Looking up message... ···

provoost · 5h ···

Still have to read this, but the most suspicious part is: why is Pertsev not named? It's not like the US doesn't know he's being prosecuted in The Netherlands.

Looking up message...

1 Likes

29 1

Write your reply

provoost · 5h ···

It's also interesting that the indictment doesn't have a date on it. It starts out with references to "up to and including at least on or about August 8, 2022"

Is that because they considered Tornado cash dead the moment OFAC hit it? Or did they hold it sealed waiting for this to settle: www.coindesk.com/policy/2023/08/22/privacy-mixer-tornado-cash-is-an-entity-judge-says

1

provoost · 5h ···

That ruling is here: storage.courtlistener.com/recap/gov.uscourts.txwd.1211705/gov.uscourts.txwd.1211705.94.0.pdf

1

provoost · 3h ···

Fascinating. I think what the judge is saying here is that, in the context of what OFAC is allowed to do, if you create a vending machine and relinquish all

control of it, it's still your "property" and so it can be sanctioned.

The judge doesn't discuss whether it's relevant that the vending machine doesn't and can't pay you. Such discussion would be remenescent of how the Dutch tax authorities treat trusts (even if it never pays you, you pay wealth tax as if it's your own money).

But I think the better analogy would be donating the vending machine to a non-profit. You spent resources building it, but it now serves the commons, not you. Hopefully they'll try that argument in the appeal.

a. The Smart Contracts are Property Within the Meaning of the Statute

Plaintiffs contend that the smart contracts are not property because they are incapable of being owned, and that, even if they were, Tornado Cash does not have a "legal or equitable claim or right in property" to them. But OFAC's regulations define "property" and "interest in property" as follows:

> The terms property and property interest include money, checks, drafts, bullion, bank deposits, savings accounts, debts, indebtedness, obligations, notes, guarantees, debentures, stocks, bonds, coupons, any other financial instruments, bankers acceptances, mortgages, pledges, liens or other rights in the nature of security, warehouse receipts, bills of lading, trust receipts, bills of sale, any other evidences of title, ownership, or indebtedness, letters of credit and any documents relating to any rights or obligations thereunder, powers of attorney, goods, wares, merchandise, chattels, stocks on hand, ships, goods on ships, real estate mortgages, deeds of trust, vendors' sales agreements, land contracts, leaseholds, ground rents, real estate and any other interest therein, options, negotiable instruments, trade acceptances, royalties, book accounts, accounts payable, judgments, patents, trademarks or copyrights, insurance policies, safe deposit boxes and their contents, annuities, pooling agreements, services of any nature whatsoever, contracts of any nature whatsoever, and any other property, real, personal, or mixed, tangible or intangible, or interest or interests therein, present, future, or contingent.

31 C.F.R. §§ 510.323, 578.314.

The Court finds that OFAC's determination that the smart contracts constitute property, or an interest in property, is not plainly inconsistent with the regulatory definition of those terms. Plaintiffs argue that the smart contracts cannot be considered property because they are immutable and therefore cannot be owned. However, OFAC's definition of property encompasses "contracts of any nature whatsoever," and—as other courts have recognized—smart contracts are merely a code-enabled species of unilateral contracts. *See, e.g.*, *Rensel v. Centra Tech, Inc.*, No. 17024500-CIV, 2018 WL 4410110, AT *10 (S.D. Fla. June 14, 2018) ("Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code"). *In re Bibox Grp. Holdings Ltd. Sec. Litig.*, 534 F. Supp. 3d 326, 330 (S.D.N.Y. 2021) ("A smart contract

with the terms of the agreement between buyer and seller being directly written into lines of code"). *In re Bibox Grp. Holdings Ltd. Sec. Litig.*, 534 F. Supp. 3d 326, 330 (S.D.N.Y. 2021) ("A smart contract allows the parties to define the terms of their contract and submit the crypto-assets contemplated in the contract to a secure destination," and may also "function[] as an automated, secure digital escrow account."); *Williams v. Block one*, No. 20-CV-2809, 2022 WL 5294189, at *2 n.19 (S.D.N.Y. Aug. 15, 2022) (citing plaintiff's explanation that smart contracts "are programs that verify and enforce the negotiation or performance of binary contracts"); *Snyder v. STX Techs.*, Ltd., No. 19-6132, 2020 WL 5106721, at *2 (W.D. Wash. Aug. 31, 2020) (breach of contract action for violation of a smart contract term). Even if not every smart contract can be considered a contract, the record shows that Tornado Cash promoted and advertised the contracts and its abilities and published the code with the intention of people using it—hallmarks of a unilateral offer to provide services. (*See, e.g.*, A.R. Vol. 1, Dkt. 91-1, at 62–63 (discussing blog post's advertising Tornado Cash's features and services)).

In fact, Plaintiffs acknowledge that smart contracts are "like a vending machine" because "the smart contract automatically carries out a particular, predetermined task without additional human intervention." (*Id.* at 10). This reinforces the Court's point. Vending machines are examples of unilateral contracts. And like vending machines, a smart contract is a tool that carries out a

particular, predetermined task. The fact that smart contracts do so without additional human intervention, like a vending machine, or that they are immutable, does not affect its status as type of contract and, thus, a type of property within the meaning of the regulation.

provoost · 3h

Tokenomics is really biting Tornado Cash in the arse here. The judge is not making a clear distinction between the autonomous and DAO-controlled smart contracts. Arguments that make (some) sense for the latter are then applied to both.

b. Tornado Cash Has a Property Interest in the Smart Contracts

Plaintiffs further argue that Tornado Cash does not have a property interest in the smart contracts. Plaintiffs urge the Court to instead adopt the "ordinary meaning" of "interest," which would restrict the definition to a "legal or equitable claim or right in property." *Interest*, BLACK'S LAW DICTIONARY (11th ed. online 2019). But OFAC's definition of "interest" is expansive. 31 C.F.R. §§ 510.323, 578.314. The regulations define the word "interest" as "an interest of any nature whatsoever, direct or indirect." *Id.* The phrase "any interest" should be construed broadly, and it includes even interests that are not legally enforceable. *Regan*, 468 U.S. at 224, 225–26, 233–34 (recognizing that the phrase "any interest" should be construed broadly); *Holy Land Found. for Relief & Dev. v. Ashcroft*, 219 F. Supp. 2d 57, 67 (D.D.C. 2002), aff'd, 333 F.3d 156 (D.C. Cir. 2003) ("IEEPA does not limit the President's blocking authority to the existence of a legally enforceable interest."). The beneficial interest Tornado Cash derives from the smart contracts falls within this definition.

Tornado Cash has a beneficial interest in the deployed smart contracts because they provide Tornado Cash with a means to control and use crypto assets. The smart contracts generate fees in the form of TORN tokens for the DAO when users execute a relayer-facilitated transaction. Plaintiffs disagree on several grounds. First, they insist that the use of a relayer is entirely optional, but the record shows that almost eighty-four percent of Tornado Cash transactions use these relayer services. (A.R. Vol. 1, Dkt. 91-1, at 58; *id.* at 58 n.11).

Next, Plaintiffs argue that Tornado Cash may have an interest in the TORN tokens but not in the smart contracts themselves, because Tornado Cash does not have a "right or expectancy" in

1 1 1

provoost · 3h

When your tokenomics scheme gets compared to Hamas...

Rough translation of 'cascading economic causation": exit liquidity from degenerate gamblers. I find the argument that TORN token holders make money from mixing somewhat persuasive. Though it's not spelled out here. Relayers stake tokens in order to receive priority (from the frontend javascript code), which improves their ETH revenue.

> the smart contracts. (Defs.' Reply, Dkt. 17). Plaintiffs' claim that a possibility of future indirect profits is too remote because it depends on a "cascading economic causation" theory that could, theoretically, increase the value of TORN. (*Id.* at 17–18). However, the benefits to Tornado Cash are not hypothetical or remote. Tornado Cash receives a regular stream of revenue from the smart contracts in the form of TORN tokens transferred to the DAO for relayer-enabled transactions, which, as the Court noted above, encompass the vast majority of the transactions. (A.R. Vo. 1, Dkt. 91-1, at 33, 40, 57, 63). The D.C. Circuit has construed the IEEPA to encompass this kind of economic potential. In *Holy Land Foundation for Relief & Development v. Ashcroft*, the D.C. Circuit concluded that Hamas had a beneficial interest in Holy Land's property because the purported charity acted as a fundraiser for the terrorist organization—that is, because Hamas would profit in the future from the fundraising proceeds. 333 F.3d 156, 162–63 (D.C. Cir. 2003); *see also id.* (("The language ['any interest' in IEEPA] therefore imposes no limit on the scope of the interest, and OFAC has defined this statutory term, pursuant to explicit authorization from Congress, 50 U.S.C. § 1704, to mean, 'an interest of any nature whatsoever, direct or indirect.'"). *Holy Land* confirms that, within the expansive regulatory meaning, Tornado Cash has a beneficial interest based on its expectation that the smart contracts it deployed will continue to generate this revenue.

provoost · 2h

There is no 'stream of revenue" whatsoever from the immutable core Tornado Cash contracts to the DAO. Only (indirectly, by means of their owners investing in TORN tokens) from the relayers to the DAO. The judge doesn't notice this distinction, and I can't fully blame them.

Defendants also cite *Centrifugal Casting Mach. Co., Inc. v. American Bank & Trust Co.* for the proposition that interest must be a "legal or equitable claim to or right in property." 966 F.2d 1348, 1353 (10th Cir. 1992) (concluding that Iraq did not have a property interest in the proceeds of a contract). However, the Court's analysis is not inconsistent with *Centrifugal Casting*. In that case, the government argued that Iraq had a property interest in the money plaintiff received under a letter of credit "because it was allegedly a contract payment made by Iraq" and plaintiff had allegedly breached the contract. *Id.* However, as the Tenth Circuit noted, Iraq was an account party to the letter of credit, and it had not even made an actual breach of contract claim against plaintiff. *Id.* The

20

Case 1:23-cv-00312-RP Document 94 Filed 08/17/23 Page 21 of 25

government was essentially claiming breach on their behalf, but such an interest was not only too remote but antithetical to the nature of a letter of credit, in light of Iraq's status as an account party. *Id.* Here, in contrast, the stream of revenue Tornado Cash received, which was directly claimed by the Tornado Cash DAO, is a much more direct interest. Furthermore, while Iraq could have only claimed an interest by ignoring the basic structure of the financing device, Tornado Cash designed the compensation structure to generate this revenue for the DAO.

1

provoost · 2h

The weather probably wasn't the best analogy, but the judge misses the point here imo. Again perhaps because it was near impossible to explain with all the tokenomics noise.

The weather in this analogy is the immutable core smart contract, not the 'the crypto-economy'. It may have an "property interest in smart contracts" but not in that particular one. Which happens to be the one that causes the most egregious violation of property rights for all American users (who could otherwise retrieve their coins with some manual commands not involving anything controlled by the DAO).

> Plaintiffs' other proffered analogies are similarly unpersuasive. For example, Plaintiffs argue that the Tornado Cash DAO is like a power company, which may "profit from hot summer weather that causes increased use of air conditioning," but which could not claim to have a property interest in the weather. (Pls.' Mot., Dkt. 41, at 25–26). This analogy is misleading. Such a company may not have a property interest in the weather, but it would undoubtedly own interests in the physical infrastructure and equipment, and even more abstract rights, such as transmission rights, that allow it to produce and transmit energy. Likewise, Tornado Cash may not own the crypto-economy, but, within the meaning of the statute, it has a property interest in smart contracts, which are simultaneously contracts and tools that allow it to provide privacy to its users.

Show less

1

provoost · 2h

Imo by far the biggest problem here is the sanctioning of the core contract.

1

provoost · 2h

The free speech part of the ruling suggests to me that they could have made a good case, but just didn't.

In the appeal, maybe try explaining how it is impossible to build an alternative system that would not inevitably get sanctioned. But then perhaps the judge will say: if you can't use a decentralized system to pay someone, that's tough luck, use a centralized shitcoin like USD.

Plaintiffs argue that the government is prohibiting some of them from engaging in socially valuable speech because they, if not for the designation, they would use the Tornado Cash software to make donations to important political and social causes. (Pls.' Mot., Dkt. 41, at 28–29). Indeed, the First Amendment protects the right of individuals to donate money to social causes of their choosing. *See, e.g.*, *McCutcheon v. Fed. Election Comm'n*, 572 U.S. 185, 191 (2014) ("The right to participate in democracy through political contributions is protected by the First Amendment, but that right is not absolute."); *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958). However, it does not protect the right to do so through any particular bank or service of their choosing, and Plaintiffs do not cite any case to the contrary.

In fact, Plaintiffs' evidence does not sufficiently support their arguments. Plaintiffs claim that "[w]ithout the privacy afforded by Tornado Cash, users such as [Plaintiff] Almeida are hindered in expressing their views" of the Ukranian conflict. (Pls.' Mot., Dkt. 41, at 29 (*citing See Citizens United v. Federal Election Commission*, 558 U.S. 310, 351 (2010)). But Mr. Almeida's affidavit does not describe such a hindrance, nor does it state that he has stopped donating to his preferred causes, that he would be unable to donate through other services, or that his speech has otherwise been chilled. Furthermore, Plaintiffs do not explain how the designation prevents them from using other services that may allow them privacy for their transactions.

22

provoost · 2h

"You didn't do your homework, therefore government wins" (and anyone with coins trapped remains, as they have been for the past year, royally screwed.

C. Takings Claims

Plaintiffs Almeida, Van Loon, and Welch also allege that they are unable to access Ether that belongs to them because it is trapped in a Tornado Cash smart-contract pool. Accordingly, they raise Fifth Amendment Takings claims, claiming that they did not receive any process prior to the deprivation. (Compl., Dkt. 21, at 26). However, Plaintiffs did not move for summary judgment on this ground. (Pls.' Mot. Summ. J., Dkt. 41, at 8, 30). The government moved for summary judgment on all counts. (Defs.' Mot. Summ. J., Dkt. 80, at 25–26, 52).

"The Fifth Circuit has found when a plaintiff fails to pursue a claim or defense beyond the party's initial complaint, the claim is deemed abandoned." *Weaver v. Basic Energy Servs., L.P.*, No. MO-13-CV-022, 2014 WL 12513180, at *2 (W.D. Tex. Jan. 8, 2014), *aff'd*, 578 F. App'x 449 (5th Cir. 2014); *Black v. Panola Sch. Dist.*, 461 F.3d 584, 588 n.1 (5th Cir. 2006) (plaintiff abandoned retaliatory abandonment claim when she failed to defend claim in response to motion to dismiss). The parties agreed to resolve the claims through the administrative record and cross-motions to dismiss. (Joint Mot. Entry Sched. Order, Dkt. 23). However, Plaintiffs did not pursue their Fifth Amendment claim, even after the government raised the issue of waiver in its cross motion. (Defs.' Mot. Summ. J., Dkt. 80, at 25–26). Because Plaintiffs failed to pursue their Fifth Amendment claim, they have waived it. Accordingly, the Court will grant the government's motion for summary judgment as to this claim.

1

provoost · 2h

Now back to the indictment...

(I might get some sleep first though)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA v. ROMAN STORM and ROMAN SEMENOV, Defendants.	**SEALED INDICTMENT** 23 Cr. 23 CRIM 430

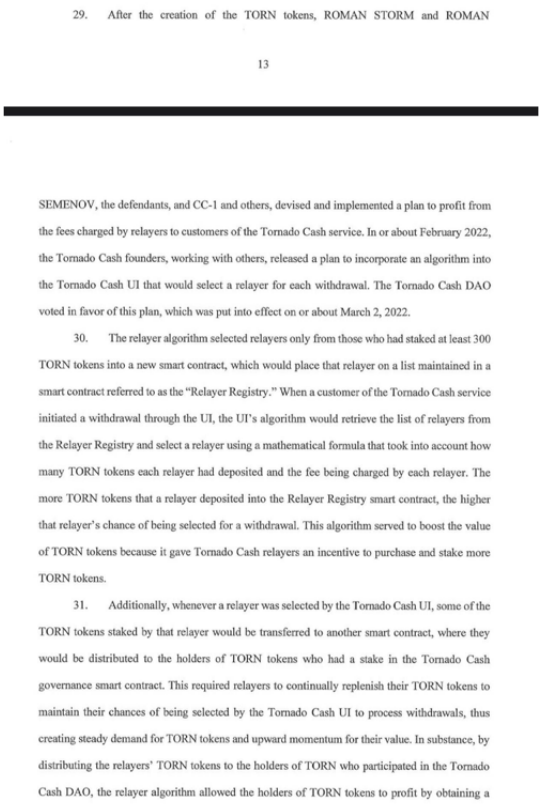
OVERVIEW

1. From at least in or about 2019, up to and including at least on or about August 8, 2022, ROMAN STORM and ROMAN SEMENOV, the defendants, developed, marketed, and operated a cryptocurrency mixing service known as Tornado Cash, a business from which they sought to make, and did make, substantial profits. The Tornado Cash service combined multiple unique features to execute anonymous financial transactions in various cryptocurrencies for its customers. Claiming to offer the Tornado Cash service as a "privacy" service, the defendants in fact knew that it was a haven for criminals to engage in large-scale money laundering and sanctions evasion. Indeed, as the defendants well knew, a substantial portion of the funds the Tornado Cash service processed were criminal proceeds passed through the Tornado Cash service for purposes of concealment. The defendants also knew that the Tornado Cash service received funds from, and provided services to, the Lazarus Group, a U.S.-sanctioned North Korean cybercrime organization,

1

provoost · 1h

At least up to point 31 it provides a solid explanation of the whole system, which matches my understanding of it. Worth reading.



29. After the creation of the TORN tokens, ROMAN STORM and ROMAN

13

SEMENOV, the defendants, and CC-1 and others, devised and implemented a plan to profit from the fees charged by relayers to customers of the Tornado Cash service. In or about February 2022, the Tornado Cash founders, working with others, released a plan to incorporate an algorithm into the Tornado Cash UI that would select a relayer for each withdrawal. The Tornado Cash DAO voted in favor of this plan, which was put into effect on or about March 2, 2022.

30. The relayer algorithm selected relayers only from those who had staked at least 300 TORN tokens into a new smart contract, which would place that relayer on a list maintained in a smart contract referred to as the "Relayer Registry." When a customer of the Tornado Cash service initiated a withdrawal through the UI, the UI's algorithm would retrieve the list of relayers from the Relayer Registry and select a relayer using a mathematical formula that took into account how many TORN tokens each relayer had deposited and the fee being charged by each relayer. The more TORN tokens that a relayer deposited into the Relayer Registry smart contract, the higher that relayer's chance of being selected for a withdrawal. This algorithm served to boost the value of TORN tokens because it gave Tornado Cash relayers an incentive to purchase and stake more TORN tokens.

31. Additionally, whenever a relayer was selected by the Tornado Cash UI, some of the TORN tokens staked by that relayer would be transferred to another smart contract, where they would be distributed to the holders of TORN tokens who had a stake in the Tornado Cash governance smart contract. This required relayers to continually replenish their TORN tokens to maintain their chances of being selected by the Tornado Cash UI to process withdrawals, thus creating steady demand for TORN tokens and upward momentum for their value. In substance, by distributing the relayers' TORN tokens to the holders of TORN who participated in the Tornado Cash DAO, the relayer algorithm allowed the holders of TORN tokens to profit by obtaining a

1

provoost · 1h

Or you can listen to aaronvanw and me explain it last year: podcast.sprovoost.nl/@nado/episodes/bitcoin-explained-69-the-tornado-cash-trial

1

provoost · 1h

I physically visited the first couple of hearings in The Netherlands. But the Dutch prosecutor is less transparent than the Americans. All we had until today were (fairly high level) oral arguments made in court.

I assume they've collaborated in making the case (or even copy pasted stuff). But it's also possible they're both making completely different arguments.

And the biggest question: will Pertsev (CC-1) get the 'best' deal of all with just a few years in Dutch prison (if he's convicted at all), or the worst - by doing that and then, only after being release, suddenly getting extradited at the request of an extra vindictive US prosecutor?

But anyway, continuing to read... what's the charge?

Show less

1

provoost · 1h

They're facing up to 45 years in the US, I'd be shocked if it's more than 5 over here. I think the max is 8: www.om.nl/onderwerpen/beleidsregels/richtlijnen-voor-strafvordering-resultaten/richtlijn-voor-strafvordering-witwassen-2021r004

1

provoost · 1h

The plot thickens, but it seems to hone in on the centralized parts of the system - as opposed to the core contract.

34. Throughout the time period charged in this Indictment, the Tornado Cash service failed to establish an effective AML program or to engage in any KYC efforts. Customers of the

15

Tornado Cash service could access the Tornado Cash UI to make deposits to and withdrawals from the Tornado Cash service without providing any identifying information aside from an address on the Ethereum blockchain. As discussed below, this failure to implement AML/KYC facilitated the ability of customers of the Tornado Cash service to transfer criminal proceeds between addresses on the Ethereum blockchain without being traced, and to engage in transactions meant to conceal the nature, location, source, ownership, and control of criminal proceeds.

1

provoost · 1h

They're going for the "profit from tokenomics" angle it seems... Remember that's very indirect: relay operators buy tokens in order to get priority from UI users (this can be bypassed with some technical skill, certainly by the North Koreans), which drives up the price. More realistically, and what probably ACTUALLY happened, is that degens pushed up the price. So the profits came from gambling, not laundering. But maybe that's why they're only charged with conspiracy.

Reading on...

41. For instance, on or about October 4, 2021, ROMAN STORM, the defendant,

18

participated in a video recorded interview in which he misleadingly stated that the Tornado Cash service was "not for profit. It's not a commercial project." In fact, as STORM well knew, he and the other Tornado Cash founders had developed the Tornado Cash service as a business, had pitched it to investors as an opportunity to make profits, and were in fact operating the Tornado Cash service with the intention of making profits from increasing the value of their TORN tokens.

Show less

1

provoost · 1h

Yes they could have. And then someone would clone the UI code and remove the KYC stuff. So it's a non-starter. It's misleading of both the Dutch and US prosecutor to pretend otherwise.

42. On or about March 20, 2022, ROMAN SEMENOV, the defendant, issued a public Tweet in which he misleadingly stated, in part, that "my opinion cannot affect [the Tornado Cash service] even if I really wanted to change something." In fact, as SEMENOV well knew, he and the other Tornado Cash founders had control over multiple features of the Tornado Cash service, including the Tornado Cash UI. SEMENOV and the other Tornado Cash founders had the ability to implement a KYC process, an AML program, and other compliance features into the Tornado Cash UI, but had chosen not to do so.

1

provoost · 1h

What is it with people and self-incriminating (appearing) text messages ffs.

THE FBI CAN READ ANYTHING YOU EVER ENTERED ON ANY FUCKING KEYBOARD - or least you should live accordingly. Like how a gun is always loaded even if you just checked and saw it wasn't loaded

44. Nonetheless, ROMAN STORM, the defendant, ROMAN SEMENOV, the defendant, and CC-1 continued to exercise control over the Tornado Cash UI and to pay to

19

maintain critical infrastructure for the Tornado Cash service, and took no steps to block or even monitor deposits or withdrawals, or to collect any identifying information from customers of the Tornado Cash service. On or about May 5, 2022, CC-1 sent a message to STORM and SEMENOV through the Encrypted App, asking "I just wondered from a legal point of view, is everything ok here? Maybe it's a dead giveaway if we pay for tornado from the peppersec account."

1

provoost · 1h

Anyway, very hand-wavy argument from the prosecutor.

Ya'll better crowdfund them good lawyers. Because the same reasoning can be used against, say, a non-custodial phone wallet that doesn't have KYC.

1

provoost · 1h

Because the attorney in question was a moron. Tornado Cash is non-custodial and does not have possession. And there was nothing they could do.

48. In or about December 2021, another cryptocurrency exchange ("Cryptocurrency Exchange-2"), publicly announced that it had suffered a security breach caused by a stolen private key, resulting in the theft of approximately $200 million worth of cryptocurrency. Millions of dollars in proceeds from this security breach were deposited into the Tornado Cash service. On or about December 14, 2021, an attorney for Cryptocurrency Exchange-2 sent a letter to the Tornado Cash founders, stating, in sum and substance, that Cryptocurrency Exchange-2 had traced the proceeds of the security breach to the Tornado Cash service, and informing the Tornado Cash founders that "it appears that Tornado Cash is in possession of stolen Assets." ROMAN SEMENOV, the defendant, responded to the attorney, declining to offer any assistance.

1

provoost · 54m

Or they're really playing the same dirty trick as the Dutch prosecutor. First they pretend adding KYC to the UI would have been effective. Full well knowing that's false. Then, when it suits them, they suddenly argue it would NOT be effective.

The paper over this glaring contradiction with the red underlined nonsense. None of those things would have stopped the transactions. The developers understood this, so they didn't act. The prosecutor understands this too but hopes the jury doesn't. Or in the case of the Dutch system - where judges are way less educated on the topic and there's isn't a single attorney who can teach them - the judge doesn't.

61. ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 were aware that OFAC had designated the 0x098B716 Address as blocked property of the Lazarus Group. On or about April 14, 2022, STORM sent SEMENOV and CC-1 a message through the Encrypted App with a link to a news article about the FBI's attribution of the Ronin Network hack to the Lazarus Group. In the message, STORM wrote: "guys we are fucked."

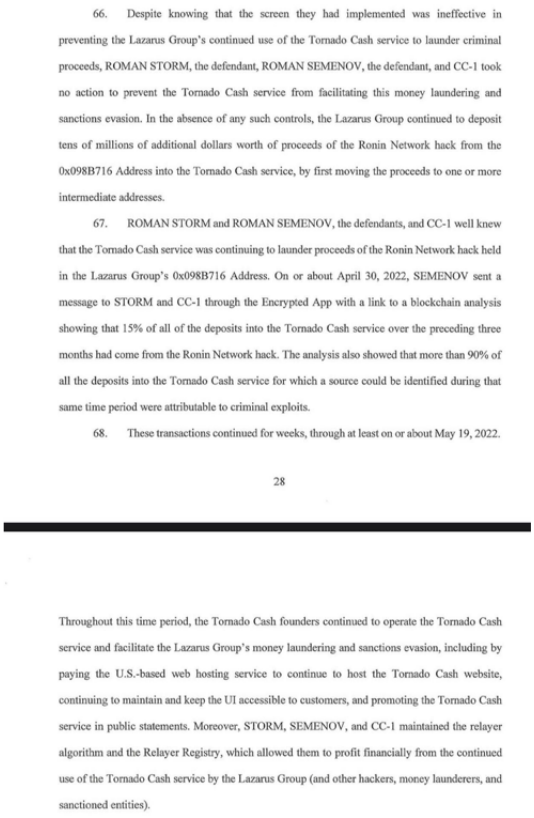
62. Following this message, ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 discussed a plan to change the Tornado Cash UI to block deposits directly from OFAC-designated addresses, so they could make a public announcement claiming that the Tornado Cash service was compliant with United States sanctions. However, as STORM, SEMENOV, and CC-1 well knew, this change to the UI was ineffective and could be easily evaded in the absence of any KYC procedures, transaction monitoring, or blockchain tracing. To evade the screen, a customer of the Tornado Cash service who was using an OFAC-designated address could simply transfer the funds to a new Ethereum address and then deposit the funds into the Tornado Cash service, using the UI. The purpose of the change was to mislead the public into believing that the Tornado Cash service complied with the law, while continuing to allow and profit from transactions in funds originating in the OFAC-designated 0x098B716 Address.

Show less

1 1

provoost · 44m

They keep playing this game fpr a while. But notice what's absent: there's no allegation, let alone evidence, that the North Koreans used the UI. In fact they had no reason to. It would save money for their great leader to just do it themselves. And if the UI ran on CloudFlare it wouldn't even work in NK.



66. Despite knowing that the screen they had implemented was ineffective in preventing the Lazarus Group's continued use of the Tornado Cash service to launder criminal proceeds, ROMAN STORM, the defendant, ROMAN SEMENOV, the defendant, and CC-1 took no action to prevent the Tornado Cash service from facilitating this money laundering and sanctions evasion. In the absence of any such controls, the Lazarus Group continued to deposit tens of millions of additional dollars worth of proceeds of the Ronin Network hack from the 0x098B716 Address into the Tornado Cash service, by first moving the proceeds to one or more intermediate addresses.

67. ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 well knew that the Tornado Cash service was continuing to launder proceeds of the Ronin Network hack held in the Lazarus Group's 0x098B716 Address. On or about April 30, 2022, SEMENOV sent a message to STORM and CC-1 through the Encrypted App with a link to a blockchain analysis showing that 15% of all of the deposits into the Tornado Cash service over the preceding three months had come from the Ronin Network hack. The analysis also showed that more than 90% of all the deposits into the Tornado Cash service for which a source could be identified during that same time period were attributable to criminal exploits.

68. These transactions continued for weeks, through at least on or about May 19, 2022.

28

Throughout this time period, the Tornado Cash founders continued to operate the Tornado Cash service and facilitate the Lazarus Group's money laundering and sanctions evasion, including by paying the U.S.-based web hosting service to continue to host the Tornado Cash website, continuing to maintain and keep the UI accessible to customers, and promoting the Tornado Cash service in public statements. Moreover, STORM, SEMENOV, and CC-1 maintained the relayer algorithm and the Relayer Registry, which allowed them to profit financially from the continued use of the Tornado Cash service by the Lazarus Group (and other hackers, money launderers, and sanctioned entities).

1

provoost · 43m

This last bit is highly relevant in the Dutch case since they're accused of laundering 'billions' and without the Lazarus funds that would drop to way less.

1

provoost · 40m

The SEC might have an opinion about that...

70. On or about December 1, 2021, shortly before one-third of the Tornado Cash founders' TORN tokens were set to unlock, ROMAN SEMENOV, the defendant, sent a text message to ROMAN STORM, the defendant, and CC-1 through the Encrypted App, saying, in part, that "it is important to pump Torn." In the same text message, SEMENOV discussed having an "auction" at which the Tornado Cash founders could "collect information … as to how much and at what price the folks are willing to pay."

1

provoost · 37m

It seems like they're undermining their case here. Clearly the money is coming from investors, not money launderers. This should have been a securities case.

72. Over the following months, ROMAN STORM, ROMAN SEMENOV, the defendants, and CC-1, continued to focus on increasing the profitability of the Tornado Cash service to increase the value of their holdings of TORN tokens and to appeal to potential investors in the Tornado Cash service. On or about June 16, 2022, STORM sent a message to SEMENOV and CC-1 through the Encrypted App in which he wrote "need help to push tornado to make some money / need to sell a sweet fantasy to investors."

73. At various times in 2022, ROMAN STORM, the defendant, sold TORN tokens that had been distributed to him and to ROMAN SEMENOV, the defendant, and CC-1. In an effort to

1

provoost · 30m

Ok, that was quite possibly the worst move ever. Assuming it was unilateral move by Storm, now the other two co-founders are sitting on coins (fiat?) received after the sanctions were into effect. Which comes with onerous reporting requirements, $1000+ / hour lawyers and countless ways for an eager prosecutor to (selectively) make your life hell.

It's the kind of thing you do *after* you've all moved to a non-extradition tropical island of choice. Not when two of you are sitting ducks. (Not legal advice)

75. After the sanctions on the Tornado Cash service were announced, ROMAN STORM, the defendant, again accessed the Binance account, where he was holding at least approximately $8 million worth of cryptocurrency that represented the proceeds of sales of TORN tokens. On or about August 8 and 9, 2022, STORM transferred approximately $7.8 million worth of U.S.-dollar pegged stablecoins from the Binance account to three separate cryptocurrency wallet addresses in payments of approximately $2.6 million each. Each of these three wallets was owned by one of the Tornado Cash founders. On or about August 9, 2022, STORM sent messages through the Encrypted App to ROMAN SEMENOV, the defendant, and CC-1, saying "I offloaded 8,000,000 yesterday / I sent you guys 2.6 each." He then sent further messages advising SEMENOV and CC-1, in substance, to conduct further transactions to make it more difficult to trace these funds, saying "my personal advice: create new wallets, new seed phrases, transfer money to new addresses."

Show less

1

provoost · 25m

But also irrelevant to the Dutch case; these are US sanctions. Though perhaps there's an indirect case for laundering the proceeds of a crime (violating sanctions law of a befriended country). In any case this is the first time I hear about it. Pretty sure the Dutch prosecutor would have brought this up in the courtroom full of journalists if she knew about it at the time.

1

provoost · 22m

Didn't fincen write in like 2014 that non-custodial services don't need this license? Or was it more ambiguous?

COUNT TWO
(Conspiracy to Operate an Unlicensed Money Transmitting Business)

The Grand Jury further charges:

79. The allegations contained in paragraphs 1 through 75 of this Indictment are repeated and realleged as if fully set forth herein.

80. From at least in or about March 2022, up to and including on or about August 8, 2022, in the Southern District of New York and elsewhere, ROMAN STORM, the defendant,

32

ROMAN SEMENOV, the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit an offense against the United States, to wit, operation of an unlicensed money transmitting business, in violation of Title 18, United States Code, Sections 1960(b)(1)(B) and (b)(1)(C).