

About Bitcoin And Blockchain: A Cultural Paradigm Shift

Ferdinando M. Ametrano
Milano-Bicocca University

ferdinando@ametrano.net

<https://onename.com/nando1970>

<https://speakerdeck.com/nando1970>

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

Bank of Italy, Rome, June 21, 2016

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 crossroad 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*

Table of Contents

- 1. Blockchain needs a native digital asset**
2. Decentralized transactional economy
3. Money without Caesar's stamp of approval
4. The regulatory challenges
5. Banks: competition and opportunities

Really?

*“Blockchain –
not bitcoin –
will prove
revolutionary
in banking”*

1 2 3 4 5



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

Bitcoin Today 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>

 **Marc Andreessen** 
@pmarca  **Following**

Big companies desperately hoping for blockchain without Bitcoin is exactly like 1994: Can't we please have online without Internet??



RETWEETS 988 LIKES 983



2:17 AM - 18 Dec 2015



Ferdinando Ametrano 2016

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

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 using a P2P file transfer protocol
- Updated by peculiar “miner” nodes, appending new blocks of transactions

A Distributed Back-office

- All network nodes perform transaction validation
- The nodes willing to clear and settle transactions , called *miners*, perform additional work
- How do miners reach consensus on the transaction history?
- Consensus in a distributed network with faulty (or malicious) nodes is a very complex problem known as Byzantine General Problem (BGP)

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

What is Bitcoin?

*bitcoin is the native digital asset
of the first (and most relevant so far) blockchain*

- It exists only as scriptural asset, i.e. validated transactions 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

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

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 | 13809 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.

Blockchain Needs A Native Digital Asset

- All existing blockchains are based on a native digital token (bitcoin, ether, Ripple XRP, etc.)
- “Blockchain without bitcoin” is a technological chimera looking for a problem to solve
- Many proposed blockchain applications are actually (just) cryptographic applications

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?*

The Shifting Narrative

2014 bitcoin

2015 blockchain technology

2016 distributed ledgers

2017 *bilateral DB + secure messaging +
cryptographic proofs*

2018 *bitcoin, again!*

Blockchain Beyond Bitcoin

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

<https://twitter.com/aantonop/status/701925047632535552>

 **AndreasMAntonopoulos** 
@aantonop  **Following**

Blockchains far beyond currency - Yes, you understand correctly
Blockchains without currency - No, you misunderstood blockchains

RETWEETS 70 LIKES 79



1:22 AM - 23 Feb 2016



Ferdinando Ametrano 2016

The Blockchain Promise

- 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

(Bitcoin) Blockchain Use Cases

- OK: time-stamping, anchoring (data certification using tamper-evident validation), and notarization services
- OK: cryptographic proofs and digital IDs

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 / maybe / no)
- Blockchain is absolutely not suited for storing large amount of data

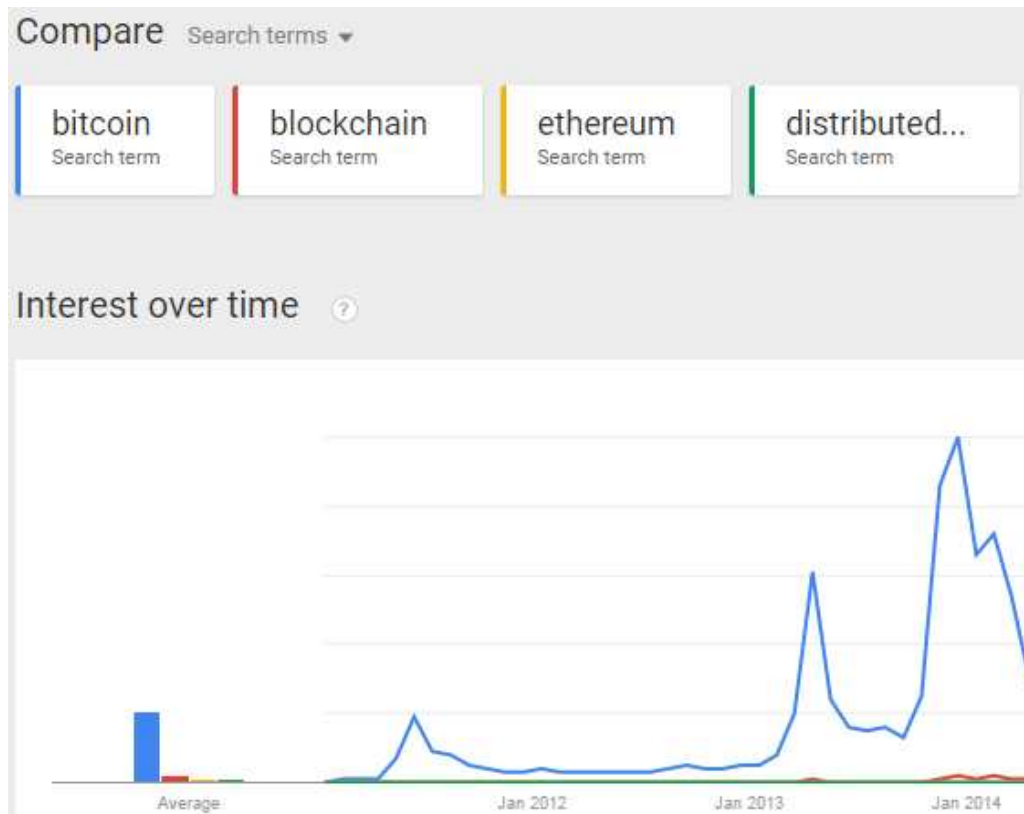
Is Bitcoin The Definitive Native Digital Asset

might not be bitcoin

- will be encryption-based
- will preserve privacy
- will be the evolution and optimization of the bitcoin model

might be bitcoin!

Bitcoin: the Leader in Search Interest and Market Cap



| | | |
|------------------------------|------------------|--------|
| Total | \$13.697.626.962 | 100,0% |
| Bitcoin | \$11.920.111.988 | 87,0% |
| Ethereum | \$ 989.073.390 | 7,2% |
| Litecoin | \$ 259.033.488 | 1,9% |
| Ripple | \$ 238.883.376 | 1,7% |
| The DAO | \$ 92.675.039 | 0,7% |
| Dash | \$ 52.759.141 | 0,4% |
| NEM | \$ 42.208.290 | 0,3% |
| Lisk | \$ 36.623.100 | 0,3% |
| Dogecoin | \$ 34.940.577 | 0,3% |
| MaidSafeCoin | \$ 31.318.573 | 0,2% |

Table of Contents

1. Blockchain needs a native digital asset
- 2. Decentralized transactional economy**
3. Money without Caesar's stamp of approval
4. The regulatory challenges
5. Banks: competition and opportunities

Bitcoin as value transfer protocol

- 7+ years up and running; whoever may crack its security:
 - would collect a multi-billion USD bounty
 - would enjoy world-wide fame
- The bitcoin protocol could be improved
- Even bitcoin core-devs are working at such improvements, but consider bitcoin replacement unfeasible
- TCP/IP is inefficient at streaming but impossible to replace: throw bandwidth at it and live happily ever after

Permissionless Innovation

Fast and Effective

- No centralized security mechanism, no barrier to enter, no editorial control
 - Email has not been designed by a consortium of postal agencies
 - Internet has not been developed by a consortium of telcos
- Will a decentralized transactional economy be shaped by a consortium of banks?

The Information Economy



- Data is transferred with zero marginal cost
- Why pay a fee to move bytes representing wealth?
- Why only 9-5, Monday-Friday?
- Who (and when) will gift humanity with a global instantaneous free p2p payment network?

Bitcoin:

Money For The Information Economy

- Decentralized: no authority
- Permissionless: no regulator
- Censorship resistant: no frozen funds
- Open-access: no discrimination, no amount limits, 24/7, 365 days
- Free: negligible transaction costs
- Borderless: no geographic limits
- Transnational: no specific jurisdiction applies
- Secure: non falsifiable, non repudiable transactions
- Resilient: nothing has been able to stop it or break it

Internet as Transactional Agora

- Internet today:
 - Permissionless access to communication
 - Permissionless content creation and fruition
- Being added right now:
 - Permissionless ability to transact

A New Security Paradigm

- Bitcoin blockchain network security is preserved by a computation power unparalleled in human history
- All transactions are validated by everybody
- This power is available through *anchoring* (and maybe *merge mining*) to other transactional networks
- Bitcoin miners might become the global outsourced decentralized security of the future

Table of Contents

1. Blockchain needs a native digital asset
2. Decentralized transactional economy
- 3. Money without Caesar's stamp of approval**
4. The regulatory challenges
5. Banks: competition and opportunities

Money As A Social Relation Instrument

- Human beings are born into a gift economy
- Enlarged relationship circle requires exchange economy
- Barter economy: coincidence of wants
- Trade economy: money as medium of exchange
- Global information economy: supranational digital money

From gold standard to fiat money

- Gold: the commodity money standard
 - resistance to corrosion and oxidation
 - high malleability
 - relative ease of purity assessment
 - Pleasant color
- Gold purity certification
- Representative money
- Fractional receipt money
- *Fiat* money and legal tender

Friedrich August von Hayek

Denationalisation of Money

- history of coinage is an almost uninterrupted story of debasements; history is largely a history of inflation engineered by governments for their gain
- why government monopoly of the provision of money is regarded as indispensable? It deprived public of the opportunity to discover and use a better reliable money

Blessed will be the day when it will no longer be from the benevolence of the government that we expect good money but from the regard of the banks for their own interest

A Free-Market Monetary System, Gold and Monetary Conference, New Orleans, Nov. 1977, <https://mises.org/daily/3204>
Hayek, F. A., Denationalisation of Money, The Institute of Economic Affairs, <http://www.mises.org/books/denationalisation.pdf>

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

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

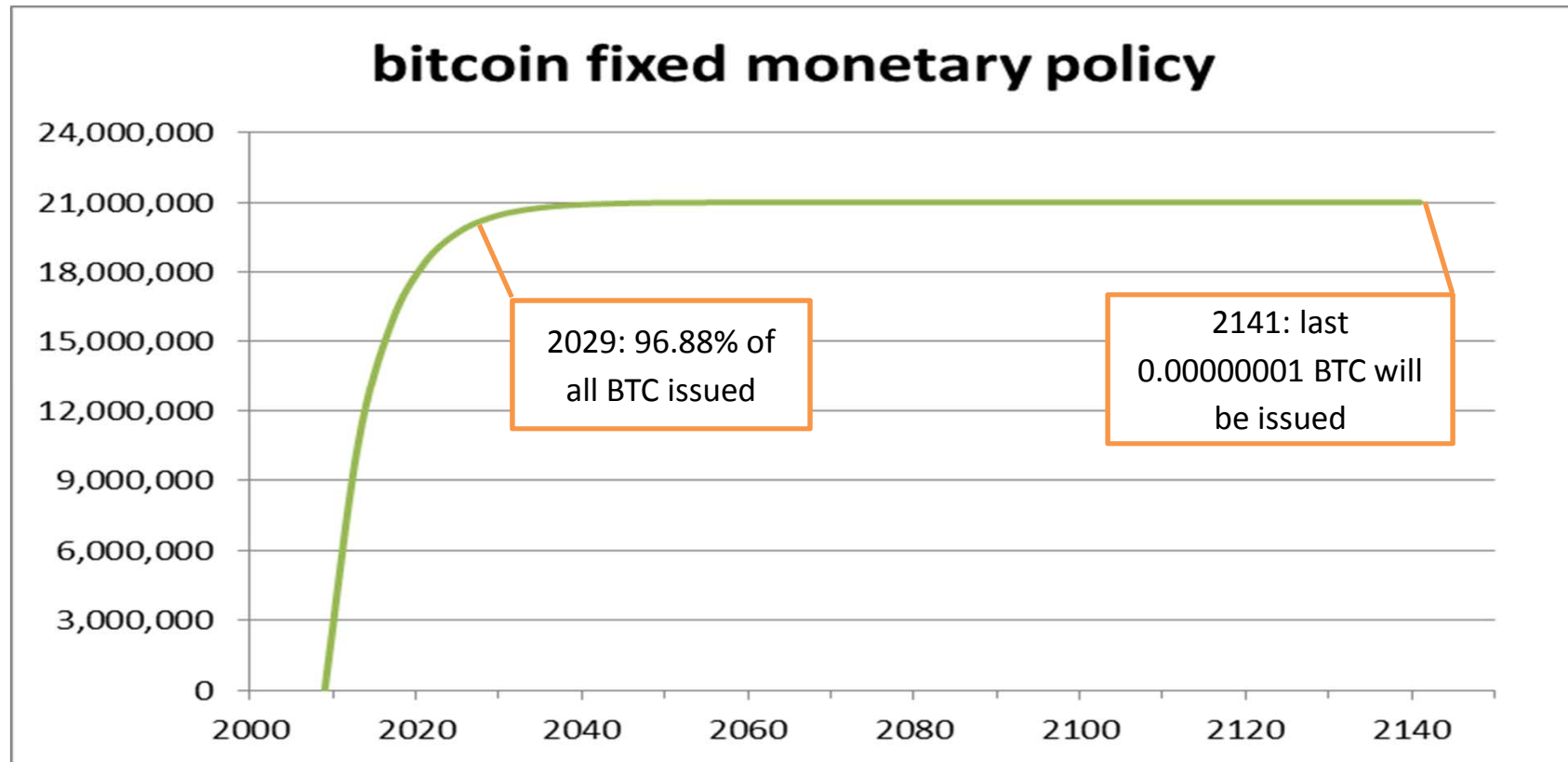
gold

- Its adoption was not centrally planned
- For centuries gold 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

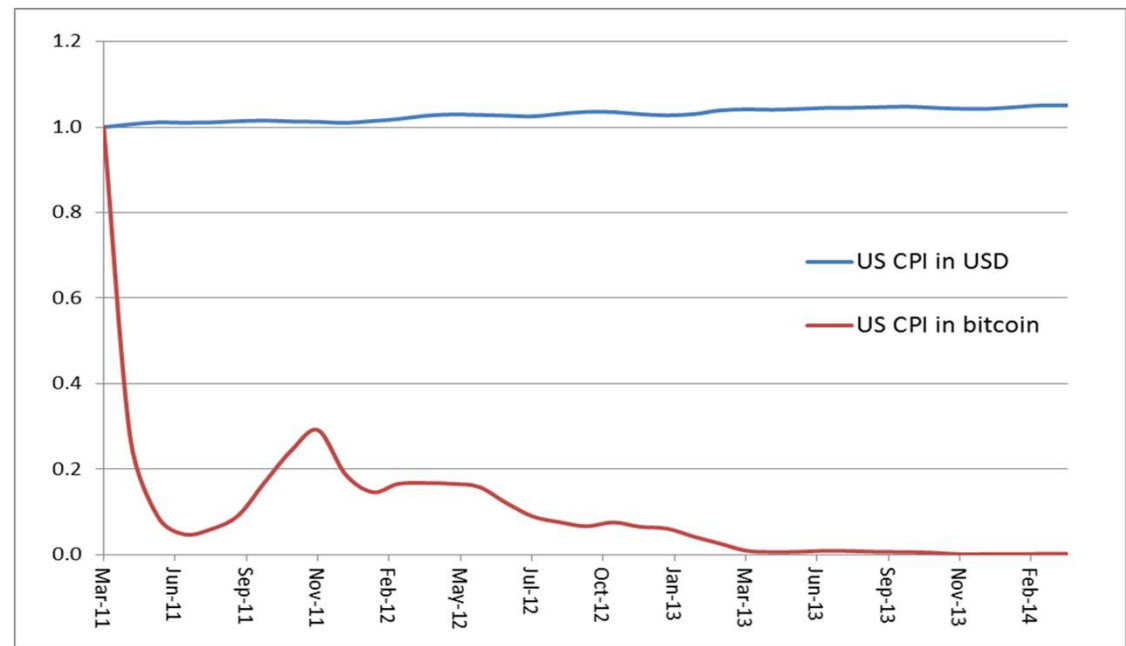
- Its adoption has not been centrally planned
- Bitcoin is the most successful form of cryptocurrency
- It will bootstrap new monetary systems
- It might be surpassed by more advanced type of cryptocurrencies without becoming obsolete

Inelastic Money Supply: Deterministic Decreasing Rate



Statement of the bitcoin problem

- successful at getting rid of a centralized monetary authority, it has given up the flexibility of an elastic supply of money
- no salaries, no mortgages, no stable purchasing power



Next Generation of Cryptocurrencies: Hayek Money

- The cryptocurrency monetary standard of elastic non-discretionary supply regulated to achieve stable prices with respect to a (commodity) price index

(2014) *Hayek Money: the Cryptocurrency Price Stability Solution*

<http://ssrn.com/abstract=2425270>

- A Reserve Bank DAO (decentralized autonomous organization) using bitcoin as reserve asset for a stable coin, with seigniorage shares absorbing profit/loss

(2016) *Price Stability Using Bitcoin as Reserve Asset*

<http://ssrn.com/abstract=2508296>

Table of Contents

1. Blockchain needs a native digital asset
2. Decentralized transactional economy
3. Money without Caesar's stamp of approval
- 4. The regulatory challenges**
5. Banks: competition and opportunities

Bitcoin for Money Laundering

UK HM Treasury: *The money laundering risk associated with digital currencies is low, though if the use of digital currencies was to become more prevalent in the UK this risk could rise*

<https://www.gov.uk/government/publications/uk-national-risk-assessment-of-money-laundering-and-terrorist-financing>

Table 1.A: National risk assessment on money laundering

| National risk assessment on money laundering | | | | | | |
|--|-----------------------------|------------------------|-----------------|-----------------------|------------------------------|--------------------|
| Thematic area | Total vulnerabilities score | Total likelihood score | Structural risk | Structural risk level | Risk with mitigation grading | Overall risk level |
| Banks | 34 | 6 | 211 | High | 158 | High |
| Accountancy service providers | 14 | 9 | 120 | High | 90 | High |
| Legal service providers | 17 | 7 | 112 | High | 84 | High |
| Money service businesses | 18 | 7 | 119 | High | 71 | Medium |
| Trust or company service providers | 11 | 6 | 64 | Medium | 64 | Medium |
| Estate agents | 11 | 7 | 77 | Medium | 58 | Medium |
| High value dealers | 10 | 6 | 56 | Low | 42 | Low |
| Retail betting (unregulated gambling) | 10 | 5 | 48 | Low | 36 | Low |
| Casinos (regulated gambling) | 10 | 3 | 32 | Low | 24 | Low |
| Cash | 21 | 7 | 147 | High | 88 | High |
| New payment methods (e-money) | 10 | 6 | 60 | Medium | 45 | Medium |
| Digital currencies | 5 | 3 | 15 | Low | 11 | Low |

Bitcoin used by terrorists

Europol: Despite third party reporting suggesting the use of anonymous currencies like bitcoin by terrorists to finance their activities, this has not been confirmed by law enforcement

https://www.europol.europa.eu/sites/default/files/publications/changes_in_modus_operandi_of_is_in_terrorist_attacks.pdf

Avoid Stifling Innovation

- New York Department of Financial Services: *strike an appropriate balance that helps protect consumers and root out illegal activity, without stifling beneficial innovation*
<http://www.dfs.ny.gov/about/press/pr1407171.htm>
- EU Parliament: *to avoid stifling innovation, we favour precautionary monitoring rather than pre-emptive regulation*
http://www.europarl.europa.eu/pdfs/news/expert/infopress/20160524IPR28821/20160524IPR28821_en.pdf
<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2016-0228+0+DOC+PDF+V0//EN>
- UK HM Treasury: *regulatory requirements must be proportionate to the risk posed, to avoid unnecessarily stifling competition and innovation in a nascent industry*
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_on_final_changes.pdf

Level Playing Field

- EBA: *discourage credit institutions, payment institutions and e-money institutions from buying, holding, or selling virtual currencies*

<https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>

- Why hinder the regulated FSI in the innovation race?
- Financial institutions and fintechs, incumbents and new players: a level playing field is required
- *Widening access to central bank money for non-bank Payments Service Providers and new forms of wholesale securities settlement*

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

<http://www.bankofengland.co.uk/publications/Documents/speeches/2016/speech914.pdf>

Consumer and Saver Protection

- Customers and savers demand for bitcoin is satisfied by unregulated financial entities
- Savers had very limited protection in the MtGox bankruptcy as it was unregulated
- There are real Ponzi schemes masked as cryptocurrencies

Privacy, A Basic Human Right

For consumers and savers, also required:

- by financial firms for any blockchain use case
- to ensure blockchain native digital token fungibility
- In our digital age, all communications (financial transactions included) transparent to regulators and investigators are eventually transparent for everybody
- That's why Apple has refused the FBI request to create an iOS security backdoor

Privacy or Transparency

- Cryptography backdoors are ineffective:
 - Expose honest people's privacy
 - Easily patched with robust cryptography by criminals
- *Rather than rely on out-of-date approaches to law enforcement, the FBI must develop 21st-century investigative capability [...] the alternative of permitting bad actors access to our systems is unacceptable*

Susan Landau, Professor of Cybersecurity Policy at Worcester Polytechnic Institute

<http://science.sciencemag.org/content/352/6292/1398.full>









Regulatory Technology?

- *The DAO* (distributed autonomous organization) is the main Ethereum project; it has raised >\$160m as leaderless VC
- *The terms of The DAO are set forth in the smart contract code [...] Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or guarantees beyond those set forth in The DAO's code*
- Based on the self-executing nature of smart contract code 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

Table of Contents

1. Blockchain needs a native digital asset
2. Decentralized transactional economy
3. Money without Caesar's stamp of approval
4. The regulatory challenges
5. **Banks: competition and opportunities**

Disruptive Innovation

- The entertainment industry wasted its resources fighting MP3, streaming, and illegal p2p sharing
- We now get MP3/movies/stream from iTunes, Google, Amazon, YouTube... not Sony or Universal
- Banks should not make the same mistake
-    did not understand disruptive innovation
-      have used it to build new businesses

Finance is Scared by Bitcoin

Cryptocurrencies increasingly look like becoming ubiquitous challengers to more familiar, established currencies. And, as they grow in popularity, so too will the risks for banks [...]
Banks must accept that they are increasingly part of the broader ecosystems that customers are constructing around themselves. However, their place in these ecosystems is far from secure.

British Bankers' Association

<https://www.bba.org.uk/publication/bba-reports/digital-disruption-uk-banking-report-2/>

Why finance is interested?

Blockchain transactions are cleared and settled as soon as the transaction is validated, 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: a check and balance system that allows for prescriptions, corrections, and restrictions

Insecure Snake-Oil Sold To Bank

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

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

 **AndreasMAntonopoulos** 
@aantonop  **Following**

Most of the blockchain stuff being sold to banks is insecure snake-oil

RETWEETS 113 LIKES 121

2:42 AM - 24 Feb 2016

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?

Permissioned Distributed Ledgers

- Incremental evolution, not disruptive innovation. Small impact, if any.
- *A private blockchain is an intranet, and a public blockchain is the internet. The world was changed by the internet, not a bunch of intranets. Where companies will be disrupted the most is not by private blockchains, but public ones*

Brian Forde, MIT, former senior adviser for mobile and data innovation at the White House
<https://bitcoinmagazine.com/articles/mit-s-brian-forde-companies-will-be-disrupted-the-most-by-public-blockchains-1466028606>

Unrealistic Expectations

Current interest in mutual distributed ledgers has established significant momentum, but there is a danger of building unrealistic expectations [...] achieving all the potential benefits from mutual distributed ledgers will require board level buy-in to a substantial commitment of time and resource, and active regulatory support for process reform, with relatively little short term payoff.

Michael Mainelli, Alistair Milne (2016)

The Impact and Potential of Blockchain on the Securities Transaction Lifecycle

<http://ssrn.com/abstract=2777404>

Cash Digitization

- *Central bank digital currency [...] 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 token is similarly unrealistic as it would severely undermine the US dollar
- A free instantaneous P2P payment network should be a priority for retail banks

Banking Sector Real Asset: Trust

- Trust is always needed and it is scarce
- Distributed consensus blockchains are more trust-worthy (efficient) for value transmission than banks
- Banks should focus on trust-the-intermediary services; e.g. email is decentralized but many prefer to use centralized services such as Gmail

Conclusions

Thank You

- Blockchain needs a native digital asset;
- Unrealistic expectations arise from distributed ledger hype;
- Decentralized transactional network are permissionless;
- We are at a turning point in the history of money;
- Regulation can hinder the FSI in the innovation race;
- A level playing field for incumbents and fintechs is needed;
- Customer/saver protection should be high priority;
- The understanding of real innovation is critical for banks;
- Cash digitization is urgent and decisive.