

Blockchain in Development – Part I: A New Mechanism of ‘Trust’?

Blockchain is an exciting new technology that may prove to be a radical innovation—similar to technologies such as the steam engine and the Internet that triggered previous industrial revolutions—with the power to disrupt existing economic and business models. It has the potential to deliver productivity gains to multiple industries, from the financial sector to energy markets, supply chains, intellectual property management, “virtual firms”, the public sector, and beyond. Its ability to provide disintermediation, improve transparency, and increase auditability can significantly reduce transaction costs, introduce efficiency into existing value chains, challenge revenue models, and open new markets. And blockchain may prove particularly valuable in emerging market economies. Yet the technology is in its early stages of development and serious challenges and risks, both technical and regulatory, will need to be addressed before it achieves widespread adoption. Questions remain about blockchain’s scalability, interoperability, security, transition costs, data privacy, and governance. And business leaders and policy makers will need to think long and hard about when and under what conditions a blockchain initiative may be warranted.

Blockchain has generated an enormous amount of interest over the last three years, with evangelists for the technology calling it a pillar of the Fourth Industrial Revolution and sceptics dismissing it as an overhyped combination of existing technologies.¹

So, what is blockchain?

Confusion persists among the public, businesses, and policymakers as to blockchain’s structure, utility, and applicability—and even its name. The term blockchain is often used interchangeably with the term distributed ledger technology, and the technology is still associated with its first incarnation, bitcoin.

Though it has existed since 2009, blockchain has attracted a new level of interest over the last two years amid growing awareness that it could be exploited beyond digital currencies and used for other types of inter-organizational cooperation and value transfer.

Thanks to its enabling potential for digital proof of identity and costless verification, blockchain could have a wide range of applications, in the financial sector and beyond. These include peer-to-peer technology, energy markets, supply chain certification and intellectual property management.

Overview of distributed ledger technology

Evolution of ledgers: from centralized to distributed

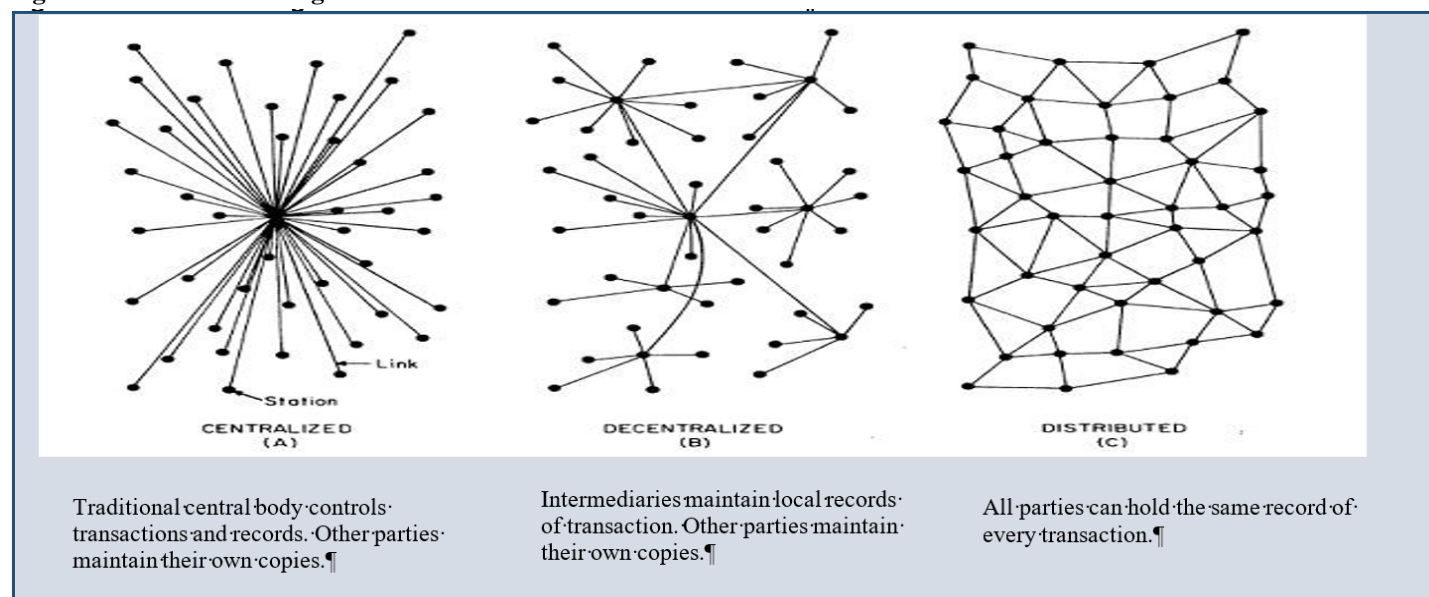
Blockchain introduces a database that functions like a distributed network, hence the term ‘distributed ledger’—with the promise of near friction-free cooperation between members of complex networks that transfer value to each other without central authorities or middlemen.

Blockchain is often referred to as a ‘radical innovation’² or general-purpose technology (GPT) not unlike the steam engine or the electric motor.³ In other words, a technology that can create “subsequent innovation and productivity gains across multiple industries,” similar to the Internet before it.⁴

Blockchain’s primary value is its ability to deploy cryptographic mechanisms to reach consensus across parties in the ledger. This eliminates the need for a central authority or intermediary, thereby creating a *distributed trust* system of value transfer.⁵ No single entity can amend past data entries or approve new additions to the ledger (**Figure 1**).⁶ Eliminating the need for a central trusted party can increase speed, lower transaction costs, and enhance security in the network.

Blockchain first appeared in the form of bitcoin, a peer-to-peer electronic cash system launched by Satoshi Nakamoto in 2009.

Figure 1: Evolution of Ledgers



Source: Paul Baran, *On distributed communications networks*, 1964, and Marina Niforos, 2017.

“based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without any need for a trusted third party.”⁷ Cryptographic proof refers to the cryptographic process of reaching consensus through proof of work eliminating the need for a trusted intermediary. Bitcoin originally had a strong anti-establishment undercurrent, backed by a community of techno-libertarians or crypto-anarchists seeking to establish a currency outside of government control and censorship.

Bitcoin’s commitment to anonymity in transactions unfortunately also opened the platform to illicit activities such as drug trafficking and tarnished its reputation with governments and the public alike. Despite this, the development of bitcoin continued. Its market capitalization is approximately \$42 billion and it is used by millions of people for payments, including a growing remittances market.⁸

Designed to be much more than a payment system, Ethereum was launched in 2014 as an open-source, public, blockchain-based distributed computing platform that provides a ‘cryptoeconomically-secured’ platform for the development of any kind of decentralized application.⁹ Given the extended capabilities it provides to the original bitcoin-oriented technology, it is often called Blockchain 2.0.

Ethereum uses ‘ether,’ a cryptocurrency token to compensate participant nodes for computations performed. Ethereum introduced the possibility of smart contracts, or “deterministic exchange mechanisms controlled by digital means that can

carry out the direct transaction of value between untrusted agents.”¹⁰ Ethereum’s market capitalization exceeded \$26 billion in July 2017, which is especially noteworthy since it stood at under \$1 billion just six months earlier.¹¹

How does blockchain work?

Blockchain is essentially a meta-technology that consists of game theory, cryptography, and mainstream software engineering.¹² Blockchain protocols verify numbers or programs, time stamp them, and enter them as a block into a continuous chain linked to all previous blocks linked to the original transaction.¹³ Assets may be created directly on the network. For example, cryptocurrencies and rights to real world assets can have a digital representation as a token¹⁴ (referred to as “tokenized assets”).¹⁵

A distributed ledger technology, or DLT, network can be either open (permission-less) or private (permissioned). Assets on a DLT network, whether the network is public or private, are cryptographically secured using a public-private key combination. A *public key* is the “address” where the digital asset is located on the network. A *private key* is the code that gives the holder access to the asset at the address represented by the corresponding public key. Once a transaction is initiated, it is broadcast on the network to all ‘nodes’, or participating computers,¹⁶ and the nodes acknowledge acceptance of the block by using its *hash*¹⁷ as an input when working on creating the next block.¹⁸

This publication may be reused for noncommercial purposes if the source is cited as IFC, a member of the World Bank Group.

Figure 2: Blockchain Value Chain



Source: The Blockchain Lab; theblockchainlab.com

A cryptographic hash function represents the process by which *miners* (nodes participating in the computational review process performed on each "block" of data) verify and timestamp transactions. Time stamped records are displayed in a sequential manner ('blocks in a chain') to all parties on the network who have the appropriate access levels (Figure 2).¹⁹

The time required to verify and record a transaction on the distributed ledger technology network varies depending on the process employed (for example, 'proof of work'²⁰ for bitcoin or 'proof of stake'²¹ for Ethereum).

Open versus private distributed ledger technology networks

Open (permission-less) networks are accessible to anyone wishing to join, without restriction on membership. Data stored on these networks is visible to all participants in encrypted format. Digital currency bitcoin is an example. Open distributed ledger technology networks do not have a central authority. Instead, they rely on network participants to verify transactions and record data on the network, based on a certain protocol.

The '*miners*' participating in the verification process are incentivized to perform computationally complex tasks in exchange for bitcoin rewards ('tokens'). This consensus-based process ('proof of work' in bitcoin) to ensure encryption of the data requires intense computational power, which some qualify as wasteful and restraining to the scalability of the system. However, it is this feature that guarantees the chain's robust security, making bitcoin more resilient to attacks. On a public blockchain, sensitive data needs to be encrypted to ensure privacy, but encrypted data cannot be used by smart contracts, so there is less flexibility on bitcoin for complex or highly regulated 'transactions' (see Challenges below).

By contrast, **private or permissioned networks** cannot access data without prior permission. Permission levels may be tiered,

such that different entities and individuals may have varying levels of authority to conduct transactions and view data (as such, they are closer to relational databases currently in use in large corporations). There are 'trusted' nodes or system administrators that control access and rights onto the network. They can still have an important effect in reducing transaction costs within the ecosystem of participating entities.

Established companies, particularly those in the financial industry, are gradually adopting private distributed ledgers for internal use, as well as for conducting transactions with trusted partners, attempting to experiment with the new technology while maintaining data confidentiality. This also allows them to comply with regulations, something not possible under the conditions of complete anonymity of open networks.

Box 1: Key advantages for Distributed Ledger Technology

Distributed and sustainable. The ledger is shared, updated with every transaction and selectively replicated among participants in near real-time. Privacy is maintained via cryptographic techniques and/or data partitioning techniques to give participants selective visibility into the ledger; both transactions and the identity of transacting parties can be masked. Because it is not owned or controlled by any single organization, the blockchain platform's continued existence isn't dependent on any individual entity.

Secure and indelible. Cryptography authenticates and verifies transactions and allows participants to see only the parts of the ledger that are relevant to them. Once conditions are agreed to, participants can't tamper with a record of the transaction. Errors can only be reversed with new transactions

Transparent and auditable. Participants in a transaction have access to the same records, allowing them to validate transactions and verify identities or ownership without the need for third-party intermediaries. Transactions are time-stamped and can be verified in near real-time.

Orchestrated and flexible. Business rules and smart contracts that execute based on one or more conditions can be built into the platform, helping blockchain business networks to evolve as they mature and support end-to-end business processes and a wide range of activities.

Consensus-based and transactional. All relevant network participants must agree that a transaction is valid. This is achieved by using consensus algorithms. Blockchains establish the conditions under which a transaction or asset exchange can occur.

Source: IBM Institute for Business Value

This publication may be reused for noncommercial purposes if the source is cited as IFC, a member of the World Bank Group.

Noteworthy industry initiatives to pilot private distributed ledger technology in financial services include Digital Asset Holdings, Chain, R3's Corda (which describes itself as a distributed ledger technology but not a blockchain), and Ripple/Interledger. Linux Foundation's HyperLedger Project and Ethereum Enterprise Alliance, while focusing primarily on the financial sector, have a vision to test applications beyond financial services, with HyperLedger already involved in proofs of concept in supply chain provenance initiatives.

Enabling a 'distributed trust' system through Distributed Ledgers—Economic and business model implications

The innovation of blockchain is capable of transforming the infrastructure of our economic systems, not only financial services, where most of the attention is currently concentrated, but entire global value chains and revenue models. It offers a chance to reimagine industries, rebuild financial processes, and build markets once considered improbable or unprofitable.

The blockchain provides an infrastructure where trust in transactions is not brokered by intermediaries—as has been the case until now—but is embodied algorithmically in the transaction itself.

The algorithmic consensus process is the trust agent. Its effectiveness can be further enhanced if combined with the use of smart contracts and digital compliance (Box 1)

This process of disintermediation and decentralization, coupled with increased transparency and auditability, provides for improved efficiency, speed, and cost reduction (such as in Know-Your-Customer verification). Its

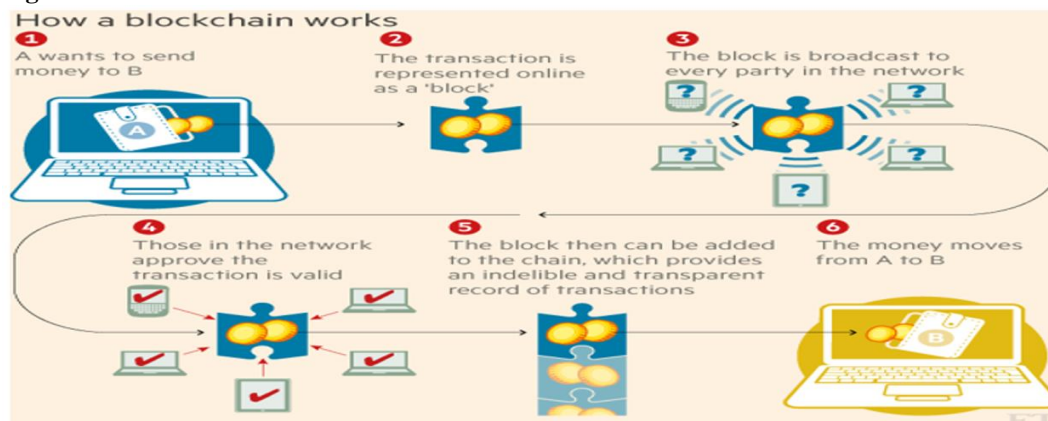
immutability provides for a verifiable audit trail of any physical or digital asset.²⁴

Financial Services: Blockchain was first used in the financial services industry, where it has been enabling digital payment systems and remittances as well as testing more complex financial instruments and transactions such as insurance, deposits, lending, capital raising, and investment management.²⁵

Global payments, trade finance, and automated compliance are some of the most active experimentation domains for blockchain today. There have been more than 2,500 blockchain related patent filings and over \$1.4 billion in investments in just three years.²⁶ At least 24 countries are investing in the technology, 50 corporations have joined consortia around it, and 90 banks are in discussions about it worldwide. Deloitte reports that 80 percent of banks will be initiating projects on blockchain by next year.²⁷

Beyond financial services — A potential business and public governance paradigm shift: In principle, any type of asset can be tokenized, tracked, and traded through a blockchain. Blockchain can serve as a registry, inventory system, and transaction platform for recording, tracking, monitoring, and transferring rights to different asset classes, including intellectual property, votes, digital identity, health data, and real estate. Information about the origin of goods, identity

Figure 3. How does blockchain work?



Source: Financial Times

While private networks are practical and encourage other companies to adopt the technology, they may hinder security, since private blockchains are paradoxically more vulnerable to external attacks. And questions about the interoperability of these coexisting private blockchains may arise in the future.

A heated debate, akin to that of the 1990s Internet versus intranet concepts, surrounds the question of open or private networks relating to improved security, creating new markets, and promoting inclusiveness.²² However, public or private blockchains are not mutually exclusive. There may also be “partially decentralized” blockchains. In these, the right to read the blockchain may be public, or restricted to the participants, or have hybrid routes that allow members of the public to make a limited number of queries. Additionally, data from a private blockchain can be periodically fingerprinted (hashed) and sent to a public one, which can provide additional auditability.²³

The blockchain ecosystem is currently in full experimentation mode, bringing new innovations and hybrid solutions. Consortia are emerging globally to discuss and provide solutions, address governance and industry standard issues, and provide regulatory insights. These include The Ethereum Enterprise Alliance and China Ledger, which are attracting participation from dozens of major industry players, innovators, regulators, and governments.

This publication may be reused for noncommercial purposes if the source is cited as IFC, a member of the World Bank Group.

credentials, and digital rights can be securely stored and traced with a distributed ledger.

Although its innovation is in early stages, blockchain use already includes medical record companies such as MedRec and Pokitdok; digital rights and micropayments innovators such as the Brave browser, Ascribe, and Open Music Initiative; identity companies such as Uport, BitNation, and BanQu; supply chain innovators such as Everledger, Hyperledger, and Provenance; and peer-to-peer renewable energy disruptors such as LO3 Energy and the Sun Exchange.²⁸

“We should think about blockchain as another class of thing like the Internet – a comprehensive information technology with tiered technical levels and multiple classes of applications for any form of asset registry, inventory, and exchange, including every area of finance, economics, and money; hard assets including physical property; and intangible assets such as votes, ideas, reputation, intention, health data, information, etc.” — Melanie Swan, Founder, Institute for Blockchain Studies

“A distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within the network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes or seconds.” — Mark Walport, UK Government Chief Science Advisor

“It has math. It has its computer science. It has its cryptography. It has its economics. It has its political and social philosophy.” - Vitalik Buterin, Founder of Ethereum

Additionally, distributed ledger technology can replace partially or entirely the government’s role as the direct authority in identity authentication, issuing certificates, land titles, storing health records, disseminating social security benefits, and managing votes and civic participation.

Estonia is a good example of how blockchain can be used in this way, with the country’s blockchain-enabled platform, known as X-Road, used to provide integrated services to citizens across multiple programs. Similarly, the Dubai government recently announced a comprehensive blockchain strategy to help its agencies run more efficiently, with the aim of saving up to 5.5 billion dirhams per year.²⁹

Since it operates without the need for a central authority, distributed ledger technology challenges the assumptions of governance systems that underpin today’s business models and economic and political systems, threatening entire professions and even governments. Blockchain has both the economic and organizational potential to reduce costs across global value chains and ‘redefine an organization’s traditional boundaries.’

This publication may be reused for noncommercial purposes if the source is cited as IFC, a member of the World Bank Group.

blurring the lines between private and public, individual and collective.³⁰

Conclusion

In the real world, the choices for business leaders regarding blockchain will not be clear cut. While the potential of blockchain is immense, so is the uncertainty surrounding it. The technology is not a complete solution to be applied ubiquitously, but instead is one piece of a well-articulated digital transformation strategy that probably includes artificial intelligence and big data management, among other emerging technologies. Companies need to proceed deliberately but cautiously, in the context of a thorough cost-benefit analysis. There is no magic formula that fits all firms or situations.

Before embarking on a blockchain initiative, organizations need to determine whether blockchain is anchored in their strategy and how it will address existing business problems. They will also need to decide if blockchain can reduce costs and promote market expansion, and determine whether and when to reengineer their business model to stay ahead of the competition.

Decision makers must also measure the potential technical, financial, and reputational risks associated with blockchain implementation, and find ways to hedge against them, for example by limiting the perimeter of the project or starting with middle- or back-office improvements that have no direct customer exposure. Businesses also need to determine the direct and organizational costs of testing and adopting blockchain technology, as it may stress already limited resources. ■

About the Author

Marina Niforos is the founder and Principal of Logos Global Advisors, a strategic advisory firm to high-growth startups and large multinationals, helping them form partnerships and leverage opportunities for growth. She is also Visiting Faculty of Leadership at HEC Hautes Études Commerciales de Paris. (marina.niforos@logosglobaladvisors.com)

Acknowledgments

The author would like to thank the following colleagues for their review and suggestions: Vijaya Ramachandran, Senior Fellow, Center for Global Development; Michael Pisa, Policy Fellow, Center for Global Development; Susan Starnes, Strategy Officer, Sector Economics and Development Impact, Economics and Private Sector Development, IFC; William Haworth, Consultant, Financial Institutions Group, IFC; and Thomas Rehmann, Senior Economist, Thought Leadership, Economics and Private Sector Development, IFC.

Additional EM Compass Notes about Blockchain

This note is the first in a series of five complementary EM Compass Notes by this author: The notes focus on: (1) a general overview of blockchain technology (this note), (2) an outlook for blockchain’s implications for emerging markets (Note 41);

(3) a general overview of the impact of blockchain on financial services (forthcoming), (4) an emerging market regional analysis of blockchain developments in financial services (forthcoming) and, (5) implications of the technology beyond financial technology (forthcoming).

Please also refer to EM Compass Note 38, “Can Blockchain Technology Address De-Risking in Emerging Markets?” by Vijaya Ramachandran and Thomas Rehermann, for how blockchain can be used to mitigate de-risking by financial institutions, which affects recipients of remittances, businesses that need correspondent banking relationships, and charities working in conflict countries.

¹ The Fourth Industrial Revolution is the digital transformation economies are undergoing, characterized by a fusion of technologies that blur the lines between physical, digital, and biological spheres.

² Beck, Roman and Christopher Müller-Bloch. 2015. “Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers as incumbent organization.” Proceedings of the 50th Hawaii International Conference on System Sciences, 5390-5399.

³ Bresnahan, Timothy and Manuel Trajtenberg. 1995. “General purpose technologies ‘Engines of growth’?” Journal of Econometrics, 65(1), 83-108.

⁴ Catalini, Christian and Joshua S. Gans. 2016. “Some Simple Economics of the Blockchain.” MIT Sloan Research Paper No. 5191-16.

⁵ Casey, Michael. 2016. “The Blockchain: Decentralized trust to unlock a decentralized future.” oreilly.com, September 8.

⁶ World Bank Group. 2017. “Distributed Ledger Technology (DLT) and Blockchain.” April. FinTech Note 1 (draft).

⁷ Nakamoto, Satoshi. 2008. “Bitcoin: A Peer-to-Peer Electronic Cash System, www.bitcoing.org.

⁸ Bitcoin Market Capitalization. July 7 2017. CoinDesk, coindesk.com/price/.

⁹ The CoinTelegraph, “A Brief History of Ethereum From Vitalik Buterin’s Idea to Release.” <https://cointelegraph.com/ethereum-for-beginners/a-brief-history-of-ethereum-from-vitalik-buterins-idea-to-release>

¹⁰ Szabo, Nick. 1997. “The idea of smart contracts.” Nick Szabo’s Papers and Concise Tutorials.

¹¹ Cryptocurrency Capitalizations, Coinmarketcap.com.

¹² Mougayar, William. 2016. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Wiley.

¹³ Davidson, Sinclair, Primavera De Filippi, Jason Potts. 2016. “Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology.” SSRN.

¹⁴ Cameron-Huff, Addison. 2017. “How Tokenization is Putting Real-World Assets on Blockchains.” March 30. nasdaq.com.

¹⁵ “Distributed ledger technology: Implications of blockchain for the securities industry.” January 2017. Finra.

¹⁶ Ibid.

¹⁷ A hash function is a mathematical process that takes input data of any size, performs an operation on it, and returns output data of a fixed size. In the bitcoin protocol, hash functions are part of the block hashing algorithm which is used to write new transactions into the blockchain through the mining process.

¹⁸ A consensus-based verification process requires that a majority of network participants confirm the integrity of the data in a transaction before that transaction is verified and recorded on the blockchain.

¹⁹ “Blockchain - Out of the blocks: From hype to prototype.” 2016. Efma.com. <https://www.efma.com/study/detail/25582>.

²⁰ A proof-of-work-based verification process typically requires participants on the network to conduct some work and establish an economic interest (for example, obtain a bitcoin) in the process of validating the integrity of the data in the transaction.

²¹ Investopedia, *Proof of Stake (POS)*, definition. www.investopedia.com/terms/p/proof-stake-pos.asp.

²² “Fast Forward: Rethinking enterprises, ecosystems and economies with blockchains. 2016. IBM Institute for Business Value, Executive Report Blockchain.

²³ Gupta, Vinay. 2017. “Building the Hyperconnected Future on Blockchains.” Report for the World Government Summit.

²⁴ World Bank Group. 2017. “Distributed Ledger Technology (DLT) and Blockchain.” April. FinTech Note 1 (draft).

²⁵ Swan, M., *Blockchain: Blueprint for a new economy*, 2015.

²⁶ “Over the horizon: Blockchain and the future of financial infrastructure.” 2016. Deloitte.

²⁷ “Blockchain - Out of the blocks: From hype to prototype.” 2016.

²⁸ Catalini, Christian. 2017. “How Blockchain Applications Will Move Beyond Finance.” March 2. Harvard Business Review.

²⁹ “Dubai Blockchain Strategy.” 2016. Smart Dubai.

³⁰ “Fast forward: Rethinking enterprises, ecosystems and economies with blockchains.” 2016. IBM Institute for Business Value.