



BLOCKCHAIN UNCHAINED:

CYBERSECURITY IMPLICATIONS & MARKET OVERVIEW

WIOLETTA BRZĘCKA, FAUSTINE FELICI, DR. MICHAEL MYLREA,
ROBERT SIUDAK, BARBARA SZTOKFISZ
FOREWORD: PROF. KRZYSZTOF PIECH
EDITOR: BARBARA SZTOKFISZ



THE KOSCIUSZKO INSTITUTE



BLOCKCHAIN UNCHAINED: CYBERSECURITY IMPLICATIONS & MARKET OVERVIEW

AUTHORS: WIOLETTA BRZĘCKA, FAUSTINE FELICI, DR. MICHAEL MYLREA,
ROBERT SIUDAK, BARBARA SZTOKFISZ

FOREWORD: PROF. KRZYSZTOF PIECH

EDITOR: BARBARA SZTOKFISZ

Publisher: The Kosciuszko Institute
Editor: Barbara Sztokfisz
Proofreading: Adam Ladziński
Typesetting: Joanna Świerad-Solińska

Copyright © 2019

Wioletta Brzęcka – The Kosciuszko Institute
Faustine Felici – The Kosciuszko Institute
Michael Mylrea, PhD – George Washington University
Robert Siudak – The Kosciuszko Institute
Barbara Sztokfisz – The Kosciuszko Institute

© The Kościuszko Institute, 2019

This report has been funded with support
from the Małopolska Region.



Responsibility for the information and views
set out in this publication lies entirely with the authors.

Kraków, 2019

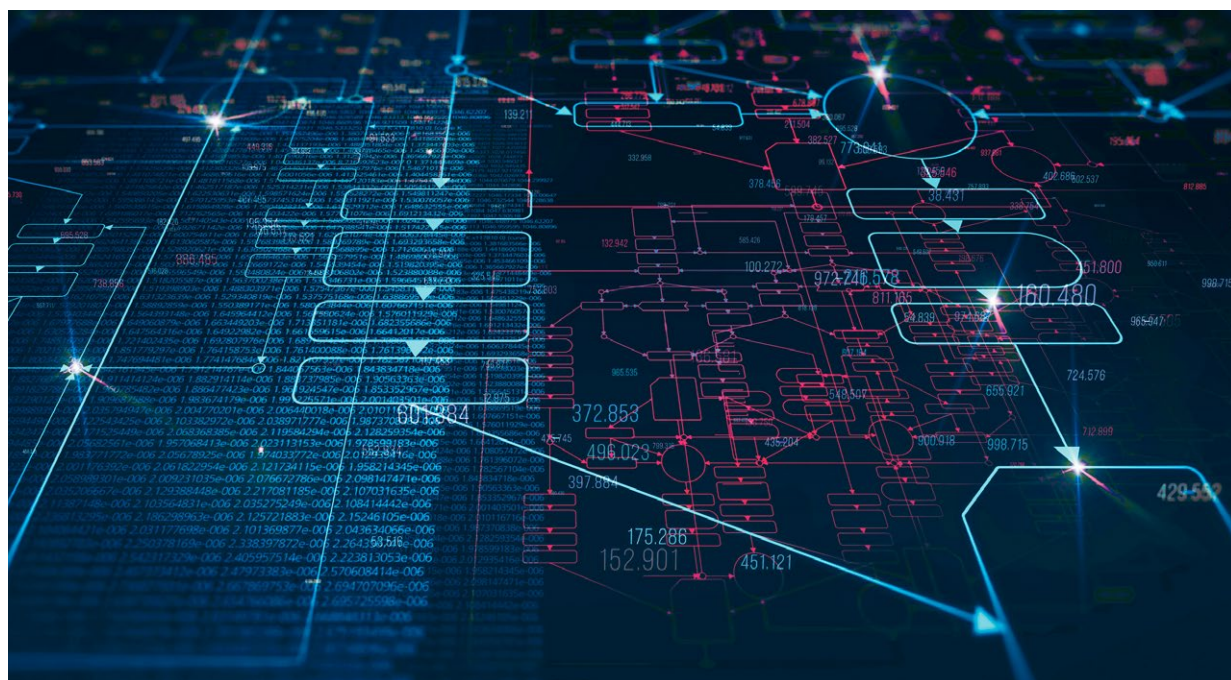
CONTENTS

FOREWORD	4
1. TRUST ON THE RISE – GENERAL OVERVIEW OF THE BLOCKCHAIN TECHNOLOGY	7
2. CYBERSECURITY OPPORTUNITY – TOWARDS RESILIENT IOT NETWORKS, SMART CONTRACTS AND DISTRIBUTED AUTONOMOUS ORGANISATIONS.....	11
3. BLOCKINGS TO BLOCKCHAIN: CHALLENGES TO OVERCOME	15
4. PRACTICAL BLOCKCHAIN APPLICATIONS AND REAL-LIFE CASE STUDIES.....	19
5. REGULATORY STATE OF PLAY IN THE EUROPEAN UNION.....	27
EXECUTIVE SUMMARY:	36

FOREWORD

Blockchain technology can have numerous uses. What is more, it seems difficult to pinpoint the areas in the modern-day digital economy where it could not or definitely should not be used. This technology has existed for a decade; for an IT solution, that is not much, and yet already dozens of millions of people take advantage of it, including up to 10% of Poles (the percentage declaring they own cryptocurrencies). As economic incentives are written into blockchain-based currencies and the system has been designed in an inflexible way market-wise, most cryptocurrencies are in the throes of financial speculation. Which on the one hand is good, since it attracts the attention, regarding blockchain, of those who are completely out of the loop, too, but on the other hand it is a bane, as three B-words are being associated and lumped together: Bitcoin, bubble and blockchain. This technology would not be the focus of global media interest were it not for Bitcoin. And since most cryptocurrencies are designed (sometimes on purpose) so that they can be the domain of speculation, they may result in speculative bubbles as well as in other phenomena deemed unwanted by both regulators (who sometimes fiercely oppose cryptocurrencies, as do Polish Financial Supervision Authority and National Bank of Poland) and amateur investors, oblivious to the risks they run.

Such dangers aside, what lies at the core of cryptocurrency functioning is still technology. Even though this technology has been successfully employed hundreds of times, uses as spectacular as cryptocurrencies are still being sought. One of its effective applications is document notarisation. It involves putting a cryptographic hash of a digital document on (private or public) blockchain. In the Polish Accelerator of Blockchain Technology, we prepared (and tested at the Lazarski University) one of the first such solutions in Poland to secure university graduation documents against counterfeiting. A similar idea was executed by a Polish-Canadian start-up in Dubai which received generous funding and considerable leeway and which we support in terms of know-how. A subsequent use of the similar concept took place in Alior Bank, and then another bank, PKO BP, outdid everyone with its solution to the 'durable medium' problem. Due to implementing a small and closed private blockchain (which means it is cheap to maintain), around 5 million of its customers could have received their documents in digital instead of paper versions while being sure there was no forgery. Interesting and worth underscoring: this was the largest blockchain technology implementation in Europe and it came from Poland. As I estimate, it bought the Bank savings of a few million zlotys annually.



The beginnings of blockchain use in Poland were very promising. We hit the ground running with Polish zloty being the third most popular currency exchanged to bitcoin until 2013. That's why in early 2014 in Poland as many as 15 projects to run a cryptocurrency exchange were proposed (during one of Bitcoin seminars at the Warsaw School of Economics). Even the US did not have so many drafts. Most of them fell through, but BitBay turned out to be a high achiever in the European cryptocurrency market. As early as 2014, the first regulatory initiative, namely 'Minimal security standards for cryptocurrency exchanges', was proposed, whose project was later continued, not only by the Polish Bitcoin Association but also under the Ministry of Digital Affairs' aegis, giving us one of the first global examples of self-regulation in the sector – the document 'The canon of good practices for digital currency market actors in Poland' along with certificates issued in conjunction with this canon (signed by the deputy minister of digital affairs, no less). Unfortunately, later this work has been hampered, mostly due to financial oversight's unfriendly approach. From the position of a global leader in regulatory processes we slid to the second tier (and in terms of market development we are already in some respects behind the top 20 states). In Europe, the trailblazers are Malta, Lithuania, Gibraltar and Switzerland. Regulatory framework inactivity or actions that were downright hostile to the cryptocurrency market have resulted in nearly all blockchain start-ups closing down or emigrating. They are seeking friendlier jurisdictions to carry out their ICOs.

Why should so much space be devoted to cryptocurrencies when discussing blockchain technology? Apart from obvious IT relations, there are other reasons:

- a) workforce availability – almost all blockchain programmers start their education with cryptocurrency code and with internship or work in cryptocurrency projects;
- b) financial incentive – blockchain start-ups have developed a unique fundraising structure that makes use of ICO (or ITO, STO and the like), which is able to attract considerable capital from international markets, whether we are talking about a start-up from Silicon Valley, Bangalore or a one-horse town;
- c) experience – cryptocurrencies are a testing ground for other projects, partly because of the financial incentive (in this case, incentive for hackers: a poorly secured blockchain and the assets accumulated in apps, for instance in digital wallets or digital exchanges, are a common target for criminals), which – somewhat paradoxically – increases the security of such code-based projects.

We are thus living in interesting times indeed, when various issues interweave: technology, market and finances, law and regulations, education and research activity. All these issues are necessary to create an innovation system that will let us to become a powerful leader in the worldwide blockchain market. Is Poland going to seize this opportunity? I hope this report will play a useful and constructive role to help it.

Krzysztof Piech, PhD

Professor at Lazarski University, Director of its Centre for Blockchain Technology
CEO, Polish Accelerator of Blockchain Technology

1. TRUST ON THE RISE – GENERAL OVERVIEW OF THE BLOCKCHAIN TECHNOLOGY

While still at a nascent stage of adoption, blockchain technology may give impetus to the fourth industrial revolution, transforming modern infrastructures from decentralised to more distributed, resilient and intelligent. Today, most critical infrastructures, from transportation to energy and from defence to financial institutions, do not collect, aggregate and exchange data in a secure way that is interoperable, smart and intelligent. A paradigm shift is needed for our smart cities' infrastructures to become more intelligent, decentralised and distributed. Blockchain technology may present a disruptive solution to give impetus to this change through an atomically verifiable cryptographic signature that provides data provenance and attribution to help increase the trustworthiness and integrity for prodigious data sets that are being exchanged.

Blockchain technology is identified with entering the Internet's second era, whose cornerstone is the exchange of not only information but also value¹. The rise of blockchain is related to the most popular cryptocurrency at the moment, bitcoin, with the capitalisation at its peak exceeding USD 320 billion². However, the features and fundamental principles of blockchain technology have in a short time span made it widely used in numerous other sectors of economy.

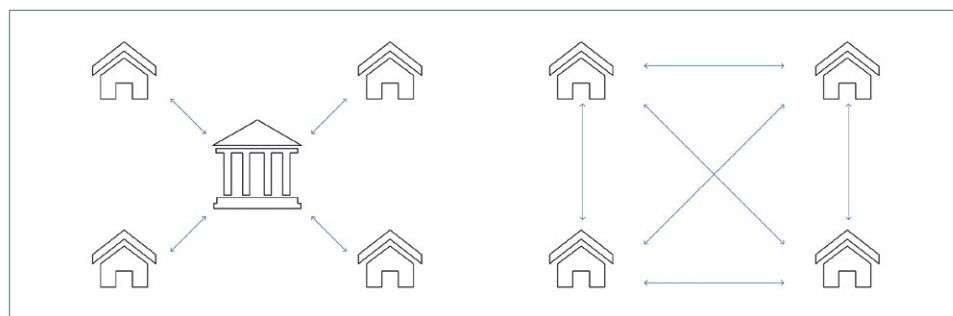
Blockchain is not the only example of Distributed Ledger Technology (DLT), but is the most widespread and recognisable one. Its basic premise is to eliminate intermediaries from the transaction

¹ Tapscott D., Tapscott A. (2016), *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, Penguin Random House, New York.

² *Blockchain Charts*. [ONLINE]:
<https://www.blockchain.com/en/charts>

process and to introduce trustworthiness into conducted processes. Based on the distributed database idea, blockchain does not have a central entity that would administer the data, and each network participant has access to information. Even if the basics of blockchain operation (such as asymmetric cryptography or distributed peer-to-peer network) are nothing new, it is precisely their combination that has led to the innovative and revolutionary character of this technology. The distributed nature of blockchain network is shown in the following diagram.

Figure 1. Centralisation vs the distributed nature of blockchain network



Source: Own work.

In a blockchain system, data is grouped into blocks, which are then added to the whole chain. Each block, apart from the data on transactions it contains, also includes information regarding the previous block and its confirmation method based on the consensus stemming from the network architecture. Various consensus algorithms exist. The most popular, used in the Bitcoin network for example, is Proof of Work (PoW). Alternative methods are Proof of Stake (PoS, and its variant, delegated Proof of Stake), which involves rewarding network users for the very fact they keep a cryptocurrency in their wallets, or Proof of Authority (PoA), where network user authentication is needed.

Data blocks are recorded chronologically and possess a unique timestamp that confirms the exact date and time when information was added

to the block. The stamp is thus proof that data in a given form existed at a specific time. This trait secures against counterfeiting attempts and forms of appropriation.

Thanks to public data recording (in public blockchains³) and the free data access for each network participant, the records are trustworthy and may be verified all the way to the moment the chain was set up (when the so-called *genesis block* appeared). This system is unlike traditional approaches to security where only a trusted third party can access the transactional information. Still, privacy is ensured as transactional information is not linked to any specific entity.

Proving one's identity (**authentication**) and one's permissions (**authorisation**) are two key elements of digital-world transactions. In other words, it is essential to demonstrate that a person is who they say they are and that they are entitled to do what they are planning to do.⁴ To check it, traditional systems (such as banks, financial institutions or state administration bodies) set a costly and complicated infrastructure in motion and employ numerous people to maintain it. Very frequently, the users are burdened with related costs in the form of subscriptions, transaction fees or commissions. Blockchain technology architecture makes conducting transactions that

³ It is worth noting that private blockchains, which regulate who may join them, exist as well. Currently, the largest and most widely used ledger is still public blockchain called Bitcoin, with its bitcoin (lowercase) currency.

⁴ Defining digital trust. [ONLINE]: <https://www.coindesk.com/information/what-is-blockchain-technology/>

PROOF OF WORK CONSENSUS

In the case of Proof of Work consensus network participants compete, trying to compute the block checksum with the SHA256 hash function that conforms to certain criteria. Calculating checksums is based on trial and error and related to network difficulty at current point in time. Once the mathematical problem is solved, the rest of the network can easily confirm the solution is correct. This happens because SHA256 is a one-way function, which makes calculating a reverse function impossible in practice. One-way hash functions are also put to good use in creating public keys on the basis of private keys to help encrypt transactions and keep a record of network data. The private key serves as the basis to compute an alphanumeric string necessary to sign outgoing transactions. That way the network remains sure that a transaction is done by a given participant and that he or she possesses sufficient amount to conduct the transaction. With the hash function a checksum of any existing digital object (including property rights documentation, cadastre, intellectual property rights – cf. 'Practical Blockchain Applications') may be calculated and recorded in the blockchain.

involve no intermediaries possible, and consequently is cheaper and limits onerous bureaucracy. No organisation or person owns the network. With no central organ and with its distributed nature, the network lets anyone verify and maintain data. Hence, blockchain is a danger to the intermediary institutions' status quo, because it replaces trust that transaction participants have to have in the third party with cryptographic proof.

Trust is fundamental both for business relations and for public administration, yet preserving it is in many cases very costly, time-consuming and ineffective. Due to such factors, blockchain technology ability to ensure authentic transactions and data ledgers without engaging public trust institutions in the process does give rise to a completely new category of market relations. As a number of reports show, problems such as frauds, thefts, tax evasion and corruption might be greatly limited in many countries if we only employed this technology.⁵

What ensures trust in blockchain networks is mostly such features as:

- **System transparency** – data in the network is distributed to every user. Both the information and the operation of the network itself undergoes constant testing and verification. Traditional system remain opaque and isolated from an average user.
- **Providing high-quality data** – data in the network is complete, accurate, widely available, and their record allows for tracing a transaction history and a ledger down to the very beginning of a network. Data modification is principally impossible as it would require recalculation of all hash function values.

⁵ Blockchain: Democratized trust. [ONLINE]: <https://www2.deloitte.com/insights/us/en/focus/tech-trends/2016/blockchain-applications-and-trust-in-a-global-economy.html>

- **Single point of failure absent** – there is no single central database that manages registered information. A copy of the data is at each participant's disposal. Internet access (or access to another source of blockchain, e.g. a satellite) coupled with appropriate software is enough to be able to use public blockchain networks.
- **High security level thanks to cryptographic mechanisms** – currently data verification based on a one-way hash function is impossible to break in practice. This is how private keys, helping us sign digital transactions, are protected.

To sum up, the following points present the chief features of blockchain technology:

- Blockchain is a distributed database where information is stored as a series of blocks.
- The chain contains the record of all data and its modification since the start of the network.
- Once written, in principle data cannot be changed without it being noticed, due to cryptographic mechanisms and consensus procedure.
- Blockchain removes the need for an intermediary and makes information on verified transactions publicly available (in public blockchains).

At the end of the day it is all about trust. Blockchain has the potential to disintermediate many third parties that are creating inefficiencies in the current system. Banks, aggregators, distribution system operators are there because trust is not a commodity. The exciting promise of blockchain is that it can help get closer to the commoditisation of trust.

Dr. Michael Mylrea (Senior Fellow for Cyber Security, George Washington University) during 4th European Cybersecurity Forum – CYBERSEC 2018

2. CYBERSECURITY OPPORTUNITY – TOWARDS RESILIENT IOT NETWORKS, SMART CONTRACTS AND DISTRIBUTED AUTONOMOUS ORGANISATIONS

Cybersecurity is complex, non-linear and evolving. Blockchain and the data it protects will never be 100% secure. Change is a constant and nothing is immutable. Yet, something needs to change as both systems and policies have not kept up with the cyberthreats. Cybersecurity paradigms are antiquated. From a cybersecurity perspective, blockchain shows potential to help improve the following areas: identity management – providing a secure ledger of actions for vulnerable Internet of Things (IoT); configuration and patch management; and supply chain security – tracking through the entire chain of custody. While most cybersecurity solutions increase costs, reduce functionality and ease of use, blockchain solutions might provide a unique value proposition to both increase security and optimise systems.

Blockchain technology's distributed form complements the increasingly distributed security function and requirements of global supply chains. For example, modern cities and their increasingly networked infrastructures have an array of vulnerable IoT. Security of these systems and networks could be significantly increased with a blockchain ledger of things for asset management and machine state integrity. Blockchain helps fill that gap securely via a digital ledger and cryptographic hash that signs the who, what, when and where of the data in a block that becomes a widely witnessed, auditable and inherently immutable event. This presents a number of potential opportunities to increase the cybersecurity of critical systems supply chains

which are increasingly distributed, data driven, global and vulnerable. Blockchain also facilitates the auditability of IoT environments that have been developed through a global supply chain. This can help fill a significant gap found in modern organisations, which often don't have an inventory or risk registry of their critical cyber assets detailing where they were developed, shipped, installed and when they were last patched. Malicious hackers continue to exploit these knowledge gaps to compromise critical systems.⁶ Blockchain can also increase visibility and monitoring of the machine state integrity of field devices and other embedded systems. IoT in critical infrastructures is often times not monitored, patched or securely configured, making it very challenging to identify, detect and protect against malicious cyber behavior.⁷

It is especially important in the context of today's smart cities, which increasingly weave together cyber and physical, information and operational technology, software and hardware, with ubiquitous sensors that exchange prodigious data sets. Securing these IoT environments and the data being exchanged is not a trivial task, especially when organisations increasingly rely on a vulnerable global supply chain. A recent report by the cybersecurity firm Crowd Strike suggests that supply chain cyber-attacks hit about two-thirds of companies surveyed with an average cost of USD 1.1 million.⁸

Blockchain provides an innovative trust anchor that can help transform decentralised cities and organisations to make them more distributed, autonomous and secure. In the process, it may also disrupt various industry verticals, creating

new services, markets and more distributed autonomous organisations. Blockchain's trust anchor can help disintermediate the many unnecessary third party brokers involved in exchanges of value. A more egalitarian economy could potentially emerge as producers and consumers regain value from across the supply chain. More control over transactions would occur as consumers become prosumers. Some related use cases that are being explored include blockchain solutions which enable owners of distributed energy resources to sell energy to their neighbours using blockchain smart contracts that execute autonomously when the agreed terms and conditions are met.⁹

Blockchain smart contracts allow for the execution of digital code which results in various transactions within defined perimeters. These executions of complex transactions take place over the blockchain and are recorded over the distributed ledger. Smart contracts could also help automate supply chain security through dynamic patch management alerts and updates, role-based access controls and baselining and monitoring machine state integrity. Once a smart contract is initialised on the blockchain, it gets an address associated with it. That address can be used to interact with the smart contract. That smart contract is present in the form of bytecode on the blockchain. Blockchain provides an atomically verifiable cryptographic signed distributed ledger, which provides a unique way of distributing trust. Instead of storing supply chain data such as inventory of critical hardware or the time of patch for critical software, critical supply chain data is stored in the distributed escrow of the blockchain, which maintains time stamped data blocks that cannot be modified retroactively, which increases the trustworthiness and integrity of the data. Several Proof of Authority blockchain technologies enable secure communications from operational technology protocols and industrial control systems

⁹ Mylrea M., *AI Enabled Blockchain Smart Contracts: Cyber Resilient Energy Infrastructure and IoT*. AAAI Spring Symposium.

⁶ M. Mylrea, *Smart Energy-Internet-Of-Things Opportunities Require Smart Treatment Of Legal, Privacy And Cybersecurity Challenges*, *Journal of World Energy Law and Business*, 10(2), 147–158, 2017.

⁷ M. Mylrea during European Cybersecurity Forum – CYBERSEC 2018.

⁸ A. Daniel, *Supply chain cyber-attacks hit two-thirds of firms*. [ONLINE]: <https://www.cips.org/en/supply-management/news/2018/july/supply-chain-cyber-attacks-hit-two-thirds-of-companies/>

by including an advanced cryptographic signature that assigns the time of signing and data signer as well as authentication to a data asset.

DISTRIBUTED AUTONOMOUS ORGANISATIONS

Blockchain technology combines cryptography and distributed computing to provide a multi-party consensus algorithm to securely exchange value. Combining the disintermediation benefits of blockchain with the intelligence of smart contracts can help automate energy exchanges and give impetus to more **distributed autonomous energy organisations (DAEO)**. DAEO may also help simplify and improve the efficiency of energy utilities by securely linking producers with consumers and creating prosumers with increased flexibility and control of how they generate, consume and exchange energy. Advances in blockchain and artificial intelligence (AI) continue to spur disruptive innovation, automating exchanges in value in new ways that are reducing the need for third-party trust mechanisms.¹⁰

These advances could help pave the way for more distributed, autonomous and resilient infrastructures. While grid modernisation has helped spur a more distributed and flexible smart grid, it has also created new challenges, such as increasing the number of intermediaries involved in exchanging energy. Grid modernisation has also increased the cyberattack surface through the increased use of smart energy devices that network, digitise, automate, and increasingly converge energy supplies in the cyber-physical energy supply chain. Blockchain or distributed ledger technology shows potential in identifying and monitoring these complex IoT environments, characterised by an increasing number of critical cyber assets and data being exchanged in a complex energy value chain. Blockchain technology shows potential in overcoming some of these challenges needed to give impetus to more distributed autonomous energy organisations.¹¹

¹⁰ Ibidem.

¹¹ Ibidem.

In the same way, the Internet transformed centralised organisations into decentralised ones, blockchain technology provides an innovative cryptographic proof that works as a distributed consensus algorithm to securely exchange and store value. As a result, today's smart decentralised cities will become more distributed as infrastructures become increasingly interoperable, networked and autonomous.

Blockchain has several benefits that could improve cybersecurity, especially supply chain and security and identity management. Some of these benefits include:

1. Increased transparency and auditability of the system throughout the manufacturing, shipping, deployment, maintenance and retirement life cycle;
2. Immutable archived records about the firmware, hardware, and software components of the system including the past and current patch management information;
3. Expedited and enhanced inter-vendor cooperative system development through increased visibility and accessibility of supply chain data;
4. Improved security of the supply chain process through increased trustworthiness and integrity of data through blockchain consensus mechanism which reduces reliance and can even replace the need for intermediary trust mechanisms and brokers that are susceptible to manipulation and compromise;
5. The principle of component traceability throughout the system lifecycle to incorporate efficient systems engineering processes;
6. Improved reliability through transparency and information sharing.

3. BLOCKINGS TO BLOCKCHAIN: CHALLENGES TO OVERCOME

All revolutionary technologies, including block-chain, bring along not only a number of chances but also their own set of challenges. In this case, each iteration of the technology (currently three generations are distinguished¹²) strives to overcome the imperfections which hinder widespread use of blockchain.

THREE GENERATIONS OF BLOCKCHAIN TECHNOLOGY

1. Bitcoin – a network aimed to form a decentralised payment system.
2. Ethereum – currency transactions notwithstanding, the network also offers smart-contract creation, so that terms and conditions are clear to each network participant.
3. The generation intended to solve network scalability problems and to ensure interoperability between various blockchain systems.

Some challenges, mostly the ones related to the most common sort of blockchain, that is Bitcoin, are presented below.

HIGH ENERGY COSTS

The keystone of safe and secure operation for blockchains is the result of cryptographic equation, unique for every block, that is based on a complex algorithm. In some types of block-chain (PoW-based), very large computing power

¹² Three generations of Blockchain Technology.
[ONLINE]: <https://medium.com/@bitbawa/three-generations-of-blockchain-technology-22658d02e067>

is necessary to solve this equation (cf. 'General Overview of the Blockchain Technology'), which generates substantial energy cost. When we look at the whole bitcoin market energy consumption, it turns out to be roughly equal to the power consumption of Austria.¹³

SCALABILITY

Decided advantages of blockchain technology are in a more sophisticated analysis also its drawbacks. Complexity level, intricate encryption or the distributed nature of DLTs make data processing time longer and throughput lower for first- and second-generation networks, especially with a large and rapidly growing user base, than is the case for traditional payment instruments. Blockchain architects are aware of these limitations and are working to make the technology more efficient. Lightning Network is one proposed improvement – a blockchain layer that would make a theoretically unlimited number of transactions possible.¹⁴

LACK OF LEGAL NORMS

As is the case with all modern technologies, legal regulations concerning blockchain are clearly behind in terms of providing security framework that would counter potential fraud and manipulation. Even though several small European states have attempted to form legal regulations and some EU institutions try to take up the topic (cf. 'Regulatory State of Play in the European Union'), they are still insufficient, given the swift pace of technology development. The problem mostly concerns cryptocurrency exchange. Even currencies with market position as established as bitcoin, litecoin or ether fail to offer complete certainty that virtual wallet will not be hacked into or that a government entity will not start suspecting

unfair practices or black-market transactions.¹⁵ Globally standardised legal framework would greatly increase system predictability, which could translate into a stronger interest among potential investors, who would be more willing to allocate their assets in blockchain-based undertakings if the legal stability was greater.

CRIMINAL ACTIVITIES

Somewhat related to the lack of legal framework discussed above, another challenge is facing policy-makers who are going to shape the future of DLTs. It is the possibility to use blockchain for illegal activities. Bitcoins remain the most vulnerable to criminality (due to their massive popularity) along with monero (which guarantees a higher level of anonymity). These cryptocurrencies have become a payment method for transactions in the so-called dark web, that is a hidden section of the Internet which lets its users buy, to take an example, illegal weapons or drugs, while users' anonymity and lack of regulatory framework make identifying felon particularly difficult.

PRIVACY

In terms of transparency, two types of blockchain technology are distinguished: public ledger, which anyone with access to the Internet can join, and private ledger, which only those who have been invited may use.¹⁶ Public ledgers are designed so that they are available for all network users. This means that if you want to conduct a transaction, which is closely tied to the necessity of disclosing information, not infrequently sensitive, about you, you need to bear in mind that all other network users are going to be able to access it. Obviously, the whole process is marked as anonymous and encrypted, but there are cases when trusted processing of confidential data is not attainable

15 Li X., Jiang P., Chen T., Luo X., Wen Q., A Survey on the Security Blockchain Systems, Cornell University Library 2018. [ONLINE]: <https://arxiv.org/pdf/1802.06993v2.pdf>

16 Joshi A. P., Han M., Wang Y., A survey on security and privacy issues for blockchain technology, American Institute of Mathematical Sciences 2018. [ONLINE]: <http://aimsciences.org/article/doi/10.3934/mfc.2018007>

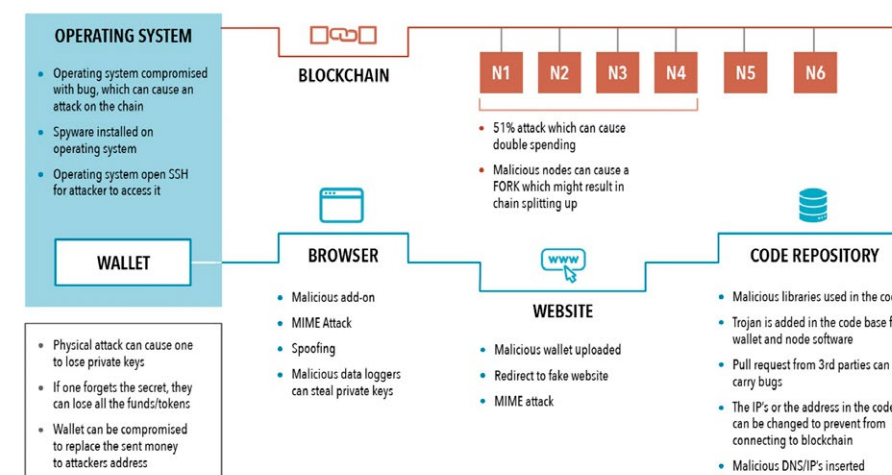
13 Digiconomist, Bitcoin Energy Consumption Index. [ONLINE]: <https://digiconomist.net/bitcoin-energy-consumption>

14 What Is Lightning Network And How It Works. [ONLINE]: <https://cointelegraph.com/lightning-network-101/what-is-lightning-network-and-how-it-works>

with the current state of the technology.¹⁷ A good example of the issue is the implementation of blockchain in the healthcare system, now being considered by many state entities. Such a measure would require the use of a public ledger, which gives rise to concern about data confidentiality in areas as crucial as medical history or medical records.

computing could also potentially decode the meta data stored in the blockchain hash, exposing information. The following graphic highlights common blockchain cybersecurity vulnerabilities.

Figure 2. Common blockchain cyber vulnerabilities



Source: Mylrea and Gourisetti, 2018.¹⁸

CYBERSECURITY

With the prospect of improved cybersecurity (cf. 'Cybersecurity Opportunity') also comes peril. A number of cybersecurity gaps remain: vulnerable code, bad deployments and misconfigurations of blockchain could actually create more cybersecurity challenges than solutions. A couple of these vulnerabilities have been exploited, resulting in significant economic and reputational damage: If you compromise 51% of the blockchain nodes, you can fork or manipulate the consensus algorithm. Vulnerabilities in crypto hot wallets make for excellent targets. It is similar to a bank advertising that it has no guards, no locks and all of the cash it holds is untraceable. Another cybersecurity gap is that malware or illegal data may be stored in the blockchain. Its immutability then possibly becomes a big problem. Quantum

17 Goebel A., Blockchain: the Privacy Problem. [ONLINE]: <https://e3zine.com/2018/04/16/blockchain-privacy-problem/>

The challenges outlined above, which need to be analysed before the blockchain technology implementation phase, are merely some of the many illustrations of DLT imperfections; much work is currently being done to counteract or minimise them. Policy-makers who are going to shape global standards and legal regulations should analyse the potential in depth and determine the realms where blockchain can be perfected and adjusted to function on a large scale – and those where applying this technology may result in irreversible negative consequences eclipsing positive impacts. In-depth debate in this regard should help establish technology guidelines that will maximise the profits blockchain offers and minimise the losses it incurs.

18 Mylrea, M., Gourisetti, S., Bishop, R., & Johnson, M. (2018). Keyless Signature Blockchain Infrastructure: Facilitating NERC CIP Compliance and Responding to Evolving Cyber Threats and Vulnerabilities to Energy Infrastructure. Paper presented at the IEEE PES Transmission & Distribution Conference & Exposition.

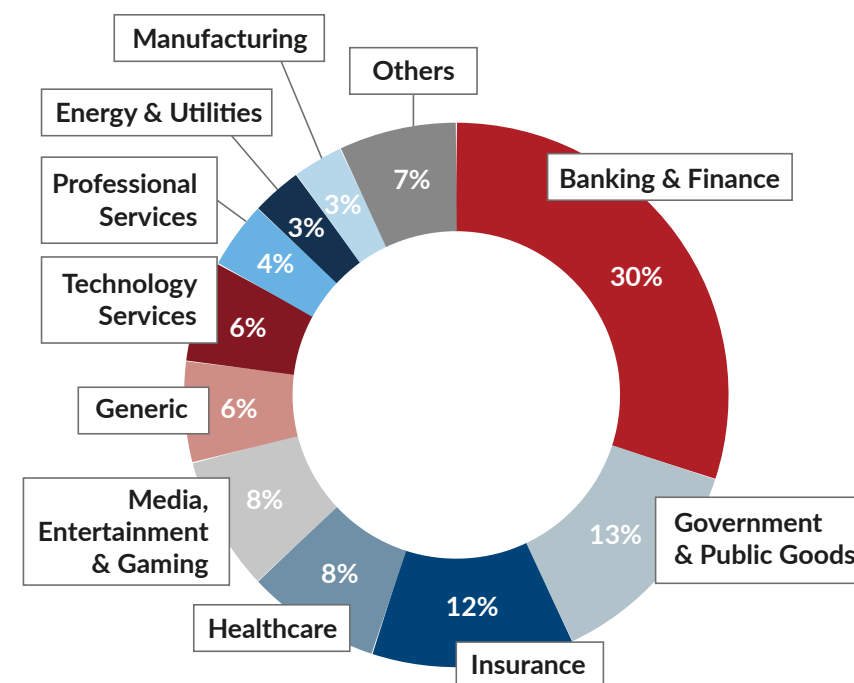
4. PRACTICAL BLOCKCHAIN APPLICATIONS AND REAL-LIFE CASE STUDIES

Although blockchain is mostly associated with cryptocurrencies today, its use can be much broader in scope. In fact, this system has the potential to become the foundation of digitisation process in many aspects of our lives. The fields presented below are just some of all domains where blockchain can be used and where it is being developed, in the process revolutionising the solutions that we know.

BANKING AND FINANCE

Blockchain, working as a transparent digital ledger, can be effectively used in the banking and finance sector, especially in accounting. Such transformation leads to a number of benefits and eliminates costly human mistakes. Blockchain, thanks to the altered way it stores and gives access to the data, provides a more transparent and secure transaction retrieval to all authorised users, including auditors, for whom controlling becomes safer and easier.²⁰ The technology also simplifies financial book-keeping for an enterprise, since instead of many separate ledgers all it needs is one common ledger for all its subsidiaries' transactions, which would make accounting much more streamlined.

Figure 3. Sectors which already use blockchain



Source: Global Blockchain Benchmarking Study¹⁹.

¹⁹ Global Blockchain Benchmarking Study. [ONLINE]: <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/global-blockchain/#.Wms8ZrPtypo>

²⁰ Tysiac K., Blockchain: An opportunity for accountants? Or a threat? [ONLINE]: <https://www.journalofaccountancy.com/news/2017/nov/blockchain-opportunity-for-accountants-201717900.html>



CASE STUDIES

Implications of blockchain technology use in the financial sector are profitable for both customers and financial service providers. No wonder, then, that banks in cooperation with various stakeholders are particularly interested in enhancing ways to use this technology. As early as October 2013, **German Fidor Bank**, teaming up with other financial institutions, mostly clustered around cryptocurrencies (Kraken, Bitcoin.de and Ripple Labs), developed a mechanism and platform to trade virtual currencies among EU states²¹. The American stock exchange, **NASDAQ**, disclosed in 2015 that it was planning to use blockchain as the backbone technology in order to develop the capabilities of its subsidiary NASDAQ Private Market, whose important capital is bitcoin²². Considered a leader in developing and implementing the blockchain technology, **IBM** declared in October 2017 in cooperation with a dozen banks from various continents its groundbreaking initiative that is going to upend cashless transaction system. IBM's universal blockchain payment solution aims to get rid of cross-border inconveniences related to payments and is supposed to lower high fees and to accelerate the transaction accounting process, which at the moment takes several days²³.

21 Spaven E., Kraken partners with Fidor Bank to offer bitcoin trading services in the EU. [ONLINE]: <https://www.coindesk.com/kraken-partners-fidor-bank-offer-bitcoin-trading-services/>

22 Know more about Blockchain: Overview, Technology, Application Areas and Use Cases. [ONLINE]: <https://gomedici.com/an-overview-of-blockchain-technology/>

23 Inside the new IBM universal blockchain payment solution for banking. [ONLINE]: <https://www.i-scoop.eu/ibm-cross-border-payment-blockchain-universal-blockchain-payment-solution/>

DATA MANAGEMENT AND BUILDING A DIGITAL IDENTITY

Another topic where blockchain technology can improve day-to-day functioning is data management and building a digital identity. As the world is moving fast to become ever more digital and grounded in cutting-edge technologies, personal data and identity protection has become paramount. Most of our Internet activity demands entering sensitive and confidential information, such as personal data or, in the case of online shopping, payment card number and its CVV code. Each time such information is entered, it is kept in numerous Internet databases that, should a hacker successfully attack, may let thieves steal your identity or, e.g., buy something at your expense. Because of its distributed database, blockchain can help properly secure this system and build a highly resilient authorisation and verification mechanism, immune to manipulation and with good management of encrypted digital identities.

Digital identity, thanks to the decentralised blockchain system and comprehensive verification of any Internet user, may thus become a type of electronic watermark stamped on every transaction and online activity of a given user. Not only does this offer effective protection against potential theft, but also a secure digital ID platform will notably lower the client identification costs (KYC – Know Your Customer procedures), help freely define which data are to be made available in a particular case, finally replace the repeated and time-consuming need to type logins and passwords. Setting up a blockchain-based digitised identity will also give its owner greater control over who and how can gain access this identity.



CASE STUDIES

One of the first states in the world that decided to implement the idea of digital identity is **Spain**,²⁴ which to that end started its cooperation with a blockchain-based tool provider, the **Alastria** company. Alastria's objective is to enable and speed up the digital transformation process in various industries and businesses. The consortium is tasked with building the world's first well-regulated state-wide blockchain network with the major focus on creating the digital identity system. Alastria is supposed to ensure security and verifiability of any natural or legal person who is going to be certified and vouched for by an entity with certification privileges, and all this is going to happen in accordance with the letter of the Spanish law.

Another and perhaps the most momentous example of building a blockchain-based system of digital identity is the **ID2020 Alliance** supported by the **United Nations**²⁵. This project strives to provide legal electronic IDs to people who do not have any, and as a result have no access to basic state-sponsored services that existing human and civil rights ensure (including education, healthcare etc.). It is estimated that all over the world more than 1 billion people have no ID²⁶.

24 Alastria: the first national multi-sector blockchain ecosystem in the world. [ONLINE]: <https://www.i-scoop.eu/alastria-consortium-red-alastria-blockchain-dlt/>

25 Johnson P., Partnering for a path to digital identity. [ONLINE]: <https://blogs.microsoft.com/blog/2018/01/22/partnering-for-a-path-to-digital-identity/>

26 Williams S., This is Really Happening: Microsoft Is Developing Blockchain ID Within Its Authenticator App. [ONLINE]: <https://www.fool.com/investing/2018/02/16/this-is-really-happening-microsoft-is-developing-b.aspx>

The biggest partner of this endeavour is **Microsoft**, a company that is offering its money, resources and know-how in the effort to give every person the chance for computerised identity verification and access to services which are indispensable in fulfilling living needs even if a person does not possess a physical ID.

VOTING PROCEDURE

The problem of election is in a way related to the one described above; each time, the procedure necessitates identity verification for those eligible to vote. Transparency and decentralised nature of blockchain technology can find their use in digital elections: the vote may in a sense become a blockchain transaction that is impossible to change and keeps both the trace of the vote and the identity of the person who cast it.²⁷ The technology is open and verifiable enough to allow any authorised moderator (e.g. a person who oversees the e-voting process) to check at any moment whether the voting blockchain has not been tampered with, for instance whether non-eligible people voted or some eligible ones voted twice. Used in the voting process, blockchain may be a source of trustworthy confirmation for the final tally and reduce the number of election frauds, thus refuting the basic argument of e-voting opponents that the security level and fraud resilience are uncertain. An additional benefit when employing this technology in voting procedure is the ability to receive the result immediately, with precision decidedly higher than that of a manual vote count. The use of this system in the public sector notwithstanding, blockchain can also be useful in voting within diverse organisations and companies,

27 Ayyash A., How Blockchain Will Make Electronic Voting More Secure. [ONLINE]: <https://hackernoon.com/how-blockchain-will-make-electronic-voting-more-secure-fba15d752bee>

for instance among shareholders on stock exchange, which e.g. NASDAQ deems practical and necessary today.²⁸



CASE STUDIES

Attempts to use blockchain technology in voting procedures now assume the form of noncommittal pilot studies or consultative referendums. Among them is the **Active Citizenship programme** launched in Moscow in 2014.²⁹ The app lets residents of Russian capital vote to make decisions on important city matters and to actively participate in shaping urban space. Initially, such local referendums were traditional in nature – Moscow communities gathered in designated sites to cast their votes. To make it possible and easy for all residents to have a measure of control over their lives, a digital platform was set up for e-voting; it was easily manipulated, though. Blockchain turned out to be the solution and was implemented in December 2017 in the application, whose performance (security, reliability, resistance to modification) it was then possible to openly and publicly assess. PwC took on the auditing task, which proved there were no grounds to be afraid the results could be manipulated either from the inside or by an outside attack.

Another example of e-voting execution is **Follow My Vote (FMV)**, which offers open access to verified blockchain-based software for government institutions that organise elections. FMV aims to improve

digital voting system integrity and to make voting safe, convenient and easily available for all eligible people. Its first pilot e-voting project was carried out in 2016 in the United States. The software is meant to oppose the fundamental shortcomings of American voting process and electronic voting, which include problems to count votes on time or missing votes in the states where citizens use traditional postal service for that purpose. In the US, a significant problem was the questionable reliability of WinVote software (mostly in the state of Virginia), which was revealed as ineffective and susceptible to interference even from beginner hackers. As the state report disclosed, the password in this program, widely used between 2002 and 2014, was 'admin' and 'abcde', and anyone within a kilometre range from the device the program ran on could, having entered the password, freely modify particular votes³⁰.

INTELLECTUAL PROPERTY PROTECTION

As the blockchain technology shows the potential to become the mechanism of controlled intellectual property distribution and a register of license fees copyright holders are owed, another group that should keep a very close watch on how these capabilities are being developed are work authors and their lawyers. Currently, copyright owners struggle with the problem of incomplete information they obtain on how their royalties were calculated as well as with the lack of database that would list where and how their intellectual property is used. A number of bureaucratic complications and high cost of intermediaries in copyright enforcement do not help the situation. Blockchain

28 Banking Is Only the Beginning: 42 Big Industries Blockchain Could Transform. [ONLINE]: <https://www.cbinsights.com/research/industries-disrupted-blockchain/>

29 Kshetri N., Voas J., Blockchain-Enabled E-Voting. [ONLINE]: https://www.researchgate.net/publication/326239528_Blockchain-Enabled_E-Voting

30 Thielman S., Voting machine password hacks as easy as 'abcde', details Virginia state report, The Guardian 2015. [ONLINE]: <https://www.theguardian.com/us-news/2015/apr/15/virginia-hacking-voting-machines-security>

can grow to be a much simpler and cheaper global platform than current legal regulations as it stores immutable information that is simultaneously a verified proof of a copyrighted work having been used, its author and its original date. Transparency and openness of the emerging encrypted blockchain certificates minimises the risk of fraud or plagiarism. Apart from the merits in the domain of copyright protection discussed earlier, it is worth a mention that a global blockchain-based platform may become a new means of distributing works by unknown authors who, to date, had to curry favour with a producer or publisher and agree to be bound by long-term unfavourable contracts in order to present their pieces where they would be available to the general public. Consequently, blockchain may have varied and profound impact in this regard.



CASE STUDIES

Ascribe, started in 2014, is one of DLT platforms that is revolutionising the complicated issues of copyright. This German company not only provides trustworthy certificates which confirm authorship and provenance of works, but also facilitates digital intellectual property management for their authors as it enables them to share and sell their works with no commission-charging intermediaries. The authors also remain in control regarding further copyright protection of the pieces they have sold.

A similar platform, although dedicated solely to photography copyrights, is Binded (earlier known as Blockai). Binded encrypts all photographs sent by its registered users and issues a certificate to confirm the ownership of each photo. The platform not only stores the pictures, but also monitors them and informs the owner if their rights have been infringed. Its aim is also to simplify and standardise the protection of routinely violated authors' rights.

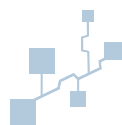
SUPPLY CHAIN MANAGEMENT

Each one of us has surely experienced a purchase where several or even a dozen entities took part in the process between product delivery and the signal to start package preparation before sending (which is usually the payment). Naturally, such is the case most often with increasingly popular Internet shopping.³¹ If the package is delivered on time and undamaged, hardly anyone is interested in who and at which moment was responsible for it. Yet, if the product is lost, delivered late or defective, we start the whole investigative process of checking when the package got lost or was damaged. Supply chain management and monitoring appears to be the field where blockchain potential has a chance to be the answer to the main challenges. Their number is substantial, including a great deal of daily transactions, the involvement of many intermediaries or the reliance on paper trail for particular order fulfilment stages. Small wonder, then, that supply chains, logistics and transport take second place in blockchain technology exploitation, right behind the financial sector.³² As was mentioned before, traditional interaction channel among intermediary entities and order fulfilment tracking relied on forms as obsolete, impermanent and easily destroyed as fax or paper, for which production cost can reach up to half of the container transport price.³³ Transparency and durability of shared ledger that blockchain offers are going to let buyers track each stage of transport in real time and significantly cut production costs via the elimination of paper trail and, as with every digital and automatised service, reduce the risk of human error.

31 The Statistic Portal, Retail e-commerce sales worldwide from 2014 to 2021. [ONLINE]: <https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/>

32 Blockchain technology: digital trust and distributed ledger technology (DLT) in business. [ONLINE]: https://www.i-scoop.eu/blockchain-distributed-ledger-technology/#Supply_chain_management_logistics_and_blockchain

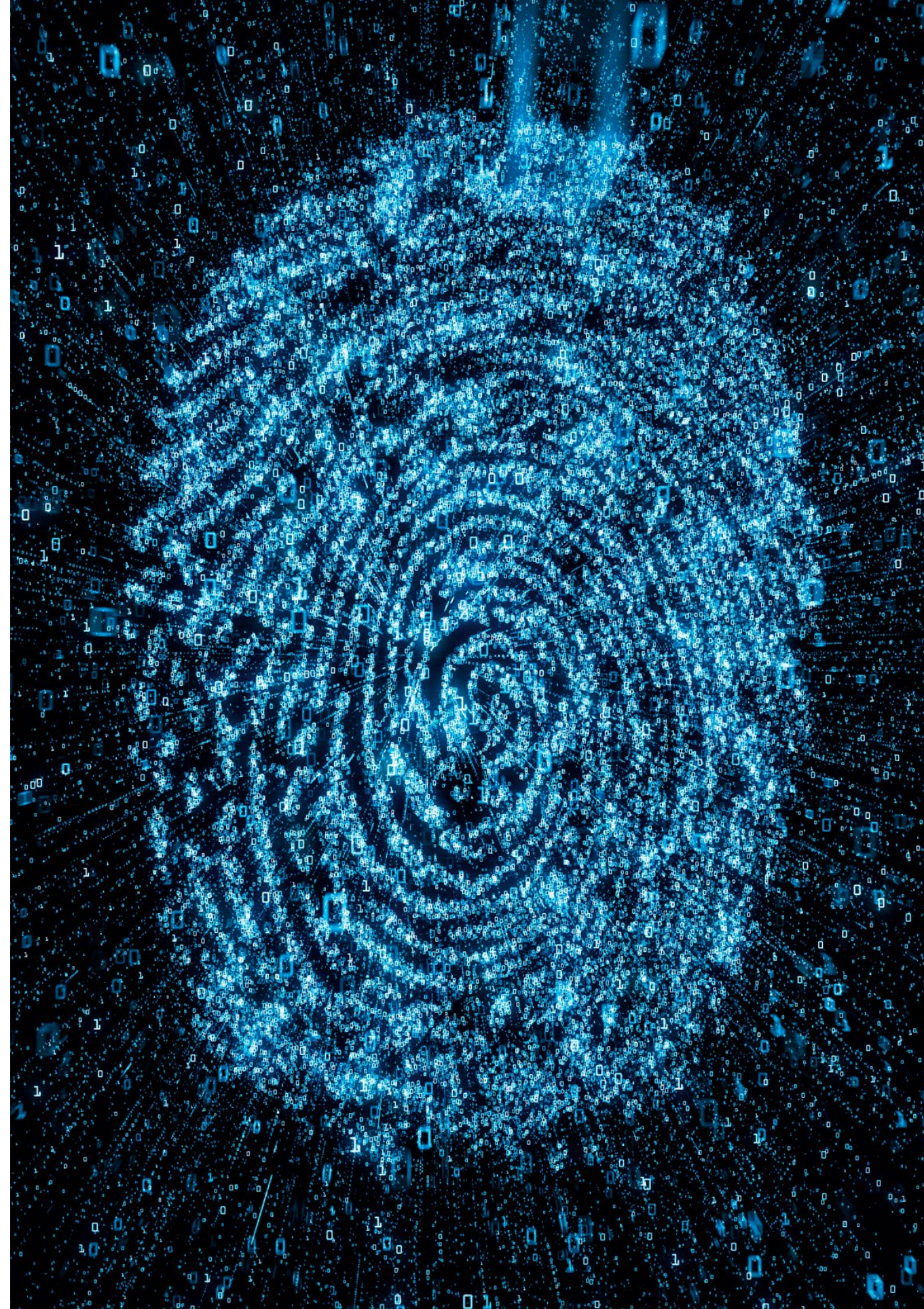
33 Ibidem.



CASE STUDIES

Blockchain-based **Provenance** is a type of software that offers not only transparency in tracking an ordered product, but also enable the enterprises themselves and their customers to compare their data, verify key information about the products and keep a permanent and distributed ledger of this data. Blockchain stores the most important information regarding a given supply chain and product, and due to its transparency lets all interested parties verify their validity. A common advantage of deep restructuring that blockchain makes possible in various service sectors is the ability to acquire a trustworthy certificate that confirms correctness or authenticity. In the case of Provenance, along with the product you receive its 'passport' – all the information that is basic and relevant to the consumer, such as where the product comes from, what its quality is, its authenticated origin or the environmental impact of its production. Interestingly, this solution has a far wider use – should bacterial food poisoning occur, blockchain technology may help detect the source of a given food product much faster. This software very vividly demonstrates another area of blockchain use, the last one to be discussed here: the possibility for confirming product origin authenticity or the originality of an ordered item. This advantage of immutable DLTs is immensely valuable and mostly followed by the food industry (but not only there).

The above shows that we are only just beginning to discover the DLT potential, which may find its uses in innumerable sectors that influence both aspects of our everyday lives (supply chain monitoring, financial transactions) and the activities that make us citizens and allow us to enjoy our statutory rights to the full (digital identity, e-voting). The character and pace of these changes depend both on the citizens or companies and on state governments, for as much as it would seem the blockchain technology was created with minimising or bypassing the presence of state institutions in mind, it is them who ought to actively stimulate the legitimisation, improvement and dissemination process concerning the tools which will optimise global infrastructure and combat many urgent problems that seem intractable with traditional instruments; all that is going to contribute to the wealth and prosperity of the state and of its citizens.



5. REGULATORY STATE OF PLAY IN THE EUROPEAN UNION

Nature abhors a vacuum, and so do regulatory bodies. Emerging disruptive technologies undoubtedly bring economical and societal improvements in a large variety of ways, but they also give rise to many new puzzles, including regulatory ones. Since the emergence of the blockchain technology ten years ago, policy-makers and legislators all over the world have continuously looked into the issue of bringing it under a regulatory framework. Blockchain regulation is not an easy task as it finds itself based on a fragile equilibrium which should ensure the protection of users against criminal misappropriation, while fostering further development of this innovation. The approach ought therefore to be cautious and is still being developed, but the state of play in the European Union at the moment is unique and deserves to be examined in more depth.

While many would argue that the very concept of regulating a disruptive technology such as blockchain is unworkable because the pace of its evolution would render any regulation almost immediately outdated, some governments took up the challenge. As of today, two of the smallest territories in the European Union have created a legal framework designed to regulate the Distributed Ledger Technology (DLT) underpinning blockchain technology:

In October 2017, the government of **Gibraltar** introduced the 'Financial Services (Distributed Ledger Technology Providers) Regulations 2017'³⁴ and became the first to enact a legislative framework of this kind. The regulation is based on a licensing scheme that should enable the creation of a secure and sound ecosystem for businesses that rely on DLT and blockchain

³⁴ *Financial Services (Distributed Ledger Technology Providers) Regulations 2017*, Gibraltar Gazette, No 4401, 12 October 2017.

technologies. Applicant DLT-providing firms operating in or from the territory of Gibraltar are initially subjected to a general assessment of their business model. Subsequently, the Gibraltar Financial Services Commission – the regulator of the financial services market in the territory – takes the decision to grant the license, assessing the application against nine core regulatory principles that cover the conduct of the business, communication with clients, maintenance of sufficient resources, risk management, protection of customer's money, corporate governance, high-standard security protocols, prevention of financial crime risk and resiliency in case of wind-down³⁵.

While this regulatory framework does not apply at a country level, it seems worth mentioning for its pioneering character and as a source of inspiration for potential future blockchain regulations to come.

Shortly after, in July 2018, **Malta** passed three bills into law setting out regulatory frameworks for blockchain, cryptocurrency and DLT.³⁶ Following a scheme rather similar to that launched in Gibraltar – it is based on the registration of innovative technology service (ITS) providers and on the certification of innovative technology arrangements (ITA) suppliers – the system goes one step further in creating a new agency dedicated to this task. The Malta Digital Innovation Authority has indeed been established by the same laws and entrusted with the task to provide a set of guidelines aimed at assisting ITS providers with registration and ITA applicants with certification.

When passing the laws, Gibraltar and Malta adopted a technology first and long-term approach. In both cases, the ultimate aim of regulating blockchain and DLT technology is to ensure the new business ecosystem being built on it is framed and rests on legal certainty. Setting up a stable and legally well-developed environment is vital

to attract entrepreneurs, to ensure a fair level of competition and to achieve economic growth in the sector. In this respect, and thanks to its new crypto-friendly legislation, Malta is now considered a hub for crypto-based initiatives. Some of the biggest cryptocurrency exchanges, for instance Binance, relocated to the island, hiring several hundreds of people.³⁷

On the other hand, many European countries adopted a partial approach, regulating only one application of DLT technology – cryptocurrencies. The latter indeed emerged unregulated and free from government currency control, and the financial gains associated with the rapid rise of cryptocurrencies sparked many concerns among EU states, which decided to regulate on this issue. Today, almost half of the EU-28 members either created new laws or extended the existent rules to cover revenues and transactions with cryptocurrencies.³⁸ However, as it was already emphasised, blockchain can be used for a wider range of assets than just cryptocurrency, from real estate to smart contracts to voting, therefore reinforcing the need for a general legal framing of the technology. While the process of regulating blockchain is still subdued at the national level, a breakthrough could well lie in a more global approach.

Recently, the **European Parliament** has taken a step in this direction and spelt out its approach to the blockchain technology in a 'resolution on distributed ledger technologies and blockchains: building trust with disintermediation'.³⁹ Presented by Eva Kaili on behalf of the Committee on Industry, Research and Energy, it has been

37 Binance, *The World's Largest Crypto Exchange, Announces Investment In Malta*. [ONLINE]: <https://medium.com/binanceexchange/binance-the-worlds-largest-crypto-exchange-announces-investment-in-malta-4c7e51136563>

38 *Regulation of Cryptocurrency Around the World*. [ONLINE]: https://www.loc.gov/law/help/cryptocurrency/world-survey.php#_ftnref137

39 European Parliament, *Resolution on Distributed ledger technologies and blockchains: building trust with disintermediation*, 3 October 2018.

35 Ibid.

36 Malta Digital Innovation Authority. *The Acts*. [ONLINE]: <https://mdia.gov.mt/acts/>

adopted in plenary session on 3 October 2018. The text is interesting in several respects. As a prerequisite, it acknowledges the difficulty of legislating on an evolving technology and grapples with the fragile nature of a potential blockchain framework, which 'necessitates an innovation-friendly, enabling and encouraging framework that provides legal certainty and respects the principle of technology neutrality, while at the same time promoting consumer, investor and environmental protection, increasing the social value of the technology, reducing the digital divide and improving the digital skills of citizens'.⁴⁰ To this aim, the resolution sets out two principles on which any regulatory approach toward DLT should be based:

- technology neutrality, by directing the regulation towards the uses and users of blockchain technology but not to the technology in itself. Defined in the Framework Directive 2002/21, technology neutrality requires that each member state's national regulatory body 'neither imposes nor discriminates in favour of the use of a particular type of technology, does not preclude the taking of proportionate steps to promote certain specific services where this is justified'.⁴¹ It ensures consumer protection by preventing misuses of DLT applications and does not hinder the further development of innovation in the sector.
- business-model neutrality, safeguarding free and fair competition within the market and making sure that no business model is favoured over another. It ensures that the disruptive capacity of DLT technology is not hampered and in this regard is akin to the previous principle. It guarantees the fact that blockchain should be able to bring positive disruption in existing value chains or business models.

40 Ibidem

41 European Parliament and Council, *Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (Framework Directive)*, OJ L108/33, 7 March 2002.

The resolution of the European Parliament also shows support for the further development of the technology and the assessment of its impact and potential risks for the society. It indeed asks that the post-2020 multiannual financial framework includes an increase in funding to DLT technology projects and research initiatives. According to the European Commission, EUR 83 million have already been granted to blockchain-related projects and up to EUR 340 million could follow between 2018 and 2020. Finally, emphasising that 'the Union has an excellent opportunity to become the global leader in the field of DLT and to be a credible actor in shaping its development and markets globally, in collaboration with our international partners',⁴² it calls on the European Commission to take policy initiatives in order to promote EU's position in the field of DLT.

The resolution was presented as a tool to raise awareness among members of the European Parliament and citizens regarding many possible applications of blockchain and its enabling characteristics.⁴³ Although it is quite ambitious, what has to be noted is that European Parliament's resolutions are not binding and therefore do not impel any other institution – in particular the European Commission – to take action. They signal a political desire to act in a particular area and to advance the legislation in a given field. The procedure in European Parliament being now over, the resolution will be forwarded to the European Commission for consideration, but there is no certainty about further actions by the European Commission or member states.

However, looking at the past couple of years, we can argue that the importance of the topic and the potential – be it economic or societal – of blockchain was not lost on the European Commission. Despite having no legislative powers,

42 European Parliament, *op. cit.*

43 *Blockchain in the European Union: How the European Parliament approaches DLTs*. [ONLINE]: <https://www.openaccessgovernment.org/blockchain-in-the-european-union-how-the-european-parliament-approaches-dlts/47762/>

the Commission launched several initiatives for the exploration of DLTs that are worth mentioning:

- **The European Blockchain Partnership.**
Aimed at reinforcing cooperation among the 28 member states and some neighbouring countries of the European Economic Area in this sector, this partnership signed in April 2018 will reinforce trust in blockchain technology by supporting the delivery of cross-border digital public services, with the highest standards of security and privacy.
- **The Blockchain4EU:** Blockchain for Industrial Transformations project explored existing, emerging and potential applications of DLTs in the industry sector, in businesses and SMEs.
- **The EU Blockchain and Observatory Forum,** mapping and analysing existing successful initiatives in the field of blockchain in the EU and promoting education and knowledge sharing. It proposes an online forum which gathers various stakeholders from entrepreneurs to researchers and aims to advance the debate on blockchain further.

All initiatives mentioned above enter in a scheme that should allow the European Commission to gather knowledge about various aspects of blockchain in light of a future legislative proposition. Other European institutions also engaged on blockchain topic, signalling a certain level of maturity. Back in 2015, for instance, the Court of Justice of the European Union rendered its first judgement on a blockchain-related matter – namely Bitcoin – and ruled that transactions to exchange a traditional currency for other virtual currencies and vice versa are exempt from VAT.⁴⁴ In addition, the Council Conclusions of 19 October 2017 also highlighted blockchain, along with artificial intelligence, as ‘key emerging trends’.⁴⁵

44 Court of Justice of the European Union, Case C-264/14, Skatteverket v. David Hedqvist, ECLI:EU:C:2015:718, 22 October 2015.

45 European Council, European Council meeting – conclusions, 19 October 2017.

Given the global phenomenon that blockchain represents and given its cross-border nature, it seems that an appropriate regulation should be thought and implemented at a global or regional level.

Initiatives already emerged at the EU level and many reflexions have been launched at a smaller level – in the Baltic states, for instance, where a Memorandum of Understanding on capital market development⁴⁶ was signed and lists distributed ledger technology as a potential area of extended cooperation. It is undeniable that regulation, in any field, brings an element of stability and therefore economic growth as well as societal improvements. Now that the EU holds all the cards, if it wants to explore the full potential of blockchain, it has to engage in a bold move to close the regulatory gaps or imbalances among its member states and then only it could fulfil its much-wanted destiny to be the blockchain leader.

46 Memorandum of Understanding between the Ministry of finance of the Republic of Estonia and the Ministry of finance of the Republic of Latvia and the Ministry of finance of the Republic of Lithuania in respect of their co-operation for regional capital market development in the Baltics, 6 November 2017.

BLOCKCHAIN VALUE – MARKET OVERVIEW

The disruptive potential of blockchain is becoming widely recognised by a growing number of market sectors. Businesses outside of narrowly defined cryptocurrency world are slowly but steadily incorporating distributed ledger technologies into their core products and services. This evolution is partly possible thanks to the advancement in the blockchain itself. The idea of Blockchain 3.0 pushed forward by crypto-enthusiasts and the new wave of start-ups aims to overcome limitations of generation 1.0 (e.g. Bitcoin) and 2.0 (e.g. Ethereum).⁴⁷

As it was already mentioned in chapter 3 of this report, main drawbacks of those early adoptions have been mapped in the areas of: scalability, interoperability, sustainability, privacy and governance. Limitations in these matters constricted wide adoption of blockchain technology outside crypto/financial sector in the past. As of 2019 markets are slowly maturing to include product and services based on DLT in the form of record keeping, smart contracts or transfer of value. Due to the growing familiarity of blockchain among traditional businesses and dynamically developing 3.0 projects such as e.g. Cardano, ICON or Zilliqa, the future of blockchain technology and DLT market in general looks bright. The size of the current global market varies among different reports – from USD 228 million in 2016,⁴⁸ USD 604.5 million in the same year,⁴⁹ USD 411.5 million in 2017,⁵⁰

47 Blockchain 3.0 The Future of DLT? [ONLINE]: <https://cryptoresearch.report/crypto-research/blockchain-3-0-future-dlt/>; cf. Swan, M. (2015), Blockchain: Blueprint for a New Economy, O'Reilly Media, Sebastopol.

48 Blockchain Distributed Ledger Market Overview. [ONLINE]: <https://www.alliedmarketresearch.com/blockchain-distributed-ledger-market>

49 Blockchain Technology Market Size, Share & Trends Analysis Report. [ONLINE]: <https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market>

50 Blockchain Market. [ONLINE]: <https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html>

to USD 708 million in that year⁵¹. Regardless of the market size, all researches are foreseeing dynamic growth in the next four to six years. With Compound Annual Growth Rate (CAGR) projected between 57.6%⁵² and 79.6%⁵³, the market should reach the size of USD 5.43 billion by 2023 according to moderate estimates⁵⁴ and even USD 7.7 billion by 2022,⁵⁵ or USD 60.7 billion by 2024⁵⁶ in some scenarios.

The most dynamic sectors of the market in terms of revenue creation are: banking, financial services and insurance (BFSI/Fintech), manufacturing and supply chain and healthcare. The BFSI is by far the biggest and most profitable sector of blockchain technology, with 60% share in the market revenue (2017).⁵⁷ Other analyses estimate that Fintech blockchain market is currently (2018) valued at the level of USD 370.3 million, with predictions of growth to over USD 6 billion by 2023 (75.9% CAGR).⁵⁸

If BFSI is the blue-eyed boy of the blockchain market today, manufacturing will be tomorrow. By 2020 roughly 40% of the global business value added by blockchain will be coming from the manufacturing sector.⁵⁹ Furthermore, logistics and supply chain management are expected to provide the biggest part of the growth between 2020 and 2025,

51 *Blockchain and Cybercurrency: Market Shares, Strategies, and Forecasts, Worldwide, 2018 to 2024*. [ONLINE]: <https://www.researchandmarkets.com/reports/4459916/blockchain-and-cybercurrency-market-shares>

52 *Blockchain Distributed Ledger Market Overview*. [ONLINE]

53 *Blockchain Market*. [ONLINE]

54 *Blockchain Distributed Ledger Market Overview*. [ONLINE]

55 *Blockchain Market*. [ONLINE]

56 *Blockchain and Cybercurrency: Market Shares, Strategies, and Forecasts, Worldwide, 2018 to 2024*. [ONLINE]

57 *Blockchain Market Size*. [ONLINE]: <https://www.gminsights.com/industry-analysis/blockchain-technology-market>

58 *FinTech Blockchain Market by Provider, Application, Organization Size, Vertical And Region - Global Forecast to 2023*. [ONLINE]: <https://www.reportbuyer.com/product/5439558/fintech-blockchain-market-by-provider-application-organization-size-vertical-and-region-global-forecast-to-2023.html>

59 Gartner (March 2017), *Forecast: Blockchain Business Value, Worldwide, 2017-2030*.

with 80% CAGR and final value of the sector at the level of USD 556 million at the end of that period.⁶⁰

New technologies should be able to save the global healthcare industry even up to USD 100 billion per year by 2025.⁶¹ Big part of that optimisation will be possible thanks to blockchain. From health information exchange systems⁶² to pharmaceutical R&D procedures to drug supply chain⁶³ – all that fields might successfully accommodate blockchain solutions. Therefore, the global value of blockchain in the healthcare sector is expected to reach as much as USD 5.61 billion by 2025.⁶⁴

VC INVESTMENT AND ICOS

The growing market size is also stimulated by rapidly increasing investments into blockchain and DLT start-ups, with venture capital and corporate venture capital in the leading role. In 2017, more than USD 1 billion across 185 deals have been poured into the sector, showing a surge from 2016 which accounted for USD 545 million spread among 135 deals.⁶⁵

60 *Blockchain: Manufacturing Market Forecast until 2025*. [ONLINE]: <https://www.reportlinker.com/p05581104>

61 *Global Blockchain in Healthcare Market - Analysis and Forecast (2018-2025)*. [ONLINE]: <https://www.reportbuyer.com/product/5381406/global-blockchain-in-healthcare-market-analysis-and-forecast-2018-2025.html>

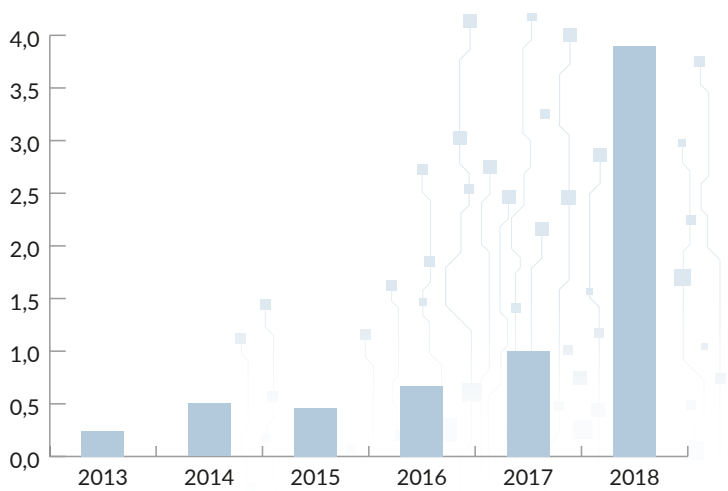
62 Tsung-Ting K., Hyeon-Eui K., Ohno-Machado L. (2017), *Blockchain distributed ledger technologies for biomedical and health care applications*, Journal of the American Medical Informatics Association, Volume 24, Issue 6, p. 1211–1220.

63 Clark B., Burstall R. (2018), *Blockchain, IP and the pharma industry—how distributed ledger technologies can help secure the pharma supply chain*, Journal of Intellectual Property Law & Practice, Volume 13, Issue 7, p. 531–533.

64 *Global Blockchain in Healthcare Market - Analysis and Forecast (2018-2025)*. [ONLINE]

65 *Blockchain Market worth over \$16 bn by 2024*. [ONLINE]: <https://www.gminsights.com/pressrelease/blockchain-market>

Figure 4. Venture Capital Blockchain Investments (USD, billion)



Source: Diar, *Venture Capital Firms Go Deep and Wide with Blockchain Investments*.⁶⁶

As presented in the graph above, in 2018 the size of investments is expected to raise even fourfold. This will be possible in part thanks to the highest VC deal in the history of blockchain start-up market, with investors led by Sequoia Capital providing USD 450 million to Bitmain, a Chinese-based producer of cryptocurrency mining hardware. Other major 2018 investments include the Internet-based distributed computer DFINITY (USD 164 million), the price-stable algorithmic cryptocurrency system Basis (USD 133 million) and the R3 team building its Corda platform for business transactions.

Apart from direct VC and CVC investments, blockchain start-up scene is also dynamically raising valuation due to the growing numbers of Initial Coin Offerings (ICOs). ICO is a blockchain-based alternative to traditional Initial Public Offering (IPO). It might be used by start-ups from all sectors, not only those from the blockchain market.

66 *US Cryptocurrency Exchanges Move at Different Speeds*. [ONLINE]: <https://diar.co/volume-2-issue-39/>

Figure 5. Largest Venture Capital investments in blockchain/DLT companies (as of 11.2018)











COMPANY	SIZE (USD, MILLION)
Bitmain	450
Circle Internet Financial	246
Coinbase	225
Basis	133
R3	122
DFINITY	102
Digital Asset	107
Ripple	93

Source: Pitchbook, *Blockchain Market Map*.⁶⁷

In the standard IPO procedure, a company is publicly selling its shares on one of the regulated stock markets for the first time. ICO provides alternative opportunity for community-based fundraising not regulated by stock-market barriers.

67 *Blockchain Market Map*. [ONLINE]: https://pitchbook.com/news/reports/3q-2018-blockchain-market-map?utm_medium=nl-na&utm_source=reports&utm_campaign=3q-2018-blockchain-market-map

Using blockchain technology, a company is able to generate a restricted number of digital tokens (coins) and to put all of them publicly on sale at one point in time. Every interested person – not only dedicated institutions affiliated with a specific stock market as in case of IPO – might buy tokens using cryptocurrencies. There are several types of ICOs, but the one most similar to IPO is based on the idea of equity tokens, in which case tokens work similarly to shares on the stock exchange. If the company is successful, the price of tokens goes up, if not, it drops. In 2017 over 250 companies took advantage of ICO to raise more than USD 2 billion using that process.⁶⁸ The interest in this alternative way of capital raising has not decreased significantly in 2018, even though research shows that 70% of tokens are currently valued less than at the point of ICO and more than a half of them have dropped by over 0% from their all-time high price.⁶⁹

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply
1	 Bitcoin	\$99 368 929 228	\$5 718.63	\$7 302 806 233	17 376 350 BTC
2	 XRP	\$19 036 347 675	\$0.472697	\$958 181 393	40 271 748 947 XRP *
3	 Ethereum	\$18 645 728 276	\$180.67	\$2 560 433 352	103 204 245 ETH
4	 Bitcoin Cash	\$7 692 678 839	\$440.63	\$1 163 738 787	17 458 275 BCH
5	 Stellar	\$4 377 151 039	\$0.231177	\$98 852 993	18 934 231 065 XLM *
6	 EOS	\$4 189 296 093	\$4.62	\$1 228 883 894	906 245 118 EOS *
7	 Litecoin	\$2 579 100 891	\$43.59	\$595 831 893	59 161 063 LTC
8	 Cardano	\$1 670 752 676	\$0.064440	\$54 075 209	25 927 070 538 ADA *
9	 Tether	\$1 657 372 618	\$0.971256	\$4 658 569 471	1 706 421 736 USDT *
10	 Monero	\$1 503 730 394	\$90.75	\$30 462 794	16 569 936 XMR

Source: Coin Market Cap.⁷⁰

68 Blockchain Market Size. [ONLINE]

69 US Cryptocurrency Exchanges Move at Different Speeds. [ONLINE]

70 Top 100 Cryptocurrencies by Market Capitalization. [ONLINE]: <https://coinmarketcap.com/>

CRYPTOCURRENCY MARKET

Last but not least, blockchain still is commonly perceived through the prism of cryptocurrency market. There are at least 2500 cryptocurrencies in use, with global capitalisation of USD 187,523,091,732 (as of 15.11.2018).⁷¹ The last two years, and especially the last quarter of 2017 and the first two quarters of 2018, have been the time of rapid rise both in their capitalisation and in market diversity. As presented in the following table, currently top three currencies in terms of market value are bitcoin (BTC), ripple (XRP) and ether (ETH). In the light of that, it is worth noting that each of those three cryptocurrencies is built on different blockchain protocols.⁷²

Figure 6. Top Cryptocurrencies by market capitalisation (as of 15.11.2018)

71 Cryptocurrencies. [ONLINE]: <https://www.investing.com/crypto/currencies>

72 A Comparison Between 5 Major Blockchain Protocols. [ONLINE]: <https://medium.com/edchain/a-comparison-between-5-major-blockchain-protocols-b8a6a46f8b1f>



EXECUTIVE SUMMARY:

Blockchain technology is identified with entering the Internet's second era, whose cornerstone is **the exchange of not only information but also value**. Its architecture makes conducting transactions that involve **no intermediaries** possible, and consequently is cheaper and limits onerous bureaucracy.

What ensures **trust** in blockchain networks is mostly such features as: system transparency, high-quality data, single point of failure absent, high security level thanks to cryptographic mechanisms.

From a cybersecurity perspective, blockchain shows potential to help improve the following areas: **identity management** – providing a secure ledger of actions for vulnerable Internet of Things (IoT); **configuration and patch management**; and **supply chain security** – tracking through the entire chain of custody.

Blockchain provides an innovative trust anchor that can help transform decentralised cities and organisations to make them more **distributed, autonomous and secure**. A more egalitarian economy could potentially emerge as producers and consumers regain value from across the supply chain. More control over transactions would occur as consumers become prosumers.

The growing number of sectors are using blockchain to introduce innovations and become cheaper, more transparent and effective. This technology is going to change traditional cumbersome and error-prone systems improving, among others, **banking and financial services, data management, global economy, fair trade, and open societies**.

Thought it's revolutionary and beneficial to the numerous areas of modern-day digital economy blockchain has a few limitations (mostly referred to its widespread type Bitcoin) like high energy cost, scalability, **lack of legal norms, use in illegal activities, privacy issues** and **cybersecurity gaps** which have to be overcome to optimise use of this technology.

Blockchain regulation is not an easy task as it finds itself based on a fragile equilibrium which should ensure the protection of users against criminal misappropriation, while fostering further development of this innovation.

The ultimate aim of regulating blockchain and DLT technology is to ensure the new business ecosystem being built on it is framed and rests on legal certainty. Setting up a **stable and legally well-developed environment** is vital to attract entrepreneurs, to ensure a fair level of competition and to achieve economic growth in the sector.

According to different reports the size of the global market for blockchain based solutions varied between **411.5 and 708 million USD** in 2017. The most dynamic sectors of the market in terms of revenue creation are: **banking, financial services and insurance** (BFSI/Fintech), **manufacturing** and **supply chain** and **healthcare**.

Venture Capital Blockchain Investments in 2018 reached almost **4 billion USD globally**.

There are at least **2500 cryptocurrencies** in use, with **global capitalisation of USD 187,523,091,732** (as of 15.11.2018).



The Kosciuszko Institute is a non-profit, independent, non-governmental research and development institute (think tank) founded in 2000. The Kosciuszko Institute aims to influence the socio-economic development and the security of Poland as a new member of the EU and a partner in the Euro-Atlantic Alliance. Studies conducted by the Institute have been the foundation for both important legislative reforms as well as content-related support for those responsible for making strategic decisions. The Kosciuszko Institute is the originator and organizer of the European Cybersecurity Forum – CYBERSEC, an annual conference dedicated to the strategic aspects of cyberspace.

