# Bitcoin Day

PescaraLUG
08.03.2014
(Nicola Battista/Dj Batman)
Maze Eclectic Circle

# Il fenomeno Bitcoin

- Cosa sono le criptovalute
- Famiglie di criptovalute
- La nuova corsa all'oro è su Internet?
- Chi ha inventato il Bitcoin
- Chi ha paura del Bitcoin?
- Come fare mining
- ATM e altri servizi
- Anarcocapitalismo, monete improbabili & prospettive future

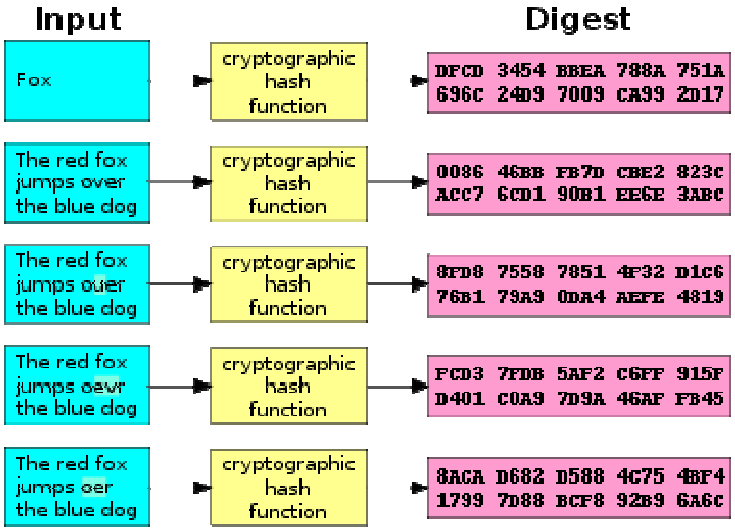
# Cosa sono le criptovalute

- **Intermediario di scambio digitale (una sorta di moneta virtuale)**
- **Fanno uso di crittografia (**κρυπτός **+** γραφία **= "scrittura nascosta", offuscare/cifrare un messaggio) al fine di creare una rete di informazioni che sia distribuita, decentralizzata, sicura, con un certo livello di anonimato.**
- **Gli algoritmi sono usati per generare e verificare la moneta, per avere una rete protetta da attacchi e soprattutto decentralizzata: non esiste autorità centrale di controllo (come una banca di stato o altro)**
- **Il network Bitcoin è la rete più potente al mondo di Calcolo Distribuito**
- **Valute p2p e Open Source (= tante derivazioni del Bitcoin con elementi molto simili quali portafoglio, blockchain ecc.)**

# 3 grandi famiglie di cryptocurrency

## In base all'algoritmo che utilizzano, legate a:

- **Bitcoin – SHA256 (Secure Hash Algorhythm, algoritmo di crittografia a 256 bit presentato dalla NSA nel 2001). Vengono svolte numerose operazioni matematiche: è necessaria una notevole potenza di calcolo.**



# 3 grandi famiglie di cryptocurrency

In base all'algoritmo che utilizzano, legate a:

- Litecoin – Scrypt

  Richiede più RAM che potenza di calcolo (basta una buona scheda grafica per cominciare).

  Usa SHA256 solo come subroutine.
- Primecoin – Confusa da molti come una valuta legata a una delle famiglie precedenti, lavora invece con un algoritmo diverso, scoprendo catene di numeri primi sempre più grandi.

# Tante (troppe) criptovalute

- Dollaro = $ = USD
- Bitcoin = BTC (o XBT)
- Litecoin = LTC
- Feathercoin = FTC
- Primecoin = XPM
- Sexcoin = SXC
- DogeCoin = DOGE

...e via dicendo

# La nuova corsa all'oro è su Internet?

- Il Bitcoin va "cercato" in rete come si cercava l'oro
- Confronto con la "corsa all'oro" di oltre un secolo fa in Nord America, Australia, Nuova Zelanda, Sudafrica
- Pochi si arricchiscono davvero
- Tra questi, i venditori di strumenti utilizzati dai "cercatori"
- Speculazioni, truffe
- Tanti finiranno per rimetterci economicamente e non solo

# Il Bitcoin è frazionabile

- 0.01 BTC = 1 cBTC
- 0.001 BTC = 1 mBTC
- 0.000 001 BTC = 1 μBTC = 1 microbitcoin
- 0.000 000 01 (1 milionesimo di Bitcoin) = 1 Satoshi

# Chi ha inventato il Bitcoin?

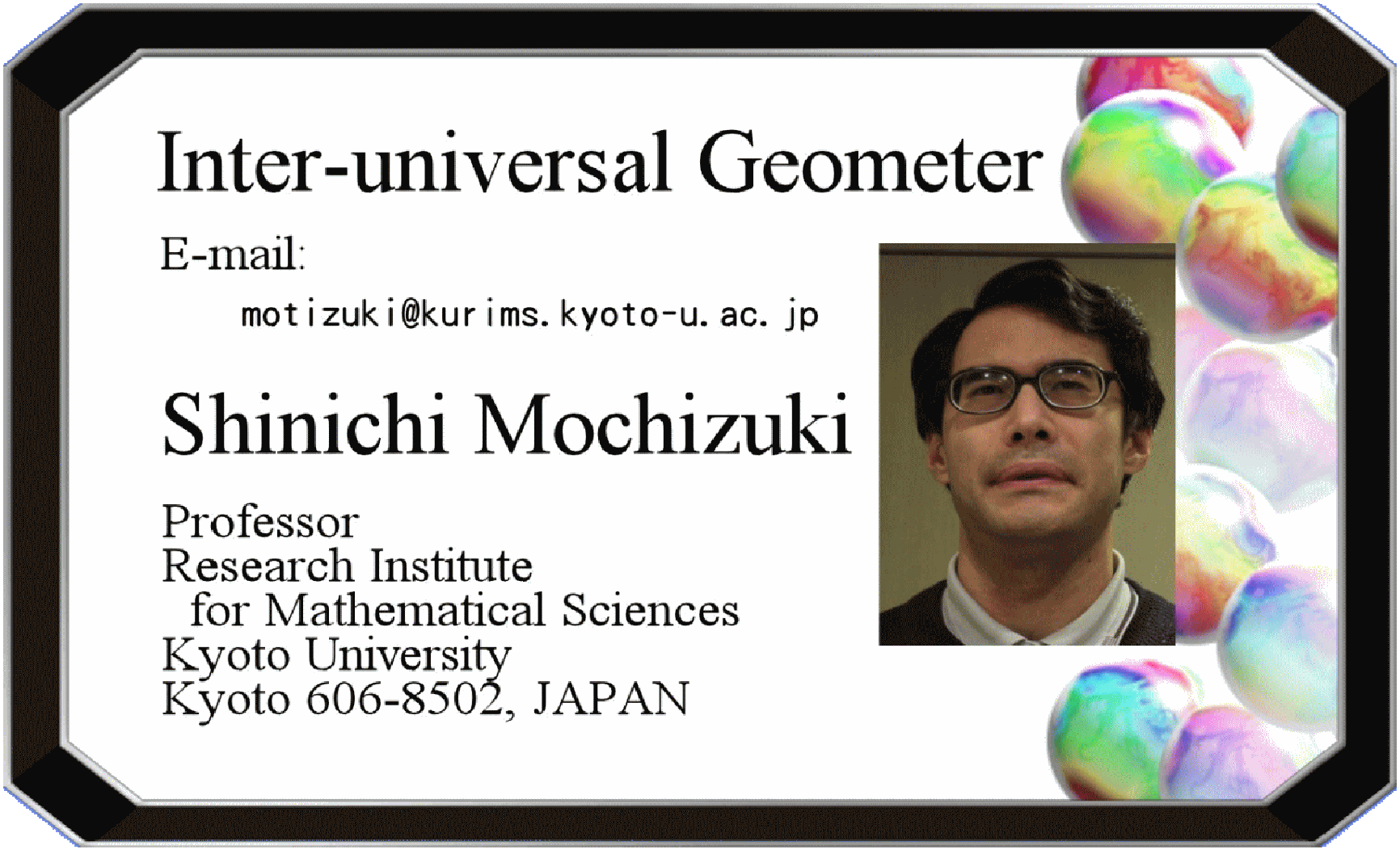
# Chi ha inventato il Bitcoin?

- Testo pubblicato da Satoshi Nakamoto (中本 哲史), 2008
- Lancio del Bitcoin nel 2009
- Satoshi lascia a Gavin Andresen nel 2010
- Varie illazioni sull'identità di Satoshi

Tra le più probabili:

- Shinichi Mochizuki (matematico giapponese nato nel 1969, che parla un ottimo inglese)

# Chi ha inventato il Bitcoin?



# Chi ha inventato il Bitcoin?

- **6 marzo 2014: controverso scoop di Newsweek su Dorian Prentice Satoshi Nakamoto, varie smentite**

# Chi ha paura del Bitcoin?

- Diversi governi: Russia, Cina, Thailandia
- Pressione anche all'interno di alcune aree degli Stati Uniti (California) come pure in Europa, per divieti o forme di regolamentazione
- Il pretesto delle attività illecite svolte con l'utilizzo di Bitcoin: il caso Silk Road, non diverso però dal tempo in cui si criminalizzava l'uso di file mp3 oppure si definiva l'intera Internet come "covo di mercenari" e luogo dove comprare ogni sorta di bene pericoloso/illegale.

# Chi ha paura del Bitcoin?

- La crisi economica o altri fattori di instabilità spingono verso Bitcoin; alcuni esempi:
- la crisi di Cipro (il caso dell'Università di Nicosia)
- i disordini in Ucraina (finanziare una rivoluzione col Bitcoin?)
- il problema dell'utilizzo di contante in Cina anche per fare grandi acquisti (la banconota più grande: 100-renminbi = circa 16 dollari)
- Un caso a parte è il mondo del gambling online

# Come fare mining

- Come “scavare” per trovare Bitcoin e simili?
- CPU – processore del computer (improduttivo/antieconomico)
- GPU – scheda grafica (ormai antieconomica per Bitcoin, perfettamente usabile per Litecoin e derivati)
- FPGA/ASIC – moduli esterni programmabili o preconfigurati per eseguire le operazioni necessarie al mining (al momento soprattutto per Bitcoin; in arrivo anche per la famiglia Litecoin)

# Come fare mining

- Se ci interessa Bitcoin, procurarsi una scheda da montare nel computer o uno o più moduli esterni ASIC (i costi non sono esattamente contenuti…)
- Vantaggio: possibilità di usare un Raspberry Pi come controller, risparmiando energia (non occorre tenere acceso un computer ingombrante per far andare gli ASIC)
- Svantaggi: è difficile recuperare i costi iniziali
- Se ci interessano altre valute che lavorano con Scrypt, una scheda grafica decente tipo Nvidia o Radeon è l'unico requisito oltre al computer e ai software (no moduli esterni)

# Come fare mining

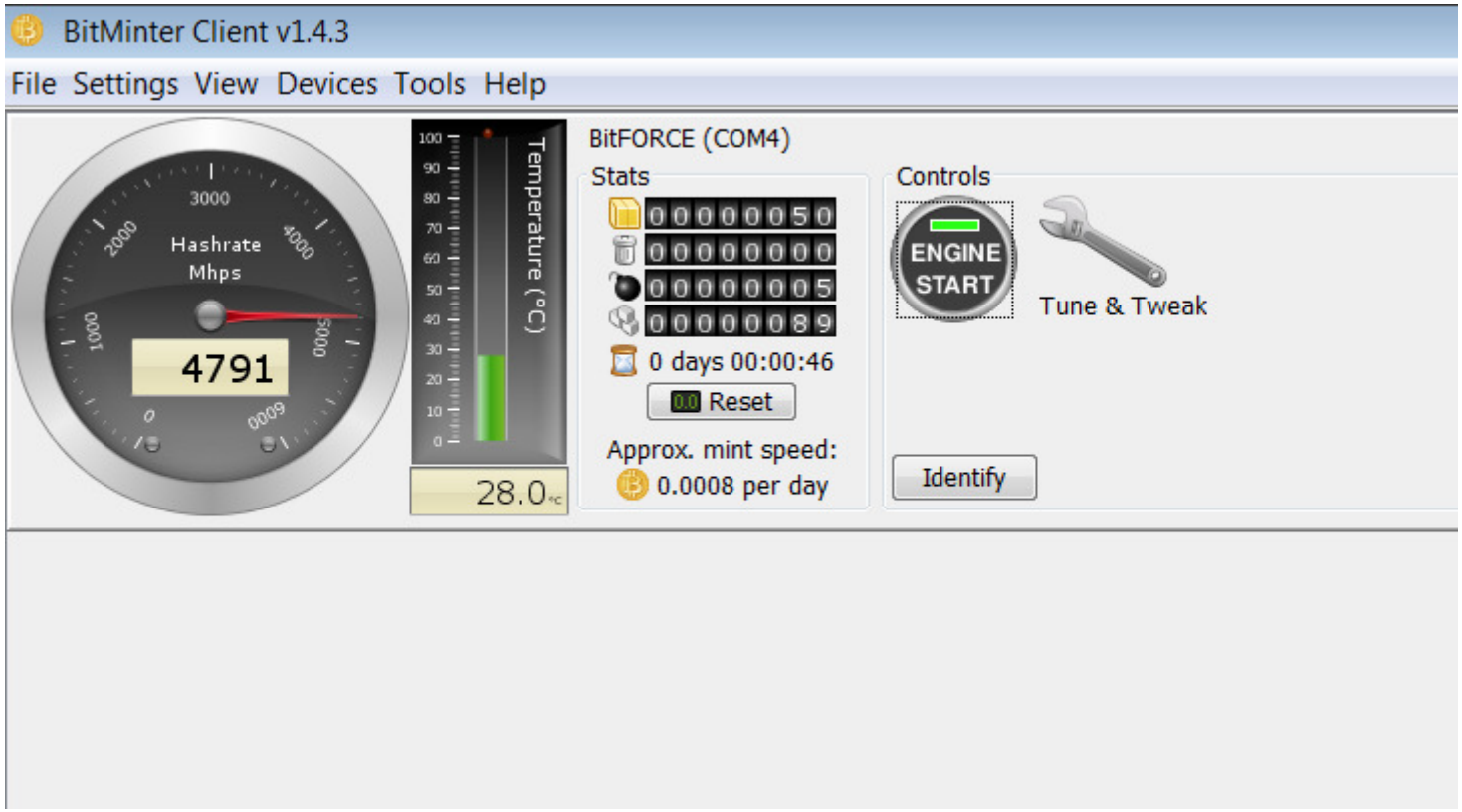
cgminer Sexcoin

```
cgminer version 3.1.0 - Started: [2014-02-13 08:03:16]
--------------------------------------------------------------------------------
(5s):58.63K (avg):56.77Kh/s | A:10323  R:180  HW:478  U:14.4/m  WU:43.9/m
ST: 1  SS: 0  NB: 1  LW: 23818  GF: 0  RF: 0
Connected to sxc.outhashed.com diff 2 with stratum as user SJimak3bmPYxjVBZ5Q49
Block: cd899f60db259872...  Diff:243K  Started: [08:03:15]  Best share: 35.3K
--------------------------------------------------------------------------------
[P]ool management [G]PU management [S]ettings [D]isplay options [Q]uit
GPU 0:                | 58.63K/56.77Kh/s | A:10323 R:180 HW:478 U:14.43/m I:11
--------------------------------------------------------------------------------

[2014-02-13 19:57:50] Stratum from pool 0 requested work restart
[2014-02-13 19:57:58] Accepted ec5c3104 Diff 3/2 GPU 0
[2014-02-13 19:57:59] Accepted 980671ce Diff 5/2 GPU 0
[2014-02-13 19:58:03] Stratum from pool 0 requested work restart
[2014-02-13 19:58:04] Accepted 4aa28c35 Diff 3/2 GPU 0
[2014-02-13 19:58:07] Stratum from pool 0 requested work restart
[2014-02-13 19:58:11] Accepted 1da7ed91 Diff 25/2 GPU 0
[2014-02-13 19:58:21] Accepted 93cd4c79 Diff 8/2 GPU 0
[2014-02-13 19:58:24] Accepted dcd7ef7a Diff 2/2 GPU 0
[2014-02-13 19:58:24] Accepted 4e278558 Diff 3/2 GPU 0
[2014-02-13 19:58:24] Accepted 030bfafa Diff 39/2 GPU 0
[2014-02-13 19:58:30] Stratum from pool 0 requested work restart
[2014-02-13 19:58:31] Accepted cca87d11 Diff 7/2 GPU 0
```

# Come fare mining

```
cgminer version 3.1.0 - Started: [2014-03-06 01:16:01]
--------------------------------------------------------------------------------
(5s):57.80K (avg):21.83Kh/s | A:758  R:2  HW:24  U:1.2/m  WU:20.2/m
ST: 2  SS: 0  NB: 620  LW: 3618  GF: 0  RF: 0
Connected to pool.teamdoge.com diff 16 with stratum as user djbatman.djbatman
Block: 0cfc847f7e5372e4...  Diff:69.7M  Started: [11:51:47]  Best share: 29.7K
--------------------------------------------------------------------------------
[P]ool management [G]PU management [S]ettings [D]isplay options [Q]uit
GPU 0:                | 57.75K/21.83Kh/s | A:758 R:2 HW:24 U:1.19/m I:11
--------------------------------------------------------------------------------

[2014-03-06 11:48:02] Accepted 5defd4cb Diff 16/16 GPU 0
[2014-03-06 11:48:32] Accepted c339dce0 Diff 42/16 GPU 0
[2014-03-06 11:49:08] Accepted de898c6d Diff 17/16 GPU 0
[2014-03-06 11:49:12] Accepted 299634d5 Diff 225/16 GPU 0
[2014-03-06 11:50:04] Stratum from pool 0 detected new block
[2014-03-06 11:50:32] Accepted f62e927f Diff 21/16 GPU 0
[2014-03-06 11:50:46] Accepted 7f444b3d Diff 18/16 GPU 0
[2014-03-06 11:50:49] Stratum from pool 0 detected new block
[2014-03-06 11:51:00] Accepted 41193acb Diff 180/16 GPU 0
[2014-03-06 11:51:03] Stratum from pool 0 detected new block
[2014-03-06 11:51:23] Accepted 3d7315a7 Diff 18/16 GPU 0
[2014-03-06 11:51:38] Accepted b3d9ff17 Diff 16/16 GPU 0
[2014-03-06 11:51:47] Stratum from pool 0 detected new block
```

# Come fare mining



BitMinter Client v1.4.3
File Settings View Devices Tools Help
GPU: GeForce GTX 560 Ti (#1)
Stats
Controls
Hashrate Mhps
0.04
00000000
00000000
00000000
00000003
0 days 00:01:00
Reset
Approx. mint speed:
0.0000 per day
ENGINE START
Tune & Tweak
8 CUs
Hashrate Mhps
4674
Temperature (°C)
33.0
BitFORCE (COM4)
Stats
Controls
00000198
00000000
00000011
00000290
0 days 00:02:57
Reset
Approx. mint speed:
0.0008 per day
ENGINE START
Tune & Tweak
Identify
Total: Sum of all devices
Stats
Controls
Hashrate Ghps
4.67
00000198
00000000
00000011
00000293
0 days 00:02:57
Reset
Approx. mint speed:
0.0008 per day
ENGINE START

# ATM e altri servizi

- Cosa posso fare con Bitcoin (oltre che lo speculatore) ;-) ?
- Alcuni negozi e locali fisici cominciano ad accettarlo in pagamento
- Da gennaio 2014 accettato su Ebay inglese (sezione annunci)
- Molti siti lo affiancano a metodi più tradizionali (lo aveva annunciato Mega.co.nz che però si appoggia ancora a Paypal, per gli account PRO)
- Esperimenti con ATM (bancomat) che consentono versamenti/prelievi/transazioni in Bitcoin, in USA e Asia
- bitboat.net (Bitcoin nelle ricevitorie/tabaccherie italiane del circuito ITB)
- Negozi di informatica e marketplace solo in Bitcoin

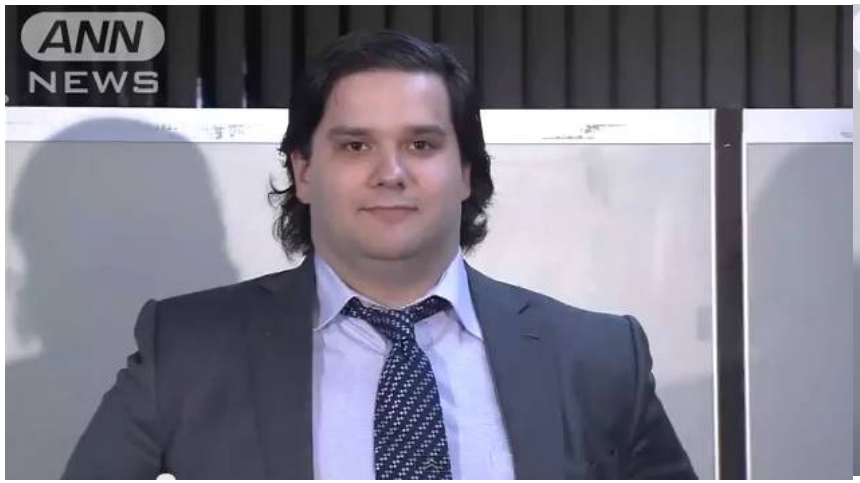
# ATM e altri servizi

# Anarcocapitalismo, monete improbabili & prospettive future

- L'anarchia è affascinante, ma un sistema del tutto anarchico sul lungo periodo non regge
- La situazione di caos attuale non mondo delle criptovalute è insostenibile ed è paragonabile a quella presente nel mondo della distribuzione musicale online intorno al 1999: ogni giorno spuntavano nuovi siti, formati e servizi; da quell'esperienza sono sopravvissute pochissime cose; altre che hanno preso il sopravvento sono invece nate addirittura 4-5 anni dopo il periodo di caos.
- Nonostante esistano già da alcuni anni, le criptovalute sono ancora giovanissime: è difficile prevedere se il futuro sarà del Bitcoin, o di altre "monete" simili

# Anarcocapitalismo, monete improbabili & prospettive future

- Gli eventi degli ultimi giorni (il tracollo di "banche" ed exchange come Tibanne/Mt.Gox e Flexcoin) stanno dando una battuta d'arresto almeno momentanea al Bitcoin, e uno spostamento verso alternative.



# Anarcocapitalismo, monete improbabili & prospettive future

- Iniziative come DogeCoin, Sexcoin, Nyancoin e altre, al di là dell'aspetto pittoresco che diverte pubblico e stampa e delle possibili speculazioni già in essere su alcune di queste criptovalute, sul medio-lungo periodo si riveleranno impraticabili, specie in un mondo in cui è lentamente in corso un processo di unificazione monetaria in diverse aree (zona Euro, Nordamerica, Cina-Giappone, Africa)
- Potrebbero sopravvivere solo alcune di queste, per caratteristiche intrinseche, ma finirebbero per diventare più una sorta di token/coupon per ottenere maggiore anonimato, che una moneta a parte (es. Sexcoin per un sito per adulti)

# Bibliografia minima


- Tony “Merc” Mobily: Bitcoin: io mi fido, tu ti fidi, noi ci fidiamo http://www.olografix.org/bitcoin-io-mi-fido-tu-ti-fidi-noi-ci-fidiamo-by-merc-metro-olografix/
- Dennis Jaromil Rojo: Bitcoin, the end of the taboo on money: http://www.dyndy.net/2013/04/bitcoin-ends-the-taboo-on-money/
- In italiano: Bitcoin, la fine del tabù della moneta http://quaderni.sanprecario.info/2014/01/bitcoin-la-fine-del-tabu-della-moneta-di-denis-jaromil-roio/
- http://Bitcoin.org
- https://litecoin.org