From: "jeffrey E." <jeevacation@gmail.com>
To: Vincenzo Iozzo <[redacted]>
Subject: Re: proof of burn (re: bitcoin&anonymity)
Date: Thu, 24 Jul 2014 10:14:01 +0000

---

the goal is to creat a fully transparant currency, but secure, It does not need to replace dollars wuth complement them, for ex . corporate cash. so corporations and gocts can transact transparantly, much more like a game world. inflation is needed if there will be loans, (to compensate for risk). yes to santa fe. in addition it would be nice to tag the transaction with a code (refund, loan, advance, income, sale etc).

On Thu, Jul 24, 2014 at 5:37 AM, Vincenzo Iozzo <[redacted]> wrote:

> Jeffrey,
>
> not sure if you're still interested in this but.. to answer in a more explanatory way the question of how to remove anonymity from bitcoin, here it is:
>
> The bitcoin network has a couple of things that are particularly important for any crypto currency, the first one is that the network is big 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 sci-fi) to generate the private key for a random bitcoin identify/public key 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 also because people lose wallets/keys so potentially a lot of the mined coins will never see the light of the day
>
> 2) You can create as many wallets/keys as you want, in theory this allows you to keep separate identities.. in practice this is not entirely true
>
> 3) A little known fact is that you can mess with the blockchain/ledger quite a lot, for instance somebody forced specific values into the ledger. For instance, these values could be virus signature,
> so antiviruses would quarantine/delete the blockchain from people computers. Not only that, but people have been storing all sort of stuff into the blockchain and it's permanent you cannot undo it.
> See: [redacted] and [redacted]
> photographs.html
>
> ok so here's what you do if you want to fix (1) and (2), I don't have a good solution for (3) unless you change the power forces inside the network (eg: unless you allow a centralized unit to 'clean' the blockchain)
>
> You create another crypto/alt currency that is inflationary so it mimics real money better, then you tell people: "everyone who has Bitcoins can get them exchanged for this other currency".
>
> The way this would work is that you actually require people to sign up for a *single* identify/key/wallet linked to their real identity and then you do something called 'proof of burn', which in practice means that you tell people that to prove they 'exchanged' their bitcoins they need to send them to a non-existent address (remember that it's impossible to generate 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 that blockchain to record the transactions of your own currency without any major issues (there are some technicalities involved but nothing much).

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

So some people do it already to get on board new currencies, so it's mostly a speculation/ideology/belief. But if say you're a government, you can sweeten the deal saying something like "your holdings in bitcoins 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 and its strengths. As I said, not sure if it's useful/interesting but I figured I'd share it

Another thing: any chance I can crash at your place in Santa Fe say aug 8-10? I'm still not sure whether I'm supposed to be there or not, but 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 significant privacy problem. Meaning that now everyone knows what you buy/sell through bitcoin, it's advertisers (among others) sweetest dream but probably your worst nightmare