Social Slashing
An introduction

Eric Wall
Unaffiliated
The signaling methodology is widely misinterpreted to mean the hash power is voting on a proposal and it seems difficult to correct this misunderstanding in the wider community...

...soft forks rules are actually always enforced by the nodes, not the miners.
...the signaling methodology is widely misinterpreted to mean the hash power is voting on a proposal and it seems difficult to correct this misunderstanding in the wider community...

...soft forks rules are actually always enforced by the nodes, not the miners.“
THE PEOPLE DON'T KNOW THEIR TRUE POWER.
WHO WOULD WIN?

COINBASE, BLOCKCHAIN.INFO, CIRCLE, SHAPESHIFT, BTC.COM, BITCOIN.COM, BITMAIN, BITFURY, BITPAY, DIGITAL CURRENCY GROUP, ABRA, PURSE, XAPO, 80%+ OF THE NETWORK HASHRATE, AND EVERYONE ELSE WHO SIGNED THE NY AGREEMENT

A SINGLE PSEUDONYMOUS DEVELOPER NAMED SHAOLINFRY
Event: The DAO hack (Jun 2016)

At risk: Immutability

Event: The Shanghai DDoS (Sep 2016)

At risk: Availability

Event: OFAC OFUK (Aug 2022)

At risk: Neutrality
feat: address screening #1017

Merged

defispartan merged 25 commits into main from feat/trm-compliance on Aug 12

Conversation 17

Commit 25

Checks 32

Files changed 10

grothem commented on Aug 11

Prevents wallets that are sanctioned or have known links to terrorist financing from using the interface. Leverages the TRM wallet screening functionality to screen the connected account.
H.E. Justin Sun
@justinsuntron

I’m officially blocked by @AaveAave since someone sent 0.1 eth randomly from @TornadoCash to me. @StaniKulechov

3:48 PM · Aug 13, 2022 · Twitter Web App
2,116 Retweets 609 Quote Tweets 8,324 Likes

sassal.eth
@sassalOx

sassal.eth now blocked from using the official Aave front-end because someone sent 0.1 ETH to my address via Tornado Cash 😞

11:04 AM · Aug 13, 2022 · Twitter Web App
flashbots censorship confirmed

@Micah Are you able to confirm whether or not the Flashbots operated relay will be censoring post Merge?

Hasu Today at 6:48 PM
Flashbots Relay and Builder are OFAC compliant today and will be OFAC compliant in the future

10:30 PM · Aug 17, 2022 · Twitter Web App
128 Retweets 47 Quote Tweets 809 Likes
Sanctioning a technology (as opposed to an individual or entity) seems like a bad precedent to me, and it should probably be challenged. Could have many downstream unintended consequences.

#TornadoCash

Hopefully obvious point: we will always follow the law.

3:49 AM · Aug 15, 2022 · Twitter for iPhone

274 Retweets 72 Quote Tweets 2,102 Likes
BAD PATH:
- POW
- CENSORSHIP
- CENTRALIZATION
- HIGH ENERGY USE

GOOD PATH:
- POS
- COORDINATION
- NON-FINANCIAL USE CASES
- CENSORSHIP RESISTANCE
- NEUTRALITY
- DECENTRALIZATION
In the PoS case, however, things are much brighter. For certain kinds of 51% attacks (particularly, reverting finalized blocks), there is a built-in "slashing" mechanism in the proof of stake consensus by which a large portion of the attacker's stake (and no one else's stake) can get automatically destroyed. For other, harder-to-detect attacks (notably, a 51% coalition censoring everyone else), the community can coordinate on a minority user-activated soft fork (UASF) in which the attacker's funds are once again largely destroyed (in Ethereum, this is done via the "inactivity leak mechanism"). No explicit "hard fork to delete coins" is required; with the exception of the requirement to coordinate on the UASF to select a minority block, everything else is automated and simply following the execution of the protocol rules.
For other, harder-to-detect attacks (notably, a 51% coalition censoring everyone else), the community can coordinate on a minority user-activated soft fork (UASF) in which the attacker's funds are once again largely destroyed.
In BTC, Changing PoW algorithm to break all ASICs is the nuclear option and it can only be used once. If adversary has GPUs, game over.

In ETH, the adversary can be removed without harming any honest party. It is the high precision laser option and it kills instantly.
Post-Merge OFAC Compliant Blocks

⚠️ 50% enforced OFAC compliance
Validator

- Filters transactions
- "I'm going to exclude certain transactions from the blocks I build"
- Refuses blocks
- "I'm going to refuse to build on other validators' blocks if they include those transactions"

- 99.9% = non-compliant txs still get in!
- 20-50% = system-wide censorship!
Actually @laurashin, I think the law is pretty clear: nothing compels miners, stakers or anybody else at the base lawyer to monitor or censor transactions.

Laura Shin 😊 @laurashin · Sep 4
Replying to @betterlawMLA @coinbase and 2 others
Right … but it's not clear what the law requires …
Eric Wall X | @ercwl · Aug 16

Question for the Ethereum community. If a majority of stake chooses A in this poll, will you:

X) Consider the censorship an attack on Ethereum and burn their stake via social consensus
Y) Tolerate the censorship

Lefteris Karapetsas | Hiring for @rotkiapp @LefterisJP · Aug 15

Question for @LidoFinance, @coinbase, @krakenfx, @stakedus, @BitcoinSuisseAG

If regulators ask you to censor at the #ethereum protocol level with your validators will you:

A) Comply and censor at protocol level
B) Shut down the staking service and preserve network integrity
twitter.com/TheEylon/statu...

Poll

- X: 61.2%
- Y: 9.3%
- Show results: 29.5%

9,584 votes · Final results
Poll

X 61.2%
Y 9.3%
Show results 29.5%

9,584 votes • Final results

Eric Wall X @ercwl • Aug 16

RYAN SEAN ADAMS • rsa.eth @RyanSAdams

Replying to @ercwl

X

2:25 AM • Aug 16, 2022 • Twitter Web App

14 Retweets 2 Quote Tweets 70 Likes
...the signaling methodology is widely misinterpreted to mean the hash power is voting on a proposal and it seems difficult to correct this misunderstanding in the wider community...

...soft forks rules are actually always enforced by the nodes, not the miners."
What is the role of SWIFT in relation to financial sanctions that are imposed by regulators?

SWIFT does not monitor or control the messages that users send through its system. All decisions on the legitimacy of financial transactions under applicable regulations, such as sanctions regulations, rest with the financial institutions handling them, and their competent international and national authorities. As far as financial sanctions are concerned, the focus of SWIFT is to help its users in meeting their responsibilities to comply with national and international regulations.
THESE ETHEREUM POW MINERS... ARE THEY IN THE ROOM WITH US RIGHT NOW?
Thank you!

Eric Wall
Unaffiliated
info@ericwall.ninja
@ercwl