I will be straightforward here, because I think it needs saying.

As a public blockchain, it will be impossible for Ethereum as a platform to deliver any meaningful or realistic guarantees of privacy or anonymity, unless some fundamentals are addressed first. On private blockchains, such as deployed ‘in enterprise’, this is less of problem - iif all participants use the same privacy mechanism and somehow get around the ‘gas payer problem’.

However, the crux of the problem is that if more than one

‘privacy solution’ gains traction on Ethereum main-net, the fact that the anonymity pool is split into factions will do nothing more than reduce privacy for everybody

. In this sense - competition will hurt the ecosystem, aside from in a few specific situations.

What do I mean by privacy?

- No previous or future actions can be associated with, or correlated to, a specific actor.

Think of it in the sense of Perfect Forward Secrecy™, that even if my Ethereum account is fully compromised - my secret keys are leaked to the world etc., nobody should be able to see what I did in the past - and no other key holder should be able to see what I do in the future. It is an ideal.

Ethereum is fundamentally unable to accomplish any part of this Ideal, especially so in a public blockchain setting, because transactions need to be paid for, and there is a linkable history of the movement of funds between accounts this puts the burden of anonymity on the gas payer - they must somehow fund a one-time account without linking it to any of the other accounts. Good luck with that.

One solution is to have ‘transaction proxies/relays’, where you somehow refund the transaction submitter when they successfully execute your transaction, this introduces three really nasty things:

1. You now have an intermediate with a profit-seeking incentive between you and the miner, who are offering a potentially unreliable service which shouldn’t ever need to exist
2. You have to re-design all of the smart contracts (imo… design them ‘properly’), to handle relayed transactions, this puts 99% of the current Ethereum ecosystem out of reach of transaction relay services due to ‘custodial risk problems’ (e.g. msg.sender being the owner of your funds

)

1. Censorship, IP logging, capitalist market capture etc. etc. (hello Infura)

The other solution is to use ‘account abstraction’, where any legitimate transaction will be executed iif it appropriately compensates the miner, this is essentially the same solution as ‘transaction relays’, just replace ‘miner’ with ‘relayer’ - it has the same problems: you need to re-design/re-implement a lot of the current smart contract infrastructure to not give anybody and everybody your funds due to shared msg.sender

, or to be able to access your funds again (because your previous msg.sender

isn’t the same as your current one).

Many ‘anonymity factions’ are worse than a fundamental fix.

Even if we were to implement account abstraction, and then re-design all of the smart contracts to handle the subtleties, then deal with all of the privacy-breaking bugs in the 1000 different implementations, and make everything stop relying on msg.sender

as a concept of authorisation/authentication etc.

The reality is that 99% of people would just use transparent transactions, without any anonymity or privacy.

But, an issue which is specific to Ethereum, is that instead of - like with ZCash - the remaining 1% of ‘private transactions’ all use the same technology with a shared anonymity set. Instead - you have many competing and incompatible ‘privacy solutions’ with their own anonymity sets, if there are 10000 users who want privacy, but they are equally spread across 10 different ‘privacy solutions’ - they all have far less privacy than if they stuck with one - and they started with even less

than they should’ve had because everybody else doesn’t know/care/whatever.

Where is ZCash is now? 99% of the transactions are ‘transparent’, but the majority are traders/exchanges speculating about the value of anonymity and privacy by investing in a ‘privacy coin’ while not using its one and only benefit compared to BitCoin (the irony, it burns…) meanwhile teams of PhDs analyse every ‘private transaction’, with an anonymity set of hundreds, or possibly thousands, compared to the millions that it could be

.

That is worse than Monero, but both are 10x what Ethereum ever possibly could be without really fundamentally addressing this problem - instead we are doomed to add our wishes to the pyre, which only encourages the flames.

TL;DR any privacy technology based on Ethereum, which isn't used in a strictly controlled enterprise environment, is not only fundamentally dead and floating, but even more than that - trying to compete in 'privacy on public ethereum' is causing self inflicted harm and collateral damage.

…