

# WHAT IS (AND CAN BE) BITCOIN

Jaromil @ dyne.org

DYNDY.net - Freecoin.ch - BitcoinConsultancy.com

Free Software Day 2011, Amsterdam Science Park, CWI

# OUTLINE

- 1 TRANS-MODERNISM
- 2 BITCOIN
- 3 CONCLUSIONS
- 4 BUZZING IN AMSTERDAM
- 5 REFERENCES

## INCIPIT

*The most powerful forces, those that interest us the most, are not in a specular and negative relation to modernity, to the contrary they move on transversal trajectories. On this basis we shouldn't conclude that they oppose everything that is modern and rational, but that are engaged in creating new forms of rationality and new forms of liberation.<sup>1</sup>*

*We can't imagine to enter the Information Age without changing the fundamental and most used communication tool: Money.<sup>2</sup>*

---

<sup>1</sup>Negri and Hardt, 2010

<sup>2</sup>Bernard Lietaer, 2005

# COMMONS AND THEIR ABSTRACTION

The financial system is a complex machine to **represent** affect, values, interests and nature into an abstract game.



Finance works by **abstraction**, hence the importance of mathematical models. Nevertheless the possibility of producing abstractions resides in the **social nature** of richness being represented.

The power of abstraction is rooted in the commons, while at the same time it mystifies them.

# MONEY AS MEDIA

*Is most important to connect the growth of the financial system with the parallel growth of biopolitical production. As biopolitical work becomes autonomous, finance becomes the most appropriate capitalist instrument for external expropriation of the commons, operating in a condition of **radical abstraction** from production processes.* <sup>3</sup>

*Money is the purest reification of means, a concrete instrument which is absolutely identical with its abstract concept; it is a **pure instrument**. The tremendous importance of money for understanding the basic motives of life lies in the fact that money embodies and sublimates the practical relation of man to the objects of his will, his power and his impotence; one might say, paradoxically, that **man is an indirect being**.* <sup>4</sup>

---

<sup>3</sup>Negri and Hardt, 2010

<sup>4</sup>Simmel, 1900

# BITCOIN MANIFESTO

A mail excerpt ended up being called the Bitcoin Manifesto..

- Emerging technologies can have bad taste
- The end of **flow capitalism**
- Horizontal framework for networks of trust
- Way out of revenue stagnation
- Digital immanence

# P2P TRANSACTIONS

Bitcoin is a **digital born currency**: a finite resource which is algorithmically limited to 21 million units (8 floating point digits) and is therefore comparable to precious minerals like gold.

Bitcoins are exchanged via **peer to peer** software applications. When executed on a computer connected to the Internet they can authenticate transactions of sums between digital wallets, **without relying on end user trust**.

# MINERS

- A bitcoin miner uses computing power for the generation of bitcoins
- To **mine coins** basically consists in a simple trial-and-error algorithm
- Mining consolidates the authenticity of the whole network

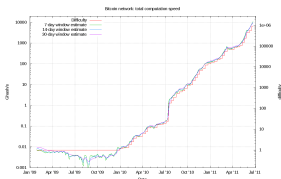


FIGURE: Mining difficulty grows proportionally to the quantity in circulation

# PSEUDONYMS

- Node on the network can generate new “addresses” to sign transactions
- The generation of such addresses is unlimited and unconditioned
- Every node has a history of all transactions taking place

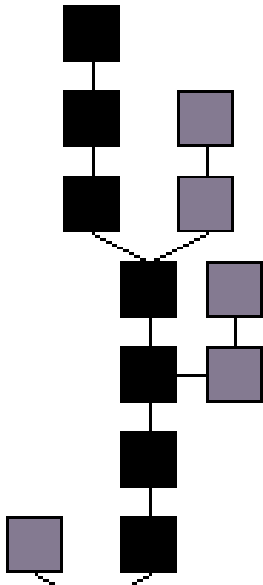
This makes the bitcoin network **pseudonymous** and not anonymous.

# BLOCKCHAIN

- Sequential identifiers
- Timestamped list of all known transactions

A block-chain contains the cryptographic ownership history of (all) coins from their creator-address to their current owner-address. Therefore, if a user attempts to reuse coins he already spent, the network rejects the transaction.

# BLOCKCHAIN



# GENESIS BLOCK

## The pszTimestamp

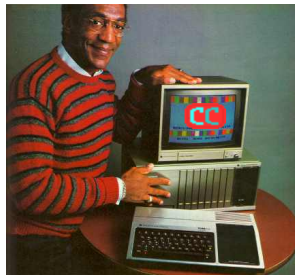
- Main net:

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”

- Weeds:

“York Times 26/Apr/11 The question is, what is the exchange of the future? said Richard Repetto, an analyst at Sandler O’Neill”

Namecoin, Freecoin, Multicoins, Witcoin, Cosbycoin... :)



“CosbyCoin.. It's the FUTURE”

# USER INTERFACE

Bitcoin communicates using JSON serialization with the GUI and using IRC (over TCP/IP) with other nodes



FIGURE: RPC JSON per i client e messaggi IRC in WAN

# DEPENDENCIES

All protected under MIT licensing

- Statiche
  - CryptoPP (Wei Dai)
  - Json Spirit (Wilkinson)
- Dinamiche
  - Boost (system, FS, prog. options, thread)
  - OpenSSL
  - libCrypto
  - Berkeley DB<sup>5</sup>
  - GThread (GLib)
  - MiniUPNP (opzionale)
  - WX (GUI opzionale<sup>6</sup>)

---

<sup>5</sup>libDB 4.7 nei binari distribuiti, sara' 4.8 in bitcoin 0.4

<sup>6</sup>solo WX 2.9.1 o ancora meglio ultima versione in GIT

# API RPC

- `getaccount <bitcoinaddress>`
- `getaccountaddress / getaddressesbyaccount`
- `getbalance [account]`
- `getnewaddress [account]`
- `getreceivedbyaccount / getreceivedbyaddress`
- `gettransaction <txid>`
- `getwork [data]`
- `move / sendfrom / sendtoaddress / validateaddress`
- `setaccount <bitcoinaddress> <account>`
- `setgenerate <generate> [genproclimit]`

`getblockcount, getblocknumber, getconnectioncount, getdifficulty,`  
`getgenerate, gethashespersec, getinfo, listaccounts, listreceivedbyaccount,`  
`listreceivedbyaddress, listtransactions`

# PROBLEMS

- The C++ code is not documented, shows some early planning but has grown chaotically
- The **WX GUI** uses binary linkage instead of the new GUI design based on JSON RPC
- The **Berkeley DB** handles different versions of databases in a non portable way
- The wallet is preserved in clear, password inputs is not secure, users are left alone to organize their security
- The majority of algorithms consist in binary arithmetics and aren't well portable (LE)

# DEVELOPMENT

- Lower storage needs: Merkle tree
- Lower I/O needs
- Intuitive storage security
- Code cleanup/rewrite and documentation
- Service applications (Intersango)
- Community applications (Witcoin, DYNDY's CULTOS...)

# USEFULNESS

## Which advantages are brought by bitcoin?

- Open the financial status-quo to new actors
- Acceleration of micro-payments and donations
- Lighter infrastructure
- Network neutrality
- Tax Innovation

# COLLATERAL EFFECTS

## What worries?

- End of another State monopoly (neo-liberism or anarchy?)
- Increased deregulation of markets and financial products
- Potential alienation of local economies
- Security depends more on user habits
- Immature software

# WHAT'S COOL (IMHO)

- Content syndication: Witcoin <http://www.witcoin.com>
- Naming system: Namecoin <https://en.bitcoin.it/wiki/Namecoin>
- Real world traders: <https://en.bitcoin.it/wiki/Trade>
- The community

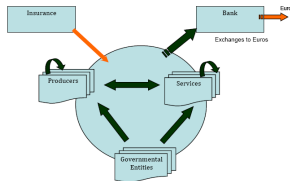
# SHARING THE PRODUCTION MEANS



<http://Freecoin.ch>

- Experiments beyond the specific Bitcoin currency
- New complementary and alternative currencies
- Open the possibility to create new value systems
- New opportunities for emerging constituencies
- Monetary rhizome and diversity (resiliency vs. efficiency)

# INTEGRATION OF C3 AND P2P CURRENCY



- Money as a glue for communities
- Labor as commons
- Shared resources
- CULTOS  
A DYNDY project for a Cultural Credit Circuit in the Netherlands
- Moneylab.eu  
Coming up... get in touch!

Some books referred in this speech:

- Negri, Hardt (2010) “Comune. Oltre il privato e il pubblico”
- Lietaer, B. (2007) “Of Human Wealth: Beyond Greed and Scarcity”
- Arvidsson, A. (2011) “General Sentiment: how value and affect converge in the information economy”
- Simmel, G. (1900) “Philosophie des Geldes”
- Foucault, M. (1979) “Cours au Collège de France 1978-1979”
- Nakamoto, S. (2009) “Bitcoin: A Peer-to-Peer Electronic Cash System”
- Ijiri, Y. (1993), “Variance analysis and triple-entry bookkeeping”