
From: Vincenzo lozzo <[REDACTED]>
Sent: Sunday, January 31, 2016 9:40 AM
To: jeffrey E.
Subject: Re:

Hmm I realized that yesterday I might have drown you in too much tech details, sorry.

I think the short answer is: aside from the mesh network (which is doubtful and a=bit weak, mostly for lack of details) the rest mostly sounds good/feasible in theory. The practice might be, and almost always is, weaker. </=iv>

The stuff I said yesterday are the things I would start going after first if I were tasked to attack it.

Sent from my Iphone

On Jan 30, 2016, at 13:27, Vincenzo lozzo <vincenzo@tiqad.com</=>> wrote:

<mailto:vincenzo@tiqad.com>

=div>Sent from my Iphone

On Jan 30, 2016, at 13:16, Vincenzo lozzo <[REDACTED]> <mailto:[REDACTED]> wrote:

It's hard to tell w/o proper code/documentation (couldn't find much online). In general the four things are:

1) the devil is in the details, meaning that even if in theory it's all solid the implementation might have bugs. There's no definitive technical solution for that though

2) anything that is "custom" (eg: they have a custom wifi protocol) is a red flag because it means that it hasn't been properly vetted and might be broken/buggy </=iv>

=) there aren't enough details online to tell but it seems to me that to speed up the blockchain verification they partially centralize the network by using their own "supernodes" (essentially the wallets talk to the supernodes via the actual blockchain). The security of those servers seems key to me and they gloss over it online

4) the mesh network implementation is completely up in the air (judging from what's public) and it could go horribly wrong. So that needs further verification

Also (5), in general the disadvantage of distributed /open things is that it is a lot easier to steal money via a closed network (like swift).

Are you looking to invest into this thing? If so, I'd suggest a few things:

A) because problem (1) above is not completely solvable, they need to have a plan. Part of it is technical (do continuous code auditing, pentesting, on board proper crypto people, etc), the other part is legal/financial and physical. Specifically they should have some kind of insurance and they should have a pr disaster recovery plan. A disadvantage of decentralized system is that you don't have anybody to trust and you don't have a closed network that can make stealing money hard, they need to address that

B) realistically nobody is going to attack them until they become significant enough from a financial standpoint. This gives them time to work on A. That said they should avoid making enemies (the="disgruntled" hacker type)

</=iv>

Hope this is useful, if you get more stuff from them I'm happy to look into it more. Also if you do invest I can help them with (A) if needed.

It's a very dumb platitude but "security is a process" is true.

Unrelated: checkout edge.org <http://edge.org> , I think you'll like it.
There's a short video with Minsky that is absolutely fantastic

Sent from my Iphone

=br>On Jan 30, 2016, at 11:26, jeffrey E. <jeevacation@gmail.com <mailto:jeevacation@mail.com>> wrote:

(<https://mycelium.com/phone/index.html> <<https://mycelium.com/phone/index.html>>). =nbsp;
what are its weak points?

--

 please note

The information contained in this communication is confidential, may be attorney-client privileged, may

constitute inside information, and is intended only for
the use of the addressee. It is the property of
JEE

Unauthorized use, disclosure or copying of this
communication or any part thereof is strictly prohibited
and may be unlawful. If you have received this
communication in error, please notify us immediately by
return e-mail or by e-mail to jeevacation@gmail.com <mailto:jeevacation@gmail.com> , and
destroy this communication and all copies thereof,
including all attachments. copyright - all rights reserved

=