Intellectual Output 1

Rationalisation Phase

Deliverable: IO1/A1

BCT4SMEs

10.03.2021

ASSERTED KNOWLEDGE

Authored by: [NAME OF THE AUTHOR]

Project Number: 2020-1-UK01-KA202-078895

Co-funded by the Erasmus+ Programme of the European Union

REVISION HISTORY

Version	Date	Author	Description	Action	Pages
1	24/2/2021	AKNOW	Template Creation	C	8

(*) Action: C = Creation, I = Insert, U = Update, R = Replace, D = Delete

REFERENCED DOCUMENTS

ID	Reference		Title
1	2020-1-UK01-KA202-078895		BCT4SMEs Proposal
2			

APPLICABLE DOCUMENTS

ID	Reference		Title
1			
2			

Executive Summary

This documents presents the deliverable of the activity IO1.A1 of the BCT4SMEs Project (henceforth, "Project").

Small businesses confront several problems in the business economy. Many of them face barriers in entering trade markets, while others can confront difficulties in several sectors, such as transactions, data storage, cash flow, and security. Blockchain technology can offer a solution to these challenges, as it can have a wide range of application in many fields, such as IoT, monetary exchange (bitcoin), storage, etc.

The project aims to support SMEs managers and owners in integrating blockchain technology and benefit from the advantages it comes with.

The present document contains information regarding:

- The security and financial issues that SMEs face in partner's countries;
- Information about the successful application of blockchain technology in the EU;
- Conclusions on the gap between the desired situation and the present situation.

Table of Contents

1. Methodology

During the rationalization phase, we will conduct research regarding the current problems that SMEs confront in terms of finances and security in partners' countries (UK, Netherlands, Spain, Greece, Cyprus, Poland). This phase will be called the "National Phase". The conclusions of the National Phase will reveal the present situation ("AS-IS").

We will also identify the winning practices from SMEs that use blockchain technology to address the issues that have proved challenging to SMEs. This phase will be called the "Transnational Phase". The best practices will include information on the successful implementation of blockchain technology in SMEs across the EU.

The comparative analysis of the Transnational Phase with the National Phase will reveal the gap between the desired situation ("TO-BE") and the present situation ("AS-IS").

2. National phase

2.1 Financial Challenges for SMEs

In this section you can include the main problems that SMEs confront in terms of finances and their consequences. The industry sectors that these problems are most common should be also identified.

Examples of areas that financial challenges can be found: access to financing, investments, payments, exports, cash flow management

Maximum length: 3 pages

This desk research has the objective of collecting existing information on the financing needs of SMEs in Cyprus, focusing on the main financial challenges that SMEs confront and their consequences [1]. The report focuses on: (i) Information on the macroeconomic market environment in Cyprus and (ii) The lessons learnt from past experiences with financial instruments (FIs) in Cyprus.

SMEs are the backbone of the Cypriot economy, since they produce nearly 75% of the value added of the non-financial business sectors, which is 17% higher than the then EU average [1]. At the same time Cypriot SMEs generate 83% of jobs in the non-financial sectors, in contrast to approximately 66% which is the EU average [1]. As a result, promoting growth and investment by among SMEs is a top EU policy priority, which requires that financial challenges are tackled.

As defined in the Small Business Act for Europe (SBA) Factsheet report for Cyprus in 2019 [4], Cyprus' SBA performance is mixed. State aid & public procurement and internationalisation are now both above the EU average. In particular, State aid & public procurement improved substantially compared to last year that this was below the EU average last year. Secondly, the Entrepreneurship, 'responsive administration' and skills & innovation are in line with the EU average. Finally, 'Second chance' and single market are below the EU average. In fact, Cyprus is among the EU's weakest performers for SMEs' access to finance [4].

The main European Investment Fund (EIF) SME Access to Finance Index (ESAF) results for 2018 are presented in Figure 1 [7]. The leaders in this updated version of the ESAF is now Sweden, with Germany and Finland in the second and third place respectively. Greece is ranked last in the ESAF ranking for the sixth consecutive year in a row, preceded by Cyprus and Romania.

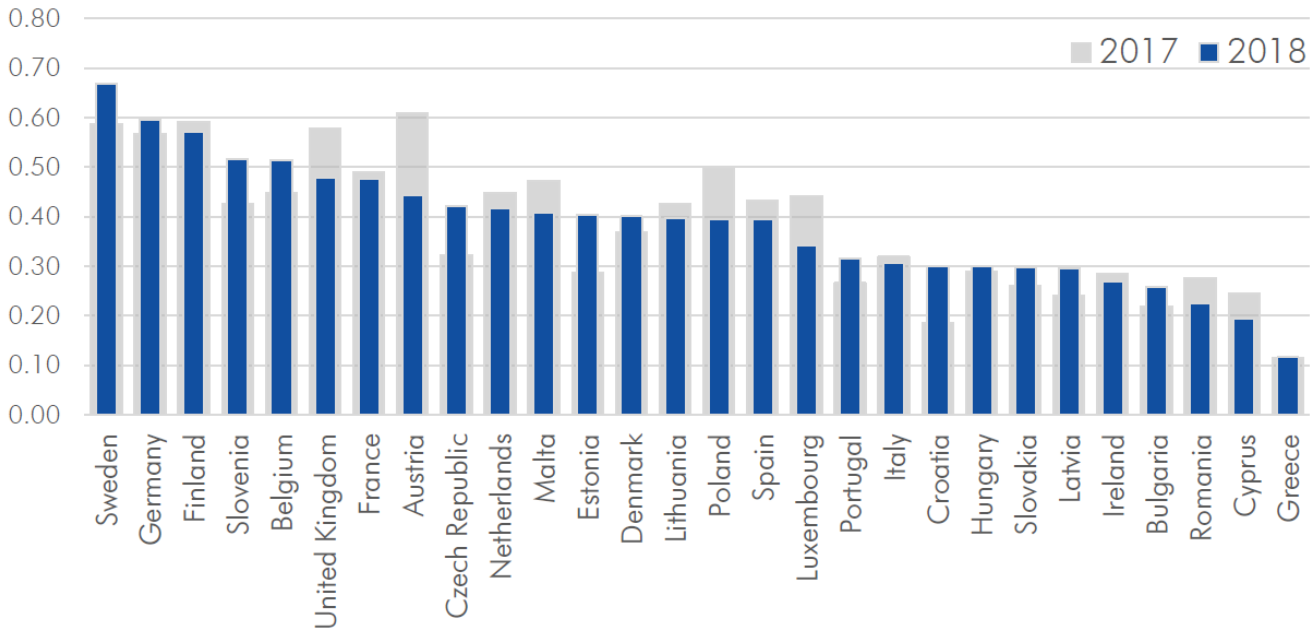

Figure 1: The EIF SME Finance Index: country comparison and evolution over time – Source: Torfs (2019)

Access to Financing

The primary challenge faced by Cyprus SMEs is generally the lack of access to financing. In order for SMEs to grow and/or drive innovation they need to be able to have access to finance. Especially in Cyprus, following the financial crisis, financial intermediaries have been limited by creditworthiness constrains, and by the need to apply strict risk management standards, making it difficult for SMEs to qualify for access to finance. Therefore, they are overly dependent on bank lending, and alternative financing options such as Venture Capital (VC), Business Angels (BA) and crowd funding are limited. This significantly hampers their capability to invest and grow. According to a 2016 survey, 25% of Cypriot SMEs cited difficulties in access to finance as their most important concern, the highest across EU [2]. As such, the introduction of FIs could be a good means to develop businesses in Cyprus.

On the other hand, Cyprus performs above the EU average in State aid & public procurement [4]. It has the EU's highest score for the proportion of bids coming from SMEs. This score is one of the highest percentages of awards won by an SME. Despite a drop, in 2019, of approximately 7 percentage points in the share of the total value of public contracts awarded to SMEs, it is still above the EU average [4]. Still a problem that remains in terms of State aid & public procurement is the long time required to receive the actual payments.

Securing Investments

Despite the fact that the Cypriot government, since 2008, has defined and put in place some actions and specific measures to financially support SMEs, still access to finance and particularly investments is a continuous and key obstacle for start-ups and SMEs [4]. In specific, the Ministry of Finance introduced several tax incentives to encourage individuals to invest either directly or via investment funds in innovative start-ups and SMEs [10]. This was performed in order to counter the drop in public financial support. Moreover, in other actions, the Ministry of Energy, Commerce and Industry also introduced measures to extend finance and investments for specific target groups (e.g. young people and women). Another relevant measure was adopted, namely the Alternative Investment Funds Law that aims to introduce: (i) the Reserved Alternative Investment Fund (RAIF); (ii) limited partnerships

with legal personality as an alternative investment fund vehicle; and (iii) arrangements for establishing a variable capital company to increase the versatility of limited companies as a corporate vehicle for open-ended funds [4].

Duruflé, Hellmann and Wilson (2017) identify the main elements of a strategy to help Europe catch up to the US in terms of scale-up funding: creation of larger venture funds and a venture debt market, reinvigoration of tech IPOs, improved markets for secondary shares and avoiding to sell companies too early [8].

Late Payments

The entire European economy is negatively affected by late payment. To protect European businesses, particularly SMEs, against late payment, the EU adopted Directive 2011/7/EU on combating late payment in commercial transactions in February 2011. Each year across Europe thousands of small and medium-sized enterprises (SMEs) go bankrupt waiting for their invoices to be paid. Jobs are lost and entrepreneurship is stifled. Late payment causes administrative and financial burdens, which are particularly acute when businesses and customers are in different EU countries. Cross-border trade is inevitably impacted.

On the face of it, late payments to businesses in Cyprus have fallen significantly in the post-bail-in period, with fewer than half of all respondents affected [3]. It is almost certain that this trend reflects the reduction in trade credit, as opposed to an improvement in credit conditions. If this interpretation is true, then it suggests that a substantial number of businesses in Cyprus have reverted to working mostly on a cash basis, post-bail-in.

Although things have improved since then, still the amount of time it takes to get paid by customers and the share of bad debt loss (i.e. the number of receivables that have to be written off because of not being paid) is among the highest in the EU [4]. According to a 2016 Commission report on the implementation of the Late Payment Directive [5], Cyprus ranked last for payments in business to business (B2B) transactions with an average payment period of 85 days (business to public (B2P) 84 days) [6].

In addition, the average delay in payments from public authorities continues to be a significant challenge for SMEs in Cyprus. The length of delay continues to be among the longest in the EU [4].

Cash Flow Management

For Europe's valued SMEs, any disruption to cash flow can mean the difference between solvency and bankruptcy [9]. The economic crisis presented numerous difficulties, but for SMEs the challenges presented by late payment have grown disproportionately as credit lines and bank loans become less available. In many countries, the loan financing gap appears to have increased (see Figure 2). In Ireland, Austria and Germany (north-eastern quadrant), banks tightened the supply of credit to SMEs while facing increased loan demand [7]. Furthermore, banks in Cyprus, Greece, Malta, Latvia, Slovakia Luxembourg and Italy kept credit standards constant but reported an increase in loan demand. In Belgium, Slovenia and Spain, loan demand reportedly stayed constant, but credit standards were tightened (considerably so in Belgium) [7]. All these cases imply an increase in the financing gap, from the (supply) perspective of bank. In overall, Cyprus faces serious challenges in terms of access to finance, including other credit lines and bank loans, investment funds and heavy delays in terms of payments, which all contribute to the cash flow management issue.

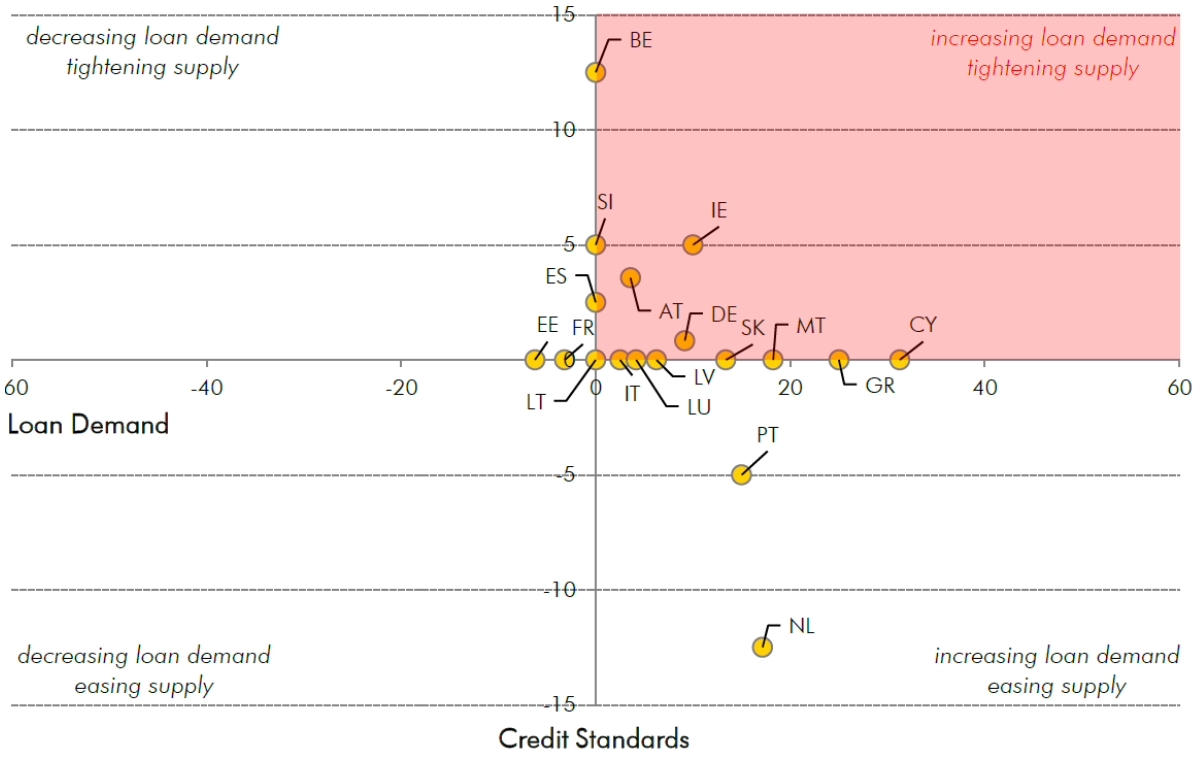

Figure 2: The SME financing gap from a supply perspective (HY1/2019) – Source: Authors, based on ECB Bank Lending Survey (ECB, 2019c)

2.2 Security Challenges for SMEs

In this section you can include the main problems that SMEs confront in terms of security and their consequences. The industry sectors that these problems are most common should be also identified.

Examples of areas that security challenges can be found: cyber threats, infringements, transactions and payments, data storage (cloud storage).

Maximum length: 3 pages

Commonly larger enterprises have more digital capabilities and are more concerned with their security, while SMEs tend to be less digitally intensive, have less ICT capabilities and smaller to no IT teams. Therefore, depending also on specific factors, such as the nature of their business, their sector of activity and/or immaturity to apply appropriate digital security practices, SMEs have a higher probability of suffering an incident [11]. Furthermore, although digital transformation is essential and required given the vulnerabilities that the COVID pandemic revealed, still it increases SMEs exposure to digital security risks and likelihood to be victims of cybercrime. In fact, it makes SMEs more exposed to digital security incidents and making them more reliant on digital technology [11]. The Internet of Things increases digital connectivity, the number of vulnerabilities to exploit and the potential frequency or probability of attacks, while other technologies such as cloud computing further increase the exposure due to the use of cloud services and data storage in the cloud. Cyprus has a cybersecurity strategy in place since 2012 [17], while the Digital Security Authority has proposed a new cybersecurity strategy, which is pending final approval from the Ministry of Communication and the Council of Ministers [18].

Cyberthreats

Cybercrime is considered a huge threat to states' economies. Therefore, it is critical to raise awareness, to have a good level of collaboration with relevant stakeholders but most importantly have the right tools that can shield business and the economy in general. In an effort to address the above issue the conference titled "How S@fe is Your Business?" was organized in Cyprus back in 2017, by the by the Cyprus Chamber of Commerce and Industry and the Cyprus Neuroscience and Technology Institute [11]. It was addressed, among others, by Luigi Rebuffi, secretary general of European Cybersecurity Organization and George Michaelides, commissioner of Electronic Communications and Postal Regulation of Cyprus [11]. It is estimated that 43% of cyberattacks target SMEs. Cybercrime costs are projected to reach €2 trillion ($2.15 trillion) by 2019 whereas 19% of business in the EU admitted that they have been attacked. Some 68% of funds are lost as a result of a cyber attack and these funds were declared unrecoverable. In 2015 there were 38% more security incidents detected than in 2014 while only 38% of global organizations claim they are prepared to handle a sophisticated cyberattack.

Infringements

Digitalization has made the protection of trade secrets increasingly difficult. The revolution in data codification, storage and exchange (i.e. cloud computing, emails, USB drives) are prime drivers of a rise in trade secret infringements [12]. Increasing value given to intellectual property (and de facto its misappropriation), staff mobility and changing work culture and relationships (e.g. temporary contracts, outplacement, teleworking) or the fragmentation of global value chains (with more foreign parties involved within more diverse legal frameworks and uneven enforcement conditions) also contribute to increase exposure and risk of disclosure [13].

A trade secret is a valuable piece of information for an enterprise that is treated as confidential and that gives that enterprise a competitive advantage. Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) harmonises the definition of trade secrets in accordance with existing internationally binding standards [4]. With much delay, in 2021, Cyprus has transposed the directive for the protection of undisclosed Know-how and business information (trade secrets) against infringements.

Transactions and Payments

Data are increasingly generated along business operations, e.g. production and delivery (process data), and compiled at various stages of business transactions (user, consumer and supplier data) [15]. User, consumer and supplier data are crucial for developing market knowledge, improving customization and shaping new products and business models. In addition, the COVID-19 crisis has made more businesses reliant on digital technology than before, giving an opportunity for malicious actors to intensify attacks, e.g. phishing then fraud, taking advantage of sudden and massive surge in teleworking arrangements and online transactions. The typical criminal is primarily interested in obtaining credentials and personal data [16]. After those two categories, medical, internal or payment data are roughly the same in terms of interest.

SMEs make up 99% of the European businesses and while 77% of SMEs have a website only 17% are selling online (Digital Economy and Society Index (DESI) 2019). At the same time, 41% of Europeans are concerned about the security of online payments (Eurobarometer Europeans' attitudes towards cyber security – January 2020). Moreover, Web sales was the dominant mode of conducting e-sales in

all EU Member States in 2019. The percentage of enterprises receiving electronic orders only over websites or apps ranged with Cyprus being only at 12% (below the EU average – 15%), ranked 24th and well beyond leaders such as Denmark (24%) [18]. Consequently, websites or apps are increasingly offered by enterprises or third parties for various purposes. By contrast, in 2019, the percentage of enterprises that used only EDI-type messages for their sales ranged from 1 % of enterprises in Bulgaria, Romania, Luxembourg, Cyprus and Poland to 8 % in Czechia and 9 % in Sweden [18]. Although Cyprus, is not one of the leading EU countries in terms of web transactions and payments, especially from SMEs, still the COVID pandemic and the need and strategy of digital transformation of the EU and its Cyprus steps to adopt it have contributed to an increase in SMEs interested to enhance their e-commerce capabilities, while over the last years scams and frauds in online transactions and payments are increasing in volume and frequency also for Cyprus. This can be attributed to the strive for digital transformation.

Data storage (cloud storage)

Due to its flexibility and scalability, cloud computing reduces the costs of technology upgrading by exempting firms of upfront investments in hardware and regular expenses on maintenance, IT team and certification, turning ICT management model into a model based on software acquisition (codes) and digital (hyper)connectivity [19]. Data on business use of ICT across OECD and EU countries highlights the close relationship between digital vulnerability, and hyper-connectivity and codification. As firms tend to increasingly purchase cloud computing services or their employees to use computer with Internet access, they are more likely to experience ICT related security incidents. In fact, the increasing connectivity of data-intensive activities adds layers of complexity, volatility and dependence on existing infrastructures and processes [20]. Cloud computing is resulting in increased migration of sensitive data to external parties to the enterprise in question, which means that security and protection of that data are technically managed by an external party.

The leading sectors in terms of ICT spending in Cyprus are the financial sector, followed by the ICT and the public sectors [18]. In terms of digital technology integration, even though Cypriot SMEs engage in the use of social media and e-commerce activities, they are less inclined to take up new technologies such as Cloud Computing, partly due to concerns about security and the ownership and availability of data [18], as attested in the DESI 2018 Cyprus report. However, recently as defined in DESI 2020, digital transformation (DX) projects appear to be gaining momentum among Cypriot enterprises, even though they are still at an early development stage, which is evident from the growth of cloud adoption from 12% (DESI 2018) to 18% (DESI 2020) and big data technologies from 3% (DESI 2018) to 12% (DESI 2020) and big data technologies. As a result of the increased adoption of cloud computing and big data technologies, SMEs in Cyprus and the government (new cybersecurity strategy to be approved in 2021) have a vital need for these technologies to offer security in their use, which is defined as the preservation of the principles of confidentiality, integrity and availability of information during its transmission, processing and storage [17].

References

[1] European Investment Bank, Assessing the potential use of Financial Instruments in Cyprus, A study in support of the ex-ante assessment for the potential future use of Financial Instruments for SMEs,

ICT, and the Low-Carbon Economy in Cyprus, Final Report, Prepared by PricewaterhouseCoopers (PwC), 21 July 2017.

[2] European Commission, "Small and Medium Sized Enterprises Access to Finance", European Semester Thematic Factsheet, 2016.

[3] ACCA (the Association of Chartered Certified Accountants), "Access to finance for SMEs in Cyprus: an update from ACCA", 2014.

[4] European Commission, Performance Review – 2019 SBA Fact Sheet, CYPRUS, Available Online (Last Accessed: 15 April 2021): https://ec.europa.eu/docsroom/documents/38662/attachments/6/translations/en/renditions/native

[5] European Commission, Report from the Commission to the European Parliament and the Council on the implementation of Directive 2011/7/EU of the European Parliament and of the Council of 16 February 2011 on combating late payment in commercial transactions, COM/2016/0534 final. Available Online (Last Accessed: 15 April 2021): https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2016%3A534%3AFIN

[6] Commission Staff Working Document, Evaluation of the Late Payment Directive/ REFIT evaluation, Available Online (Last Accessed: 15 April 2021): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0278&from=en

[7] Kraemer-Eis, Helmut; Botsari, Antonia; Gvetadze, Salome; Lang, Frank; Torfs, Wouter, "European Small Business Finance Outlook: June 2019", EIF Working Paper, No. 2019/57, European Investment Fund (EIF), Luxembourg, 2019, Available Online (Last Accessed: 15 April 2021): https://www.eif.org/news_centre/publications/EIF_Working_Paper_2019_57.htm

[8] Duruflé, G., Hellmann, T. and Wilson, K. (2017). From Start-up to Scale-up: Examining Public Policies for the Financing of High-Growth Ventures. Prepared for the CEPR/Assonime Programme on "Restarting European Long Term Investment Finance". Date Written: 01.09.2016. Saïd Business School WP 2017-05.

[9] European Commission, "Internal Market, Industry, Entrepreneurship and SMEs – Late Payment Directive", Available Online (Last Accessed: 15 April 2021): https://ec.europa.eu/growth/smes/sme-strategy/late-payment_en

[10] European Commission, "Internal Market, Industry, Entrepreneurship and SMEs – SME Performance Review", Available Online (Last Accessed: 15 April 2021): https://ec.europa.eu/growth/smes/sme-strategy/performance-review_en

[11] Financial Tribune Daily and Contributors, "Cyprus Says Cybercrime a Huge Threat to Economy", Available Online (Last Accessed: 16 April 2021): https://financialtribune.com/articles/world-economy/58821/cyprus-says-cybercrime-a-huge-threat-to-economy

[12] Organisation for Economic Cooperation and Development (OECD), "Chapter 2. Digital security in SMEs – The Digital Transformation of SMEs", OECD Studies on SMEs and Entrepreneurship, OECD Publishing, Paris, https://doi.org/10.1787/bdb9256a-en, Available Online (Last Accessed: 16 April 2021): https://www.oecd-ilibrary.org/sites/cb2796c7-en/index.html?itemId=/content/component/cb2796c7-en

[13] Almeling, D. (2012), "Seven Reasons Why Trade Secrets Are Increasingly Important", Berkeley Technology Law Journal, Vol. 27, p. 1091, http://dx.doi.org/10.15779/Z38SM4F.

[14] European Commission, "Trade secrets: Commission decides to refer Cyprus to the Court of Justice for not transposing the Trade Secrets Directive", Press release, 30 October 2020, Brussels, Available Online (Last Accessed: 16 April 2021): https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1683

[15] OECD (2019), OECD SME and Entrepreneurship Outlook 2019, OECD Publishing, Paris, https://dx.doi.org/10.1787/34907e9c-en.

[16] Verizon (2020), "2020 Data Breach Investigation Report", Available Online (Last Accessed: 16 April 2021): https://agio.com/newsroom/key-takeaways-from-verizons-2020-data-breach-investigation-report/

[17] European Union Agency for Cybersecurity, "Cybersecurity Strategy of the Republic of Cyprus - 2021", Available Online (Last Accessed: 16 April 2021): https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf/view

[18] European Commission, "Digital Economy and Society Index (DESI) 2020, Cyprus", Available Online (Last Accessed: 16 April 2021): https://ec.europa.eu/cyprus/sites/default/files/desi2020-cyprus-eng.pdf

[19] OECD (2019), OECD SME and Entrepreneurship Outlook 2019, OECD Publishing, Paris, https://dx.doi.org/10.1787/34907e9c-en.

[20] OECD (2017), OECD Digital Economy Outlook 2017, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264276284-en.

3. Transnational Phase

3.1 Best practices in application of blockchain technology in finances

Name of the company	we.trade
Website	https://we-trade.com/index.html
Sector	ICT: serves Finance, Banking, Business Trading
Country	Ireland
Description of the issues that the company was facing before the application of blockchain technology (if applicable).	Traders, particularly SMEs, who traditionally did not have access to bank guarantees, invoice financing and credit insurance, use we.trade to enhance their cashflow and digitise their existing paper-based processes. Companies are using we.trade's digital platform to address challenges such as the late payment of invoices, cyber fraud and where pre-payments are requested by sellers.

Desciption of the blockchain stategies that the company adopted.	A secure digital platform that makes it easier for buyers and sellers to trade globally. we.trade develops and licenses the world's first enterprise-grade blockchain-enabled trade finance platform. Through distributed ledger technology and smart contracts, we.trade makes it easier and more reliable for buyers and sellers to trade globally.

Name of the company	block.co
Website	https://block.co/
Sector	ICT: serves Accounting & Audit, Banking – Financial Services, Education, Government, Maritime & Shipping, Legal – Corporate Services
Country	Cyprus
Description of the issues that the company was facing before the application of blockchain technology (if applicable).	Identified a need in education for secure and self-verifiable documents. A growing market in forged documents and the vulnerability of certification documents in the face of manmade and natural disasters meant a solution was increasingly necessary. It quickly became clear that it was not solely academia that could benefit from the reliable credential authentication that blockchain technology offered.
Desciption of the blockchain stategies that the company adopted.	The ONLY truly decentralized solution to secure PDF documents from fraud without intermediaries. Block.co transforms the way organizations leverage open-source vPDF technology in the issuance, revocation, and validation of self-contained and self-verifiable documents.

3.2 Best practices in the application of blockchain technology in security

Name of the company	iExec
Website	https://iex.ec/
Sector	Business

Country	France
Description of the company's challenges before the application of blockchain technology (if applicable).	iExec strives to develop the best technologies and to invent new protocols that will bring cloud decentralization economy for business. The aim of Blockchain is to resolve business issues related to multi-enterprise interactions and facilitate the creation of new business models. iExec specialize in: Smart Contracts, Record Keeping, Transfer of Value, Digitized Assets, Off-Chain Computing, Confidential Computing & Marketplace Creation.
Description of the blockchain strategies that the company adopted.	Decentralized Marketplace for Cloud Resources and for Scaling blockchain applications with open-source software and protocols. A decentralized network giving applications access to trusted off-chain computation and data. iExec introduces a new paradigm for cloud computing. Cloud resources can now be traded on a global market, just like any other commodity. Instant access to a large capacity of computing power from the provider offering the best rate.

Name of the company	Limechain
Website	https://limechain.tech/
Sector	Supply Chain, Real Estate, Pharma, Healthcare
Country	Bulgaria
Description of the company's challenges before the application of blockchain technology (if applicable).	Blockchain and its application has the potential to impact most problematic industry challenges like supply chain management, asset tracking, claims management, proof of origin, KYC and KYS, eliminating middlemen, reducing costs, eliminating frauds and others.
Description of the blockchain strategies that the company adopted.	Propy takes holistic approach to solving real estate challenges with blockchain-based platform.

Name of the company	Blockchain reactor

Website	https://bcreactor.com/
Sector	Banking, Finance
Country	Serbia and Ireland
Description of the company's challenges before the application of blockchain technology (if applicable).	International payments are slow, costly, and lack transparency. Big companies can negotiate a good deal from their bank, but consumers and SMEs get a bad deal, and there are three reasons why. Also, another issue that reducing e-fraud, enabling safer transactions and getting more people through the online sales pipeline.
Description of the blockchain strategies that the company adopted.	Blockchain reactor makes international payments easier through blockchain. A conglomerate of European banks has come together to find a secure, scalable solution for their clients to pay international bills. As the solution provider, Blockchain Reactor is liasing with these banks to provide a user-friendly and intuitive application for their end-users. Also, Blockchain reactor delivered a complete end-to-end design, development, testing and maintenance of an AI-backed fraud detection system.

Maximum length: 3 best practices

References

Recommendations

-Use Arial 11 fonts for the body text

-Use APA for in-text citation and references

- Make sure that the author/source you have taken information from, is clearly stated in the main body and the references

Resources

https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/583788/EPRS_BRI(2016)583788_EN.pdf

https://ec.europa.eu/growth/access-to-finance/data-surveys/

https://ec.europa.eu/growth/access-to-finance_en

https://ec.europa.eu/growth/access-to-finance/funding-policies/fintech_en

https://www.enisa.europa.eu/news/enisa-news/european-smes-facing-increased-cyber-threats-in-a-changing-digital-landscape

https://www.enisa.europa.eu/publications/blockchain-security

https://www.enisa.europa.eu/publications/challenges-and-opportunities-for-eu-cybersecurity-start-ups

https://www.enisa.europa.eu/publications/privacy-and-security-in-personal-data-clouds

https://www.enisa.europa.eu/publications/challenges-of-security-certification-in-emerging-ict-environments