An Analysis and Disclosure Regarding the Deterministic Nature of the Wasabi Wallet CoinJoin Algorithm

Abstract: Wasabi Wallet is a bitcoin wallet with privacy enhancing tools built in that are designed to break the link between inputs and outputs of a transaction. Bitcoin transactions are recorded on a public ledger referred to as the "blockchain". These types of privacy enhancing tools are popular with users of the Bitcoin network, and are often used to obtain a basic level of financial privacy from the prying eyes of the general public. The primary method employed to break these links within the Wasabi Wallet software is their implementation of the "ZeroLink" coinjoin framework. Coinjoin is commonly referred to a "mixing" or "tumbling". In this paper, we focus primarily on two vulnerabilities discovered by OXT Research analysts in the Wasabi Wallet client and coordinator software that when exploited break the fundamental proposition offered in ZeroLink coinjoin by allowing the attacker to deterministically predict which transaction outputs of the targeted wallet will be selected for each round of mixing.

August 21, 2020

"**LaurentMT"**: OXT Research,
Email: laurent@oxtresearch.com

"ErgoBTC": OXT Research
Email: **ergo@oxtresearch.com**

I. INTRODUCTION

In late July 2020, OXT Research analysts were working on an analysis of bitcoin flows related to the recent "Twitter Hacker".

As it was reported by multiple articles, a part of these funds had entered the Wasabi Wallet mixing software. That led us to work on an analysis of mixes related to these funds. Our first action was to gather information by analysing the main "peeling chain" of unmixed change outputs generated in these mix transactions. This is a standard way to attack coinjoin transactions for implementations that allow for unmixed change outputs as part of the actual coinjoin transaction.

After analysing the standard peeling chains, we decided to check if we could identify idiosyncrasies of Wasabi Wallet software that would allow us to weaken the anonymity sets of some mixed outputs potentially controlled by the hacker.

The approach used here is similar to one used previously for attacking coinjoin transactions created by the "JoinMarket" software as it leverages additional information based on the specific coinjoin algorithm. The vulnerabilities of leveraging additional information about the CoinJoin algorithm has largely been ignored by the Bitcoin privacy community but unlikely to have been ignored by malicious actors.

In reviewing the code of both the Wasabi Wallet client and the Wasabi coinjoin coordinator looking for such idiosyncrasies we identified the first vulnerability.

II. VULNERABILITY #1

Review of the Wasabi Wallet code base led us to the conclusion that there is no randomness introduced by the client or by the coordinator during the selection of TXOs (transaction outputs) that will participate in a given mix.

Within the code of the Wasabi Wallet client, the unique random factor that we were able to find is related to the switch between "lazy mode"/"non lazy mode" [1] but this mechanism provides only a weak protection considering that it only triggers if the selection of a single TXO or of a low number of TXOs has previously failed.

This lack of strong randomness consistently introduced by the client and/or the coordinator means that the system acts as a deterministic automaton.

For instance, the Wasabi Wallet client can be modelled as an automaton composed of:

> ***(A)*** *Table of Instructions that is the set of coin selection rules mainly defined in ClientState.GetRegistrableCoinsNoLock().*
>
> ***(B)*** *State Register storing the set of TXOs controlled by the wallet*
>
> ***(C)*** *Tape composed of cells storing events related to the mixing process ("input registration of round N starts", "input registration of round N ends", "confirmation of transaction associated to round N", etc...)*

2.1 – Consequences

The main consequence of this lack of strong endogenous randomness is that an observer having knowledge of events related to the mixing process and of the composition of the targeted wallet at a given *step N*, is able to predict which TXOs of the wallet will be selected for each round of mixing after *step N*, hence cancelling the benefits of the previous mixes.

Specifically, this means an attacker is able to use the coin selection algorithm to isolate remixed TXOs based on the coin selection rules. As a result, the anonset of the previous mix(es) does not contribute to the actual anonset.

Let us illustrate an example scenario of a typical coinjoin transaction with an additional coinjoin transaction after the preceding one, which is commonly referred to as a “remix”.

Remixing is widely recommend as a best practice and users of most coinjoin platforms are encouraged to remix their outputs for an increase in the overall anonymity set of the remixed outputs and increase "distance" between their entrance into the mixer and their current TXO(s).

The flow of a typical coinjoin with a remix is as follows:

1. ***round_N*** *generates a 0.1 mixed output* ***A***
2. *output* ***A*** *remixed by* ***round_N+1*** *into txo* ***B***

We would normally expect the anonymity set of remixed outputs to follow this formula:

EXPECTED REMIX ANONYMITY SET

$$anonset(B) = anonset(A) - 1 + anonset(round_{N+1})$$

Instead, deploying this vulnerability may result in a reduced anonset, and in some cases, drastically reduced.

ACTUAL REMIX ANONYMITY SET

$$anonset(B) = anonset(round_{N+1})$$

A second consequence of this first vulnerability is that anonymity sets of TXOs that weren't selected for a given round may also be decreased when applied to other wallets participating in the same round (process of elimination).

For example, if we know that

1. *mixed output **A** is controlled by the target wallet and created by **round_M***
2. *mixed output **A** wasn't selected for **round_N***
3. *TXO **B** also created by **round_M** and with the same denomination as **A,** was selected as an input of **round_N***

With this knowledge we can infer that **B** isn't controlled by the target wallet. This inference allows for a decrease of the anonset of both **A** and **B**.

The lack of consistent randomness introduced in the coin selection process negates the privacy gained by previous mixes, reducing the actual privacy to that of the most recent mix.

2.2 – The role of exogenous randomness

When we think about randomness we do so in two ways. Endogenous randomness can be thought of simply as having an origin that is inherent to the system. On the other hand, exogenous randomness has its source outside of the system.

So far we have determined that there is no endogenous randomness present in the Wasabi Wallet coin selection algorithm, however we have still excluded the case of exogenous randomness that may decrease the reliability of results provided by an attack based on this first vulnerability.

It's important to reiterate that exogenous randomness may have different sources. Thus, we're going to use the following typology of randomness.

TABLE 1 – TYPOLOGY OF EXOGENOUS RANDOMNESS

Type A	Randomness introduced by the user and for which the attacker has no prior knowledge. (e.g.: new funds unknown to the attacker are enqueued, user temporarily stops her client and resumes the mixing later, custom target anonset value set by the user, etc…).
Type B	Randomness introduced by events independent from the user. (e.g.: unconfirmed TXOs are rejected by the coordinator, connection failure, etc…).

2.3 – Typology of attackers

For this analysis we propose the following typology of attackers:

TABLE 2 – TYPOLOGY OF ATTACKERS

Type A Attacker	Attacker having the same knowledge as the coordinator (i.e. attackers with knowledge of the technical logs of the coordinator).
Type B Attacker	Attacker with no access to coordinator's technical logs but able to eavesdrop the Wasabi and Bitcoin network and, optionally, to participate in each round in order to gather additional information about the mixes.

(Type A) Attackers are subject to the limitations imposed by Type A exogenous randomness but aren't concerned by Type B exogenous randomness.

(Type B) Attackers are potentially subject to both types of exogenous randomness but they should be able to deal with some occurrences of Type B randomness.

For instance, a (Type B) Attacker can observe and analyse the transactions available on the bitcoin blockchain to detect if the rejection of unconfirmed TXOs has been activated by the coordinator.

III. VULNERABILITY #2

In order to mitigate the effects of exogenous randomness, both types of attackers can leverage a second vulnerability that is based on the existence of “peeling chains” composed of unmixed change outputs deterministically connected to the mixed outputs propagating across the Wasabi Wallet coinjoin transactions.

Much of the focus of our prior research into Wasabi Wallet focused on exploiting these peeling chains to undermine some of the benefits of the mixed transactions. These peeling chains leave a trail of metadata on the blockchain that cannot be overwritten or obfuscated. These peeling chains can reliably indicate the first mix a user participates in if a user does not remix.

3.1 – Beacons and Checkpoints

In the context of this attack, peeling chains can be leveraged against the system in a different way with the attacker viewing these unmixed change outputs as *"beacons of certainty"* because it is possible to identify which mixes have spent the unmixed change.

The attacker can also view these unmixed change outputs as *"expected checkpoints"* because it is possible to predict which mixes will spend the unmixed change output in absence of exogenous randomness

Thus, when an expected checkpoint doesn't match with the mixes generated by Wasabi, an attacker knows that there was an occurrence of exogenous randomness and he can start to investigate concurrent hypotheses of exogenous randomness that may lead to the observed results.

OXT Research analysts were able to confirm the “Beacon and Checkpoints” approach during testing. In one case, there was an expectation that a toxic change output would be mixed after the first two rounds of mixing, but after a few hours, mixing still hadn’t occurred.

After further analysis, it appeared that this TXO was repeatedly rejected by the coordinator because it was unconfirmed (like others TXOs controlled by the wallet).

Mixing resumed as expected after the transactions associated to the first two rounds were confirmed a few hours later.

This second vulnerability can be used by both types of attackers but we suspect that it's especially effective when used by (Type A) Attackers in order to mitigate the effect of Type A randomness.

IV. TESTING IN THE WILD

In early August 2020, a series of tests were completed that allowed OXT Research analysts to confirm that the coin selection algorithm implemented by the Wasabi Wallet client is indeed deterministic and that inputs selected for a given round could be predicted.

4.1 – Summary

From our observations, the main source of exogenous randomness during these tests seemed related to temporary scalability issues encountered by the coordinator and leading to TXOs failing to participate to mix rounds (see: PR: 4133[2], 4134[3], 4135[4], 4136[5], 4137[6]).

Technical issues like these ones make the interpretation of results more challenging for the (Type B) Attacker. However, these types of issues do not affect the (Type A) Attacker. For example: a failure during a registration phase or during the signing phase is part of information available internally available to the Wasabi Coordinator software.

Moreover, as we can expect that issues like these get fixed soon after being reported, this de facto decreases the randomness experienced by (Type B) Attackers.

4.2 – Principle of the test

We simulated 2 actors for this test of the attack.

TABLE 3 – TEST ACTORS

Alice	Simulates the Wasabi user targeted by the attack. Runs an unmodified Wasabi client. Sends 0.4 BTC (single UTXO) to her Wasabi Wallet and enqueues this UTXO for mixing with a target anonset target of 120.
Eve	Eve simulates an attacker tracking the funds controlled by Alice and leading to Wasabi mixes. She acts as a "low-level" (Type B) attacker. She eavesdrops the Wasabi coordinator

	but doesn't participate in any mixes. She runs a slightly modified Wasabi client that logs the details of mix rounds and if rounds failed or succeeded modifications made in ClientState.UpdateRoundsByStates().

4.3 – Detailing the attack

The supplemental spreadsheet *"analysis.ods"* provides a sample of a test illustrating how this attack can be used to decreases the anonset provided by multiple rounds of mixing.

The first sheet titled *TXOs* lists the first mixes and TXOs related to **Alice**'s activity during the test (plus the related bitcoin addresses and private keys)

The second sheet titled *Timeline* is a timeline of events built by **Eve** thanks to data gathered thanks to her Wasabi client.

The third sheet titled *Simulated Memory of Deterministic Automaton* is the different stages of the State Register (Alice's wallet) as predicted by Eve when running a deterministic automaton simulating Alice's Wallet.

Bold green cells identify elements modified by each step.

In the context of this specific test, the deterministic coins selection algorithm can be reduced to the following heuristic:

DETERMINISTIC SELECTION HEURISTICS

"Select the first available TXO covering the required funds with TXOs sorted by confirmation status, increasing anonset and decreasing amount"

This order corresponds to the order defined for the selection of a single TXO.

Comments in the last column try to make explicit the details of the heuristic for each step.

As predicted by our model of the attack, we can observe that:

- Remix of **[9e01:81]** by **[79bc]** leads to a first weakening of anonymity sets:
  - [9e01:81]: Adjusted anonset is **4** instead of expected anonset of 10
  - [79bc:33]: Adjusted anonset is **4** instead of expected anonset of 13
  - [79bc:46]: Adjusted anonset is **81** instead of expected anonset of 90
- Remix of **[79bc:46]** by **[3de0]** leads to a second weakening of anonymity sets:
  - [79bc:33]: Adjusted anonset is **2** instead of expected anonset of 13

    (2 TXOs with same amount as [79bc:33] are inputs of [3de0])
  - [79bc:46]: Adjusted anonset is **2** instead of expected anonset of 90

- [3de0:45]: Adjusted anonset is **53** instead of expected anonset of 142.

4.4 – Illustrating the attack

A supplemental diagram illustrating the contents of the Simulated Memory of Deterministic Automaton spreadsheet is attached to this report [Fig 1].

The diagram illustrates the ordered timeline of the Wasabi coinjoin network as observed by Eve (green underlined text). The diagram is ordered sequentially from top to bottom based on Eve's observed timeline.

Alice's TXOs are sorted into two buckets at each event. The left bucket represents Alice's TXO waiting list (coins available for registration to the next mix round).

The TXOs in the left bucket are ordered from top to bottom in the order specified by the deterministic coin selection algorithm. In the context of this test the deterministic coins selection algorithm can be reduced to the following heuristic:

DETERMINISTIC SELECTION HEURISTIC

"Select the first available TXO covering the required funds with TXOs sorted by confirmation status, increasing anonset and decreasing amount"

The details of why a TXO is not registered for a mix are included above the left bucket. The first sorted TXO meeting the coin mixing requirements is selected by algorithm and placed in the right bucket for mix registration.

Eve is able to marry her observed timeline, knowledge of Alice's wallet state at a given point in time (TXO and mixed output sizing), and the deterministic coin selection algorithm to predict the remixing of Alice's TXOs and exploit the attack.

V. SEVERITY

In our opinion, these vulnerabilities should be considered as **High/Critical.**

In the case of a mixed output being remixed, these vulnerabilities break the ZeroLink guarantee for the previous mix and cancel the benefits provided by the previous mix.

These vulnerabilities break the global guarantees provided to users by the mixer.

An effective attack against the user of a mixer doesn't require the de-anonymization of all user outputs. De-anonymizing or significantly reducing the anonset of a single TXO is often enough to advance an attack.

5.1 – Low Liquidity Mixes

For unlucky users participating in a final low liquidity mix (e.g. [105d...f55c] or [9035...1c9c]), the expected and actual anonymity set can be off by an order of magnitude.

5.2 – Widespread

Considering that these vulnerabilities have existed for a long time, it's our belief that if we were able to detect them, it's more than likely that they were already detected by someone else and perhaps already exploited in the wild.

VI. Potential Mitigations

As it was shown in previous sections, the unique protection currently available to users against these two vulnerabilities is the occurrence of exogenous randomness.

This cannot be considered as a satisfying solution, because protection should be consistent and verifiable and shouldn't rely on external factors which aren't under the control either of users or operators of the mixing platform. Relying on this type of randomness offers weak protection from (Type A) attackers.

It is the opinion of the OXT Research analysts that the best fix against these two vulnerabilities is the introduction of consistent randomness in client code (i.e. in ClientState.GetRegistrableCoinsNoLock()).

We understand that prioritizing the selection of some TXOs over others TXOs might be an important factor for Wasabi operations and we believe that it's still possible to do that while introducing randomness only known by the client.

The principle of such a solution would be to replace the current selection process based on a strong ordering of TXOs, by a random selection of a Coingroup, with an unequal probability of being selected depending on the factors currently used for the ordering.

For instance, the strong ordering of TXOs by anonset and amount in the current code base [7] may be replaced by:

THE COMPUTATION FOR EACH COINGROUP OF A METRIC

$$\boldsymbol{metric}(\boldsymbol{CG}_1) = \boldsymbol{f}(\boldsymbol{anonset}(\boldsymbol{CG}_1), \boldsymbol{amount}(\boldsymbol{CG}_1))$$

THE COMPUTATION FOR EACH COINGROUP OF A PROBABILITY OF BEING SELECTED:

$$\boldsymbol{P}(\boldsymbol{CG}_1) = \frac{\boldsymbol{metric}(\boldsymbol{CG}_1)}{\sum_{i=1}^{N} \boldsymbol{metric}(\boldsymbol{CG}_i)}$$

VII. Responsible Disclosure

These findings and potential mitigation were made available to the maintainers of the Wasabi Wallet software (ZkSnacks Ltd.) on 19 August 2020, less than 48 hours after the OXT Research analysts verified the deterministic nature of the Wasabi client and coordinator. OXT Research classify these vulnerabilities as **High/Critical** with a high probability that these vulnerabilities are already known and perhaps being exploited in the wild.

VIII. ADDENDUM

ZkSnacks Ltd. has denied the findings in this disclosure – despite the results being reproducible – and on 20 August 2020 Wasabi Wallet founder Adam Ficsor (nopara73) publicly disclosed these vulnerabilities in a comment thread on the Wasabi Wallet official Reddit community. Unfortunately, zkSnacks Ltd. are denying that there are any vulnerabilities that need to be addressed

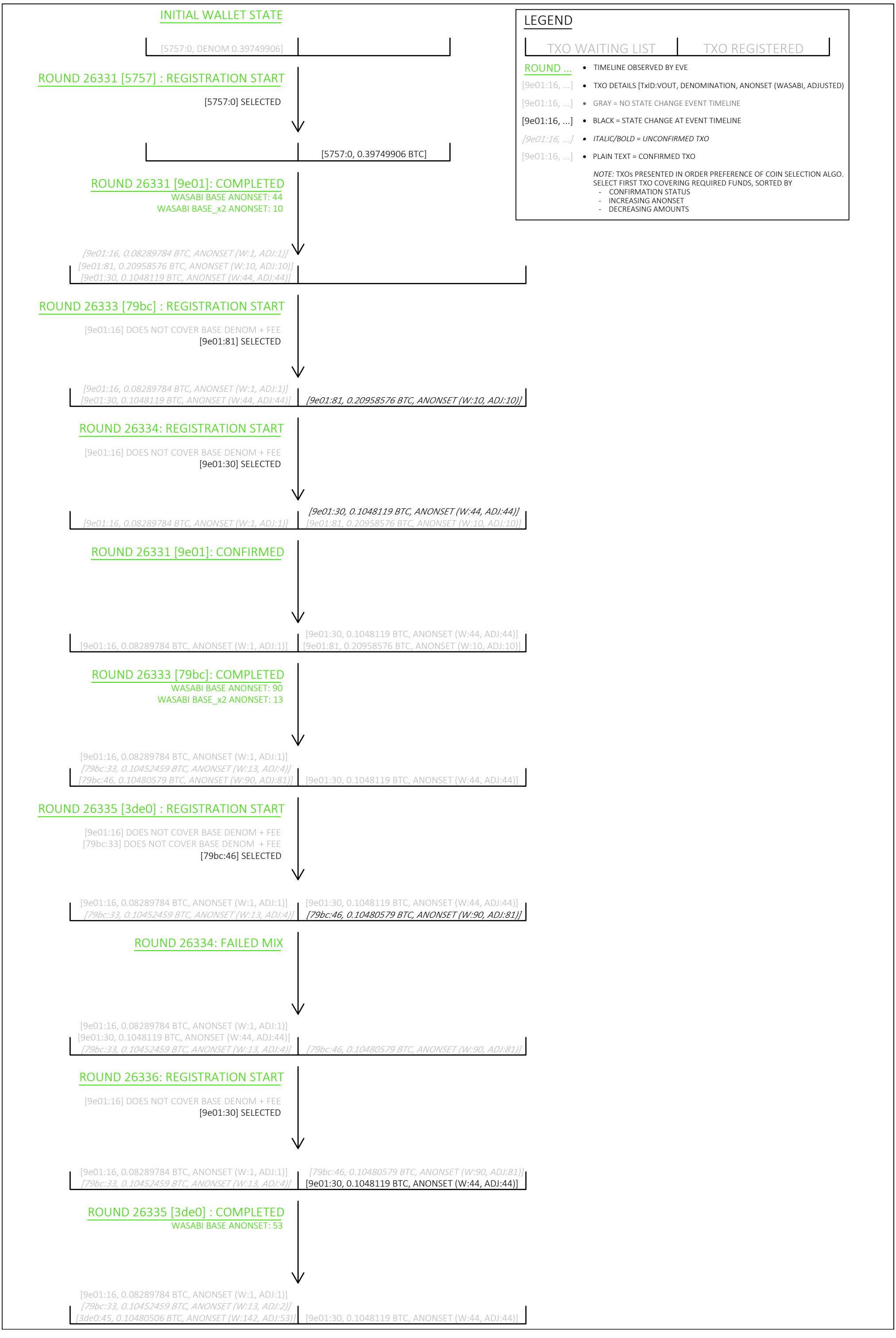
> "… wasabi is working as design and then there is no vulnerability, unknown bug nor anything …" [8]

- Lucas Ontivero, Wasabi Wallet Developer

> "… I think it's silly…" [9]

- Adam Ficsor (nopara73), Wasabi Wallet Founder

FIGURE 1 - DIAGRAM OF SIMULATED MEMORY OF DETERMINISTIC AUTOMATON



Tx generating the TXO	vout	Amount	Tx type	TXO type	Mix round	Mix round spending the TXO	Anonset (Wasabi)	Adjusted anonset	Bitcoin Address	PrivKey
5757e8a904927a75d161aa3b3283b1	0	0.39749906	PREMIX	DEPOSIT		26331	1	1	bc1q3rne8jfcpkzq6zx3s66s6hadt5krmqhyl4txmz	KxcWAjrHgGM8gSbFiw1F7wyUp1DZoCUbwncr4i7BPyPJpdEEZVZk
9e01681bc521d568aa877b1ce2bf6e9	30	0.1048119	MIX	DENOM_BASE	26331	26334-26336 (failed)	44	44	bc1qlwpkj7vkz4k7gt8guyc520cxrf2nvx5luek83h	L2sLZQcGTQxgBa88JdnpZkuR8X3RosdeTobY7nAa8jB8xZC5nD6E
9e01681bc521d568aa877b1ce2bf6e9	81	0.20958576	MIX	DENOM_x2	26331	26333	10	**4**	bc1q254ju8hnnuyq52u2e2tq57vu62pex5s27w9pwf	L46Z56Ksm54p9ZzACNyUaSFow2yUAAtKPvpwmZ9ATj3gfeF8W9eB
9e01681bc521d568aa877b1ce2bf6e9	16	0.08289784	MIX	CHANGE	26331		1	1	bc1q0c5wrt4gz966faqeyq69pn7mf68j63tg8vmnqc	Kz9ddDq8F4Wt9TK8FR3Uq6MWRfNFNiQDRUQLwdyrGwBhYYcktBhu
79bc55101e35a0a5f0bf8dd42ec40a9	46	0.10480579	MIX	DENOM_BASE	26333	26335	90	**81 / 2**	bc1q77z2xl9x933j3rshmpdtt03hrenmv93xenz36x	L3SsawLvpyHQ1jFMphXUKFLfA8i1GJGEoJtuyoopJFbEb2dkmw8Q
79bc55101e35a0a5f0bf8dd42ec40a9	33	0.10452459	MIX	CHANGE	26333		13	**4 / 2**	bc1qlshxut9uu69mqkntf5ektau7y9ghw7yq0fll7a	L3jQqQ1AJyY9G73s4nPDpQU8TvfTLbv1moe4jiF4ryPsdDJnnLq4
3de0e3d8ddf225fc8bed7ca68222be3	45	0.10480506	MIX	DENOM_BASE	26335		142	**53**	bc1qgltll4z4mfzsgwwlc2xgfdr5gxjmewerw0q8re	KwobvdTbcZRcLEfMdKyqDb7E4Cxh43bMGgumRUPrgGGbikbp6gmU

Reception of event by Eve (UTC)	Estimate of Date/Hour of event by Eve (UTC)	Event Type	Mix round	Block Height	Notes
08/16/2020 14:24:57	08/16/2020 13:41:11	MIX REGISTRATION OPENED	26331		Eve starts listening
08/16/2020 14:24:57	08/16/2020 13:43:50	MIX REGISTRATION OPENED	26332		
08/16/2020 14:44:27	08/16/2020 14:41:11	MIX REGISTRATION CLOSED	26331		Successful mix
08/16/2020 14:44:27	08/16/2020 14:44:06	MIX REGISTRATION OPENED	26333		
08/16/2020 14:46:45	08/16/2020 14:43:50	MIX REGISTRATION CLOSED	26332		Successful mix
08/16/2020 14:46:45	08/16/2020 14:46:20	MIX REGISTRATION OPENED	26334		
08/16/2020 15:01:00	08/16/2020 15:01:00	MIX CONFIRMATION	26331	644016	
08/16/2020 15:47:05	08/16/2020 15:44:06	MIX REGISTRATION CLOSED	26333		Successful mix
08/16/2020 15:47:05	08/16/2020 15:46:47	MIX REGISTRATION OPENED	26335		
08/16/2020 15:51:38	08/16/2020 15:46:20	MIX REGISTRATION CLOSED	26334		Failed mix
08/16/2020 15:51:38	08/16/2020 15:50:54	MIX REGISTRATION OPENED	26336		
08/16/2020 15:54:37	08/16/2020 < 15:54:08	MIX REGISTRATION CLOSED	26335		Successful mix
08/16/2020 15:54:37	08/16/2020 15:54:08	MIX REGISTRATION OPENED	26337		
08/16/2020 16:31:00	08/16/2020 16:31:00	MIX CONFIRMATION	26333	644027	
08/16/2020 16:56:28	08/16/2020 16:50:54	MIX REGISTRATION CLOSED	26336		Failed mix
08/16/2020 17:13:32	...	...	...	...	Eve stops listening

Step	TXO confirmed	Anonset Wasabi	TXO amount	TXO in waiting list	TXID	vout	Adjusted anonset	Notes
INITIAL WALLET STATE								
	T	**1**	**0.39749906**	**T**	**5757e8a904927a75d161aa3b3283b186564c3204dd8079c90b2035eea727da**	**0**	1	
REGISTRATION TO ROUND 26331								
	T	1	0.39749906	**F**	5757e8a904927a75d161aa3b3283b186564c3204dd8079c90b2035eea727dad	0	1	A single UTXO is available for selection
ROUND 26331 SUCCESSFULLY COMPLETED								
	F	**1**	**0.08289784**	**T**	**9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060**	**16**	1	
	F	**10**	**0.20958576**	**T**	**9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060**	**81**	10	
	F	**44**	**0.1048119**	**T**	**9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060**	**30**	44	
REGISTRATION TO ROUND 26333								
	F	1	0.08289784	T	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	16	1	Amount of [9e01:16] is too low for covering base denom.
	F	10	0.20958576	**F**	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	81	10	[9e01:81] is selected.
	F	44	0.1048119	T	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	30	44	
REGISTRATION TO ROUND 26334								
	F	1	0.08289784	T	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	16	1	Amount of [9e01:16] is too low for covering base denom.
	F	10	0.20958576	F	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	81	10	[9e01:81] isn't in the waiting list.
	F	44	0.1048119	**F**	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	30	44	[9e01:30] is selected.
CONFIRMATION OF ROUND 26331								
	T	1	0.08289784	T	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	16	1	
	T	10	0.20958576	F	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	81	10	
	T	44	0.1048119	F	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	30	44	
ROUND 26333 SUCCESSFULLY COMPLETED								
	T	1	0.08289784	T	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	16	1	
	T	44	0.1048119	F	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	30	44	
	F	**13**	**0.10452459**	**T**	**79bc55101e35a0a5f0bf8dd42ec40a92099e86f2f44fb6b5815c98d030523799**	**33**	**4**	
	F	**90**	**0.10480579**	**T**	**79bc55101e35a0a5f0bf8dd42ec40a92099e86f2f44fb6b5815c98d030523799**	**46**	**81**	
REGISTRATION TO ROUND 26335								
	T	1	0.08289784	T	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	16	1	Amount of [9e01:16] is too low for covering base denom.
	T	44	0.1048119	F	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	30	44	[9e01:30] isn't in the waiting list.
	F	13	0.10452459	T	79bc55101e35a0a5f0bf8dd42ec40a92099e86f2f44fb6b5815c98d030523799	33	**4**	Amount of [79bc:33] is too low for covering base denom.
	F	90	0.10480579	**F**	79bc55101e35a0a5f0bf8dd42ec40a92099e86f2f44fb6b5815c98d030523799	46	**81**	[79bc:46] is selected.
REGISTRATION TO ROUND 26334 FAILS								
	T	1	0.08289784	T	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	16	1	
	T	44	0.1048119	**T**	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	30	44	
	F	13	0.10452459	T	79bc55101e35a0a5f0bf8dd42ec40a92099e86f2f44fb6b5815c98d030523799	33	**4**	
	F	90	0.10480579	F	79bc55101e35a0a5f0bf8dd42ec40a92099e86f2f44fb6b5815c98d030523799	46	**81**	
REGISTRATION TO ROUND 26336								
	T	1	0.08289784	T	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	16	1	Amount of [9e01:16] is too low for covering base denom.
	T	44	0.1048119	**F**	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	30	44	[9e01:44] is selected.
	F	13	0.10452459	T	79bc55101e35a0a5f0bf8dd42ec40a92099e86f2f44fb6b5815c98d030523799	33	**4**	
	F	90	0.10480579	F	79bc55101e35a0a5f0bf8dd42ec40a92099e86f2f44fb6b5815c98d030523799	46	**81**	
ROUND 26335 SUCCESSFULLY COMPLETED								
	T	1	0.08289784	T	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	16	1	
	T	44	0.1048119	F	9e01681bc521d568aa877b1ce2bf6e9f008cf3001e47d09cc35782bfa35b9060	30	44	
	F	13	0.10452459	T	79bc55101e35a0a5f0bf8dd42ec40a92099e86f2f44fb6b5815c98d030523799	33	**2**	
	F	**142**	**0.10480506**	**T**	**3de0e3d8ddf225fc8bed7ca68222be35dd1e74313cc5470cbd9a543c1574e2c45**		**53**	

...