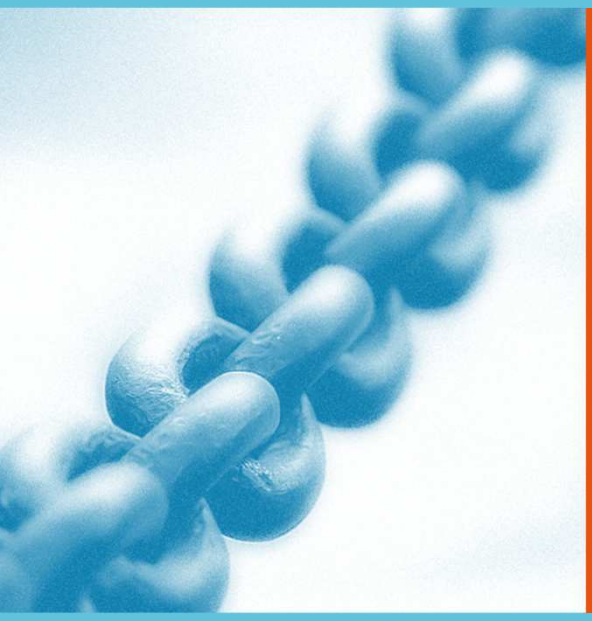
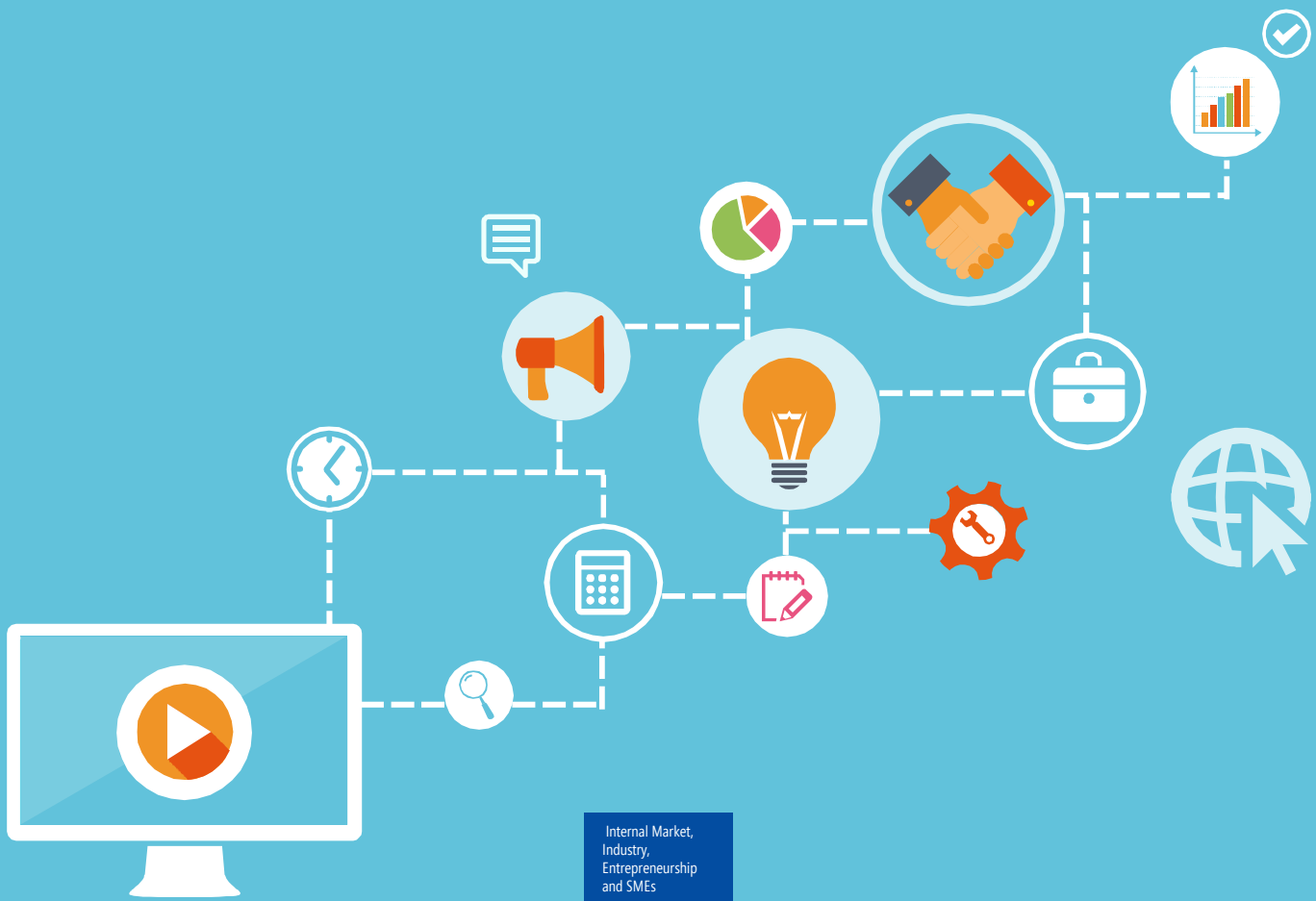
European Commission



Digital Transformation Monitor

Blockchain

January 2018



Internal Market, Industry, Entrepreneurship and SMEs

Blockchain

Emerging from the world of crypto-currencies, Blockchain appeared as a new class of IT infrastructure with numerous applications in the financial sector but also in many other domains. It is a secure way to share digital information that reduces the need for intermediaries and regulatory authorities. This raises several challenges, particularly regarding Blockchain's ability to disrupt ecosystems, its legal acceptability and other risks linked with its use in financially speculative activities.

1

Trusted Infrastructure

Blockchain gained notoriety with the rise of the Bitcoin cryptocurrency; but beyond this initial use, it can be an important piece of infrastructure with which trusted digital applications can be built.

The technology behind Bitcoin

Blockchain is the technological heart of the cryptocurrency known as Bitcoin. It acts as a shared digital registry that records and stores every Bitcoin transaction. It ensures the security of exchanges in an online ecosystem where there is no trust between parties.

The need for a transaction ledger

The Bitcoin cryptocurrency was launched in 2008-2009[1], and was seen by its founders as a technological response to the global financial crisis.

The objective of the Bitcoin initiative was to create a form of currency that would serve as a day to day means of exchange and that would be independent, both from nation states and central banks.

The new currency needed a dependable digital infrastructure to ensure the security and validity of transactions. This led to the creation of Blockchain: a secure digital registry that, for Bitcoin, is used to monitor and store every past transaction.

Mining - peer to peer validation in an untrusted environment

To validate transactions, Bitcoin relies on a decentralized network of "miners"[2]. Each "miner" is a computer – a node of a decentralized network - which competes with other computers to validate transactions. The first "miner" to validate a transaction receives a financial incentive through the creation of new currency.

This mechanism, called "Proof of Work" ensure the security of the system by demanding that miners invest significant amounts of computing power and time in the validation of transactions.

To compromise the system, an attacker would have to control over 50% of the processing power of the whole network[3].

Limits of cryptocurrencies

Although it brings security to the system, the "Proof of Work" mechanism is one of the limits of cryptocurrencies because it limits the number of transactions per second and contributes to the high energy cost, limiting its scalability and making it impractical as a global payments system.

A technology not limited to cryptocurrencies

Beyond its use in cryptocurrencies, Blockchain has found other applications that have built upon its high level of security.

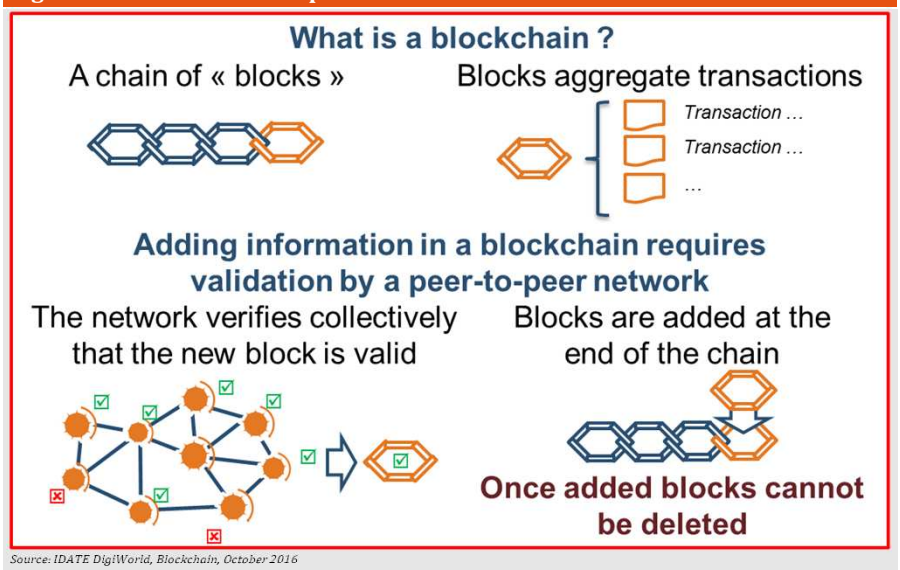
Secure, shared information storage

Blockchain has evolved to define a large range of technologies, that are fundamentally secure digital storage facilities.

Even if the implementation differs, the core principles of Blockchain are decentralization (no central authority), and immutability (impossibility to delete or alter stored data). Blockchains can be either public or permissioned registries (that limit their access to a consortium).

Public or permissioned, the main and most important feature of Blockchain is to act as a neutral infrastructure, over which no single actor has full control. Blockchain thus allows the exchange of data with third parties in which trust is limited (from complete strangers to the ecosystems of competitors).

Figure 1: Blockchain Principles[4]



Source: IDATE DigiWorld, Blockchain, October 2016

A registry for any type of data

Blockchain was first used as a secure transaction ledger, and it has continued to expand in this role, to the point where it can now be used as a secure ledger for all kinds of transactions.

Some of the key features of Blockchain infrastructures, such as immutability and authentication have rapidly attracted the attention of users with other purposes in mind for the Blockchain ecosystem.

In addition to acting as a transaction ledger, Blockchain is now increasingly used to securely store documents[5]. This is especially relevant for documents where the time of creation and authenticity must be preserved and secured.

Automated transactions: smart contracts

Another extension of the initial principle of Blockchain the possibility to use it to define conditional financial transactions, that will execute only when the predefined conditions are met.

This possibility, widely known as a "Smart Contract"[6] creates the option of automated financial transactions. The "contract" is defined in software, and stored in the blockchain.

Once agreed between the parties, the execution of the "contract" is entirely automated, with no need for third party authority and no possibility of modification.

Limits of the technology

Although some Blockchain applications are fully deployed and can be considered mature, the technology still has substantial limitations.

Limits of consensus algorithms

Alternatives to the "Proof of Work" concept underpinning traditional cryptocurrencies, such as "Proof of Stake"[7] algorithms, do exist, though they are not as secure as Blockchain. The limits of "Proof of Work" mostly apply to public Blockchain, like that used by cryptocurrencies, because it limits the level of scalability. Conversely, "Proof of Work" favours Blockchain applications that are limited to a known, restricted ecosystem (consortium Blockchain, with different security requirements) such as those commonly used in B2B scenarios.

A consensus algorithm that would be secure, scalable and efficient in both open and restricted ecosystems would have wide application potential, and remains an open research problem.

Limits of Smart Contracts

Another important limit of Blockchain concerns so-called "Smart Contracts", a promising but immature technology. In particular, the immutability and lack of recourse options make them inappropriate for use as legal contracts as defined by traditional legislative standards[8]. Beyond this, the immutability of a "Smart Contract" can cause significant issues if the computer program representing the contract is faulty or malfunctions, as occurred in the case of "The DAO" [9], where substantial financial loss was incurred.

Controlling the edges of the system

A final limit of Blockchain technology involves interactions between Blockchain environments and other less secure systems[10]. Information stored in Blockchain can be trusted only to the same extent as its original source – this constitutes a serious challenge from a systems-engineering standpoint, and is one of the main reasons why only a few applications of Blockchain have found widespread usage, despite many for which proof of concept exists.

2

Applications in Finance and Beyond

Still mostly used in financial applications, Blockchain is increasingly considered an application-neutral infrastructure.

Financial applications

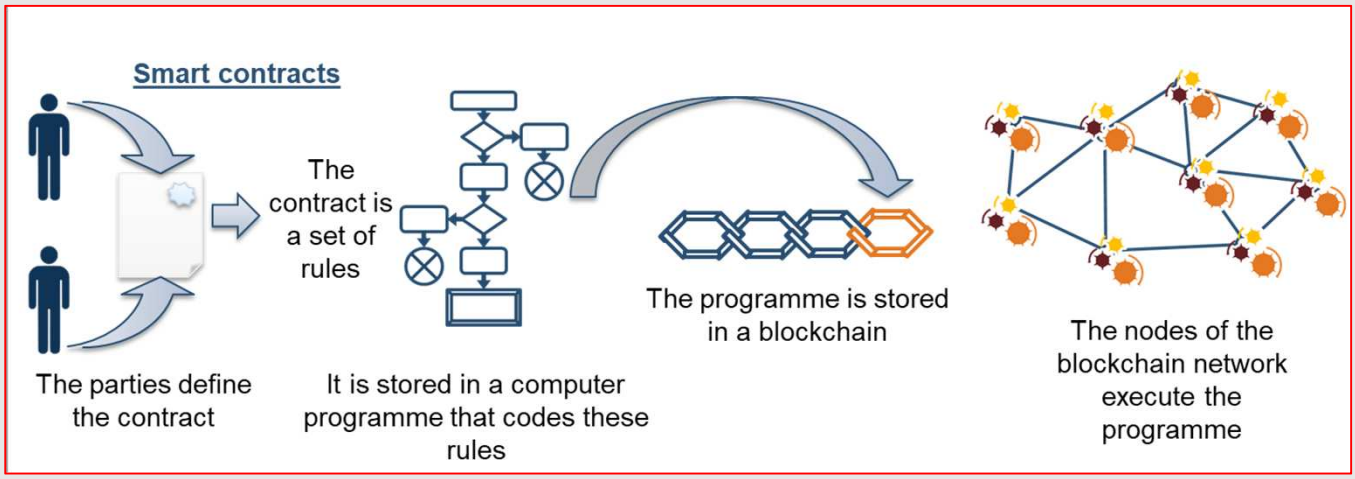
Financial applications remain the most common use for Blockchain. A distinction should however be made between applications targeting cryptocurrencies and those using Blockchain as a form of back-office infrastructure in traditional finance.

Financial services for cryptocurrencies

Arising from Blockchain's initial ability to perform direct peer-to-peer financial transactions, a whole financial ecosystem now exists to service cryptocurrencies. Its vendors provide similar operations to classic financial institutions, including portfolio management, loans, short and long-term investment, trading, savings accounts and crowdfunding (including the "Initial Coin Offering"[11] model). The Chicago Stock Exchange recently started to allow the trading of Bitcoin futures and derivatives[12] in a sign of just how accepted cryptocurrencies are becoming.

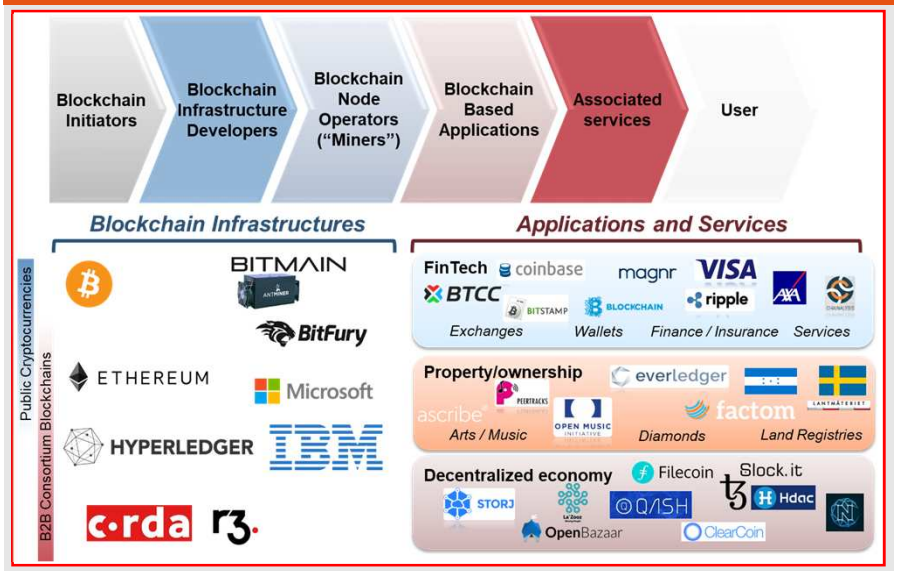
This being said, despite their initial conception as a means of online exchange, cryptocurrencies have instead evolved mostly as a speculative asset and in some cases, a reserve asset. For example a part of the Bitcoin community consider bitcoin as a reserve asset similar to gold.

Figure 2 : Smart Contract principles.



Source: IDATE DigiWorld, Blockchain, October 2016

Figure 3 : Value chain and key applications.



Source: IDATE DigiWorld, Blockchain, October 2016

Blockchain as a back office solution

Blockchain has also been adopted by the traditional financial sector as a back office infrastructure solution for facilitating data exchange between financial institutions and reducing the need for intermediaries and/or state supervision. Several experiments have seen banks form consortiums such as the R3VEC initiative, which included more than 70 banks[14], in order to explore the perceived benefits of Blockchain infrastructure, particularly its ability to cut costs, intermediary numbers and transaction times, especially for international fund transfers.

Banks are not alone in this, with insurance companies also closely examining the possibilities offered by Blockchain, especially for "Smart Contracts" to automate payments. For example, a initial service offering developed by AXA automates the payment of flight-delay insurance through a Blockchain[15].

The use of Blockchain for bank to bank transactions could reduce the cost of international payments by up to 42% [16].

Property and asset management

Blockchain's ability to hold a secure, future-proof ledger of transactions is also attractive for tracking valuable non-financial assets. A range of initiatives are taking Blockchain technology and applying it to other asset classes, including digital art works[17], diamonds[18], music files[19], land registry[20], asset tracking[21] etc.

The main advantages of applying Blockchain like this include lower registry costs, lower costs for the validation of ownership certificates or deeds and the level of security of the record, which reduces the risk of fraud.

The use of "Smart Contracts" also opens up a host of possibilities for transferring ownership or rental and leasing arrangements[22] (pay-per-use).

Blockchain as a form of secure infrastructure isn't necessarily revolutionary, but its ability to deliver cost reduction and optimization opportunities across many industries makes it a technology worth watching.

Opportunities for infrastructure

The demand for Blockchain infrastructure, arising from its wide range of applications, represents an opportunity for new and established digital infrastructure providers, who have duly gone about devising a growing portfolio of Blockchain infrastructure solutions.

Infrastructure for cryptocurrencies

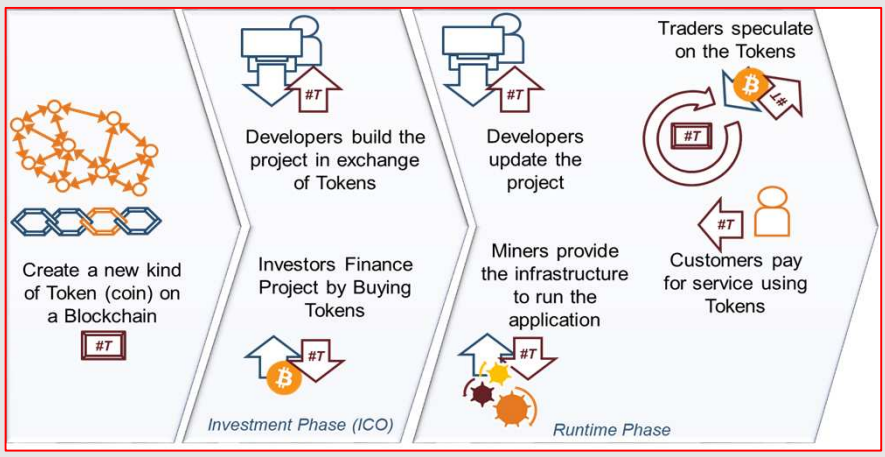
An important aspect in the expansion of Blockchain infrastructure has been the development of solutions targeting cryptocurrencies. A whole industry revolves around the "mining" activity, including providers of specialized "mining" software and hardware, as well as operators of "mining" nodes. Indeed, Chinese companies such as Bitmain[23] and BitFury[24] have gained significant notoriety from their Bitcoin mining activities. Various approaches to profit exist, with some operators joining forces to form node pools, where any rewards earned are shared, whereas others have pursued large, purpose-built datacenters with optimized microprocessors devoted to Bitcoin mining.

The Blockchain technology market is estimated to grow in value from $210.2mn to $2.3bn between 2016 and 2021 [25].

The main opportunity for the IT industry lies in integrating Blockchain with their traditional portfolios of IT and security software. Blockchain is well-suited for this, given its ability to act as a neutral data exchange platform within a complex existing ecosystem (co-opetitors[26]). This has presented market opportunities for a range of start-ups focused on providing Blockchain for specific application domains.

Perhaps more importantly, it has attracted industry leaders like IBM (strongly positioned with its Hyperledger[27] Blockchain ecosystem), Microsoft (promoting Blockchain as a Service[28] offering based on Microsoft Azure and Ethereum), and other IT service companies (Accenture, ATOS, CapGemini, etc.).

Figure 3 : Initial Coin Offering (ICO) Funding and Business Model.



Source: IDATE DigiWorld, Blockchain, October 2016

3 Challenges

While it may be tempting to consider Blockchain as "just another form of IT infrastructure", the technology is unique due both to its link with the cryptocurrency world and, more generally, to its disruption potential for existing business models.

The challenge of disintermediation

One of the most important challenges related to Blockchain thus far is its ability to remove intermediaries from transactions and interactions.

Blockchain: intermediary free

Despite its wide and varied applicability, Blockchain technology in all its forms is considered a neutral data-sharing infrastructure. As such, much of its promise lies in its power to enable true, direct peer-to-peer interactions while reducing the transaction cost by removing intermediaries who would typically take a percentage of the transaction as a fee for its facilitation.

Blockchain therefore poses a threat firms whose main business model involves being a "trusted third party"; this can include those who facilitate B2B relationships, maintain transaction ledgers, arbitrate disputes etc.

A necessary evolution of the trusted third party role

Despite this potential, the widespread adaption of a fully decentralized model seems unlikely in the near future. In fact, most trusted third parties will benefit from Blockchain in the short-term as it will help streamline the complexity of their exchanges and reduce their operating costs. For the time being, it seems that the majority of end-consumers will continue to access the services they require through their existing trusted third parties, with Blockchain causing changes in their role and organization rather than their demise.

The main challenge for Blockchain therefore appears to be one of how it can facilitate changes that strengthen the trusted third parties it may one day replace, while continuing to understand and exploit the opportunities inherent in its design.

Blockchain for public services

Public services themselves also stand to be directly impacted by Blockchain due to their common role in establishing and certifying trusted third party institutions.

Despite this, Blockchain offers the potential for digital public services to be provided in a manner that is more secure, decentralized and open, to both citizens and corporations, than today. Experiments with Blockchain use in land registries have become notorious[20], but other uses have also been considered (notably in Estonia[29]) including public digital notaries and secure health record applications.

The challenges of cryptocurrencies

Cryptocurrencies were created as a challenge for both nation states and the established financial sector. Despite the failure to achieve their original goals (wide usage in day-to-day transactions), they have been subject to regulation and a reputation as a risky asset, meaning that they still face significant challenges.

Risks linked with speculation

The use of cryptocurrencies (notably Bitcoin) as speculative assets has raised concerns about the creation of a speculative bubble. While the short-term impact on the global economy of such a bubble bursting would be limited due to the lack of existing ties with the traditional financial system, the trend toward the development of cryptocurrency-based derivatives may open the door to much higher risk levels in the future if cryptocurrencies begin to become entwined with traditional financial products.

Legal uncertainties

Cryptocurrencies are generally not governed by well-defined legal frameworks, even though financial regulators do closely monitor their development. This lack of framework creates uncertainty for citizens, business and states regarding the status of cryptocurrency holdings as an asset, particularly from a fiscal and tax perspective.

Similarly, even if the archive of a document held in a public cryptocurrency Blockchain is technically able to prove the document's provenance, the status and validity of the archive itself is subject to no legal precedent, leaving great uncertainty as to the outcome of any legal dispute.

References

[1] Bitcoin, 2008, Bitcoin: A Peer-to-Peer Electronic Cash System, Available at: https://bitcoin.org/bitcoin.pdf

[2.] O'Reilly, 2015, Mastering Bitcoin: Unlocking Digital Cryptocurrencies ISBN: 978-1449374044

[3.] Bitcoin Stackexchange, 2011, What can an attacker with 51% of hash power do? Available at: https://bitcoin.stackexchange.com/questions/658/what-can-an-attacker-with-51-of-hash-power-do

[4.] IDATE, 2016, Blockchain a new IT infrastructure, Available at: https://en.idate.org/product/blockchain/

[5.] Brave NewCoin, 2014, Using Blockchain Technology To Prove Existence Of A Document, Available at: https://bravenewcoin.com/news/using-blockchain-technology-to-prove-existence-of-a-document/

[6.] The Economist, 2016, Not So Clever Contracts, Available at: https://www.economist.com/news/business/21702758-time-being-least-human-judgment-still-better-bet-cold-hearted

[7.] Blockgeeks, 2016, Proof of work vs Proof of stake: basic mining guide, Available at: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

[8] Georgetown Law, 2017, The law and Legality of Smart Contracts, Available at: https://www.georgetownlawtechreview.org/the-law-and-legality-of-smart-contracts/GLTR-04-2017/

[9.] Bloomberg Markets, 2017, The Ether Thief, Available at: https://www.bloomberg.com/features/2017-the-ether-thief/

[10.] Oraclize, 2016, Understanding Oracles, Available at: https://blog.oraclize.it/understanding-oracles-99055c9c9f7b

[11.] Forbes, 2017, Initial Coin Offering: A New Way To Fundraise For Your Business, Available at: https://www.forbes.com/sites/theyec/2017/11/20/initial-coin-offering-a-new-way-to-fundraise-for-your-business/#610e26e2307d

[12.] Financial Times, 2017, US regulator gives green light for bitcoin futures trading, Available at: https://www.ft.com/content/43d69af8-d6b0-11e7-8c9a-d9c0a5c8d5c9

[13.] The Telegraph, 2017, Bitcoin could be the new gold, says JP Morgan , Available at: http://www.telegraph.co.uk/business/2017/12/04/bitcoin-could-new-gold-says-jp-morgan/

[14.] R3CEV, 2015, Building the new operating system for financial markets, Available at: https://www.r3.com/about/

[15.] AXA, 2017, AXA goes blockchain with fizzy, Available at: https://www.axa.com/en/newsroom/news/axa-goes-blockchain-with-fizzy

[16.] Ripple, 2016, The Cost-Cutting Case for Banks, Available at: https://ripple.com/files/xrp_cost_model_paper.pdf

[17.] Coindesk, 2015, How Ascribe Uses Bitcoin Tech to Help Underserved Artists, Available at: https://www.coindesk.com/ascribe-bitcoin-tech-underserved-artists/

[18.] Financial Times, 2017, De Beers to invest in blockchain-based diamond platform, Available at: https://www.ft.com/content/e86024d8-ce6f-3116-bf77-64341c4b1a0b

[19.] Business Insider, 2017, Blockchain tokens could transform the music industry, Available at: http://www.businessinsider.fr/us/blockchain-could-transform-the-music-industry-2017-11/

[20.] Kairos Future, 2017, The Land Registry in the blockchain, Available at: https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

[21.] Provenance.org, 2016, From shore to plate: Tracking tuna on the blockchain, Available at: https://www.provenance.org/tracking-tuna-on-the-blockchain

[22.] RTInsights, 2016, Blockchain and Smart Contracts: A Pilot in the Car-Leasing Business, Available at: https://www.rtinsights.com/blockchain-pilot-smart-contracts-docusign-visa/

[23.] Quartz, 2017, China's Bitmain dominates bitcoin mining. Now it wants to cash in on artificial intelligence, Available at: https://qz.com/1053799/chinas-bitmain-dominates-bitcoin-mining-now-it-wants-to-cash-in-on-artificial-intelligence/

[24.] Bitcoin.com, 2017, Bitfury is Building the "Largest Bitcoin Mining Operation in North America, Available at: https://news.bitcoin.com/bitfury-is-building-the-largest-bitcoin-mining-operation-in-north-america/

[25.] The blockchain.com, 2016, Blockchain Market Worth 2.3 Billion USD by 2021, Available at: http://www.the-blockchain.com/2016/10/11/blockchain-market-worth-2-3-billion-usd-2021/

[26.] Stewart Southey, 2018, Blockchain and Coopetition. Show me the Money, Available at: https://medium.com/@sgs_292/blockchain-and-coopetition-show-me-the-money-5f74fb2c1e3a

[27.] Fortune, 2017, Blockchain Is Pumping New Life Into Old-School Companies Like IBM and Visa, Available at: http://fortune.com/2017/12/26/blockchain-tech-companies-ibm/

[28.] Nasdaq, 2017, Microsoft Azure Bringing Blockchain Closer To Real World Use, Available at: http://www.nasdaq.com/article/microsoft-azure-bringing-blockchain-closer-to-real-world-use-cm835914

[29.] Coin Telegraph, 2017, How Estonia Brought Blockchain Closer to Citizens: GovTech Case Studies, Available at: https://cointelegraph.com/news/how-estonia-brought-blockchain-closer-to-citizens-govtech-case-studies

About the Digital Transformation Monitor

The Digital Transformation Monitor aims to foster the knowledge base on the state of play and evolution of digital transformation in Europe. The site provides a monitoring mechanism to examine key trends in digital transformation. It offers a unique insight into statistics and initiatives to support digital transformation, as well as reports on key industrial and technological opportunities, challenges and policy initiatives related to digital transformation.

Web page: https://ec.europa.eu/growth/tools-databases/dem/

This report was prepared for the European Commission, Directorate-General Internal Market, Industry, Entrepreneurship and SMEs; Directorate F: Innovation and Advanced Manufacturing; Unit F/3 KETs, Digital Manufacturing and Interoperability by the consortium composed of PwC, CARSA, IDATE and ESN, under the contract Digital Entrepreneurship Monitor (EASME/COSME/2014/004)

Authors: Bertrand Copigneaux, IDATE; Laurent Probst, Virginie Lefebvre, Julian Brown, PwC