CAN THE LAW TAME CRYPTO CRIME?

BY GIDEON SAMID
gideon@bitmint.com

EVEN CRYPTO BUSINESSES that keep saying crypto crime is tolerable recently had to acknowledge a whopping $14 billion in reported criminal crypto activity occurred in 2021. The true figure is at least an order of magnitude higher, since many ransomware victims don't even report the crime.

The sad reality is that criminal empires have never had it so convenient, financially speaking. Drug trafficking, human trafficking, illegal arms sales, blackmail, and extortion of all kinds are mostly using Bitcoin as a shield, keeping one step ahead of the law. Yes, there are millions of law-abiding citizens trading with Bitcoin, and some see a handsome profit. But it is time for these honest traders to admit that, by taking part in the decentralized trade, they give aid and comfort to the destructive forces in society.

And it is not needed. Privacy is perfectly achievable with coins that are administered by a registered entity subject to the law of the land. Much as cash leaves the bank, moves around through unknown traders, and then is deposited by someone, somewhere, so can digital coins transact cash-like among anonymous traders, with the mint identifying only the purchaser and the redeemer. We already have the technology to establish a good balance between privacy and the law (for example, BitMint*LeVeL).

Decentralized money is considered by common wisdom to be out of reach of the law. After all, you can't sue a protocol. Indeed. But you can outsmart a protocol. It's time for the law to be as imaginative as its targets.

You can't sue a protocol. But you can outsmart it.

Bitcoin relies on the continuous attention of its traders to the notorious ledger of payments. It would be fair, therefore, to require the traders to peruse an FBI-alert crypto ledger. This ledger would list Bitcoin accounts that have been mentioned in a lawsuit. For example, a merchant paying ransom to regain its data might sue the owner of the receiving account. If that owner can take money anonymously, it should also be declared as a defendant in a lawsuit –owner identity unspecified.

The owner, perusing the FBI-alert ledger, will have the option to get out of the shadows and defend itself. If it doesn't, the trial will proceed on the merits of the complaint. If the court rules against the unknown accountholder, the account will be added to a second ledger: the FBI-wanted ledger.

Over time, money from the condemned account will traverse from one account to the next (all recorded on the Bitcoin ledger). At some point, the current account holder will surface with its identity (for example, in proving that a bank deposit it made is a legitimate Bitcoin profit). When this identity is so exposed, the law will see that some of this money came from a condemned account, and confiscate it.

The very prospect of this confiscation will prompt each Bitcoin trader to check the FBI-wanted ledger to see if any payment made to them has a history of having been owned by a condemned account. If so, the payee will reject it.

And this is where the law flexes its muscles. Ransomware artists collecting their criminal fortunes will suddenly realize their money is no good. No one will want to accept it!

Now of course these wily criminals will think of something. They always do. But it is time for the good guys to use their imagination and show some determination. Suing an anonymous account may require administrative accommodation, regulatory accommodation, or even legislation. Let's rise to the challenge. The destructive impact of Bitcoin-aided crime is motivation. I hope an enterprising lawyer will take this baton and run with it! DT