Post-Mortem: What Happened Between Samourai Wallet and Me

AUTHOR
Ádám Ficsór

PUBLISHED
2026-07-11

EDITION
Version 1.0.0

SOURCE REVISION
`75e545620927f75ba487997bb1cf03360738ffe9`

ABSTRACT

A first-person post-mortem and primary-source archive documenting the conflict between Ádám Ficsór and Samourai Wallet. The record covers ZeroLink authorship, wallet-backend xpub collection, Tor and Dojo defaults, public technical claims, retaliation, and evidence made public after the server seizure. It distinguishes primary records, recollection, inference, government allegations, and defense claims so that readers can independently evaluate the account.

Source SHA-256 `7f9fca7748f9e87b58e43ac70a3c1b3dc25899c4b00539daacd5cfec60ee2518`

How a wallet that adopted my privacy framework turned technical disagreement into a reputational war—and what I got wrong too

After law enforcement seized Samourai Wallet's servers, William Hill—TDevD—messaged an associate: "Not good." Then he named the thing that worried him: "I'm not thinking so much about Whirlpool as I am about the wallet backends (xpubs)."[33]

An extended public key cannot spend a user's bitcoin, but it can reveal the addresses derived from a wallet and follow their history. For years, I had argued that Samourai's default backend created exactly this point of failure. Hill's message showed that he understood why the seizure of that backend mattered.

at 6; Hill Subm. at 17, 19). But Rodriguez and Hill's public and private statements and their Samourai marketing materials unmistakably reveal that, even if general user privacy generally was *one of* the overarching features of the platform, soliciting criminals to use Samourai was likewise a feature, and one that the defendants expressly touted.[18]

With respect to Hill, his instant attempts to disavow or downplay his public statements is no more than a transparent bid for leniency at sentencing. Hill—in an about-face from his yearslong public persona—brushes off his prior public and private statements, claiming they were simply "guerilla" marketing and "must be understood in the context of his autism."[19] (Hill Subm. at 36; Hill Letter at 106). Hill's disavowals ring hollow. As explained above, his contemporaneous statements are not ambiguous and self-evidently promoted Samourai as a tool for criminals. Hill's statements were made over a period of years, in multiple public and private forums, and were consistent in tone and content—they demonstrate that Hill meant what he said, and these statements were not merely marketing hyperbole. Indeed the argument that this could have been the purpose of Hill's *private* communications with colleagues and associates strains credulity.

XPUB information with past, present and future Whirlpool transactions to associate input and output addresses belonging to its mobile-only users. After law enforcement seized Samourai's servers, Hill messaged an associate, "Not good," and noted "I'm not thinking so much about Whirlpool as I am about the wallet backends (xpubs)." (PSR ¶¶ 19-20).

[18] Rodriguez and Hill do not dispute the substance of their statements or marketing materials. They only dispute the inferences that can be drawn from them regarding Rodriguez's and Hill's intent to solicit criminals as Samourai users.

[19] Hill also claims that his autism "reduces his moral culpability." (Hill Subm. at 28). The Government acknowledges that the Court should consider Hill's autism as relevant to the "history and characteristics of the defendant," but the defendant has not shown or even attempted to show that his autism precluded him from understanding right from wrong, and the Court should reject any suggestion that the defendant's autism "reduces his moral culpability."

The government's sentencing memorandum records Hill's post-seizure message: "Not good," followed by his concern about "the wallet backends (xpubs)." Open the archived filing.

The seizure did not create the xpub problem. It exposed the consequences of a design choice that had been there from the start.

I do not offer this post-mortem as vindication. A prison sentence cannot settle a protocol dispute, and an indictment cannot make every allegation true. I will distinguish what the

public record establishes, what I infer from it, and what I remember but cannot independently prove.

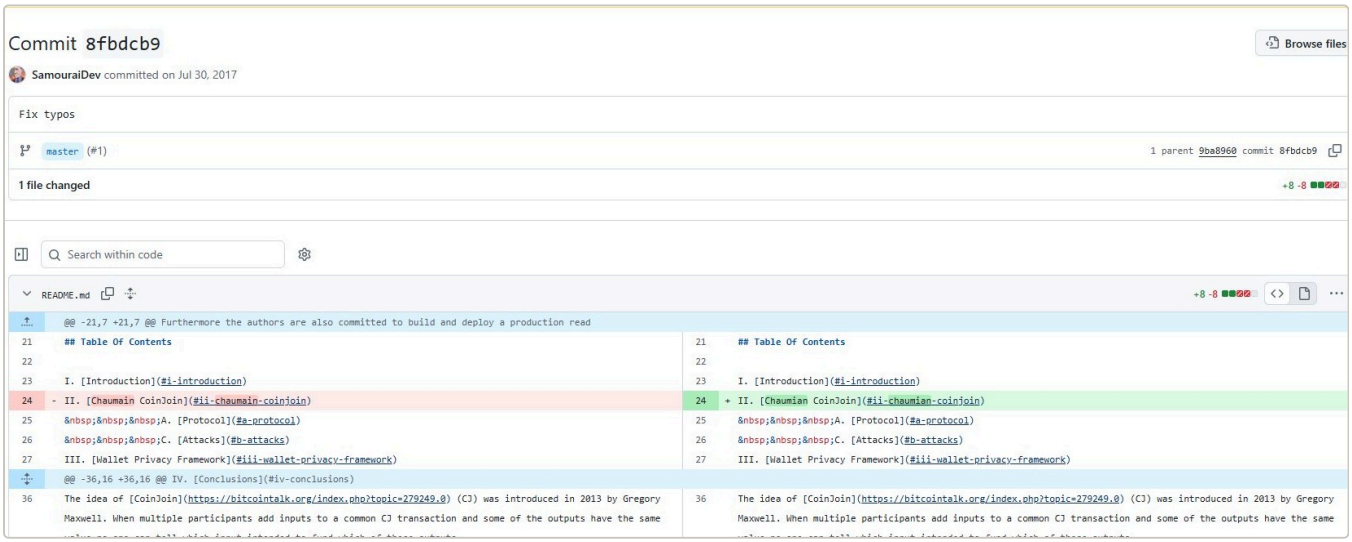
To understand what was sitting on that server—and why I had spent years shouting about it—we have to go back to a README file in July 2017, before the feud began.

How ZeroLink actually began

I wanted Samourai to succeed in implementing ZeroLink. I wanted more wallets to implement serious Bitcoin privacy, and I wanted ZeroLink to become useful software rather than another specification admired by a small circle and ignored by everyone else.

I created ZeroLink. The repository makes the chronology clear. I opened it on July 28, 2017. Before Samourai made a single commit, I had made 19 and written a 184-line, 2,883-word document containing the framework's core architecture. Samourai's first commit arrived two days later. Its title was "Fix typos". It did exactly that.

ZeroLink was not merely a name for a CoinJoin transaction. It was a privacy framework for Bitcoin wallets: blinded coordination together with rules for network privacy, coin selection, transaction chains, and spending after the mix. I described that scope plainly in a 2021 Wasabi Research Club discussion: Chaumian CoinJoin was the protocol; ZeroLink was the broader wallet framework. That is the work Samourai later claimed to have co-created.[1]



SamouraiDev's first ZeroLink commit, July 30, 2017: "Fix typos." Open the commit.

At the August 14 publication snapshot, Git blame attributes 6,126 of the document's 6,627 words to me and 242 to Bill/TDevD. Their only sizeable technical addition concerned BIP47 and stealth addresses. I did not understand what problem it solved or why it belonged in ZeroLink. Instead of challenging it, I assumed that I was missing something and accepted it out of politeness. Two days later I clarified that BIP47 was not part of the protocol, and I removed

the section in 2019. The rest of their work was overwhelmingly light editing. The complete commit and line-churn audit is preserved in the source note.[1]

I had also put TDevD in the Authors section before the BIP47 proposal was committed. Both decisions came from the same reflex: they spoke with confidence, I assumed that any confusion was mine, and I tried to be generous. Their confidence made me doubt my own judgment, while my politeness was later used to support a claim of authorship that the repository does not support.

By 2022—three years after I had publicly challenged the joint-creation claim, with the Git history still open for anyone to inspect—Samourai was still repeating it.[2][5]

I regard those later repetitions as a lie. “Collaboration” can be innocent shorthand while nobody has disputed it. It stops being innocent after the primary record is placed in front of you and you keep telling the version that promotes you from reviewer and prospective implementer to co-creator. The false version gave Samourai ownership of the intellectual foundation it had adopted and made my later objections sound like jealousy over something we had supposedly invented together.

Our contact was limited. We barely spoke, and I was never part of Samourai. I had created ZeroLink; Samourai said it intended to implement it. Brian “Shinobi” Trollz, who observed the dispute at the time, later recalled a specific turning point. I asked for a week to consider whether coordinators could be run altruistically. During that week, he said, Samourai’s posture toward me shifted into mockery. By April 2019, I had recorded that they were no longer interested or responsive and that I had continued independently. People can disagree about why that limited contact ended. The authorship record is not a matter of recollection.

The authorship dispute mattered to me, but the architectural difference between the wallets affected users directly.

The central privacy difference

The two wallets exposed users to very different risks from their service operators.

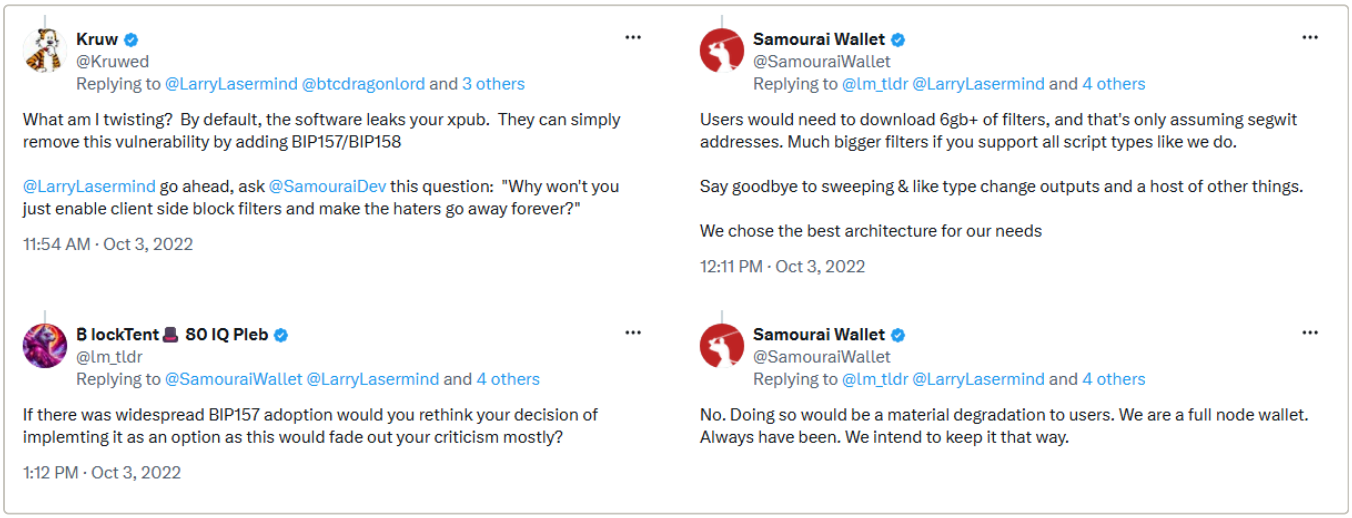
Wasabi’s default architecture was built to deny its own operator the wallet graph. The backend distributed block filters; clients checked addresses locally; wallet traffic went through Tor; and blinded CoinJoin credentials prevented the coordinator from linking a registered input to its output. A user did not need to operate a personal server to hide addresses and transaction history from us. Privacy from the service operator was the default.[2]

Samourai’s default client sent extended public keys to Samourai’s hosted backend. Whoever holds an xpub can derive its associated addresses and follow their transactions. Samourai’s own Dojo documentation disclosed the consequence indirectly. Running MyDojo improved

privacy by “completely bypassing” the default hosted servers, while its Tracker recorded registered xpubs and addresses.[2]

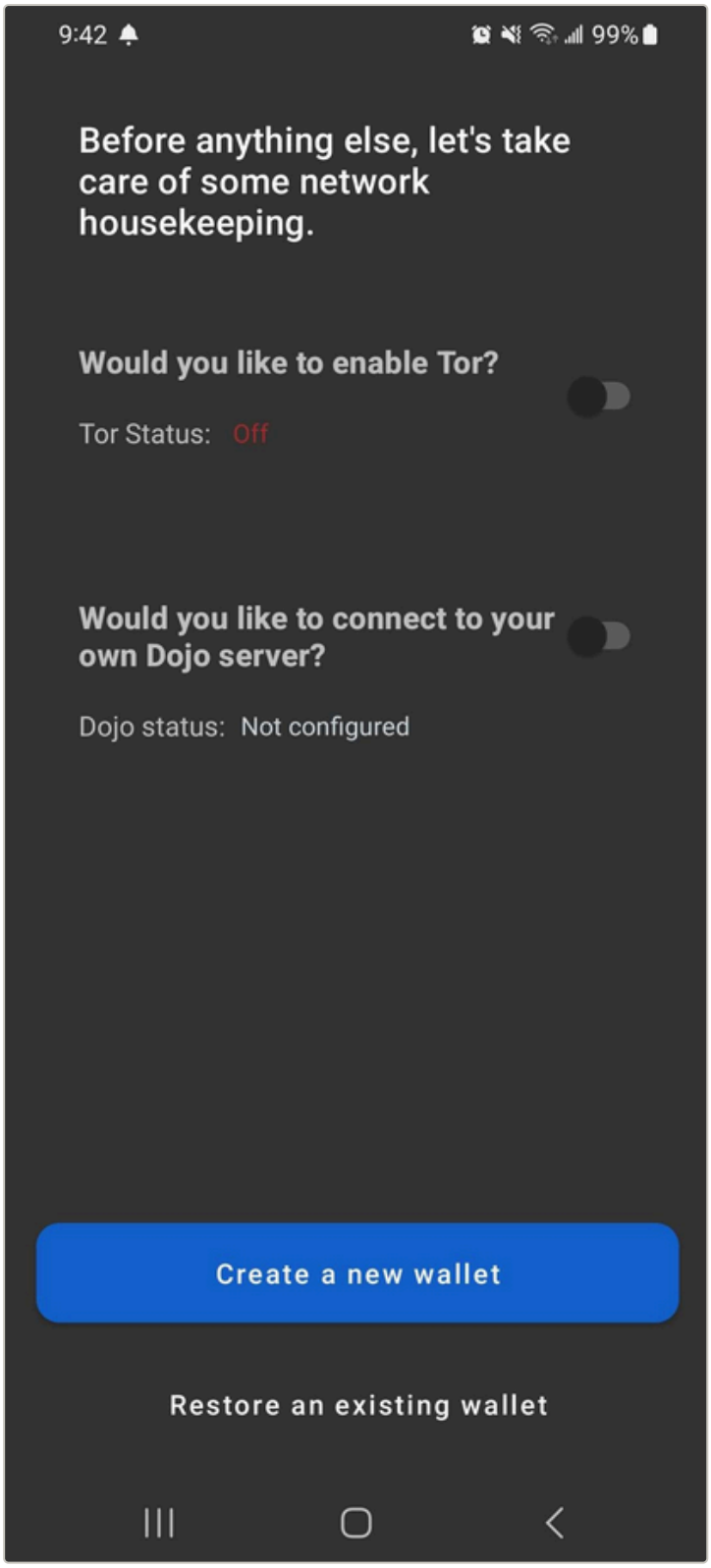
Then came the clearest lie in the xpub argument. In October 2022, Kruw said that the default app exposed the user’s xpub and asked why Samourai would not use BIP157/BIP158 client-side filters. The official wallet account refused, said it had chosen “the best architecture for our needs,” and soon afterward claimed it had been “open and truthful from day one.” When asked whether wider BIP157 adoption would change its decision, it answered: “We are a full node wallet. Always have been.”[3]

That was false. The Android app was a light client of a backing server. Dojo could put that server and the Bitcoin Core node behind it under the user’s control, but it did not turn the phone into a full node. Samourai’s own 2019 announcement said default users had to trust its servers with their public keys. Hill’s sentencing submission later described the affected architecture as one used by “light wallets.”[3]



Four posts from the October 3 exchange, in chronological order: the default xpub disclosure is raised; Samourai defends its chosen architecture; a user asks whether wider BIP157 adoption would change the decision; and Samourai falsely calls the Android app a full-node wallet. Open the final reply.

Tor support existed, but it was not enabled by default. Samourai’s signed source allowed a user to create a wallet while Tor remained off, treated the Tor preference as `false` unless the user enabled it, and used the ordinary network path for xpub requests when Tor was disabled. A screenshot preserved in an April 2023 issue on Samourai’s own GitLab showed the wallet-creation screen with both Tor off and Dojo unconfigured. The user could continue by pressing “Create a new wallet.” That default exposed the user’s IP address to Samourai’s hosted service while the same service received the wallet’s xpubs.[15]



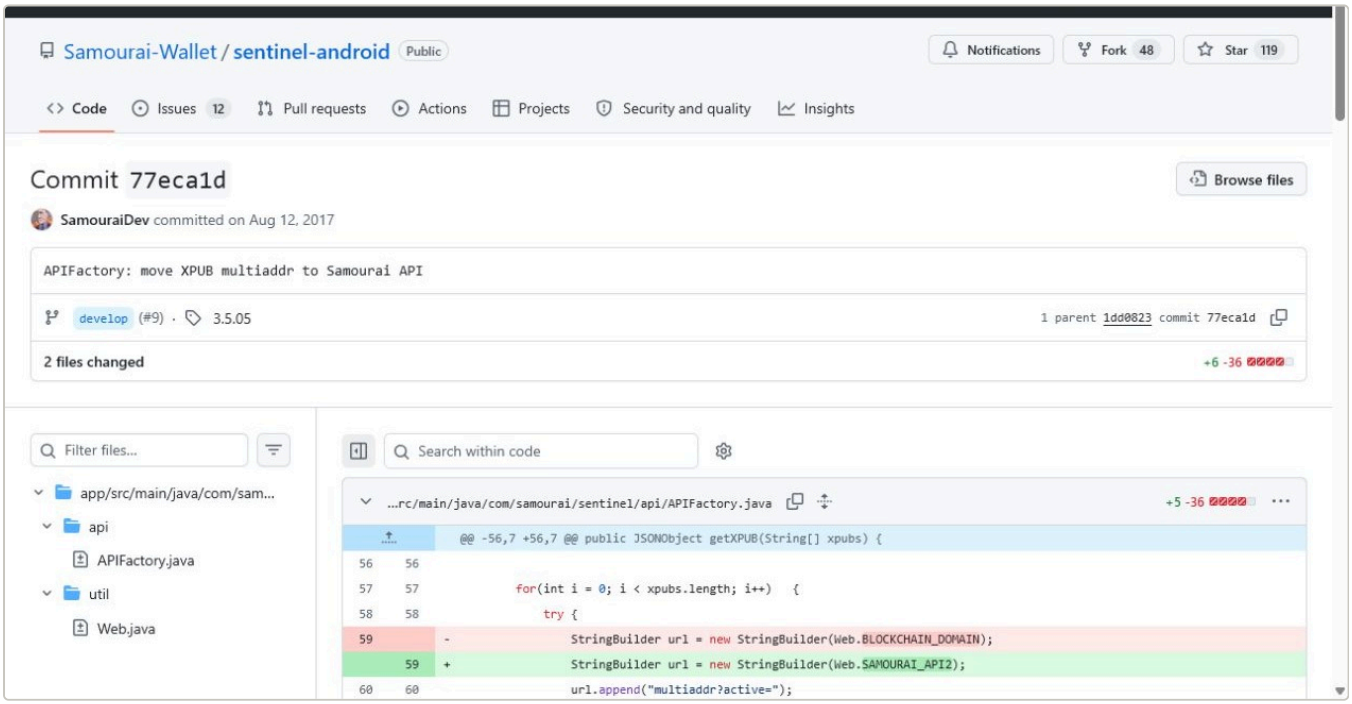
The wallet-creation screen attached to Samourai's own issue tracker: Tor off, Dojo not configured, and "Create a new wallet" still available. Open the archived issue.

The issue was titled "Important privacy features are disabled by default." It proposed enabling Tor and Dojo by default or, at minimum, warning users what the off settings exposed. A Samourai project owner replied that the proposal would not be merged, called the report "concern trolling," issued a "first and final warning," and immediately closed the issue.[15] The

privacy problem was reported on their own development platform. Their answer was to reject the change and threaten the person who reported it.

The October claim followed an earlier evasion. In July 2022, a user wrote: “Xpub is sent to whirlpool servers.” Hill answered by changing the noun: “No xpubs are handled by the coordinator.” The xpubs went to Samourai’s wallet backend, not the Whirlpool coordinator. He also claimed that Samourai had implemented ZeroLink “on spec,” something I supposedly “didn’t have the skill set to do.” The reply avoided the backend issue and falsely reversed the authorship record.[14]

Sentinel, Samourai’s watch-only app, made the same architecture even easier to see. A watch-only wallet legitimately needs an xpub, and Sentinel correctly said that it could not spend the user’s coins. But the privacy question was what happened to the xpub after the user imported it. In August 2017, Samourai committed a change titled “move XPUB multiaddr to Samourai API.” From then on, Sentinel sent each tracked xpub to Samourai’s hosted backend. It did so for more than two years before Tor routing was added; when Tor arrived, its preference defaulted to off. The last pre-seizure source still let a user choose Samourai’s server, answer “No” to “Connect through Tor?”, and then posted imported xpubs to that server.[16] Sentinel could not spend users’ coins, but its hosted mode let Samourai map their wallets. That collection was integral to the product rather than incidental telemetry.



The Sentinel commit that moved `XPUB multiaddr` *queries to Samourai’s API. Open the commit.*

William led the Blockchain.info Android wallet project that preceded Samourai. He opened the surviving `Android-Wallet-2-App` history with its April 2014 initial commit and is its dominant visible developer by commit count. His own sentencing submission calls him Blockchain.com’s senior mobile developer; contemporary coverage identifies Keonne as the product lead responsible for the refreshed wallet’s interface and user experience. William’s commits even

include “UI prep for shared coin,” Blockchain.info’s earlier mixing product. They did not create Blockchain.info itself, but they led the mobile-wallet project from which Samourai emerged.[5]

Samourai then kept its own source private for about a year. At the time, it said the delay was deliberate and intended to give the product a competitive “leg-up.” When the first public Samourai snapshot finally appeared in March 2016, it contained unmistakable Blockchain.info lineage: among other examples, its `BitcoinScript`, `BitcoinAddress`, `Hash`, and swipe-listener files descend closely from the earlier wallet. The lineage does not make the entire codebase a copy, but it contradicts the image of a clean-sheet privacy wallet appearing from nowhere.[5]

SharedCoin matters because the old trust model was already understood. It was non-custodial, but its server constructed the joins and knew their links. In two Research Club discussions, participants treated that server knowledge as obvious: public transaction ambiguity could not provide privacy from the operator that already knew the mapping. When a 2021 paper named that weakness in SharedCoin but omitted Samourai’s default xpub collection, I objected. The products used different mechanisms, but the operator occupied the same privileged position. Samourai had rebuilt the problem it claimed to have left behind.[6]

Dojo did not change what the default client disclosed. Most users of a mobile wallet will use the default, and even people who ran Dojo entered Whirlpool rounds alongside default-server users. If the common operator could identify or eliminate the outputs belonging to wallets it already knew, the effective anonymity set shrank for everyone; in some rounds, the remaining participants could be exposed by exclusion.[19]

None of this is hindsight invented after the servers were seized. In an April 2020 Wasabi Research Club presentation about ZeroLink, I described the rejected design plainly: a trusted central server to which everyone sends their xpubs. That, I said, “obviously sounds pretty stupid,” which is why ZeroLink used blinded coordination instead. In July 2021, while reviewing a paper that contrasted Blockchain.info’s SharedCoin with Samourai, I objected that the comparison omitted the decisive fact: Samourai also learned wallet relationships because its default server collected xpubs. If the server has the xpub, repeated mixing cannot erase what the server already knows; and Dojo users still share rounds with users known to that server. In September 2022, discussing balance-query architectures, I warned that any other computer retaining an xpub could later be hacked or seized. The government seized Samourai’s servers in April 2024.[6]

The practical distinction was whether the operator was prevented from learning wallet relationships or merely trusted not to use them.

Wasabi was not perfect against every imaginable adversary. No honest system built on Bitcoin, Tor, fallible software, and human behavior can promise perfection. But against the service operator—the adversary at the center of this dispute—Wasabi placed cryptography and local processing between the user and us. Samourai relied on trust in its operator.

Samourai preached resistance to third-party surveillance while ordinary users entrusted it with a durable view of their wallets. When developers pointed out the contradiction, the honest response would have been simple: our default server receives your xpub; if that threat matters to you, run Dojo. Instead, Samourai attacked the people who explained the trust assumption.

Sockpuppets and attacks on critics

My first *SamouraiLeaks* investigation began with a suspicion: one of Samourai's developers appeared to be promoting the project and attacking its critics through an identity presented as independent.

In April 2019, I published the evidence that "foneBTC" and "fone-btc" were TDevD/William Hill's sockpuppet accounts. The investigation is the proof. Its concluding exhibits are preserved below so the record does not depend on Medium remaining online.

▶ **View the sockpuppet investigation's concluding exhibits**

But the moral question does not turn on whether Bitcoin developers use pseudonyms. Pseudonyms are normal here. The problem is hidden affiliation used to manufacture consensus: one participant appearing to be several, promotion made to look organic, and an interested party presenting himself as a neutral observer. In a field where few users can audit every cryptographic claim themselves, reputation becomes part of the security model. Astroturfing corrupts that model.

Before publishing, I tried private conversation, sought a mediator, and offered to stop discussing Samourai if the attacks stopped. I eventually concluded that my silence was being treated as permission rather than de-escalation.

Other developers then began describing the same experience.

Gregory Maxwell said architectural criticism was answered with harassment and accusations rather than a technical response. Nicolas Dorier reported the same reaction after pointing out that the default backend received users' extended public keys. Their comments remain in the original discussion, including Dorier's account. Luke Dashjr said that disclosing an RPC-password exposure in a setup guide brought an accusation that he ran a criminal protection racket; his own qualification—that local networking or a VPN could limit the exposure—remains in the thread. I gathered those and similar accounts in *SamouraiLeaks Part 2*.

▶ **View Gregory Maxwell's contemporaneous account**

They were independent developers, not a Wasabi group, and several had also criticized Wasabi. Their accounts described the same response: technical objections were redirected toward the critic's motives, status, or character.

Chris Belcher later described substantive BIP47 objections being answered by smears against the people raising them. ZmnSCPxj said Samourai had misrepresented his technical comments and again emphasized the privacy cost of the default server.[20] A JoinMarket contributor acknowledged that individual criticisms on both sides could be valid while identifying Samourai's counterattacks as the reason productive discussion became so difficult.[21]

Accuse loudly, qualify quietly

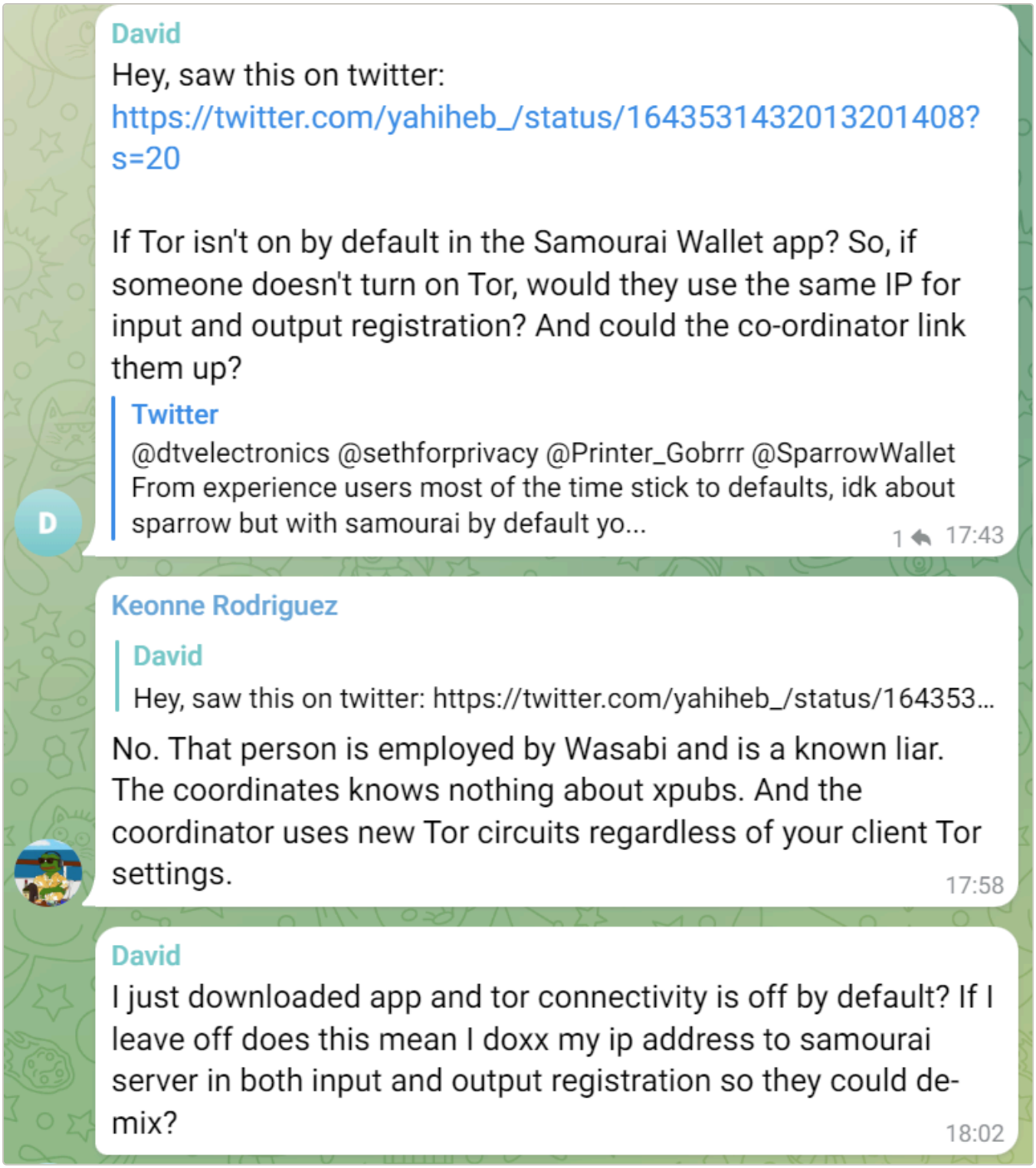
After enough repetitions, the sequence became predictable: start with something real—an uncertainty, a compromise, or a bug—then attach the most damaging interpretation available and promote it until it becomes the headline. When contrary evidence arrives, place the qualification where fewer people will see it: inside a reply, outside a screenshot, or silently inside a later code change.

The claim that I had admitted Wasabi supplied its own liquidity followed this pattern. I had made no such admission. The journalist responsible for the report corrected the characterization, but the correction never travelled as far as the accusation. Another observer documented how Samourai's presentation excluded my correction and contrary replies.

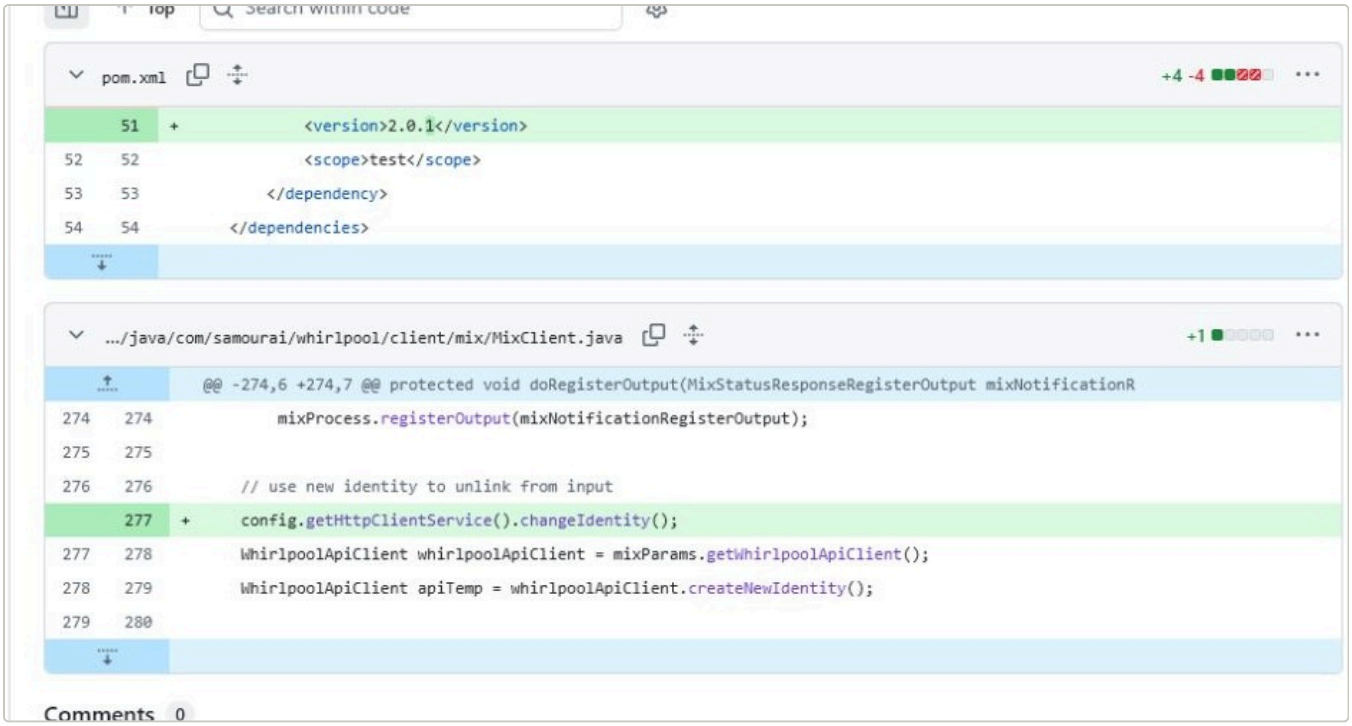
A cropped account can be misleading even when every visible fragment is genuine, because the omitted context changes its meaning.

The same technique appeared elsewhere. In 2023, Samourai circulated criticism from Matt Corallo while omitting his concluding post. BlockDigest documented a smaller but revealing PayNym episode: a question about short-name mappings drew insults and brigading, and the issue was later patched without the public acknowledgment that would have turned a quarrel into routine engineering.[22]

The Tor identity dispute provides another example. In April 2023, a user asked whether Whirlpool changed Tor circuits between input registration and output registration. Keonne Rodriguez answered categorically that it did and dismissed the questioner as a known liar.[23] In March 2024, the Whirlpool client added an explicit `changeIdentity()` call before output registration. The code comment explained that the new identity was used to unlink the output from the input.



April 2023: Rodriguez answered that the coordinator used new Tor circuits regardless of the client's Tor settings and called the questioner a liar.



March 2024: the client added `changeIdentity()` *immediately before output registration, with the comment "use new identity to unlink from input." Open the commit.*

▶ **View the commit header**

The later commit cannot establish whether earlier Whirlpool rounds were deanonymized or whether anyone exploited the behavior. It does establish that the categorical denial was unsafe. A precise answer in 2023 would have explained what the client did, what had been verified, and what remained uncertain. Rodriguez instead answered with certainty and an insult; the code changed later.

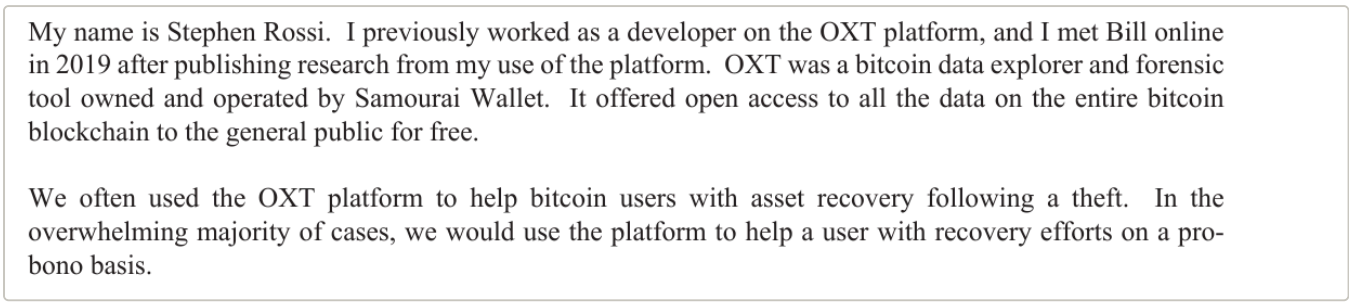
This response culture encouraged users to treat disclosures as tribal attacks and raised the social cost of reporting problems. Even small bugs became hard to discuss because the reporter risked becoming the subject.[22]

Accusations presented as security research could damage Wasabi without demonstrating a break.

The OXT "critical vulnerability" that failed its own test

OXT was not an independent research group that happened to agree with Samourai. In December 2017, Samourai announced that it had "finalized the acquisition" of OXT in an all-bitcoin transaction and called it a long-term strategic investment. OXT would remain a separate entity, the announcement said, but one "complementary" to Samourai. Years later, an OXT developer's support letter included in William's own sentencing submission described OXT as a Bitcoin forensic tool "owned and operated by Samourai Wallet." The government

separately noted that William and Keonne operated OXT as a tracing and wallet-attribution tool.[8]



My name is Stephen Rossi. I previously worked as a developer on the OXT platform, and I met Bill online in 2019 after publishing research from my use of the platform. OXT was a bitcoin data explorer and forensic tool owned and operated by Samourai Wallet. It offered open access to all the data on the entire bitcoin blockchain to the general public for free.

We often used the OXT platform to help bitcoin users with asset recovery following a theft. In the overwhelming majority of cases, we would use the platform to help a user with recovery efforts on a pro-bono basis.

An OXT developer's letter in William's sentencing submission describes OXT as a forensic tool "owned and operated by Samourai Wallet." Open the archived filing.

We did not reject OXT's work because it came from a rival. In March 2020, five months before OXT's ultimatum, the Wasabi Research Club devoted an entire session to LaurentMT's Boltzmann—the transaction-analysis tool Samourai's own acquisition announcement had praised. We examined how it counted possible transaction partitions and where that number stopped being a measure of an individual user's privacy. A high transaction-wide entropy score does not include everything a targeted observer may know from the network or the wider transaction graph, and computing all partitions becomes impractical for large Wasabi transactions. We engaged with the work in public before OXT attacked us. We rejected the later "critical vulnerability" because its premises failed.[11]

In August 2020, this Samourai-owned research arm announced two supposed Wasabi vulnerabilities, rated them High/Critical, claimed they could cancel the privacy gained from earlier mixes, and gave us forty-eight hours to publish a warning on their terms. The full report contained a fatal premise: the attacker had to know the composition of the target's wallet at a chosen point in time and know events affecting the wallet's participation in later rounds. That was not a minor condition. It supplied the wallet membership that the alleged attack was supposed to uncover.[2][4][8]

OXT avoided that problem in its demonstration by controlling both sides. Its target, "Alice," received one known 0.4 BTC coin. Its observer, "Eve," already knew which funds belonged to Alice and ran a modified Wasabi client that logged round events. Given the wallet's exact starting state, the public coin-selection code could sometimes predict which of Alice's coins the client would offer next. That showed that known software can behave predictably when the observer is handed its private starting state. It did not show how an outside observer could discover an unknown wallet's contents, identify an unknown mixed output as the target's, or recover an input-to-output link hidden by the protocol.[2][4]

Even in that constructed test, the predictions did not simply work. The report recorded expected coins failing to enter rounds because of confirmation state, failed rounds, and coordinator behavior. OXT called these deviations "exogenous randomness." Its second "vulnerability" was a proposed use of change-output "beacons and checkpoints" to notice

when the first prediction had failed and investigate why. The report's reduced "adjusted anonsets" were values produced by OXT's own model. They were not identities uncovered, owners identified, or blinded input-output links recovered.[24]

OXT's follow-up speculated that a powerful adversary might possess exchange data, pooled surveillance information, or coordinator logs, but it never demonstrated how the attack would acquire the wallet state it required. My contemporaneous line-by-line response made the distinction: the report assumed near-complete knowledge of the target wallet; its conclusion that prior mixes were "cancelled" did not follow from that assumption; and OXT's own spreadsheet had failed to predict the exact coins selected in its own wallet.[24]

Adding randomness can be reasonable hardening without validating a claimed exploit. Samourai later treated Wasabi 2's different selection behavior as an admission that OXT had been right.[25] The timeline disproves that story. We established the Wasabi 2 research effort in January 2020 and publicly presented WabiSabi in June, before OXT's August disclosure. Wasabi 2 was an already-planned replacement of the CoinJoin protocol and user experience, not a patch accepting OXT's conclusions.[24]

OXT's hypothetical Wasabi attacker needed to begin with a target's wallet map, while Samourai's real default backend collected wallet maps. OXT's own follow-up declared that privacy guarantees must come from "default software behavior," not from placing the burden on the user. Samourai's default failed that standard; its users had to run Dojo to escape the hosted server that OXT's owner operated.[8]

The trap of criminal association

The OXT report was part of a broader tactic. Samourai and OXT repeatedly attached Wasabi's name to alleged criminal activity, then treated the association itself as evidence against us. The trap worked either way. If we answered, we helped spread the association. If we stayed silent, they presented the silence as a concession.

In several instances we never had a safe opportunity to answer. A meaningful response would have required disclosing operational knowledge, investigative methods, or decisions that could not be made public without compromising opsec. Some claims therefore circulated largely unchallenged. The absence of a public response reflected that constraint, not agreement.

Samourai made that double standard explicit after Luke Dashjr's theft. On January 4, 2023, OXTObserver flagged 204.77460928 BTC under `#LUKE-JR_STOLEN_FUNDS` and described the wallet as controlled by hackers. Samourai Wallet quoted the alert as "Luke-jr stolen coins on the move." When a user asked what Samourai would do if the thieves tried to mix the coins in Whirlpool, the official account answered: "If they go into Whirlpool? Relish in the delicious irony and extra salt in Luke's gaping wound." The exchange does not show that the coins

entered Whirlpool. It shows the official account expressing pleasure at the possibility because the victim was Luke.[9]

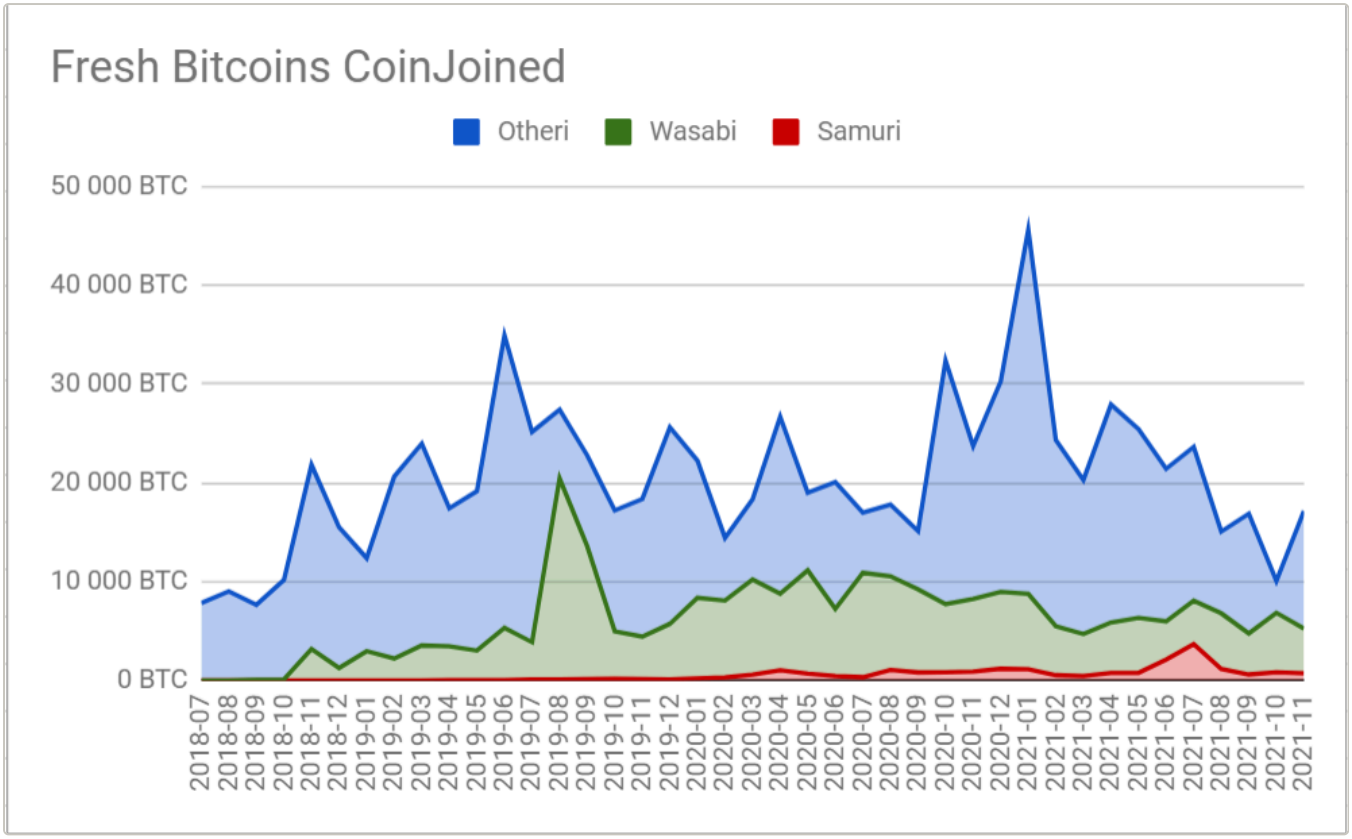
I cannot draw a straight causal line from one Samourai post to one institutional decision. I can say what followed: exchanges scrutinized Wasabi CoinJoin deposits, journalists carried the criminal-association narrative outward, and legal and regulatory pressure on the company increased. By 2022, the survival of the company-run coordination service was in question.

The default zkSNACKs coordinator then began rejecting some UTXOs. I had argued against blacklisting, and people who felt betrayed had a legitimate grievance. The policy was censorship by one service, but it did not reveal the relationship between accepted inputs and their outputs. The protocol still blinded that relationship; Wasabi remained MIT-licensed; and other coordinators could run without zkSNACKs' policy.[26]

Samourai converted that policy dispute into the claim that Wasabi had become a surveillance wallet. The comparison ignored the relevant architectures: zkSNACKs refused some inputs without learning their outputs, while Samourai's default backend received and retained ordinary users' wallet maps.

The megaphone was bigger than the product

Samourai's Twitter presence made the rivalry look symmetrical despite the large difference in usage. Dumplings—my reproducible CoinJoin scanner—separated fresh bitcoin entering a mixer from coins merely being remixed and called fresh bitcoin the best on-chain proxy for adoption. From Whirlpool's first detected month in April 2019 through the dataset's end in August 2022, it identified 247,675 fresh BTC entering Wasabi and 30,228 entering Whirlpool. Wasabi led in every one of those forty-one months. This is a measure of bitcoin, not a user headcount, but it is the opposite of adoption parity.[7]



Dumplings' original "Fresh Bitcoins CoinJoined" chart. Wasabi is green; Whirlpool—labelled "Samuri" in the scanner—is red. The chart shown runs through November 2021; the archived data continues through August 2022. Open the reproducible scanner.

Whirlpool's headline transaction totals were enlarged by free remixes: the same bitcoin could appear in round after round without representing a new user or newly arriving funds. Samourai's much larger Twitter presence made the products look more evenly adopted than the Dumplings data supported.

OXT's report gave a marketing attack the appearance of a vulnerability disclosure through a technical PDF, severe labels, a deadline, and claims of immediate danger. Its demonstration showed predictable code only after the observer was given the information the protocol was designed to hide.

Moving the problem did not solve it

Whirlpool's strongest design slogan was that its CoinJoin transactions contained no toxic change. `TX0` kept the change out of the CoinJoin transaction and placed it in a separate account so users would be less likely to spend it with mixed coins, but the toxic change still existed. Samourai itself later called these coins "unmixed toxic change" while proposing a way to swap them into Monero.[12]

The same `TX0` publicly joined the deposit inputs, created the fixed-denomination premix outputs, and exposed which first Whirlpool rounds spent them. In a 2023 Research Club panel, a participant compared this directly with Wasabi 1 and made the narrow point that peeling

change off before the CoinJoin did not create an additional break between that change and the first mix. It moved the point at which the change appeared.[12]

Fixed denominations created another cost at both ends. A user could have to combine inputs publicly in `TX0` to enter a pool. Later, an ordinary payment would rarely equal one pool denomination, so the user could have to combine multiple post-mix outputs and create new change. The official Whirlpool server configuration enforced those denominations. Equal-output CoinJoins still provided privacy, but the clean CoinJoin transaction was only one part of the user journey, and remix counts could not show whether that privacy survived the eventual spend.[12]

Ricochet had the same gap between a useful trick and a sweeping privacy impression. Its source built a default four-hop chain in which each transaction spent the previous one and reduced the forwarded amount by a calculated per-hop fee. That could frustrate a crude system that looked back only a fixed number of transactions. It also produced a recognizable shape. The Research Club flagged the unique fingerprint in 2020 but deferred a full analysis, so the source supports only the narrower conclusion that Ricochet's marketing certainty was not earned.[13]

Security claims require precision

The archive contains well-supported findings, ambiguous claims, and some historical mislabeling. They should not be treated as one undifferentiated charge sheet.

In 2021, an independent researcher disclosed a real local PIN-bypass weakness in Samourai Wallet. Restarting the app reset the attempt counter; wallet metadata required for an offline PIN search was available on the device; and the PIN space was small. The issue became CVE-2021-36689. According to the researcher's timeline, Samourai acknowledged the report and initially decided not to fix it before public disclosure.[27]

That is a legitimate security failure with a defined version and threat model. It concerned a local attack, not the remote draining of every Samourai wallet.

My *SamouraiLeaks Part 3* investigation concerned a different and earlier codebase: the Blockchain.info Android wallet project William led as senior mobile developer while Keonne served as product lead. The visible repository begins with William's initial commit and attributes more commits to him than to any other developer. That history tied him to a generator that fetched entropy from Random.org over unencrypted HTTP. Under a narrow fallback path on older Android devices, a redirect combined with failed local entropy could produce deterministic key material.[28][5] Ars Technica independently reported the conditions and risk in 2015.[29]

That history documents a serious engineering failure under specific conditions. It does not support claims that every Samourai wallet used broken randomness or that William stole

anyone’s coins.

Those limits are essential to responsible disclosure, which requires defining what happened, who was affected, what is inferred, and what remains unknown. Samourai’s communications culture treated those distinctions as weakness when answering critics, then demanded endless qualification when scrutiny turned inward.

The official account made the imbalance visible. It responded to technical and community critics with obscenities, slurs, and personal humiliation.[30] A former r/Bitcoin moderator preserved his allegation that Samourai lied about how it received sidebar placement and free advertising.[31]

A sample of replies from the official Samourai Wallet account. The language is reproduced because the conduct itself is part of the record.

The volume and repetition make these exchanges more than a momentary failure of tone. Intimidation became part of the product's public identity.

When you wrestle with a pig, you both get dirty

The screenshots document individual incidents but cannot convey their cumulative effect over several years.

I began to approach technical conversations as possible trials of character because bug reports, imprecise reporting, and edited audio could all be reframed as evidence of bad intent. Leaving a false claim unanswered allowed it to spread, while answering prolonged the conflict.

I spent time preserving evidence that I wanted to spend on code. Friends and independent developers had to decide whether correcting the record was worth becoming the next target. The authorship distortion affected me most: a framework I created was folded into a joint-origin myth, and the project that benefited from my premature credit presented me as an enemy of privacy.

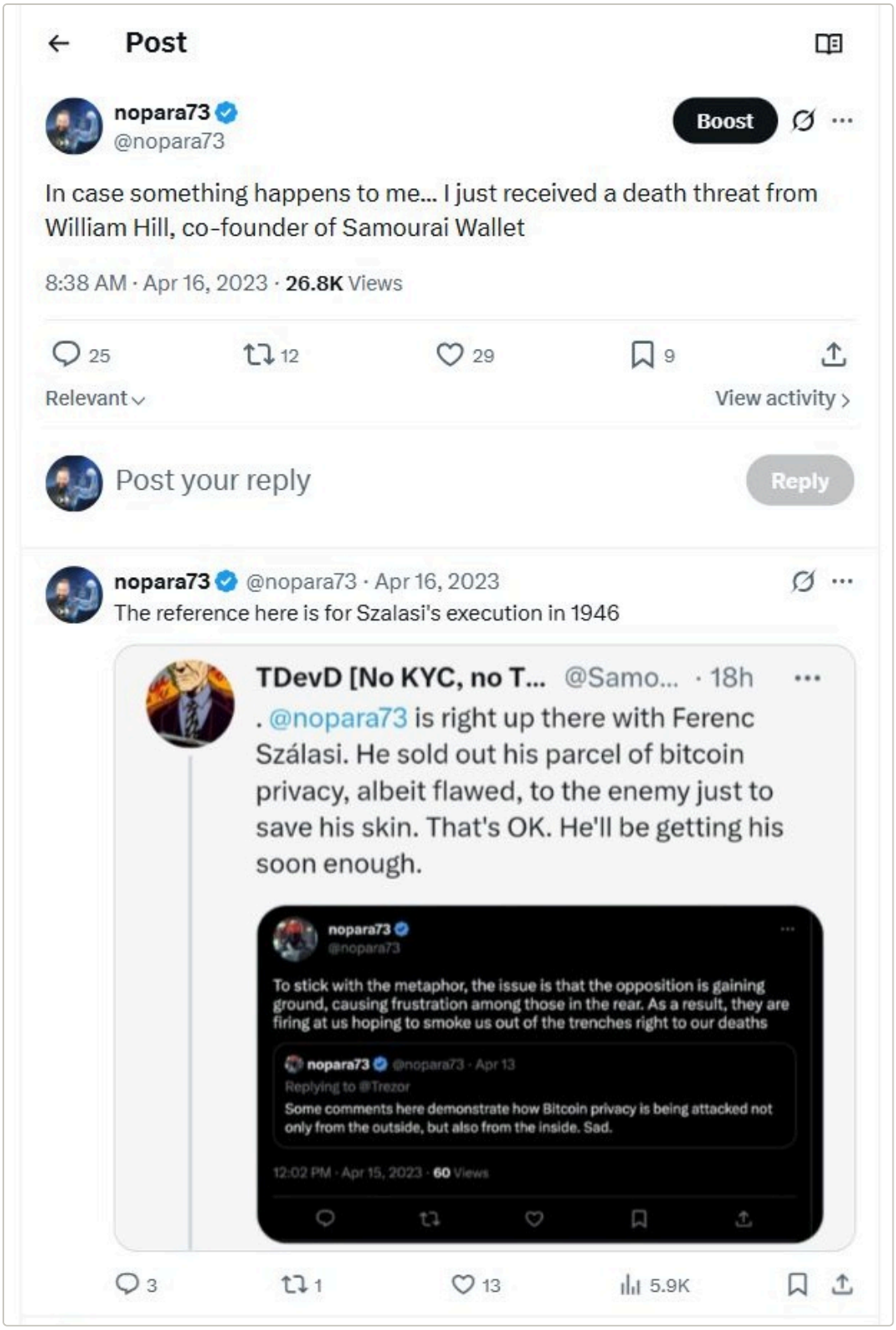
I did not handle that well.

I called the project “Scamourai” and swore at them; in 2019, CoinDesk quoted one of my replies simply saying “Fuck you.”[32] That anger produced little of value. The childish nickname allowed a long evidentiary record to be mistaken for reciprocal mudslinging and made it easier for outsiders to conclude that both sides were merely marketing tribes.

I also sometimes spoke with more certainty than the evidence allowed. Receiving an xpub, retaining it, selling it, and maliciously querying it are separate claims. I knew the default backend received wallet-level public information. Before the server analysis became public, I did not know everything Samourai retained or did with it. I should have marked those boundaries in an angry tweet as carefully as I would in a protocol review.

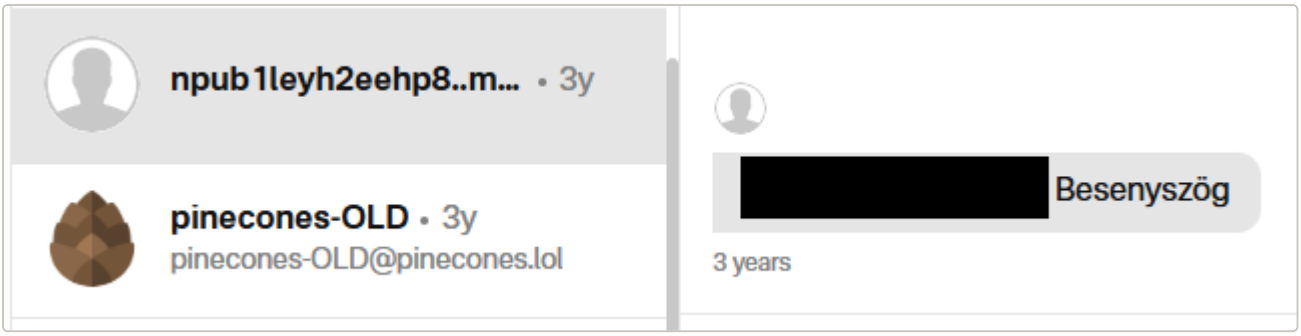
I regret the way I spoke. It made the documented issues easier to dismiss, even though it does not change the Git history or the evidence preserved here.

By April 2023, the conflict had passed far beyond professional hostility. I had received multiple death threats from William Hill—not one. I also received anonymous private threats during the same campaign. The screenshots alone cannot establish who controlled those anonymous accounts. After another dispute about Whirlpool’s Tor behavior, I wrote: “In case something happens to me… I just received a death threat from William Hill”. I did not publish every message, and what I did publish was only part of what I received.

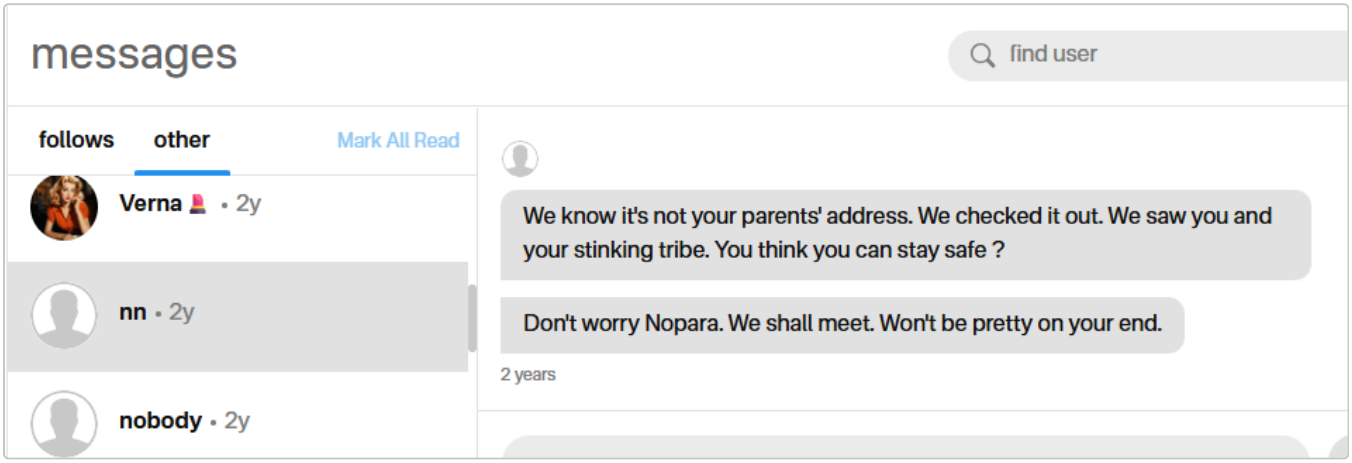


My public statement on April 16, 2023, together with the reference I said I understood as threatening.

One private message sent me a full address in Besenyszög. I blacked out the street-level portion before supplying the screenshot below. Another sender claimed to have checked an address and seen me and my “stinking tribe,” asked whether I thought I could stay safe, and ended: “We shall meet. Won’t be pretty on your end.” An interface label is not enough to identify who controlled an anonymous account, so the screenshot establishes only what I received.



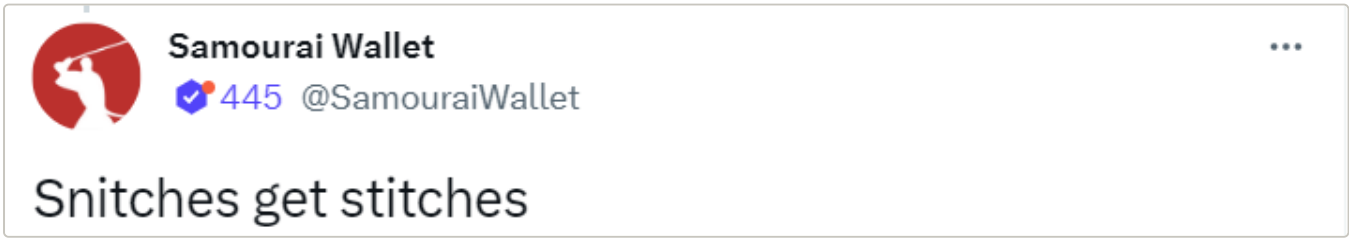
A private message containing a full address in Besenyszög. I supplied this image with the identifying portion already blacked out; the archive contains no uncensored copy.



A second anonymous account claimed to have checked an address and seen me, asked whether I thought I could stay safe, and threatened an eventual meeting. The screenshot records the message, not the sender's identity.

The threats were accompanied by doxxing. Hill posted my parents' home address more than once. I will not reproduce or link to those posts, because proving that it happened does not require exposing them again. His public `@SamouraiDev` profile still names me, says, "It ain't over until the fat boy is gutted," and appends the name of the small town where my parents live.[17] Publishing my family's location beside violent language was intimidation.

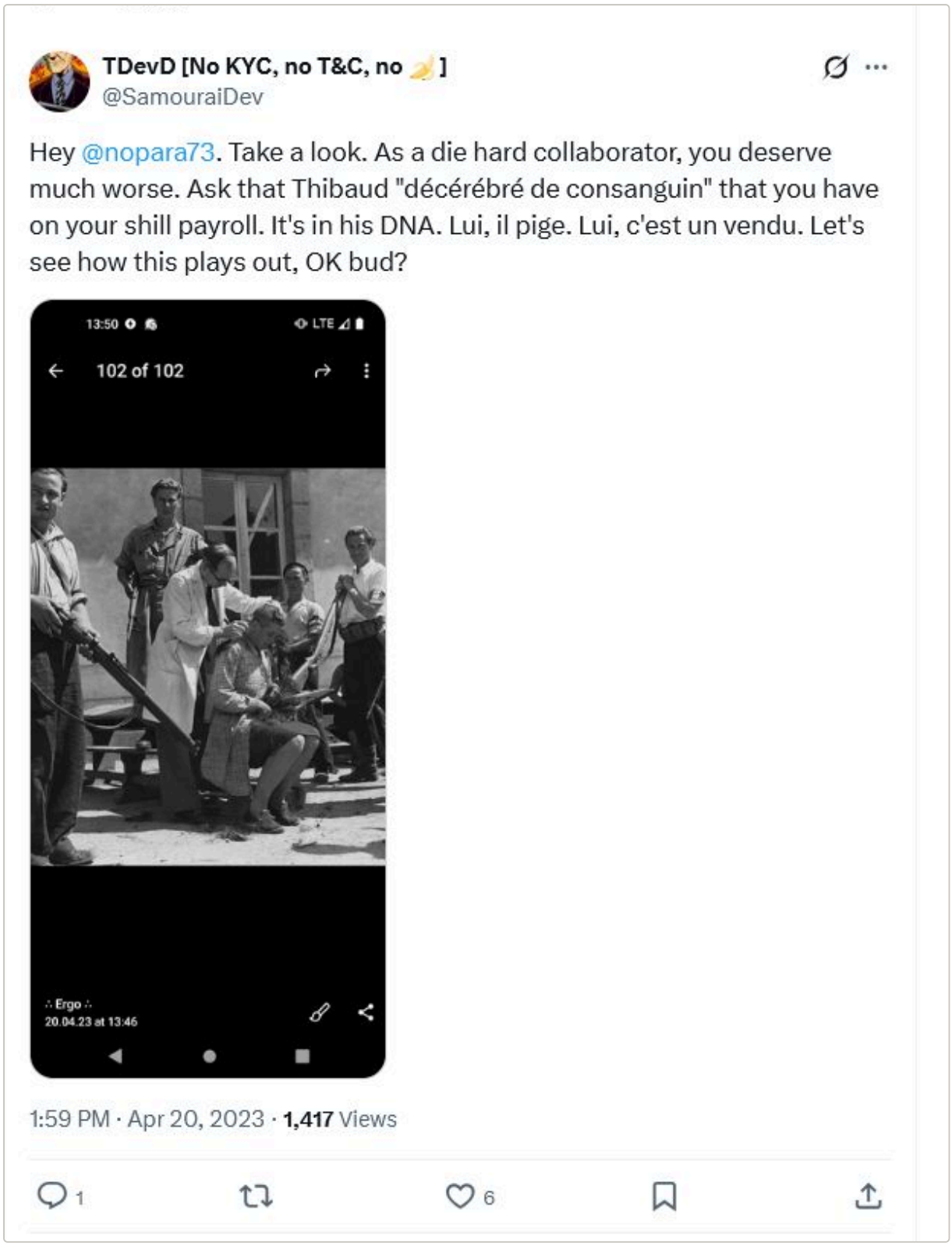
The public `@SamouraiDev` profile as preserved on July 10, 2026. I have not reproduced my parents' street address.



The complete source image from the official Samourai Wallet account's "Snitches get stitches" post, preserved again in my contemporaneous record on April 18, 2023. X's timeline preview cuts off part of the text; this archived source image does not.

Two days later, Hill addressed me directly: "As a die hard collaborator, you deserve much worse." He ended with, "Let's see how this plays out, OK bud?" The attached image showed

armed men surrounding a seated captive whose head was being shaved. I understood the combination of that image and those words as a threat.[18]



Hill's April 20, 2023 post paired "you deserve much worse" with an image of an armed public punishment. Open the post.

The campaign continued the next year. In February 2024, Hill wrote that I was "way overdue to get yours" and appended `#Besenyszög`. A follower replied, "Hope he gets stitches and ends up

in a ditch.” Hill answered: “Yes.” Then: “Soon.”[18]

The public February 20, 2024 thread: a location-linked warning, a reply hoping I would end up in a ditch, and Hill’s “Yes” and “Soon.” Open the first post and Hill’s reply.

Six weeks later, Hill made the violent reference unmistakable. “It ain’t over until the fat boy is gutted (see bio),” he wrote above Yasushi Nagao’s famous photograph of the assassination of Japanese Socialist Party chairman Inejirō Asanuma. I had incorrectly remembered the victim as a Japanese prime minister; the recovered post identifies him correctly. That correction does not change the nature of Hill’s post.[18]

Hill's April 4, 2024 post paired "gutted" with the photograph of Asanuma's onstage assassination. Open the post.

The criminal case later produced records independent of the feud.

What the server seizure revealed

When Samourai's founders were arrested in April 2024, I refused to treat the indictment as a verdict. Privacy software is not money laundering merely because criminals use it. The legal boundary around noncustodial software was—and remains—important.

But law enforcement also seized Samourai's servers, and the later filings addressed technical issues I had been raising for years.

In an October 2025 sentencing memorandum, the government said its analysis showed that Rodriguez and Hill had retained enough information to trace or "demix" mobile users' Whirlpool transactions. By cross-referencing stored xpubs with past, present, and future Whirlpool transactions, an analyst could connect the inputs and outputs of many transactions through complex analysis. The filing also stated an important limit: this did not by itself connect those transactions to real-world identities.[33]

on balance, each defendant is equally deserving of the Stipulated Guidelines Sentence of 60 months.

2. The Defendants Minimize the Scope and Gravity of Their Conduct

Although the defendants admitted in their plea allocutions and plea agreements that they knew criminal drug traffickers and hackers used Samourai to conceal their crime proceeds, the defendants, at several points in their sentencing submissions, minimized their offense conduct and downplayed or outright denied their marketing of Samourai to criminals for money laundering.[16] The defendants make various arguments in this vein. They both emphasize that the main goal of Samourai was to enhance privacy on the Blockchain[17] (Rodriguez Subm. at 2, 7; Rodriguez Letter

---

[16] Hill concedes, though undersells, his intent for criminals to use Samourai to launder crime proceeds, admitting that "he took things way too far when he . . . actively encouraged its use for money laundering." (Hill Subm. at 1; *see also* Hill Letter at 3 ("our marketing suggesting that computer hackers and other criminals should use Samourai instead of our main competitor's wallet spiraled well beyond acceptable limits.")

[17] Hill claims that he and Rodriguez created Samourai to frustrate Chainalysis and other forensic companies that conducted sophisticated blockchain tracing and wallet attribution because they were "stripping bitcoin of the privacy and fungibility that were the Cypherpunks' ideals." (Hill Subm. at 24). The Government notes, however, that Hill and Rodriguez operated OXT.me, a free, public blockchain explorer that was also a tool for blockchain tracing and wallet attribution, including for Silk Road and Hydra Market. (PSR ¶ 38). Thus, it appears that Hill's animating concern was not fidelity to anonymity, but hostility to forensic companies--like Chainalysis--known to assist law enforcement.

Likewise, notwithstanding Rodriguez and Hill's strong pro-privacy public comments, they did not always practice what they preached. As confirmed by law enforcement's seizure and analysis of Samourai's servers, despite claiming that Samourai was a "privacy" service, Rodriguez and Hill retained sufficient information to trace or "demix" its mobile users' Whirlpool transactions. In other words, with this information, one could for many Whirpool transactions, with complex analysis, connect the input and output of a Whirpool transaction (although this does not deanonymize the transactions). Rodriguez and Hill collected the information by requiring users to share their extended public key ("XPUB") information with the Coordinator Server. While there was no technical or operational necessity to do so, the defendants chose to retain their mobile users' XPUB information on Samourai's servers. This allowed the defendants to cross-reference

The government's description of the server analysis: retained mobile-user xpubs could be cross-referenced with Whirlpool transactions to connect inputs and outputs, without by itself identifying the real-world user. *Open the archived filing.*

The defense did not deny xpub collection. Hill's sentencing submission tried to recast it as a functional necessity: users without their own nodes needed the backend to calculate their balances, it said, and the design affected "only 20%" of Whirlpool users. That was a consequence of Samourai's chosen architecture, not a universal requirement of light wallets. Wasabi obtained block filters and checked addresses on the client without giving our server

the wallet's xpub.[2] The filing also gave no source, methodology, underlying counts, or independent measurement for its percentage. It may have been nothing more than a figure supplied by Samourai and repeated by its lawyers. The submission gives us no way to know.[33]

▶ **View the defense's xpub argument and "only 20%" claim**

"Only" is doing a great deal of work there. So is the unsourced percentage.

Even if the defense's estimate is accepted for the sake of argument, one in five Whirlpool users is a significant part of the user base. More importantly, the argument concedes the architecture I had objected to: a class of users provided its wallet graph to Samourai's infrastructure; Samourai retained that information; and the seizure placed it in government hands.

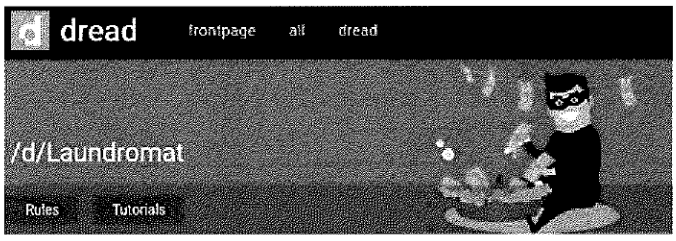
Dojo was not a practical escape for wallet users during Samourai's first four years. Its server code was released on June 2, 2019, but Samourai's announcement said the wallet still needed another update before it could pair with Dojo. Version 0.99.81 added pairing on July 11 and supported only newly created wallets; restoring an existing wallet was explicitly unsupported. An earlier user who wanted to stop using Samourai's servers at that point had to create a new wallet behind Dojo and move the balance out of the old one. That prevented the new wallet's xpub from being disclosed, but it could not erase the old xpub and history already sent to Samourai. A direct transfer between the wallets would also remain visible on-chain.[4]

The June 2025 superseding indictment reproduced private messages and Dread posts in which Hill steered people who openly described criminal proceeds away from a competing mixer and toward Whirlpool. It said Rodriguez knew Hill was conducting substantial promotional work on Dread.[34]

Samourai's commercial success was driven in large part by such transactions, as over $250 million in crime proceeds were laundered through Samourai.

20. As one example, on or about January 5, 2018, in a WhatsApp chat, when asked by an associate what "mixing"—*i.e.*, what Samourai did and advertised itself as doing—was, KEONNE RODRIGUEZ, the defendant, described that it was "money laundering for bitcoin." In other words, RODRIGUEZ admitted that the Samourai mixing service was a *money laundering* service, the crime he is charged with conspiring to commit in Count One of this Indictment. Rodriguez's associate then responded with an emoji: "🤯."

21. As another example, on Dread, a Reddit-like dark web message board featuring discussions about darknet marketplaces, WILLIAM LONERGAN HILL, the defendant, expressly advertised Samourai as a money laundering service. As pictured below, the discussion occurred in the subforum titled "Laundromat," bearing the banner photograph of a masked criminal washing money in a bathtub (*i.e.*, laundering or cleaning his dirty money), and in a post titled "How to clean dirty BTC."



2 How to clean dirty BTC?

In this forum, a Dread user asked what were the most "[s]ecure methods to clean dirty BTC" so that the BTC would become "untraceable, clean" and the Dread user would "never get caught." On or about October 2, 2023, HILL responded by criticizing a competitor mixer ("Mixer-1") by directing the Dread user to "Avoid [Mixer-1] at all costs" and, instead, encouraged the Dread user

to use Samourai, writing that "Samourai Whirlpool is a much better option" to clean dirty BTC—or, in other words, to launder money.

22. In another Dread post, WILLIAM LONERGAN HILL, the defendant, again encouraged darknet marketplace customers to use Samourai to conceal their crimes. In a discussion thread in the subforum "DarkNetMarkets," titled "Payments on darknet markets," a Dread user asked why darknet marketplaces still allowed BTC for transactions when "Bitcoin is a well know[n] traceable tool, LE [*i.e.*, law enforcement] have proved it time and time again," and expressing concern that "people are buying drugs here playing with their freedom." On or about November 14, 2020, HILL responded by criticizing Mixer-1, directing the Dread user to "avoid[]" Mixer-1 "at all costs," and, encouraging the Dread user to use Samourai Whirlpool.

23. KEONNE RODRIGUEZ, the defendant, was well aware that WILLIAM LONERGAN HILL, the defendant, advertised Samourai specifically on dark web message boards, including Dread, because on or about August 18, 2020, RODRIGUEZ stated in a Telegram thread with an associate that "we're making a space on the dark net boards, dread in particular" and HILL "has been doin[g] a lot of work there."

24. In private Telegram messages with an associate, KEONNE RODRIGUEZ, the defendant, made clear that he intended for criminals to use Samourai to conceal their crime proceeds and that he believed that Samourai's competitor, Mixer-1, inadequately concealed crime proceeds, which likely would result in incarceration. For example, on or about July 27, 2019, RODRIGUEZ wrote that Mixer-1 was "playing fast and loose" with its concealment methodology, and "is likely to get someone locked up." RODRIGUEZ's associate replied, "[e]specially as some of the people that have BTC from obvious hacks etc haven't mixed them in a sophisticated way." RODRIGUEZ endorsed the message by responding, "yeah it is crazy."

Pages 10–11 of the superseding indictment reproduce the Dread context and allege that Hill steered users describing criminal proceeds toward Whirlpool, while Rodriguez knew he was doing promotional work there. An indictment is an allegation, not a verdict; both men later entered guilty pleas to the offense described below. Open the archived indictment.

This mattered because Samourai and OXT had repeatedly turned criminal use of Wasabi into part of the public case against us. Yet the later record showed Samourai pursuing those same users as customers. On Dread, competitor disparagement was not an abstract contribution to privacy research. It was a sales pitch aimed at people asking how to conceal criminal proceeds.

On July 30, 2025, Rodriguez and Hill each pleaded guilty to conspiring to operate a money-transmitting business knowing it transmitted crime proceeds. The money-laundering conspiracy count was dropped through the plea agreements. The Justice Department announced the pleas on August 6, and its account included their Dread marketing.[35] In November, Rodriguez received five years in prison and Hill four.[36]

The sentences did not resolve the software issues, and the prosecution raised troubling questions of its own. Before the pleas, the defense argued that prosecutors had disclosed too late a FinCEN communication saying Samourai's lack of control over users' keys strongly suggested it was not a money-services business under FinCEN's rules. The government disputed the communication's significance.[37] Anyone who cares about open-source privacy software should care about that due-process issue.

The case added previously unavailable information about retention, intent, and marketing, although the sentences themselves say nothing about who was right technologically.

The lies and hypocrisies

Developers can be mistaken, remember events differently, or speak with unjustified confidence. I use "lie" more narrowly: a materially false account repeated after contrary evidence has been presented because the false version remains useful.

By that standard, the ZeroLink co-creation story was a lie. The framework predated Samourai's involvement; the first Samourai contribution fixed typos; and they repeated the joint-origin account years after I challenged it with the repository.[1][2][5]

The claim that I had admitted Wasabi supplied its own liquidity was false. The journalist corrected that interpretation, but Samourai continued promoting the damaging version while omitting my correction.

The categorical Tor answer was false. The public record cannot establish whether Rodriguez knowingly lied or answered with reckless certainty, but it does show that he insulted the questioner and that the code later added the identity change the question had asked about.[2][3]

The "full node wallet" claim was false too. It appeared in a thread explicitly about the default app sending xpubs to Samourai, after the official account had defended its chosen backend architecture. A user-run Dojo could place the backend on the user's full node. Without Dojo, the Android app was a light client of Samourai's backend.[3]

Samourai's use of OXT was another direct hypocrisy. It denounced surveillance companies while owning and operating a blockchain tracing and wallet-attribution tool of its own. It then used that tool's research label to issue a severe public warning against its principal competitor. OXT's own declared rule was that privacy must be protected by the software's defaults, not by

work pushed onto the user. Samourai's default collected the xpubs; avoiding that collection required the user to run Dojo.[82]

The coordinator-fee address shows the double standard directly. In February 2020, Samourai condemned Wasabi's reuse of such an address in absolute terms. Even after Wasabi changed it, Samourai said the damage had already been done: "There's no going back from more than a year of address reuse." In October 2023, Kruw reported on Samourai's own GitLab that Whirlpool's coordinator had reused one fee address across 37 transactions. In one transaction cited in the report, 36 outputs from that address were consolidated as inputs.[10]

The reuse alone does not prove that Whirlpool users were demixed. The `TX0` fee output was already recognizable, and a contemporary critic argued that rotating its address would not improve Whirlpool's CoinJoin privacy. The issue is the standard Samourai applied: it described the same practice in Wasabi as irreversible architectural damage, while Kruw says his Whirlpool report was deleted. The surviving Wayback capture is an open issue archived less than a minute after it was filed, so the deletion claim rests on Kruw's same-day account rather than a later Wayback capture.[10]

The privacy promise itself was contradicted by the product's defaults. Samourai marketed resistance to financial surveillance while the wallet sent xpubs to its hosted backend and left Tor off unless the user enabled it. The hosted service could therefore receive the wallet graph and the connecting IP address together. They also called Sentinel the "easiest and most secure" way to watch cold storage, while its hosted-server mode handed Samourai the xpub that allowed Samourai to watch it too. When the wallet's unsafe defaults were reported on Samourai's GitLab, the project owner rejected the proposed change, threatened the reporter, and closed the issue. The server seizure later demonstrated why the backend's wallet-level information mattered.[21516][33]

Samourai also used criminal association selectively. It repeatedly tried to turn alleged criminal use of Wasabi into a case against us while privately promoting Whirlpool to darknet users who openly described criminal proceeds.[34][35]

zkSNACKs deserved criticism for blacklisting, but that policy did not turn Wasabi into a surveillance wallet. The coordinator decided which inputs to accept while the blinded design still prevented it from linking those inputs to their outputs. Samourai's default backend, by contrast, retained wallet-level information.[22][33]

I use the name Scamourai to describe what I see as a false central promise, not as a legal accusation of fraud. The product sold protection from surveillance while placing its operator in a position to surveil, and it promoted verification while requiring default users to trust that Samourai would not misuse wallet information that its servers retained. To me, this went beyond imperfect privacy because the contradiction was built into the default architecture.

Post-mortem

The lasting damage was to the authorship record and to the possibility of productive competition. I gave TDevD more credit than the repository justified, and Samourai inflated that credit into co-creation. Minor edits became joint research through repetition. The same culture made correction look like surrender and uncertainty look like weakness, turning technical competition into personal hostility.

I contributed to that hostility by answering contempt with contempt. I cannot undo those words, but I can document the history more carefully now.

Future privacy developers should not take this essay as a request to trust me or as a rule that every server and coordinator is unacceptable. The practical lesson is to examine what an operator can learn if its infrastructure is compromised, coerced, or seized. Team identity and a founder's character are not privacy guarantees. A sound protocol should continue protecting users when trust in the operator fails.

Sources and notes

Further reading

- BlockDigest, SHI256 episode 1, July 2019. Shinobi distinguishes the architectures and records the contemporary "two competing approaches" view; that framing does not negate the default xpub disclosure.
- Yuval Kogman, "Unbreaking Whirlpool's Privacy", Bitcoin Development Mailing List, December 2024. Kogman discloses his connection to WabiSabi and analyzes a coordinator key-consistency problem affecting both protocol families; he states that he found no evidence the Whirlpool coordinator had exploited it.
- WalletScrutiny, historical reproducibility record for Samourai Wallet. Results varied by release and build conditions; the current seizure-era status should not be projected backward onto every version.
- nopara73, *ScamouraiWallet* source archive. The archive preserves useful leads but contains mislabeled links; this essay relies on the underlying sources rather than treating the repository's labels as evidence.

---

1. The figures in this section were reproduced from the ZeroLink repository using the full commit graph, non-merge `README.md` numstats, and line-porcelain blame at commit 25d1502, the August 14 publication snapshot used for the audit. The 13 Bill/TDevD commits comprise 97 additions and 43 deletions; nopara73's 134 non-merge commits comprise 1,151 additions and 684 deletions. Line churn is not equivalent to intellectual authorship, which is why the chronology and individual patches are also described. In Research Club episode 26, "A Survey on CoinJoin

Transactions”, at 53:47–54:52, I distinguish Chaumian CoinJoin from ZeroLink and describe ZeroLink as a broader privacy framework for Bitcoin wallets; see the local transcript. Episode 14, “ZeroLink”, at 27:39–28:24, records my qualification that parts of the broader framework had aged while its Chaumian CoinJoin core remained sound; see the local transcript. ↩ ↩ ↩

2. Wasabi’s documentation explains its block-filter and Tor architecture, including why sending an xpub to a central server enables complete wallet deanonymization, and states that its coordinator cannot link inputs to outputs. Samourai’s archived Dojo documentation says MyDojo bypasses the default hosted servers and describes a Tracker that records the activity of registered xpubs and addresses. The inference about mixed Dojo/default-server rounds is also explained by Chris Belcher and the independent thesis cited in note 1. ↩ ↩ ↩ ↩ ↩ ↩

3. The October 3, 2022 exchange began with Kruw identifying the default xpub disclosure and proposing BIP157/BIP158. Samourai refused block-filter support, defended its chosen architecture, and said it had been “open and truthful from day one”. It then answered a direct question about reconsidering BIP157 with the “full node wallet” claim. The posts and the focused context image are archived under `sources/social/`. The Bitcoin developer guide defines a full-node client as one that downloads and validates blocks from genesis to the chain tip; BIP157 describes compact filters as a protocol for light clients. Samourai’s production source at `4bf9870`, merged four days before the post, shows `APIFactory` sending joined xpubs to the selected backend and `BackendApiAndroid` selecting Samourai’s backend whenever Dojo was absent. The exact cited files are preserved locally. Samourai’s own 2019 Dojo announcement and Hill’s later submission are cited in notes `dojo-release` and `xpub-seizure`. ↩ ↩ ↩

4. Samourai’s June 2, 2019 Dojo 1.0 announcement, preserved locally, said that users had previously needed to trust Samourai’s servers with their public keys and that one further wallet update was still required for Dojo pairing. The July 11 version 0.99.81 announcement, also preserved locally, introduced pairing for “a newly created Samourai Wallet,” instructed the user to create a new wallet after scanning the Dojo QR code, and stated that restoring an existing wallet was “currently unsupported.” Moving bitcoin directly from the old wallet to the new one would reveal that transfer on-chain; avoiding future xpub disclosure is not the same as erasing information already disclosed. ↩

5. The reproducible source-lineage audit preserves the exact commits, files, archives, and comparison scope. The surviving Blockchain.info `Android-Wallet-2-App` history begins with William Hill’s April 30, 2014 `9f4e200` “Initial commit”; across its preserved refs, 352 commits are attributed to Hill identities, compared with 189 for the next-largest author. Hill also authored the September 2014 `4063b3a` “UI prep for shared coin”. A contemporary interview, preserved locally, identifies Keonne Rodriguez as Blockchain.info’s product lead for the refreshed wallet’s UI and UX, while Hill’s sentencing submission, submission pp. 21–22 (PDF pp. 26–27), identifies him as its senior mobile developer. Samourai’s public history begins with TDevD’s March 30, 2016 `c6274d1`; contemporary coverage, preserved as a local text snapshot, quotes Samourai saying it had delayed publication for about a year to gain a competitive advantage. The audit documents several high-confidence file descendants without claiming that the whole application was a verbatim fork or that Hill and Rodriguez founded Blockchain.info. ↩ ↩ ↩

6. The complete locally archived Wasabi Research Club transcript collection includes the cited discussions. Episode 8, “CashFusion with Jonald Fyookball & Ethan Heilman (Part 2)”, at 1:13:45–1:15:36, says the Blockchain.info server knew everything and that SharedCoin offered no privacy guarantee from the server; see the local transcript. Episode 10, “CoinJoin Sudoku”, at 30:57–31:59, likewise treats the server’s knowledge of the links as the starting assumption; see the local transcript. Episode 14, “ZeroLink”, at 04:17–04:48, rejects the hypothetical trusted server collecting everyone’s extended public keys and explains blinded coordination; see the local transcript. Episode 26, “A Survey on CoinJoin Transactions”, at 55:47–59:01, records the SharedCoin comparison, Samourai’s default xpub collection, the Dojo/default-user intersection, and the exclusion argument; see the local transcript. Research Club episode 30 (playlist position 32), “Checking Bitcoin balances privately”, at 1:11:55–1:12:26, discusses the risk that an xpub retained on another computer could be exposed through hacking or seizure; see the local transcript. The transcripts are YouTube auto-captions and are cited with timestamps; the essay paraphrases obvious recognition errors rather than silently quoting them as exact speech. ↩ ↩

7. The Dumplings repository describes `FreshBitcoins` as its “best proxy for user adoption”: bitcoin entering a recognized CoinJoin for the first time, excluding remixes. The exact source files used here are preserved at commit `36f28f2` in the local adoption-data archive. The reproduction note records the grouping method, monthly comparison, totals, scope, and limitations. From April 2019 through August 2022, the data sum to 247,675.31 fresh BTC for Wasabi and

30,228.14 for Whirlpool, a ratio of 8.19 to one; Wasabi's monthly total is higher in all forty-one months. This metric measures fresh bitcoin volume, not unique installations or people. ↩

8. Samourai's December 21, 2017 acquisition announcement, preserved locally, says it had "finalized the acquisition" of OXT in an all-Bitcoin transaction, calls the purchase a long-term strategic investment, and describes OXT as a separate but complementary entity. OXT developer Stephen Rossi's support letter in Hill's sentencing submission, PDF p. 130, calls OXT a forensic tool "owned and operated by Samourai Wallet"; the relevant passage is preserved as a focused screenshot. The government's sentencing memorandum, PDF p. 37 n.17, independently describes OXT as a tracing and wallet-attribution tool operated by Hill and Rodriguez. OXT's August 2020 follow-up, archived locally, calls OXT a "sparring partner for Samourai Wallet" and states: "The default software behavior should be responsible for maintaining the guarantees of a service, not the end user." ↩ ↩ ↩ ↩

9. The public January 4, 2023 sequence is preserved through the original posts and local oEmbed records. OXTObserver labeled 204.77460928 BTC as `#LUKE-JR_STOLEN_FUNDS` and "Wallet Controlled By Hackers." Samourai Wallet quoted that alert and described the stolen coins' movement. A user then asked what Samourai would do if the coins entered Whirlpool, and the official account gave the quoted answer. Kruw's February 2026 post resurfaced the exchange. The corresponding JSON records and the original OXT graph image are archived under `sources/social/`. The thread documents Samourai's expressed reaction to a hypothetical Whirlpool deposit; it does not establish that the stolen coins actually entered Whirlpool. ↩

10. In Stephan Livera Podcast episode 150, Samourai criticized Wasabi's fixed coordinator-fee address and said that changing it could not undo more than a year of reuse; the transcript is preserved locally. Kruw's October 25, 2023 GitLab issue #462, preserved locally, identifies `bc1qhyls4wa9hlpvwa0y980mz0qhjyfhjkf4t5v6lh` as a Whirlpool coordinator-fee address used in 37 transactions. The issue cites transaction `05a400…`; its archived mempool API record shows that 36 of its 182 inputs spend outputs previously sent to that address, totaling 4,155,000 sats. Kruw's same-day Bitcointalk thread, preserved locally, says the report was deleted and contains the technical objection that the `TX0` fee output was already identifiable, so the reuse did not itself reduce the privacy of the subsequent Whirlpool CoinJoin. The Wayback Machine exposes only the open capture made at 11:28 UTC, so it preserves the report but does not independently prove its later deletion. Kruw's December 2025 post, preserved as oEmbed metadata, brought the archived issue back into the public record. ↩ ↩

11. Samourai's own OXT acquisition announcement specifically praises LaurentMT's Boltzmann as an open-source tool for measuring transaction plausible deniability. Wasabi Research Club episode 11, "Boltzmann (Bitcoin)", was published March 17, 2020; the local transcript records the full discussion. At 39:52–40:56, I question how transaction entropy applies to individual-user privacy, call anonymity set clearer for that purpose, and note that the partition calculation is infeasible for large Wasabi transactions. Episode 8, at 44:12–45:46, makes the related distinction between the public fungibility of a transaction and the privacy of a particular user against an observer with additional network and graph information; see the local transcript. These are limitations on what the metric establishes, not an allegation that Boltzmann itself was fraudulent. ↩

12. Samourai's own July 2021 statement about atomic swaps, preserved as a local text snapshot, describes "unmixed 'toxic change' from Whirlpool CoinJoin transactions" and a proposed way to move it through Monero. The official Whirlpool server configuration, preserved at exact commit `f23c2d3` in a local source archive, defines a fixed denomination for every pool, `TX0` fee rules, and equal input/output amounts for mixing. Research Club's April 2023 panel "Bitcoin Toxic Change in Coinjoin" is preserved in the local transcript. At 15:00–17:37, the panel's Samourai-side explanation says `TX0` creates and isolates toxic change; at 50:33–52:42, another participant explains why moving that change before the CoinJoin does not add an on-chain break from the first mix; and at 1:04:39–1:07:44, the panel traces the public input consolidation in `TX0` and the post-mix consolidation and change required by arbitrary payments. The argument in the essay is limited accordingly: `TX0` improves accidental-spend protection and removes change from the CoinJoin transaction, but it does not make toxic change disappear from the user's transaction history. ↩ ↩ ↩

13. The pre-seizure Samourai Android source at commit `c71f21a` provides the narrow implementation evidence. `RicochetMeta.java` sets a default of four hops; its loop makes each hop spend the preceding transaction and computes the forwarded amount from the final spend plus the remaining per-hop fees. The exact file is preserved in the local cited-source archive. Research Club episode 8, at 1:25:04–1:26:07, contains the brief fingerprint objection and

explicitly defers the debate; see the local transcript. For that reason, the essay calls the pattern recognizable but does not claim a demonstrated deanonymization. ↩

14. Hill's July 27, 2022 post is preserved as oEmbed metadata and a context screenshot. The backend/coordinator distinction can be checked against the code and documentation collected in notes `operator`, `tor-default`, and `sentinel`; the authorship claim can be checked against the repository audit in note `zerolink`. ↩

15. Samourai's signed Android source at commit `c71f21a` (v0.99.95, June 17, 2020) provides direct evidence of the defaults. `LandingActivity.java` permits wallet creation independently of the Tor switch and reads `ENABLE_TOR` with a `false` fallback. `SamouraiApplication.java` starts Tor only when that preference is true. `APIFactory.java` sends xpub queries through the ordinary `postURL` path when Tor is not required, and its xpub-registration method makes the same direct/Tor distinction. The archived April 17, 2023 GitLab issue #458 preserves the screenshot of Tor off and Dojo unconfigured, the proposed safer defaults, the project owner's response, and the immediate closure. Samourai's own 2021 account described Tor as something users could activate with a button; contemporary setup guides likewise instructed users to enable it. ↩ ↩ ↩

16. Sentinel's own welcome text called it the "easiest and most secure" way to watch cold storage and emphasized that private keys were never communicated to the app; that statement addressed custody, not xpub privacy. The official repository shows the relevant history directly. On August 12, 2017, commit `77eca1d` changed the xpub `multiaddr` request from Blockchain.info to Samourai's API. Commit `1a4722f`, dated September 20, 2019, added Tor routing and a network dashboard. In the ensuing v3.6 source, `APIFactory.java` sends each xpub as `multiaddr?active=<xpub>`; `InsertSegwitActivity.java` separately posts the imported xpub to the `/xpub/` endpoint; and `WebUtil.java` reads the Tor preference with a `false` fallback, while its API selector uses the public Samourai endpoint when Tor is not required. A mirror preserving the last pre-seizure GitLab history shows the same design in v5: the first-run screen offered Samourai's server and a separate yes/no Tor prompt, while `ApiService.kt` posted the imported xpub to `/xpub`. RoninDojo's contemporary v5 guide independently describes the choice between the user's Dojo and Samourai's node. ↩ ↩

17. My April 16, 2023 public statement records one of the threats. Hill's public `@SamouraiDev` profile, checked July 10, 2026, names me, uses the quoted "gutted" language, and appends my parents' town. Current social-media index caches independently reproduce the same profile text, including this TwStalker index and this second index. My parents' street address is intentionally neither reproduced nor linked. ↩

18. The public sequence is preserved through the original posts and local records: Hill's April 15, 2023 Szálasi comparison and "getting his soon enough"; the official wallet account's April 18 "Snitches get stitches" post; Hill's April 20 "you deserve much worse" image post; his February 20, 2024 "overdue to get yours #Besenyszög" post and "Yes ... Soon" reply; and his April 4 "gutted" assassination-image post. The corresponding oEmbed JSON, screenshots, and two original media files are archived under `sources/social/` and `sources/screenshots/`. World Press Photo identifies Nagao's image as Otoya Yamaguchi assassinating Socialist Party chairman Inejirō Asanuma during a speech at Hibiya Hall. ↩ ↩ ↩

19. Denis Varga, *CoinJoin Protocols and Implementations Analysis*, Masaryk University master's thesis, 2022, especially pp. 58–70. The thesis found that Whirlpool closely followed its detailed specification, described Wasabi 1's specification as outdated relative to its implementation, and emphasized the privacy trust placed in Samourai's default backend. See also Greg Maxwell's 2018 architectural criticism and Chris Belcher's explanation of the mixed Dojo/default-server anonymity set. ↩

20. ZmnSCPxj, Reddit comment, January 2021. He said Samourai had misconstrued his "pure ZeroLink" comment and distinguished using the default backend from running one's own node and software. ↩

21. *Citadel Dispatch*, "JoinMarket Dev: Wasabi vs Samourai", December 2022, especially 11:24–19:43. The relevant clip was also posted to Reddit. ↩

22. BlockDigest, SHI256 episode 256, especially 57:42–64:10, discussing PayNym short-name caching, the response to questions, and the later patch. ↩ ↩

23. Screenshots of the April 2023 Telegram exchange. The gallery preserves Rodriguez's categorical answer and the surrounding dispute. The later code commit is linked in the body. ↩ ↩

24. OXT's archived full technical report supplies the details omitted from its public warning. On pp. 2–3 it requires knowledge of the target wallet's composition at step N and knowledge of subsequent mixing events. On pp. 5–7 its test gives "Eve" knowledge of "Alice's" funds and wallet state, starts Alice with a single known 0.4 BTC input, and uses a modified client to log round events. The report's "vulnerability #2," on pp. 4–5, uses change-output "beacons and checkpoints" to detect deviations from the first model. The resulting "adjusted anonsets" are OXT's analytical estimates; the test does not identify Alice as a real person or recover a blinded input-output mapping. OXT's initial warning demanded a public statement within forty-eight hours and labeled the claims Critical. My contemporaneous line-by-line response identifies the assumed wallet knowledge, the unsupported leap to "cancelling" previous mixes, and OXT's failed predictions in its own spreadsheet. OXT's follow-up answers the missing-knowledge objection by hypothesizing powerful adversaries with pooled data and coordinator logs, but does not demonstrate how its tested observer acquired the target wallet state. The claim that Wasabi 2 was a response is also contradicted by the public timeline: Bitcoin Optech covered WabiSabi on June 17, 2020, and the Wasabi 2 status report says the research team was established in January 2020—both before OXT's August disclosure. ↩ ↩ ↩ ↩ ↩

25. Bitcoin Takeover, interview with Samourai Wallet, June 2022, especially 15:20–18:58. The interview repeats Samourai's joint-origin account of ZeroLink and presents Wasabi 2's later selection behavior as confirmation that OXT's criticism forced a fix. The ZeroLink repository does not support co-creation, while the WabiSabi timeline in note 6 predates OXT's disclosure. ↩ ↩ ↩

26. The original March 2022 announcement is quoted in contemporaneous coverage. zkSNACKs later explained in this open discussion that the company was under legal and regulatory pressure, did not want to perform its own surveillance, and expected alternative coordinators to remain possible. The operational pressure described in the body is my first-person recollection; the linked public sources corroborate the general context, not every internal detail. ↩ ↩

27. Justin Steven, "Samourai Wallet Bitcoin PIN Authentication Bypass", August 2021. The post contains the technical report, proof of concept, affected version, and disclosure timeline. ↩

28. My article, "SamouraiLeaks Part 3: Is random.org Random Enough?", July 2019; the historical `RandomOrgGenerator.java`. Repository history attributes the relevant 2014 commit to William Hill. ↩

29. Dan Goodin, "Crypto Flaws in Blockchain Android App Sent Bitcoins to the Wrong Address", *Ars Technica*, May 2015; original technical discussion. ↩

30. Gallery of posts from the official Samourai account; one surviving March 2021 post. The purpose of citing these is to document tone and targeting, not to endorse repeating the slurs. ↩

31. BashCo, archived post about the r/Bitcoin promotion dispute, August 2020. ↩

32. Leigh Cuen, "A Battle Between Bitcoin Wallets Has Big Implications for Privacy", *CoinDesk*, August 2019. The article is a useful contemporary record of the dispute, but its competitive framing should be read against the default xpub asymmetry documented above. ↩

33. The U.S. Attorney's Office said that Icelandic authorities seized Samourai's web servers and domain on April 24, 2024. The government's later sentencing memorandum, *United States v. Rodriguez and Hill*, No. 1:24-cr-00082-DLC, ECF No. 157 (S.D.N.Y. Oct. 31, 2025), pp. 36–37, says server analysis showed retained xpub data could be used, through complex analysis, to associate inputs and outputs for many mobile users' Whirlpool transactions; it also reproduces Hill's post-seizure messages about the "wallet backends (xpubs)." Hill's own sentencing submission, ECF No. 155 (S.D.N.Y. Oct. 24, 2025), pp. 23–24 & n.20, argues that xpub collection was necessary for light-wallet balance calculation and asserts that it affected 20 percent of Whirlpool users. The submission provides no citation, methodology, underlying counts, or independent study for that percentage, and the government's memorandum does not validate it. The government's "demix" finding is itself a representation in a sentencing memorandum, not an independently published forensic report. ↩ ↩ ↩ ↩ ↩

34. *United States v. Rodriguez and Hill*, Superseding Indictment, No. 1:24-cr-00082-RMB, ECF No. 109 (S.D.N.Y. June 24, 2025), especially pp. 10–16. These passages were allegations at the time of filing; later admissions are separately cited below. ↩ ↩

35. U.S. Attorney's Office, Southern District of New York, "Founders of Samourai Wallet Cryptocurrency Mixing Service Plead Guilty", August 6, 2025. For the plea bargain's dismissal of the laundering count, see contemporaneous reporting. ↩ ↩

36. U.S. Attorney's Office, Southern District of New York, "Founders of Samourai Wallet Cryptocurrency Mixing Service Sentenced to Five and Four Years in Prison", November 19, 2025. ↩

37. Defense letter alleging late disclosure of FinCEN communications, *United States v. Rodriguez and Hill*, May 5, 2025. This was a defense argument, not a judicial finding. ↩

This is the canonical HTML edition of version 1.0.0, published 2026-07-11.

Built from `75e545620927f75ba487997bb1cf03360738ffe9`; source SHA-256 `7f9fca7748f9e87b58e43ac70a3c1b3dc25899c4b00539daacd5cfec60ee2518`.