The Blockchain Paradox and the LDoS Attack

By Roy Friedman

14/09/2017

Blockchains implement a persistent, censorship resilient and publically accessible ledgers. Most existing blockchains enable coding arbitrary data as part of the transactions records, e.g., as part of the value or memo fields. However, what if some information that should not be published were to be published on a blockchain? Examples may include copyright infringing material, information that poses fundamental national security risks, etc.

Consider for instance the copyrighted material example, as copyrights laws tend to be highly draconian. Suppose copyright infringing data is published on a given blockchain. Under the DMCA law and similar legislation in other countries, the entity owning the infringed material could potentially seek injunctions forcing deletion of all relevant blocks, placing great financial and criminal liability on anyone running a mining node or a full node for the respective blockchain. In the extreme, this could effectively shut down the network. In other words, this could serve as a *legal denial of service* (LDoS) attack vector.

In some blockchains it might be possible to roll back such transactions and replay the others, like in the hard fork of Ethereum following "The DAO". Yet, such an attack can be launched continuously, leading to repeated forced hard forks that would slow down the network and reduce public confidence in it. Moreover, in privacy preserving blockchains this might not be possible, especially if a sophisticated attacker hacks the code-base of some popular wallet and use it to sprinkle copyrighted material inside multiple legitimate transactions.

As for motivation for launching such an attack, in addition to pure malice and terrorism, an attacker might short sell the targeted blockchain's currency just before launching the attack.

Presumably, a potential solution to this paradox lies in the realization that the damage caused by any given copyright violation can be capped by an amount of money that is much lower than the market value of most leading blockchains. Hence, legislation should be amended to weigh the damage from interfering with the blockchain vs. the financial loss for copyright owners, forcing the courts to take the least financially damaging solution (even when the copyright owner is an American citizen and all cryptocurrency holders are not).

Yet, the above solution would still keep small cap blockchains in danger. And, what if the published information includes illegal material, stolen celebrity nudity photos, or information that poses fundamental national security risks?

Perhaps the solution can be to design blockchains so that retrieving any information other than an emitting account, a receiving account, and the amount transferred would require “significant external decoding data”. By doing this, blockchains might be able to seek “safe harbor” protections. However, this places significant challenges to smart contracts networks since a contract can simply state the offending information, or assign it to a variable. So maybe the concept of tightly coupling cryptocurrencies and transaction settling with a public censorship resilient bulletin board is not such a great idea in the first place?

Disclaimer: This is a purely speculative write-up. The sole purpose of this document is to raise awareness to the mentioned potential conflict posed by blockchains so policy makers and developers alike start thinking about it. Obviously, I do not encourage anyone to launch such a potential attack (or misuse blockchains in any way). Misusing and attacking blockchains is immoral and probably illegal. Note that I have no legal training, and this document should ***not*** be taken as an advice, legal or other, of any sort.