Massachusetts Institute of Technology

MIT Connection Science

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Blockchain & Financial Services: The Fifth Horizon of Networked Innovation

PART 1

MAY 2016

David Shrier, Deven Sharma, Alex Pentland
Connection Science & Engineering
Massachusetts Institute of Technology

connection.mit.edu

Massachusetts Institute of Technology

MIT Connection Science

The authors would like to thank the team that helped develop this document, including Jackie Iarossi, German Canale and Weige Wu at MIT Sloan, Michael Casey at the MIT Media Lab Digital Currency Initiative, and Alex Lipton.

This paper is the first of a 4-part series:

- Blockchain & Financial Services: 5th Horizon of Networked Innovation: May 3
- Blockchain & Transactions, Markets & Marketplaces: May 10
- Blockchain & Infrastructure (Identity, Data Security): May 17
- Blockchain & Policy: May 24

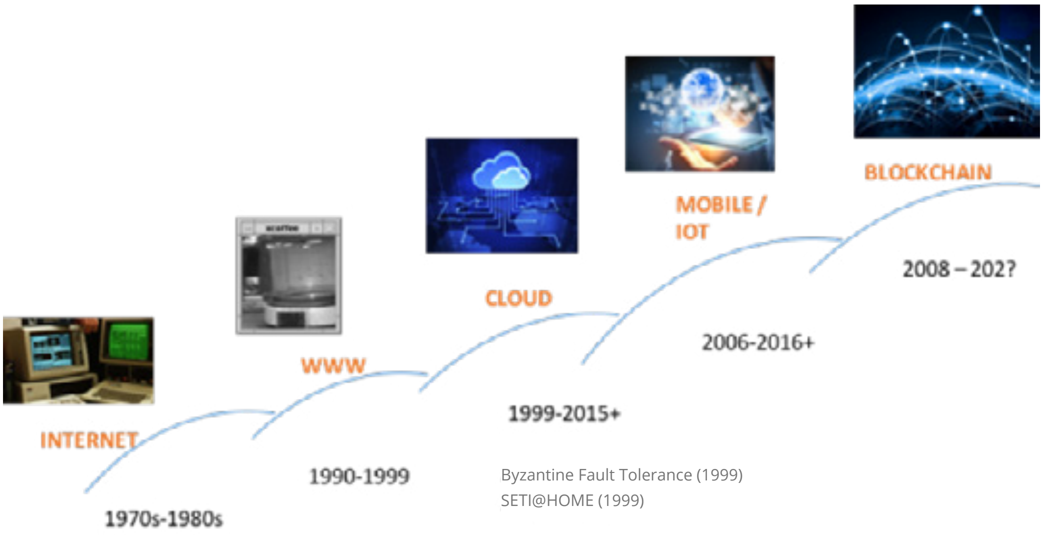
Disclaimer

The Massachusetts Institute of Technology may have financial or other relationships with one or more entities described in this document. No endorsement, implied or explicit, is intended by discussing any of the organizations or individuals mentioned herein, and is expressly disclaimed.

I. Introduction: the Fifth Horizon of Networked Innovation

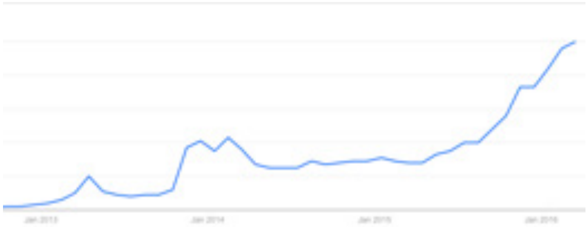
How can you capitalize on the disruption that blockchain is introducing into the global financial system? What are the risks and opportunities that this new technology represents? What roles can each of government, academia and private industry play in shaping the new future that blockchain can enable?

While blockchain is, today, an immature technology, it holds the potential to unleash a wave of innovation across multiple industries – including financial services. Just as we saw transformation driven by earlier technologies like the HTTP protocol (unlocking the World Wide Web) and the rise of pervasive computing and intelligent devices (so-called “Internet of Things”), so too blockchain may create new businesses and applications not even dreamed of at this writing.



Blockchain: Popular Topic of 2016

Rising interest (2012-2016)



“blockchain” search term trend[3]

Blockchain technology has entered the top strategic priorities of the CEOs of the Fortune 1000[1]. Venture investment in the field has grown to $1 billion in 2015, representing 7% of all Fintech VC funding, with some forecasting investment in blockchain to grow to $10 billion in 2016[2].

Potential for Transformation

Blockchain represents a technology innovation that enables transparent interactions of parties on a new type of trusted and secure network which distributes certified and auditable access to data. Although the technical components have been in existence for decades, blockchain *qua* blockchain is a novel, resilient, and general purpose approach to data, transaction analytics and networks. It holds the potential to address inefficiencies, reduce cost, unlock capital, improve trust in societal fabric, and open new business models. It also could accelerate the growth of the informal economy or even criminal elements of societies, complicating efforts of governments to provide security and safety to their citizens. Like any new technology, it holds the potential for good and for harm, and benefits from an enlightened, informed, and ethical application by its users.

Blockchain has generated extensive interest and enthusiasm in financial markets. Why? Trust and confidence in the promise to meet obligations is the cornerstone of any financial transaction. Substantial parts of financial markets are designed to solve for problems of trust and asymmetry in the financial transactions through the risk management infrastructure.

- Substantial costs in the financial infrastructure are designed for identity checking, transaction authenticating, reliably and accurately transacting, supporting records, and securely storing records. These activities solve for trust, fraud and error.
- Substantial capital and collateral gets locked in the financial system to buffer against lack of trust and confidence in certainty and predictability of outcomes.
- The cost burden of the risk infrastructure makes the economics of small size transactions expensive and unaffordable, and therefore inaccessible to low income members of society.

Blockchain solves for problems in trust, asymmetry of information and economics of small transactions without burdensome risk infrastructure and central intermediaries.

Financial Services Opportunities

In financial services, examples of blockchain applications include the ability to:

- Streamline records transfer of stock ownership;
- Improve speed and reduce cost of syndicated loans, by enabling the possibility of direct syndication;

- Increase transparency into collaterals embedded in many financial transactions;
- Enhance regulatory compliance by automated, instantaneous record validation;
- Reduce costs of money remittance and currency exchange;
- Create self-executing contracts that reduce or eliminate the possibility of fraud or corruption;
- Improve rule of law regarding transfer of property title;
- Eliminate most of the costs and friction in issuance and trading of securities such as equities and debt;
- Reduce cost and improve access in insurance markets by creating the potential for easier implementation of self-insured risk pools;
- Allow the creation of new forms of identity separate from a central issuing authority; and
- Provide a means of exchange of value in systems where trust in central authority has been lost.

Beyond the banking sector of financial services, the impact in the insurance sector will also be substantial from: efficient transaction processing, reduction of claims fraud and better evaluation of risks.

We are seeing blockchain currencies being used to transfer value out of markets where currency regulations are strict and trust in central banks is weak. As this level of activity increases, regulatory authorities will undoubtedly take a more severe view on these activities. Yet, as governments that have attempted to restrict Twitter usage have found, once the genie is out of the bottle, it is difficult to recapture.

New models being pursued range from a primary “distributed trust” structure which makes it possible to use a pseudonymous cryptocurrency like bitcoin that is completely open and public, to permissioned, private, trusted systems, such as those being implemented by some investment firms as a faster, lower-cost means of settling and clearing trades.

A Note of Caution

We are currently in the invention/experimentation state of market evolution with blockchain technology. Today, we can’t predict which application will be the “killer app”, but the speculation is that as much as $15 billion to $20 billion can be saved in the financial services sector alone using blockchain[4], translating to more than $150 billion of potential equity value creation based on current market multiples. These savings will primarily come through greater efficiency, i.e., job loss. Benefits from unlocking collateral and greater liquidity might be substantial as well.

Barriers to Adoption

Many hurdles remain towards adopting this new technology, and as with any new tool, human and organization attitude poses a high barrier, including:

- **Standards:** An absence of well-adopted standards in documentation and practices exists, for example, even invoice and bill formats are unique to each issuing organization although varying formats adds very limited value. Standards could start with industry specific action, or be government initiated;
- **Organization and Human Behavior:** Behavior to embrace and adopt harmonized standards and practices is difficult to achieve;
- **Infrastructure legacy:** Given large existing infrastructure within any organization, the costs of replacing existing technology with new Blockchain investment are high;
- **Confidentiality:** Protection of private and confidential information and comprising competitive advantage;
- **Processing cost:** High and escalating cost of proof verification;
- **Legal and regulation:**
    - Settlement finality and dispute resolution – consumer risk protection;
    - Liability of security risk and related losses driven by introducing a new financial infrastructure;
    - Protection against risk of attack or dominance by few players – may discourage players to link “off-chain” assets – as well as anti-trust regulations and implications;
    - Conduct: priority of verification of transactions;
    - Regulation and legal classification jurisdictions of assets, data location & flow and how existing regulations apply.

Looming Dislocations

The rise of digital media in the 1980s led to a disruption of the newspaper industry, ultimately reshaping the face of media globally. Copyeditors, press operators, delivery agents, even paid journalists, all became redundant in an era of Huffington Post and Twitter. We see the potential for similar levels of disruption in the financial services, supply chain and logistics, and other industries. One startup recently formed at MIT by students in our Future Commerce class on Fintech innovation suggests removing three to five layers of intermediation between poor farmers and global agribusiness suppliers. This represents benefit to the farmer, and to the supplier, but could ultimately result in the loss of 5 to 25 jobs among the intermediaries for that single transaction stream.

Efforts to convince people to adopt blockchain technology could result in the pursuit of "Potemkin village" solutions, without tangible benefit, or with benefits that generate perverse outcomes (such as the creation of additional cost). There are examples in other industries of failed promise of technology. For example, electronic medical records (EMRs) were hailed as a revolution in medicine that would transform health outcomes, but a 2009 study by the European Commission spanning 10 countries showed the benefits to primarily be financial in nature[5]. Validating this, the Chief Medical Officer of a top-3 EMR company shared with the authors that EMRs were optimized for financial reporting, not clinical care, and were never intended to improve health outcomes – in no small part because the "buyer" of the technology was the chief financial officer of the provider organization. This has created market opportunity for more user-friendly EMRs, but the most widely-adopted EMRs are built around billing improvement not medical care quality. One could argue that this has contributed to the continued rise of healthcare costs in the U.S., to 17% of GDP in 2015[6].

Given the potential as well as the dangers of blockchain development, we ask:

- How can policy interventions shape the future of blockchain in productive directions?
- Is there any way to effectively manage productivity improvements, that may lead to significant employment disruption in financial services?
- What steps can we take to mitigate the negative impacts of innovation-driven employment dislocation?

To answer these questions, we need to understand the evolution of blockchain and draw parallels to similar technology (re/e)volutions.

An Origin Story

The antecedents of the current environment have been developing for some time, since the publication of the bitcoin protocol in October 2008. We note that the first blockchain applications emerged out of eroded trust in traditional institutions, yet eight years later, more than 60% of the global financial system has entered into a consortium to apply blockchain to remove cost and create efficiency in their businesses. Have we gone from "revolution now!" to "reengineering processes"?

In the summer of 2014, MIT hosted the Ecology of Digital Assets summit, leading to the creation and adoption of the Windhover Principles[7] for anti-money-laundering (AML) and Know Your Customer (KYC) compliance among over 20 bitcoin and blockchain companies in informal consultation with U.S. government officials. At MIT, we have developed new open-source technology solutions such as Enigma[8] for secure data management and ChainAnchor[9] to address some of the issues related to AML/KYC in cryptocurrencies, but are only beginning to see awareness of the need, much less moves for adoption. Understanding and adoption of compliance solutions remains weak both within the fintech startup community and among regulatory agencies.

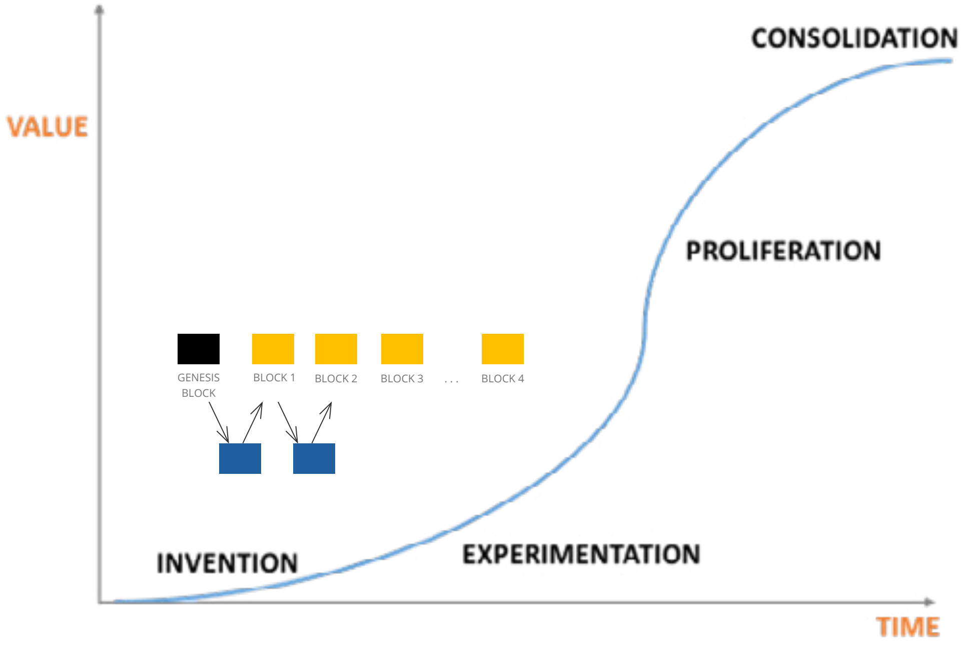
In our conversation with global leaders at Davos this past January 2016, we heard rising interest in the C-suite around blockchain technologies as a tool for transformation in the financial services industry. The theme has continued in 2016 as we see top tier financial institutions funding both external experimentation and setting up internal "skunk works" groups to develop blockchain applications. Governments, as well, have begun to explore how blockchain can address certain intractable issues of trust and transparency. Yet, the technology, commercial models and adoption, and the regulatory and legal frameworks surrounding blockchain, remain in their infancy.

According to the World Economic Forum's survey on technology tipping points, 58% of respondents expect that by the year 2025, 10% of global GDP will be stored on blockchain variations, up from about 0.008% in March 2016.

The Evolution of a New Technology

We are in the early stages ("invention/experimentation") of the adoption of blockchain. As with other new technologies, blockchain is undergoing a phase of invention and experimentation. Blockchain is a revolutionary innovation in its approach to building trust, transparency and traceability in financial transactions. The innovation is in the

concept and approach of piecing together **technology components**, not necessarily a technology magic silver bullet.



Just as ARPANET led to the Internet and ultimately the World Wide Web, we have early precursors like SETI@HOME and Amazon Mechanical Turk leading to the rise of distributed networks and outsourced distributed computations and tasks. Despite the high degree of excitement, a large number of venture capital investments in the sector are funding a proliferation of companies built on immature technology.

If we examine the evolution of networked innovation, the 1970s and 1980s saw the development of the Internet, the “first horizon” in our paradigm. Beginning in 1990, Sir Tim Berners-Lee and others promoted the creation of intuitive navigation and cross-connection of information, making possible the “second horizon” of the World Wide Web. While “cloud computing” had its origins in other technologies, we argue that the formation of Salesforce.com in 1999 marked a key milestone in its evolution into the “third horizon” of networked innovation[10]. A notable publication around Byzantine Fault Tolerance (critical to the theoretical underpinnings of blockchain), and the launch of projects like SETI@Home (which anticipates the distributed nodes of blockchain), also were produced in 1999. With decreasing bandwidth costs and increasing ubiquity of smart phones and smart devices, we trace the “fourth horizon” to the launch of mobile broadband services in 2006. This brings us to the blockchain, with Satoshi's October 2008 paper launching the "fifth horizon".

The current state of blockchain industry reminds the authors of the early days of World Wide Web commercialization, as chronicled in Michael Wolff's Burn Rate. While a large number of companies are being funded, not all with sound business models, some hold the potential to become the next Google, the next Apple, or the next Facebook.

In 1993, no one could have realistically envisioned an Uber, or an Airbnb, or a viable ZipCar. In 2001, no one could have predicted Facebook's success (an earlier version of a "university-member-driven-social-network", The Square, was a casualty of the dotcom bust) or YouTube's market dominance (bandwidth constraints and other issues led companies like Broadcast.com and TheFeedroom to relatively modest outcomes). And today, in 2016, we can only dimly imagine what the "killer app" for blockchain will be. The near-term future is somewhat more clear, and we will concentrate the majority of this white paper series on the 5-year horizon of blockchain innovation and financial services.

A Call to Action

In our discussions with an array of individuals among industry, academia, and policymakers, the authors have found that understanding of blockchain is poor, and appreciation is modest of both the dangers that the technology can generate as well as the benefits it can deliver. We observe a generalized awareness, but heterogeneous comprehension of the nuances.

Recognizing the need for strategic clarity, and framework solutions, the Massachusetts Institute of Technology's Connection Science & Engineering team seeks to offer context on the blockchain revolution, pose policy questions to regulators and lawmakers, and provide inspiration to blockchain innovators.

MIT is frequently called a place where "the future is invented," informed by our mission of solving humanity's biggest problems. Our belief institutionally is that innovation can be a positive force for change, if guided by a responsible, ethical framework. Despite the notes of caution that we inject into this report, we believe that blockchain technology can deliver material benefits to society, and will provide guidance around potential areas for application that we feel hold promise.

We invite you to enter the fifth horizon of innovation, and help us create the future of blockchain.

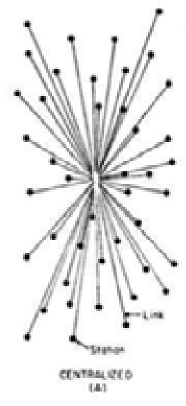
II. How Blockchain Works

Blockchain and its Attributes

Blockchain is a distributed database with an open ledger. Broadly, this means data isn't stored on a single computer but rather on many different computers (known as "nodes") in a peer-to-peer network. This represents a radical paradigm shift in financial services. Blockchain's democratization principles has captured the imagination of the financial market place:

- Distributed data ledgers used, updated and verified by participants in the blockchain versus centralized data base
- Identity verification and authentication executed by the participants
- Logic and rules embedded in the transaction versus in a separate application layer
- Traceability of changes from the beginning
- Documents maintained separate from the ledgers

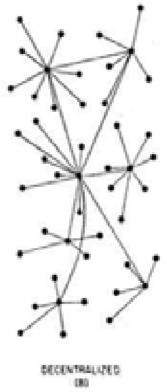
Centralized Ledgers



Traditional centralized ledger systems, such as those used by central banks to manage sovereign currencies, have one central ledger, which records currency transactions. Trust is centralized within a single entity who is tasked with governing the management of sales, purchases and transfers of the currency. Centralized ledgers have the advantages of organizational simplicity, control through a single point of record-keeping, and lower cost to maintain. Disadvantages include limitations on scalability, the potential for hacking and other security concerns, and the risk that if the central authority either shuts down or decides to unilaterally alter the record, there's nothing the individual can do about it (short of legal recourse).

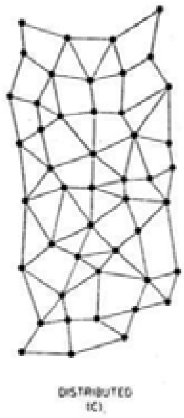
Decentralized Ledgers

In a decentralized ledger, there are multiple copies of the ledger stating who owns what. I go to my money transfer agent, to whom I hand cash. My agent records that in their system. He contacts another broker in a foreign country who exchanges my dollars for their pesos or euros, and records the transaction in their system. Later the two agents meet up



to reconcile accounts. There are multiple copies of the ledger, but they are brought into agreement through trusted parties. This system has some benefits of redundancy, but still places control into a few hands and has reconciliation challenges.

Distributed Ledgers

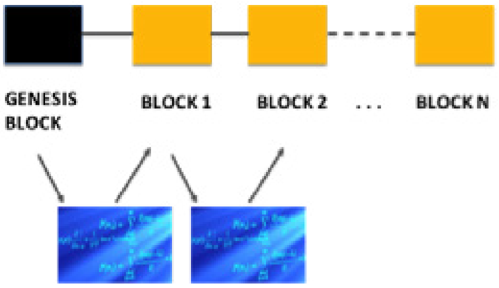


With a distributed ledger, each node has a copy of the ledger. A democratic voting system, where 51% of nodes need to agree on a transaction to effectuate it, makes properly-designed networks of nodes exceedingly difficult to hack.

The advantages of distributed ledgers over other systems are:

- Resiliency
- Security
- Creation of trust

The reason blockchain is called a "chain" is that there is an initial block, called a genesis block, to start the chain. When you want to perform a transaction, such as to sell a bitcoin or a litecoin to another person:



- The blockchain software puts out a call for the nodes in the distributed network to perform a calculation to create a "hash" which is a complex calculation.
- The act of choosing a random number, whose hash results in the desired value with respect to a target chain value, is referred to as "mining".
- The new block links back to the previous block, in this case the genesis block, creating a "chain". As each new block is mined, the chain lengthens.
- The calculation conducted presents what is known as "proof of work". This serves to validate adding blocks to the chain, and allows for defense against bad actors by having the entire network create the system of trust, versus needing to trust each party (or node) on the network.

Let's look at how the bitcoin blockchain works:

> Every ten minutes or so mining computers collect a few hundred pending bitcoin transactions (a "block") and turn them into a mathematical puzzle. The first miner to find the solution announces it to others on the network. The other miners then check whether the sender of the funds has the right to spend the money, and whether the solution to the puzzle is correct. If enough of them grant their approval, the block is cryptographically added to the ledger and the miners move on to the next set of transactions (hence the term "blockchain"). The miner who found the solution gets 25 bitcoins as a reward, but only after another 99 blocks have been added to the ledger. All this gives miners an incentive to participate in the system and validate transactions. Forcing miners to solve puzzles in order to add to the ledger provides protection: to double-spend a bitcoin, digital bank-robbers would need to rewrite the blockchain, and to do that they would have to control more than half of the network's puzzle-solving capacity[11].

Interestingly enough, although "proof of work" used to be central to blockchain theory, it has (at least in the case of bitcoin) become a bit of a burden. Some industry executives believe that the bitcoin blockchain spends $600 million per year on proof of work to essentially validate three bitcoin server farms in Asia[12]. One prominent industry executive speculated to the authors that for much less money he could give a better result just by using brute force to validate certain nodes. Technically, the payments are being made to validate transactions, but his point remains noteworthy.

Blockchain isn't a panacea. Artificial limits built into the bitcoin experiment mean that it will never be a widely used currency – as of May 2016 it is valued at approximately $7 billion. Other forms of blockchain may enjoy wider adoption. Moreover, many early users of the bitcoin blockchain were engaged in illicit commerce who were seeking to avoid government scrutiny. (The authors note that other fringe markets developed and adopted new technology before they became mainstream, like streaming video or micropayments).

Consolidation in the mining of bitcoin, which has become computationally (and thus energy-wise) expensive, has placed significant mining capacity into a few hands, which introduces the risk of defrauding the network – defeating the original purpose of the distributed network. This may promote adoption of new cryptocurrencies, but may also weaken trust in the paradigm for consumer and corporate adoption of digital currency.

The bitcoin blockchain's scalability is currently hindered by a 1MB limit on the amount of data allowed in each block, which at some point will curtail the number of transactions that can be confirmed in any 10-minute period. Bitcoin developers have been unable to reach consensus on how to change the protocol to address this problem, with one side fearing that larger blocks will require miners to maintain more data storage, which could further favor a more centralized, industrial market structure for mining. Pieter Wuille from Blockstream has proposed a method called "segregated witness" to reduce the amount of data required for each transaction so as to allow more to be included in a block. Others, including KTKT Nn TNk of the Lightning Network, have suggested methods for processing transactions "off chain" before aggregating their data into a single entry in a bitcoin block. It's not clear that either solution will be effective or sufficient to permit a continued expansion in bitcoin transactions.

Other forms of blockchain are enjoying growing adoption, such as Ethereum, which has created a platform for smart contracts. Unlike the Bitcoin blockchain, which requires substantial expertise to learn how to program, developers can begin building applications on Ethereum using the Solidity programming language in a matter of days or weeks. Industry incumbents have begun supporting Ethereum, such as Microsoft, which added support for Ethereum applications to Visual Studio in collaboration with ConsenSys in March 2016.

An Ideological-Technological Exploration of Blockchain

Most blockchain taxonomies focus on the functional architecture (is it permissioned or permissionless? Is it public or private?). We find useful the division proposed by ArthurB, although it has been pointed out that his statement "Applications which do not attempt to evade oppressive governments have little or no reasons to use decentralized systems" isn't precisely true. There are numerous examples of a need for trust technologies when absolute trust in a third party is absent, having nothing to do with governments – eBay selling is the most trivial example, but equities security trading would be another.

In our view, understanding implementation of blockchain requires understanding implementers, users, and their respective objectives. This context-based analysis of blockchain provides a novel lens on selecting a platform and allocating resources to it. Broadly speaking, when we incorporate ideology into the technological analysis, we see three broad categories:

- **Libertarians:** A substantial number of bitcoiners believe that government has no role in regulating society, and bitcoin usage is an expression of political belief. AML/KYC is anathema to their belief systems. This isn't to say that all bitcoin users and companies feel this way – to the contrary, a large number of bitcoin companies employ or developed policies based on the Windhover Principles that MIT helped shepherd.

Rather, a vocal segment of bitcoin miners and developers assert a proprietary ownership of the technology, and vigorously reject anything that compromises their idealized view of how it should be used. To quote a recent post on Reddit: “if you aren't working to make Bitcoin better (read: more private, more fungible, more scalable) then you should keep your dirty, groveling sycophant paws off of it.”[13] It’s a vigorously-expressed point of view but one shared by a number of users who engage each other regularly in self-reinforcement.

- **Technocrats:** A broad middle of technocrats don’t automatically assume either government regulation or total freedom from regulation, but rather see blockchain as a flexible technology without ideology. Ethereum would fall clearly into this category.
- **Rules Followers:** The industry-led consortia such as R3 and Hyperledger accept, a priori, that regulation applies to blockchain (particularly with respect to AML/KYC as it applies to currency and other financial-related matters). While perhaps not as passionate in espousing their views as the Libertarians, these Rules Followers are making an ideological choice embedded into the fabric of their chosen technology platform. (Corda doesn’t technically use “blocks” but we are describing all distributed ledger technologies as blockchain for convenience).

Longer-term use of blockchain at scale will likely come from one of the latter two categories. At same time, the passion that the libertarians feel has caused them to think “outside the box” and question assumptions, resulting in a new way of transacting that is transparent, open and decentralized. In fact, blockchain as such would not exist with those passionate libertarians driving its creation and adoption.

Let a Thousand Blockchains Bloom

With the proliferation of funding for blockchain has come a proliferation of blockchains. And, with this, comes the need for interoperability. Enter the InterLedger Protocol, which seeks to interlink the companies, individuals and technologies behind this proliferation[14]. Facing the proliferation of blockchains, Ripple and others in the industry are seeking to provide a better mechanism for connecting blockchains to each other, while preserving the security of private blockchains. The Hyperledger Project, likewise, seeks to disseminate an open standard for distributed ledgers to facilitate connectivity.

How will the path to adoption broaden?

The extraordinary promise of blockchain initiates a conversation and likely leads to experimentation. The development of foundational blocks would accelerate the path of adoption. Tools that support the activity flow might accelerate the adoption.

What is the Likely Path to Adoption?

There are several possible paths for adoption of blockchain, which are not mutually exclusive but might potentially become mutually reinforcing over time. We see three primary axes of adoption:

- **Incumbent Intra Organization Permissioned/Private Blockchain:** Most organizations operate with enormous silos that lead to friction in information sharing and duplicating of work. Adoption of Blockchains within an organization might raise the openness and comfort in adopting across organizations/external parties.
- **Incumbent Inter-Organization Permissioned/Private Blockchain:** A plausible scenario is where organizations apply the concepts underlying blockchain to their existing technology infrastructure, and gradually migrate to new technologies over time.
- **New Ventures:** Many new ventures have already been funded that are experimenting at all levels of the technology stack. These new ventures explore both foundational components (the ledger, smart contracts, other kinds of smart assets) and experimentation into challenge areas (e.g., provenance for diamonds; property rights in countries with weak rule of law; remittance of funds across borders or currencies).

What mechanisms can be put into place to facilitate adoption and continued innovation? How can governments, private citizens, companies and academia best collaborate to empower this exploration and growth?

III. Towards the Fifth Horizon of Networked Innovation

How can we proceed towards development of this fifth horizon of networked innovation? The issues of blockchain are as much about technology and business model development as it is about regulation and industry dynamics. 2015 was about gaining attention for the technology. 2016 will be about rapid and widespread experimentation with this new technology.

Joichi Ito, Director of the MIT Media Lab, wrote this note of caution: “Many people are so excited about the potential applications [of blockchain] that they have ignored completely the architecture of the system on which they would run. Just as many Internet companies assume that the Internet works on its own, they assume that all blockchains are the same and work, but blockchain technology is not as mature as the Internet where you can almost get away with that... Governments and banks are launching all kind of plans without enough thought going into how they're actually going to build the secure ledger.”

In strategic discussions with regulators, the authors were invited to contemplate not only the positive potential of blockchain, but also the dystopian inverse, where the promise of blockchain failed to materialize. Imagine a world where five of the largest banks collapse due to coding errors that result in hundreds of thousands of smart contracts mis-executing. It’s possible: in 2012, Knight Trading collapsed due to a $460 million trading error; shifting the decimal a few places to the right could have a systemic impact on the global financial system. What if quantum computing breakthroughs were combined with blockchain to create a truly impenetrable money-laundering network for criminals? Perhaps scariest of all for the investors who have poured billions into blockchain: what if, 10 years from now, there is no meaningful adoption of blockchain?

Another issue that the bitcoin blockchain community will need to confront first, but that is faced by all mining-incentive-driven markets, is that the security of the chain can disappear if mining becomes unprofitable.

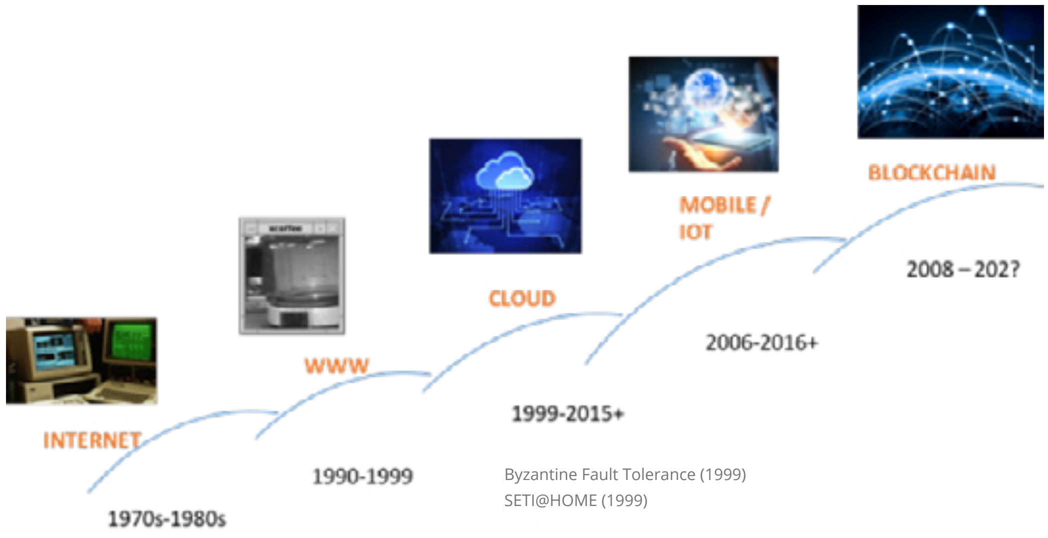
The authors remain convinced that the potential benefits outweigh the possible downside scenarios. New avenues of exploration may expose previously unconsidered opportunity. Imagine a world where the internet of distributed autonomous devices meets the internet of distributed data. What if the smart cars driving on the roads in a city and the smart buildings around which they drove were linked in a network that powered the financial system of the country? What if idle capacity of autonomous vehicles were harnessed to oversee efficient distribution of goods and services? It could be wonderful, or it could be a nightmare.

Difficult, and intractable, problems may end up stimulating widespread adoption of blockchain technology. MIT believes that cybersecurity, and specifically data security, may be one such application. A blockchain-based system such as Enigma represents a means of storing critically sensitive corporate data in a virtually hack-proof decentralized network, yet still perform computation on the data while it remains encrypted. We are also intrigued with the notion of "bringing the algorithm to the data", rather than the current model of separation of data from computation.

Yet, adoption is an open question. Is there an incentive structure that could be derived that would encourage a notoriously siloed, and competitive, industry like financial services to form a community with free flow of ideas to adopt uniform standards? How could this be developed and promoted?

We encourage readers to share their thoughts on a path forward to the 5th Horizon.

David Shrier
Managing Director, Connection Science & Engineering
Massachusetts Institute of Technology
Email: 5th-horizon@mit.edu



THE FINANCIAL WORLD IS FOCUSED ON FINTECH.

ARE YOU?

If you don’t want to get left behind, consider updating your expertise and upskilling yourself with this **12-week online certificate course from MIT**.

EXperimental Learning

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Fintech certificate course: Future Commerce

Presented in collaboration with leaders in online education, GetSmarter.

DOWNLOAD COURSE INFO PACK

getsmarter.mit.edu

> *“You need to understand what's going on in this highly chaotic environment. And we can help.”*

DAVE SHRIER - MANAGING DIRECTOR, MIT CONNECTION SCIENCE, COURSE INSTRUCTOR

SA+P Massachusetts Institute of Technology | School of Architecture + Planning

IN COLLABORATION WITH getsmarter

REFERENCES

[1] MIT personal conversations with CEOs of over 60 leading financial services and technology companies, Davos Switzerland, January 2016.

[2] Prediction: $10 Billion Will Be Invested in Blockchain Projects in 2016 http://coinjournal.net/prediction-10-billion-will-be-invested-in-blockchain-startups-in-2016/

[3] Google Webtrends, accessed 19 March 2016.

[4] Santander InnoVentures, Oliver Wyman, Anthemis Group, "The FinTech 2.0 Paper" (2015).

[5] "The socio-economic impact of interoperable electronic health record (EHR) and ePrescribing systems in Europe and beyond" (2009) European Commission Information Society and Media Directorate.

[6] "US Health Care Costs Surge to 17 Percent of GDP", The Fiscal Times (2015) http://www.thefiscaltimes.com/2015/12/03/Federal-Health-Care-Costs-Surge-17-Percent-GDP

[7] Clippinger J, Bollier D *From Bitcoin to Burning Man and Beyond* (2015).

[8] MIT Enigma Project: https://enigma.media.mit.edu

[9] T. Hardjono, ChainAnchor: Cloud-Based Commissioning of Constrained Devices using Permissioned Blockchains, Proceedings of ACM IoT Privacy, Trust and Security 2016.

[10] Others have pointed out earlier antecedents to blockchain - http://www.ofnumbers.com/2015/07/09/a-blockchain-with-emphasis-on-the-a/

[11] http://www.economist.com/blogs/economist-explains/2015/01/economist-explains-11 accessed May 2016.

[12] Personal conversation between a CTO of a blockchain company and the authors, March 2016.

[13] /u/throw_awa5 posted 27 April 2016 https://www.reddit.com/r/Bitcoin/comments/4givro/upcoming_ama_mit_connection_science_team_will/d2jig1r accessed 30 April 2016.

[14] Metz C (2016) "The Plan to Unite Bitcoin With All Other Online Currencies" Wired. http://www.wired.com/2016/01/project-aims-to-unite-bitcoin-with-other-online-currencies/