From: Vincenzo Iozzo [redacted]
Sent: Thursday, July 24, 2014 11:58 AM
To: jeffrey E.
Subject: Re: proof of burn (re: bitcoin&anonymity)

oh also.. thanks for santa fe :)
I was taken by the discussion and I forgot that important detail.. my =om would be upset

On 24/lug/2014, at 12:41, Vincenzo Iozzo [redacted] wrote:

> no in the case I was sketching in my email you don't actually replace =he dollars, you just replace bitcoins. The only reason why you want to =eplace bitcoin is to get their network power which is needed to solve =he multiparty consensus problem (the double spending attack).
>
> Now in one of the other potential options you don't even need that, =f you enforce identities you can also guaranteed benign multiparty =onsensus on transactions as long as less than N/4 actors are malicious. =hich in practice means you don't need to have that many people in your =etwork mining coins.
>
> Also yes you can easily embed transactions descriptions/codes.
>
> There's always the risk of actually losing or having your 'wallet' =tolen, but you cannot avoid that 100%. You can either do what some =itcoin services do (it's called called/hot storage) or have the govt as =n insurer of last resort.
>
> I feel like that story you told me about you trying to decode hand =ignals back in the days, in the sense that I'm either missing something =ere or my pessimistic view of things is shaping my thinking too much - = don't see why anybody but governments would want to have this. In any =ase, forgetting that for a moment and assuming companies want to do =his then you can do it quite easily.
>
> anyhow, it's probably worth to talk about this F2F in Santa Fe if we
> =anage to work that out
>
>
> On 24/lug/2014, at 11:14, jeffrey E. <jeevacation@gmail.com> wrote:
>
>> the goal is to creat a fully transparant currency, but secure, It =oes not need to replace dollars wuth complement them, for ex . =orporate cash. so corporations and gocts can transact transparantly, =much more like a game world. inflation is needed if there will be =oans, (to compensate for risk). yes to santa fe. in addition it =ould be nice to tag the transaction with a code (refund, loan, =dvance, income, sale etc).
>>
>>
>> On Thu, Jul 24, 2014 at 5:37 AM, Vincenzo Iozzo [redacted] =rote:
>> 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
>> =ut also because people lose wallets/keys so potentially a lot of the
>> =ined coins 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
>> =lockchain/ledger quite a lot, for instance somebody forced specific =alues into the ledger. For instance, these values could be virus =ignature, 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.ht
>> ml
>>
>> ok so here's what you do if you want to fix (1) and (2), I don't have
>> = good 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 =imics real money better, then you tell people: "everyone who has =itcoins can get them exchanged for this other currency".
>>
>> The way this would work is that you actually require people to sign
>> =p for 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 =eed to send them to a non-existent address (remember that it's =mpossible to generate the private key of a random bitcoin =ddress/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 =eople would 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

>> =ug 8-10? I'm still not sure whether I'm supposed to be there or not,
>> =ut I figured 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
>>
>>
>>
>>
>>
>>
>> --
>> 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,
>> and destroy this communication and all copies thereof, including all
>> attachments. copyright -all rights reserved
>

<?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>1406203120</integer>
	<key>flags</key>
	<integer>8590195713</integer>
	<key>gmail-label-ids</key>
	<array>
		<integer>6</integer>
		<integer>2</integer>
	</array>
	<key>remote-id</key>
	<string>426766</string>
</dict>
</plist>