Intellectual Output 1

Rationalisation Phase

Deliverable: IO1/A1

BCT4SMEs

19.04.2021

Danmar Computers

Authored by: [Konrad Wiśniewski]

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
2	19/04/2021	Danmar Computers	National report		10

(*) 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

In Poland, SMEs constitute the vast majority of enterprises (99.8%), of which more than 2 million are micro-enterprises (employing fewer than 10 workers). Thus, employment rests to a large extent on their shoulders (they are responsible for 68.7% of all people employed in enterprises). The dominant sector of SME in Poland is services (52%) trade (23.5%), industry (13.3%) and construction (10.3%). The significance of SME's for the economy is enormous. However, this sector is facing its own problems. The financial challenges will be presented here (PARP, 2020).

The launch or ongoing operation of enterprises in an industry is, of course, linked to the raising of funds and their allocation. The primary objective of enterprises is naturally to maximise market value. In order to make it easier for SMEs to make a profit, there must be an attractive legal background and transparency and opportunities to raise capital.

Problems of a financial nature can usually be linked to external financing. The main problem is limited access to sources of finance. Both bank loans for SMEs and external investment in them are associated with high risk (Rymarczyk J. 2019).

At the first stage, therefore, their financing often takes place mainly using own resources, thanks to financial support from family and friends. Recently, croundfunding services have become more and more popular. In a nutshell, they consist in raising money from fundraising platforms such as Kickstarter, Experiment or Polish platforms such as Wspieram.to or PolakPotrafi. Croundfunging itself is often associated mainly with start-up activity. Apart from that, there are also methods such as using business angels or venture capital funds.

The first problem faced by Polish SMEs (although this is common problem in big part of Europe) is obtaining funds for setting up and starting a business.

Only 27% of SME companies use external finance, which reflects a reluctance and fear of getting into debt. Unfortunately, innovation is expensive. SMEs are encouraged to use external financing, for example through de minimis guarantees (guarantees to secure the repayment of a working capital or investment loan) offered by BKG (Wierciszewski M, 2021).

Another problem that afflicts Polish SMEs is the lack of timely payments from contractors. It is estimated that almost half of Polish companies are affected by this problem (in pre-pandemic reality). It causes serious problems with financial liquidity, which affect the functioning of the company and its development opportunities (Witkowski R, 2020). The problem of financial liquidity and causing so-called vicious circle of payment backlogs (is also reinforced by the Covid-19 pandemic. Currently (in pandemic reality), the problem with financial liquidity is reported by 7/10 SMEs.

The problem of overdue payments causes a snowball effect. The BIG InfoMonitor research states that micro companies' entrepreneurs, forced by the situation, will not be able to pay their own contractors (due to lack of financial liquidity). The pandemic itself is also a huge (probably the biggest at the moment) financial crisis for the SME sector in Poland. It has frozen the operations of many businesses, necessitated a wage freeze for employees or even caused businesses to collapse (Wiadomości Handlowe, 2020).

Funding from the EU, the European Investment Bank or public money has been a solution to some of the financial problems associated with, for example, paying for the necessary research or implementing innovation for some SMEs. However, this is a drop in the ocean of needs.

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).

Very quickly, the biggest challenge facing SMEs in Poland (and probably the world) became the Covid-19 pandemic. The economic downturn and changes in business management (unexpected downturns, high volatility, lack of liquidity) affected the work of a huge proportion of companies in Poland. Thus, security for many SMEs in Poland has simply taken the form of a form of surviving. The slowdown and downturn also affect the acquisition of finance and willingness to invest.

Many companies are looking for digital solutions that allow their businesses to continue working. Some companies where this has been possible have decided to move to a remote working mode.

Working in a digital environment is inextricably linked to cyber security, and it is cited as one of the biggest threats that SMEs face. Losses resulting from cyberattacks worldwide are estimated at $600 billion (Allianz Risk Barometer, 2019).

As far as cyber-attacks are concerned, they are mainly directed not strictly at the digital architecture of companies, but at their employees. An important statistic here is that (globally) 95% of cybersecurity breaches are due to human error (cybintsolutions.com/cyber-security-facts-stats/). Among the types of

cyberattacks, phishing (79%), Advanced Persistent Threat (77%), ransomware (77%), DDOS attacks (75%) and Bring Your Own Device (74%) are still the most common (CyberDefence24, 2018).

The solution to this problem lies in the continuous education of employees and business owners in the SME sector. To do this in Poland, public institutions organise, for example, courses such as:

- *Cyberbezpieczeństwo w MŚP* (Cyber security in SMEs) organised by PARP (Polish Agency for Enterprise Development). A course for employees and employers who want to take care of their company's cyber security. More information on: https://akademia.parp.gov.pl/course/view.php?id=63

There are also guides being developed (at government level) for SME entrepreneurs on how to take care of cyber security. Examples include:

- *Poradnik dla małych i średnich przedsiębiorstw* (*Guide for small and medium-sized enterprises*) created by the Cyber Security Working Group of the Ministry of Digitalisation in Poland. More information on: https://www.gov.pl/attachment/6dfcd10b-9124-416f-8d09-2f7bb8de0221

You can also get grants to support cyber security in your business through contests such as:

- CyberSecIdent – Cyberbezpieczeństwo i e-Tożsamość (CyberSecIdent - Cyber Security and eIdentity) organised by NCBR (National Centre for Research and Development).

Another example that SMEs currently face in terms of security is the topic of personal data protection and storage.

An even bigger challenge for SMEs when it comes to cyber security is brought by the new fourth industrial revolution. The report "Smart Industry Poland 2019", states that 31.6% of industrial SMEs in Poland have already implemented innovations based on Industry 4.0, and another 38.3% will introduce Industry 4.0 technologies in the next 3 years (BiznesTuba, 2020).

These technologies, while revolutionary, are not without risks when it comes to their implementation and use. The dangers include IoT devices (vulnerable to cyber-attacks) or the risks associated with the use of cloud computing or cloud-based solutions. So it seems that Polish entrepreneurs seem to give these solutions a lot of credence.

According to the latest data, 52% of Polish companies use (or plan to use) cloud computing. They use it, among others, for data archiving and creating backup copies. Additionally, almost half of companies (48%) declare that they trust their cloud computing solutions provider. (Pasławski K, 2020)

With the GDPR policy entering law, SME companies also have new responsibilities. They need to do more work to communicate to customers how they are using their data. Still, one of the most significant risks lurking for SMEs is when customers' personal data is stolen.

Often, the main problem that SMEs have is also outdated cyber security tools and a lack of qualified staff.

Companies believe that a lack of adequate IT staff can be replaced by using cloud computing technology, where data is secured by professional providers (as many as 68% of medium-sized companies move data to the cloud to increase security). However, at the same time, as many as 92% of medium-sized companies worldwide have a director responsible for security (CISCO, 2018).

Moving operations to the cloud (while this practice is legitimate from a security or workforce reduction point of view) is certainly a trend, but there is no denying that organisations must not think they are getting rid of security responsibilities so easily. Businesses should understand the dynamics and ways in which cloud mechanisms work.

3. Transnational Phase

3.1 Best practices in application of blockchain technology in finances

Name of the company	Veem
Website	https://www.veem.com/
Sector	Payment services
Country	USA
Description of the issues that the company was facing before the application of blockchain technology (if applicable).	NA
Desciption of the blockchain stategies that the company adopted.	Veem is a P2P payment platform that uses blockchain technology to execute payments. The company was founded as an alternative to complicated and full of procedures banking processes. Its offer is particularly aimed at small businesses. Transfers are made in 3 ways: - Treasury, - SWIFT, - Blockchain. The assumption, however, is that the customer never knows which way has been used. The company is trying to simplify transfers, especially cross-border transfers.

3.2 Best practices in the application of blockchain technology in security

Name of the company	Cambridge Blockchain
Website	https://www.cambridge-blockchain.com/
Sector	Security
Country	USA

Description of the company's challenges before the application of blockchain technology (if applicable).	NA
Description of the blockchain strategies that the company adopted.	Cambridge Blochchain is a company that was founded in 2015 and specialises in protecting personal data through the use of Blockchain technology. It also supports the exchange of sensitive information, allows to empower digital identity with data privacy rights and seamless data validation. The company thus uses Blockchain technology to support other companies and their customers in the aspect of privacy.

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:

1. PARP. (2020). *Raport o stanie sektora małych i średnich przedsiębiorstw w Polsce*. Retrieved from: https://www.parp.gov.pl/storage/publications/pdf/ROSS-2020_30_06.pdf
2. Ramczyk J. (2019. *Publiczne notowanie akcji jako źródło finansowania małych i średnich przedsiębiorstw*. Retrieved from: http://ssp.amu.edu.pl/wp-content/uploads/2019/03/ssp-2019-1-11.pdf
3. Wierciszewski M. (2021). *Małe i średnie firmy nie korzystają z finansowania zewnętrznego. To problem, bo będą wymagać ogromnych inwestycji*. Retrieved from: https://businessinsider.com.pl/finanse/przedsiebiorstwa-msp-nie-korzystaja-z-kredytow-ostrzega-michal-gajewski-santander/99xwbjr
4. Witkowski R. (2020). *Kryzys w sektorze MŚP. Czy jest się czego obawiać?* Retrieved from: https://witkowski-partnerzy.pl/kryzys-w-sektorze-msp-czy-jest-sie-czego-obawiac/
5. Wiadomości Handlowe. (2020). *Koronawirus a sektor MŚP. 70 proc. firm może utracić płynność finansową*. Retrieved from: https://www.wiadomoscihandlowe.pl/artykul/koronawirus-a-sektor-msp-70-proc-firm-moze-

utracic-plynnosc-finansowa/2

6. Allianz.(2020). *Allianz Risk Barometer. Identifying the major business risks for 2020.* Retrieved from: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020.pdf
7. CyberDefence24. (2018). *Cyberbezpieczeństwo sektora MŚP – wysokie ryzyko i konieczność poprawy standardów.* Retrieved from: https://www.cyberdefence24.pl/cyberbezpieczenstwo-sektora-mspwysokie-ryzyko-i-koniecznosc-poprawy-standardow
8. BiznesTuba. (2020). *4 wyzwania, z którymi muszą się zmierzyć polskie MŚP w 2020 r.* Retrieved from: https://biznestuba.pl/featured/4-wyzwania-z-ktorymi-musza-sie-zmierzyc-polskie-msp-w-2020-r/
9. Pasławski K. (2020). *Raport: MŚP bezpieczne w chmurze*. Retrieved from: https://crn.pl/aktualnosci/raport-msp-bezpieczne-w-chmurze/
10. CISCO. (2018). *Małe, lecz potężne Jak małe i średnie firmy mogą wzmocnić swoją obronę przed zagrożeniami dla bezpieczeństwa?* Retrieved from: https://www.cisco.com/c/dam/global/pl_pl/solutions/small-business/pdf/cisco_2018_smb_revised_092518.pdf?fbclid=IwAR1PzstPFsz07NP2Ub1tDjHdXlYFycMlTwjDNaN1g9kcQwImdbpYXEoRzqk