ The two implementations differ a bit at this point.

Wasabi actually has a reverse incentive that rewards them with higher fee revenue if they attempt to sybil or pump liquidity into the system since fees by users scale up with the number of utxos in a round.

5/ Wasabi is also setup in a way that allows participants to choose which rounds they participate in which can allow an external sybil attacker to pick and choose which rounds to attack based on their desired target. This reduces the cost of an attempted sybil attack.

6/ Samourai on the other hand does not allow users to choose their rounds. Round selection is random. Furthermore, if you attempt to run multiple clients simultaneously - which is what an attacker would do - you pay a higher effective fee then if you run a single client.

7/ To pay the lower effective fee, samourai requires you to queue your total desired coinjoin amount in the same TX0 transaction. Any child utxos in this queue transaction are not included in the same rounds as each other by design.



WHIRLPOOL ENTRY FEE EXAMPLE (0.01 BTC POOLS)

POOL SIZE (BTC)	0.01
FLAT ENTRY FEE RATE (% POOL DENOMINATION)	5%
FLAT ENTRY FEE PAID (BTC)	0.0005

MIX DEPOSIT[1] (Tx0 AMOUNT, BTC)	MIX OUTPUTS	POOL ENTRY FEE	ENTRY FEE % OF MIXED BTC[2]
0.01	1	0.0005	5.00%
0.02	2		2.50%
0.05	5		1.00%
0.10	10		0.50%
0.15	15		0.33%
0.25	25		0.20%

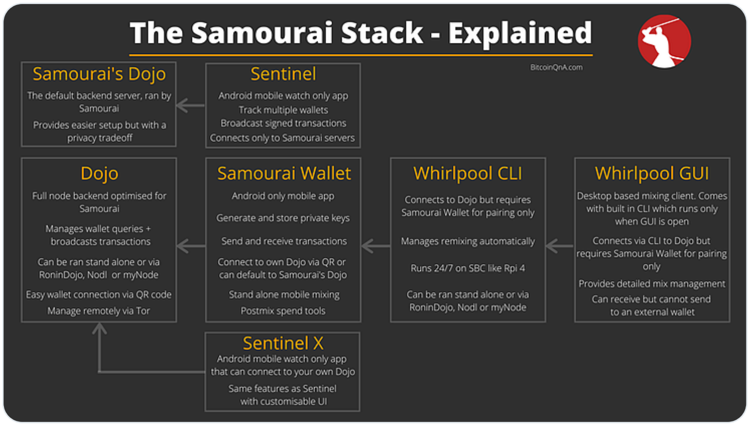
[1] YOUR MIX DEPOSIT TRANSACTION (Tx0) MUST BE SLIGHTLY LARGER THAN THE DESIRED MULTIPLE OF POOL DENOMINATION TO INCLUDE ENTRY AND MINER FEES

[2] ACTUAL FEES WILL BE SLIGHTLY HIGHER DEPENDING ON NUMBER OF UTXOs AND FEE REGIME, IN SOME CASES IT'S CHEAPER TO MIX IN LARGER POOLS DUE TO MINING FEES

8/ Another important piece of information is that the more coinjoin rounds you do, the more difficult it is to be the victim of a sybil attack since the attacker will need to be in every round. Samourai provides an incentive to remix while remixing in wasabi costs more in fees.

9/ samourai tangent:

There are two types of samourai users. Those who use their own node and those who trust samourai's node. If you don't use your own node then you trust samourai with your transaction history but not IP address(es) since the wallet defaults to Tor.



The Samourai Stack - Explained

BitcoinQnA.com

Samourai's Dojo
The default backend server, ran by Samourai
Provides easier setup but with a privacy tradeoff

Sentinel
Android mobile watch only app
Track multiple wallets
Broadcast signed transactions
Connects only to Samourai servers

Dojo
Full node backend optimised for Samourai
Manages wallet queries + broadcasts transactions
Can be ran stand alone or via RoninDojo, Nodl or myNode
Easy wallet connection via QR code
Manage remotely via Tor

Samourai Wallet
Android only mobile app
Generate and store private keys
Send and receive transactions
Connect to own Dojo via QR or can default to Samourai's Dojo
Stand alone mobile mixing
Postmix spend tools

Whirlpool CLI
Connects to Dojo but requires Samourai Wallet for pairing only
Manages remixing automatically
Runs 24/7 on SBC like Rpi 4
Can be ran stand alone or via RoninDojo, Nodl or myNode

Whirlpool GUI
Desktop based mixing client. Comes with built in CLI which runs only when GUI is open
Connects via CLI to Dojo but requires Samourai Wallet for pairing only
Provides detailed mix management
Can receive but cannot send to an external wallet

Sentinel X
Android mobile watch only app that can connect to your own Dojo
Same features as Sentinel with customisable UI

10/ If samourai were to attempt to sybil attack full node (dojo) users this xpub info could be used to reduce attack cost. If their wallet server were to get compromised or they are compelled to disclose it by gov, an external attacker could also use it to reduce attack cost.

11/ Is this a concern for full node users? Yes and no.

Let's circle back to item (3) in this thread. A key aspect of sybil resistance is the amount of liquidity from sources acting in "good faith." Liquidity not controlled by an attacker.

12/ If light client users provide the majority of liquidity then it becomes a threat to full node users. Unfortunately it's impossible to verify how much liquidity comes from these users without trusting Samourai. A user only knows how much liquidity they provide themselves.

13/ To assess this risk we will have to go into further nuance.

Samourai whirlpool is compromised of two types of users. Those doing on-demand coinjoin and those locking up liquidity 24/7 to participate in free remixes.

14/ In order to participate 24/7 you have to run whirlpool cli on an always on computer. Usually a SBC, such as a raspi. These users tend to be more tech savvy and privacy focused, if they are going to go through the trouble it stands to reason they will also run their own node.

15/ Node packages such as myNode and RoninDojo which make it easy to run whirlpool cli also offer the user to easily run their own node (dojo) alongside it.

Connecting to your own node or a friend's node is easy in samourai. You simply scan a QR code connecting it through Tor.

16/ For this reason, I suspect that most light client users are (1) not adding much liquidity and (2) aren't running it 24/7. As such, it stands to reason that the majority of liquidity is being provided by users using their own node or a friend's node rather than samourai's.

17/ To circle back, this sybil risk is not unique to samourai. If a single external actor is providing a substantial amount of liquidity to wasabi - especially a KYC exchange - that can also degrade the quality of coinjoin rounds if their utxo data is shared, leaked, or stolen.

18/ Last but not least, these risks can be further mitigated across all implementations by making it easy for users to do uncoordinated coinjoin rounds with people they trust. You can already do two wallet coinjoins in samourai wallet and they are working on making that easier.

19/ Since these uncoordinated coinjoins do not include external actors they are inherently not subject to sybil attacks. You do however have to trust the person you coinjoin with. Used in combination with coordinated coinjoin rounds they can be very effective.

• • •