Mold*innova*: Trusted DLT Infrastructure for FDI

Pieter van YSSELDIJK[*]
Golnaz A. JAFARI[*]

Abstract
A theoretical analysis of the relative correlation between the implementation of a new information and communications technology (ICT), i.e. distributed ledger technology (DLT), and the establishment of an e-governance system which would enhance communications, security, efficiency of public service-delivery, transparency in transactions, as well as install accountability of decision making. A trusted e-governance based on DLT in combination with a self-sovereign identity (SSI) framework for, among others, security purposes and the development of Industry 4.0 including, among others, Internet of Things (IoT), test cased in Moldova's Free Economic Zones (FEZ), would result in a significant divergence in Moldova's overall credibility and reputation, a consequence of which would be most apparent in the rapid advancement in the field of foreign direct investment (FDI) and the country's inclusive economic growth.

Key words: Moldova, e-governance, distributed ledger technology, digital identity, reputation, foreign direct investment, free economic zones

Introduction

The transition from a resource-based economy to a knowledge-based inclusive economy signifies a major social and economic shift for the Republic of Moldova (Moldova). A key driver in this process is the rapid emergence of ICT and, as proposed, DLT. A strong DLT infrastructure would create the ecosystem in which a substantial growth in the field of FDI could be foreseen. Empirical studies on a number of developed countries are supportive of this argument.

The geographical location of Moldova with its particular political situation places the country in an almost unique position with easy access to both the European Union (EU) and Commonwealth of Independent States (CIS) markets, creating a significant potential for FDI.

ICT is passing through a dynamic development phase in Moldova, with Internet connection services considered as one of the most developed in the world. Various strategies such as 'Digital Moldova 2020' and 'ICT Competitiveness' showcase the ambitious stance of the country.

The implications of a successful e-governance system on the political and social infrastructure of a country become apparent through the increase in transparency and accountability within governing organs and administrative authorities resulting in efficiency in the provision of services and an increased citizen and corporate participation in different spheres. The economic implications of e-governance can result in the elimination of numerous barriers to FDI, the streamlining of lengthy bureaucratic protocols and enhanced accessibility to communication, interaction and business services.

[*] Pieter van Ysseldijk, LL.M. MSc. Ipso Microelectronics Sàrl
E-mail: pietervy@chainreactor.com
[*] Golnaz A. Jafari[*], LL.M.

This paper takes an informative and analytic approach towards the close correlation between disruptive ICT, in particular DLT, and building a trusted infrastructure for e-governance with the embedding of a secure self-sovereign digital identity (SSI) framework compatible with the different privacy laws in the EU. The study will convince the reader that a trusted and transparent e-governance using SSI built on DLT, coupled with the unique geo-political position of Moldova and the different preferential conditions offered through the county's designated Free Trade Zones (FEZ) and Industrial Parks (IP), would pave the way for establishing an attractive environment for FDI and overall economic growth.

1. e-Governance using Distributed Ledger Technology (DLT)

Moldova has a population of around 3.5 million and is considered a lower-middle-income country. It has a small, open economy with economic and financial links predominantly reliant on the EU. The country's transition to a market economy was relatively weaker than in neighbouring countries. GDP per capita in Romania for example was only about a third larger than that of Moldova's in 1990, but stood at three times larger in 2015.

After the global crisis in 2008, the EU has implemented programmes for maintaining economic, social and political stability, as FDI in the country was gradually declining. In addition, a serious fraud case orchestrated by three of its banks in 2014 culminated in a sharp depreciation of its national currency, high inflation and its economy contracting further. Overall, the crisis is considered to be a failure of governance and in the case of the large bank fraud, a lack of banking supervision, with the country's Central Bank held responsible for serious negligence.

Although there is projected economic growth in 2017 due to the implementation of structural reforms, restoring trust in governance of not just the banking sector has been in question more than before, which is continuing political instability. In addition, perceptions of public sector corruption have seen a further decline. The country is 123 among 176 countries in total in the 2016 Transparency International Corruption Perception Index. However, its ranking in the 2017 World Bank Doing Business index has increased to 44 from 52 in 2016.

Moldova has pursued several successful economic reform programmes in the past, as seen in FDI in the area of telecommunication and broadband electronic communication infrastructure. Moldova is currently third worldwide, after South Korea and Estonia, in the ranking of internet access speed.

However, according to the World Bank, for Moldova to get the most out of the digital revolution, the government would need to work on the strengthening of regulations in order to enhance competition, implement an education programme in line with the demands of the new economy and ensure the implementation of effective e-governance, which would render its institutions more accessible and its decisions transparent and accountable.

In comparison, Estonia implemented a number of advanced legal and administrative reforms almost immediately in its post-Soviet era, allowing for a successful transitioning to a digital market economy, and is currently ranking 9th in the EU's Digital Economy and Society Index 2017.

Estonia made access and the use of Internet a basic human right since 2000, well ahead of the United Nation's report, requesting such, from 2011. Also in 2000, Estonia's ID-card digital signature was declared to have equal legal force as a handwritten signature. The country's foundational focal point in this process has been e-governance, in particular the involvement of citizen's rights of representation by means of attestation of their digital identities in for example e-voting in local and Parliamentary elections. Arguably, transparency and accountability as a result of e-governance has helped Estonia to rank 22nd of the least corrupt nation out of 175 countries in 2016, with its GDP per capita reaching 154% of the world's average in 2015 (as opposed to Moldova at 27%).

It has been estimated that the economic effects of digitisation of industry in Europe would create an additional €110 billion of revenue annually. In particular, the "Industry 4.0" programme would involve the integration and interoperability of developments in smart manufacturing, the

digital supply chain, new-generation information technologies such as the Internet of Things (IoT), cloud computing, DLT, add-on services, new business models and big data and data analytics.

However, there is a clear correlation between the development of e-governance and cyber security, which is central to the protection of the availability and integrity of networks, its infrastructure and, in principle, the confidentiality of the information contained therein.

Again, Estonia has also been one of the first countries to develop a national cyber security strategy in 2008 after a series of exploits had brought predominantly government sites down for weeks.

Equally, Moldova's Information Society Development Strategy is aligned with the EU's Single Digital Market (DSM) with its main focus on personal data protection, information systems security and cyber security.

Of all innovations in ICT, DLT is considered, among others, to facilitate advanced solutions in the field of cyber security as data gets copied in a minimum number of decentralised and distributed digital ledgers over a peer-to-peer network of servers.

DLT allows for the storage and broadcasting of digital assets by means of smart contracts, which can be verified and shared in a transparent and immutable manner, depending on the protocol of the network and status of the digital identity, i.e. whether the network is privately or publicly accessible.

Although the scope of applications through use cases are yet to be implemented on a large scale, DLT has already made considerable progress in interoperability with Industry 4.0.

Effects of implementing DLT in the financial services industry for example are proven to be cost efficiencies, reduction of fraud and errors in transactions and overall better accountability and supervision.

In addition, DLT has already brought about eight years of experience in the usage and exchange of alternative digital currencies like Bitcoin. In addition, further development in the field of smart contracts, representing assets and debt instruments, in combination with a secure digital identity framework could structure new forms of liquid crypto-assets, which would for example benefit access to funding to small and medium sized enterprises (SME) and ignite sustainable economic growth.

A recent research by IBM found that out of 200 government organisations worldwide 90% are exploring use cases for DLT that can impact their jurisdictions, in particular in the fields of regulatory compliance, contract management, identity management and citizen services.

The access to trusted data would increase efficiency and would allow authorities to focus on priority sectors, whereby the technology would facilitate the building up of the reputation of institutions and individuals alike, which, in case of publicly accessible DLT networks with full transparency and accountability, would deter and could eventually make fraud and corruption technically too complex to be viable.

DLT would facilitate the transition from economic development promotion based on inward capital investments towards constituting a policy based on institutional change and market openness. Some countries have established special economic zones such as private cities to smoothen transitions in governance. One example is Dubai which has built on its success as a trading and services centre with free trade zones and which has recently focused on implementing an advanced digital economy that would rely heavily on DLT.

2. Digital Identity Framework

As mentioned, cyber security in online data and communication systems is a global issue and is partly due to the practice of centralising the storage of personal data by third party data processor and data controllers.

Across the EU, 68% of Internet users are concerned about digital identity theft, which can be defined as the misappropriation of one's digital identities without consent. Many attacks are made possible by soft spots that are known, ignored or inadequately addressed. One of these weaknesses is related to the vulnerability of commodity hardware and software.

Moreover, as data associated with people's digital identities are typically stored in centralised databases, controlled by third parties, so-called "honey pots" become magnets for exploits, which, in the USA, amounted to a loss of $112 billion during the last six years, affecting 6.15% of U.S. consumers (up from 5.30% in 2015).

Further, more than 1bln digital identities were stolen from Yahoo in 2013 and, more recently, on the east coast of the USA, a large number of so-called distributed denial of service (DDoS) attacks were made possible through the exploitation of IoT devices by simply switching default passwords on thousands of smart devices.

Overall, the human factor in this respect is considered a weakness, whereby bad habits, such as the insecure storage of passwords, re-using of passwords and sharing of passwords can all result in security breaches despite the deployment of costly centralised data storage systems operated by third party data processors and data controllers.

The new legislation in the EU affecting data processors and data controllers targeting EU based data subjects from any worldwide location is further increasing the general governance, risk and compliance (GRC) burden in terms of technology, administration, increased costs and high risks and liability. In financial services for example, it is estimated that GRC costs account for up to 20% of the total overhead cost base of most major banks.

DLT as a peer to peer network technology in principle would align with the new General Data Protection Regulation (GDPR) where it provides for the possibility to function as a neutral, trusted and secure platform mechanism for self-managed pseudonymous digital identities, thus mitigating liability and administrative burdens away from data processors and controllers, as personal data would become ultimately controlled by the data subject or individual.

A digital identity framework built on DLT can be defined as a medium for an immutable method of (part-) storage and communication for cryptographic public-private key pairs, irrespective whether these are representing an individual, real world or virtual asset, machine, smart device or robot.

In 2015 a draft report of the JURI Committee of the European Parliament (EP) set out a series of recommendations on civil law rules on robotics. The Committee stresses the importance of human end-users maintaining the capacity to control its own creations, whereby autonomous robots could be considered as pertaining specific rights and obligations. The draft also proposes a registry for smart autonomous robots to ensure they are legally accounted for.

For full accountability of control over digital identities, a so-called self-sovereign identity (SSI) framework built on DLT would offer solutions.

SSI can be defined as the capability of a digital identity to interact on the basis of trust without compromising the privacy rights of its human end-user. SSI allows exclusive control by an individual over his or her digital identities.

The individual can now provide so-called zero-knowledge proof of attested claims to relying parties and initiate full portability of his or her own data independent from any third party processor or controller. He or she can further act online under the security of pseudonymity using as many digital identities as needed, representing not only one self, but also machines or smart devices under his or her control in full compliance with e-privacy and GDPR regulations.

Moreover, cyber security using SSI becomes a lesser issue in this respect and such would be enhanced by the complexity and economic inefficiency of mounting an attack on individual transactions.

At this stage of technological development, there is still insufficient cross-border interoperability and accessibility of digital identities, digital attestations or claims which is preventing commerce, especially SMEs, from benefitting fully from the opportunities the Digital Single Market is offering.

However, within the DLT innovative worldwide eco system, new networks are being created which would fill this void of interoperability. At the Sovrin Foundation for example, issuers can provide attestations of claims, which individuals, through their relevant digital identities, can forward to requesting relying parties.

3. Privacy and Security: Legal Perspective

Despite the fact that human rights in the fields of ICT and cyber security are central to the EU legal framework and policy making, respect for right to privacy and personal data protection have so far not been aligned with the current practices of centralised control and maintenance by third party data processors and data controllers.

Data centric digital governance in principle requires an effective balance between maintenance of optimal technical security throughout its service delivery and a strong data protection mechanism by design geared towards individual privacy and ethics where, individuals are enabled to retain maximum control over the processing of their personal data at any given time.

In Estonia, the underlying technology for personal data management and online government services, the X-Road, is aimed at minimising individual privacy breach threats. The X-Road's central authority, the Data Protection Inspectorate, is mandated to monitor the implementation of the system. All data is stored on a single platform and is complemented with a number of backup stations outside Estonia. The system is claimed to offer high technical immunity against potential cyber risks, a national policy put in place after the country's governmental services were subject to massive DDoS attacks in 2007.

Nevertheless, given the particularities of every single country in terms of history as well as political and economic landscapes, a 'one size fits all' approach for digitisation of governance and cyber security does not seem feasible. A custom-tailored infrastructure which would better correspond with legal, political and institutional peculiarities of a given country would better address its operative shortcomings.

The Moldova-EU Association Agreement (AA), which entered into force as of 1 July 2016 structured far reaching cooperation. It requires Moldova to align its legal framework with those of the EU and be fully bound by its formal commitments. This includes legal harmonisation in favour of personal data protection. No third country legal entity with a potential to enter into commercial engagements, in the form of a data processor or a data controller, whereby the data of EU citizens are subject to a scrutiny, shall be barred from a defined threshold.

As mentioned, GDPR is the governing legislation behind protection of personal data within the EU which will take effect by May 2018. Complementary to GDPR is the proposed *lex specialis* draft e-Privacy Regulation (replacing the 2002 e-Privacy Directive) which will focus on the processing of data in connection with electronic communication services. Both legal instruments shall be monitored by a single supervisory authority.

It is yet to be seen where DLT would stand from a GDPR perspective, given that the distributed nature could complicate the definition of both a data controller and that of jurisdiction. The definition of personal data per se could also become opaque. Whether a public key could be considered as personal data, given that its association with a natural person could be made, is an intricate question. The GDPR's purpose limitation and data minimisation principles could also be seen as inconsistent with DLT.

From a Moldovan perspective, as of 15 April 2012 a new Act (no. 133/2011) on protection of personal data has entered into force in Moldova, thereby repealing its 2007 predecessor (Act no. 17/2007). The legislation which mainly addresses amendments in the area of processing of personal data puts an emphasis on notification requirement, consent given by data subjects and trans-border transfer of personal data. Notification to the National Centre for Personal Data Protection of Moldova (NCPDP) shall take place prior to any processing of personal data. Freely given, express and unconditional consent from data subjects either in written or electronic format, subject to a number of exceptions, is obligatory. Subject to prior authorisation by the NCPDP on a case by case basis, trans-border transfer of personal data would generally require a similar reciprocity on the protection of personal data in the country of destination, or alternatively the processor in question is conditioned to provide adequate guarantee.

As of November 2016 the Moldovan Parliament has announced a number of amendments to Act no.133/2011. The draft document would further strengthen the role of NCPDP as the sole

regulator while broadly defining 'personal data', creating an apparent divergence from the definition in the GDPR.

Further, Moldovan parliament has passed a law approving the National Development Strategy of the Personal Data Protection and its Action Plan for the period of 2013-2018. The strategy identifies significant inconsistencies in current practices of data operators, processors and collectors, which are continuously undermining the requirements of security and confidentiality. The strategy acknowledges the direct impact of respect for fundamental rights of individuals in the light of Moldova's overall credibility from an international perspective.

Nevertheless, a proposed draft 'Big Brother' law as of October 2016 has created significant controversy. The draft law (no. 161 on Amendments and Supplements to Certain Legislative Acts) allows for obligatory preventive measures in fight against cybercrimes which could arguably pave the way for mass digital surveillance and censorship on Moldovan citizens through retention of metadata. In this scenario, telecommunication service providers would be permitted to practise unjustified data collection, in a clear incompatibility with the GDPR. Moreover, the right to privacy and the right to freedom of expression would be compromised to a large degree, explicitly contrary to the principles enshrined in the European Convention on Human Rights (ECHR).

Further, Article 13 of AA (L260/4 2014) explicitly mandates protection of personal data in accordance with the EU, Council of Europe (CoE) and international legal instruments and standards. Article 99(d) additionally reads *''... enhancing the level of security of personal data and the protection of privacy in electronic communications.''* Specifically, adequate safeguards also ought to be taken with regards to transfer of personal data. (Article 245(2))

The Venice Commission of CoE, as a result, has issued a joint opinion on the 'Big Brother' draft law in December 2016 where outstanding issues are explicitly addressed. Given that Moldova is a member of CoE, amendment of the draft proposal therefore seems inevitable.

The EU has committed itself to a contractual Public-Private Partnership (cPPP) as of July 2016 in order to stimulate a proactive cooperation between public and private actors across Europe in order to create a trustworthy digital environment for innovation where safeguarding measures are obligatory in favour of the right to privacy.

On the other hand, in early April 2017, Moldova signed a memorandum of cooperation with the Eurasian Economic Union (EAEU) requesting an observer status from the EAEU. Such a politically fragmented step, seen as a hindrance to Moldova-EU relations both by the Moldovan parliament and the government, came shortly after the president Igor Dodon signalled the possibility for denouncement of the Moldova-EU AA by 2018. Although from a legal standpoint, the Moldova-EAEU cooperation does not seem incompatible with its commitments under the AA, political polarisation in the absence of an independent judiciary is a strong indicative of cross-disciplinary causality for continued legal uncertainty and unpredictability.

As a consequence, in order for Moldova to be able to shift away from its status quo and to turn the opportunities granted by the EU in to real time accomplishments, the country's existing legal framework must be fine-tuned and made coherent. A predictable regulatory and legal landscape with political stability would be a precursor for a progress not only from an ease of doing business angle, but also for facilitating an innovative domain allowing for an all-inclusive economic growth.

4. Trust and Transparency: Structuring FDI

With digitalisation and enabling innovative technologies, the paradigm of trust and the public perception of this concept have been rapidly going through a shift where the trend is geared towards trust-less and disintermediated infrastructures. Regaining trust in public institutions, as a result, has inevitably been given a priority in working agendas of central governments.

As seen in the case of Moldova, corruption and low institutional quality within an operating system and governance and the consequential lack of transparency and accountability have been indicative of a direct link with low economic growth and underdevelopment.

However, transparency enhancement in governance is not an overnight process and cannot be easily quantified or isolated from other complementary factors. It requires strategic planning, collective policy making, aligned motives among governing authorities alongside employment of technology know-how with timely implementation and supervision.

According to an OECD report, obstacles to transparency-oriented reforms can be political, institutional, technological or financial in any combination. Overcoming the dynamics of the concept of 'concentrated benefits' within a given political system is often considered cumbersome, so is the task of capacity building.

As seen before, growth by inward FDI, either vertical or horizontal, requires various incentives before a relationship between the host country and an enterprise is duly established. From market potential, investment climate and competitive landscape to procedural bureaucracy and applied barriers to trade, all are directly stimulated by quality of governance and institutional functionality. Determinants are numerous and often subjective.

However, objectively speaking, certain variables could generally be considered as definitive. Stability within a country's legal and regulatory framework, its predictable policy-making environment, the accountability and auditability of governance, as well as respect for foreign investors' right to access and use of policy information, are equally taken into account together with market characteristics and prospects for market growth.

In Moldova the existent irregularities in particular with regards to volatile amendments to fiscal policies has resulted in an unpredictable environment which inevitably pose a great challenge for commercial purposes and for building long term strategic plans for doing business with foreign countries. In particular, the lack of corporate governance in banking sector and independent judicial oversight has equally compromised general public trust in Moldova's financial industry. Moreover, limited access to finance and inefficiency in public administration has as a result been deterrence for entrepreneurs and foreign investors.

In short, obstacles to FDI in Moldova include all the three phases of pre establishment, installation and post establishment. Procedural complexities, multi-layered authorisation requirements and licensing requires substantial amount of human resource involvement. Lack of infrastructural development and unjustified regulatory volatility are among the key considerations under the Moldova 2020 agenda.

Moldova's FEZ and IPs, on the other hand, carry a substantial potential for the creation of an advantageous eco system for foreign investors. There is currently a handful of FEZ in Moldova, which are managed by independent administrators, together with IPs, the Free International Port of Giurgiulesti on the Danube in the south and the Free International Airport of Marculesti in the north of the country.

All have preferential customs tariff treatments and attractive fiscal and non-fiscal exemptions. Being export-intensive by design, FEZs in Moldova are generally immune from volatility of legal and regulatory reforms, whereby customs bureaucracy is also streamlined to some degree. As a result, increasing the number of FEZ and IP establishments throughout the country and the stimulation of a complementary rather than fragmented environment would undoubtedly be beneficial for improving the FDI growth. Such stimulus was also placed among the determinants in Moldova's Strategy for attracting investment and promotion of exports between the years 2016-2020.

Public-private partnership and an active engagement of actors through dialogue is also an essential feature in establishing an all-inclusive economic growth in a digitised society which as a programme has also strongly been endorsed by the EU for the purpose of establishing a reliable digital community in Europe. Incentives behind an accountable and auditable model of digital governance for Moldova should therefore be clearly defined from the outset to ensure good practice. An emphasis is placed accordingly in Article 63(b) of AA.

From the outset, Moldova's geographical location between Europe, Asia and Russia together with its accessibility to the Black Sea creates many opportunities, with the added advantage that skilled labour and cost of living are relatively economical and accessible.

Further, with Moldova being a member of WTO and as part of its AA, the country is among the DCFTA (Deep and Comprehensive Free Trade Agreement) countries together with Georgia and Ukraine. This framework provides a preferential trade mechanism which includes enhanced investment conditions. DCFTA sets ground for Moldova to harmonise its trade-related laws in line with the EU. Furthermore, the EU's Eastern Partnership with its Eastern neighbour countries including Moldova aims at creating a Digital Community where improved digital governance and ICT infrastructure for the Eastern bloc is foreseen. Article 22 of AA demands the introduction and implementation of e-governance in order to ensure a participatory and transparent transition. This is indicative of Moldova's formal commitments for implementing extensive structural reforms.

A modernised ICT infrastructure for governance operating on a DLT platform would strongly level the playing field by enabling SMEs for example to have easier access to real time data on a given foreign market through interactive communication. A better understanding of decisive factors for FDI which includes prediction of prospective trends and prompt identification of a new market demands would therefore enable SMEs to easily adjust to emerging dynamics of a foreign country. In addition, DLT implementation would capacitate SMEs to minimise counterparty risk and fraud.

However, DLT in itself has not been free from security risks as it has been subject to a number of large scale cyberattacks where in most cases rather than being a technical vulnerability, the compromise has been stemmed from relatively insecure and inadequate computational programme coding.

Gaining national trust is a pre requisite for rebuilding Moldova's image beyond borders. As such would only be feasible with a transparent disintermediated mechanism where public institutions are held accountable for their policy decisions and where information is easily accessible both for Moldovan citizens and foreign investors.

Therefore, a SSI framework structured on DLT, namely the Mold*innova* model, would provide the possibility for creating blocks of information and transactional data that are immune from third party manipulation, revision or corruption once information and transactional data have securely entered into the chain. Such infrastructure thus has the potential to improve traditional legacy designs for governance in Moldova through a shift towards a participatory model with strong auditability, where for example local governmental budget allocations and expenditures are instantly verifiable and traceable.

Given the favourable conditions geared towards acceleration of economic and technological development as well as the relative regulatory stability offered within the Moldovan FEZ and other specially designated territories, the authors of this paper take a view in favour of establishing a pilot project in a nominated FEZ within the scope of the Mold*innova* model.

In case of trade, as a use case, trust between parties would become verifiable due to the fact that attestation and authentication of digital identities of trade partners and the authorisation of transactions can only be performed to a near perfect level of assurance, facilitating the burden of proof in case of litigation. In case of manufacturing, on the other hand, the ability to hold specific entities behind issuing digital identities responsible for quality attestations would lead to increased efficiency, reduced litigation and higher levels of trust.

Based on the experience with the pilot project in a FEZ, regulators in Moldova are given the opportunity to build the necessary institutional and technical processes into a nationwide DLT and SSI based e-governance infrastructure, and to focus their efforts on stimulating FDI and inclusive economic development.

Conclusion

Through an informative and analytic approach, the authors of this paper have aimed at bringing initial clarity to the concepts of e-governance, SSI framework and DLT infrastructure. Relevant legal and regulatory aspects have also been touched upon in depth, especially in the areas where Moldova and the EU meet in crossroads, given the formal and reciprocal commitments the two parties have signed up for.

Lastly, the paper sheds light on the significance of FEZ and other specially designated territories in Moldova, where preferential conditions could be taken advantage of ,with the aim of introducing a maximum level of transparency and trust to Moldovan society, in particular by means of implementing a strong e-governance and digitisation programme and by achieving gradual inclusive economic growth.

Personal data protection, in line with the EU's DSM, is a fundamental right enshrined in national law in Moldova. Any new e-governance model would have to facilitate trust among investors and Moldovan citizens as a whole, not only by providing the right technical infrastructure but also by assuring cyber security, e-privacy, regulatory compliance and ease of use in communications.

The authors propose a model for e-governance by utilising a SSI framework built on DLT, the Mold*innova* model, which would be implemented as a pilot project in a given FEZ in the country, where digital identities in control of FEZ residents would be attested, and digital interactions established, maintained and communicated in an innovative way in every element of the FEZ eco system.

More specifically, Mold*innova* would provide FEZ residents and individuals the means to interact digitally on the basis of pseudonymity whereby the data from multiple digital identities, representing humans, machines, smart devices, etc. would be stored and broadcasted in a secure manner on different DLT networks. Spin-offs to IoT, M2M, and Industry 4.0 would enhance transparency in finance, trade and manufacturing, benefitting in particular SMEs.

In addition, through this model of e-governance enhanced efficiency, optimised security and real time regulatory compliance could be foreseen for Moldova's industrial sectors nationwide.

The most significant anticipated outcome of the strategic planning and implementation of the Mold*innova* model is however the creation of a trustworthy and transparent landscape, with consequences for inclusive economic development for Moldova, which would eventually be most apparent on an international scale.

References:

1. Act no. 133/2011, Law on Personal Data Protection, Official Gazette of the Republic of Moldova, No. 170-175/492, 2011
2. Bergmann, Christoph, Autonomy or Just Another Slavery?: Ukraine and Bitfury Start Full-scale Blockchain e-Governance Programme, 2017
3. Birch, David, Identity is the New Money, 2014
4. Chirtoaca, Marian, Incentives and Exemptions offered by Moldovan Free Economic Zones, 2016
5. Czarnecki, Jacek, Blockchains and Personal Data Protection Regulations Explained, 2017
6. Doing Business, Economy Rankings, World Bank, 2017
7. EDRi (European Digital Rights), The Republic of Moldova ''Big Brother'' Law, 2017
8. EU Special Eurobarometer 423, Cyber Security, 2015, p.57
9. European Civil Law Rules in Robotics, 2016, p.12
10. Foreign Investors Association (FIA), White Book: Proposals for Improvement of Investment Climate in the Republic of Moldova, 2015, pp. 9-25
11. G20 Blueprint on Innovative Growth, 2016
12. Halford, Ch. and Cameron-Perera, Sh., Moldova - Parliament announces amendment to draft data protection law, 2017
13. IBM Institute for Business Value, Building trust in government. Exploring the potential of blockchains, 2017, p.6

14. IDIS Viitorul, Attracting foreign direct investment in Moldova – potential, impediments and achievements, 2017
15. IMF Mission, Extended Credit Facility and Extended Fund Facility (ECF/EFF) arrangement, 2017
16. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN (2013) 1 final, 2013
17. Kuchler, Hannah, Cyberattacks raise questions about blockchain security, 2016
18. L260/4. 2014, Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and the Republic of Moldova, of the other part. Official Journal of the European Union, 2014
19. RFE/RL, Moldova's Dodon signs Memorandum on Cooperation with Eurasian Economic Union, 2017
20. Lurkovski, Vladimir, Moldova: New Act on Personal Data Protection in Moldova, 2012
21. Memminger, M. and Baxter, M. and Lin, E., Think You've Heard of Fintech, Get Ready for 'Regtech', 2016
22. Moldova Activity Program, European Integration: Freedom, Democracy, Welfare, 2009, p.15
23. Moldova 2020 National Development Strategy, 7 Solutions for Economic Growth and Poverty Reduction, pp. 33-38
24. Monahov, A. Jobert, Th., Case Study of the Moldovan Bank Fraud: Is Early Intervention the Best Central Bank Strategy to Avoid Financial Crises?, 2017, p.16
25. OECD, Public Sector Transparency and the International Investor, 2003, pp.28-32
26. Pascual, Al. Marchini, K. Miller, S., Identity Fraud: Securing the Connected Life, 2017
27. PwC, Opportunities and Challenges of the Industrial Internet Industry 4.0., 2014, p.30
28. Schmaljohann, Maya, Enhancing Foreign Direct Investment via Transparency? Evaluating the Effects of the EITI on FDI, 2013, p.6
29. Sovrin Foundation, The Inevitable Rise of Self-Sovereign Identity, 2016
30. Tabarrok, A. Rajagopalan, Sh., Private Cities, Open to All, 2015
31. Transparency International, Corruption Perceptions Index 2016, 2017
32. UNCTAD World Investment Report, FDI from Developing and Transition Economies: Implications for Development, 2006
33. United Nations, Frank la Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2011
34. Venice Commission and DGI of the Council of Europe, Joint opinion on the draft law no.161 amending and completing Moldovan legislation in the field of cybercrime, 109th Plenary Session, 2016
35. World Economic Forum, How Technology Can Unlock the Growth Potential along the New Silk Road, 2017, p.6
36. World Bank, Moldova Trade Study Note 4. The Performance of Free Economic Zones in Moldova, 2014, pp.7-12
37. World Bank, Moldova report, Special Topic: Paths To Sustained Prosperity, 2016