3 steps to destroy Bitcoin for anonymous usage

Arne Babenhauserheide

2015-01-28

Bitcoin is often treated as a haven for black market buyers and people who want to avoid illegitimate laws. However 3 simple steps would suffice to mostly obliterate Bitcoin for black market usage of ordinary users.

Breaking Bitcoin

Three steps to break Bitcoin for small scale anonymous usage:

1. infrastructure: Make it possible for users to register their Bitcoin wallets with their real identity.
2. law or terms of service: Make it illegal to accept money from unregistered users.
3. program: create a script to check transactions whether the transferred bitcoins were tainted by being in wallets of unregistered users. Tainted bitcoins lose value, because non-anonymous services won't be able to accept tainted Bitcoins anymore, so anonymous services become more expensive.

That's it. It will not deanonymize all of Bitcoin, but it will deanonymize most users and making any kind of sustainable profit from Bitcoin will require identity fraud - which carries so harsh penalties that most small scale black market sellers will not dare going that far.

And enacting this does not even need a state. It can be be pulled off by any large entity which accepts Bitcoin as payment, like Paypal or Microsoft.

It gets worse

And it gets worse: large scale Bitcoin owners and black market sellers will have an incentive to pressure their buyers into registration after their sale, because that will increase the effective value of their Bitcoins. Implement the method I outlined, and greed will drive the users themselves to make Bitcoin a hostile place for anonymous users.

People might run shemes to sell at high price to anonymous users and then pressure them into registering, so the bitcoins will become more valuable. Or to sell them registration with false identities. Which they could even report later, when they transferred their bitcoins at high value to someone else to disrupt a competitors business.

Happy Ending

Voilà, for ordinary Bitcoin becomes a viable, happy do-good, decentralized currency with full public accountability which can reduce the trust requirement in the banking system and simplify tax enforcement, while people who can launder money today can still use that power in Bitcoin and even get a few new tools in their toolbox to increase their power relative to ordinary and/or law-abiding users.

The prince marries the princess, the king exercises his right of the first night and all live happily ever after.

Epilogue

I hope I could show that Bitcoin isn't the haven for freedom and state-free happiness it is often touted to be. It can reduce the power of banks due to the required trust in their actions - and I think that it will be used by banks themselves as a very efficient backend for reliable transactions - but the total accountability inherent in Bitcoin is hostile to any kind of free expression and independent life, because it allows others to judge you by your actions years later and as such creates pressure to self-censor how you use Bitcoin.

And as I showed here, on the longterm only large criminal organizations will be able to retain anonymous usage of Bitcoin, while all others will either be driven into buying the services of these organizations to stay anonymous (which makes them susceptible to blackmail: their Bitcoins could lose most of their value at any point) or into registering their Bitcoin identity and giving up on anonymous usage of Bitcoin.