From: Vincenzo Iozzo [redacted]
Sent: Friday, August 22, 2014 6:33 PM
To: jeffrey E.
Subject: Fwd: answer to the bitcoin questions

It's a long email, but if you're still thinking about bitcoin it might =rovide a couple of useful hints

The questions that I auto-asked myself were
1) What's the real value of bitcoin
2) Is the bitcoin heritage/stamp a good or a bad thing
3) Who 'rules' the financial system (a bit more complicated than this =ut that was the gist of it)

Begin forwarded message:

> From: Vincenzo Iozzo [redacted]
> Subject: answer to the bitcoin questions
> Date: 22 agosto 2014 14:10:35 GMT+1
> To: Joi Ito [redacted]
>
> Ok after some more thinking & reading I think I can answer question =1).
>
> The real value of bitcoin is the following:
> 1) The proof that the Byzantine generals problem can be solved without
> =rust given enough people and the right set of incentives
>
> 2) A reminder that "anacyclosis"
> =http://en.wikipedia.org/wiki/Anacyclosis) is a thing and works for
> all =omplex systems not just politics. Currencies were
> 'revolutionized' in =he past and eventually will be revolutionized
> again. This sounds philosophical but =t's not - it's a good way to
> instill fear into the institutions that =urrently have control over
> the 'system' and I think bitcoin to a =ertain extent did well at it
>
> 3) The empirical proof that you can combine distributed =ystems&transparencies (the public ledger) in a system where real value =s at stake. This is sort of an enabler, both technologically and in =erms of 'mindset', for future application in the same realm.
>
> 4) I need to look into this more and technically it's not bitcoin
> =ut.. another key factor is that you can use zero-knowledge proofs to
> =tune' transparency in a distributed system. Zero knowledge proofs
> =eren't really used for a long time in any practical way, so I guess
> we =ave to thank bitcoin for that
>
> This also implies that the currency itself is irrelevant, it might or =ight not work but that's not where the real value is. Likewise I don't =hink that the 'crypto' nature of the protocol is the key, that is an =bvious consequence - At the end of the day SWIFT (to name one) uses a =ot of crypto too and PGP/CA are the proof that crypto can be used for =uthentication purposes.
>

> Also given the above I'm strongly convinced that the heritage is a bad =hing, besides the technical background (given by the fact that they =ctually worked on the thing) there's nothing of real value there and if =nything there's a lot of skepticism given their cyberpunk nature.
> Or in pompous terms: they started the 'revolution' now we need =serious' people to actually make something of it.
>
>
> I don't have a full answer for the question (3), but I think we can =asily say that who 'rules' the financial system is "America" and at the =ame time is "Not consumers". This implies that there's probably =onsensus in the fact that all the backoffice compliance work mandated =y law/America can/should be made better (both in terms of transparency =nd also in terms of efficiency for banks), and the fact that is "not =onsumers" kind of guarantees that banks will not feel too threaten by =tuff in that realm because in the worst case scenario (assuming future =osts < current costs) they can offset the costs to consumers.
>
> So I think that 'attacking' SWITF/Sepa/ACH is doable, I would love to =o the other crazy thing (the currency pegged to oil in the "spaghetti" =mail - I'd love to discuss that a bit at some point) but if we want to =eep things simple we can start with SWIFT.
> "Observe everything, endure a lot, fix one thing at a time" quote of
> =ome random catholic person I don't remember (can't get away from the
> =talian heritage I guess)
>
> For the SWIFT stuff, we can have a public ledger (consensus based) of =ll the transactions, the transactions can be encrypted but we/govts =ill also have a copy of the private keys to decrypt them when/if needed =or legal purposes. Also maybe this level of transparency is good enough =o convince govts to subsidize some of costs needed to implement the =ystem on the banks side.
>
>
> Thoughts?


```
<?xml version=.0" encoding=TF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version=.0">
<dict>
        <key>conversation-id</key>
        <integer>299361</integer>
        <key>date-last-viewed</key>
        <integer>0</integer>
        <key>date-received</key>
        <integer>1408732365</integer>
        <key>flags</key>
        <integer>8590195713</integer>
        <key>gmail-label-ids</key>
        <array>
                <integer>2</integer>
        </array>
        <key>remote-id</key>
        <string>433769</string>
</dict>
</plist>
```