**From:** Vincenzo Iozzo [redacted]
**Sent:** Tuesday, August 26, 2014 12:52 PM
**To:** jeffrey E.
**Cc:** Joi Ito
**Subject:** zero knowledge proof/SNARK

One interesting thing I stumbled upon in my reading is ZeroCash, which =s essentially a 'privacy preserving' version of Bitcoin.

Now besides the currency itself, what's interesting is that they use a =pecific kind of zero knowledge proof (ZKP) systems called zk-SNARK.
I'll save you the full lengthly explanation, but the reason why this is =nteresting is that:

1) ZKP (http://en.wikipedia.org/wiki/Zero-knowledge_proof) can be used =o proof statistically/computationally that a user (A) knows something =ithout reveling the secret itself. eg: A can prove to user (B) that he =nows the password of a certain system without showing the password to B. Usually that =equires some kind of interaction between the users (user B asks a round =f questions to user A, if A gets them right then it's statistically =ery unlikely that he got all of them right without knowing the secret) =
2) zk-SNARKs are interesting because:
    a) They are not interactive
    b) They are 'short' and easy to prove
On top of that essentially you can prove in zero knowledge almost =nything that is 'computable'.

What this means is that if we use zk-SNARKS/similar ZKP for our currency =e can enforce arbitrary rules on how the currency is spent ("this coin =s of type X and can only be spent with these following merchants", or =this coin can be spent because it was not obtained illegally and the =uy payed taxes"). I'm exaggerating a bit with expressiveness, but it's =lose.

Also this allows us to tweak the privacy vs transparency bit.

Generally speaking we have other easier options to do all these things =multi-party signatures, centralized black lists, etc etc), but this is =nteresting.

Thoughts?

Also Jeffrey, any updates on the govt side of the house?


```
 =?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>299867</integer>
        <key>date-last-viewed</key>
        <integer>0</integer>
        <key>date-received</key>
        <integer>1409057525</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>434491</string>
</dict>
</plist>
```