

THE CONSEQUENCES OF CONSEQUENTIALISM

How the trolley-switchers derailed
decentralization

Edwin den Boer, Monero Konferenco, Lisbon, 18 June 2022



**We're going to discuss the
trolley problem...**

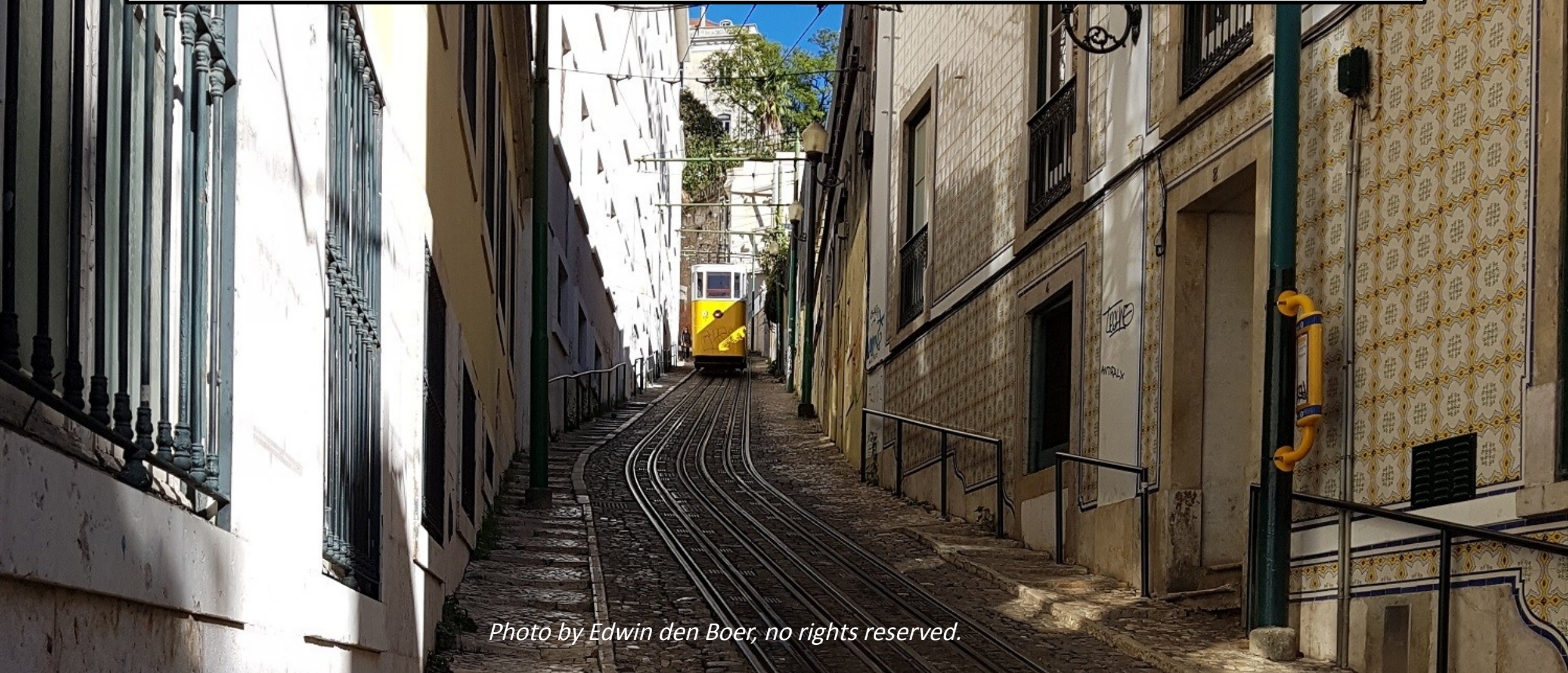


Photo by Edwin den Boer, no rights reserved.

But first... why FIAT?

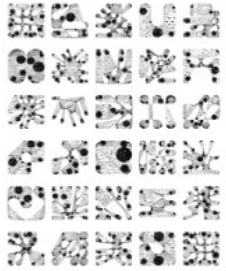


- Monero = fiat money, not digital gold.
- It's not a Ferrari...
- “Fiat iustitia, pereat mundus” is the inspiring motto of the philosophy I’m talking about today: “Let justice be done, even if it destroys the world”.
- Not endorsed by Fiat Automobiles S.p.A

Going against my nature

apertamono

Collected



Dead Ringers: Edit...
Dead Ringers: Edition

Last \uparrow 0.0189

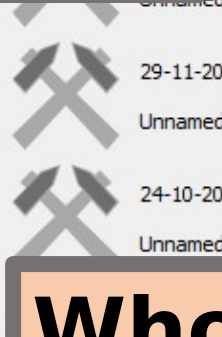


Circle Drop
Circle Drop 0183

Price
 \uparrow 1
Last \uparrow 0.01



Circle Drop
Circle Drop 0464



2020 11:34

+75.335169 HBN

Unnamed

29-11-2020 06:24

+120.949476 HBN

Unnamed

24-10-2020 13:21

+151.039025 HBN

Unnamed



Export



Debug window



HoboNickels-Qt (OSS GUI client for Hobo



HoboNickels - Information

Date: 29-11-2020 11:34

Amount: +75.335169 HBN

Type: PoS Mined

Address: Unnamed

11:34



HoboNickels - Information

Date: 29-11-2020 06:24



GayCoin - Wallet

File Settings Help



Overview



Send



Receive

Gaycoin Wallet

Balance:

690000.00 GAY

Who you'd expect to tell you we are morally superior:

- A maximalist

Who you're getting:

- A shitcoiner
- An altcoin historian



Core question:

In the short history of cryptocurrencies, why were so many key decisions made which were clearly contrary to the spirit of decentralization?

Not just for convenience or accidentally, but thoroughly debated moral dilemmas.

And I'm not talking about natural centralization here either (like the dominance of one or two mining/staking pools). Straightforward scams are out of scope too.



Contents: first philosophy, then its consequences

1. Explicit consequentialists
2. Three moral frameworks
3. The Monero mentality
4. Ethereum's irregular state change
5. Consequences for crypto in general
6. A happy conclusion for Monero



Thanks to Zooko

“To me, it is never the right thing to enact a policy based on good intentions, sentiment, or ideology unless you can determine that the *consequences* would be good. I feel like what the Monero devs and community are doing is that: going with good intentions, sentiment, and ideology.” (Zooko Wilcox, Zcash forum, April 2018)



Edwin den Boer @edbwt · Apr 20, 2018

On the #Zcash forum, @zooko reveals his core character fault, which explains why such a goody-two-shoes is able to make such unethical decisions: he's a consequentialist.

about ideology versus science really stuck with me, because it kind of “hit home” about me. I’m definitely, at heart, a scientist, engineer, and hacker, not a CEO, community leader, or politician. I want to learn the latter skills as fast as possible in the service of this mission. :-))

the question of changing the PoW algorithm is a science question.

There is no objectively right answer—or at least an objectively *better* answer—but we just don’t know. Hopefully—we’ll be able to learn what it is by experiment, observation (including observation of Bitcoin, Ethereum, Monero, and Siacoin), and analysis.

It is never the right thing to enact a policy based on good intentions, sentiment, or ideology unless you can determine that the *consequences* would be good. I feel like what the Monero devs+community are doing is that: going with good intentions, sentiment, and ideology. I’m glad they do things their way, but it means we can do things a different way and collectively humanity will explore more alternatives.



1



3



6



Edwin den Boer @edbwt · Apr 20, 2018

This means:

1. He can justify anything if he thinks it's for the greater good (transparent addresses, tracing criminals, dev tax, trusted setup).
2. But he needs to be able to predict the future to make any decision.



2



1



Explicit consequentialist: Sam Bankman-Fried

- Inspired by his mother Barbara Fried, a consequentialist philosopher, and the Effective Altruism movement.
- Decided to become a billionaire, so he could do the most possible good by giving away his money.
- Founded the trading firm Alameda Research and the crypto exchange FTX.
- Supports the Serum DEX and the Solana ecosystem.

Do these dorks look like evil geniuses?



Photos: Zooko Wilcox (cropped), Steve Jennings/Getty Images for TechCrunch (cropped), FTX.

Three moral frameworks

Focused on character:

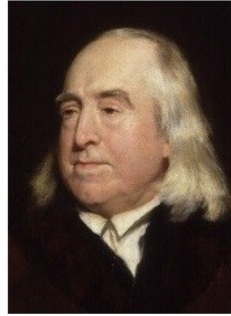
- Virtue ethics

Focused on choices:

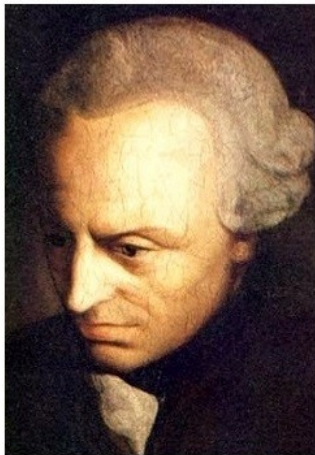
- Deontology: Is the action moral according to general rules?
- Consequentialism: Are the consequences good or bad?



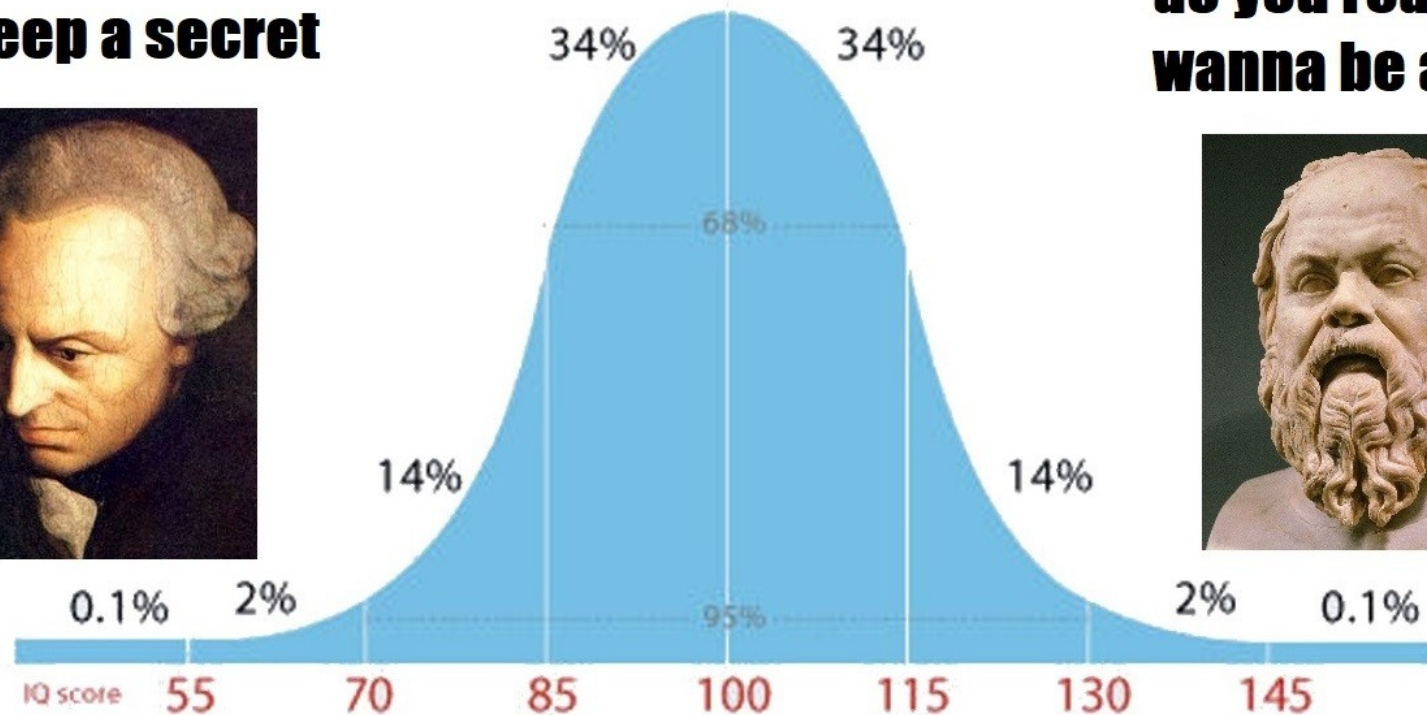
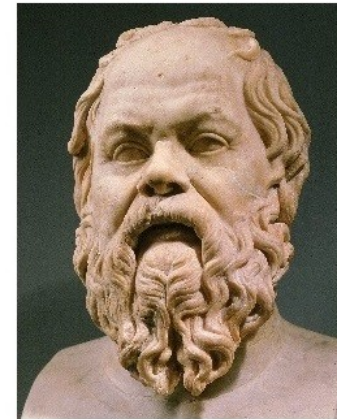
**if telling a secret
makes more people happy
you gotta do it**



**you have a duty
to keep a secret**



**do you really
wanna be a snitch**



Virtue ethics

Virtue ethics has a larger bandwidth than rational debate because it's subjective and subconscious.

On the other hand, that makes it unreliable. Obvious scammers still have thousands of followers.

And the whole point of crypto is to avoid relying on people.



NOT SATOSHI

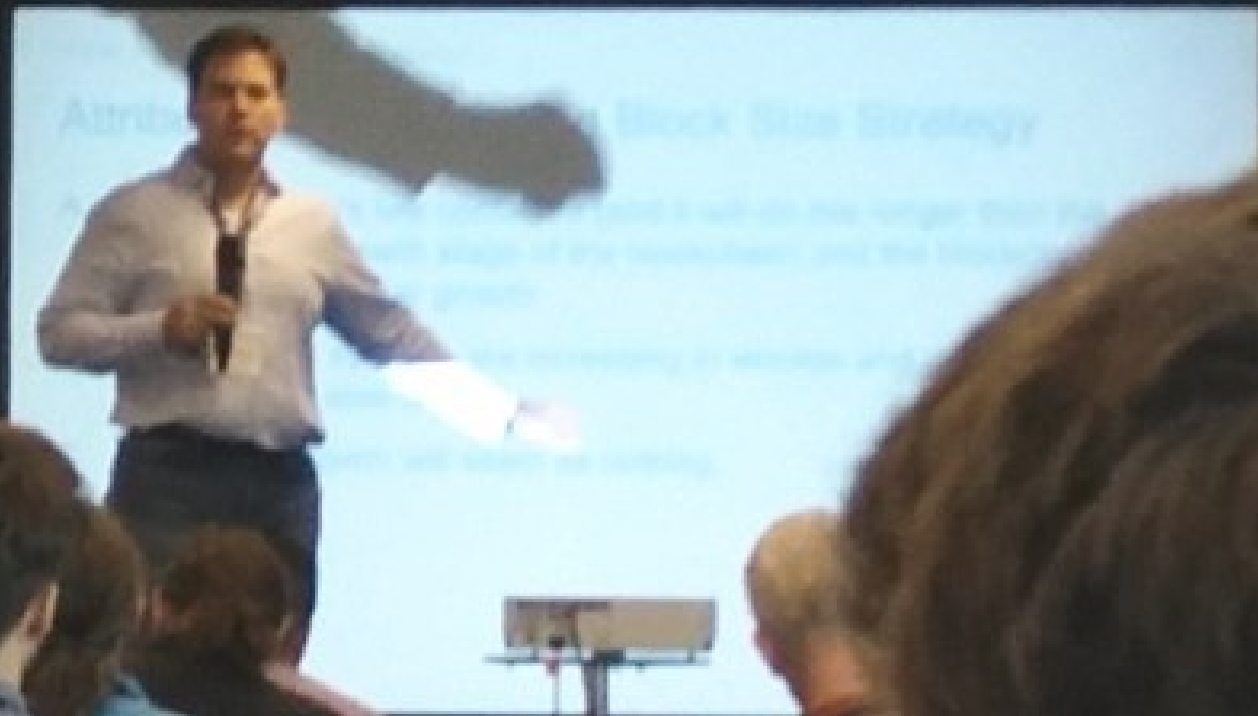


Photo by Edwin den Boer, no rights reserved.

Good or bad for whom?

Some types of consequentialism:

- for the greatest number of people: **utilitarianism**
- for myself: **egoism**
- for others: **altruism**

Focusing on utilitarianism, but it could be an excuse for egoism.



What makes consequentialism so attractive?

- It's rational – you can even calculate what's the best option, weighing life years lost or gained.
- It doesn't seem to require any shared norms (but it does require shared values).
- It promises a way to create a better world.



The trolley problem

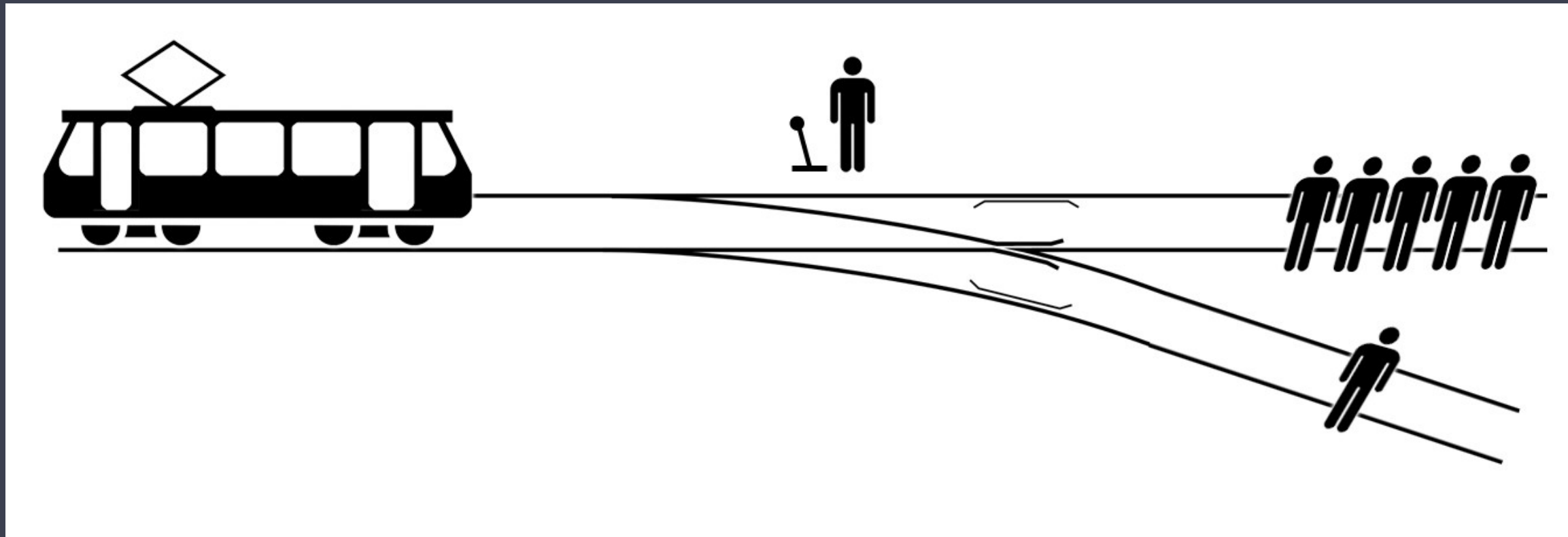
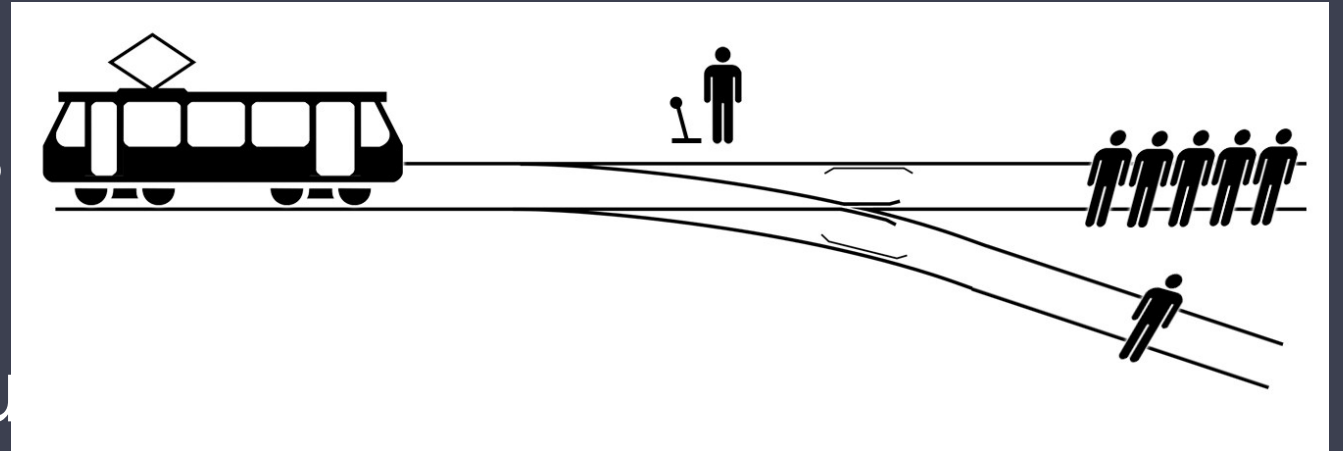


Image source: Wikipedia users McGeddon

One problem with the trolley problem

Hello, there's something tying people to the train tracks!

Why is it such an absurd scenario? Because a realistic scenario would involve uncertainty.



Duty and freedom

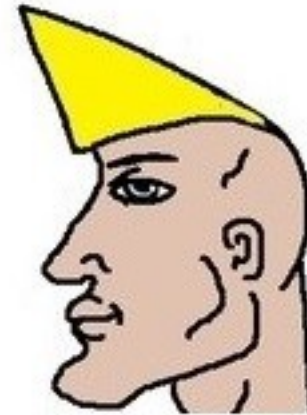
Q. The word *deontology* is derived from *deon*, the Greek word for *duty*. How does that rhyme with a freedom-focused project like Monero?

A. It's a self-imposed duty. And we're not responsible for making the world a better place. We just do the right thing: we create private, secure and fungible money.



Deontologist Moneristo answers objections (1)

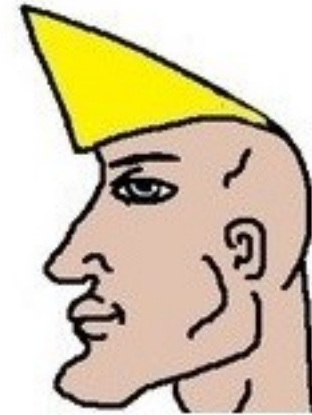
- “But if you make payments private for everyone, criminals could use them!”
- “But if addresses can't be traced, some exchanges won't list XMR.”
- “But it’s not a stablecoin, the dollar value is volatile.”



Yes.

Deontologist Moneristo answers objections (2)

- “But if there's no premine, devs will have to beg for money.”
- “But if your money’s not in a bank account, tax authorities can’t automatically check your wealth and income.”
- “But you’re using energy for an economic purpose!”



Yes.

Ethereum's irregular state change

Background: The DAO was already doomed to fail before it was 'hacked': an investment fund without a plan, besides funding the company Slock.it who created it, rushed into production despite security warnings.

On June 17, 2016, a bug in the smart contract was exploited to steal 3.6 million ether, around a third of the funds invested.



Ethereum's irregular state change

Eventually, Ethereum developers decided to hard-fork the chain in order to give the investors their money back and set the attackers' balances to zero. Some consequentialist arguments I remember from community members:

- Professional investors won't take us seriously when we let thieves get away.
- We'll switch to proof of stake soon, which means the attacker would have significant power. (There's uncertainty again!)



Ethereum's irregular state change

Ethereum designer Alex Van de Sande even said they were 'trolled into' the hard fork by someone pretending to be the attacker. How can you be trolled into betraying your most basic principles?

<https://twitter.com/avsa/status/1499381879967031299>



Alex Van de Sande (avsa.eth)

@avsa

Going through @laurashin incredible "Cryptopians" and I'm still shocked with the revelation that this guy, Andrey Ternovskiy who was known for creating Chatroulette in his teens, might have single-handedly trolled Ethereum into the DAO hard fork.

This is no exaggeration.



Ethereum and property rights

The most common argument was that it wouldn't be right to let the attacker get away with theft at such a large scale.

But this opened a can of worms!

- At which scale do we start editing the blockchain?
- Unlike EOS, Ethereum's original social contract was clearly 'code is law'.
- Many of the people who lost money were ETH insiders.



Consequences for Ethereum

OP Optimism (🌟🔴_🔴🌟) @optimismPBC · Jun 8 ...
So far none of the misappropriated OP has been used for anything related to governance.

If this changes, we will engage in targeted community discussion at that time, with the benefit of a more comprehensive set of facts.

8 6 108

OP Optimism (🌟🔴_🔴🌟) @optimismPBC ...
In principle, a network upgrade could be carried out to halt the movement of those OP tokens which have not already been transferred or sold.

We will not take this step at this time due to the precedent it would set. Optimism is a permissionless network and behaved as intended.

10:21 PM · Jun 8, 2022 · Twitter Web App

The precedent will never go away, even when it's not applied on the main chain anymore.

This makes the claim that Ethereum is 'credibly neutral' unconvincing.

Consequences: a rudderless community

EIP-1559 was a proposal to stabilize the transaction fee market which required burning the base fee. Suddenly, Ethereum influencers became fans of deflation and started promoting 'ultra-sound money'. Ether was originally described as a 'cryptofuel' and it was debated whether it was money at all.

Which 180-degree turn will be next?



Consequences for crypto in general

- Now that the project which sets the tone can't promise 'permissionlessness' or 'unstoppable applications' anymore, our ambition has become '**decentralization**'.

<https://ethereum.org> › dapps ⋮

Decentralized applications (dapps) - ethereum.org

Dapps are a growing movement of **applications** that use **Ethereum** to disrupt business models or invent new ones. Explore dappsWhat are dapps?

Missing: ~~unstoppable~~ | Must include: **unstoppable**



Consequences: the other D word

- **Decentralization** used to be disruptive when Satoshi was around. Now it's become a vague organizational ambition. It's not a hard promise like financial privacy. **Web3** is even vaguer!
- Criticizing smart contract projects for not being really decentralized only confirms that this is the goal.
- Should everything be decentralized? No, but a weak ideal makes it harder to attract new users.



A happy conclusion for Monero

- Unprincipled competitors aren't necessarily evil.
- We don't need to be toxic, because there's already a fundamental difference.
- We can avoid getting dragged into debates about immediate consequences by making moral frameworks explicit.
- We have a stronger ideal than decentralization.
- We have a firm footing and a clear conscience.

