ICC ITALIA
INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

Bitcoin and Blockchain Technology

Ferdinando M. Ametrano

Politecnico di Milano, Milano-Bicocca University

ICC Italia Conference, Rome, November 10, 2016

ferdinando@ametrano.net

@Ferdinando1970

http://www.slideshare.net/Ferdinando1970

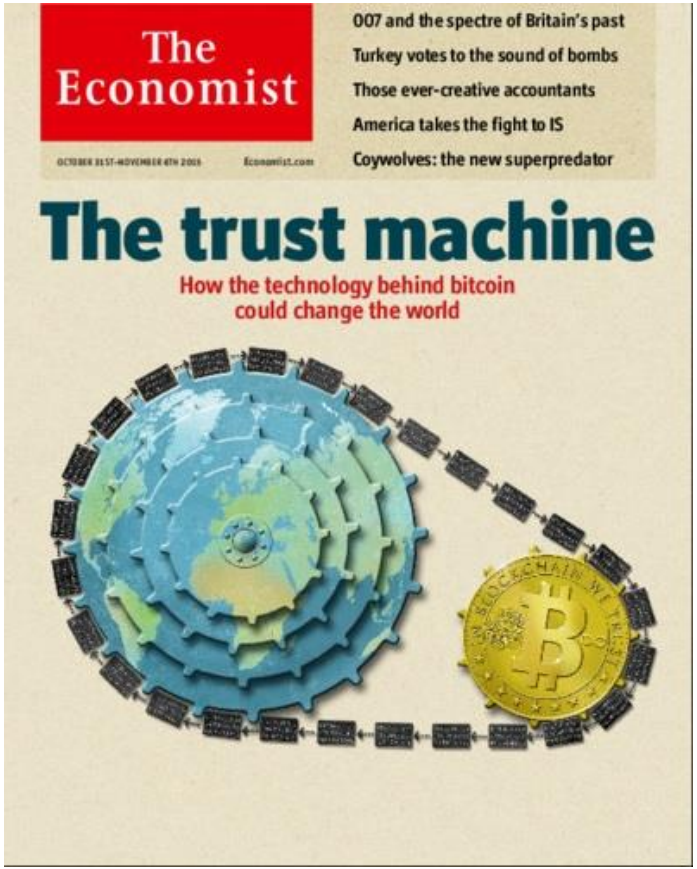
https://it.linkedin.com/in/ferdinandoametrano

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

POLITECNICO MILANO 1863

Really?

"Blockchain – not bitcoin – will prove revolutionary in banking"



http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

Bitcoin in 2014 Is Like Internet in 1994: Weird and Scary

Marc Andreessen: American entrepreneur, investor, and software engineer.
Coauthor of Mosaic, cofounder of Netscape

https://twitter.com/pmarca/status/677658844504436737

The Walled Garden Model

- Controlled access to web content and services
- Offered in the late ‘90s and early ‘00s by Compuserve, AOL (and to some extent MSN)
- Corporates wanted to go online, but not in the wild unregulated internet, populated by anonymous agents
- They eventually realized that perceived risks, which are real, are outweighed by benefits

Understanding Lags Well Behind The Hype

Understanding of the technology however lags well behind the hype, amongst practitioners, policy makers and industry commentators alike. 'Blockchain' technology seems to promise major change for capital markets and other financial services – some say it may ultimately prove to be as important an innovation as the internet itself – but few can say exactly how or why.

Michael Mainelli, Alistair Milne (2016)
The Impact and Potential of Blockchain on the Securities Transaction Lifecycle
http://ssrn.com/abstract=2777404

Why Bitcoin Is Hard To Understand

At the crossroads of:

1. Game theory
2. Cryptography
3. Computer networking and data transmission
4. Economic and monetary theory

Mainly not a technology,
a cultural paradigm shift instead

What is The Blockchain?

[A hash pointer linked list of blocks]

- An append-only sequential data structure
- New blocks can only be appended at the end of the chain
- To change a block in the middle of the chain, all subsequent blocks need to be changed
- Very inefficient compared to a relational database

Blockchain:
A Distributed Transaction Ledger

- Every block contains multiple transactions
- Massively duplicated across network nodes
- Shared with a P2P file transfer protocol
- Updated by peculiar nodes, known as *miners,* appending new blocks of transactions

A Distributed Back-office

- All network nodes perform transaction validation and clearing.
- Miners perform the additional work required for settlement. How do they reach consensus on the transaction history?
- Consensus in a distributed network with faulty (or malicious) nodes is a very hard problem known as Byzantine General Problem

Distributed Consensus

- Nakamoto reaches consensus using (game theory) economic incentive for the mining nodes to be honest
- Miners are compensated for their *proof-of-work* using seigniorage revenues, i.e. with issuance of new bitcoins

Blockchain Without Bitcoin

Does it make sense?

No bitcoin

➡ No asset available to reward miners

➡ Appointed validator officials required

Why should validators use a blockchain,

i.e. a subpar data structure, instead of a database?

Blockchain Needs A Native Digital Asset

https://www.finextra.com/videoarticle/1241/blockchain-needs-a-native-digital-asset

Blockchain needs a native digital asset

01 June 2016 | 16619 views

Ferdinando Ametrano, Head of Blockchain and Virtual Currencies, Intesa Sanpaolo, discusses the relationship between bitcoin and blockchain, and outlines how banks can stay ahead of this evolving landscape.

What is Bitcoin?

bitcoin is the native digital asset,
tracked by the first (and most relevant so far) blockchain

- It exists only as scriptural asset, i.e. validated transaction recorded on the blockchain
- It is a bearer instrument: the (private key) holder is the actual effective owner

What Makes Bitcoin Special?

- It is scarce in digital realm, as nothing else before
- It can be transferred but not duplicated
- (i.e. it can be spent, but not double-spent)

Bitcoin is digital gold: this is the brilliant groundbreaking achievement by Satoshi Nakamoto

Bitcoin as (Digital) Gold in the History of (Crypto)Money

gold

- Its adoption was not centrally planned
- For centuries it has been the most successful form of money
- It has bootstrapped all monetary systems we know of
- It has been surpassed by other kind of money without becoming obsolete

bitcoin

- Its adoption has not been centrally planned
- It is the most successful form of cryptocurrency
- It will bootstrap new monetary systems
- It might be surpassed by more advanced type of cryptocurrencies without becoming obsolete

Explain Money To An Alien

fiat money

- No intrinsic value (legal tender, social contract)
- Currency based on paper/ink security
- Discretionary governance
- Wicksellian interest-rate approach

bitcoin

- No intrinsic value (digital gold)
- Currency based on math/cryptographic security
- Algorithmic governance
- Deterministic supply

Blockchain Transactional Economy

- Bitcoin is the only blockchain asset
- Everything else tracked with blockchain technology is somebody's liability

the same is true for other native digital assets (ethereum, litecoin, etc.) of less secure blockchains

A healthy digital transactional economy requires
a native digital asset
to be used for payment and collateral;
it makes no sense to only have liabilities!

Blockchain Without Bitcoin: No Blockchain Beyond Bitcoin: Yes

- 1992: email was the killer Internet app
- Impossible to imagine Google, Facebook, Amazon

- 2016: bitcoin is the killer Blockchain app
- More ambitious apps will be built on blockchain, but they have not been really imagined yet, and they will need a native digital asset

Time-stamping and Notarization

- A generic data file can be hashed to producing a short unique identifier, equivalent to its digital fingerprint.
- Such a fingerprint can be associated to a bitcoin transaction (irrelevant amount) and hence registered on the blockchain
- Blockchain immutability provides non-repudiable time-stamp, proving the existence of the data file in that specific status at that moment in time
- This generic process is even undergoing some standardization to achieve third party auditable verification: broker-dealers could use it to satisfy regulatory prescriptions

Anchoring: A New Security Paradigm

- Bitcoin blockchain network security is preserved by a computation power unparalleled in human history
- Other transactional networks can tap into this security via *anchoring* (i.e. periodic time-stamping of the network status)
- Bitcoin miners as global outsourced decentralized security of the future

Other Blockchain Use Cases

OK: applications based on cryptographic proofs and digital IDs [not really blockchain]

As for the rest, it is basically hype. Questions always to be answered:

- Can be achieved with a database?
- What consensus is required? (distributed, bilateral, centralized)
- What kind of security is required: preventive, detective, or corrective? (ok / yes today, probably not in the future/ no)

- Blockchain is absolutely not suited for storing large amount of data

The Shifting Narrative

2014 bitcoin

2015 blockchain technology (Economist)

2016 distributed ledgers

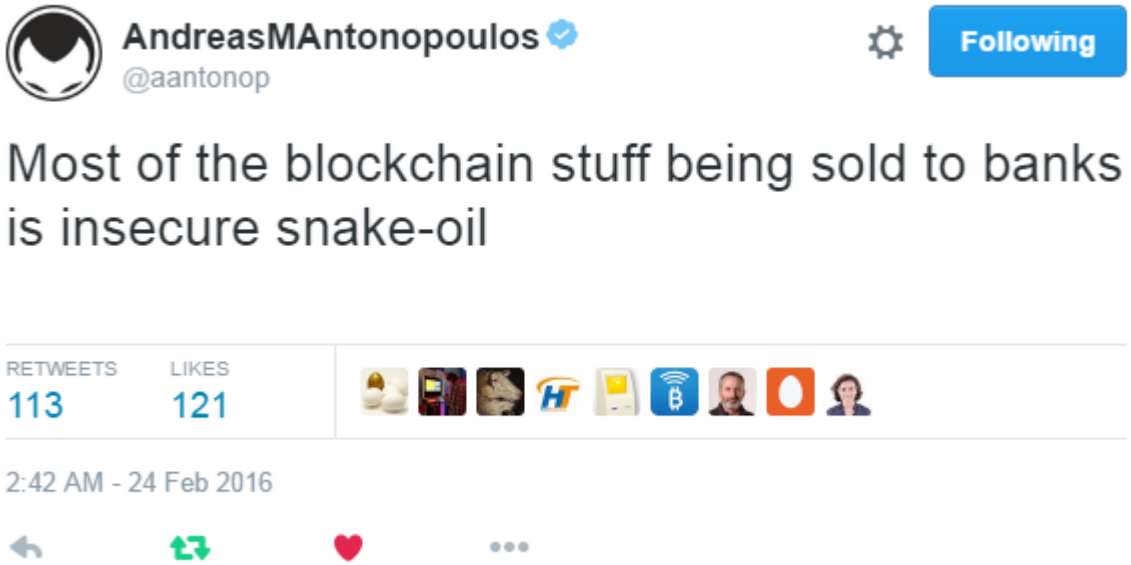
2017 *bilateral DB + secure messaging + cryptographic proofs*

2018 *bitcoin, again!*

Insecure Snake-Oil Sold To Bank

Andreas Antonopoulos: technologist, serial entrepreneur, one of the most well-known and well-respected figures in the bitcoin ecosystem

https://twitter.com/aantonop/status/702307516739428353



R3 Corda

http://r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services

- R3 was originally touted as "*a project intended to bring blockchains to finance*"
- Its Distributed Ledger Group is developing a proprietary platform, named Corda: "*Corda is a distributed ledger platform […] we are not building a blockchain*"
- A revamped SWIFT secure messaging protocol on cryptographic proof & bilateral ledger steroids?

Why is finance fascinated with blockchain?

Blockchain transactions are immediately validated and cleared, then settled shortly thereafter, automatically without a central authority

- In the financial world, cash transactions only are cleared and settled automatically without a central authority

Consensus by reconciliation

- Financial transactions that take milliseconds to execute, clear and settle in days
- Not a technological problem
- Consensus by reconciliation of multiple independent ledgers: a *checks and balances* system that allows for prescriptions, corrections, and restrictions

Instant Settlement

- Instant settlement would reduce liquidity making leverage, short selling and netting almost impossible
- Instant settlement (e.g. for payments) has costs: who should pay for them?
- Cash-on-the-ledger is imperative for Delivery vs Payment

Cash on the Ledger

- Central bank digital currency is problematic: *[… it] is appealing […] it would mean people have direct access to the ultimate risk-free asset [...] it could exacerbate liquidity risk by lowering the frictions involved in running to central bank money [...] it could fundamentally and perhaps abruptly re-shape banking.*

  Mark Carney, Governor of the Bank of England, June 2016

  http://www.bankofengland.co.uk/publications/Documents/speeches/2016/speech914.pdf
- IMF sponsored blockchain tokens might replace Special Drawing Rights: unrealistic as it would severely undermine US dollar predominance
- A free instantaneous P2P payment network is a great opportunity for retail banks (probably worth a consortium)

Single Shared Data Set

- Single data source, avoiding reconciliation
- Without a central governing node how to manage priorities between conflicting updates? Which consensus model?
- Bilateral consensus? Really?!?!?
- Central governance: back to DB admin
- What if the single authoritative data source is hacked? Which reference can be used to fix it?

Improved Automation: Smart Contracts

- The DAO (decentralized autonomous org): the main Ethereum project, it raised >$160m as leaderless Venture Capital
- *The terms of The DAO are set forth in the smart contract code […] Nothing […] may modify or add any additional obligations or guarantees beyond those set forth in The DAO's code*
- Based on its self-executing nature an agent diverted about $50m from The DAO to its own child-DAO start-up
- If code is law, then this is not a theft: it is a feature
- Beware of extreme automation

Conclusions

Thank You

- Blockchain needs a native digital asset such as bitcoin;
- Bitcoin is digital gold and can be as relevant as physical gold for the history of money, finance, and civilization
- See F. Ametrano, “Hayek Money” https://ssrn.com/abstract=2425270
- Time-stamping and anchoring are promising applications
- Unrealistic expectations arise from distributed ledger hype: no reference implementation has emerged yet
- Instant settlement, cash on the ledger, shared data set, and improved automation are not easy to obtain
- Hardly disruptive, DLT might be evolutionary database technology
- See F. Ametrano “Bitcoin, Blockchain, and DLT” http://ssrn.com/abstract=2832249