

---

**From:** [REDACTED] on behalf of Whitfield Diffie [REDACTED]  
**Sent:** Thursday, January 31, 2013 9:09 PM  
**To:** Jeffrey Epstein  
**Subject:** When next?

> when next?

I think you proposed this coming weekend but I told you I would probably be off in the hills and we might have to wait until next week.

I realize that I don't know whether your response to bitcoin is purely a business response or whether it is driven by social issues and I am equally ignorant of the motivations of the guys who visited you.

You said you told them, I wasn't sure in what advisory capacity:  
were they willing to serve time as a cost of making money or as a risk of a program to introduce digital money.

> great, taxes are the key,

Taxes are important but it is not necessarily true that taxes have to be collected in the current surveillance-based manner.

> unlike the coal issues in England, There is an already existing army  
> of laws, penalties and enforcement people ready to take down a whole  
> host of money related initiatives. bit coin is anonymous, anti govt.

Certainly wood versus coal is not a perfect analogy but what I recall being told was that at one point it was capital crime to burn coal in London and that a century later, it was commonplace. Things do change. There was an army of laws prepared to squelch blacks, women, queers, and sexuality in general. Each of those groups has done better over our lifetimes and a lot of law has changed. The move of human culture into cyberspace appears to me to be a move into a manmade world without precedent in five-thousand years. The introduction of a digital currency seems a natural development. It may succeed or it may not but I don't think it can be dismissed out of hand.

> I think we could design a combo of zero knowledge. - encrypted, but  
> transparent, currencies so that for example. the extreme would be  
> every unit of currency has a serial number. there is a transaction  
> record, I give you ten specific dollars, it is coded according to the  
> nature of the transaction, etc. the govt has a record as it is the  
> issuer. it takes its cut. directly, (taxes). it can't increase money  
> supply without everyone seeing it.

If you don't want anonymity (or at least the money having value in itself, independent of the bearer) I don't see that any of the fancy cryptography (as opposed to the non-fancy cryptography of the banking security measures) is needed. Don't current credit-card techniques serve adequately?

> I am talking to Mike Rabin about zero knowledge auctions, ...

This also sounds as though it must involve anonymity.

I make no claim that bitcoin itself will be successful or is the right approach. On the other hand, I don't think that the fact that powerful people don't like it is any guarantee that it will fail. Your discussion about lack of monetary systems in Africa is interesting.

Should some new form of money become successful there, the rest of the world would probably have to accommodate it.

> the biology should be shelved to next, but offers more play

I presume that is to the next conversation; I look forward to it.

```
Whit <?xml version="1.0" encoding="UTF-8"?> <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST
1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>date-last-viewed</key>
  <integer>0</integer>
  <key>date-received</key>
  <integer>1359666539</integer>
  <key>flags</key>
  <integer>8623750145</integer>
  <key>gmail-label-ids</key>
  <array>
    <integer>27</integer>
    <integer>7</integer>
  </array>
  <key>remote-id</key>
  <string>273042</string>
</dict>
</plist>
```