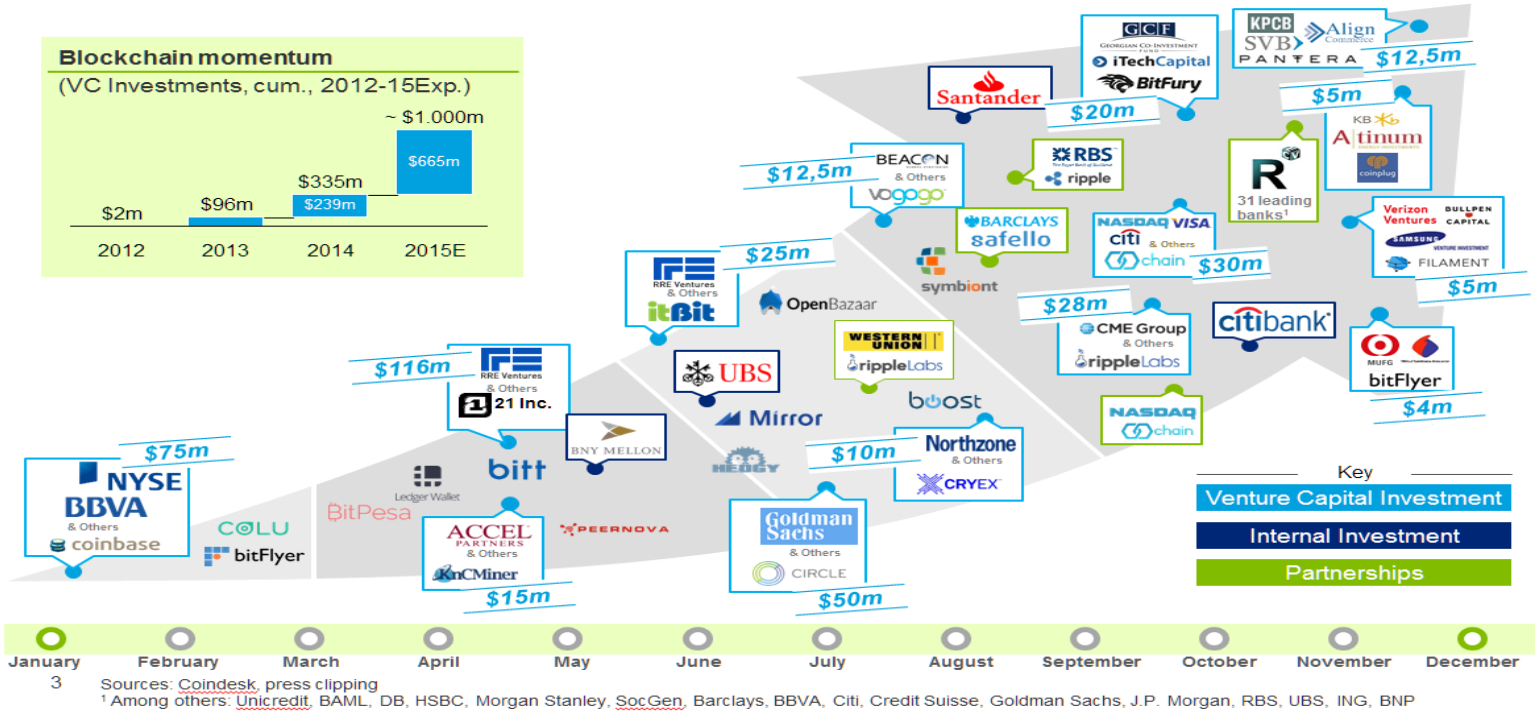
About Bitcoin And Blockchain: A Cultural Paradigm Shift

Ferdinando M. Ametrano
Intesa Sanpaolo, Milano Bicocca University

ferdinando@ametrano.net
https://onename.com/nando1970
https://speakerdeck.com/nando1970
https://it.linkedin.com/in/ferdinandoametrano

Università della Calabria
Rende (CS), June 13, 2016

Investments Landscape



Opinions

- **Ben Bernanke**: *[the virtual currency] may hold long-term promise, particularly if the innovations promote a faster, more secure and more efficient payment system.*
- **Alan Greenspan**: *It's a bubble. It has to have intrinsic value: you have to really stretch your imagination to infer what the intrinsic value of Bitcoin is. I haven't been able to do it. Maybe somebody else can. I do not understand where the backing of Bitcoin is coming from.*

http://qz.com/148399/ben-bernanke-bitcoin-may-hold-long-term-promise/
http://www.bloomberg.com/news/articles/2013-12-04/greenspan-says-bitcoin-a-bubble-without-intrinsic-currency-value

Bitcoin Is At The Crossroad Of

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

- Hard to understand: impossible without asking the right questions
- Mainly not a technology, a *cultural paradigm shift* instead

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.

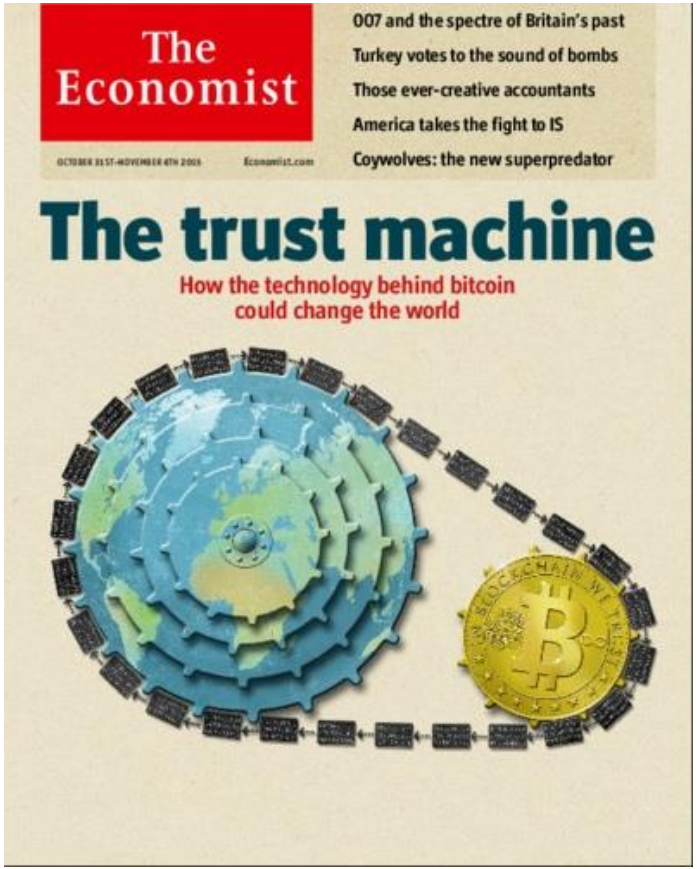
Michael Mainelli, Alistair Milne (2016)

The Impact and Potential of Blockchain on the Securities Transaction Lifecycle

http://www.swiftinstitute.org/wp-content/uploads/2016/05/The-Impact-and-Potential-of-Blockchain-on-the-Securities-Transaction-Lifecycle_Mainelli-and-Milne-FINAL.pdf

Table of Contents

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

What is Blockchain?

[A hash pointer linked list of blocks]

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

A Distributed Transaction Ledger

- Every block contain multiple transactions
- The blockchain is a distributed transaction ledger massively duplicated across network nodes
- Updated appending new blocks of transactions
- It is shared using a peer-to-peer file transfer protocol over the Internet
- The longest chain is authoritative

A Distributed Back-office

- Non-vetted network nodes, know as miners, perform transaction validation, clearing, and settlement
- How do miners reach consensus on the transaction history?
- Consensus in a distributed network with faulty (or malicious) nodes is a very complex problem know as Byzantine General Problem (BGP)

Distributed Consensus

- Nakamoto has obtained Practical Byzantine Fault Tolerance using economic incentive for the 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 blockchain native digital asset

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

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

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

Bitcoin Today Is Like Internet in 1994 Weird and Scary (Marc Andreessen)

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)

- Corporate wanted to go online, but not in the wild unregulated internet, populated by anonymous agents

Blockchain Needs A Native Digital Asset

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

#2 2016 video on finextra.com

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

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

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 databases with cryptographic proofs*

2018 *back to bitcoin*

Blockchain Beyond Bitcoin

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

Blockchain Use Cases

- OK: time-stamping, anchoring, and notarization services
- OK: cryptographic proofs and IDs

For the rest the hype is excessive, questions 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)

- Large amount of data cannot be put on blockchain

The Digital Token of The Future

- might not be bitcoin
- will be encryption-based
- will preserve privacy
- will be the evolution and optimization of the bitcoin model

might be bitcoin!

Table of Contents

Bitcoin as TCP/IP value protocol

- 7+ years up and running, despite whoever crack it
  - would collect a multi-billion USD bounty
  - would enjoy word-wide fame
- The bitcoin protocol could be improved, so it might be replaced by a better successor
- TCP/IP is inefficient at streaming, impossible to redesign it, just throw bandwidth at it

Permissionless Innovation Fast and Effective

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

The Information Economy

- Data is transferred with zero marginal cost
- Why paying a fee to move bytes representing wealth?
- 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 apply
- Secure: non falsifiable, non repudiable transactions

Internet as Transactional Agora

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

The 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 be the global outsourced decentralized security of the future, available to everybody

Table of Contents

1. Blockchain needs a native digital asset
2. Decentralized transactional network
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 easiness of purity assessment
  - Pleasant color
- Gold purity certification
- Representative money
- Fractional receipt money
- *Fiat* money and legal tender

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
- algorithmic supply

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

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

gold

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

bitcoin

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

IMF's SDR, F. Saccomanni

- Special Drawing Rights are international reserve assets, created in 1969 by IMF to supplement existing official reserves of member countries and address the lack of a non-national currency to be used as reserve asset
- Could a supranational cryptocurrency have that role?
- F. Saccomanni: *cryptocurrencies could be an effective monetary policy instruments [...] we should pay more attention to the geniuses working on them, try to understand what of interest they could teach us*

https://it.finance.yahoo.com/notizie/saccomanni-non-bisogna-demonizzare-cripto-valute-172912255.html
http://www.ufficiostampa.rai.it/pdf/2014/2014-10-09/2014100928490498.pdf

Money Comparison

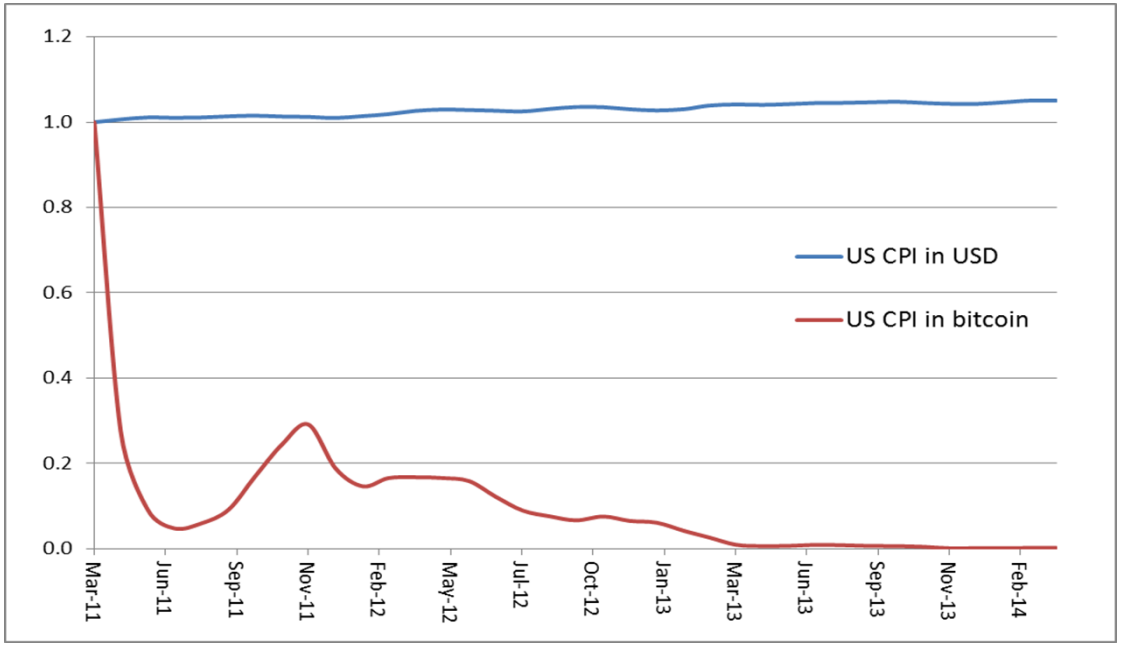
	Medium of Exchange	*Store* of ~~Constant~~ Value	Unit of Account
Live cattle			
Diamonds			
Gold			
Fiat coins and notes			
Bitcoin			
	• swappable • fungible • portable • divisible • recognizable • resistant to counterfeiting	• reliably saved, stored, and retrieved • retain usefulness over time • Maintain its storage properties • non-perishable or with low preservation cost	• relative worth unit of measure • stable value for stable price comparison • supply must be controlled in some way

Unit of Account - Money as numeraire

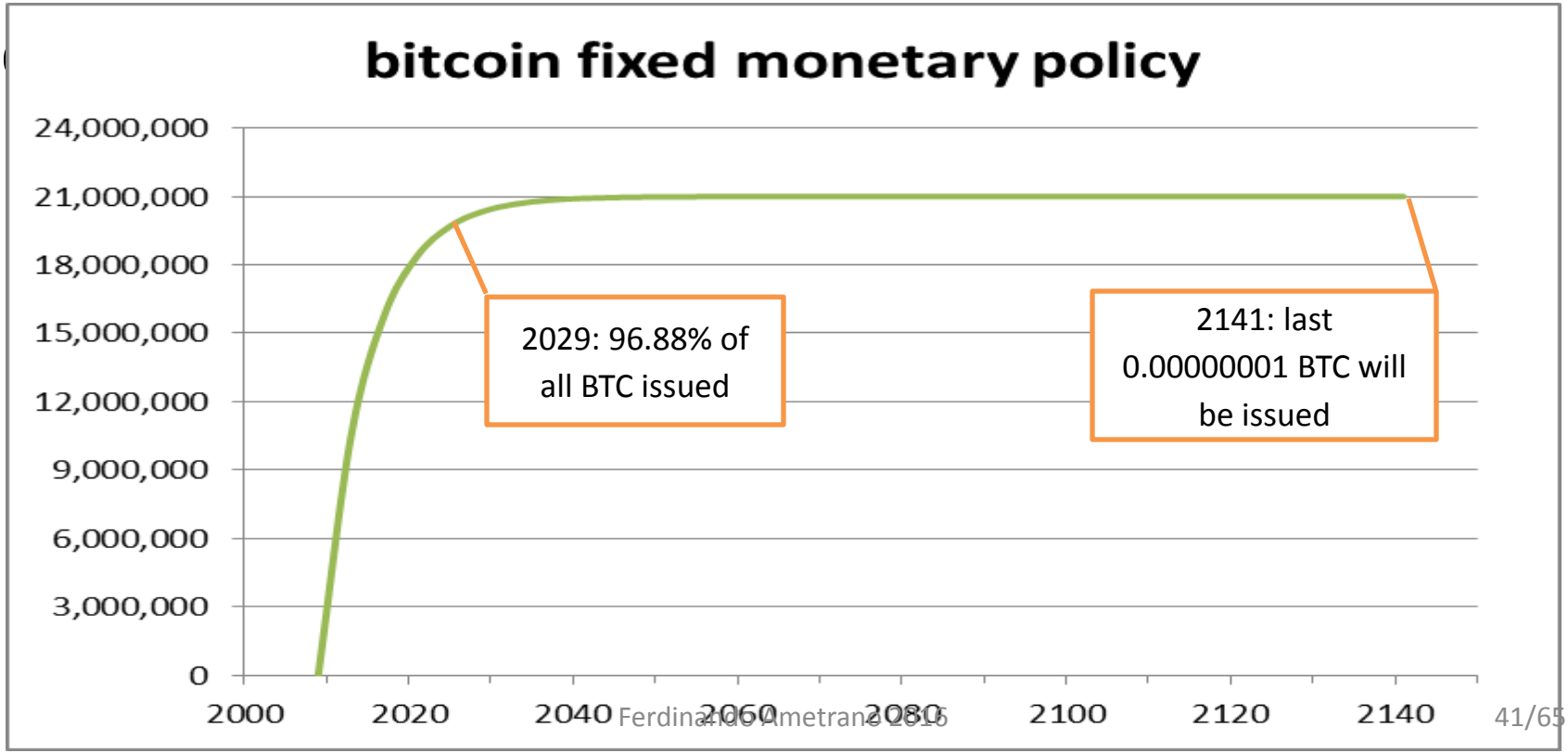
- Money is the unit of account against which the value of every other good is measured
- The price system measures the value of goods relative to the value of money
- Good money should provide stable prices to best perform its role as unit of account

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



Inelastic Money Supply: Deterministic Decreasing Rate



Hayek Money

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

Ametrano, Ferdinando M. (2014)
Hayek Money: the Cryptocurrency Price Stability Solution
http://ssrn.com/abstract=2425270

Dual Asset Ledger

Split *transactional* and *speculative* money demand with two non-fungible assets:

- (stable) transactional coins
- (unstable) speculative shares

Sams, Robert (2015)
A Note on Cryptocurrency Stabilisation: Seigniorage Shares
https://github.com/rmsams/stablecoins/blob/master/paper.pdf

Bitcoin As Reserve Asset For A Reserve Bank

- The Reserve Bank is a DAO (decentralized autonomous organization)
- On a dual (coin/share) asset ledger
  - Stable coins are backed by bitcoin reserves, provided by Reserve Bank shareholders
  - Reserves absorb profit/loss from stabilizing the coin
  - Shareholder are entitled to the Reserve Bank profits

Ametrano, Ferdinando M. (2016)
Price Stability Using Seigniorage Shares, Decentralized Autonomous Reserve Bank, Bitcoin as Reserve Asset, and Proof-of-Payment
http://ssrn.com/abstract=2508296

Scalability

- If bitcoin is digital gold does not really need to scale to huge number of transactions, being just a real time gross settlement system
- Bitcoin transaction can (and will) scale (see Lighting Network, Sidechain)
- Stable coins can use the same tech for high number of transactions

Table of Contents

Level Playing Field

- Regulation should not burden reliable institutions
- *To discourage credit institutions, payment institutions and e-money institutions from buying, holding, or selling virtual currencies*. Why?
- Financial institutions and fintechs, incumbents and new players: a level playing field is required

Consumer and Investor Protection

- Do not leave customers and investors to pirates
- Investors had very limited protection in the Mt Gox bankruptcy because it was not a regulated financial entity
- There are Ponzi schemes masked as cryptocurrencies

Privacy or Transparency

- In a digital age whatever is transparent to regulators and investigators is eventually transparent for everybody
- Apple has refused the FBI request to create an iOS backdoor for this reason
- Cryptography backdoors are ineffective:
  - Expose honest people privacy
  - Easily patched with robust cryptography by criminals

Privacy

- Beside being a human right

- privacy is also required:
  - by financial firms for any blockchain use case
  - to ensure digital token fungibility

Bitcoin used by terrorists

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

Europol

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

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/news/government-publishes-anti-money-laundering-assessment-and-commits-to-action-plan

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

Regulatory Technology

- Regulators (NYDFS, EU Parliament, etc.) declared their intention *not to stifle innovation*
- Actually, bitcoin might be the first case of *regulatory* technology
- Technical feasibility changes the landscape: e.g. entertainment industry with MP3 and streaming

Table of Contents

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

Disruptive Innovation

- The music industry wasted its resources fighting MP3, streaming, and illegal p2p sharing
- The result: we buy MP3 and stream from iTunes, Google Play, Amazon, YouTube… NOT from Sony or Universal
- Banks should not do the same error

- 

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

- Trading can be real time, but clearing and settlement is a convoluted legacy t+2 process
- Not a technological problem
- Consensus by reconciliation: a check and balance system that allows for prescriptions, corrections, and prohibitions

R3 Corda (1/2)

- 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***"

R3 Corda (2/2)

- *our starting point is individual agreements between firms*
- *legal prose is considered from the start […] there will always be disputes and we specify how they will be resolved*
- *we need more than just a consensus system. We need to make it easy to write business logic and integrate with existing code; we need to focus on interoperability*

It looks like a revamped SWIFT protocol
on cryptographic proof steroids

Permissioned Distributed Ledgers

- Incremental evolution, not disruptive innovation. Small impact, if any. Intranet, not internet.
- *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://www.swiftinstitute.org/wp-content/uploads/2016/05/The-Impact-and-Potential-of-Blockchain-on-the-Securities-Transaction-Lifecycle_Mainelli-and-Milne-FINAL.pdf

Insecure Snake-Oil Sold To Bank

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

Cash Digitization

- A free instantaneous P2P payment network should be a priority for commercial banks
- Hard to imagine digital €/$/£-tokens by Central Banks, as it would severely undermine deposit-taking role of commercial banks
- IMF sponsored blockchain token would severely undermine the US dollar

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 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
- Do not slow down banking innovation with regulation
- A level playing field for incumbents and fintechs is needed
- Customer/investor protection should be high priority
- Banks: understand and ride innovation, do not fight it
- Cash digitization is urgent and crucial