From: Vincenzo Iozzo [redacted]>
Sent: Thursday, July 24, 2014 9:38 AM
To: jeffrey E.
Subject: proof of burn (re: bitcoin&anonymity)

Jeffrey,

not sure if you're still interested in this but.. to answer in a more =xplanatory way the question of how to remove anonymity from bitcoin, =ere it is:

The bitcoin network has a couple of things that are particularly =mportant for any crypto currency, the first one is that the network is =ig enough to prevent double-spending kind of attacks and the second one is that there's no way (I mean there is, but it's =ci-fi) to generate the private key for a random bitcoin identify/public =ey that is not yours.

A number of annoying things about bitcoin are:
1) It's deflationary, not just because the amount of coins is finite but =lso because people lose wallets/keys so potentially a lot of the mined =oins will never see the light of the day

2) You can create as many wallets/keys as you want, in theory this =llows you to keep separate identities.. in practice this is not =ntirely true

3) A little known fact is that you can mess with the blockchain/ledger =uite a lot, for instance somebody forced specific values into the =edger. For instance, these values could be virus signature, so antiviruses would quarantine/delete the blockchain from people =omputers. Not only that, but people have been storing all sort of stuff =nto the blockchain and it's permanent you cannot undo it.
See: http://pastebin.com/ct2WHUK5 and =ttp://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html

ok so here's what you do if you want to fix (1) and (2), I don't have a =ood solution for (3) unless you change the power forces inside the =etwork (eg: unless you allow a centralized unit to 'clean' the =lockchain)

You create another crypto/alt currency that is inflationary so it mimics =eal money better, then you tell people: "everyone who has Bitcoins can =et them exchanged for this other currency".

The way this would work is that you actually require people to sign up =or a *single* identify/key/wallet linked to their real identity and =hen you do something called 'proof of burn', which in practice means =hat you tell people that to prove they 'exchanged' their bitcoins they need =o send them to a non-existent address (remember that it's impossible to =enerate the private key of a random bitcoin address/public key, so nobody can ever claim those coins and they are lost forever).

On the top of that, since the bitcoin network is flexible you can use =hat blockchain to record the transactions of your own currency without =ny major issues (there are some technicalities involved but nothing =uch).

This brings to the last and probably hardest point which is: Why people =ould do it?

So some people do it already to get on board new currencies, so it's =ostly a speculation/ideology/belief. But if say you're a government, =ou can sweeten the deal saying something like "your holdings in =itcoins will not be taxed if moved to this other currency".
If you're not a govt then things are more complicated, but well..

Anyway, this is in short how you go from bitcoin to another currency =with the properties you care for) while preserving the bitcoin network =nd its strengths. As I said, not sure if it's useful/interesting but I =igured I'd share it

Another thing: any chance I can crash at your place in Santa Fe say aug =-10? I'm still not sure whether I'm supposed to be there or not, but I =igured that maybe it's worthwhile to go and visit anyway

ps: note that the moment you remove anonymity from bitcoin there's a =ignificant privacy problem. Meaning that now everyone knows what you =uy/sell through bitcoin, it's advertisers (among others) sweetest dream =ut probably your worst nightmare


```
<?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>132701</integer>
	<key>date-last-viewed</key>
	<integer>0</integer>
	<key>date-received</key>
	<integer>1406194688</integer>
	<key>flags</key>
	<integer>8590195717</integer>
	<key>gmail-label-ids</key>
	<array>
		<integer>6</integer>
		<integer>2</integer>
	</array>
	<key>remote-id</key>
	<string>426659</string>
</dict>
</plist>
```