Hacking the Unhackable: The Missing Crypto-Currency…

Source: Giza Death Star

by Joseph P. Farrell
February 20, 2019

Yesterday I blogged about JPMorgan's daliances with crypto-currency, and its plans for a new crypto-currency pegged to the dollar,. in a system that could also handle other real currencies and even securities. And you'll recall, I crawled out to the end of the twig of trademark High Octane Speculation once again, and probably managed to crawl off the twig as well. But just in case you missed it, here is that speculation:

> *My high octane speculation – and I think I'm on the end of the twig on this one – is that this is an attempt to create a version of the old European "Snake", the Exchange Rate Mechanism whereby the currencies of smaller countries were pegged, within certain percentage points of valuation, against the German Deutschmark. When currencies fluctuated outside that benchmark, the central bank (in this case, the Bundesbank) stepped in to restabilize those currencies. It was this mechanism which France later joined, and the emergent result was the euro and the Eurozone. So it's those parts about JPMorgan's new crypto being tied to (1) the dollar and (2) the possibility of expanding that to handle other currencies and possibly even types of securities that really catches the eye, for it suggests that it is a move to peg other currencies, and securities, to the dollar and dollar-evaluation. Think of it as a kind of combination of SWIFT, the Exchange Rate Mechanism, and a securities*

> *brokerage all in one fell swoop. And, oh yea, lest I forget, you'll notice it's also a nifty move to allow JPMorgan to become a kind of international central bank, too.*

Judging from some of the comments on the blog, there were a few other people willing not only to crawl to the end of that twig with me, but right on off the edge.

Well, believe it or not, crypto-currencies are back in the news again, and if you've been following various stories about missing money and financial fraud, you'll want to pay attention to this article that was shared by Ms. K.M.:

Once hailed as unhackable, blockchains are now getting hacked

I remember well the halcyon days when crypto-currencies were going to give us complete financial security, anonymity and "unhackability," and best of all, make central banks and central banksters obsolete. Of course, that was the latest in the long list of impenetrable armor, unsinkable ships, unbreachable barriers, irresistible and invincible weapons, unbreakable records, and flawless plans that have dotted human history, and at the time – if I may be permitted to toot my own kazoo for a moment – I was in a decided minority warning people that "there just aint no such thing as a secure cyber system."

Now, it seems even MIT has seen past Utopia into reality. But that reality is taking on a shape and dimension that, in my opinion, calls for a revision and extension of my High Octane Speculation remarks from yesterday. Here's the paragraphs from the article that made me think once again. We'll start with this one:

> *A hacker had somehow gained control of more than half of the network's computing power and was using it to rewrite the transaction history. That made it possible to spend the same cryptocurrency more than once—known as "double spends." The*

> *attacker was spotted pulling this off [to the tune of $1.1 million](#).*

To my mind, that conjured images of what we all know good and well that some banks and banksters do and which they all deny they do or have ever done, and that's use that "in between" period when a bank holds a check, and waits for it to clear, during which time it makes (quick) use of the money that's in "transactional limbo." How much better it would be if one could simply "re-write" transaction history, "double spend" that "in-limbo money" and then go back and re-write everything once again. I may be off the end of the twig on that one, but there's a reason that ink, and not pencils with erasers, were used in the good old days of actual ledgers and accountants.

But then there's this:

> *In total, hackers have stolen nearly $2 billion worth of cryptocurrency since the beginning of 2017, mostly from exchanges, and that's just what has been revealed publicly. These are not just opportunistic lone attackers, either. Sophisticated cybercrime organizations are now doing it too: analytics firm Chainalysis recently said that just two groups, both of which are apparently still active, may have stolen a combined $1 billion from exchanges.*
>
> *We shouldn't be surprised. Blockchains are particularly attractive to thieves because fraudulent transactions can't be reversed as they often can be in the traditional financial system. Besides that, we've long known that just as blockchains have unique security features, they have unique vulnerabilities. Marketing slogans and headlines that called the technology "unhackable" were dead wrong.(Emphasis added)*

It's that non-reversibility of fraudulent transactions in blockchains that caught my eye, because if one were say, a bankster working in one of those too big to fail too big to

jail banks, what a golden cyber-opportunity to harvest even more money, re-write the transaction history, and make off with – well, hey, this is the twenty-first century, and we have to think big – trillions. (And given the Pentagon's inability to find out where all its missing money went, and the private corporations handling all that financial data for the federal goobernment, who's to say it's not already been beta-tested?)

Which brings us back to JP Morgan's plans for a crypto-currency tied to the dollar (and possibly other currencies) in a system that could not only handle other currencies, but securities too: talk about a golden opportunity for currency speculation, for playing (and rigging) markets, and so on. And then, lest those pesky regulators come around, just re-write the transaction history. Nobody but the NSA would know, and they probably wouldn't talk lest "national security secrets" be reviled… er… I mean, revealed.

But have no fear, too big to fail and too big to jail banks and banksters, who resorted to fraudulent mortgages, robo-signing fraudulent mortgages, opening fake accounts in their customers' names and using them for "transactions" and other money laundering schemes, not to mention forging their signatures, would never resort to such outright theft using blockchains and organized teams of hackers.

Perish the thought!

(Cough, hack wheeze…)

See you on the flip side…