CONTENTS

Editorial - The Whatness of Digital Accounting: Status Quo and Ways to Move Forward
Othmar Lehner, Susanne Leitner-Hanetseder, Christoph Eisl 1

Digital Accounting: Opportunities, Threats and the Human Factor
Shawnie Kruskopf, Charlotta Lobbas, Hanna Meinander, Kira Söderling 1

Big Data, Cloud Computing and Data Science Applications in Finance and Accounting
Jennifer Huttunen, Jaana Jauhiainen, Laura Lehti and Annina Nylund 16

Current State and Challenges in the Implementation of Robotic Process Automation and Artificial Intelligence in Accounting and Auditing
Max Gotthardt, Dan Koivulaakso, Okyanus Paksoy, Cornelius Saramo 31

Blockchain in the Fields of Finance and Accounting: A Disruptive Technology or an Overhyped Phenomenon?
Aino Nordgren, Ellen Weckström 47

FinTechs: Their Value Promises and Disruptive Potential
Sara Laahanen, Eemil Yrjänä 59

RegTech- A Necessary Tool to Keep up with Compliance and Regulatory Changes?
Ellinor Johansson, Konsta Sutinen, Julius Lassila, Valter Lang 71

Prevention and Detection for Risk and Fraud in the Digital Age – The Current Situation
Hanna Donning, Mathias Eriksson 86

Cybercrime in a Business World: Behavioral Perspectives
Böckelman Petter, Björkman Henrik 98
EDITORIAL

THE WHATNESS OF DIGITAL ACCOUNTING: STATUS QUO AND WAYS TO MOVE FORWARD

OTHMAR LEHNER¹, SUSANNE LEITNER-HANETSEDER², CHRISTOPH EISL²

¹ University of Applied Sciences Upper Austria and Hanken School of Economics, Helsinki, Finland
² University of Applied Sciences Upper Austria

Introduction

Digital Accounting has found its way into the everyday language used by accounting practitioners, with the Big 4 auditing companies pouring massive resources into the digitalisation of accounting processes in order to create an early-mover business advantage.

In research, digital accounting is used as summarizing term for a variety of research endeavours into the digitalisation and automatization of accounting processes based on emerging technologies (Quattrone, 2016). The existing literature deals for example with the role of digital technology in accounting and reporting (Güney, 2014; Ghasemi et al., 2011; Taipaleenmäki and Ikäheimo, 2013), the integration of the competences required in the accounting curricula (Sledgianowski et al., 2017; Janvrin and Weidenmier Watson, 2017) and the detection of fraud (Pearson and Singleton, 2008).

Already by its name, a research field of digital accounting will have to be interdisciplinary, as it includes the disciplines digital (information) technology and accounting (Lehner and Martikainen, 2019). However, due to the broadness of accounting itself, comprising financial as well as management accounting (Taipaleenmäki and Ikäheimo, 2013), insights and theories from these subfields as well as from auditing, innovation and engineering, business law, organizational theory and ethics as well as accounting education amongst others, will provide further fruitful avenues to enrich the field of digital accounting.

While this variety of related fields and theories and the related insights from particular angles certainly provides value and drives the field forward, a common, holistic understanding of the whatness of the field of digital accounting and a related research agenda that would allow to join forces and interlink the various perspectives is missing so far.

In the past, accounting information systems (AIS) have changed the way that data is collected and prepared for the decision-making by stakeholders (Neely and Cook, 2011). The further development of such systems, for example through partly-autonomous robots for process automatization, through advances in creating fully digital workflows and finally also innovative algorithms based on data-science certainly form a major part of how digital accounting needs to be understood in current research. However, most scholars would agree that digital accounting in the future will certainly be more than just collecting and processing data, as advances in artificial intelligence (AI) research already predict some sort of multi-functional, cognitive capabilities and the ability to make decisions given complex scenarios. Therefore, digital transformation in accounting needs to be seen as an ongoing process that ultimately may lead to a fully autonomous accounting system (FAAS), which will be defined later in this paper. Such a fully autonomous accounting system would include (AI) based cognition and high-level decision making as special and new areas within the wider field of accounting. Of course, such developments are necessarily embedded within a larger societal
THE WHATNESS OF DIGITAL ACCOUNTING: STATUS QUO AND WAYS TO MOVE FORWARD

change process induced amongst by a variety of technological advancements (Vial, 2019) and societal movements (Colignon and Covaleski, 1991; Englund et al., 2011; Hopwood, 1983).

With this special issue, we thus like to invite and motivate the community of scholars interested in digital accounting to collaborate, to take in the various field-specific perspectives and to finally holistically map and delineate the field of digital accounting. For this, we propose an early framework and a research agenda that may unite and guide researchers towards a holistic understanding of the field.

In addition, and for this special issue we have asked grad-students and researchers from the department of accounting at the Hanken School of Economics, Helsinki to provide their research papers and perspectives on the “whatness” of Digital Accounting.

Utopian Spotlights of a Fully Autonomous Accounting

Here we provide a selection of five spotlights on different aspects of digital accounting to illustrate the insights we have gained so far from an ongoing delphi study on this topic.

Spotlight 1: Extending the customer base

A new customer X in a B2B scenario sends an inquiry for a certain quantity of our top-selling product A. The AI deploys a robot to crawl all external data sources including company-register, company web-site, social-media, banks and triangulates the findings with the response from the credit-agency. The credit-worthiness has been confirmed and starts a price calculation that includes current sales and production-capacities as well as the previously determined credit-risk. The price is confirmed by X and we receive a full order. Immediately, a robot transfers all data from the order as well as the previously retrieved additional data from the crawler into a newly generated customer item within the virtual data store and logs the order into the ERP subsystem.

Spotlight 2: Ad-hoc reporting and decision support

Our marketing manager receives information from a media partner that a top athlete and multiple medal winner would be available for a long-term sponsorship contract. The marketing manager sends an ad hoc request to the FAAS via voice recognition to get decision support. The FAAS assesses the effects of sponsoring on the image values and price willingness of the customers, updates the sales forecast, checks the available advertising budget or suggests budget reallocations and, taking into account a risk assessment, makes a final recommendation on the range of the rationally justifiable sponsoring amount.

Spotlight 3: FAAS-warning message

Early in the morning the production manager arrives at the office and asks the FAAS to provide an internal status report and update in natural language by asking “What’s news?”. The FAAS scans all relevant real-time reports and data trends and compiles the top news. The FAAS places the focus on a warning message that requires immediate action: “Current machine sensor data indicate urgent maintenance work in a production plant”. In the background, the system has already checked possible production shifts to another flexible manufacturing cell as well as outsourcing options and has determined the cost-optimal time for the upcoming maintenance work, taking into account adherence to delivery dates and maintaining a high level of customer satisfaction. The gathered data is presented as a working scenario and potential solution to the manager. After her confirmation, the FAAS automatically initiates the execution of the plan. Based on the severity of this maintenance, the FAAS classifies it as a major inspection
according to current GAAP (generally accepted accounting principles), recalculates the real-time forecasts and updates the top-management reports.

**Spotlight 4: Valuation of a Leasing Contract using timely WACC**

Our FAAS applies AI for the extraction of lease data attributed from the contracts and for the following classification, valuation and presentation of leasing contracts in the financial reports. In addition to the classification of the leasing contract, several internal as well as external information sources are used by the FAAS to calculate the average weighted capital costs (WACC) for each contract based on the commencing dates and maturity. For this, yield rates based on the maturity as well as current risk-based equity costs are calculated. Because of differences between the various applicable, local and international accounting and taxation standards, the FAAS acts accordingly concerning the classification, recognition, measurement and reporting. The data and underlying set of applied rules is automatically transferred to the contracted auditing firm.

**Spotlight 5: Reflecting Strategic Decisions in the Accounting System: The Case of End-of-Life of a major product line**

Product line B has seen the best of its days. With a number of product variations and related, then well-crafted cost-centres, line B was among the core lines of the company for a long time. Due to innovation and inevitable changes in the markets, the board has decided to cease line B three years ago and the sales and production transition is now complete. In an attempt to reflect these changes now in the accounting system and to clear it from any remaining clutter, the FAAS has now been tasked to take care of the necessary steps. The AI first takes into account respective regulations for financial accounting and also considers the change in demand for internal information on all levels. All data and features that need to be kept for external regulatory compliance are archived and marked with a due date for deletion, and the internal accounting structure is adapted by marking the cost-centres as obsolete, deleting all related items for possible new entries in the ERP system, adjusting the calculations for the various key performance indicators (KPIs), and by remodelling and optimising the management dashboards to make better use of the now empty space. It then provides an update to the CFO including how the sales volumes of the discontinued line B have already been successfully transferred to the new lines by the individual customers and creates a list of recommendations for the sales team which customers might need to be better addressed as their current volumes indicate that they have replaced B by alternative products from outside of our company.

**Three Maturity Levels of Digital Accounting**

Based on our preliminary literature review of the state of the art, see for example (Taipaleenmäki and Ikäheimo, 2013; Sledgianowski et al., 2017; Kokina and Davenport, 2017; Janvrin and Weidenmier Watson, 2017; Güney, 2014; Davenport and Kirby, 2016; Belfo and Trigo, 2013; Crookes and Conway, 2018; He, 2018; Huang et al., 2018; Robson and Bottausci, 2018), and the derived utopian scenario we now propose an early framework (see figure 1) of digital accounting and subsequently outline its main defining characteristics.
THE WHATNESS OF DIGITAL ACCOUNTING: STATUS QUO AND WAYS TO MOVE FORWARD

![Figure 1 Three maturity levels of digital accounting, source: Lehner, Leitner-Hanetseder and Eisl (2019)](image)

**Level 0 (Software Assisted Accounting):** In this basic level accountants are assisted in their traditional roles by standard functions of silo-based software applications. Level 0 is characterised by the extensive use of often spreadsheet-based, idiosyncratic software and follows predominately paper-based filing and workflows.

**Level 1 (Digitally Assisted Accounting):** Within this first maturity level of a truly digital accounting, accountants focus on data preparation, company-wide planning and reporting and are digitally assisted by enhanced and in many cases cloud-based accounting information systems, with connections to all major sub-systems (ERP etc.) using semi-automatic interfaces for data translation and transfer. Level 1 is characterised by a mixture of manual and automated document processing, the use of optical character recognition (OCR) for standardized documents as well as an electronic filing system. Repetitive, standardized processes on a large volume of documents are carried out by (often offshore) service-centres using a mixture of cheap manual labour and simple automatization approaches. The use of software robots is in its pilot phase. Planning, budgeting and forecasting are performed by using a highly integrated software solution with automated management workflows.

**Level 2 (Semi-autonomous Accounting):** Within the second maturity level of digital accounting, accountants focus on the interpretation of system-generated information and take on a stronger internal advisory-role that is supported by a fully integrated AIS for financial as well as management accounting. This AIS is characterized by high levels of automatization and has advanced data science algorithms implemented. Within Level 2, automated document processing within a fully automated workflow is employed, specialised software robots are used in almost all areas, digital reporting is fully XBLR-based and overall reporting-cycles have been tremendously shortened. The AIS uses In-Memory-database technologies and Blockchain-based distributed ledgers and is connected with social media platforms for financial disclosures and non-financial insights. Process-mining controls and documents all accounting processes. Accountants include external and unstructured data in their enhanced Business Intelligence (BI) solutions and use data science tools to tackle big data analytics, predictive analytics and fraud detection. Early stage AI-powered applications provide human decision makers with high-quality based for decision-making. Managers can retrieve ad-hoc information via Chat bots and use cutting-edge technologies-based devices and digital boardrooms for their meetings and video conferences.
Level 3 (Fully Autonomous Accounting): Maturity level three of the digital transformation focuses on artificial intelligence in an autonomous accounting system, with self-aware cognition and (albeit) limited decision-power. A multi-functional, deep-learning powered AI provides the automated application and adaption of accounting and tax-regulations, implements optimization measures, provides target-audience specific reporting and forecasting in real time, runs simulations and scenarios and issues regular management warnings on major key performance indicators with detailed analyses and recommendations. The AI also controls the deployment of the specialised robots according to the necessary tasks at hand as directed by management. It uses a deeply-integrated virtual data warehouse that includes internal and external data and is fully managed concerning data protection, security and availability. Managers communicate with the system via natural language processing from everywhere. The system improves its own performance by deep learning mechanisms. At this stage the accounting information system (AIS) becomes a fully autonomous accounting system (FAAS). Based on our analysis of the future, utopian scenario, we define such an FAAS as follows:

“A FAAS is a firm-wide, fully autonomous, self-aware and self-improving accounting system. The centre of an FAAS is a state-based, multi-functional, deep-learning network as artificial intelligence (AI) that is able to holistically simulate and potentially outpace human-cognition and decision-making processes. This AI manages structured and unstructured data and regulations from various sources and delivers timely and apt information to the right audience in the right format.”

Discussing a Research Agenda in 5 Items

We finally combine the insights gained from the literature review with the early empirical findings from the Delphi study into a research agenda to invite and motivate the community of scholars to collaborate and interlink the various field-specific perspectives with the ultimate aim to holistically map and delineate the field of digital accounting.

This research agenda may help to better understand the digital transformation towards a fully autonomous accounting and may also assist to make this very transformation happen by providing empirical data-based guidance to practitioners as well as policymakers. The outcome of our collective research should also inform society on the broader opportunities and threats stemming from a fully autonomous accounting and help them form an educated opinion on the implied societal changes with its ethical challenges.

The agenda is structured into the following five perspectives as follows in figure 2.

Figure 2 Perspectives on Research in Digital Accounting, source: authors
1. Organisational transformation

Many scholars would agree that any transformation of such gravity in accounting most likely goes together with a substantial organisational transformation. Depending on the chosen theoretical framework however, causations can be assumed in either, or even neither direction between these two. Thus, the interplay between the nucleus of accounting transformation and the immediate organisational context as well as the larger societal context will be one of the important issues from an organisational science perspective.

Insights from empirical studies framed for example in a neo-institutional theoretical setting that accepts the separation of human actors and structure (such as the norms and traditions of the accounting profession) and takes a certain drive for standardisation and isomorphic adaption for granted, will certainly provide valuable starting points. Giddens structuration theory (Englund and Gerdin, 2014) with its notion of transcending the structure-agent separation towards a system of accountability with situated practises (Conrad, 2014), Latour’s actor-network theory (ANT) that adds non-humans as actors (Robson and Bottausci, 2018; Latour, 2005) and creates fluid accounting objects that are translated into a system, or configuration theory (and earlier contingency theory) with its focus on the organisational gestalt or habitus (Bourdieu and Nice, 1977) being shaped by a complex contextual interplay (Otley and Berry, 1980), may be other worthwhile perspectives to understand and explain the organisational changes we expect to see in the coming years.

What all these theoretical approaches have in common is that they lean towards a pragmatic worldview, which is not limited by the often artificially-conjured dichotomy of a realist versus constructivist ontology in the social sciences and thus allows researchers to embrace a variety of epistemological approaches with a range of suitable research designs. This may also be particularly necessary because the sheer dimensions in terms of size and speed (Crookes and Conway, 2018), and especially the interconnectedness between the levels on which change is about to happen will potentially transcend current literature on change in organisations - while at the same time we expect much of the current theory of change to remain at least partially valid in this new, rapidly changing context. Following Edmondson and McManus (2007), such an intermediate state of theory needs to be approached by mixed-methods designs, combining inductive and deductive reasoning.

2. Individual: workers, managers, shareholders and other stakeholders

A strong focus on the human and societal factor in the transformation towards a fully autonomous accounting seems timely and apt. On the one hand, it is certainly pressing from a practice point of view, as the technological advancements will inevitably have a strong impact on the existing roles, duties and corresponding skills of workers, managers and recipients of reports in the accounting profession (Neely and Cook, 2011), as well as on stakeholders in general.

For the employees in the field, we need to understand the new job-roles and matching qualifications that are necessary in order to not only persist in this new area but also to help deal with the aberrations that any change process will inevitably bring with, with the ultimate goal to further develop the accounting profession. Questions in this area will be about the career-prospects, related skills and how our education systems can deal with the demand, but also about the necessary tools to support human cognition given a highly abstract and aggregated level of information (such as visualisations and interactions); about the psychological factors when it comes to change management and the necessity to adapt, and finally to questions of power and control. In this, Foucauldian perspectives on what constitutes power from a critical discourse perspective may help to identify problematic developments and allow to raise the right questions in society. The meta theories of capabilities or the resource-based view (RBV) may provide other suitable and less critical approaches to understand and
guide the interplay between organisational leadership and the role of humans in an autonomous accounting world. From a strategic management perspective these theories may help us understand how a competitive advantage can be created and maintained given such rapid organisational transformations.

The decisive change for individuals in this can be seen as a FAAS will not only provide the decision-relevant information but already propose the decision itself based on this very information. Following these lines of thought; how to ensure a bias-free cognition, and who ultimately controls the firm and its resources for what purpose will be amongst the most pressing issues in this. Thus, from the perspective of the individuals having to deal with the output and decision making of a fully autonomous accounting system several questions will arise. Such questions will not only include the role of trust into the decisions of such systems but also comprise more collective fears concerning how sustainable a functionalist, AI-based assessment without human values can be.

3. Regulation: Standards and Transparency

From a regulatory side, the need for transparency of the internal processes and internal decision-making criteria of the AI to comply for example to the GDPA criteria is still not sufficiently solved and it may take a while to reach a satisfactory level. In the meantime, accounting and information systems researchers may need to look into which levels of transparency for which applications are really necessary. There will certainly be a difference from a regulatory requirements perspective, internal advisory systems based on AI-derived cost-predictions and external compliance-reports based on true big data when it comes to traceability, confirmability and finally transparency. To solve the problem of transparency and accountability of an FAAS, researchers need to first fully understand how deep learning systems simulate cognition, especially when it comes to multi-functional networks. The learning process based on feedback loops, which leads for example to the known problems of overfitting and easily introduces a potential sample-bias may provide more hurdles to take before a truly transparent, traceable and accountable autonomous accounting can be possible.

Besides the necessary regulatory changes, for example concerning labour-rights and standards, taxation and data protection, other interesting insights may include the necessity to redefine the role of auditors and authorities to ensure compliance with these changes.

Other worthwhile endeavours may be to define how accounting standards need to adapt to better reflect the quality and worth of the collected data and the derived intelligence of such an FAAS as intangible assets.

Finally, research needs to carefully monitor and guide regulatory communication that is not only comprehensible by humans but can be processed by accounting systems, such as the already existing IFRS or FASB codifications.

4. Innovation

Research in this area needs to look at IT-architectures and infrastructures, and how these technological artefacts in term influence the practice and control of an FAAS. The above described necessity to include external data of various sources and with various formats into a vast, virtual data repository will bring with many questions. What is more, a variable-efficient problem-modelling that is informed by information-theoretical concerns of which data is needed and what may be available in abundance would catapult current solutions towards a much higher practical usability. In this, accounting and information-science scholars would need to work together with data-scientists to identify both, theoretical frameworks as well as corresponding algorithmic solutions.
In this perspective, we identified the most salient questions as:

1. How should the ideal infrastructure be laid out depending on the tasks and context - including considerations on cloud versus internal storage and computing power, speed, scalability and flexibility, but also most importantly concerning availability?
2. How to algorithmically define and enforce data rights and ensure protection and compliance to data-regulations. What may the role of public or private Blockchains be in this?
3. How the FAAS can base its calculations and decisions on just the relevant information and by this use its resources efficiently - for example through clever feature selection and by avoiding overly complex models. In other words, how can the human domain know-how and related heuristics be translated into an FAAS and how can algorithms such as ridge or L2 regressions help avoid overfitting to enhance external validity?
4. How standardization might help but also diminish the (open) data exchange depending on the various sources in various contexts.
5. What is the meaning of Artificial Intelligence in an FAAS and where may be its limits and the potentially ongoing necessity for a human-interaction?
6. Following the previous question, how can the inner workings of a deep learning network as the basis of an FAAS be made transparent and how can the system create targeted communication (including visualisation) of complex data structured on an aggregated level that still allows to validate the outcome by interaction?
7. Related to this, how can an isomorphic bias, based on hindsight learning from the machine-based decisions (leaving out alternatives) be avoided and what security measures need to be in place to control an FAAS.
8. How to ensure a practical decision making when the existing data does not sufficiently specify the problem at hand.

5. Ethical Implications

Finally, but potentially most important, research needs to bring in the different voices from society about how ethical boundaries need to be in place when it comes to fully autonomous decision making of AI powered accounting systems. The role of cultural standards, and potentially the role of the firm itself needs to be revisited. We already see for example in entrepreneurship research with its recent discussions on hybrid business-models, that environmental, social as well as commercial factors need to be taken into account when it comes to strategic decisions. Such factors may be underrepresented in any purely data-based FAAS, as the more unstructured and less-quantifiable non-financial information may be harder to process and much more scarce compared to “hard” and easy to digest financial information. Critical literature on sustainability already questions the rationality behind any ESG (environmental, social and governance) guided decision-making and identifies mostly reputation risks and legitimacy as rational motivations. Reading the current streams of literature in digital accounting it becomes clear that any ethical considerations need to be enforced by rules and regulations and cannot be based any more on the personal, human values of managers. The AI answers to how a data-derived strategy shall be put into place needs to be carefully monitored and a societally accepted way of integrating the people, planet and profit thoughts into the mere functionalist approaches of non-human actors has to be found in a process that includes more than industry and policy-makers.

Any ethical considerations, as far as such considerations are even possible on a meta-level without a cultural context will need to be inserted as rules and the impact of potential sample-bias in machine learning has to be looked at from various, critical angles. However, that’s not to say that such AI data-derived decision making cannot have its merits, as nepotism and other
irrational behaviour of managers would be potentially reduced. Therefore, agency theory may well interplay with philosophical and (critical) sociological approaches to build a solid foundation of what the role of ethics should be in FAAS.

**Conclusion**

In our understanding and based on the existing literature digital accounting needs to be seen as an interdisciplinary research field. Therefore, based on literature from various disciplines, scholars as well as practitioners from various disciplines are invited to collaborate on future scenarios of a fully autonomous accounting.

Based on the literature review and early empirical insights, we propose an early maturity-level framework and derive a corresponding research agenda. This maturity level framework starts from a digitally assisted accounting focusing on providing support for data preparation, planning and reporting and ends in a fully autonomous accounting system focusing on artificial intelligence as accountant and advisor with advanced cognitive abilities. In order to reach the final stage of a fully autonomous accounting system, an organizational and social change process is necessary in addition to the necessary technological advances.

The research agenda for the field of digital accounting finally comprises five perspectives, namely organisation, individual, regulation, innovation and ethics, and potential theories within each of these perspectives are proposed.

We sincerely hope you enjoy this special issue of the ACRN Oxford Journal of Finance and Risk Perspectives on Digital Accounting, and are looking forward to your replies and comments, and to further research papers on this fascinating topic.

We would also like to extend a special thank you to Prof Minna Martikainen from the Hanken School of Economics, Helsinki for her fantastic support and co-editorship and to all the authors in this special issue from Hanken who dedicated a lot of time and resources to come up with insights and research papers from a great variety of perspectives.
References

Otley DT and Berry AJ. (1980) Control, organisation and accounting. Accounting, Organizations and Society 5: 231-244.
Abstract: This paper gives an overview of the current and future technologies impacting accounting and auditing fields. The aim is to present the technological disruptions shaping these fields and also look at how they might influence future jobs and required skills. Starting with a historical background check on how Industry 4.0 emerged, we survey four main areas of the topic: 1) current developments supported with real-life cases, 2) a literature review of on-going research, 3) possible future job descriptions, and 4) required skills and how to acquire them.

Keywords: Digitalisation; Accounting; Auditing; Industry 4.0; Skills

Introduction

In this paper we look at how current and future technologies are impacting the fields of accounting and audit which are thus shaping the future of new job descriptions and required skills in these fields. These fields are moving full force into the digital age, where many predict that in five to ten years humans will become obsolete in many areas in accounting and audit.

However, though many tasks will be automated, humans will still be able to create value for clients and for the way the business world is developing through continuous learning of new skills. Here we will discuss how humans can grow alongside advancing technologies to keep up with the demand that will be present in a few short years. To do this we will first introduce the fourth industrial revolution and its advancements. Next, we will review how this revolution is changing the worlds of accounting and audit, presenting which technologies and advances are relevant to the fields and are creating the largest impacts. In addition, we will review on-going research from (e.g. Zhang, Dai & Vasarhelyi, 2018, Pan & Seow, 2016, and others) and how it is affecting the fields, jobs, and the skills required to adapt. Once we set up this potential future, we will go through additional demands that will be placed on employees of the fields.

Next, a detailed list of what the most valuable skills going into the future will be analyzed. We will then discuss an overview of the critiques that are forming due to the rapid changes occurring in the fields and employment opportunities. Lastly, we will predict how the future will evolve in our view and from the view of on-going research.

While there are many predictions of how the future will be, many reports do not focus on what will be required of employees going forward to add value to clients. This report gives an in-depth analysis of new job descriptions and which skills will be potentially needed to survive in digital future and thus allowing for further research on which of these skills are the most useful going forward.
Theoretical frames

The revolution in which we are now has many names, such as the 4th industrial revolution, Industry 4.0 (which we will use in our paper), the digital revolution and the artificial intelligence revolution (Hoffman, 2017). The McKinsey Global institute estimates that “It’s happening 10 times faster and at 300 times the scale than the Industrial Revolution in the early 19th century” (Hoffman, 2017). In order to understand the potential future in accounting and auditing, we first must understand the revolution we are in now. In this section we will discuss what Industry 4.0 is, how it will change the future and how it will specifically change accounting and audit.

The fourth industrial revolution is a continuation of the third revolution, in which we started to use computers and automation to improve upon it with autonomous and smart systems driven by data and machine learning. In the current revolution and when Industry 4.0 evolves further, computers will be interconnected and communicate to make decisions without humans. The combination of Internet of Things, Internet of Systems and cyber-physical systems, makes Industry 4.0 possible. The power in the Industry 4.0 lays in the network of smart machines that are interconnected and can create, analyse and share information. (Marr, 2018a) In other words, Industry 4.0 is about the ways smart, connected technology will be embedded in companies, assets and people, and is marked by the development of analytics, robotics, cognitive technologies, artificial intelligence, quantum computing, the Internet of things amongst others. One of the most important parts of these new technologies is that they will change the way data and information is used and how this will allow companies to become more efficient. (Cotteleer & Sniderman, 2017) Overall, Industry 4.0 is changing every aspect of the business world and has become an inevitable topic of discussion, next we move on to the specifics that are changing the fields of accounting and audit.

The accounting and audit professions are evolving, and everyone is talking about the digital revolution. The revolution is growing fast and there are still many aspects that are unclear about the future. These changes will lead to the disappearance of many jobs, but at the same time it will allow for many new opportunities not only for the newly graduated, but also for those who are eager to develop new skills. Information technology is nowadays part of every business and companies that can’t keep up with the new technologies will slowly fade away. Just like every other field in business, accounting and audit will benefit immensely when using digitalization to organize, process and evaluate financial data which will improve productivity and save on both cost and time. These changes will affect essentially every business as accounting is a crucial and core part of the success of a company and we have seen how failures in this area have wiped out large and bustling companies such as Enron and WorldCom. (Edupristine, 2018). For those legally required to participate in audits, these improving technologies will also affect them and help them to uncover fraud, inconsistences, and other faults that could topple a business. A further subset of these companies that will be affected immensely are the accounting firms, from the top four to the smallest and everything company in-between.

As the digital revolution is shaping the field of accounting and auditing it means that this topic is relevant for both current accounting and auditing professionals as well as for students and professors at universities as they are the ones that have the knowledge required to develop these sophisticated accounting information systems. We already know that many of the current accounting processes are being done by machines such as expense management, accounts receivable and payable processing, artificial intelligence powered invoice management and supplier onboarding. Thus, we can predict enormous changes in jobs in the future, but the role of bookkeepers and auditors will remain important. One of the most important discussion currently open is how there are a lot of tasks that machines can perform much better and faster than humans such as structured problem solving and routine tasks but then again, they don’t have the skills of improvising and using imagination (Hoffman, 2017). We will further discuss
how humans can adapt to stay competitive and add value in the fields mentioned in subsequent sections. To sum up, these current advancements are making it necessary for businesses, accounting and audit professionals, upcoming graduates, and universities, to adapt to technology and figure out the best way to interact with it going forward.

Current developments

Businesses have gone through three different waves of transformation up to present day. From the first wave of standardized processes of automobiles on assembly lines to the second wave of automated processes including computers, information technology, databases and software. Built on these two, the third wave includes adaptive processes. This wave initiates new ways of doing business. Based on real-time data these processes are more adaptive and flexible and give the possibility to reimagine innovative and more individualized products and services. (Daugherty & Wilson, 2018) According to Charles Hoffman (2017) There are three technological innovations that are primarily driving the changes of the current accounting practices, methods and procedures and which can noticeably modernize and improve accounting and auditing. These are XBLR-based structured digital financial reporting, knowledge-based systems and other application of artificial intelligence and blockchain-based distributed ledgers.

XBLR-based structured digital financial reporting stands for eXtensible Business Reporting Language, which is a global framework for exchanging business information and it is freely available for everyone. In the past, financial reports were readable only by humans, but in the future, they will be both human – and machine-readable (Hoffman, 2017). The second innovative driver in the field are knowledge-based systems and other applications of artificial intelligence (Hoffman, 2017). Robotics and artificial intelligence are at the center of the technological disruption. Robotic Process Automation, RPA, is about automating structured and rule-based tasks. RPA is not intelligent in the sense that it cannot adjust to changes or make complicated decisions (Zhang, 2018). In the area of RPA, accounting firms and RPA companies are collaborating. All big four accounting firms, Accenture, Capgemini, and others are working with Robotic Process Automation companies such as UiPath and Blue Prism (Tadros, 2016). AI research has reached a new level of development and understanding of machine intelligence. The current approach has focused on letting the system learn rules by itself from observations collected from real-life data, instead of teaching the system a wide range of rules. (ICAEW, 2018) Going forward, AI will reduce costs and time for accountants and auditors as it works in the background enhancing already existing cloud computing and increasing productivity (G2 Crowd, 2018).

The third technological innovation driving the fields and affecting future jobs is blockchain-based distributed ledgers. Blockchain is a shared database with a series of data that is time-stamped and immutable so no one can tamper with the data. The blockchain is a decentralized system – it has no master. The records are tied together into blocks and then they are added to the chain one by one. No transaction costs arise when using Blockchain, because no intermediaries are needed. It is an easy way to pass information from one person to another in a completely automated way. The blockchain is hosted by millions of computers at the same time, so the data is open for anyone on internet (Blockgeeks, 2019). Although it is at an early stage, Blockchain is changing the accounting and audit world. Companies are already testing the new technology. New opportunities and challenges for professionals in accounting and auditing will arise due to the blockchain. Blockchain is best known as the technology behind cryptocurrencies, such as Bitcoin, but is has many other potential uses and benefits in addition to that (Half, 2018). Examples on potential uses are; property records, banking, supply chain auditing, Anti-money laundering (AML), Know your customer (KYC), stock trading, smart
contracts and crowd funding (Blockgeeks, 2019). The main advantages of Blockchain in accounting and auditing is that it enables more efficient asset and data transfers, privacy and security will increase, time-consuming tasks can be removed, and financial records will become more comprehensive and precise. Blockchain may also open up new job tasks for auditors, such as, cyber auditing (Half, 2018).

As it can be seen around us and as we have talked about in this paper, the trend is that data and operational processes are more and more transferred into digital form. Unfortunately, new technology and processes bring new forms of corruption and fraud. Cybersecurity is therefore an inevitable part of strategy planning right now and in the future. Companies have to invest and manage these new risks of cybercrimes. (Gupta, 2015) Accounting firms are doing their best to protect their businesses. A rapidly evolving feature of AI is anomaly detection. Accounting firms uses this application of machine learning to prevent cybercrimes and to identify outliers in the data, such as in cases of identification of false invoices for their clients. For example, Ernst & Young’s (EY) anomaly detection program has an accuracy of 97 % and is a valuable tool in everyday work for accountants and auditors (Zhou, 2017) in order to protect both the assets, reputation and staff of the accounting firms, but also their customers (Gupta, 2015).

According to Daugherty & Wilson (2018) it is a misconception to think that machines will gradually replace humans in labour markets. They think the man-versus-machine view is old-fashioned and short-sighted. Instead we should start to think about it as a collaboration between humans and machines. They emphasize that even though technology will probably replace certain jobs and certain functions, the main power of the technology is in complementing human capabilities. Many leading firms have begun exploiting the potentials of AI in their businesses and have started to realize that organic teams including humans partnering with machines are the future. Humans and machines, each have their own strengths. The areas where each party are most capable and in which areas, they complement each other are represented in table 1. Many of these human-only activities and skills will be explained later in the article. The important part of the table is to see and acknowledge the “missing middle”, as Daugherty & Wilson (2018) explains it, where humans and machines complete each other. This middle is often forgotten, when we compare human and machine activities as excluding each other.

Table 1: Human-Machine teamwork (modified Daugherty & Wilson, 2018, p. 5 and Marr, 2018b)

Apart from these three innovative drivers in the field, there are expanding industries that will now and also in the future affect accounting and auditing. Two of these new industries are FinTech and RegTech. FinTech stands for Financial technology and it describes the businesses that use modern technology and software to provide financial services. Fintech companies are
competing with the banking sector. They provide different digital solutions in daily banking, such as robo-advisors and different apps. This enables, for example, faster and easier transactions without intermediaries. (FinTech Weekly, 2019) RegTech, Regulation Technology, addresses regulatory challenges by simplifying the increasing legal requirements within the financial industry. (W. Arner et al. 2017) RegTech companies use, for example, AI and machine learning to come up with new regulatory solutions. (ComplyAdvantage, 2018) These new technological approaches save accountants’ and auditors’ time in mundane tasks in areas of compliance and managing money (G2 Crowd, 2018). This has and will result in changes in job tasks and skills needed by employees.

**Current real-life cases**

Many of the top players in accounting and auditing have been exploiting and investing into different innovative areas to stay relevant in the field. As it was presented in the previous part, the main buzzwords disrupting the nature of accounting and auditing work now and in the near future are robotic process automation, artificial intelligence, blockchain, human-machine teamwork and new security issues. While many of these technologies are still in their infancies, they are already creating a lot of value for the investors. In addition, many of these technologies are allowing companies, accountants, and auditors to take on more global clients without as many limitations as before. In this section we look at some current examples of development affecting the work of the future accountant and auditor.

**Case: PwC Digital Accelerator Program**

In order to train their employees and keep them on top of the development, PwC (PricewaterhouseCoopers) launched a 2-year Digital Accelerator Program for 1,000 employees to boost their digital skills in 2018. The aim with the Digital Accelerator program is to train the employees in-house in three areas; data analytics, automation and AI, including machine learning. The program includes courses from data cleansing, blockchain, cybersecurity to drones and 3D printing. Instead of doing their usual work, the participants in the program get “digital-heavy” projects, client work to solve and attend weekly classes. The Digital talent leader and the head of the Digital Accelerator program, Sarah McEnaney says that the aim with the program is that the employees get more technology skills so that PwC can remain competitive in the market. The program is also an attempt to reduce costs for clients. The costs can be reduced thanks to the new technology that enables job tasks to be done faster. PwC did not reveal how much they are spending on the project, but did tell that it was one of the largest investment areas in 2018 (Liffreing, 2018).

**Case: Deloitte US Blockchain Lab**

Deloitte has dedicated a whole division to blockchain research and development. The US Blockchain lab is located in New York and is one of the many blockchain labs that Deloitte has around the world. Deloitte’s blockchain community consists of over 800 professionals in 20 countries. The aim with the lab is to support clients in utilizing the capabilities and opportunities that the blockchain technology can offer. The lab is a place for education, ideas, development, strategy and prototyping. The team in US consist of more than 20 committed designers and developers in Blockchain. The US Blockchain team works together with specialist from other countries and with more than 20 technology companies. The lab has already developed over 30 prototypes that are Blockchain-related, covering a variety area of applications, such as trade finance, cross-border payments, digital identity, fraud detection, reward programs and a lot has
also been done in the investment management and insurance sectors. As an example of a blockchain solution that can be of great benefit in the accounting and audit field, is the fraud detection solution, that is blockchain and machine learning based. This solution facilitates fraud detection in real-time. If anomalies are detected in the transactions, they are captured and get a risk score created based on the matching transaction IDs in the blockchain (Deloitte, 2019).

Case: The EY Blockchain Analyzer

EY has started to use blockchain technology in their audit process. It was in April 2018 that EY announced the pilot of the EY Blockchain Analyzer, which is a technology that is created to help auditors to collect a company’s transaction data from various blockchain ledgers. When the data is collected, auditors can examine the data, analyse the transactions and identify outliers. The technology makes it possible to do a thorough analysis of the business transactions in cryptocurrency. The technology is specifically created to support auditors when they audit companies that use cryptocurrencies. Cryptocurrencies such as BitCoin, Ether, LiteCoin, BitCoin cash and a few other crypto-assets are being tested with this technology. When the Blockchain analyzer has been developed, they have used experience acquired when working with clients around the world, with technologies such as wallet providers, investment funds, exchange platforms among others. The development of this new technology is an answer to the customer’s changing needs and to improve the audit process as a whole. As the EY Global Assurance Innovation leader, Jeanne Boillet, says: “As digital technology continues to advance, we are focused on developing innovative approaches to the audit process and providing confidence and trust to the capital markets. As companies are also focusing on how they embed technologies like blockchain into their financial processes, we are innovating the audit to meet their evolving needs and those of investors” (Thomas, 2018).

Case: PwC and ABBYY

PwC has started to automate their financial documentation processing in cooperation with ABBYY. Auditing requires dealing with a large quantity of documents and verifying that the content correlates with the information in the customer’s accounting system. In the past, the employees at PwC have manually keyed in the data into the system. This required of course a lot of time, when they had to analyse every document for important information. PwC did, in order to increase the efficiency and automate the data transfer, implement the ABBYY FlexiCapture intelligent solution for automated data collection and document processing. ABBYY uses artificial intelligence to provide content intelligence solutions and services. This technology makes the data transfer from invoices, contracts and other structured and unstructured documents much faster. When, for example, an auditor uploads documents to the ABBYY server, the ABBYY FlexiCapture can automatically identify document types and improve images. It can also identify which documents should be dealt with and can extract the required data and further transfer the data into a master spreadsheet. The auditors benefit from this because they can spend a lot more time with their customer instead of doing paperwork (ABBYY, 2019).

Case: Natural Language Processing in the leading accounting firms

Natural Language Processing, NLP, is a form of AI, that plays a big part of the ongoing developments in accounting and auditing. In its simplest form NLP is the technology behind tools such as spellcheck, autocorrect and in the Google search function that tries to figure out what you are going to say (Mills, 2019). This efficient form of AI combines both computers and linguistics (Mills, 2019), and it is guided by deep-learning, that learns from examples and
automatically obtains useful information for its user. From this extracted data, an accountant or auditor can acquire practical insights to use in one's work (Onyshkevych, 2018). Here we will look at how EY, Deloitte and PwC embody AI at the moment. Each of them has a somewhat different approach to the development. EY addresses it from a business value perspective, by doing small things and aiming to get in this way an immediate ROI. EY uses NLP in reviewing lease accounting standards in cases when the IRS issues new regulations. Previously they had to go through tens of thousands contract, but now NLP does this faster and humans only have to validate the results from the automatically extracted information. PwC employs AI as short AI sprints, where they develop quickly, in four weeks, a functioning model for a client. If approved they refine it to provide better accuracy for the client. These sprints include teams of two or three people, and PwC holds approximately 80 sprints a year. Deloitte also takes its own approach in deploying AI in the company’s operations. They have an internal innovation team, that focuses on every angle of new technology and devotes 80% of their time to AI. Their NLP system can, for example, look through hundreds of thousands legal documents in different client cases, and this way save months of time from humans (Zhou, 2017).

Next, we will look into on-going research in these topics to provide a link between the practical and theoretical.

**Ongoing research**

From on-going research, we have found many papers referring to the need for accountants and auditors to improve their skills. For example, according to Greenman’s paper “Exploring the Impact of Artificial Intelligence on the Accounting Profession”, research shows that employees need to up their skills because of the changes occurring in the fields. Accountants are being forced to adapt or risk losing their jobs. The good news is that while there will be job disruptions, there will be new jobs being continuously created. According the paper and referencing the US Bureau of Labor and Statistics, “the accounting profession is projected to grow at a rate of 11 percent over the next 10 years, an increase of over 142,000 new accounting and auditing jobs”, (Greenman, 2017). Greenman speculates that there are most likely many factors contributing to this growth in the US, but a large amount will be due to the technology advances that need accountants to have the right knowledge to make the advances work successfully. This paper shows that, yes, the accounting and auditing roles are changing, but from recent technological advancements they have not made all jobs obsolete. On the contrary, individuals with the right skills have used these technologies such as tax filing software to increase the number of clients they can take on. This further proves that with the right skills, the future will be bright.

Looking further into research done in the fields we can already see that there is a huge lack of IT knowledge in the accounting and auditing professions and that the need for these skills are becoming more important than ever before. There is already a need for professionals who have IT knowledge in auditing, data analytics and people who can handle these sophisticated IT services and programs. In Pan & Seow’s (2016) article they critically review the competencies and skills that the future accounting graduates need to prepare for. It is shown that the use of cloud computing, eXtensible business reporting language and business analytics have already set some changes in how companies do their financial reporting. The emerging use of information technology in almost every part of the accounting field have made the demand for accounting graduates to have advanced IT skills even more critical. The conclusion from the research is that it is crucial that accounting students have proper training in IT tools such as automatic identification systems, XBRL, analytical programming and data mining because this is what the future in the field will be all about, analysing and developing these IT
accounting systems. This means that the education and courses in the universities need to be more focused on IT related topics. (Pan & Seow, 2016) Further evidence from research in the topic is that accounting education is lacking the depth and breadth of the current evolving accounting practices. The author is reflecting the situation by the fact that the role of technology and information systems are not embraced enough in the current accounting textbooks (Wells, 2018).

In another research recently done by Zhang, Dai and Vasarhelyi (2018) the focus is on the impacts of disruptive technologies and how it will change the accounting and auditing profession as well as the education. As for to today there is still a lack of Information technology in the education which means that the students aren't prepared for the accounting workplace of the future. The most important question is about how the profession is going to adapt to the technological changes and how it will change the traditional procedures. One thing that is certain is that the automation will result in substantial reduction of staff especially from the traditional tasks. Automated processes mean that the accountants and auditors will need to focus on the technical maintenance of the systems and more analytical work, while repetitive and mundane tasks will disappear. Mentioned here again, the technologies that are reshaping the accounting business models are robotic process automation, artificial intelligence, advanced analytics programs and blockchain and these require more sophisticated education that will focus on these high-level skills. These changes will mean that the educators at the business schools will have to use new teaching models that could include, for example, cybersecurity and audit data analytics classes. All in all, the future of the accounting and auditing profession will require a philosophy of lifelong learning and ongoing adaption to the changing environment (Zhang et al. 2018).

Lastly, we focus on audit processes, the research again goes through the disruptive technologies and how they will affect accounting and audit. In this paper the focus is on audit and how AI is changing what parts humans play in the in audits. To begin, there are already many advancements that have taken over certain tasks, this is due to the sheer amount of data, structured and unstructured, that companies process. In Kokina and Davenport’s, “The emergence of artificial intelligence: How automation is changing auditing” research they explain how due to the requirements of audits, AI technology is a perfect fit. Yet the advancements will reduce many entry level audit jobs, which is where many accountants start their careers. This will take away a learning opportunity for many new graduates as they won’t have a job waiting for them. The next step already being foreseen by the big four accounting firms is “making increasing use of audit platforms and predictive analytics, but not the higher levels of intelligence and cognitive capability”. They have used technology to reduce repetitive tasks, but still cannot take the emotional intelligence side and fit it into new technologies. Thus, while current entry level jobs may be replaced, we are moving towards a combination of human, machine work, rather than full automation. With Kokina and Davenport predicting that, “Since AI technologies replace specific tasks rather than entire jobs, loss of employment in the short term is likely to be relatively slow and to be marginal rather than dramatic.”. This research opens further questions about, “bias in AI and whether humans using AI applications can engage in appropriate judgment and decision-making.” and how transparent it is to use AI if humans are not interpreting the results correctly (Kokina & Davenport, 2017).

**Future job descriptions**

There is no doubt that the accounting and auditing professions will change sooner rather than later because of the digital revolution that we are presently in. When time-consuming tasks are done by machines, professionals can focus on adding more value to their customers which will
reduce both cost and time spent on the given tasks. The automation of regular accounting processes will lead to accountants and auditors being able to focus on more specific tasks because many of the earlier tasks will be done by computers. Traditional accounting procedures such as inhouse invoicing and travel invoicing will be replaced by computers. Auditing processes will be automated and there will be advanced tools to detect risk and fraud. Future auditors will be able to focus on analysing the outputs instead of using several hours on collecting information from financial statements (Forbes, 2018).

The future jobs of accountants and auditors will be all about using sophisticated information systems and artificial intelligence to analyse, report and develop wanted outputs. Sophisticated information systems will take care of handling data security, connecting different parts of the financials which will become part of the big data. The revolution is changing the tasks related to management accounting and financial accounting. In the future the management accounting tasks will be more precise and detailed because of the computer’s abilities to collect and gather the information that is needed for managers to make the right decisions. Accountants in the field can then focus more specifically on preparing and analysing the data for those who are interested. The problem that accountants might face is the overwhelming amount of information that will be available. This means that the accountants’ jobs will be about recognizing the relevant and important information to be able to make decisions. These tasks require strong communication skills to be able to share the most important results in a clear way. Although computers are taking over, one important fact is that the quality of the data will remain important. To be able to produce quality data there is a need for someone who can transfer the information and serve as a service agent when working on transferring knowledge to the systems. This task can’t be done without an expert in the field. As time passes and robots are part of the daily tasks of accounting and audit professions there is going to be a need for someone at the user level support as well as someone who is capable of solving the technological problems related to the systems. We don’t know the specific job descriptions of the future accountant and auditor, but from existing information we have gathered a list of potential future job descriptions titles presented in the following table.

Table 2: Examples of future job titles (source authors based on literature review)

<table>
<thead>
<tr>
<th>Blockchain Accountant</th>
<th>Analytics Guru</th>
<th>Historical Accounting Analyst</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare Accountant</td>
<td>Cloud Accounting specialist</td>
<td>Systems Integrator</td>
</tr>
<tr>
<td>Cybercrime Accountant</td>
<td>Fintech City planner accountant</td>
<td>Strategic Accounting Analyst</td>
</tr>
<tr>
<td>Fintech Accountant</td>
<td>Data Security Accountant</td>
<td></td>
</tr>
</tbody>
</table>

**Required skills**

Now that we have seen what kind of jobs might be offered in the future, we need to figure out how we can adapt and overcome to be the kind of employee companies will be looking for. To start, base knowledge of accounting and audit will always be necessary thus the skills mentioned here are ones that are needed in addition to what accountants/auditors should already somewhat know. To conquer this topic, we have broken the skills down into more technical skills/ “hard skills” and then so called “soft” skills, which are not always taught in conventional education.
Table 2: Potential required skills now and in the future, source: authors based on the literature review

<table>
<thead>
<tr>
<th>Technical skills</th>
<th>Social skills</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding the capabilities of software</td>
<td>Basics of coding</td>
</tr>
<tr>
<td>Analysis skills</td>
<td>Fintech software knowledge</td>
</tr>
<tr>
<td>Data visualization</td>
<td>Data security, forensic tools</td>
</tr>
<tr>
<td>Knowledge of International Standard</td>
<td>Data warehouse management</td>
</tr>
<tr>
<td>Knowledge of industry specific regulations</td>
<td>ERP (Enterprise resource planning) experience</td>
</tr>
<tr>
<td></td>
<td>Strong communication</td>
</tr>
<tr>
<td></td>
<td>Conflict solving</td>
</tr>
<tr>
<td></td>
<td>Leadership skills</td>
</tr>
<tr>
<td></td>
<td>Risk management</td>
</tr>
<tr>
<td></td>
<td>Strategic decision making</td>
</tr>
<tr>
<td></td>
<td>Emotional intelligence, ethical</td>
</tr>
<tr>
<td></td>
<td>Adaptability, tolerant of uncertainty</td>
</tr>
<tr>
<td></td>
<td>Sales knowledge</td>
</tr>
<tr>
<td></td>
<td>Innovative/creative</td>
</tr>
<tr>
<td></td>
<td>Customer service orientation</td>
</tr>
</tbody>
</table>

The technical or “hard” skills include analysis, understanding of software and its capabilities, and data security knowledge amongst others, mentioned in Table 3. These are more about learning how to interact with programs, AI, robotics, and generally with the digitalization process that will take over mundane tasks. As mentioned before, many tasks will become hybrid human-robot tasks, there will be the need for people who know who to interact with the machines (Daugherty & Wilson, 2018).

As for the social or “soft” skills, these are generally harder to learn in a class, they take patience, understanding, and the ability to adapt. While the technical skills have always been deemed important, these soft skills are becoming equally valuable because they will allow individuals to bridge the gap between machines and people. As the accountancy and audit professions moves towards a more strategic and insights-based fields, these soft skills will become even more necessary. The individuals who master these skills will be immensely better off when dealing with clients, who will no longer look at their accountant/auditor as a source for just financial statements, but as someone who knows their business inside and out and can provide valuable knowledge. Thus, gone will be the days of the quiet, back office accountant, so expect to have employers increasingly ask for adaptability, innovativeness, sales skills, effective communication, and customer-oriented support capabilities (Marr, 2018b).

While the thought of needing so many skills may seem overwhelming, it is not necessary nor expected that every employee will be competent in all these areas. As mentioned earlier, jobs will most likely take a turn towards more specialized roles thus requiring employees to develop skills in certain areas. The advice here would be to explore many areas, select the top most interesting ones but only specialize in a selected few that show a promising future.

How to acquire the necessary skills?

Now that we know what kind of skills will be required, we can move on to where to acquire these skills. Due to the technological advances of the last 25 or so years, the way to gain knowledge has expanded increasingly. No longer do you need to attend a physical class when almost everything is online. Presented here are some of the best ways to expand your skill set for the future. Starting with online courses, these are offered on platforms such as edX.com, Coursera.com, in these websites you can take courses from the Arts & Humanities, social sciences, business, to languages. The variety on these websites is increasing rapidly. In addition to just taking one or two classes, they offer fully online master's degrees from accredited
universities. They also offer certifications in different professional areas such as data science, cybersecurity, deep learning, and many other beneficial skills. Many of the courses are free, but to have them recognized you need to pay a fee, while a masters may set you back about 10-25k€ depending on the program (edX.com). This may seem like a lot to spend, but compared to a campus master’s degrees, the cost is relatively cheaper.

In addition to online courses, you can still attend class at a university, for example through open university, where you only pay per credit. This offers face to face interaction with professors and other students. Here is where you can learn the material taught in class, but also how to work better in teams.

Both options mentioned are especially great for people who are already working to be able to continue learning. In addition to seeking outside learning, it may be possible to ask your own organization to provide further in-house training. This shows employee initiative to progress in their career but is also a way to help the company grow in the inevitable digital future.

Moving on to possible quick learnings solutions, there are other options such as YouTube, where knowledgeable individuals can share their insight in different areas and the same with Podcasts. Beware with these though as there could be some misleading or incorrect information. There are also plenty of LinkedIn trainings that are specifically geared towards accounting and audit. Lastly, while not the most conventional way to learn, take a chance and volunteer for leadership or teamwork experiences to build up technical skills, but also some of the interpersonal skills mentioned previously.

Table 3: Examples of ways to expand one’s skillset, source: authors

<table>
<thead>
<tr>
<th>• Online courses:</th>
<th>• Training courses offered by own company</th>
</tr>
</thead>
<tbody>
<tr>
<td>• EdX- Universities like Harvard, MIT, Brown offer courses here</td>
<td>• YouTube- channels:</td>
</tr>
<tr>
<td>• Coursera</td>
<td>• &quot;Executive Finance&quot;</td>
</tr>
<tr>
<td>• Udemy</td>
<td>• &quot;CPA Strength&quot;</td>
</tr>
<tr>
<td>• Codecademy</td>
<td>• LinkedIn trainings</td>
</tr>
<tr>
<td>• Hour of code</td>
<td>• Podcasts</td>
</tr>
<tr>
<td>• Khan Academy</td>
<td>• Volunteering for leadership or teamwork positions</td>
</tr>
<tr>
<td>• Code.org</td>
<td></td>
</tr>
<tr>
<td>• Small Biz U</td>
<td></td>
</tr>
<tr>
<td>• Alison</td>
<td></td>
</tr>
<tr>
<td>• Open university</td>
<td></td>
</tr>
</tbody>
</table>

There are endless ways to acquire the skills needed for the future and many of these are even free. Accounting and audit will be changing and moving forward so now is not the time to rest on what you know, but to start the habit of continuous learning which will be necessary to keep up in these fields.

**Critical voices from society**

Although the overall opinion from the top players is positive regarding the Industry 4.0, there are still some critical and worried attitudes towards the future of accounting and auditing and how it will affect future jobs and professionals in the fields. Changes in the workforce and labour markets are often viewed with doubt and fear. Some of these concerns towards the digital revolution are, however, the same as they were already in the First Industrial Revolution (Najjar, 2019). The most common fears and threats circle around questions of jobs, security and needed skills of employees. Also, comes the fact that our current society may not be ready for all the changes Industry 4.0 brings and big changes to our society’s structure cannot be avoided (Marr, 2016).
Another thing that many in the field are wondering about is how to teach those entering the accounting and audit field? The entry-level accountants will most likely be the ones most affected on the labour market, due to the automatization. The reason for that is that they are usually performing the basic accounting and audit tasks, that will be automated. Consequently, some fear that entry level workers will not be able to get appropriate hands on experience early in their careers (Kokina & Davenport, 2017).

In addition, many older workers feel that they are being left behind in the transition to the digital age. They fear not being able to retrain enough to stay competitive in the field. Employees older than 50 years of age are on average facing challenges associated with new technology and automation, and therefore fear that younger people will overtake their jobs. In addition to this, it has been discovered that employers do not give the older workforce the same opportunities to receive training to enhance their skills in the digital era. The biggest uncertainty arises from not having any insight of the future role in their company. (Recruitment Revolution, 2018) This does not only include the older workers, the younger ones will also need to retrain their skills, due to the increasing change and automatization in the society. The future will require the average person to adapt to new changes “that would have previously taken several generations” (Dickinson, 2018).

Professor Klaus Schwab outlines in his book “The fourth industrial revolution”, the potential risks with the revolution we are in. He points out that organisations can be unwilling or not able to adjust to the changes and that governments can fail in the application and regulation of the new technology (Marr, 2016). The implementation of new technology is complex, time consuming and under some circumstances expensive. This can be a problem for smaller firms, they may not have the capability to implement new technology to the same extent as for example the Big 4 accounting firms, and therefore not able to keep up with the changes. (Caramela, 2018) Further, Schwab assumes that there will pop up new security concerns and that inequalities can increase if things are not handled properly. When automation increases, a lot of jobs will be lost across many industries, due to that workers are replaced by computers and machines. According to an estimate, as much as 47% of the U.S jobs will be in the risk zone (Marr, 2016). We should, however, keep in mind that, although some jobs disappear, new ones will emerge.

CFOs are under a lot of pressure from all the challenges in the digital age. The concern in the CFO’s responsibilities is on the ever-broadening areas in their tasks. Their role has never been more difficult that it is now. They are under the demand to obtain and analyse real-time data all the time, have the right skillset to understand the new technology, support the correct training of their staff and also hire new employees with the appropriate skills (Ernst & Young 2016).

Risk management will continue to be an issue and constant topic as technology may advance faster than companies and employees are able to keep up with. Related to CFO’s responsibilities in the on-going technological disruption, CFOs reported in a survey of more than 700 CFOs in 2018, that the cybersecurity breaches are among the most critical things that keep them up at night (Korn Ferry, 2018).

Conclusions and future outlook

These are exciting times, the financial world as we know it is being turned upside down. With continuous digitalization and innovation, it is hard to predict with certainty how the affected fields will look in 10 to 15 years. Yet through our research we have presented which potential tools and skills will mostly likely be needed and useful to have a successful and long career in either accounting or audit. To do this we reviewed the sector’s current and upcoming
advancements, the potential job descriptions that will shape who gets employed, and finally how to potentially acquire the knowledge needed.

What do we expect from the future then? After all our research, we know that robotics and AI are at the center of the change, and therefore humans will need to adapt to the changes coming with this. As we mentioned previously, many fear that these changes will make humans obsolete, but the further we research, the less we find this to be true. We have entered an age of human-machine cooperation that will continue as far as we can currently predict. At this point, many organisations still do not know how the Industry 4.0 impacts their business or are struggling with other things, such as how to find the right talent and knowledge to know how to adapt to the changes. Thus, it is necessary and inevitable that many organisations are implementing changes and preparing for a different future with new technology that will improve their business. Industry 4.0 is still developing, and we cannot probably see the complete picture until many years in the future. However, the companies that adopt new technologies, are realizing the potential future. The same companies are also dealing with how to educate their current workforce, so that they can handle the new job tasks that Industry 4.0 brings and to recruit new employees with the right skills (Marr, 2018a).

Specifically, the future of the accounting and audit professions, it has become abundantly clear that the role of accountants and auditors are changing. Time consuming and repetitive work will be automated, and the future accountant and auditor will perform higher value work, while transforming into more advisor roles in finance and business, with more specific expertise (Forbes, 2018). This will allow for these individuals to focus their brain power on more fulfilling tasks, but those that do not adapt will not make it through the next rounds of advancement. Thus, we know that now is the time for those interested in staying in these fields to push themselves to keep learning and improving because there will be no other choice.

From on-going research, we see a shortage in required skills, especially with new graduates whose knowledge is coming directly from universities (Pan & Seow, 2016). While it might be a slow change due to bureaucracy, we see education systems, specifically universities, changing their programs to be more technology-oriented and forward looking. In addition to universities, we know companies will need to invest in technology and in their employees’ skillsets. We predict that while investment may be expensive, it will be more expensive to lose out on business and risk bankruptcy.

Overall, we expect a promising and innovative future, where human-machine cooperation will be key and the individuals with the right skillsets will be set to prosper in this future. Yet, as we know the future is unpredictable so further research will be needed to guide businesses, accounting and audit professional, and society at large into the right direction.

References

DIGITAL ACCOUNTING: OPPORTUNITIES, THREATS AND THE HUMAN FACTOR


14


**BIG DATA, CLOUD COMPUTING AND DATA SCIENCE APPLICATIONS IN FINANCE AND ACCOUNTING**

Jennifer Huttunen, Jaana Jauhiainen, Laura Lehti and Annina Nylund

Minna Martikainen and Othmar M Lehner (Editors)

1 Hanken School of Economics, Helsinki
2 University of Applied Sciences Upper Austria and Hanken School of Economics, Helsinki

**Abstract:** The aim of this paper is to get acquainted with big data and how advanced analytical tools like data science and machine learning are helping the financial sector obtain greater insights about their businesses. Further applications also include acquiring a deeper understanding about ways to provide customers the next level experience in banking and/or investing. We have briefly touched on cloud computing as the platform to support the utilization of some of these technologies. The financial sector, including the accounting industry, will experience disruption albeit at an unknown pace. Despite the benefits derived from exploiting these emerging technologies, a slow uptake is still observed. The authors believe that a more receptive attitude towards innovative technologies could pave the way to more application in the field. Consequently, standards and regulations will evolve to keep up with these changes.

**Keywords:** Big Data; Data Science; Machine Learning; Analytics; Accounting; Finance

**Introduction**

The digitalization of the world continues and new innovations within accounting and finance will affect every day work tasks. Without insights about what is currently happening on the field and what will most likely change in the foreseeable future, various professions will be put at risk. The gap between information technology and the traditional accounting and finance roles is predicted to rapidly diminish. The understanding of concepts such as Big Data, Cloud Computing, and Data Science Applications will be crucial for succeeding in the coming job market as a decision maker in financial sector. The study focuses on the efficient use of data for business decision-making in the financial industry. The paper examines the use of Big Data analysis and Data Science Applications to improve budgeting and investment decisions within accounting and finance field. As the topic itself is relatively new, the study is done as a literature review. Due to the scarcity of academic research materials, the review will include research articles complemented by various internet sources regarding current developments and ongoing applications in the field. The authors developed a theoretical framework in Figure 1 as a representation of the relationship present in this topic.

We begin by defining the relevant terms for this paper and proceed to discuss their relevance in the field of accounting and finance. We will also evaluate current developments and ongoing research in the field, including a description of commonly used machine learning algorithms in Big Data analysis. Application of these technologies in the field will be presented through some case examples. We then proceed with an investigation of the critical voices from
the society and concerns related to the ongoing development. Lastly, we will conclude based on our investigations and include speculations about the outlook.

Why and for who?

Aside from using Big Data for marketing purposes such as targeted advertising, business sectors including accounting and finance will experience a rapid change brought about by the changing technology. Both accounting and finance deals with large volumes of data, instead of physical products, but the actual use of Big Data and its analytical possibilities is still at a very early stage (Cockcroft & Russell, 2018). To progress, it is important that professionals within accounting and finance field manage to adopt some basic IT knowledge – since understanding and utilizing new techniques will alleviate monotonous manual work leaving more time for strategical thinking and decision making. This paper examines what is currently going on in accounting and finance and presents concepts related to the following topics:
• Efficient use of data for financial decision making in financial institutions
• Why: getting better insights for budgeting and investment decisions
• For who: decision maker in financial institutions, reporting

Key Terms and Concepts

Big Data

The term “Big Data” is defined in Oxford English Dictionary as: “n. Computing (also with capital initials) data of a very large size, typically to the extent that its manipulation and management present significant logistical challenges; (also) the branch of computing involving such data” (Oxford English Dictionary, 2008). Another way to try to understand the term Big Data is to examine the commonly agreed criteria of Big Data which can be described in three V’s:

Volume – the total amount of data stored, exabytes and petabytes instead of terabytes
Velocity – the intensity in which new data is created and needs to be stored, i.e. every card transaction around the world recorded in data centers and data warehouses
Variety – the heterogeneity of the data and the mess it creates, for example videos, click streams, comments, numerical information and transactions creates data without any notable structure

Nowadays two more V’s of Big Data has been widely recognized; Veracity and Value. These two V’s refer to the fact that when more and more data is collected the trustworthiness of the data and the added value it brings come into question (Reca, 2018).

Big Data consist of both structured and unstructured data. Structured data has a pattern and includes often well-organized information which are easier to embrace than the latter one. Unstructured data is in a nutshell everything else, a mess of “loose” information as streams from social media, audio, location services and Internet of Things technologies (King, 2018). A comparison of structured and unstructured data is presented in Table 1.

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Structured Data</th>
<th>Unstructured Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Pre-defined data models</td>
<td>• No pre-defined data model data model</td>
</tr>
<tr>
<td></td>
<td>• Usually text only</td>
<td>• Maybe text, images, sound, video or other formats</td>
</tr>
<tr>
<td></td>
<td>• Easy to search</td>
<td>• Difficult to search</td>
</tr>
<tr>
<td>Resides in</td>
<td>• Relational databases</td>
<td>• Applications</td>
</tr>
<tr>
<td></td>
<td>• Data warehouses</td>
<td>• No SQL databases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data warehouses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data lakes</td>
</tr>
<tr>
<td>Generated by</td>
<td>Humans or machines</td>
<td>Humans or machines</td>
</tr>
<tr>
<td>Typical applications</td>
<td>• Airline reservation system</td>
<td>• Word processing</td>
</tr>
<tr>
<td></td>
<td>• Inventory control</td>
<td>• Presentation software</td>
</tr>
<tr>
<td></td>
<td>• CRM systems</td>
<td>• Email clients</td>
</tr>
<tr>
<td></td>
<td>• ERP systems</td>
<td>• Tools for viewing or editing media</td>
</tr>
<tr>
<td>Examples</td>
<td>• Dates</td>
<td>• Text files</td>
</tr>
<tr>
<td></td>
<td>• Phone numbers</td>
<td>• Reports</td>
</tr>
<tr>
<td></td>
<td>• Social security numbers</td>
<td>• Email messages</td>
</tr>
<tr>
<td></td>
<td>• Credit card numbers</td>
<td>• Audio files</td>
</tr>
<tr>
<td></td>
<td>• Customer names</td>
<td>• Video files</td>
</tr>
<tr>
<td></td>
<td>• Addresses</td>
<td>• Images</td>
</tr>
<tr>
<td></td>
<td>• Product names and number</td>
<td>• Surveillance imagery</td>
</tr>
<tr>
<td></td>
<td>• Transaction information</td>
<td></td>
</tr>
</tbody>
</table>

To get value out of Big Data, combining both structured and unstructured data, analysis of it need to be made – and this is the real challenge. Information from different sources is useless if there is no way to find any structure in it or answers to specific problems and this cannot be done by humans due to the three V’s mentioned before. Big Data can be envisaged as the base, all the information collected need to be stored somewhere which requires cloud computing and Data Science Applications uses Big Data to do different kind of analysis. However, notice that the exist of each of these components are not dependent on one other.

**Data Science**

Data science is an umbrella term for an interdisciplinary field that uses scientific methods, processes, algorithms and systems to extract knowledge and insights from data in various forms like data mining and machine learning (Hayashi, 1998). Data mining is a data analysis technique that aims to discover patterns in big data involving machine learning with a goal to extract information from a big data and transform the information into a comprehensible structure (Cliffon, 2018). Machine learning means studying of models that computer systems use to improve their performance on a specific task. Machine learning is based on algorithms that build a model of sample data in order to make predictions or decisions without being explicitly programmed to perform the task. Machine learning can be supervised or unsupervised learning. Supervised learning is something that human knows at teaches for the application like e.g. how to create invoices. Unsupervised learning means that the machine is given certain big data, but it is not told what to look for. The application studies the data, builds clusters and learns on its own. It can detect e.g. that there are some similarities in customers that tend to pay late or not pay at all (Koza, Bennet, Andre, & Keane, 1996).

**Artificial intelligence (AI)** is defined in Oxford Dictionary as “the theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between
languages” (Oxford Living Dictionaries, n.d.). Meaning that AI is needed for machines to be able to learn to perform above mentioned tasks. AI can be described also as a science that describes how computers imitate human intelligence.

**Analytics**

Big data analytics is a form of advanced analytics. It allows the massive volumes of big data gathered to be processed. The process of extracting information can be categorised into five stages and two sub-groups, as described on Figure 2. Data Management is concerned with the technologies to acquire, store, and prepare data. Analytics is then concerned with extracting insights from the data gathered (Gandomi & Haider, 2015).

![Big data Processes](image)

Figure 2: Big Data Processes. Adapted from Beyond the hype: Big data concepts, methods and analytics by A. Gandomi & M. Haider, 2015, International Journal of Information Management, 35(2), page 141.

An abundance of analytical techniques exists for structure and unstructured data. Text, audio, video, social media analytics are all examples of these categories. Analytics can be further classified into descriptive, diagnostic, predictive and prescriptive (Decide Soluciones, 2017).

Descriptive analytics describes what has happened, and diagnostic analytics answers why something has happened. This is generally considered the traditional level of analytics used in business intelligence. The further levels are known as advanced analytics. Prescriptive analytics describes what we should do. Prescriptive analytics anticipates what will happen in the future and suggest options for future courses of action. Predictive analytics, as the name states, predicts future events based on historical and current data. Using machine learning and AI, which are described in the following sections, predictive analytics seeks to capture patterns and relationships in data. These can be, for example, historical patterns or interdependencies between factors. These techniques are mainly based on statistical methods. (Gandomi & Haider, 2015) Predictive analytics can be seen as a subset of data science in general.

**Cloud Computing**

Cloud Computing is about using flexible infrastructure in today's business. IBM defined cloud computing as the delivery of on-demand computing resources. For companies, this means the use of offsite shared servers hosted on the internet to store, manage, and process data instead of capitalizing on servers and computers locally which requires regular maintenance by the company. The flexibility of using the cloud endeared corporate consumers for the following reasons (EcourserReview, 2017; Jain, 2018):
**On-Demand Service** – use it when needed. This provides some degree of freedom for the customers.

**Network Access** – utilizes the internet and can be accessed using laptops, workstations, and smart phones.

**Pooling of Resources** – resources are pooled to provide customers customizable variable costs based on business size.

**Scalability** – scale up or down based on your current needs.

Cloud Computing Service providers offer different service models according to the customer’s needs. The service models are called SaaS, PaaS, and IaaS. These models are often depicted in a pyramid-like structure as shown in Figure 3.

![SaaS, PaaS, IaaS Pyramid Model](https://www.boxcryptor.com/en/blog/post/what-is-the-cloud-a-beginner-s-guide/)

Below are more examples of applications that utilizes these models:

- **SaaS** – Banking applications, Social media apps, Slack, App-based games
- **PaaS** – SAP, AWS Elastic Beanstalk, Google App Engine, Apache Stratos (Hou, n.d.)
- **IaaS** – these are more for system administrators and include Rackspace, Google Compute Engine (GCE)

**Machine Learning Algorithms**

As mentioned, utilizing Big Data is impossible without data mining and machine learning. Following analytics algorithms are frequently used to discover patterns in Big Data:

**Linear regression** – One of the most basic and most used algorithms. This algorithm uses the relationship between two sets of continuous quantitative measures. Linear regression examines the relationship between the independent variable(s) and the dependent variable. The goal is to
describe the dependent variable in terms of the independent variable(s), i.e. how time effects revenues, is there a relationship between age and income or what will the price of X be in 6 months.

**Logistic regression** – In difference from linear regression which examines two quantitative variables, logistic regression is used to solve problems involving categorization. The output variable values are distinct and finite instead of continuous and infinite as in linear regression. This algorithm can be used to answer clearly defined yes or no questions, i.e. credit worthiness or if it is likely that a customer will buy again. (Hiltbrand, 2018) Different regression analysis is most used for determine the strength of predictors, forecasting an effect and trend forecasting (Statistics Solutions, 2013).

**Classification and Regression Trees** – These algorithms use a decision, based on a question related to an input variable, to categorize data. The data is processed through a set of questions and for each corresponding decision it will move towards being categorized in a specific way. The way the data is processed creates a tree-like structure, where each set of question lines ends in a category called the leaf node of the tree. The classification and regression trees may easy become very large and complex, since a single tree can include several branches of logic. Hence, there is a variant version called random forest which consist of many small and simple trees instead of one big, which are then composited together to a final prediction. Classification and regression trees can be used to envisage multi-value categorizations (Hiltbrand, 2018).

**K-Nearest Neighbors** – A simple classification algorithm which allows for multivalued categorizations of the data. It is based on its samples in the training set and determines the distance of new samples to each data point, i.e. evaluates the nearest neighbours in each category. If the size and scope of the training set is very large, the process of this algorithm may be computationally expensive since the new samples needs to be compared to the whole training data set. Also, if the training data contains errors, the classifications will be misrepresented. KNN is common since it is easy to use and train, and the results that are simple to interpret. This algorithm is used i.e. in different search applications to suggest similar products (Hiltbrand, 2018).

**K-Means Clustering** – An algorithm commonly used in data exploration, which creates groups of instances with similar characteristics, and the different groups are called clusters. When the clusters are determined the new samples can be evaluated against the them to see which cluster is most suitable. The number of clusters are pre-defined where after the K-Means clustering process are dividing the data accordingly. However, the clusters are not yet categories, just closely related instances of input variables. The relevant clusters need to be discovered, analysed and renamed into business categories to bring value. It is also worth to notice that K-Means Clustering are sensitive to outliers which may distort the whole analysis (Hiltbrand, 2018).

**Neural Network** – In comparison to other algorithms, Neural Network (NN) is next level. Basically, NN is a framework for different machine learning algorithms to work together on complex data inputs. It mimics the human brain with its artificial neurons and enables the computer to learn, e.g. deep learning (AI) through a supervised or unsupervised learning process (DeMuro, 2018). Neural network can adapt to changing input without redesign the output criteria. The “neurons”, or nodes, in NN are mathematical functions that collects and classifies information, i.e. in similarity to multiple linear regression. A neural network contains layers of these interconnected nodes, and each layer combined with the learning curve minimize the
marginal of errors in the outputs. Neural network is used in applications as forecasting, trading, enterprise planning, risk assessment, fraud detection and Natural Language Processing (NLP) (Chen, 2019).

**Current Research and Developments**

The use of Big Data in accounting and finance is most researched within four areas: Financial distress modelling, Financial fraud modelling, Stock market prediction and Quantitative modelling, and Auditing. There has been progress with adapting research results into practice in the other areas, but auditors have been slow with implementing the results. One explanation could be that auditors are reluctant to implement technology which is far ahead of those used in their client firms. Although, some leading auditing firms have started to adapt Big Data techniques in practice – which can be a valuable addition to the profession especially combined with the expertise (Gepp, Linnenluecke, O’Neill & Smith, 2018).

*What is the direction of development currently?*

Financial technology applications vary from simple automation to complex decision-making tools. Many of these applications rely on big data and require investments in cloud infrastructure and analytics tools (Das, 2018). In the past years, financial companies have been looking at opportunities to shape themselves into lean and customer-centric organizations. In many cases, assuring access to viable financial and banking analytics is the key in this transformation. Analytics allows companies to make intelligent and data-driven decisions.

Many of today’s intelligent tools answer the question “what is happening”, but the more important question of, “why is this happening” is trickier to answer. Good analytics tools can help to shape this answer. Answering these important questions help financial institutions to figure out what their customers are looking for, how to shape the financial offerings to fit the customer needs, and how to best communicate to customers via marketing. Answering these questions require discovering new insights within the possessed data with data analytics.

However, it must be remembered that even the most sophisticated analytics tools are not a turnkey solution to success. Companies must educate their workforce to use these tools and make the best out of them. Some critical pitfalls must be avoided with caution, one classic example being the attempt to prove causation with correlation. Perhaps the most dangerous danger is the risk that users of data analytics are searching for answers with their own – sometimes unrecognized – bias. This causes them to find the answers they want to find, instead of the real ones that could be the stepping stone to the next innovation.

An example to the above-mentioned challenges is IBM’s so called “augmented analytics”, which infuses traditional business intelligence (BI) solutions with more analytical intelligence. Augmented intelligence refers to data analytics that can learn and adapt to different needs and guide users to new insights while removing the human bias from the equation. On the technical level, IBM’s analytics technology includes machine learning, data discovery, natural language queries, automated pattern detection and sophisticated data storytelling capabilities (Walker, 2018).

As a practical example, IBM’s analytics technology uses data patterns to identify clients with a high probability of accepting marketing offers and then adjust the campaigns accordingly. Some banking companies have seen increase of revenue by 60% in some customer segments. Some banks are now using analytics to do a fully automatized, yet highly personalized loan offers while automating the actual loan-approval process (Walker, 2018).
Forecasting

Data science plays a key role in many aspects of accounting and finance. It can boost competitiveness and profitability by allowing accounting professionals to make more accurate and detailed forecasts. Better forecasts are possible when the company can anticipate market trends better (Goh, C. 2017). Big data and predictive analytics have a key role in the development of forecast accuracy from the increasingly growing amounts of data available (Hassani, 2015). Current limitations to forecasting with big data are that traditional tools do not have the processing capabilities for the size, speed and complexity of the data, which poses challenges for organizations.

There is also a research made that suggest that business decision makers prefer to use complex forecast methods, including big data analytics when possible, instead of more simple methods. Surprisingly, the forecast accuracy did not improve when using complex methods and the errors even increased when using too much complicity in the forecast procedure. This only added unnecessary complication only because of a user’s preference. The chosen forecast method should always be understandable for the user to avoid errors (Green, 2015). Though, the veracity and value of the Big Data used in forecasts will probably play a big role in the accuracy.

However, improvement in forecasting will provide immense opportunities. Financial institutions can forecast the bankruptcy of a firm better and predict defaulters of loans with more accuracy. This can be extended to predict the reliability of a credit card applicants’ tendency to delay payments or risk of defaulting. Stocks can be ranked more accurately based on their risk, allowing investors to create portfolios based on their risk tolerance level. More accurate forecasting of interest rates can affect investment decisions.

Budgeting

A common challenge in budgeting is that setting goals and strategy, going through scorecards, reports and forecasts is time consuming. Often also the technology is designed for individual productivity rather than company-wide collaboration. Data science can optimize budgeting since data analytics tools allow companies to combine diverse financial and non-financial data and produce more comprehensive reporting (Goh, 2017).

The above-mentioned IBM planning analytics tool is giving a good example of how to automate budgeting and forecasting process. It creates reports and analyses from data it has collected from numerous sources and aggregated based on the models that were updated there. It is reducing the time spent on data analysis up to 70 % by same time improving accountability and reliability since it’s using more information than what human could use (Anderson, 2010).

Basically, anything that can be read (text, pdf, html) can be read automatically nowadays which removes human working hours and makes the time-to-market faster. Natural language processing (NLP) that combines neural networks with other algorithms can read financial statements. Machine learning and data science is used for forecasting algorithms for budgeting and it is possible to compare multiple future outcomes and customize the budgeting model to various assets and portfolios under review.

Risk Management

Analytics helps companies manage risks, as it enables continuous auditing and monitoring in a wide range of areas within the company. These areas can include for example the regulatory environment, the supply chain, or business strategy. Banks and other financial institutions can use these analytics techniques also for fraud prevention. Managing risks in both financial and operational environments is crucial for financial institutions.
Banks store vast amounts of data which can be used to analyse behavioural patterns of both new and existing customers. This can help the bank anticipate customer needs, their response to new products, and it can help the bank price loans better and calculate probability of repayment more carefully (Peric, Kozarevic & Polic, 2016). Risk management is a key area of big data analytics and applications in the financial industry, and it has only grown in importance after the recent financial crisis (Hassani, 2015). Additionally, to the previously mentioned credit risk and performance analysis, compliance and regulatory reporting and insurance evaluation can also be analysed and improved through big data.

Financial risk management refers to use of financial instruments by a firm to manage exposure to various types of risk, such as operational, credit, market, foreign exchange or liquidity risk. The key sources of risk are analysed and measured, and measures are taken to address them. Machine learning can be used to identify, prioritize and monitor these various risks. Algorithms can help develop more accurate risk scoring models, additionally being more cost-effective. An example of an area where machine learning and AI can be applied is evaluating creditworthiness. Machine learning can be used to analyse past behaviours and spending patterns. Zheng et al. (2018) describe that fintech can reach a level of technology described as ‘intelligent finance’, where financial technology can integrate the internet, finance and big data to achieve more precise and faster calculations and transform the industry through data science technology.

As mentioned earlier, improved forecasting methods can also help improve risk management processes. There are massive amounts of customer data available for financial institutions to use, which vary both in volume and structure. Processing semi-structured or unstructured data can be challenging and time consuming. For instance, natural language processing, data mining and text analytics are techniques that can transform masses of data into more easily usable forms. The financial industry already produces masses of highly structured data which can be utilized when developing AI technologies (Zheng et al. 2018).

The previously described predictive analytics can help cover patterns in data that indicate some specific event happening in the future. This event can then be acted upon already in the present day. For example, predicting price movements or anticipating customer lifetime value. Fraud detection can also be greatly improved through machine learning.

**Cases**

*Case Danske Bank*

Danske Bank has recognized early on that the banking industry is shifting to a more technology-driven world. And in order to survive and thrive, the company must adapt. The company realized that their customers’ behaviour has been changing, demanding faster response and more tailored approach as a result of increasing technological advances available at their fingertips. To stay on top of the game, Danske realized the need to address the changing customer needs and wants.

With individuals becoming more active online and creating digital footprints, a wealth of data is generated consequently. Nadeem Gulzar, Senior Development Manager at Danske Bank from [2015 - 2017], said in an interview, these big data sets are like the new oil or gold (Hortonworks, 2017). In the last few years, Danske has used data analytics to provide a more personal approach to enhance customer service.

A few years ago, the company executed a strategy using advanced data analytics to find ways to address business challenges. This strategy entailed putting together a team of data scientist to work with business managers. An example given by Büchmann-Slorup, Head of
Sales Development and Analytics at Danske Bank, in the Sternberg article (Sternberg, 2017), was a study done for a certain lending market. The use advance data analytics gave them insights into the type of customers that are most likely to avail of this facility by focusing on precise behaviour parameters. This was a more accurate understanding about their customers compared to classifying them based on a more generic category like income, age, etc. (Sternberg, 2017).

Detection of digital fraud is another solution that Danske addressed using machine learning. Figure 4 shows the challenges encountered by the bank using the traditional approach of an investigator looking at customer data. By deciding to work with Think Big Analytics, a Teradata company, Danske utilized a data driven methodology that works with machine learning and deep learning. The goal was to increase fraud detection rate and decrease false positive results. The result with using machine learning reaped a decrease in false positives by thirty five percent (35%). And by adding deep learning, accuracy of fraud detection rate increase by approximately fifty percent (50%) (Groenfeldt, 2017).

Data Driven Approach to Fight Fraud

Challenges to Fraud Detection

Low Detection Rate
ONLY ~40%
of fraud cases are detected

Many false positives
99.5%
of cases are not fraud related

High Fraud Loss
Tens of Millions €
€ lost each month

Fast evolving fraud sophistication


In an article in CMO by O’Brien (2018), Danske was heralded as mastering the use of data analytics. They are a success story of assimilating the work of engineers and data scientist with those of the business people. Their Head of Global Analytics has advocated the use of machine learning and even artificial intelligence to help give the customers a whole new experience.

“We simply use it [data analytics] to make ourselves, and our products, more relevant for the customer. So, trying to predict the need from the customer and then be there as soon as the customer needs us - that’s the key for us,” Nadeem Gulzar, Senior Development Manager at Danske Bank in 2015, said.

However, even with the success experienced by the bank with these technological tools, they caution the users to be more perceptive and pragmatic with its applications. These technologies are not akin to a magic wand that can fix everything. Sometimes, the basic information that we have is all that is needed to address a simple problem.
Case Bridgewater

Many hedge funds already use algorithmic trading today. An algorithmic trading strategy has three components: entry, exit, and position sizing (Williams, 2017). Data-driven and quantitative funds have experienced tremendous growth. Algorithmic trading utilizes intelligent predictive analytics to arbitrage the advantages of big data. No matter what strategy is used, transaction costs will be reduced for the investor (Oxford Algorithmic Trading Programme, 2010). Renaissance Technologies is a known example, functioning fully with only algorithmic funds. However, in this case, we will focus on Bridgewater, a hedge fund that is not only focusing on automating its trading but its management as well.

Bridgewater is the world’s largest and most profitable hedge fund. Their main fund utilizes algorithms to trade stocks, bonds, currencies and other assets. The fund tracks factors such as interest rates and retail sales, which creates its algorithms. The fund has anticipated many economic up and downturns in the past, including the financial crisis of 2007-2008 a year earlier (Copeland and Hope, 2016). The team in charge of the development of the algorithmic software is headed by David Ferrucci, who was also the lead developer for IBM’s Watson, the computer system capable of answering natural-language questions.

Now the fund aims to not only automate trading, but also to develop a system that will automate management decision-making for the whole fund. The company is highly data-driven. Meetings are recorded, and employees have to rank each other throughout the day. These ratings then show each employees’ strengths and weaknesses. They can also set goals and track how efficiently they are being achieved (Solon, 2016). The algorithms are now being developed to make decisions such as finding the new staff and ranking opposing arguments in the case of disagreements. The new AI system is called the “Book of the Future”. This kind of automation would remove the human emotional aspect from decision-making (Solon, 2016). The algorithms would also plan and organize the employee’s entire day, down to whether they should take a specific phone call or not.

The AI technology used by financial services businesses is evolving every day. Even though quantitative trading is becoming more and more sophisticated, the development is moving towards other areas too, such as the automation of management. This can eventually lead to an entire organisation being supported by AI decision-making.

Criticisms

In addition to all potential benefit gained from the use of data science and big data for financial institutions, drawbacks must also be considered. As banks and other institutions are developing new techniques and technologies to handle and analyse the data, they must consider the security aspects at each step. Both security issues as well as the privacy of data are key concerns. Cloud-computing has become popular due the benefits it offers – broad network access, on-demand service, and resource pooling. This presents many issues for privacy and security, as many systems are still quite young, and security protocols are not fully established. Security monitoring must be still developed. As we are still at the very beginning phases of working with big data, financial institutions must develop this ecosystem with care to avoid any possible security and privacy breaches (Sinanc, Sagiroglu & Terzi, 2015).

Regulation is also a concern for the future of financial institutions utilizing these new technologies. The question of consumer protection is highly relevant. By nature, many of these institutions are very global and serve various cross-border transactions. The legal aspect of these transactions should be considered – which country’s legal system should be followed? Financial
regulation can be fragmented and specific to certain countries and regions, so there is great risk for both consumers and financial institutions if they are not aware of all regulations.

Additionally, when the use of Big Data analysis increases, it is important to understand that not everyone will be evenly benefitted. Information technology helps investors to do less risky investment decisions but on the other side are the firms that need capital financing. One macroeconomic question today is why big firms seem to replace smaller ones and a possible explanation is the cost of capital. Large and incumbent enterprises have longer track records and thus more big data available to reduce the asymmetric information problem in comparison to new and smaller firms. More available information reduces the investors’ risks which lead to cheaper access to external capital markets and reduces the cost of capital of big firms - this again accelerates their growth while a small firm’s growth is initially idle (Begenau, Farboodi & Veldkamp, 2018). When doing investment decisions based on analyses extracted from Big Data, it is vital to be aware that there might be more profitable investment options than the suggested ones and higher risks can depend on the lack of available data rather than its inferiority.

Conclusions and Future Outlook

The disruption of fintech to the financial industry has been relatively low to date. This is partly driven due to the fact that fintech companies provide complementary services to the traditional financial sector. Although alternative lending services are provided, the users will still need bank accounts to make use of these services. There is also a need for the safety of households and firms accounts which new fintech services does not provide, traditional banks are still the best source for this (Lorente & Schmukler, 2018). However, more and more small companies are able to use big data and data science to provide services that are outside the scope of regulatory bodies, or that do not require licensing. New data analysis methods are being constantly developed, many of them being created by the small players instead of established banks (Dapp, 2014).

Customer expectations from financial services are likely to rise in the future as the various technologies develop. As more and more users gain access to fintech, and thus to financial services and credit, they will again fuel the need for the emergence of new and developing financial technologies that are faster, address customer needs better, are more convenient, and provide new solutions. Banks will likely find it difficult to operate completely in the traditional manners and business models (Lorente & Schmukler, 2018; Dapp, 2014).

Overall, the use of Big Data in accounting seems to drag behind, there is yet no academic empirical work apart from anecdotal evidence to turn to. At this stage, the focus is on determining what possible consequences Big Data will have on management accounting, financial accounting and auditing. In general, using Big Data in accounting context will be a disruptive force since it will require significant change both in skill set and the way traditional accountants work. Traditional tasks such as data registration will become less important and management accounting techniques will become obsolete. Big Data technology will soon provide alternatives for asset valuation, cost analysis, forecasting and budgeting. It will also impact the role of bookkeeping as the creator of business knowledge for managers to base their decisions on since they will have access to endless external information provided from Big Data (Rikhardsson, 2018). The principles for accounting has been generally unchangeable for ages, which possible can be an explanation why adaption of innovations is slow and why it get resistance. But Big Data techniques are best used to complement and not replace human experts (Gepp et al. 2018). Furthermore, accounting standards as IFRS and GAAP will probably need to be updated accordingly to technical advancements, if it will change i.e. the way analysis, reports and valuations are assembled and done.
At this stage, finance seems well ahead of accounting what comes to utilizing data science applications and big data to bring added value to the decision-making process. However, these concepts still seek establishment among the field – which may be hard to attain during a phase of new innovations constantly lurking around the corner. Still, the ongoing change should be embraced and not rejected, if it brings new possibilities not achievable otherwise. Resistance and issues can be won by widening the knowledge within the emerging technology and by cooperation between involved fields.

References


CURRENT STATE AND CHALLENGES IN THE IMPLEMENTATION OF ROBOTIC PROCESS AUTOMATION AND ARTIFICIAL INTELLIGENCE IN ACCOUNTING AND AUDITING

MAX GOTTHARDT, DAN KOIVULAASKO, OKYANUS PAKSOY, CORNELIUS SARAMO1
MINNA MARTIKAINEN1 AND OTHMAR M LEHNER2 (EDITORS)

1 Hanken School of Economics, Helsinki
2 University of Applied Sciences Upper Austria and Hanken School of Economics, Helsinki

Abstract: Technology development has grown rapidly in the last decades and gained importance for accounting and auditing through its identified potentials. Particularly the automation of judgment systems and systems that require human intervention, are deemed to be more relevant to confront a transformation through Robotic Process Automation (RPA). During the continuous development, the augmentation of such systems through Artificial Intelligence (AI) presents a greenfield project with high expectations. However theoretical frameworks have not yet been elaborative and sufficient to capture how such deployments can be conducted. Addressing this research gap, this study presents a summarized overview of the transforming RPA ecosystem and indicates what challenges are critical to being confronted for a successful implementation of such systems in accounting and auditing.

Keywords: Robotic Process Automation; Artificial Intelligence; Financial Technologies; Accounting; Auditing; Technology Implementation; Black Box Solutions

Introduction

In this article we discuss the use of RPA and AI in accounting and auditing. The intelligent automation of work has been a topic of discussion for over 20 years, however the implementation of RPA and AI systems in companies is still in its infancy. Only 15 percent of companies consider themselves to be mature in their use of RPA, and only 5 percent in AI (PWC 2017). Companies are still far from utilizing the vast opportunities provided by automation. As the capabilities of technology are improving in a rapidly increasing pace, it is vital for companies to adopt them successfully.

More specifically, we examine the challenges involved in the implementation of AI and RPA systems and the important factors that companies need to consider. Existing research has so far looked at the use of ERP systems in companies and its limitations (Hyvönien et al., 2008, Andersson et al., 2018)). Some research has also been done regarding the use of RPA particularly in the in the accounting profession and some of the challenges and opportunities involved (Cooper et al. 2018). However, a focused overview at how to successfully implement RPA and AI systems in accounting and auditing has been missing so far.
In order to fill this gap, we first introduce the relevant terminology needed to comprehend the possibilities of AI. We then give a brief overview of the current developments and research that has been done on the broader field. Next, we examine the challenges of AI implementation more in-depth. A typical framework of RPA is presented, and we provide two case studies, one of a global software firm and one of a small Finnish payroll company to give a more practically oriented view of the present application of AI and the challenges these companies face.

We then attempt to identify the main challenges of AI implementation and indicate some suggestions for the practice. This will provide value to practitioners and academics likewise as we provide aggregated knowledge about the typical difficulties that companies are confronted with in their use of AI systems. This article can also serve as a checklist to practitioners when adopting new technologies in their company.

**Terminology**

Robotic Process Automation (RPA) and Artificial Intelligence (AI) are two closely knit terms that both have had and will continue to have a big impact on accounting and auditing practices. RPA and AI are on two opposite ends of an intelligent automation continuum. Automation is quickly moving from a process-driven to a more data-driven kind. Whereas RPA is highly process-driven, i.e. automating rule-based tasks, AI requires good-quality data for the AI to be able to learn what to do (CFB Bots, 2018).

The use of RPA has become widespread in the last 20 years and is a useful tool in all sorts of business administration tasks. RPA is a technology that automates standardized and rule-based activities using scripts. Robots can e.g. be used to copy and paste data between applications such as invoicing, payrolls or others (EY 2018d). Conventional RPA processes are constrained by technical capabilities and the judgment needed in operating them. Robots are not capable of handling unstructured data such as scanned documents etc. Humans are still needed to manually feed the robot with processed data which maintains low-value tasks for employees. There are also constraints in automating cognitive tasks. Several tasks exist that cannot be automated with current technology. These “cognitive” tasks have rules that can’t be modeled because they require the experience of staff. An example is a request in an email, which requests to prioritize and making decisions (Perrier 2018).

RPA is sometimes misconceived as “old technology” that is being replaced by AI, which is a misperception. The two technologies do not replace each other but can be used separately or together. AI and RPA tools may increase the value of each other. For example, AI does not need RPA for creating insights from credit risk modeling, but RPA can be used to action the insights (EY 2018c).

Artificial intelligence, in fact, covers a number of interlinked technologies including data mining, machine learning, speech and image recognition, and semantic analysis. Data mining uses a combination of statistics, machine learning and AI to discover patterns in large data sets. This is important as the amount of data constantly increases, and unstructured data makes up 90% of all data. Data mining helps to find relevant information more quickly (SAS Institute 2019).

An important augmenting technology for AI is OCR, which can be used to convert typed or handwritten text into machine-encoded text. This allows the firm to eliminate time-consuming manual data entry. Another central part of AI is Machine learning (ML). ML systems get trained by absorbing the learnings from the data and decisions and can make simple decisions and classifications. ML can, for example, be used in fraud detection. PayPal uses ML tools to separate transactions such as money laundering from legitimate transactions (EY 2018d).
Natural language processing (NLP) uses learning algorithms to analyze text and unstructured data. Natural language generation (NLG) is a technology that generates text or speech from structured information. It can be used to generate financial analysis reports, reporting numbers about a company’s performance. Chatbots use both NLP and NLG to interpret voice or text and respond with standard predefined answers. Chatbots continuously learn new vocabulary to interpret the unstructured information. They are typically used in customer service functions to answer queries (EY 2018d).

Implications in Practice

Currently, only 5 percent of companies consider themselves to be mature in their use of AI and 15 percent in their use of RPA (PWC 2017). This means that AI is still in its very early stages of adoption for broad society changing use. This partially depends on costs related to the adoption of such technologies and perhaps lack of skills within companies. However, the huge potential rewards of using AI and RPA technologies means that companies ought to gain expertise in the field.

AI and RPA together mean that a large amount of data can be turned into actionable insights, which allows full automation of entire processes. Investing in intelligent automation is very costly so it is of great importance to consider what combinations of RPA and AI are most suitable for the company (EY 2018c). This requires the knowledge of accounting professionals who are both experts in the business end but also in the technologies that are available.

PwC (2017) has estimated that 45% of work activities can be automated and that this will save $2 trillion in global workforce costs annually. This shows how much companies can benefit from effectively implementing AI technology. It is strategically important for companies to start investing in innovation as AI is increasingly being adopted and the ones that have been successful in their implementation will make huge productivity gains in their work.

Automation through AI and RPA will also bring big changes to the accounting and auditing industry. Mundane and repetitive tasks typically done by junior staff will be taken over by robots. Instead, human expertise is needed at a higher level to make decisions that require judgment. RPA also brings great opportunities for internal auditing. Tasks such as testing of controls can be automated through RPA which expands the capacity of internal audit and frees auditors to more value-creating activities. Automation allows testing of full populations of data instead of sampling which increases the accuracy of auditing exponentially.

Methodology

For this analysis, relevant literature has been identified and filtered through the technologies and industries, that have been deemed relevant for the research question of presenting the current state and challenges in the implementation of RPA systems. Furthermore, an elaborative literature review has been pursued with a focus on analysis and summary of the key factors in practice rather than reflecting solely on the theoretical models. In order to capture the practical implications validly, two use cases have been carried out and an extended interview on the topic has been conducted, which has also been integrated into the argumentation of this paper. Finally, results have been reviewed by peers and a research framework has been created to present the findings.
Current Developments and Ongoing Research

Organizations suffer from inefficient processes for accounting and auditing throughout different working units, which makes it harder to allocate scarce resources and targeted decision making. Currently used spreadsheets tend to be chaotic due to the heavy involvement of manual processes and introducing high potential for lags, errors and outdated data, which can be “referred to as ‘shadow systems’ as they are not formally recognized as part of the enterprise system” (Drum and Pulvermacher 2016, p. 181). Improperly created systems and insufficient quality and quantity of data with structural disproportions in databases and spreadsheets can cause significant financial losses such as the recent error that costed USD 100 Million for the shareholders (Tan 2014). Therefore, new technologies and frameworks are needed to solve these problems and fill in the gaps of sustainable management of resources and quality of processes.

Building on complementary technologies including Big Data and Blockchain, automation is predicted to have one of the highest impacts to the field of accounting in the short term. As discussed earlier, the emergence of this technology is inevitable considering the technology transformation in accounting. This transformation has been foreseen and analyzed for a long time. In the 1950s, the vice president of the National Cash Register Company, C.L. Keenoy, commented on this: “...We do know of course that we are in the early stages of an accounting and business management revolution which, in some respects, will rival the industrial revolution in its effect on the lives of everyone…” (C.L. Keenoy 1958, p.230). Originating from the automatic recording of punched cards and their processing in bookkeeping, the use of electronic technologies was recognized as revolutionary, while particularly the development of practice concepts for such an Integrated Data Processing (IDP) has been deemed critical. In alliance with this, the expansion of AI and other expert systems to automate accounting-related tasks can be traced back to the 1980 (Baldwin et al. 2006) and has been gaining further importance ever since.

Despite being identified as critical technologies decades ago, there is no clear consensus of how such deployment processes should be conceptualized in current practice and what the tangible challenges are there to be faced. In the following, we will elaborate more on how such a project structure can be summarized in the accounting and auditing fields.

A relevant question to ask before approaching RPA in auditing and accounting is whether or not to separate these two subparts from enterprise resource planning (ERP) or general corporate financial administration or see them as mere subparts to the big picture. When looking at financial administration more broadly (auditing, management accounting, book-keeping, personnel administration, salaries, tax payments etc.), it becomes evident that there are numerous interfaces that need to be compatible with each other for relevant data acquisition/collection to be possible. This requires legislative and operational change from official institutions as well as application in companies.

Hyvönen et al. (2008) indicate that ERP systems have brought a new type of concept to the digital transformation journey, integration. To exploit the large variety of functional autonomies in an organization, ERP systems have served as a bridge between these functionalities to enable a cross-functional and process-oriented approach (Quattrone and Hopper 2005). With this central control system, the CFOs had the chance to fulfill the role of being the “captain of the ship” and manage both the design and implementation models of the system (Andersson et al. 2018). However, Hyvönen et al. (2008) highlight the solution being prone to “complexity, which is evident from the numerous links to other information systems, updates of versions, data collection problems, the need for checkups, arranging information storage, etc” (p. 46). It is also
harder to reach high automation rates in accounting for particular cases such as accounts payable/receivable or auditing through ERP systems, which makes them obsolete for in-depth tasks requiring advanced judgment models.

Interviews with public accounting professionals from the Big 4 conducted by Cooper et al. (2018) reveal that there are often challenges related to the reluctance of the firms’ clients to use RPA software. This is in part due to clients not completely understanding the capabilities of bots or how they operate. There is also some resistance because they are afraid that automation will negatively impact their employees’ position. In addition, many clients are reluctant to adopt new technologies because of data issues. There are concerns related to the protection of business processes and the flow of information between different jurisdictions (Cooper et al. 2018).

Framework

Despite the narrative in the research on possible models based on RPA, a consensus hasn’t been met in practice yet. To fill in this gap, the depiction of a typical back-office process in the background for invoicing of a purchase order by Deloitte (Schatsky et al. 2016) is guided analytically below. These operate first with human-led manual process, second with an RPA implementation and lastly with the augmentation of cognitive technologies for RPA.

In a manual process, the user periodically logs into the system and check orders, and once a request is confirmed, the purchase order is validated. Afterwards, specific pricing or discounts are applied to the order based on the client’s contract. On top of this, additional changes are applied, that are outlined in the protocol and the purchase order is shipped and invoiced. This process is prone to human error and can bear judgmental complexities.

This process can be automated by an RPA robot, which is built on a software solution. This software first extracts data from the customer system and check for new orders. After downloading the purchase order, it is redirected into the legacy system. Here a human supervisor validates the order for its validity and accuracy according to the customer’s contract terms. Afterwards, the process continues with the automated robot uploading the purchase order to the internal ERP system, for instance SAP or Oracle. Here discounts are adopted automatically based on customer agreements. The software would again pull data from customer system and check for orders, and once it is downloaded, they are pushed into the legacy system. Customer contract is processed with NLP to extract relevant information and match them. Afterwards, the discounts follow automatically based on customer agreements.

In the automated version of these three working concepts the human role is limited to supervision, and the system will be further prone to cost savings and efficiency gains due to the automated training and learning path, which is much harder for humans. Interestingly, Baldwin et al. (2006, p.79) indicate that auditors prefer human processing to decision aids or knowledge-based systems. This shows that a proof-of-concept (POC) in particular cases may support the company benefits of such systems and align on possible improvements through automation. Depending on the complexity and scope, Schatsky et al. (2016) indicate that a POC may take around two weeks, whereas a pilot can be operating within four to eight weeks.
Case Studies

In order to present current applications in the market, we will present a macro view of one of the global leaders in shared services and RPA robot developers and a micro view of a startup ecosystem in Finland. Thus, in this macro view, we focus on the analysis of the technologies and the collaborative ecosystem based on automation, whereas the micro view captures the societal implications and the role of automation in a local setting for innovation. This distinction provides the differences in approaches in environment, implications and solution concepts for further research. Additionally, we briefly present their automation ecosystem and indicate what challenges can be relevant.

Case 1: How to shape a collaborative landscape for RPA and AI in accounting and auditing

Founded in Romania in 2005, UiPath started out with software development kits (SDKs). Growing from 1 million USD to 100 million USD annual recurring revenue within 21 months, they have been counted as one of the fastest growing enterprise software companies (UiPath 9/18/2018). Having raised around 450 million USD funding up to date with their latest valuation at 3 billion USD through important venture capital funds, including Sequoia Capital, Accel, Earlybird, Kleiner Perkins and Seedcamp, they count 2100 global customers up to date and are acquiring 6 new customers per day. With a developer community of more than 250,000 peers worldwide, their platforms follow high usability marks and a direct market approach through large accounts across different industries.

The robot will open the invoice’s folder in the mail and the PDF document will be opened in background to extract the relevant information. These include company name, invoice date, invoice reference number, description, taxable amount, tax rate, total amount and contact information. The UiPath runs the robot, which opens the email, saves the attached invoice and extracts the needed information, while highlighting the activities being executed. After reading the text from the PDF, information is extracted from the file. The robot also performs data conversion and format changes in order to validate the input in SAP. A screenshot of this process in UiPath Studio can be seen in Figure 1. After this extraction is done, the robot logs into SAP with encrypted login data. Then a search is conducted if there are entries for this vendor in the system, as depicted in Figure 2. In that case, certain information can be adapted from previous internal data. Afterwards, the invoices are entered with data extracted from the files. Finally, the VAT information is checked with the invoice and database. Cases can be defined in order to send the invoice to a pre-defined user and to ask what the robot should “post” or “park” it into the system. Then the original file is moved to processed invoices folder in the mail system. Through such an automation approach, clients can majorly eliminate human intervention in invoice processing.

This invoice processing concept with UiPath Studio has been deployed with a client in automotive manufacturing (UiPath 2018), where the client faced challenges to pursue frequent manual interventions for reading, validating, registering and posting of invoices. As the number of invoices to be processed per day was at 2,000, the decision was made to automate this process. Through the solution time savings of manual work was at 65%-75%, sub-optimizations were avoided as the automation is controlled from a central system and a structure was brought into the processing concept of the client.

See Annex 1 for screenshots of the workflow.
UiPath Business and Technical Analysis

There are several ecosystems, which have enabled the growth of UiPath, according to the Chief Evangelist Guy Kirkwood (Baxter 2018). First, their clients applying RPA to develop automated processes account for the highest transaction potentials. Second, they have technology partners including Google Cloud, IBM Watson, Celonis with their capabilities in complementary technologies including NLP, OCR, ML, which are integrated to the value offerings of UiPath Orchestrator, their central control system. It can be argued that their multitenancy and backward compatibility capabilities can be seen as a unique selling proposition (USP), which other players in the industry struggle to develop (Le Clair 2018). Third, software companies including Microsoft, Google and Oracle and service providers such as Salesforce are integrating the company’s offerings into their platforms as to expand their reachability to further business operations. Such technical syndications can enable them to build on to their current offerings, for instance, developing a process mining product based on their cloud platform will give them an advantage against a competing automation provider. This can be augmented by their different cognitive solutions including ABBYY FlexiCapture to work with unstructured data. Fourth, system integrators including Deloitte, Capgemini, Accenture, KPMG utilize UiPath’s solutions for their clients during their digitalization journeys for automation projects due to high returns in their return on investment (ROI) and lower costs.

UiPath should improve their automation reusability (e.g., for error handling and logging) versioned within the platform (Le Clair 2018, p. 12). Their success factors depend highly on the operation of their direct market model, system training and how they scale. Therefore, their partnerships in training including RPAbox and Symphony are critical for the success of system deployment, as this is one of the most significant challenges in the technology implementation.

Case 2: A micro view on how to utilize RPA and AI in auditing and accounting

This chapter examines RPA in auditing in relation to broader business administration tools based on an interview with the payroll company Salaxy.com (Isosävi 2019) and has its main focus on the social implications identified by the company and how they approach technology innovation in financial industries. Salaxy offers a real-time salary payment solution with an automatic and intelligent payroll and has some of the biggest Finnish financial companies as its clients.

Currently, it may be argued that AI is overemphasized as a buzzword, whereas the majority of what is commonly referred to AI in normal process automation without machine learning. It needs to be remembered that, while some of the biggest proponents of the hype are the Big4 and their reports, they are also advertising, branding and selling their own tax and general consultation services.

One reason for this is the difficulty of acquiring relevantly structured data to learn from. A vast proportion of businesses have a lot to do in the basics of automation for AI to be relevant for them. Just combining accounts payable and due, taxes, invoices and salaries in one user interface would be revolutionary for small business (Isosävi 2019).

The national income registry that Finland has taken in use 1.1.2019 is a good example of only having one specific and not a broader societal mission of enabling automation. The registry only houses salary payment and tax information and not several other things related to paying someone’s salary such as e.g. household tax-deductions. This is because it is built only from an income tax point of view. The registry is also an example of process automation being not yet suitable for AI solutions because it is not designed to be a modern data storage as it could have
been. Without a holistic view on data and systematic collecting of it, not only present but a future application will be left undeveloped. This is due to the fact that the amount of possible AI solutions increasing together with more interfaces to combine existing structured data. A revolutionizing concept would be to combine the income registry with a real-time Value Added Tax (VAT) registry to give the real-time “pulse” of the economy. Any arguments on how the economy is doing would be rendered useless with such a tool.

The big societal discussion should not be only about having a holistic view, but also about what kind of data is gathered and who administers it. In order for data security and privacy to be secured legislation and standards need to be put in place for how to administer data and metadata and for how to access this data while also securing everything is logged for oversight. States looking at user needs instead of foundations and principles easily leads to miscalculation such as in the case of the Finnish Transport and Communications Agency. There are of course some AI in place already to justify some of the hype. Looking at bigger business and financial institutions some of the most advanced AI solutions and also examples of legislative activity in enabling use of AI can be found in banks and AML practices. How banks recognize patterns from money transactions to flag laundering and other illicit transactions are based on activities related to EU’s 5th Anti-Money Laundering Directive. The automatic processes in place in banks also become tools for gathering data that is needed for the machine learning to further enhance AML-practices.

**Future Potential**

Robotics and intelligent automation house huge potential for financial accounting (EY 2018c). However, traditional RPA has limits, as it can only process information in digital form and not e.g. check things over the phone or through informal interaction. According to Ernst & Young more digitalization and especially machine learning is needed for it to reach its full potential and value creation (EY 2018d).

Looking at digitalization in depth (E, 2018d) has described how to make clients change the way they work in order for them to deepen their digitalization capabilities. According to EY (the process of automation needs digital enablement. This means that in order to automate anything clients need to digitalize and decipher unstructured data gathered through e.g. digital forms, chatbots and voice recognition and convert it to structured data as a prerequisite for any form of robotics (RPA), which again is the prerequisite for AI (e.g. intelligent optical character recognition. Further to make the most of automated processes the digital workflow needs to include agent portals that may interact with people.

Robotic Process Automation (RPA) or digital labor or the use of software robots to automate processes are easy to configure and may deployed to automate manual tasks. They can perform activities such as copying and pasting data between applications, reconciling and cross-referencing data between different systems and conducting high-level (PWC 2017).

Within the internal audit, new testing approaches are needed for automated processes. This comes with an urgent need to also understand risks introduced by RPA and ensure that controls are well designed and effective to mitigate risks of new tech. Automation can increase compliance and reduce risk. Machines, unlike humans, do not skip a process step or become fatigued when going over transactions. Results are also always standard free of bias or variation which makes them accurate. On the other hand, this also means that possible errors become systematic and robots may not understand business environment changes that humans would notice. This means RPA governance needs to be put in place.
Beyond the automation of controls testing, RPA offers significant potential to change internal audit. Possible tasks include tracking and monitoring key risk indicators (KRIs), automated reporting and dashboard conception, shaping balanced scorecards and more (PWC 2017). In addition, the evaluation of data quality through master data and the assessment of administration through log files increase the validation of systems and gives control to the users.

Further, benefits of RPA may only be realized when deployment is managed with the same discipline and consideration as any other technology-based project. Internal audit needs to leverage companies’ digital initiatives as a technology platform to reduce cost and increase risk coverage (PWC 2017).

Using advanced RPA methods enables the use of artificial intelligence through machine learning. When teaching machines any flaws in data will naturally severely flaw the functionality of algorithms and such further emphasizing the importance of RPA governance as the robotic processes are the sources of gathering data.

General trends of artificial intelligence are of special relevance to financial transactions as vulnerabilities in these would be a lucrative target for cybercrime. Further, anyone not wanting to give a true and fair view of their concern might want to rig AI used for auditing. This means documentation and logs for user interface and other software needs to be extremely transparent when any personal information is processed. A worst-case scenario of potential problems can be found e.g. in the vulnerabilities of the digital driver's license service launched by Finnish Transport and Communications Agency (YLE 2018). Besides transparent software solutions also relevant and cleanly scraped data are of essence for any AI solutions in finance.

When looking at rapidly changing opportunities through digital services it is also important to bear in mind that we are in a process of change and that the pace of change is still not clear. Looking e.g. at how digitalization has affected the Finnish financial giant Nordea they have invested 730 million euros in compliance and functional security as well as hired 1 300 compliance experts and trained 12 000 customer service professionals for 110 000 hours in 2018. In the meanwhile, the capacity of the company’s robots now adds up to the equivalent of 1 500 personnel and it has invested over 200 million euro in digital services (Kauppalehti 2019). This shows that full automation is far from here.

Discussion and analysis

As the area of research is still relatively new, the amount of identifiable challenges and risk factors are many and of various consequence. In the following chapter we present a few of those factors that we have deemed to be critical in both the existing RPA systems and implementation of new ideas. These challenges have been identified by the Big 4 auditing firms and smaller solution providers and integrators. An overview has been created by the study based on the academical literature in line with the industrial argumentations from Deloitte (2018) and PWC (2017) in order to reflect different aspects of risks of implementing an RPA programs augmented with AI systems (see Annex 2). These have been captured mainly from the business and technical approaches and should be further augmented with societal views presented above. Therefore, originating from these findings on challenges, significant focus fields are presented for a discussion for future research and industrial investigations.
Table 1: Identified targeted risk categories for implementing a program with RPA and AI (Edited, augmented and modified from PWC (2017) and Deloitte (2018))

<table>
<thead>
<tr>
<th>Change Management</th>
<th>Business Risks</th>
<th>Automation Risks</th>
<th>Center of Excellence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>How is HR tackling the impacts of RPA?</td>
<td>Identity and access management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>How are changes to be communicated?</td>
<td>Secured business processes</td>
<td></td>
</tr>
<tr>
<td>Executive</td>
<td>Who has the ownership of RPA initiatives?</td>
<td>License Compliance</td>
<td>Proof of Concept</td>
</tr>
<tr>
<td></td>
<td>Who will manage the framework and promote efficiencies?</td>
<td>Automation strategy and governance</td>
<td></td>
</tr>
<tr>
<td>Functional</td>
<td>Who designs control systems?</td>
<td>Adaptation schemes of existing systems with new features</td>
<td>Backward Compatibility</td>
</tr>
<tr>
<td></td>
<td>Are there scalability limitations in RPA and core systems?</td>
<td>Legacy systems for simultaneous and unified operations across technical testing and rollout</td>
<td></td>
</tr>
<tr>
<td>Technical</td>
<td>How will the data quality and accuracy be ensured?</td>
<td>Incident management and business continuity</td>
<td>Implementation</td>
</tr>
<tr>
<td></td>
<td>How is the tests, validations, maintenances?</td>
<td>Regulatory compliance</td>
<td></td>
</tr>
<tr>
<td>Operational</td>
<td>What controls exist to monitor performance?</td>
<td>Data leakage and privacy</td>
<td>Business Case</td>
</tr>
<tr>
<td></td>
<td>How will the business comply with regulatory requirements?</td>
<td>Cyber threats</td>
<td></td>
</tr>
</tbody>
</table>

*Only proper guidance leads to good results*

There is a major risk that occurs when an overhaul of a previous routine is conducted in the form of the approving manager not fully grasping the concept. The programmer or IT tech that builds or supplies the system that is meant to revamp the system in place has a perfect understanding of the ins and outs of the interface and underlying processes. This is most likely not the case of most upper-level managers as seniority in a company is often linked to an older generation which means a need for an in-depth education of general concepts that they have not dealt with in the past. As the level of knowledge is at a low point, the risk of misuse can be assumed to be high and faults occurring not due to the failure of the actual system but instead from upper management. These issues might not have occurred if an RPA system was not in use and for instance, the second tier of human interaction prevents this.

Having proper motivation behind the project is key. As the introduction of an RPA serves as a business project, the main focus has to be on the benefits from a business perspective. If the IT focus becomes too high, there is a risk that the end goal of the system is forgotten. This can be a factor in figuring out how the RPA is implemented into the existing workforce and to which degree it replaces conventional jobs.

An issue regarding AI systems is how easily they can be manipulated or broken to take on unwanted characteristics. As AI tries to emulate a humanlike thought process the risk of ruining it through stimulus is a factor in the planned use. “Tay” the Microsoft experiment in 2016 is a prime example of this manipulation. It took twitter under 24 hours to fully corrupt this AI bot that was emulating an average female user into spewing out sexist, racist and other unsavory
comments in response to a dialog. This exemplifies perfectly one of the weaknesses of AI, data. If the quality of the data that is being used to learn from is weak most of today’s AI systems are not able to get past this initial hurdle and recover (Sakata 2018).

_Cybersecurity and vulnerability through malicious AI systems_

Any attempt at cracking or hacking financial systems that can be automated with use the of AI learning systems are theoretically much more effective and harder to prevent. This is relevant in the financial industry as hackers can infiltrate key systems and remain there using AI learned behavior. EY identifies four different cyber risks that are tied to the implementation and usage of RPA:

- Abuse of privileged access,
- Disclosure of sensitive data,
- Security vulnerabilities, and
- Denial of service.

These risks are factors that can be exploited by malicious users to access sensitive data that is being processed in an RPA system. But RPA systems are not different from other IT systems and countermeasures are readily available and under continuous development. There are other measures to take to ensure a safe system outside actual IT solutions, such as having strict control over who has access to the system and a transparent and traceable entity that can be monitored easily (EY 2018b).

_Correct usage and right strategies are critical_

As the financial sector is keen to be on the current trends and adopt methods that have shown to be successful in other companies and situations the risk of neglecting the true need of your company is high. This could lead to an almost impulsive choice of RPA in a situation where another system or even personnel solution is more cost-effective and/or easier to implement and use. Avoiding the trendy pick is often hard to do as it requires to distance yourself as a manager and seeing the bigger picture (EY 2018a).

_Future outlook_

_Implmentation needs resource allocation_

Ensuring that an RPA is running at maximum potential is key in the implementation process of these systems. Enabling the RPA on an enterprise level for scheduling purposes and allowing it to do the tasks “unsupervised” are keys mentioned by the symphony ventures blog. These abilities are meant to save both time and money which is the bottom line of why RPA systems are being developed in the first place (Brain 2017). The running costs for the implementation of RPA systems in terms of timeline and costs are relatively insignificant when compared to major updates in conventional IT platforms in auditing systems.

There is a fear that RPA will be struggling with the often-occurring non-standardised invoices and data that it would need to handle. OCR systems and a hierarchical system of approval and exception that is flexible enough is required to cope with the demand of the accounting industry (EY 2016a).
Financing and proof of concept (POC) needed

There is much need for POC before any major decision is made in most businesses and RPA and AI is no different. Unfortunately, this is an issue when it comes down to breaking down cost-benefit calculations before implementation as true measurements can usually only be attained after the system has been observed in action. Developing an effective way to prove the usability of a system before major monetary commitment can be crucial for the implementation and mass-usage of a system. Especially beneficial POCs are those that are tested in a similar environment as the intended real-life system (Lang T. 2019).

Black Box Solutions: Transparency needed

To properly monitor the impact that an RPA has on the business the management must have the ability to judge it fairly, meaning that transparency is key. The goal of any RPA is to deliver on its intended task better than previous methods and ensuring that this is indeed happening is vital (EY 2016b). Explainable AI is a field that intends to make AI decision-making more like human behavior patterns and thus creating a path that can be followed by an overseer. If the company understands the reasoning behind the AI, the transparency and usability of the system increases (Rao A. & Golbin I. 2018). For this explainable and interpretable systems for the testing and deployment of AI can play an important role both to detect biases in the data, flaws in the model and gaining new insights to the system (Samek et al. 2017).

Adding solutions for the smaller players

RPA service providers have often large concepts and projects in mind when pitching their ideas, but a large part of the accounting industry is still operating on a smaller scale. This opens a potential for the use of RPA or AI systems in start-ups and other smaller businesses where the need for accounting can be a problem cost-wise (CiGen RPA, Medium.com). Offering a clear path of processing financial tasks and allowing for internal growth can be a difference maker in setting up a new company.

Limitations and further research

This study contributes to academic research by implying relevant research fields in order to explain the current state of RPA and AI methodologies across the accounting and auditing professions. Besides elaborating on the challenges, the provided status quo on the technological applications have been presented with two cases to cover different aspects in practice. On top of the multi-factor qualitative analysis, this study delivers an overview on current state and categorized challenges of RPA and AI programs in a focused manner (see Annex 2), which should be further extended based on implementation fields and departmental structures. A major limitation is the scope of the study and the focus on the practical aspects rather than the theoretical implications. Originating from this, future research should combine novel academic publications with practical models. Furthermore, empirical studies on time savings and amount of human intervention should be conducted to identify areas regarding task complexity and intensity for manual work in order to indicate the fields where RPA provides the highest benefits. This should also include the testing based on cases to understand in how far the augmentation of RPA through AI systems provide additional benefits. Thus, this will help to identify business, technical and societal challenges in the implementation of such systems in both the micro and macro
views. This study should be regarded as a starting point to assess the relevance of fields for further research to connect research and implementation in the industry regarding these technological models.

**Conclusion**

With our presented cases from the industry and reviews from research, we identify that the potential of RPA and AI in the field of accounting and auditing is increasing and is already being seized. Bresnahan et al. (1999, p.11) indicate that complex and cognitively demanding work or tasks that require judgment, creativity and frequent exceptions are remarkably hard to automate with computers (see Wilson and Sangster 1992), whereas important benefits are possible to seize with RPA systems augmented by AI. Baldwin et al. (2006, 82) suggest that AI researchers play a significant role to solve key issues about audit and assurance with the use of techniques including “fuzzy logic, neural networks and perhaps other areas of AI that have never before been applied in an accounting context”. In current applications, we have presented that these applications already play an important role in the improvement of RPA systems, while also increasing the factors to consider. By automating a good deal of the manual work that requires a lot of personnel to complete through human intervention, the threshold to improve efficiency is lowered. While this presents a significant potential of time and capital savings, we have identified numerous challenges to be confronted, which are in line with the implementation experiences in the industry (PWC 2017). While AI systems will help answering important questions about data, the quality and quantity of data input for such systems is a critical question. Furthermore, opening the black box of AI is vital in order to deploy such systems with responsibility schemes and expect higher automation degrees. To fill in this gap, explainable and interpretable AI systems present a greenfield for transparent technology development. While the cyber-attacks are becoming more powerful and fraudulent activities are showing frequent progress, also cyber-defense is becoming stronger to support the system’s security and safety. Government and intra-governmental regulation and registries have a huge impact on employers needing to renew their administration. It is important to understand that these improvements in automation require broad distribution of responsibility schemes, C.L. Keenoy (1958, p. 236) suggested many decades ago that these responsibilities will bring more opportunities in the forthcoming era of automation.

Throughout our research in the field of RPA and AI in accounting and auditing, we have presented technical, societal and business contexts on the state and challenges of current technology and implementation, where the main persistent issue in all cases has been the importance of the mindset and ecosystem modeling (see Annex 2). To achieve a successful implementation of such systems in accounting and auditing, it must be kept in mind that cross-departmental support and clear mindset must be retained, both clear strategies and problem statements have to be defined and know-how has to be canalized into the right centers of excellence with right skills. This will help them mitigate the risks and ensure leaner processes when dealing with errors or insufficiencies. Only the organizations, which are considering the extensive amount of risk factors from different views, can exploit the full power of RPA and AI systems, whereas others will be investing scarce resources into untargeted and unreliable processes without significant ownership of business or technology segments.


CURRENT STATE AND CHALLENGES IN THE IMPLEMENTATION OF ROBOTIC PROCESS AUTOMATION AND ARTIFICIAL INTELLIGENCE IN ACCOUNTING AND AUDITING

ANNEX 1

Figure 1: Screenshot of UiPath Studio for data extraction and conversion

Figure 2: Screenshot of UiPath Studio for data entry and invoice processing in SAP
BLOCKCHAIN IN THE FIELDS OF FINANCE AND ACCOUNTING: A DISRUPTIVE TECHNOLOGY OR AN OVERHYPED PHENOMENON?

AINO NORDGREN, ELLEN WECKSTRÖM¹
MINNA MARTIKAINEN¹ AND OTHAMAR M LEHNER² (EDITORS)

¹ Hanken School of Economics, Helsinki
² University of Applied Sciences Upper Austria and Hanken School of Economics

Abstract: Blockchain technology became widely known with the emergence of Bitcoin in 2009 and has since gotten a lot of hype as a technology to disrupt the field of financial services. Blockchain was even suggested as a possible solution to UK’s border issues after Brexit. While many praise blockchain’s promise to enhance the speed and security of transactions, there are some who question the real-world applicability of blockchain. Is blockchain the internet of our time, a disruptive technology or just an overhyped phenomenon?

This paper looks at blockchain technology, its applications in the fields of finance and accounting, and the disruptive power of blockchain in these fields. We provide an overview of the criticism and obstacles that need to be dealt with for blockchain to realize its potential.

Keywords: Blockchain, Digital finance, Digital accounting, Digital Auditing, Smart contracts

Introduction

Blockchain, or distributed ledger technology as it’s also called, is the underlying technology in Bitcoin cryptocurrency. It has, however, many more possible use-cases. Blockchain is a transactional database that is secured by cryptography and governed by a consensus mechanism: it’s essentially an immutable record of digital events. Due to its qualities, blockchain is a safe and trusted platform for record keeping between parties that might not otherwise be able to trust each other (e.g. Beck, Avital, Rossi and Thatcher, 2017; Cong and He, 2018; Iansiti and Lakhani, 2017; Crosby, Nachiappan, Pattanayak, Verma and Kalyanatraman 2016; IBM, 2018 and Smith, 2018). As blockchain promises to prevent fraud, increase trust and transparency and save time and money by eliminating intermediaries, it is one of the most talked about technologies of today. While others remain skeptical of its real-world applicability, some argue that blockchain technology has the potential to disrupt business the same way the Internet disrupted off-line commerce (Cong and He, 2018).

Blockchain has gotten a lot of hype around it and we have heard about how it is going to revolutionize the world of business (Iansiti and Lakhani, 2017). Finance and accounting are the fields predicted to be most disrupted by blockchain technology (McKinsey and Company, 2018). Traditional financial intermediaries are in increased competition with cryptocurrencies and financial services based on blockchain technology. Blockchain is believed to reduce cost and risk on financial markets by enabling smart contracts, enhancing security and transaction speed.
The financial sector leads the way in developing blockchain applications and business models. While substantial activity exists in practice, less academic research has examined the applications of blockchain for how we organize contemporary economics, society or organizations (Beck et al., 2017). Becker at al. (2017) call for a more critical perspective on blockchain research. In order to fill this gap, we first provide an overview of how blockchain works and examine the possible applications of blockchain in finance, accounting and auditing. We then outline the criticism toward blockchain and analyze the hype it has gotten.

Blockchain research is in its infancy state; the existing research generally targets attitudes towards blockchain, technical information and “the potential future”. Research on real-life applications of blockchain is lacking. So far, most of the research has looked at the Bitcoin system and only less than 20% of the research is focused on other blockchain applications (Yli-Huumo et al. 2016). Corporations are eager to release reports on investment in blockchain and boost about the bright future ahead, focusing on theoretical applications in a marketing effort rather than practical issues. The fuzzy promise of blockchain as a revolutionizing phenomenon conflicts with the widespread criticism of the technology. Significant energy consumption, the scalability problem, the lack of regulation and the fear of security breaches raises the question whether blockchain is suitable to implement on a wider scale.

In this article we look at blockchain technology, what it is, how it works, and how the future of blockchain looks like. Specifically, we examine the way blockchain can be used in the fields of finance, accounting and auditing; and what the disruptive power in these fields is based on. We then discuss the criticism blockchain has received and outline the obstacles that need to be overcome before blockchain can become a mainstream solution.

Blockchain

What is blockchain and how does it work?

In this section we look at the basic elements of blockchain. We believe that to be able to evaluate and analyze the impact blockchain can have, it is important to understand the underlying idea behind the technology and the basics of how it works. We will not go into technical details but look at the most important attributes of blockchain and the advantages and disadvantages from the perspective of financial fields.

<table>
<thead>
<tr>
<th>Blockchain is</th>
</tr>
</thead>
<tbody>
<tr>
<td>• a transaction database</td>
</tr>
<tr>
<td>• distributed and decentralized</td>
</tr>
<tr>
<td>• validated</td>
</tr>
<tr>
<td>• encrypted with hashing</td>
</tr>
<tr>
<td>• immutable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Blockchain can be</th>
</tr>
</thead>
<tbody>
<tr>
<td>• a public or private network</td>
</tr>
<tr>
<td>• permissioned or permissionless</td>
</tr>
</tbody>
</table>

| Blockchain enables smart contracts. |

Figure 1. Blockchain’s attributes. Sources: The Accounting Blockchain 2018, McKinsey and Company, 2018 and IBM, 2018.
Blockchain first emerged in 2009 when the cryptocurrency Bitcoin was launched by an anonymous person or persons going by the name of Satoshi Nakamoto. Bitcoin is a digital currency “mined” by people on computers all around the world using software to solve mathematical puzzles. Blockchain is the underlying technology behind Bitcoin. It is important to understand that blockchain and Bitcoin are not the same. You can think of blockchain as an operating system, such as Windows or Macintosh, and Bitcoin is only one of the many applications that can run on that operating system. Despite all the technological innovations (such as telephone lines, credit card systems, and the internet) that have made trading faster, more efficient and more trusted, many business transactions remain inefficient, expensive and vulnerable. (IBM, 2018) As blockchain promises to prevent fraud, increase trust and transparency, and save time and money by eliminating intermediaries, it could be the answer for making business transactions more cost-effective, efficient, safe and secure.

IBM’s (2018) elevator pitch for blockchain goes as follows: “Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, a car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.” So blockchain is a way to record and store information in a way that is very safe for all parties involved.

![Figure 2. Triple entry accounting. Source: CEO Blog, 2015.](image)

Although blockchain technology is also called distributed ledger technology and we are looking at the possible applications in finance and accounting, it is worth mentioning that blockchain is not a financial tool on its self. Smith (2018) points out that blockchain isn’t an accounting platform, journal entry tool, or a replacement for accounting software. Blockchain does, however, build on the idea of traditional double entry accounting system by “adding a third entry” that has both sides of a transaction validated in the same block. In traditional trading situation both parties keep their own records of the event, their own ledgers. This gives room for error as the records don’t always match, and there is a need for third party confirmation in the shape of an audit. With blockchain the transaction is first validated by both parties and then the transaction is recorded in the shared ledger as figure 2 (CEO Blog, 2015) demonstrates. This way everyone always has the same, correct information in real-time thus saving time, eliminating mistakes, and the need to reconcile accounts between parties come the end of the financial year (Business Learning Institute, 2017).
Each block in the blockchain is linked to the previous block, making a chain. As the blocks cannot be changed, the history of an asset or transaction can always be tracked reliably. If there is an error in the data, instead of removing a block, a new block with the correct information is created. There are two problems with this system. Firstly, how can it be verified that the first input data is correct? Blockchain cannot verify if an asset that is recorded in the blockchain actually exists. But once it’s in the blockchain, it’s there forever and it’s considered to be true. Secondly, a blockchain can become huge and slow, since no information can be erased.

Blockchain is a decentralized and distributed network as opposed to the traditional centralized way of storing information. Figure 3 (Institute for the future, 2016) demonstrates the differences between a centralized and decentralized and distributed network. Each participant in the network becomes a part of the database that stores the blockchain and when the information is shared it is hard to hack. When a traditional centralized system is hacked all the data is corrupted, but to hack a blockchain database you would need to have access to over 50% of the network. The existing information can then be verified by comparing the individual hash ID of each block to the ID of the same block in the other computers in the network. When a consensus of 51% is reached (at least 51% of the computers verify the same hash ID) and both parties of the transaction have validated the new transactions, a new block with the transaction data can be added to the network. When this is done, the new transaction is available in real-time for all the participants of the network. Because of the consensus mechanism the blocks or the data in the blocks is immutable, which means that they cannot be altered (e.g. Smith, 2018, Crosby et al. 2016). The consensus mechanism and validation of transactions from both parties prevent fraudulent entries and so called “cooking of the books”, thus making blockchain a very safe way of making transactions.

![Figure 3. Examples of centralized and decentralized, distributed networks. Source: Institute for the Future, 2016.](image)

**Hashing**

As explained in the previous section, blockchain is very secure because it is decentralized, consensus-based, and encrypted. Blockchain uses a specific type of encryption called cryptographic hashing. We will now explain why this specific method of encryption is so safe and how it works.

Hashing differs from traditional cryptography in that it only works one way. Traditional encryption works two ways and the encrypted data can be decrypted back to the readable form with an encryption key. A hash cannot be decrypted by any known algorithm yet. This means that a hash is theoretically impossible to decrypt and the only way to “read” the information in
the block would be by guessing and this would take forever (Massessi, 2018). However, it is predicted that in the future super computers will be able to crack hashes.

The data in each block in a blockchain is secured using a cryptographic hashing algorithm resulting in a hash. The hash is always the same for the same data, so it’s kind of like a digital fingerprint. If the data changes at all, even by one letter, the hash also changes. This makes changing the block impossible, because if you would change the data in one computer the hash would not match with the hashes from all the other computers in the distributed network and the information would not be validated (Massessi, 2018).

A good example of hashing in our everyday lives is passwords (Massessi, 2018). We all have an email account and we give the email account provider a password to secure our account. Often the email provider does not save our password, but instead saves the hash of the password we give when we create the account. When we are logging in they hash the password we give them and compare it to the hash they have in store. This way, if the email provider is hacked, the hackers won’t get the password only the hashes.

While blockchain is theoretically impossible to hack, the adjacent application can be hacked. So blockchain is the underlying technology that we use to store the information and an accounting software retrieves the information from the blockchain to create a financial statement, for example, and this accounting software can be hacked.

Smart contracts

One of the big advantages of blockchain is that it enables smart contracts. Szabo coined the term “smart contract” already in the 1990’s (e.g. Tapscott and Tapscott, 2016), but there still isn’t a universally accepted definition of the term. Cong and He (2018) define smart contracts as “digital contracts allowing terms contingent on decentralized consensus that are tamper-proof and typically self-enforcing through automated execution.” So, smart contracts are self-executing contracts that work based on if-this-then-that (IFTTT), meaning that when certain predetermined terms are met the contract executes automatically. An example of this could be automated insurance payments. If certain criteria are met the insured will get the payment without any human involvement.

Another good example of an application of smart contracts in the financial field are smart bonds. Smart bonds could autonomously escrow trades, keep immutable ledger of ownership, auto pay coupons & maturity, and keeps full transaction history available to participants in real-time. Smart bonds would also enable people to invest in bonds with smaller amounts of money, thus opening up the market for a lot more people (Launay, 2018).

Blockchain in businesses

As earlier mentioned, there isn’t a lot of prior research on real-life applications on blockchain other than Bitcoin. Blockchain can, however, in theory be applied to multiple different business ideas, and there are a lot of applications being developed. While blockchain can be public or private and permissioned or permissionless; businesses would mostly benefit from private, permissioned networks (McKinsey and Company, 2018). This would mean that only the companies or individuals involved in the business could join the network and everybody would have permission to see only their own transactions. Bitcoin is a public, permissionless network that is free to download, install, and run on a computer server. This means that anybody can join the network and make transactions.

To join a private network, individuals must verify their identities and be approved by the other members of the blockchain (Smith, 2018). An insurance company could, for example, set up a blockchain network and then approve its clients and care facilities to be members. The
clients would, of course, only see their own insurance information. If the insurance company used smart contracts, insurance payments could be paid automatically through the blockchain network using smart contract as mentioned earlier.

Businesses would benefit from the real time availability of data, encryption, and security of said information. Benefits of blockchain also include reduction of business friction, and delivery of information to interested parties in a more efficient way. The elimination or reduction of intermediaries would save time and money and, in this way, create value to the end user of the information. Private blockchains could also grant review rights to external entities, such as auditors (Smith, 2018).

**Blockchain in the financial services**

Financial services’ core functions of verifying and transferring financial information and assets very closely align with blockchain’s core transformative impact (McKinsey and Company, 2018). Therefore, blockchain can be a disruptive technology especially in the fields of finance and accounting. Blockchain promises to prevent fraud, increase security, trust, and transparency; saving time and money for all parties. But as blockchain is still an immature technology the applications are mostly experimental or theoretical.

**Blockchain in Accounting and Auditing**

Smith (2018) provides an analysis on the implications of blockchain in the field of accounting, auditing, and attestation. The current audit methodology has two shortcomings: transactions and accounts are verified using sampling, meaning that not all transactions and accounts are actually verified. This means that auditors can only give reasonable assurances as opposed to a complete feedback on the performance of the organization. With blockchain technology these shortcomings can be improved upon. The transaction data in the blockchain is already validated by the transaction parties and approved by the consensus mechanism. As the data cannot be altered, as it is timestamped and hashed, auditors basically have a ready-made audit trail to examine. This way confirmations will no longer be necessary either. Blockchain also enables the development of continuous auditing of for example inventories (Smith, 2018).

The Big 4 audit firms have all started to develop blockchain based applications. According to Smith (2018) KPMG started to work on a blockchain in 2016 and partnered with IBM Watson to begin automating and streamlining audit processes and examinations. PwC and Deloitte started developing blockchain applications already in 2014. PwC is testing different blockchain technologies and advising clients on their various uses. Deloitte is developing an internal application. EY partnered with Accenture and is experimenting with editable blockchains. Each of the Big 4 companies seems to acknowledge the disruptive power of blockchain. They are piloting private, public and permissioned blockchain technologies to better adapt to client needs (Karajovic, Kim and Lasksowski, 2017).

**Blockchain in Finance**

As mentioned earlier, blockchain technology was initially created to support Bitcoin trade. The fundamental idea of Bitcoin (to eliminate intermediaries, be anonymous, and trust a system without legal protection) might not be applicable in other industries. Blockchain technology, however, can be implemented by itself. Financial markets are characterized by a system of “consensus-by-reconciliation”; transactions are verified and validated by the counterparty. Consequently, financial markets aren’t built on absolute trust in the market or competitors.
Blockchain technology could, in theory, be applied to reduce risks and costs by enabling smart contracts, digital rights management, and attractive new business models (Trautman, 2016 and Morini, 2016). At the 2016 World Economic Forum financial leaders predicted that “cash in ten years probably won’t exist” and the implementation of blockchain on a larger scale. According to cryptocurrency exchange website coinnmarketcap.com, the combined market capitalization of cryptocurrencies was $8.629 billion in 2016 (Trautman, 2016). On March 1st, 2019, the market capitalization was approximately $130,293,615,515 according to the same exchange. Cryptocurrencies are trending and evolving; creating the need for a structured and regulated market.

Friedlmaier et al. (2018) conduct a study aiming to map the impact of blockchain on various industries. The authors study a sample of 1140 startups that have implemented blockchain technology to examine industry sector, application of technology, and funding. The findings show that 42.2% of the sample companies represent the finance and insurance industry. The applications include financial exchanges and trading (181 companies), payment processing (63 companies), financial services (59 companies) and wallet (29 companies) among others. The Finance and Insurance Industry is also the industry that receives the largest venture capital funding, with $805.60 million. Approximately 50% of all venture capital funding came from the United States; a country that welcomes blockchain innovation and encourage innovation clusters to develop.

**Real-life applications of blockchain**

In this section we will describe a few of the blockchain applications we find interesting that are being developed and tested.

*The Swedish Land Registry*

Swedish Authorities have a vision to digitalize the Swedish Land Registry and base property transactions on smart contracts. An innovative project to launch an application to serve as an interface for all parties involved was started in 2016. The project is a collaboration between the Swedish Land Ownership Authority, two Financial Institutions, a Telecom Company, a Blockchain start-up, an IT Company, the Swedish Tag Agency, a Real Estate Broker and a Consulting Firm. The Lantmäteriet App would enable quick ownership-status checks, effective information sharing, and smooth signing of contracts using digital signatures. Important documents would no longer be sent by regular among the different parties, instead they would be neatly and securely stored in the App. Today, the system requires 3-6 months from signing the contract until ownership status is transferred. Up to 10% of applications are denied due to errors in contracts. Smart contracts would decrease the amount of errors, and consequently make the process faster and more secure. A successful trial was conducted in June 2018; ownership of a property on the Swedish Island of Gotland was successfully transferred using the Application. Due to lack of regulations and other practicalities, the new system has not yet been implemented (Kairos Future, 2017).

*Microsoft and Ernst & Young*

In 2018, it was reported that Microsoft and Ernst & Young (EY) are collaborating to launch a blockchain to alleviate problems afflicted with content rights and management of royalties. The aim is to eliminate intermediaries and let funds flow from users to the person with the copyright
for the property. The system will be based on smart contracts, increasing trust and transparency between actors. EY claims that the network will have the capacity to process millions of transactions per day. There are 86400 seconds in a day; indicating that the system would have to process 11 transactions per second on average to reach the 1 million mark. This is theoretically in line with the findings of Xu et al. (2016); public blockchains, like Bitcoin, have the capacity to process 3-20 transactions per second on average. EY has, however, not provided any real research regarding what the estimates are based on.

**The Australian Stock Exchange**

In 2017, the Australian Stock Exchange ASX, pronounced that they would replace their existing clearing and settlement system with a blockchain-based system in 2020. The new system is based on Digital Asset’s (a New York based fintech company) distributed ledger technology and will introduce 50 new features that will lead to cost reductions. It allows settlement participants on both sides to pre-match the transaction earlier in the settlement period without committing the transaction for settlement. The new system will be taken into use in a two-and-a-half-year period. According to the current ASX managing director and CEO, Australian Stock Exchange will be the world’s first major stock exchange to integrate blockchain technology. (Williamson, 2018) In 2019 ASX announced that the system update would have to be delayed by six months to devote more time for user development and testing (Reuters, 2019).

**Criticism of Blockchain**

**Environment & Scalability**

Blockchain, specifically Bitcoin mining, is frequently criticized for its environmental impact. Mishra, Jacob & Radhakrishnan (2017) conduct a study to map the energy consumption of bitcoin mining. The study covers a 4-year period, lasting from September 2014 to November 2018. Information is obtained from the Blockchain.com website and the public mining pool Slushpool. Estimates regarding total energy consumption are based on number of transactions, number of miners and the complexity of the cryptographic puzzle. It is assumed that miners will need more efficient and energy-consuming computers to stay competitive. The authors claim that the system will require at least 9.92 Gigawatt to process 100 million bitcoin transfers per week. Blockchain technology has, until now, failed to gain any significant market power. Consequently, it is difficult to comprehend the scale of the environmental impact.

If Blockchain technology were to be implemented in a larger scale, scalability is an obstacle to overcome. Xu et al. (2016) claim that public blockchains, like Bitcoin, has the capacity to process 3-20 transactions per second on average. This is significantly fewer than the 2000 transactions VISA has the capacity to process per second. Catalini & Tucker (2018) acknowledge that tensions between miners and developers of applications regarding scalability already exists.

**Trust & Security**

Catalini and Tucker (2018) discuss the issue of trust in blockchain systems by presenting an optimistic and a pessimistic perspective. The main question is whether a distributed ledger system can replace trusted traditional intermediaries. The optimistic view acknowledges the shared access to information and possibilities for collaboration and growth. Blockchains remain competitive thanks to forking; if users are unhappy with the current blockchain, resources can
be allocated to creating a new superior blockchain containing the same information. The pessimistic view presents the dangers associated with Bitcoin mining. As blockchain technology trusts anonymous miners to process transactions, theoretically this means that the person accountable for possible breaches of security can remain anonymous.

Stinchcombe (2018) questions the accuracy and integrity of data stored on the blockchain. The example of purchasing an e-book using smart contracts is used; how can you trust that the system is audited in a way that ensures that the transaction is correct? Who is responsible for errors in the smart contract when there are no intermediaries? Another example introduced is a theoretical voting system based on blockchain. It is argued that developing countries would benefit from an incorruptible and fair voting system based on blockchain. The question is: can an Afghan villager be sure that the vote was registered and counted correctly based on information in an application? Applying blockchain on a wider scale would require a responsibility from “regular users”; they will need sufficient software security and technical skills. The main problem is that there is no way of assuring that data stored on a blockchain is correct. In the context of supply chain blockchain: if a farmer, responsible for putting data into the supply blockchain, claims his mangos are organic, how can we be sure that they in fact are organic, and not sprayed with pesticides?

Blockchain is frequently criticized for the occurrence of 51% attacks. When an individual miner or mining pool control more than 50% the mining power, they can manipulate the system to their advantage. If a 51% attack occurs, ownership of virtual assets can be transferred. “The lie becomes the truth” and the blockchain is manipulated. The occurrence of 51% attacks raises the question of whether we can trust data stored in a blockchain (Boireau, 2018).

Cryptocurrencies, most notably Bitcoin, does not have banking intermediaries. Bitcoin trading builds on trust in the blockchain system and people within the system. Boireau (2018) claims that permissioned blockchain systems are an easy target for hackers. A permissioned network, favored among financial institutions, is a closed network that you gain access to by presenting a private key (Yeoh, 2017). If a hacker gains control of a private key it is irrelevant how secure the blockchain is. In 2016, Hong Kong based cryptocurrency Exchange Bitfinex was hacked, resulting in Bitcoin equivalent to $75 million being stolen (Popper, 2017). The threat of hackers is relevant to all cryptocurrency exchanges and corporations considering blockchain implementation. Boireau (2018) suggests implementing Hardware Security Modules to protect blockchain; this is the technology used to verify Personal Identification Numbers when withdrawing money from an ATM.

**Regulation**

Blockchain technology offers new solutions to process and store personal data. Herian (2018) discuss the impact of the EU General Data Protection Regulation (GDPR) on Blockchain. The GDPR framework was introduced in May 2018, it aims to give back control over personal data to the subjects. The idea is that no personal data can be processed or stored without the explicit consent of the person in question. Another key feature of GDPR is the “right to be forgotten”, indicating that all personal data can be erased from the system. GDPR undermines business applications of blockchain technology, this is due to the fact that GDPR is in direct conflict with the notion that no data in a block can be erased or tampered with.

Lack of regulation remains an obstacle for implementation of blockchain technology. Legislation regarding blockchain is still its infancy; the field is dominated by technical codes, lacking the consequences for non-compliance associated with traditional legal codes (Yeoh, 2017). In the European Union, a Virtual Currency Task Force has been created and virtual currency exchanges are subject to the European Anti-Money Laundering Directive. The EU has, however, ruled that cryptocurrencies aren’t subject to value-added-tax (Blemus, 2017). In
the United States of America, regulations are imposed by the Federal Reserve, The Securities and Exchange Commission, the Treasury Department and States. One notable example of state level legislation is the BitLicense, a framework imposed by the state financial regulator in New York. The goal of BitLicense is for corporations to fulfill requirements to obtain a license. The Securities and Exchange Commission published a guidance in July 2017 stating that under certain circumstances virtual tokens can be considered securities. The EU and the US both hesitate to impose strict regulations, fearing that innovation will be damaged. Japan remains the only country to officially accept virtual currencies as a legitimate method of payment (Yeoh, 2017) (Blemus, 2017).

Is blockchain just an overhyped phenomenon?

As previously mentioned, traditional blockchain technology supporting Bitcoin will have to develop to be applicable in other industries (Morini, 2016). Experts claim that features of Blockchain are already available in different forms, therefore blockchain as a revolution is unrealistic.

Philip Hammond, the UK Chancellor of the Exchequer, made headlines when he suggested that Blockchain technology could solve the Brexit border issues; “There is technology becoming available, … I don’t claim to be an expert on it, but the most obvious technology is blockchain…”. The British Government are considering Blockchain technology to monitor the border between Northern Ireland and The Republic of Ireland. The idea is that tariffs would be paid online in advance and all goods registered, and consequently the border would remain open and digitally monitored. Hammond’s statement was mocked for being unrealistic and naïve. Blockchain technology remains “a wildcard”; the system is not developed enough to be implemented on such a scale and the digital monitoring is a regulatory grey area (Harris & Chu, 2019).

The example above illustrates a key issue when discussing blockchain; blockchain technology is not a revolutionary power or game-changer in itself, it is up to us humans to create the systems. Blockchain as a mechanism to monitor a border is not a bad idea in theory. Problems arise when you consider cost of implementation, scale of the system, and the legality of surveillance.

Conclusion and future outlook

In the previous sections the technological features of blockchain, possible applications in finance and accounting, real-life examples, and criticism of the technology were presented. The technological features of blockchain are praised for enhancing speed and security by enabling smart contracts (Trautman, 2016). Due to scalability issues, lacking regulation and security threats some question if blockchain technology is suitable to implement outside the bitcoin context (Morini, 2016). So, is blockchain a revolution or just a hype?

The expression “The Sky is the Limit” is a cliché, but when discussing the future of blockchain it is suitable. If blockchain technology manages to overcome the obstacles discussed in this paper, there is no telling what we might achieve with it. Institutions, governments, authorities and corporations are eager to present innovative blockchain applications. Whether these new innovations and ambitious projects will ever be applied in practice is a different debate. As pointed out by Herian (2018), Yeoh, (2017) and Blemus (2017) stricter regulations regarding blockchain will have to be imposed to enable future application. This is in line with Stinchcombe (2018), who raises the question whether we can verify that data in a blockchain is accurate and transactions audited correctly. Trust in the blockchain is fundamental for its very
survival. The other problems (like scalability, energy consumption and security) can theoretically be solved by powerful computers and improved software security systems. Trust in a system, on the other hand, is built over a longer time-period. A blockchain with paranoid users and anonymous miners will probably not enhance collaboration and a sharing-economy.

Smith (2018) argues that it is not possible to fully project or analyse the implications of blockchain technology on the accounting profession yet. While we cannot accurately predict the future of blockchain technology, we do know that the future in general is digital. At the 2018 World Economic Forum in Davos, 100% of the participants believed that even if the cryptocurrency bubble bursts, the token economy will prevail (World Economic Forum, 2018). The fact remains that the increasing amount of data and number of transactions will require new innovative systems. It might very well be that blockchain isn’t the right technology to revolutionize the industry, but at least it’s a step in the right direction.

We urge academics, practitioners and authorities to continue researching, innovating and developing blockchain technology, applications based on blockchain and smart contracts, and the regulatory framework for blockchain and its applications. We especially call for more efforts to be put in the resolution of the obstacles outlined in this paper.

References


FINTECHS: THEIR VALUE PROMISES AND DISRUPTIVE POTENTIAL

SARA LAAHANEN, EEMIL YRJÄNÄ, MINNA MARTIKAINEN AND OTHMAR M LEHNER (EDITORS)

1 Hanken School of Economics, Helsinki
2 University of Applied Sciences Upper Austria and Hanken School of Economics, Helsinki

Abstract: In the last few years technological advancements have occurred at a rapid pace. The financial service sector is experiencing fundamental changes due to technological advancements and digitization. Traditional financial institutions are now facing competition by fintech companies. Fintech companies are filling the gaps left by traditional financial institutions, applying technology and making financial services more efficient, intelligent and customer-oriented. Fintech solutions are also enabling financial inclusion. However, there is ongoing concern regarding regulation and trust of fintech companies.

In this paper, we will focus on how fintech have and will change the financial service sector. We will provide a better knowledge of the current and future developments of fintech and also consider some critical voices from society.

Keywords: Financial technology, Fintech, Financial industry

Introduction

In past years technology has been developing rapidly. The financial service sector is experiencing radical changes in an increasing pace due to the constantly evolving technologies and digitization. In recent years traditional financial institutions have faced competition by so-called fintech companies (Green, 2017). Fintech is an abbreviation of financial technology, and according to the Oxford English Dictionary (OED), it is defined as ‘Computer programs and other technology used to support or enable banking and financial services. Fintech companies are companies that apply technology to improve financial activities (Marous, 2018). All financial institutions are increasingly starting to rely on technology, but in fintech companies, technology-driven innovation is at the core of the business. The fintech sector comprises Peer-to-Peer lending, crowdfunding platforms, wealth- and asset management platforms, cryptocurrency, mobile payment platforms etc. (Moholkar, 2018).

The use of technology in the financial service sector is not a recent trend. Technology has long been the core of banking innovations, indeed the second half of the 20th century was filled with continued innovation and application of technology in the financial service sector. Already in 1950s credit cards were introduced to the market. The decades after the 1950s saw innovations such as ATMs, electronic stock trading, more sophisticated data, and record-keeping systems and e-commerce, all relying on technology. While all these innovations became widely used, they never threatened the banking sector (Desai, 2015).

After the financial crisis in 2008 traditional financial institutions, such as banks, had to cope with more rigid requirements, and there was no room for innovation. At the same time technology was experiencing an exceptional boom. When banks got back on their feet after the crisis, there was a substantial gap between technologies offered by banks and the rising standards and demands of modern customers (The Future of Things, 2017).
Fintech companies are now filling the gaps left by traditional financial institutions, making financial services more efficient, intelligent and significantly improving the user experience (Green, 2017). They are changing the financial service sector in fundamental ways. The fundamental changes are everything from investment management to raising capital to the very form of currency. Fintech has lowered the barriers to entry and expanded access to financial services (Dong & Min, 2018). Furthermore, fintech is enabling financial inclusion by providing financial services to areas that are underserved by banks and where the local economy is more challenging. With financial inclusion, we refer to individuals and businesses having access to financial products and services, such as bank accounts, loans, and credits (Jagatiani & Lemieux, 2018).

In recent years, there has been an increasing interest in how fintech is going to change the financial service sector. Currently, we are at a point where retail financial services are being further digitized via mobile wallets, robo-advisors, we have equity crowdfunding platforms and online lending platforms. In terms of innovation speed, traditional financial institutions struggle to keep up with fintech companies. This is mainly due to regulatory reasons and the internal structures of banks (Seeburn, 2017). As the services offered by fintech companies are replacing traditional banking services, and banks cannot keep pace in terms of innovation speed, a collaboration between fintech companies and banks might be the best way to tackle this issue (Marous, 2018).

Fintech solutions and technological innovations are now more than ever disrupting the financial world. The changes are relevant for all of us, as they will affect the whole financial service sector. In today’s digital age, artificial intelligence, machine learning, and big data are becoming central to fintech solutions (Green, 2017). Blockchain will create new opportunities for innovation and growth in the fintech sector and decrease costs and reduce cyber risks. These changes already are affecting and will in the near future affect all of us (Sharma, 2018).

This paper will focus on the value promises and the disruptive potential of fintech. We will focus on how fintech has and how it will change the financial service sector. The paper will provide a better knowledge of the current and future developments of fintech and also consider some critical voices from society.

The remainder of the work is organized as follows. The next section will provide some insights into current developments in fintech. After that, we will present some real-life applications of current fintech solutions. In section 4, we will present some ongoing research within the field. Further, in section 5, we will consider some critical voices from the society. The final section concludes and discusses the potential future of fintechs.

**Current developments**

As already stated, fintech is not a brand-new concept, because its history originates back to early credit cards and onwards. However, recent developments and innovations in technology, such as smart computing, artificial intelligence, cloud computing, Big Data etc. have presented remarkable opportunities for fintech’s and for new startups in the industry. The modern technologies implemented for the financial industry have remarkably not only cut down the costs of various processes but speed up them as well. Artificial intelligence can in a modern business world execute many different, simple and more complex tasks, leaving more time for the matters that need more human effort, for example understanding human behaviour or culture.

The technologies that are implemented by fintech are simplifying the processes, which leads to time savings and also cost efficiency. Many applications are based on electronically executed payments, minimizing the need for cash or paper invoices. For a variety of companies
this makes their day-to-day activities much easier and faster, but also more reliable when electronic transactions and data can be more securely verified, recorded and stored.

Consumers are also benefitting from these emerging technologies, that are there to make their day to day lives smoother and easier. Applications for mobile banking and mobile cashless payments are implemented to smoothen the processes of paying purchases from stores and peer to peer payment transactions between consumers. Fintech solutions pursuit to simplify and speeding up the process of money movement, whether it is in business to business, business to customer or peer to peer segments.

It is a widely known fact that fintech startups pose a significant threat to traditional banks, because of the simple fact that several fintech innovations deletes the intermediary from the process, in this case, the bank. Banks have noticed the opportunities with the new fintech innovations, and several banks have invested in these new innovations in order to either pursuit future revenue or penetrate new markets with new services (Desai, 2015b). Banks have organized for example, pitching competitions for new startups to present their ideas and innovations, and the banks have then selected the ones that most probably would succeed and invested in those. Why banks are investing in new fintech startups is not only because of the significant threat these startups pose to banks, but because the banks have something important, they can offer for these new startups, that is, trust and reputation. Big traditional banks have a long, possibly several hundred years long, history behind them, and during this time, they have obtained a wide knowledge and expertise over the market and in addition, a vast clientele. These key factors are something the new fintech startups lack. For example, in many cases, when consumer has excess funds they want to invest or they are looking for a mortgage, they turn to banks for these. Therefore, this trust and good reputation is something that the new fintech startups truly need in their early stage operations. In contrary, what fintech startups can offer the banks, is innovation and capability to try new ideas. Because of the long history and complex corporate structure and strict regulations, the traditional banks have restraints concerning new innovations. Several banks have a good reputation they are maintaining, and starting a new endeavor, that might fail, would have a significantly negative effect on that reputation and trust they possess from their clients. By investing in these new fintech startups the banks are combining the strengths of the two, reputation and market insights combined with ability to innovate and try (Desai, 2015b).

**Real life applications**

In the following chapter we are going to present the main sectors of fintech with the help of examples and real-life applications of these new innovations. The main sectors of fintech that we are going to examine can be seen in the table below.
Table 1: Main sectors of fintech (Source: Authors)

**Internet & mobile banking**

Modern banking has already for a longer time been relying on internet, and many banks have moved majority of services they provide online. This has led to banks closing down their branch offices, especially in less populated regions. In several situations, where customers need to be in contact with bank personnel, internet banking enables that the meetings are conducted online through a webcam or on the phone and personal identification is being done online, this gives the customers the ability not having to be physically at the bank’s office. Several other daily routines have also been moved online, such as paying your bills. Internet banking gives the ability to pay your bills with your computer wherever you are at any given time. E-commerce has also been positively affected from internet banking, when customers can pay their purchases online through their bank directly after ordering their goods online.

Mobile banking refers to the situation where customers use an application on their mobile phone or tablet for conducting transactions in their bank. With mobile banking applications customers can access their bank accounts and conduct transactions for example paying bills or purchases. These applications can also be used for personal identification on internet banking services online. For example, Nordea has an application called Nordea Codes (Finnish Nordea Tunnusluvut), which consumer can use for identification and verifying transactions. Several mobile banking applications (e.g. Nordea Mobile) have the opportunity to take a picture of the barcode in the bill with your mobile phone and the application retrieves all information, bank accounts, reference number, amount, due date etc. All that is left for the consumer is to verify the transaction with an application such as the Nordea Codes application.

**Smart finance management**

The technology used in these applications enables users to more easily have control over their spending and have practical tools to more usefully budget their daily use of money. Applications such as Monzo or Nordea Wallet makes clear graphs of how much the user have spent on food or clothes etc. at a given time. These applications categorize the purchases according to their nature, and according to the specific card the user is using if they have multiple cards. These applications enable Smart Finance Management for consumers in
situations where they are able to budget their expenditure easily with the help of graphs and budget targets etc. and can easily see how much they have on their bank account and on different cards.

Innovative payments

New innovations in fintech’s enable transactions to occur at a much faster pace than before. Applications for innovative payments rely on cashless payments, where consumers can pay their purchases with their smart phones through applications such as Mobile Pay or Apple Pay or Monzo. Mobile Pay enables consumer pay even for other users who also uses the same application. For example, when paying purchases in a shop the customer shows their smart phone near the payment terminal and verifies the transaction. The Monzo app enables users to split their bills, for example when paying a bill in a restaurant, one user can pay the entire bill for the restaurant and add all the other diners who was part of the bill in the application and the application then sends them a payment request to pay back to the person who paid the bill for the restaurant.

Peer to peer lending

FinTech has also made Peer to Peer lending faster and easier. Individuals can easily apply for a loan of smaller amounts without having to go through time consuming process in the bank. Platform called Upstart connects people in need of money with people who are willing to lend money. Lender fills an online application, which is then assessed and given a risk and credit rating and once the application is approved the lender receives options of investors to choose from.

Table 2: Peer to Peer lending process (Source: Authors)

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online application filled by lender</td>
<td></td>
</tr>
<tr>
<td>Lender receives options of investors</td>
<td></td>
</tr>
<tr>
<td>Lender chooses the most suitable option and receives the loan</td>
<td></td>
</tr>
<tr>
<td>Application assessed by P2P firm and given risk and credit rating</td>
<td></td>
</tr>
<tr>
<td>Once approved, choices given to lender</td>
<td></td>
</tr>
</tbody>
</table>

This process is much quicker and easier for the lender, and in addition for the people who are lending the money this form of lending enables a better return for their investment than a traditional bank would give (Upstart 2019). However, with higher returns comes higher risks, there is higher risk of default, that the lender is not able to pay back the original loan. This is a result of the fact that many of the lenders, who tries to find financing from a Peer to Peer lending platform would most probably not receive a loan from a traditional bank.
Insurtech

The insurance industry has also been affected by FinTech’s, which has led to a new term Insurtech. Similar to other fintech innovations, insurtech startups pursue to offer their customers better targeted services and products. Personal identification through mobile banking applications enable users to buy insurance policies online, without having to physically visit an insurance company. Technology has carried the insurance industry forward in other ways as well, for instance, a company called Root offers their customers car insurance policies that are being based on how they drive. With the help of telematics, the speed and geographical location and other data of the car is recorded and stored, and the insurance premiums are based on that and not for example an age or gender (Root 2019). In addition, insurtech companies offer insurances for so called “micro-events” for example if a customer wants to borrow their friends’ car, they can now buy an insurance for specifically that event. This kind of targeting would be hard or even impossible for bigger traditional insurance companies because of their vast clientele, who they have to be able to serve as larger clusters of customers and not as individuals.

Robo advisory and Artificial Intelligence

Recent advancements in Artificial Intelligence and Data analytics have been a significant leap forward for Fintechs. Modern investment advisory services can provide their customers Robo advisory services. These Robo advisors provide algorithm-based portfolio management, that can fast and cost effective provide the customer with investment advisory and asset management. Further advantages with these are that they are not time or place dependent, while customers use these services wherever and whenever. Robo advisors can be seen fitting between time consuming DIY investing and expensive personal advisory, which means that there is a substantial market for this kind of services. Robo advisory services are also being provided not only for consumers but also for businesses to support the management with their investment decisions. A company called Empirica offers wealth managers an intelligent robo-advisory platform, that uses algorithms and Artificial Intelligence to find the best alternatives and insights about investment alternatives and future market conditions (Empirica 2018).

Business to Business solutions

Simplifying the processes is also the key factor in B2B fintechs. Minimizing paper and speeding up the processes is a significant advantage that is a result of the new technological innovations. E-Invoicing has minimized paper in companies, when invoices gets sent to a platform instead of in paper per mail. For example, company called Basware offer different platform solutions for companies to process their invoices. Some applications even enable automated processing and posting of invoices, without human involvement in the process, which is not only time saving but also cost effective. E-Invoicing together with Electronic Data Interchange (EDI) presents significant opportunities for companies to speed up their processes. For example, EDI-Invoses in SAP gets automatically processed and posted both in the buying and in the selling company, because of the data interchange that enables both parties to know basic information about each other’s products, such as product codes, price, measurements etc. The software cross checks the purchase order with the invoice and with the order acknowledgement and when everything is in order and there are not any differences in prices or quantities, the invoice gets posted in correct general ledger accounts automatically and the invoice gets transferred to accounts payable (SAP 2006).
Cloud based Enterprise Resource Planning software, such as SAP HANA, are also making the operations more flexible and effective for many firms. When a company has their ERP in a cloud, they can access it more flexible and the data is more securely stored in possibly several locations. Other key advantages with cloud-based ERP is that this way the company can simplify processes when everything can be done with one single ERP. Furthermore, the cost efficiency is also significant because of the decrease in data management costs (SAP 2018). Fintech offers especially effective solutions for international companies, while enabling Blockchain-based cross-border payment systems that will result in almost instant transactions internationally.

Fintech presents companies also to new forms of financing. Firms or individuals with new endeavors can find financing for their projects through various crowdfunding platforms, such as Kickstarter, Gofundme or Indiegogo. Some of these offer instant withdrawal and around the clock support services.

**Big data and Artificial Intelligence**

For a while now companies have been able to take advantages of Big Data to improve their operations. With the help of Big Data companies can gather a vast amount of data either from their customers or from the market, in order to pin point customer behavior or market trends and this way fine tune their business to better meet the demands of the customers and the market. In the modern digitalized world, every transaction leaves some sort of digital trail, which means that a lot of data exists of these transactions. With the help of Predictive Analytics and AI this data can effectively be analyzed to explore the behavior of the market or the customers in pursuit of a better position on the market. Several companies have also used Predictive Analytics or AI based applications against money laundering and for fraud detection. This results a more secure and less riskier business landscape for today’s companies. For example, client risk profiles are being made much faster and with a much broader perspective than before with the help of AI (Hudson 2018). A significant advantage of this is that the performance is constant and lacks the possibility of human error. Big Data is also useful for investment decisions for especially larger companies, who have the capability to analyze and process the vast amount of data. By using this data managers can make better informed investment decisions (Begena, Farboodi, Veldkamp 2018).
Ongoing research

Fintech is a fast-growing research topic, but as fintech is a new sector, there has not yet been that much research conducted in the field. We are going to examine ongoing research from two perspectives. First, we will present some research that examines the value promise of fintechs and then we are going to present research that examines the risks of fintechs.

Research examining value promises of fintechs

Due to the young age of these new technological innovations that are shaping the modern financial industry in form of fintech, such as cloud computing, AI, data analytics etc., there is not that vast variety of research about the effects they have on the industry. But recent studies have stated that modern fintech will not only change the financial industry remarkably, but it will rather revolutionize the entire financial industry. Paper by Gomber et al. (2018) stated that a remarkable revolution of the financial industry is about to occur due to the great improvements in customer centricity, efficiency and informedness. Furthermore, firms that are not able to keep up with this Fintech Revolution will be having difficult times ahead of them. Gomber et al. (2018) pointed out the vast scale of investments made on Fintech startups. According to statistics retrieved from VentureScanner a total of 1537 startups in 64 different countries received an amount of 80,4 billion US dollars in venture capital funding for their fintech innovation activities. The authors pin pointed three key areas that are the main forces for fintech advancement, and they are: technology innovation, process disruption and services transformation. The advantages created from these factors are significantly simplifying the processes for companies and making the lives of consumers easier.

Another paper studying the advantages of fintech by Vlad Brătășanu (2017) examined the financial industry competitive dynamics drift. The financial services are being changed due to new innovations and technologies that creates products and services for businesses and consumers with the help of data management and digital platforms. The new innovations are characterized by speed, efficiency and client-oriented strategies. The author stated that several services today are being transformed from face-to-face interaction to interaction happening online and possibly even automated. Another key take away from the article is that these technological innovations causes companies demands and challenges to not only keep up with the industry evolution, but also take advantage of these technological innovations and tools in order to better meet the demands of the customers and create customer-centric businesses. Companies with the capabilities to benefit from AI and analytics tools will have a major advantage understanding customer behaviour and creating more thorough client risk profiles and investment decisions.

The study Do fintech lenders penetrate areas that are underserved by traditional banks by Julapa Jagatiani and Catharine Lemieux (2018) examine the impact of fintech lending on the availability of unsecured consumer credit. The study investigates whether LendingClub, one of the biggest players in the peer-to-peer lending space, penetrate to potentially underserved areas, where there is less competition in banking services. The findings show that fintech lenders have penetrated areas that could benefit from additional credit supply. In addition, the study indicates that LendingClub had a higher market share in areas where economic variables indicated more challenging environment. Thus, the findings of the paper provide evidence of fintech lenders having a positive impact on underserved areas and areas where the local economy is more challenging. The study does not investigate in potential negative aspects related to fintech lenders, but the authors point out that regulations are needed for financial stability and consumer protection, and the lack of regulations is actually an ongoing concern.
Research examining risks of fintechs

The financial industry can be seen as being constrained by regulations and restrictions resulted due to the financial crisis 2008. These regulations and restrictions have had a decreasing effect on loans and mortgages for consumers. This has presented an opportunity for fintech startups to fill in the gap. An article by Buchak et al. (2018) presents the characteristics of these fintech solutions, shadow banks, that have the capabilities of the banks without their current regulations and restrictions. The authors found that the market share in mortgage origination from shadow banks has nearly doubled from 30% to 50% during the years 2007 to 2015. The paper explains this rapid growth with the increasing regulation of the traditional banking industry and the technical innovations of the new fintech startups. Key finding in the paper is that shadow banks are more likely to serve clients with a higher risk profile, people that have a higher default probability, these customers would not receive a loan from a traditional bank.

The research paper Evolutionary Approaches and the Construction of Technology-Driven Regulations by Dong and Min (2018) focus on the regulatory problems regarding fintech companies. Dong and Min (2018) indicate that there is a need for regulatory responses to the inherent risks in technology-driven financial innovations. According to Dong and Min (2018) there are insufficient regulatory techniques, outdated laws and conservative regulatory. The problem is that regulations does not keep pace with technological innovations, as technological innovations develops far faster than applicable regulations. Regulations has failed to meet the demands of fintech companies, hence technology-driven regulations will respond to the risks of fintechs. The paper emphasizes the importance of technology-driven regulations focusing on data monitoring and thus enhancing the financial consumers’ rights and interests.

Another article that covers the regulation issue is the research by Hyuan-Sun Ryu (2018). The aim of the study is to provide a better understanding on why people are willing or hesitant to use fintech. To be able to investigate and understand the fintech usage behavior, the users were divided into early adopters and late adopters. The findings show that legal risk was the major reason why people did not have intentions to continue the use of fintech solutions. Convenience was the major reason why people had continuance intention. Legal risk had the strongest significant effect on the fintech continuance intention for early adopters. The study indicates, that the perceived benefit had a much stronger impact on the usage decisions than the perceived risks. The findings also show that users were mainly concerned about regulation and security issues. However, both early adopters and late adopters shared a concern about the lack of consumer protection and operational risk. Thus, the study indicates that fintech companies should improve their reputation by establishing stability and trust.

Critical voices from society

As stated in the previous chapters, technology is strongly influencing the way business is conducted today, and there are some major changes to come in the near future when AI, blockchain and RPA are being further implemented to fintech solutions. However, people tend to resist change to some extent, as people tend to be scared of change. Since today’s technological advancements happen exponentially, people have to adjust to changes far faster than before. Hence, the fear of change is even more major in today’s society (Dickson, 2018).

Some of the primary critical voices of society concerning the change fintech solutions create, is fear of automatization and therefore uncontrollability. When technology is applied to the financial service sector, the fear of not being able to control things is a growing concern. Today it is almost impossible to understand exactly how advanced technologies work, thus people find it scary to completely rely on automated technology. This creates a sense of losing control over things that were handled manually before. In addition, if a company is too
FINTECHS: THEIR VALUE PROMISES AND DISRUPTIVE POTENTIAL

technology based, it can have major consequences in the event of a system malfunction, further illustrating the concern of losing control (Fritscher, 2018).

There is also a big, ongoing debate regarding trust. Major violations of personal data have increased consumer skepticism when it comes to trusting new technologies and fintech companies. Customers personal data becomes easily accessible and huge amounts of data is collected from customers, even information that might not be needed (Demir & Ramkumar, 2018). However, despite the fact that fintech companies might not be held to the same regulations as traditional banks, they still must follow privacy laws (Ismail, 2018).

Another concern is that jobs in the financial service sector might be lost when artificial intelligence is taking over tasks earlier made by humans. Artificial intelligence will reduce the need of employees, by taking over work that requires analysis, consistent applications of decisions and judgment calls. However, advancements in technology and AI limit the possibility for human error, as tasks previously carried out by humans are automated. Despite the criticism, emerging technologies are also creating new jobs (Fletcher & Kreps, 2017).

Lastly, a crucial concern is the lack of regulations. As fintech companies are not considered as traditional financial institutions, current legalization and regulations does not apply on them, and thus it leaves many fintech companies in a so-called grey area. This increases the concern about data privacy and cybersecurity. Further, regulations fail to keep pace with changes in technology. This often leaves new fintech companies to operate in a so-called grey area. This again results in people being unable to trust fintech companies. Regulations should therefore try to keep pace with the rapidly evolving fintech sector. Legislators are improving current privacy laws and also creating new ones, such as the GDPR, in order to hinder companies from misusing data collected from consumers and customers (Global Banking & finance review, 2018).

Conclusion & Future outlook

Technology is fundamentally changing the financial service sector, and the changes are happening faster than ever before. Fintech has already made financial services more efficient, intelligent and customer-oriented and technology is playing a crucial part in our day-to-day lives. However, as mentioned in the previous chapter some fintech companies operate in a so-called grey area. Even previous research (e.g. Ryu, 2018, Dong & Min, 2018) states that there are some concerns regarding the regulations of fintechs. Regulations are not keeping pace with technological innovations, and this is a major issue. The lack of regulations is a concern that definitely needs to be addressed in the near future.

One way of addressing the concern regarding regulation, is to collaborate with banks. In general, traditional banks have better knowledge of regulations and the banking sector as a whole. A collaboration would also bring other advantages, not only for fintech companies but for banks as well. In addition to the better knowledge of regulations, banks have the benefit of larger customer bases, stronger brands, adequate capital and customers’ trust, as they are established and have been on the market for a long time already. Fintech companies in turn, are more efficient, intelligent and better targeting customers. A collaboration between banks and fintech companies would therefore be beneficial for both parties. A collaboration would bring strengths from both banks and fintech companies together and create a stronger entity than either of the parties could be on their own. As stated earlier, banks are already investing in fintech companies, and a deeper collaboration is probably something we will see in the future.

The next decade is likely to see even more financial inclusion. Enabling individuals and companies to successfully manage, save and invest their money will contribute to a better society for all of us (Green, 2017). The findings of the paper by Jagatiani and Lemieux (2018) provide evidence of fintech companies enabling financial inclusion. Fintech is providing access
to financial services for millions of people, who might not normally be able to use financial services (Green, 2017). With a further implementation of blockchain into fintech solutions, it is possible to provide unbanked individuals a valid, easily created online identity, which will allow more individuals to be financially included than ever before. Blockchain will also provide security, thus the data collected will be better secured (Sharma, 2018).

Overall, further implementation of AI and blockchain in fintech solutions can be expected. The improvements we have seen in robots, as well as an improvement in the knowledge about RPA and AI and their potential, will increase the adoption of these in fintech solutions. It is hard to tell what the future holds, but the continuous evolution of technology is inevitable. In what direction this evolution will go can be speculated but not entirely predicted.

References

FINTECHS: THEIR VALUE PROMISES AND DISRUPTIVE POTENTIAL


SAP (2018) SAP HANA. Available at: https://www.sap.com/products/hana.html


REGTECH- A NECESSARY TOOL TO KEEP UP WITH COMPLIANCE AND REGULATORY CHANGES?

ELLINOR JOHANSSON, KONSTA SUTINEN, JULIUS LASSILA, VALTER LANG¹
MINNA MARTIKAINEN¹ AND OTHMAR M LEHNER² (EDITORS)

¹ Hanken School of Economics, Helsinki
² University of Applied Sciences Upper Austria and Hanken School of Economics, Helsinki

Abstract: The discussion about the need for regulation got fuelled after the latest 2008 Global Financial Crisis, with many demanding stricter policies to avoid history from repeating itself. These voices have been partly answered, as a plethora of new policies, regulations and standards has been implemented since then. Drafted under good intentions, these new rules have also shown to have detrimental consequences. Exclusion of potential customers and high barriers of entry are only the side-effects of the rapidly rising costs of compliance that the large set of new regulations have brought upon businesses. RegTechs, a new category of innovations that were before classified as part of FinTech, are tools of the future for complying with regulations. This article describes the past, current and future developments of RegTechs, present some real-life cases of current RegTech companies, and discusses their place in a world of ever-changing rules and policies.

Keywords: RegTech, FinTech, regulation, compliance, Global Financial Crisis, internal auditing, accounting, tax regulation, GDPR, reporting

Introduction

Since the Global Financial Crisis 2008 the financial regulations and regulatory changes have increased to almost unmanageable heights. According to Thomson Reuters (2019) a regulatory alert is issued every 7 minutes. The cost of compliance after the crisis has increased by 60% (Deloitte 2017a) for retail and corporate banks, and the pressure to obtain regulatory effectiveness and compliance, is very high. Today 15-20% of the total business costs consist of costs for compliance, risk and governance (Thomson Reuters, 2017). It’s not just the large amounts of regulations that have become overwhelming but also the complexity of them. (Deloitte, 2017a). Basel III, GDPR, PSD2, MiFID II, BCBS 239 are just some of the new regulations, which have emerged after the crisis. Regulatory changes are poised to increase in the near future, due to the ongoing technological development of the financial sector. Hence, the rapid development of the financial industry combined with growth of the regulatory and compliance burden, creates a demand for new solutions. Technology is affecting the financial industry and how companies operate, by creating new solutions, increasing effectivity and bringing change to how we comply and deal with regulations (Thomson Reuters, 2017). Are RegTechs the answer to the problem and if, what kind of solutions do they offer?

Regulatory Technology or RegTech are technological solutions for compliance and regulation, to improve regulatory processes. It has been present already from the late 1960’s, but in a different form than after the Global Financial Crisis. (Arner, Barberis and Buckley, 2017b). Today RegTech has spread all over, and new solutions are frequently presented. It has
been recognized as a sector with a lot of potential. By 2020 Regtechs are going to represent 34% of all regulatory spending (KPMG, 2018). Despite all possibilities the sector offers, there are a lot of challenges to be addressed, like for instance operational risk especially in handling risk data and a regulatory environment that doesn’t suit the technological environment we have today (Baxter, 2018; Arner et.al 2017a; 2017b; Kavassalis, 2018).

In this article we look at RegTechs and how they can be a solution for the compliance and regulatory burden, especially in the field of accounting, internal auditing and tax regulation. We try to give a broad overview of the subject, present practical solutions, and look at the potential opportunities and threats. Specifically we examine hands on company solutions offering auditing-, tax regulation- and GDPR compliance solutions. Further we present ongoing research and discuss the criticism that surrounds the subject. Existing research so far has mainly focused on the financial sector and look at RegTechs from a legal perspective. (Arner et.al 2017b; Kavuri and Milne, 2018; Micheler and Whaleys, 2018) Furthermore, existing research has also investigated the potential of RegTechs and what needs to change in order to reach the full potential (Arner et.al. 2017b: Yang and Li 2018; Baxter 2018; Kassavallis 2018). This will provide value to practitioners, professionals, researchers and students that are new to the subject, and give them an overview, general knowledge and practical implications.

RegTech- what is it and where does it come from?

Regulatory Technology or RegTech are technological solutions, mainly using information technology for compliance and regulation, to improve regulatory processes. RegTechs aim to help with new and old regulations and manual reporting. Further they deal with risk assessment and management, identity management and control, transaction monitoring, data structuring and fraud prevention like anti money-laundering. (Deloitte 2017; Arner, barberis and Buckley 2017a; 2017b; Yang and Li 2018). When dealing with different regulations the core data, processes and governance are similar, which pinpoints the largest possible benefit of RegTech, namely working in a multi-regulatory environment avoiding duplication of work and increasing efficiency. (Nicoletti, 2017, p.205). However, the sector isn’t really there yet, today most of the RegTech companies focus on specific regulatory challenges, offering solutions for manual reporting and compliance (Arner et.al, 2017a; Deloitte, 2017b).

Possible benefits of RegTechs are lower cost, effective and efficient compliance, accurate information and real time data, flexibility, easy reporting, security and analytics (Hill, 2018). Moreover, they can create business insight and new products and services. RegTechs utilize several upcoming technological advancements, especially with regards to data, like cloud computing, blockchain, machine learning, big data, data mining and analytics just to mention a few (Deloitte 2017b). The selected technological solution is dependent on the problem they are trying to solve, much like fintechs.

Financial technology or FinTech is the use of technology to create new financial solutions (Arner et.al, 2017b). According to Nicoletti (2017) RegTech is a part of Fintech (FinTechs little brother) that deals with regulations. This view is also shared with others like Hill (2018); Baxter (2016); Deloitte (2017b) and Anagnostopoulos (2018). On the other hand, Arner et.al (2017), Nicoletti (2018) and Yang and Li (2018) believe that although RegTech has roots in Fintech it should be considered as an independent sector, because it provides services for different groups not only the financial sector and has other recipients. Fintechs started from the start-up sector and are changing the financial industry with new technological solutions and forcing large financial institutions to change. In contrast RegTechs current aim aren’t to change the industry but to help large institutions and others to deal with their regulatory burden and
compliance. (Hill, 2018, p.312). Hence, the FinTech movement is bottom-up and RegTech top-down (Arner et.al 2017b).

RegTech has been categorized in three phases: RegTech 1.0, RegTech 2.0 and RegTech 3.0. (Arner et.al 2017b; KPMG 2018). RegTech 1.0 refers to the time before 2008 beginning already in the late 1960’s, and refers to technological solutions focusing on internal risk-management and monitoring. This initial development was driven by large financial institutions for their own internal processes, governance and control. The second stage: RegTech 2.0 is where we are today, sparked by The Global Financial Crisis and the regulatory burden and increased costs and complexity that followed. These technological solutions are mainly driven by financial market participants and regulators to address the problems of compliance, reporting and processes. In this phase more data is available and the environment is being more and more digitized, offering possibilities for new regulatory technological solutions. The last phase RegTech 3.0, is predicted to use technology as a tool and rethinking the regulatory environment and framework. Regulators, technology and companies working together and addressing regulation, monitoring and reporting in real time using the same technology and data. In this future phase Know Your Customer (KYC) will develop into Know Your Data (Arner et.al 2017a; 2017b).

Regulations are dependent on the political economy, which operate under constant uncertainty. This uncertainty of what regulators are going to do next create “problems” for companies and makes it hard to deliberate when change occurs and the outlook of it. (Hill, 2018). The financial market, services and institutions are more than ever before formed by the rapid regulatory changes and the new financial environment, which demands a need for regulatory technology to cope with the change (Arner et.al 2017a).

Table 1 Summary of RegTech- what is it and where does it come from? (Source: Authors)

<table>
<thead>
<tr>
<th>Definition</th>
<th>Areas</th>
<th>Technology (examples)</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technological solutions, mainly using information technology for compliance and regulation, to improve regulatory processes.</td>
<td>- Risk assessment</td>
<td>- Artificial intelligence</td>
<td>- Roots in FinTech but should be seen as an independent sector</td>
</tr>
<tr>
<td></td>
<td>- Compliance</td>
<td>- Block chain</td>
<td>- Provides services for different regulation intensive industries not only the Financial sector</td>
</tr>
<tr>
<td></td>
<td>- Reporting</td>
<td>- Cloud computing</td>
<td>- Started by large institutions to deal with the regulatory burden and compliance</td>
</tr>
<tr>
<td></td>
<td>- Auditing</td>
<td>- Machine learning</td>
<td>- Top-down development</td>
</tr>
<tr>
<td></td>
<td>- Identity management and control</td>
<td>- Big data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Transaction monitoring</td>
<td>- Data mining and analytics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Data screening</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Fraud prevention</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The selected technological solution depends on the problem.
The different phases of RegTech

<table>
<thead>
<tr>
<th>RegTech 1.0</th>
<th>RegTech 2.0</th>
<th>RegTech 3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Period from 1960-2008</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Focused mainly on internal risk management and monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Driven by large institutions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Started after the Global Financial Crisis and is the phase we are in today</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Mainly driven by the Financial market</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Focused on solutions for compliance, reporting and processes with the new technology available</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- The future</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Technology as a tool</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Rethinking the regulatory environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- All sectors working together</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- From Know Your Customer to Know Your Data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Current development and potential future

The players on the RegTech market offers solutions for the financial industry but not only, they also focus on other regulation intensive industries and solutions, like for example personal data and the GDPR regulation (Hill, 2018). Most of the companies are still in the start-up phase and the main part of them are at the most three years old. Even though the biggest potential of RegTech, is combining several areas and problems into one (Arner et.al 2017b) the companies at this stage mainly focus one a specific problem. (Deloitte 2017b). It isn’t just the new companies that are forming RegTech, as stated above everything started from in-house development and this is still present today. Companies try to find their own solutions or companies cooperate with, to not be left behind (Thomson Reuters, 2018).

Deloitte (2019) has collected a group of RegTech companies on the market right now, they include a total of 289 companies, with the biggest group being in compliance, followed by identity management & control, risk management, regulatory reporting and transaction monitoring. The geographical distribution is relatively wide, but the most part of the companies can be found in Europe (Deloitte, 2017b; 2019). Currently the RegTech sector is fast growing and it’s estimated to make up for 34 % of all regulatory spending 2020 (KPMG 2018). 2017 Deloitte (2017b) had only listed 80 RegTech companies, which show the same pattern of growth.

To be able to see the actual development amongst companies, we have looked at Thomson Reuters survey report (2019), which included 400 financial service firms. According to the survey, 21 % of the companies think that RegTech most likely impact the compliance at their company followed by on-boarding and KYC. 2017 the answers were completely different, with the main impact being interpretation an impact of regulations and implementation of regulatory changes. A total of 22% of the companies 2017 were developing inside RegTech solutions compared to only 6 % in 2018, and the same pattern can be found in the use of external sources, with 26 % in 2017 and 13 % in 2018. This is an interesting pattern, because intuitively looking at the regulatory environment and the development of the market, it would be expected to have had increased. Although, the companies using a mix and max strategy for RegTech solutions increased from 2017 to 2018 with 7 %. Another interesting remark from the survey was that the companies that reported to have implemented a RegTech solution decreased with 21 %. On the contrary the ones that hadn’t yet implemented any solution but considered to do so increased by 18 % during the same period. Thomson Reuters (2019; 2018) offers an
explanation to the interesting results. In order for a new RegTech system to really work many parts need to be in place, otherwise the risk becomes too high. When developing and going into these new solutions not only the compliance and risk functions need to be addressed but also maintain good outcomes for the customers. (Thomson Reuters 2018; 2019) It could be that we need time, research, development and testing to ensure that all parts are in place, before we are at a point were companies really can embrace all that RegTechs have to offer.

Data and information, is the key in technology driven regulation. The tools for effective data collection and monitoring, need to be in place in order to get the full potential of RegTechs. (Baxter, 2018; Arner et.al 2017a; 2017b; Deloitte 2017b). The traditional regulatory environment especially financial regulations does not match the current financial market and players, and is in need of change to support the technological development to deal with risk and compliance (Yang and Li, 2018). Baxter (2016) recognizes the same pattern that the financial regulations needs to be thought through in order to work together and achieve better regulatory environment with effective compliance, transparency, efficiency and fairness. (Baxter, 2018). Arner et.al (2017a), believe that RegTechs in the future will be able to offer almost real-time applicable regulatory tools, which identify and deal with risk and at the same time offer efficient compliance. Despite all potential companies when dealing with RegTech solutions are going to face operational risk especially in handling risk data (Kavassalis, 2018).

The current and future challenge for companies when it comes to RegTech is to find solutions that create value and work in the long-run. It is important for the industry to realize what change and solutions RegTech may bring to the table, so that they can grow and develop together and not separately. Investing in these solutions are also important to stay in the game, the big chance is coming and it’s important to realize it and act before it’s too late. (Deloitte, 2017b).

Table 2 Current development and potential future summary (Source: Authors)

<table>
<thead>
<tr>
<th>Company characteristics</th>
<th>Development</th>
<th>Potential future</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Companies are still in the start-up phase</td>
<td>- The companies that haven’t yet implemented any RegTech solution are the most optimistic</td>
<td>- Estimated to make up for 34% of all regulatory spending</td>
</tr>
<tr>
<td>- Main part of the companies are at most 3 years old</td>
<td>- The survey show that a mix and match strategy (in-house/external) seems to work the best right now</td>
<td>- Data and information are key factors for technology driven regulation</td>
</tr>
<tr>
<td>- Focus on one single problem</td>
<td>- The results show that it may be harder to implement successful RegTech solutions than initially thought</td>
<td>- The traditional regulatory environment does not match the current financial sector and technological development</td>
</tr>
<tr>
<td>- In-house development still present</td>
<td></td>
<td>- Potential to offer real-time applicable regulatory tools</td>
</tr>
<tr>
<td>- Most companies are in compliance, identity management &amp; control and risk management</td>
<td></td>
<td>- Challenge to find solutions that work in the long-run</td>
</tr>
<tr>
<td>- Relatively wide geographical distribution but focused on Europe</td>
<td></td>
<td>- Important to invest in these solutions to stay in the game</td>
</tr>
<tr>
<td>- The sector is fast growing but only a part of the companies already available has the same growth pattern</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
REGTECH- A NECESSARY TOOL TO KEEP UP WITH COMPLIANCE AND REGULATORY CHANGES?

Cases

The aim of the following case-study is to display real-life applications of Regulation Technologies. The selected case companies, display and solve clear and understandable problems. Moreover, these companies offer regulatory compliance solutions for audit and assurance purposes. The first company offers a solution that complies with GDPR and detects unstructured personal information. The second company, uses a software solution, which allows direct determination of tax effects of an investment, without further calculations. The third company, gives an artificial intelligence powered solution for auditing and internal audit.

Information about firms and their products have gathered from companies’ websites, news articles, magazine articles, and academic papers.

Aigine- GDR compliance

The General Data Protection Regulation GDPR aims to protect personal information of individuals (Burgess, 2019). The new regulation affect companies, and potentially force them to hire additional staff to be able to comply with GDPR accordingly (Burgess, 2019). Burgess (2019), claims that GDPR has already renewed the way firms handle personal data, and personal data issues will and has become a boardroom issue. Aigine offers a solution that might reduce the need for new staff hired for GDPR compliance purposes.

Aigine offers a tool to make complying with the European Data Protection Law GDPR more time efficient. The main change brought by the GDPR, applied to personal data and especially unstructured data sources, which were unregulated in many countries until the new regulation. Whereas from the 25th of May 2018 both structured and unstructured personal data have to be reviewed if it contains personal data or not (Aigine, 2019). Aigine helps in the review process by making it easier to detect personal data in these unstructured documents, like for instance emails and notes in word documents (Lindström, 2018).

Aigine (2019) claim that: “We have invented collaborative cognitive learning, making it possible for you to use our Artificial Intelligence to handle the challenge of unstructured personal data.” It means that Aigine’s competitive edge is to detect personal data from sources that are unstructured and therefore time-consuming to review entirely manually.

The actual process of using Aigine is divided into four stages, filtering, highlighting, assessing, and documenting. In the filtering stage, Aigine scans all documents in the company and separates documents that contain personal data. After that, documents that contain personal data will be forwarded to the responsible person in the organisation. The responsible person does then manually the actual review. When reviewing documents, Aigine highlights all suspected personal information making the actual review more comfortable and more time efficient. In the assessment stage, Aigine uses artificial intelligence to suggest and to help to determine legal grounds for saving personal information. By doing that Aigine makes it possible to assess documents and legal grounds for saving personal information without legal expertise. In the documentation stage, Aigine documents legal grounds for saving personal information in the document. These four stages are presented on the home page of Aigine (2019).

In Sweden, several municipalities have started together a project to use Aigine to comply with GDPR. Peter Mankesiöld (2018), project leader of municipality association Sambruk, highlights that it is essential that the machine does not decide whether there exist legal grounds for saving personal information or not. As an example, he takes up a license plate number of a car owned by a company. If the car can be attached to an employee, it may be personal
information although the firm legally owns the car. According to Mankeskiöld (2018), it is vital that human makes decisions about personal information because human understand better how different circumstances may affect the decision. Mankeskiöld's (2018) concern is understandable, but at the same time, Aigine have also been criticised about the number of human hours needed when using Aigine (Hedqvist, & Månsson, 2018).

Hedqvist, & Månsson (2018) made a case study of challenges and opportunities an Aigine type of software may include. The research question of the study is “What are the challenges and opportunities with using cognitive computing for mapping personal data in order to help comply with the GDPR?” (Hedqvist, & Månsson, 2018, p.4). Authors identified four opportunities cognitive computing may offer. Authors see as an opportunity that cognitive computing can understand both structured and unstructured data. Likewise, the ability of cognitive computing to learn to identify personal data is seen as an opportunity by authors. They see also continuous learning by cognitive computing as an opportunity because it improves the accuracy over time. Authors argue that all these opportunities may lead to increased efficiency which means cost savings. These opportunities are apparent and may lead to substantial resource savings. The fact that the detecting accuracy of personal information evolves due to Artificial intelligence under time the software is used, may end up to the almost as precise detecting accuracy as a human can do. The challenge is that during the period when Aigine learns to detect the right information the actual compliance may be insufficient. Therefore companies ought to weight the risks that are related to insufficient compliance due to deficient detecting of personal information when taking Aigine in use.

Hedqvist, & Månsson (2018) identified four main challenges with using cognitive computing for GDPR compliance purposes. According to authors one of the biggest challenges is that cognitive computing requires human work to learn to detect personal data and to become competent enough. They think that it is also challenging to make accuracy as good as in work made by a human. If the goal is to make accuracy as good as a human is capable, it would require a massive amount of human work to teach cognitive computing to detect the right information (Hedqvist, & Månsson, 2018). Additionally, cognitive computing needs a relatively large quantity of data to be able to learn to detect the right personal data (Hedqvist, & Månsson, 2018).

Based on the criticism of Hedqvist, & Månsson (2018) it seems that the preparation and teaching are vital to begin before the actual use of Aigine. A client company should also have enough data to be able to teach Aigine which is the personal data in the context of the client company. The lack of data could limit the number of potential user companies in a way that companies who do not have stored the data and recently founded companies may not be able to use the Aigine. Potentially, Aigine learns in the future to categorise different contexts using Artificial Intelligence and thereby reduce the amount of training data needed from the client company's side.

**Apiax- Tax Product**

Apiax is a RegTech company that offers advanced tools for compliance of financial regulations. The goal is to make compliance of regulations lean and efficient (Apiax, 2019). Ralf Huber (2018), Legal Lead and Co-Founder of Apiax, describes the possibilities of the Tax Product as “Financial institutions can finally make use of tax calculations in their advisory processes. This is the missing piece in the puzzle of value-added, personalised investment advice.”

The digital Tax Product allows financial advisors to focus more on tax-adjusted returns instead of only focusing on cost-adjusted returns (Shäubli, 2018). According to Huber (2018), the complexity of tax effects have been the issue why financial service providers do not have
focused on tax-adjusted returns, but Reg Tech solutions are now capable to handle that complexity and solve the problem. In practice, it means that it will be possible to estimate the tax effects of an investment directly for example in the meeting of the executive board or an advisory meeting with a client.

Software as Apiax - Tax Product may have a significant impact on the tax advisory industry by making the advisory process much more efficient. Responsibility and credibility issues have to be taken into consideration when a tax advisor is a machine. Andreas Straessle (2018), regulatory engineer of Apiax, says that user can change rules in Apiax to adapt these rules to users desire to take risk. When traditional tax advisors suggest some alternatives, they are often responsible for their suggestions at the reputation level. That type of risk of losing reputation does not exist when interacting with software. Human tax advisors may also tell about tax risks and experiences about similar cases especially when actions are questionable and include a high level of tax risks. Actions that include a substantial amount of tax risk may also be hard to take without knowing previous experiences of other clients. That part of human interaction and its possibilities in tax advising have to be taken into consideration. Apiax type of software may lead to changing demand for tax advisories. The demand for human tax advisors may shift from basic tax issues towards issues that need expertise and experience of difficult and high tax risk transactions. Apiax type of software is going to make tax advisory process much more efficient. However, it may take time until people start to use this type of software and to trust the software’s advises.

Mindbridge - AI Auditor

Mindbridge Ai is a company that offers the first and only AI-powered auditing solution in the world (MindBridge, 2018). Mindbridge Ai auditor uses machine learning and AI techniques to make the auditing process more effortless and efficient (MindBridge, 2018). They offer digital solutions for companies in audit and assurance and internal audit purposes. They have customised product also for companies that offer financial services. Following chapters focus on the internal audit as well as audit and assurance.

The big thing of Ai Auditor is that it analyses the whole dataset of transactions of the company and the analysing time is in minutes. By doing so, the auditor does not have to spend the time to think about the right size of data sample for the actual audit review which is the case in the traditional audit process. When all data has analysed the detection of fraud and mistakes is more accurate and credible. Fathi (2018), CEO of MindBridge, writes how artificial intelligence may help the U.K.’s audit system at the time of major corporate scandals. He argues that by reviewing all company data with AI-powered technology leads to a significant increase in audit quality. Fathi (2018) also offers a solution for mistrust in audit “AI is uniquely poised to fix many of the symptoms of mistrust in audit… As AI eliminates human bias from all stages of data analysis, identifying anomalies according to accepted audit standards and going beyond to spot risks that have never been conceived by a human brain, the technology will help firms of all sizes increase their audit quality and risk assurance, while decreasing engagement times.”

AI Auditor also offers many possibilities for internal audit. The detection of fraud or internal policy violations is much faster and easier. Even though internal and external audit processes will become more efficient and of better quality, it may not lead to substantial monetary savings. Reason for that is the current price level of AI Auditor service.

The price of AI Auditor Software is from £4200 to £30000 per year (The Digital Marketplace, 2018). The price of one run of audit material or a case file analysis is £4200 (The Digital Marketplace, 2018). In that case, the results are available for analysis a one year.
Instead, for unlimited engagements or case files for one year the user have to pay £120 000 per department (The Digital Marketplace, 2018). From the perspective of small and medium-size companies, the total costs of auditing may become too high with the current price level. Although, the maximum amount per company for unlimited use of AI auditor is £300000. It means that for bigger companies it may lead to savings over the maximum price if AI Auditor manages to replace human work in for example internal audit process and thus lead to savings in personnel costs.

Table 3 Case summary (Source: authors)

<table>
<thead>
<tr>
<th>Company</th>
<th>Solution</th>
<th>Benefits</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aigine GDPR compliance</td>
<td>Makes it easier and more effective to detect unstructured personal information to comply with GDPR</td>
<td>- Reduces the human contribution</td>
<td>- Companies need to ‘teach’ cognitive computing with their own data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The review can be done without a lawyer</td>
<td>- It takes time for a client to get started with the product</td>
</tr>
<tr>
<td>Apiax Tax product</td>
<td>Allows to focus on tax adjusted returns internationally without knowing national tax laws and regulations</td>
<td>- Financial institutions can use tax adjusted returns in their advisory process</td>
<td>- Responsibility issues in case of judicial proceeding</td>
</tr>
<tr>
<td>Mindbridge AI-auditor</td>
<td>AI-powered solution for audit and internal audit, which allows the company to analyse their whole dataset in minutes</td>
<td>- The quality of audit increases substantially</td>
<td>- Relatively high price</td>
</tr>
</tbody>
</table>

Ongoing research

The last financial crisis opened our eyes for the deficiency of the regulation and supervision of the financial system. As we know the amount of regulations financial institutions need to comply with has rapidly expanded in later years. The whole incubation of RegTech seems to have been carried on by the financial sector and the primal cause has been to keep the costs reasonable (Arner et al. 2017b). The main part of the research on RegTech address the subject from a legal perspective. Moreover, the research is generally associated and discussed together with Fintech. As a consequence of the fact that RegTech is a quite young term the roots of RegTech are said to go back to the 1960’s. RegTech has experienced rapid evolution and today the research in the field is quite initiatory. Nowadays the research considers the later effects of RegTech on your business environment (Butler et al. 2018).

Even if we can find some literature on RegTech the research is for the most part from a law point of view. In their recent working paper by Kavuri & Milne (2019), they state that there is lots of work and research to be done in the area of Fintech and RegTech prior to making it
an established academic discipline. The target of the paper is to offer cohesive future research themes based on group meetings with policymakers and academics and a critical assessment of the existing literature. Kavuri & Milne state that there is an opportunity for interdisciplinary approach that include law or other disciplines to analyse the implications of RegTech. The authors also outline seven research gaps existing today that they see as important to make the area of Fintech and RegTech become an established academic discipline. Two of the key areas of research the authors named are closely associated with RegTech; “the relationship between the new financial technologies and financial regulation” and “identity, security, data privacy and their regulation in financial services”. The later has according to the authors almost no existing research. It’s important to notice that the paper from Kavuri & Milne is written from a more Fintech point of view and there is differing opinion on how much linked Fintech and RegTech actually are.

Packin et al. (2018) wrote an article under the topic “RegTech, Compliance and Technology Judgement Rule”. The authors focus on regulatory compliance in the financial industry. The authors revise the supposition that RegTech will be able to improve the regulatory compliance in the financial industry, which they define as the use of technological solutions to facilitate compliance with and monitor regulatory requirements. The authors express concerns against the adoption of RegTech and argue that it’s not a panacea for all corporate governance challenges. The article points out some considerable risks and challenges of RegTech solutions such as; high costs, barriers to the adoption and development of RegTech systems, RegTech questionable impact on risk management and corporate procedures of financial companies, the problematic side-effects of no longer having a human directly working with tasks that RegTech does cheaper and faster, and the phenomenon of anti-RegTech. Many of the problems that the authors point out are in connection with the assumption that the human is capable of thinking ethical while a computer only does what it’s programmed to do.

Another article approaching the theme from a law point of view is Micheler & Whaley’s “Regulatory Technology” (2018). The article emphasizes that a learning period will be experienced when we learn about the limitations of technology. Regulated entities may not have knowledge of software development and this will probably be an opportunity for new service providers in the financial market. For the moment there is a small group of companies keeping the leading positions in data analysis and they are probably also interested in having a share of the emerging market. Lastly it’s important to remember that technology is neutral, it reflects the preferences of those who develop it.

As a different angle of approach there is Treleaven and Batrinca (2017) which is a discussion contributed by two computer scientists. The authors present the concept of algorithmic regulation modelled on the algorithmic trading paradigm. They also bring up employing technology under development for blockchain distributed ledgers and smart contracts. Lastly the authors state that blockchain smart contract technology will have a more considerable disrupting impact on legal services than Fintech is having on financial services.

Gurung & Perlman (2018) investigate the evolution of RegTech from a global view and especially how central banks in developing countries are contemplating the use of RegTech. The authors present evidence from India, Mexico, Nigeria and the Philippines. Differing from the developed countries the driving force behind RegTech has not been the interest to cut compliance costs. In the developing countries tracks increase the responsibilities of central banks to keep up with new technological developments like DFS and the evolving characteristics of market participants. In the developing countries the new technology has been very useful for improving their existing systems and providing them with new tools to use in supervision. The authors see RegTech as a possible tool for the central banks to achieve
financial stability, safety, integrity and inclusion objectives. There are also possible challenges for the central banks connected to the implementation of RegTech products. The financial, social and political situations in the developing countries can pose unique and distinct challenges for the central banks in the process of implementing RegTech.

Panisi & Perrone (2018) lead off by stating that RegTech does reduce information asymmetries and the costs related to them. RegTech allows financial institutions to comply with regulation and regulatory authorities to improve their possibilities to deterrence. Most important the authors also present important RegTech perils of the financial system mentioning risks related to the vulnerability of technology and automation biases that harm the personal responsibility and decision-making effectiveness. Further RegTech increase imbalance in resource allocation between the financial institutions and supervisory authorities. Considering the issues mentioned above the authors’ state that the most effective cure is investing in the “human factor” by re-establishing the balance between technology and humans. It’s important to contain the perils RegTech for the good of the financial system by subjecting the supervisory processes to reliable safeguards against technological problems and preserving human judgement and personal responsibility in decision-making

Challenges with RegTech adoption

The benefits and possibilities that new technological advancements bring us are almost limitless and certainly beyond our wildest imagination. But we need to tread carefully as we approach the future through new technology. For all their benefits, with new innovations and opportunities comes also new threats and perils. This is especially true for regulatory technology. If we start to replace the human regulator with machines, the possible repercussions for technological failures can be severe.

Algorithms and machines are neither malevolent nor benevolent. They are almost like traditional tools that needs our hands to be of purpose, but they don’t need our continuous presence and effort to function. Instead, we can tell them what to do and they will obediently do our bidding. Only thing is that they don’t understand our language, we need to translate it in order for them to understand us. This translation is challenging, as the subjective understanding of rules and risks are codified into rule-bound controls that are believed to satisfy regulatory mandates (Bamberger 2010).

The complex and intricate nuances of the real world is hard to fit into the binary mind of the computer. In the words of Friedmann & Nissebaum, programming often requires to "quantify the qualitative, discretize the continuous, or formalize the informal”. To do this properly and in a way free from bias is a challenging task, even with the best of intentions.

The weaknesses of regulatory technology are not only limited to the algorithms and the code itself. RegTechs rely on the data fed to them. While humans certainly make mistakes by leaning on insufficient data and false premises, we possess an ability to understand the nature of the information we use for our decisions and have the chance to be critical towards it. But for the machine, the data we feed it is all there is. A computer can’t understand that the data it’s working with is faulty, even in cases when it would be obvious to us humans. This might change in the future as we get closer to achieving general artificial intelligence, but for now the responsibility of providing the algorithms with correct data falls on our shoulders (Goertzel and Pennachin, 2007).

With all these different pitfalls, mistakes are bound to happen as we adopt regulatory technology. But even more so than with faulty data, when a mistake happens, we usually recognize it instantly and start to rectify it, leading to isolated mistakes that can provide a valuable learning experience. Computers and algorithms on the other hand with their blind
obedience can’t understand when they are wrong. Unless we humans as the monitors can recognize that the machine is mistaken, it will continue its faulty path, allowing for systematic failures and biases. The intricate mechanisms of the code and its processes can be obscure and is beyond understanding for most of us, making detection of these systematic biases harder (Bamberger 2010). If we fail to detect these faults in time and allow for build-up, the consequences can be harsh. This has already been the case in many risk management systems that were thought to take everything into account, as was the case with the latest 2008 financial crisis or the fall of LTCM in 1998.

Many of the challenges we face in today’s embrace of RegTechs will ease as technology and AI improves. But there is one question that is harder to solve and few will be the answers provided for it by technological advancements. When these mistakes happen, who will we blame? Accountability will be a central question as machines start taking over. The answers won’t be as straightforward as cases like drunk driving or armed robberies where the (ab) user of a tool is the obvious culprit. Yet we can’t allow the algorithms to completely rid us of our responsibilities. Kroll et al. (2016) emphasizes the importance of policy adoption, as the current tools were primarily designed for human decision makers. Collaboration between legislators, auditors, risk-managers and coders is paramount for a successful adoption of regulatory technology. Many are the opportunities provided, but for us to truly grab them, the warnings associated with them should not fall on deaf ears.

Tabell 4 Challenges summary (Source: Authors)

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Problem</th>
<th>Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountability</td>
<td>Who is accountable when mistakes are made by the machine</td>
<td>Unnecessary risk taking and indifference due to easy avoidance of responsibility</td>
</tr>
<tr>
<td>Translation from rule to code</td>
<td>Rules and laws are originally written for humans rather than computers</td>
<td>Wrong interpretation by the machine leading to faulty output</td>
</tr>
<tr>
<td>Automation bias</td>
<td>Machines can’t understand when they are wrong and mistakes will be repeated until humans notice</td>
<td>Build-up of mistakes resulting in critical system failures</td>
</tr>
<tr>
<td>Binary mind of computers</td>
<td>Context based judgement is challenging to achieve due to on/off machine mind-set</td>
<td>Sub-optimal outcomes due to machine prioritizing wrong parameters</td>
</tr>
</tbody>
</table>
Conclusions & future outlook

To address the present and future situation of RegTechs, we have looked at recent developments in the industry and presented some real-life cases of the companies behind today’s regulatory technology. By many standards RegTechs are still a novel phenomenon with major developments still to come. New companies focusing on regulatory technology are popping up left and right. The potential benefits of reducing costs, adding security and lessening the amount of manual and arguably boring work tasks is tempting. Yet the industry is shaped like few others, with the volatile political landscape partly dictating the pace from top-down. As we enter the era of RegTech 3.0 and businesses start to move from knowing their customers to knowing their data, both practical and ethical questions need to be answered. Current research focuses on understanding the long-term effects for the business environment companies operate in (Butler et al. 2018), while future research may have a more data-centric approach (Arner et al. 2017).

Before the technological advances reaches the point where regulatory technology can be applied with minimal effort to a broad network of rules and policies, the regulators need to acknowledge the existence and possibilities of RegTechs when preparing new regulations. This is important not only for the benefit of constructing sound policies, but also to incentivize the development of the RegTechs. Currently most RegTechs tackle specific problems and policies and sudden changes in the rules can quickly erode the long-term value of a new software that took considerable time and effort to develop. The steep price tag of some of the products offered by our case companies is partially a result of the high costs associated with the development of RegTech software. Co-operation and mutual understanding between the authorities and companies will not only protect work from going to waste, but also encourage the creation and innovation of new and better solutions (Kroll et al 2017).

RegTechs were born out of the financial industry with costs as the main driver, but they are already adapting ways beyond just reduced expenditures. The dynamical interaction between policy makers, companies and coders will ultimately decide the future of RegTechs, but with the rising costs of compliance and major advances in fields critical for regulatory technology like big data, blockchain and AI, RegTechs are here to stay. With proper care and sensible decision making, RegTechs can provide a future with more transparency, security, effectiveness and fairness.

References

Retrieve 22.2.2019


Thomson Reuters (2017), Regtech 2020 and Beyond – What Does the Future Hold?


PREVENTION AND DETECTION FOR RISK AND FRAUD IN THE DIGITAL AGE – THE CURRENT SITUATION

HANNA DONNING, MATHIAS ERIKSSON¹
MINNA MARTIKAINEN¹ AND OTMAR M LEHNER² (EDITORS)

¹ Hanken School of Economics, Helsinki
² University of Applied Sciences Upper Austria and Hanken School of Economics, Helsinki

Abstract: “Fraud”, “corporate crime” and “white collar crime” are all terms used when referring to economical- and operational crimes, where fraudulent activities has occurred. Illegal acts such as asset misappropriation, business misconduct fraud, money laundering, cybercrime, tax fraud and accounting fraud are major concern, and where an increased threat has been identified.

This paper explores the possibilities new technology used in fraud detection and prevention mechanisms could provide. Furthermore, we connect the new technology mechanisms with the aspect of organizational culture, that has been proved significant in fraud risk. The contribution is twofold. First, we provide an assessment of modern approaches for fraud detection and prevention, second the insights given by the case study and previous research add encouragement and potential directions for both future research and business practice implications.

Keywords: Fraud; Internal fraud; Advanced technology; Organization culture; Case Study

Introduction

“Fraud”, “corporate crime” and “white collar crime” are all terms used when referring to economic crimes, where fraudulent activities has occurred. From an overhead perspective, economic crimes are committed illegal acts, executed by either an individual or a group of individuals to attain financial or professional advantage (O’Brien, 2019). Illegal acts, such as asset misappropriation, business misconduct fraud, money laundering, cybercrime, tax fraud and accounting fraud are looked upon as a major concern, and where an increased threat has been identified (O’Brien, 2019; PWC, 2019).

It is not only the fraudulent activities that have increased in recent years, recent development also includes regulations, technology, extended knowledge and stakeholder expectation, where transparency is the key word in the debate regarding fraudulent activities. High pressure is put on organizations to manage a good corporate governance function alongside meeting the demand from market expectations, and therefore the organization culture also plays an important role in reducing the internal fraud risk. (Healy and Whalen, 1999; West & Bhattacharya 2014).

The research area is complex and detail oriented, all focusing on different aspects and including different variables in their research scopes. To highlight some, Sima and Satyanarayan (2016) researched the auditors view of how internal fraud is conducted in the present, and Abassi, Albrecht, Vance and Hansen (2012) researched how meta-learning frameworks would help to detect financial fraud. We will focus our research to analyzing previous literature on the internal perspective of fraudulent activities, including
intentional misstatements such as material omissions or disclosures (ISA, 240, 2009 p. 167). Furthermore, we present the Volkswagen Dieselgate Scandal of 2015 as a case study, with the aim to gain an understanding of another aspect of internal fraud and technological advancement, yet with an emphasis on the organizational culture and exemplify a case of a non-functional corporate governance instrument. An analysis of previous research will be conducted, this to examine the development for methods and systems that are able to detect risks and prevent fraud, and also find positive and negative aspects with these systems. The aim is to connect the technological advancements with the aspects of organizational culture, to provide further insight in an area of research not yet discovered as much.

The article will provide value to practitioners and academics likewise, where a thorough background presentation is provided on the subject of internal fraud, new technologies and a future outlook with the aspect of past outcomings, that will gain new perspectives and aggregated knowledge. The remainder of this article is organized as follows: next section provides a background presentation and literature review regarding economic crime in general and internal fraud more specifically. Section three, presents the current development of methods and systems to detect risks and fraud. In section four the Dieselgate case is examined and conclusions from the case follows. Section five provides relevant research on organizational culture and modern approaches versus traditional ones in fraud detection, then follows a review of setbacks in regards of technological advancement. The final section concludes the main findings and propose some thoughts on future research.

Theoretical frames

For detecting risks and fraud, a lot of data must be analyzed and for detecting upcoming risks and fraud, even more data must be evaluated to learn patterns to which firms and individuals tend to act in. Because of the size of big data, traditional methods for fraud detection can also be considered impractical (West & Bhattacharya 2014).

Developing fraud detection systems is not an easy process and can affect the organizations reputation when done wrong. In the Global Economic Crime and Fraud Survey by PWC from 2018, about 34 percent of the respondents said that financial crime technologies produced too many false positives (PWC 2018). The progress in fraud detection systems and technologies are still evolving, and with time financial institutions will have more accurate and efficient mechanisms for attacking fraud and financial crimes (SAS 2018).

However, according to the PWC survey organizations today have access to a wealth of innovative and sophisticated technologies which they can use to defend themselves against fraud. These technologies help with monitoring, analyzing, learning and predicting human behavior and includes machine predictive analytics, machine learning and other artificial intelligence techniques (PWC 2018).
Internal fraud

From the organizations’ perspective, internal fraud is fraud committed within the organizations or by the organizations. The risk of fraud internally could be explained by the triangle of fraud firstly developed by Cressy (1953). Incentive and pressure together with rationalization and opportunity are all components in fraudulent activities, and the triangle of fraud could be used for internal fraud risk assessment (Murphy and Free, 2016). Pressures are seen as the situational events in forms of personal satisfaction, fear of failures or money.

Figure 1 Triangle of fraud (Source: Authors)

Opportunities are the opening of situations where fraudulent activities are possible, for example weaknesses in internal controls within organizations could be one such opportunity event. The rationalization is the typical personal feature, which includes the willingness for intentional dishonesty and therefore the last component in the triangle of fraud that needs to be present for potentially fraudulent activities to occur (Waymond et al., 2015; Coleman and Cressey, 1980).

A common type of internal fraud is when management uses its own interpretation in financial reports (PWC 2018). This to either mislead stakeholders regarding the company’s underlying financial situation, meeting the capital market’s estimates and expectations or in contract negotiations benefit by reporting a more lucrative financial result. This can also be called earning management (Healy and Wahlen 1999). Safitiri, Kustono and Miqdad (2018) found that information asymmetry between the company in question and external parts can create an agency problem where the agent has more information than the principals. An agency problem could lead to an opportunistic behavior, where the agent also maximizes his private benefits or the utility, instead of prioritizing the principals' interest.

Among the different types of internal frauds, another common type is consumer fraud. Consumer fraud is business practices that cause the consumer to suffer, financially or by other losses. Fraud against consumers are often related to marketing, or other promises the firms ensures the consumer with, which later will appear to be inaccurate claims (Winston & Strawn 2019). Furthermore, money laundering and employees stealing from firms are crimes frequently occurring.
Prevention and detection for risk and fraud in the digital age – the current situation

Prevention of fraud

The process of preventing fraudsters is costly and time-consuming, but fighting fraudsters is important to ensure a well-functioning society. Good corporate governance can make sure that the firm’s top management don’t misappropriate assets and manage results in an unethical manner, while internal processes can help preventing employees stealing from the firm (Murphy and Free, 2016).

Fraud risk has been discussed as long as companies have existed and will probably exist as long as firms and people face benefits through committing frauds. Since frauds are becoming more sophisticated, devastating and thorough, more advanced and modern techniques are always needed to fight and predict fraudsters. We will in the next chapter look at the current development of modern techniques for fraud detection.

Current development

Organizations nowadays invest more in technology to prevent fraud, since fraud can be a business problem which could affect growth and reputation negatively. Therefore, use of artificial intelligence and machine learning is now a worldwide phenomenon and companies in developing territories are investing in these technologies more compared to companies in developed territories (PWC, 2018). The technology is still expensive to buy and to adopt across large organizations as well as for smaller organizations. So, the decision when to invest in more innovative technologies regarding fraud detection is a question organizations’ must ask themselves (PWC 2018; Simha and Satyanarayan, 2016).

Development of methods and systems to detect risks and fraud

There are several different statistical and computational techniques for financial fraud detection. West and Bhattacharya (2015) presented data mining as a method for fraud detection. Data mining is the process of sorting through large data sets, with the purpose to identify patterns and establish relationships to solve problems. With the help from the information of data-mining, it is then easier to predict future outcomes. One method of data mining is artificial immune systems (West and Bhattacharya 2015).

Artificial immune systems imitate the behavior of biological immune systems to detect antigens, creating detector cells and their ability to detect foreign bodies. As mentioned, it functions in the same way as the human immune system, by cells fighting antigens and by that the cells will later be better suited for detecting antigens. This method is suitable for classifying problems with imbalanced data, such as fraud detection (West and Bhattacharya 2015).

Machine learning is also a commonly used method for fraud detection and prevention. Machine learning algorithms discovers patterns in big data and the process is much more efficient compared to humans doing the same task. With the information acquired throughout the process, it is easier to predict and prevent frauds. Machine learning can be divided into supervised and un-supervised machine learning. Supervised machine learning is the more commonly used by these two. What differs these two machine learning methods, is that in supervised machine learning guidelines and what conclusions it should come up with are given to the algorithms, this requires that possible outputs are already known. Unsupervised machine learning is instead identifying complex processes and patterns without any guidelines and human intervention, which can help with solving problems that humans normally couldn’t do (DataScience 2017).
Another method is meta-learning. Meta-learning is a form of machine learning which uses information acquired through data mining or machine-learning with the purpose to increase the quality of results obtained in future applications, also called learning-to-learn. It differs from machine-learning, since meta-learning provides a way to learn about the process itself and by that, also providing knowledge about which features and algorithms that can be most efficiently applied (Abbasi, Albrecht, Vance & Hansen 2012).

Figure 2 - Three techniques used when developing system and methods to detect risks and frauds (Source: Authors)

The current development of machine learning and artificial intelligence for risk and fraud detection is that firms do invest more in these technologies and that they are more efficient, but they are also costlier. Advantages with more innovative technologies is that it helps financial institutions to earlier detect risks and fraud. This with help from more innovative approaches for fraud detection (SAS 2018).

“Dieselgate” – Volkswagen Group

To further understand how the organizational culture of an organization, corporation, firm or company can change the prosperity for technological advancement in fraud prevention and detection, the Volkswagen Dieselgate scandal is one example that we believe could provide a thorough picture of how organizational culture mixed with tech improvements impacts reality.

Background to the case: Volkswagen anti-pollution system

Volkswagen amongst other automobile companies were all developing a cleaner line of diesel engines in the years prior to 2008, when the first defeat device was installed. The EA 189, was the new diesel engine line of Volkswagen, and one of the most important engines for the Volkswagen brand. The EA 189 came both as 1.6- and 2.0-liter versions and were planned to be used in vehicles of other brands included in Volkswagen group, such brands were Audi, Skoda and Seat. Moreover, the new engines were also scheduled to be included in Golf, Passat, Beetle and Jetta cars sold in the United States as a concept of “clean diesel” and make American drivers responsible for their environmental surroundings. Pressure put on the engineers employed by Volkswagen was high, and the developed EA 189 engines proved to be a disappointment, not able to meet the standards of emission regulations, in not only United States, but also in the European Union. The setback of canceling the production, was found to be too costly, therefore Volkswagen decided that an easier way out was to install a developed manipulation software, which later came to be called the Defeat Device (Eiwing, 2015).

The scandal erupted in September of 2015, after an illegal manipulation software (also named the “defeat device”) was discovered by EPA (Environmental Protection Agency) on the basis of tests conducted by ICCT (International Council on Clean Transportation), who found
significant differences between lab tests and road tests, where in the testing of the later one higher doses of pollutants such as nitrogen oxides (NOx) where reported. Volkswagen admitted to have had installed the so-called defeat device in approximately 500,000 cars sold in the United States (Tovey, 2015). The defeat device was found to enable the Volkswagen cars to detect when they were being tested, and therefore the engines of the cars emitted less CO₂ and NOx than they would under normal circumstances emit (Siano et al., 2017). The instant negative impact on both Volkswagen and various stakeholder groups involved followed, and a public outrage made the shares of Volkswagen to drop with more than 20% in one day on the Frankfurt Stock Exchange (Siano et al., 2017). Both internal and external investigations begun not only in the United States, also Germany, France and several other states decided to investigate potential fraud further, where Volkswagen was the main suspect.

![Figure 3 Sequence of events the years prior to the reveal of Dieselgate (Source: Authors)](image)

**The internal organization culture and management response**

Siano et al., (2017) performed a content analysis on the revelations and findings from Dieselgate reported in media, and the reported content from Volkswagens personal statements and sustainability communication to their share- and stakeholders. The result proves that Volkswagen in fact did not report a true and fair view, instead they presented an inconsistent picture of what the reality looked like. Looking to the sustainability communication, Volkswagen did communicate more ambitious statements compared to other automobile companies, where they specifically highlighted the reduction of emissions such as CO₂ and NOx. “Due to climate change issues and ever scarcer resources, we reduce the CO₂ emissions of our vehicles on an ongoing basis”; “Reduce global facility CO₂ emissions per vehicle by 30 percent by 2025 compared to a 2010 baseline” (Siano et al., 2017, p. 31) are two examples found in the annual statements of Volkswagen group.

When seeking parallels in prior fraud cases, Enron and Worldcom are two cases that has similar characteristics to Dieselgate. When following the individual investigations of each fraud case, all related suspected data led to senior managements fraudulent acts, in order to camouflage the businesses financial situations or operational failures (Crete, 2016). After its first internal investigation Volkswagen found that a handful of software engineers within the management, were the ones responsible, and the CEO of Volkswagen group in the United States claimed to the Congressional Subcommittee that no allegations towards the organizational management were in line (Crete, 2016; Boston, 2015). The CEO was not able to convince neither the Subcommittee, external investigators nor the public and suspicions...
were drawn to the management of the corporate governance function within the Volkswagen group.

In December of 2015, the senior management of Volkswagen Group released the preliminary results of the more in-depth internal investigation. They found following observations: (1) misconduct and shortcoming were compelled by individual employees, (2) Volkswagen did have some weaknesses in certain internal control processes, and (3) the mindset within some divisions of Volkswagen were wrong, and lacked ethical behavior where breaches of rules were tolerated.

Conclusions from Dieselgate

The Dieselgate scandal was the result of ambitious production and market targets, for specifically the United States market, with strict time and budget limits. Furthermore, this led to encouragement of the employees to make unethical decisions in order to meet the operational goals and achieve the objectives of Volkswagen group’s business model. The internal control mechanisms did not work, and therefore the misconducts within the organization could not be discovered. Issues has been found especially within the compliance system, which were there to ensure that the respect of legal requirements were met (Eiwing, 2015). Among other circumstances that led up the outcome of Dieselgate, poor corporate governance managed by senior management is the main one. The external investigations did see a centralization of decision-making to the senior management, and where the organization culture of Volkswagen made the internal communication between mid-level management to senior management, not functional. Passing on “bad news” were discouraged, and pressure to deliver was high (Crete, 2017; Ewing, 2015).

Research

This section provide a presentation of what previous research found about the relationship between organizational culture, artificial intelligence, machine learning and fraud detection. Also, to further investigate whether more modern approaches to detect frauds are in favor of traditional ones.

Organizational culture

Decision making within organizations are dependent on both individual and organizational factors, and where the organizational ethical culture will influence the ethical behavior (Douglas, Davidson and Schwartz, 2001). Fraudulent activities could be looked upon as intentional dishonesty, and could derive from either perceived pressures, perceived opportunities or rationalization (Waymond, Söderbom and Guiral, 2015; Cressy, 1953). As mentioned in section two, the three components (pressure, opportunity and rationalization) put into the fraud triangle are also the three requirements for fraud to potentially occur (Cressy, 1953). Previous research has clearly seen a connection between the triangle of fraud and employees within organizations who commit fraud. This could also be explained by the upper echelon's theory (Hambrick and Mason, 1984), which suggest that senior management are a reflection on the organizational culture within the organization. Therefore, the praxis for fraudulent activities and the questions of whose responsible in prior fraud investigations has also changed its direction to some extent. For example, the guidelines of the Principles of Federal Prosecutions of Business Organizations, issued by the U.S. Department of Justice still emphasis the further investigation of individual wrongdoers in fraud cases, but recent
development has also started to seek explanations for fraud in the organizational environment (Crete, 2016).

Modern approaches for fraud detection versus traditional ones

Abbasi, Albrecht, Vance and Hansen (2012) conducted a research paper about how a meta-learning framework will help to detect financial fraud. To evaluate the proposed framework, thousands of legitimate and fraudulent firms were investigated (Abbasi et al., 2012).

Prior studies suggest that data based on financial statements does not have a high fraud detection rate and because of that the use of ratios and financial statements are incapable of accurately identifying financial fraud or at least, that it has a limited capability (Kaminski 2004). So, the question to ask is if meta-learning do increase the fraud detection rate.

By comparing meta-learning processes with traditional approaches for detecting risks and fraud, Abbasi et al., (2012) found that the Meta-Fraud framework was remarkably effective. The framework was found to improve the performance and the results, therefore using meta-learning methods where confirmed to be more effective compared to traditional approaches, such as studying financial ratios (Abbasi et al., 2012).

Soviany (2018) studied how artificial intelligence can come to help with detecting online payment frauds and transactions in real time. The design focus is on a supervised learning engine to support high-performance fraud detection of the data, as well as improving the predictive value. With this AI method, the design exploits the discriminant properties of customer data and by that, finding hidden patterns. Soviany (2018) found that artificial intelligence was superior compared to the static rule-based methods. This due to that the method is considered more effective and can manage a greater data set with less human intervention. Soviany (2018) claims that in many legacy-rules based fraud detection systems, the target performance achieves a lot of false positive results, while artificial intelligence has a faster adoption process and can therefore find more detailed data as well as hidden patterns. Furthermore, statistics provided in the study found an increase from 85 to 90 percent, comparing the methods with detection of fraudulent transactions (Soviany 2018).

The complexity of using artificial intelligence in fraud detection

Baldwin, Brown and Trinkle (2016) reviewed the relationship between auditing and accounting problems and artificial intelligence. The paper examines the problem between two totally different professions. Accounting and auditing are in its nature a specialized domain requiring significant education as well as expertise and experience, which can result in a low number of persons. Because of that, research on accounting is also done most successfully by accountants. The significant differences and the expertise required for both artificial intelligence and auditing, is that auditing and artificial intelligence researchers must bridge the gap and improve collaboration to improve fraud detection using artificial intelligence. Baldwin, Brown and Trinkle (2006) do say that artificial intelligence researchers hold the key to solve issues regarding auditing and assurance through techniques as fuzzy logic, neural networks and other areas of artificial intelligence. Because of that, collaboration and further investigation into the topic is a requirement for the future in fraud detection (Baldwin, Brown & Trinkle 2016).
Critical voices expressed by society

The link between technology and fraud is not only identified as a helpful tool used to detect and prevent fraud. As previously mentioned, the organizational environment and its culture do play a significant role in detection and prevention of fraud of the internal control methods. Therefore, critics has suggested that technology and advanced methods to detect fraud do not matter in an organizational culture of high pressure to meet targets, similar to the case of Volkswagen and Dieselgate (Donelson, Ege and McInnis, 2017; Ewing, 2015).

The presence of technology advancement seems to distance the employees from their responsibility towards dishonest actions, such as fraudulent actions. Prior research on the subject has found that information systems has a tendency to depersonalize fraudulent situations (Schwartz and Wallin, 2002), and therefore the opportunity to commit fraud seems to rise above the rationalization, where justifications of the dishonest actions could be that they are not the ones committing to anything, rather the system or software itself would be the ones accused. Technology loops are exploitable, where the advancement also could help the fraudsters to commit fraud. Moreover, future concerns regarding unsupervised machine learning indicating that systems could learn how to commit fraud on their own is a possibility has been expressed.

Furthermore, the discussion regarding whether to apply technological fraud prevention and control system or not, depends on the setting-up costs, Sima and Satyanarayan (2016) found that even though small organizations are affected tremendously by fraudulent activities, the cost of setting up a smart system is too costly to be handled by smaller organizations (SAS, 2018).

Figure 5 The main arguments in negative response (Source: Authors)
Conclusion and future outlook

Our paper intends to connect the aspect of technological advancement with organizational culture in order to reduce internal fraud. The paper highlights that frauds are committed in situations where benefits can be gained. From the company's perspective, frauds are committed by organizations through, for example, asset misappropriation, to gain private benefits as well as keeping the firm competitive.

It is important to consider that one of the peculiarities of internal fraud is that the person, or persons, that commit fraud often sees it as a victimless crime and can neither visualize any person who will be directly harmed (PWC, 2018; Shwartz and Wallin, 2001). This would also explain why the main perpetrators of economic crimes are internal actors, including human resources fraud (81%), insider trading (75%), asset misappropriation (75%), accounting fraud (74%) and also procurement fraud (73%) (PWC 2018).

Current development of innovative and modern fraud and risk detection methods includes machine learning algorithms, data mining and meta-learning. They are all useful means accessible in risk and fraud prevention and detection systems (West and Bhattacharya, 2015; Data Science, 2017 and Abbasi et al., 2012). With that said, these methods will not be utilized in an efficient manner, if the organizational culture emphasize dishonest actions from perceived pressures, opportunities or rationalization (Waymon et al., 2015). Therefore, as showcased in the case study (Dieselgate, a well-managed corporate governance function is essential in order to not create opportunities and prevent rationalization internally. PWC 2018, implies the same conclusions where they suggest that focus needs to be drawn to the environment that governs employee behavior. To assess the strengths and weaknesses of the culture, surveys and comprehensive interviews should be made as well as consistent training. If people clearly understand what’s right and what’s wrong, and why, the process of fighting fraudulent activities will also be easier (PWC 2018).

Furthermore, when connecting technological advancement with organizational culture, we find that future research should investigate this connection in more detail. For example, the aspects of the principal-agency theory could in future be applied to answer the questions regarding the possible situations of asymmetric information and conflicts of interest between management and stakeholders. Moreover, the practical business implications given from our findings, is that a combination of further development in organizational culture and more advanced technologies are the key to reduce the risk of fraud (see figure 4).
Figure 4 The combination of tech and a positive organizational culture in order to prevent and detect fraudulent activities internally (Source: Authors)

References


PREVENTION AND DETECTION FOR RISK AND FRAUD IN THE DIGITAL AGE – THE CURRENT SITUATION


CYBERCRIME IN A BUSINESS WORLD: BEHAVIORAL PERSPECTIVES

BÖCKELMAN PETTER, BJÖRKMAN HENRIK1
MINNA MARTIKAINEN1 AND OTHMAR M LEHNER2 (EDITORS)

1 Hanken School of Economics, Helsinki
2 University of Applied Sciences Upper Austria and Hanken School of Economics, Helsinki

Abstract: As we are living in a fast-growing digital age it is crucial to keep in mind risks related to digitalization. The current digital work environment enables cybercrime and the practice of cybercrime has become more and more common. Because of the fast digitalization of our society many people miss out on important parts such as cyber security and only focus on development. This means that social behaviour is a big issue when it comes to cybercrime and cyber security.

This work explores cybercrime in a business world with a focus on social behaviour. It explains how big an impact social behaviour has on cybercrime and it also explains how you can protect yourself of becoming a victim of cybercrime.

Keywords: Cybercrime; Social behaviour; cyber security; Social engineering

Introduction – What is Cybercrime and why is it relevant?

In today’s society it is almost a prerequisite that we have smart devices and connection to the internet. In both the work environment and social environment, we can see that the digital age is evolving e.g. through artificial intelligence and autonomous systems. Because of these sorts of developments, it is also crucial to look at the security. As the technology and systems are evolving, the ways of taking control and hacking into these systems are also getting more sophisticated and these sorts of breaches are called cybercrime. Cybercrime is explained by Arief et al. (2015) that it is computer-oriented criminal activity to gain economic, psychological and/or personal benefits. Computer-oriented criminal activity means that, by using a computer or smart device with connection to the internet, the attacker can remotely access high profile information or confidential data, copy credit information, access different systems and a lot more.

There are many ways to access your private computer or your business computer and servers. When discussing about ways of exercising cybercrime, Schinder DL. et al. (2008) categorizes these types in their book as following:

- Pre-intrusion/attack activities
- Password-cracking methods
- Technical exploits (taking advantage of characteristics of the equipment or protocols)
- Malicious code attacks (Viruses, worms, trojans)

Even though there are many ways to exercise cybercrime, it is not always the actual cyberattack that is sophisticated and many times it can be a very simple virus or malicious code. Often the malicious code finds the information that the attacker is after, because of human errors or social behavior. This means that as the technology evolves, the need of education on risks related to this needs to be up to date. This is also something that Sabillon E et al. (2016) takes in consideration, “Technology by itself is not enough, the integration of other fields like training, awareness, social aspects, culture…”

**Types of cybercrime**

In the following chapter the different types of cybercrime are presented and shortly explained. The importance here is to get a view over how attackers are trying to reach out for your information. In this chapter the focus lies on social engineering.

**Viruses – Worms - Ransomware**

Viruses are malicious programs that infect other programs or applications by transferring its own code into theirs. Files that are thought to be legit are reprogrammed into something completely else. Once the code has been injected into the designated targets, the virus starts to spread. Usually in a rapid pace over networks. In most cases, the initial injection is affiliated with social engineering. The end-user is tricked into opening certain links or download files contained with the virus. One common way to create an entry is to attach malicious files to emails, once opened, the virus has been infused into the system. Viruses can also be classified into different categories depending on their characteristics. There are resident viruses which are embedded in the system memory and are activated every time the OS is started. Non-resident viruses are on the other hand executable viruses that does not store itself in the computer memory. As the anti-virus software evolves, so does the viruses.

 Nowadays we can find the likes of Metamorphic viruses, Stealth viruses and Polymorphic viruses. Metamorphic viruses have the ability to change its own code after every new infection. Being able to rewrite the code leads to the functions of the code being the same but the detections of the virus really complicated. Stealth viruses can remove itself from infected files to then appear somewhere else to confuse the antivirus software. Once the Polymorphic viruses have infected the target, it can duplicate and at the same time slightly alter its’ own code. What it achieves by doing so is making it very hard for the detection software due to a large number of slightly different versions of the same virus. (Symantec Corporation)

Worms are interchangeably used for viruses, but there are things that distinguish viruses from worms. The main one is the reproduction part. Worms are unlike most viruses able to duplicate and are not dependent on existing programs to spread itself. Worms are capable of leaving copies of themselves in every infected computer, without any assistance. Worms have their name for a reason. They are always looking to dig deeper. Worms are continually looking for new possible vulnerabilities to explore. The worms are often designed to either extract valuable information from the inflicted computer, or to take control over them and use them as bots. The purpose of creating zombie computers is being able to use them as proxies when engaging in activities such as sending spam emails or attacking governmental computer. Networks of bots - Bot nets - can then be sold or rented out to criminal organizations that have the intention to use it for different types of cybercrimes. The worms are often classified by the way they are spread. The four most common ways are through emails, networks and internet. (TechTarget)

According to O’Gorman et al. (2012), ransomware is a type of malware that infects your computer and denies access to your files. The malicious software is keeping your files hostage by encrypting your files and demanding a ransom payment for a decryption key. If the ransom
fee isn’t met, the files will be deleted. The most common way for the ransomware to infect the computers is by phishing attacks.

**Social engineering – The impact on businesses**

Cybercrime has a very negative impact on businesses, for instance if a business is targeted by cybercrime there are different risks that the company faces. There are risks related to reputation & market, financial risks and risks related to processes. Social Engineering is one of the most common ways to commit cybercrime. Social engineering involves an attacker and a target, the attacker slowly builds up a trust through e.g. email or by phone with the employee. So basically, social engineering consists of psychological manipulation of the employee in intent to get confidential- or high-profile information or economical benefits. Abraham S. et al. (2010) verifies this by defining social engineering as “the use of social disguises, cultural ploys, and psychological tricks to get computer users to assist hackers in their illegal intrusion or use of computer systems and networks”. So what Abraham S. et al. (2010) implies is that the employees in this case unintentionally help the attacker by assuming that the attacker is for an example a team member or a client for the company. Let’s assume that an employee works for a big international company, this often means that the employee does not know every person that works for the company. Because of this the attacker can easily disguise as a team member and for example present a problem to the employee and ask if they can help them. After this the attacker can use this email thread to talk to the next person in line, slowly getting higher up on the corporate ladder until they reach the person/system the attacker really is targeting.

Krombholz et al. (2014) talks about the future and BYOD policies or bring your own device policies and emphasizes that as all sorts of devices are evolving, also the ways of how to attack these devices evolve. So Krombholz et al. (2014) suggests that “a detailed understanding of the attack vectors is required to develop efficient countermeasures and protect knowledge workers from social engineering attacks.”. So, by knowing how the attack is done, you can more easily defend yourself from these sorts of attacks.

Social engineering is often done through something called phishing and phishing can be put into two main categories, spear phishing and whale phishing. An attacker that is concentrating on acquiring illegally passwords, credit information or other volatile information is a spear phisher or in other words it is called targeted phishing. On the other hand, an attacker that is targeting high profile targets such as government officials, CEO: s, CFO: s etc. is committing whale phishing. Whale phishing is also targeted phishing but on a more detailed level. According to Gupta B. B. et al. (2018) there has been many cases of phishing throughout 2005-2018, targeting large businesses such as VoIP (identity theft), Facebook (ad spams) and Sony (credit & debit information stolen) just to mention some. These attacks have had crucial effects on the businesses such as reputation and financial losses, for instance according to Gupta B. B. et al. (2010) the cost of the phishing attack towards Sony consisted of losses up to $1 - $2 billion dollars not to forget to mention the impact this attack had on their reputation.

The figure 1 below shows the phases of an email phishing attack and gives an overview of how phishing is executed through email.
Motives behind cybercrimes

Because of the constant growth of cyber criminality, it is important to understand the motives behind the people behind the screens. The different actors operating in the cyberspace can be distinguished from each other based on their motivations. The three main motivations are:

1. Financial gain
2. Political agenda
3. Intellectual challenge

Hacktivists are actors that are trying to achieve social changes or promoting a political agenda with the help of technology. It is important for the hacktivists to bring awareness and highlight a problem. The actions are often done in the name of freedom of speech, freedom of information or human rights. Hacktivists are often targeting governmental institutions or big corporations that are imposing censorship. Different methods are used in order to voice the activist’s opinions. Examples of methods used by the activists are denial of service attacks on websites and stealing and publishing of sensitive and classified governmental information. Wikileaks and Anonymous is a prime example of an organization politically motivated (Ablon, 2018).

The largest group of actors are engaging in this type of activities of the sole purpose of money. Cybercrimes have been proven very profitable at the same time as the risk, if done right, is very low. Users of the peer-to-peer network Tor as well as people dealing with cryptocurrencies are basically untraceable, and because of the limited collaborations between countries’ law-enforcement, it makes it even harder to get hold of the people responsible. There are a lot of different types of crimes than can be executed to make a profit. Stealing trade secrets, health information, intellectual property, credentials, bank details are a few of them. As most industries, the cybercriminals are differentiating their services to acquire as many new customers as possible. By customers, I mean people that are willing to either buy cybercriminal services or products. Monetizing on these activities are the top priority for the criminals and are...
done via reliable black markets where payments are completed using cryptocurrencies. These black markets are both easy to access at the same time as they are very professional, both the likes of agents and intermediaries are found. The markets possess a hierarchy structure with the most knowledgeable administrators and subject-matter experts at the top. Because the lack of entry barriers, a lot of interested buyers find their way into these markets. Both services and products are provided here, some of the sellers are only providing certain exploit kits for the buyers to use themselves, where some provide a full-scaled cyberattack from initial hacking to the desired outcome. Extortion, stealing of intellectual properties and stealing of data is the most common types of services provided (Ablon, 2018).

![MOTIVES BEHIND SOCIAL ENGINEERING ATTACKS](image)

Figure 2. The Figure 2 is taken from Conteh, N. Y., & Schmick, P. J. (2016). “Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks” (figure 2), but the figure design has been changed by the authors.

Even though we present three main motives behind cybercrime, the above figure illustrates the distribution over the different motives behind social engineering attacks which was presented in chapter 1.4. Here we can see that the three biggest reasons are financial gain, competitive advantage and access to proprietary information.

**Behavioral science**

Up until this day, the approach for identifying and hindering cybercriminal maneuvers have been mostly technological. New computer software, advanced encryptions, password managers, multifaceted authentication are a few of the prevention methods used for stopping the cybercriminal threats. Considering that stolen data has become so simple to monetize from, cyber-criminal activities have grown into a profitable business of large scale. Seeing that the criminals easily can further financial gains from accessing data, new methods of exploiting vulnerabilities in businesses will always continue to be developed. Technological defense systems are of utmost importance, but the criminals have a tendency of circumventing these protection systems and instead focus on the weakest link in the security chain, the humans themselves (Eddolls 2016).

IBM’s” Cyber Security Intelligence Index” from 2014 finds that 95 % of all security breaches include human errors. These numbers indicate that successful prevention requires a
shift from the technological approach to a more behavioral one. The technological systems will provide a protection for the organizations but are still vulnerable to human errors. A strong relationship between behavioral patterns and vulnerabilities need to be acknowledged. Cybercrime is in fact more about behavioral science than it is about computer science. Hence, we need to understand the relationship between behavioral patterns and cyber victimization.

Creating a cyber aware workforce and educating the employees how their personal cyber behavior is affecting the organization is an effective way of mitigating risk. The business leaders need to prioritize this matter and implement a cyber culture based on awareness. For this to become a reality, strong leadership is needed. The new corporate culture shall be implemented from the top and needs to permeate the organization as a whole. Cyber security shouldn’t be an area that is left over for the IT-department to take care of. Instead, it should be embedded in all the processes of the business. By achieving that, and by focusing on the individuals instead, the businesses become sufficiently prepared and protected for threats. The business will still be a target for criminal activity, but now has a response plan in case it occurs (Eddolls 2016).

McBride et al. (2012) means that, by understanding employees’ psychological profiles, companies act even more preventive. The reason for it being, employees with specific personality traits and behavioural patterns possess a bigger risk for being targeted by cyber criminals. Companies can therefore conduct personality tests and customize their education for those at bigger risk. The research made to this day has already helped us a bit on our way of understanding how different personalities possess different kind of risk. However, future evidence will most likely help us with how companies will be able to quantify personality traits and how they practically can implement this information in their cyber security training.

Existing research on the connection between cyber victimization and personality traits

In 1990 Gottfredson and Hirschi demonstrated through their general theory of crime that people with lower self-control are more likely to engage in criminal activities. The individuals with lower self-control are more impulsive, they take more risks and they are unmindful of future consequences. Numerous studies have applied the general theory of crime as a corner stone for further studies in the field of criminal cyber victimization. One study that uses the general theory of crime for cybercrime victimization research is Holtfreter et al. (2008). They have concluded that there is a connection between low self-control and victimization of several types of cybercrimes. These types are commonly scenarios where the end-user needs to provide the point of entry, for example opening an attachment in a phishing email. However, intrusions where no help from the end-user are wanted, the individual characteristics are less important. Schreck also found evidence in his study of a link between low self-control and being able to predict the risk of an individual falling victim for cybercrimes. The reason behind it is logical. Risk-taking and impulsiveness are not characteristics of a behavior that is known for its’ preventive nature.

Scholars have also extended their studies to include personality traits, which indeed is part of” self-control”. One study that investigates the relationship between the Big Five model of personal traits and cyber victimization is van de Wijer et al. (2017). The Big Five personal traits are Openness to experiences, Conscientiousness, Extroversion, Agreeableness, Neuroticism. Using a large sample of 3648 Dutch individuals, the authors find evidence that people with lower conscientiousness and emotional stability and that felt more openness to experience have higher risk of falling victim for cybercrimes. This result is in line with previous literature since
the results gathered from the different traits reflects the characteristics of low self-control in the general theory described above.

McBride et al. (2012) has extended the research about the role of individual employee characteristics by including the role of sanctions and protection motivation theory. The findings of the current study are consistent with those of van de Wijer and Leukfeldt which are that there’s evidence that employees with specific personal traits are more likely to violating cybersecurity policies and therefore becoming a victim. The interesting part about McBride et al.’s study is that it incorporates the Big Five personal trait model with deterrence methods and protection motivation theory. The researchers were interested in finding out how deterrence effects the likelihood of violating corporate policies and how this differs between individuals. For example, some employees will choose the benefit from policy violation over the punishment received from breaking the rules. McBride et al. (2012) also wanted to assess how employees reacted differently when they perceived threats. The survey was designed so the authors could assess employee’s personality traits, and then how these people would act differently. The results from the study shows that people with different personal traits, act differently in the same situations.

These findings suggest that a new approach should be undertaken by the organizations. Instead of focusing on a “one fits all”- training method, the organizations should focus on how different personality profiles are more likely to violate cybersecurity protocol. Generic training methods should be put aside and customized training methods depending on employee profiles should be implemented. By utilizing the information about how personality traits affect the perception of deterrence and threat, the training methods can be designed to target specific personality traits and therefore be much more effective.

*Framework for building a corporate cyber culture of awareness*

In a business context, social engineering techniques are commonly used when trying to get the end-user to commit a mistake. A cooperation between the intruder and the employee is needed. For the employee to make a mistake, he is manipulated into making something he shouldn’t do, a human error.

Cyber security is a part of risk management. By creating a corporate culture of cyber awareness, organizations will decrease the likelihood of human errors occurring. Changing the corporate culture is not happening overnight, but every little help. The way of safeguarding towards social engineering is creating a defence system built by multiple layers. If one layer is penetrated, there are several more to hinder it from leading to total havoc. Conteh et al. (2016) have in their research article provided a few measures against social engineering. By adapting these changes with the addition of a few other modifications, organizations are taking big steps towards a change in their cyber security culture.

**Human errors**

Firstly, Human errors will always occur, there is no getting by that fact. Changing the corporate culture, the way cyber security is looked upon, is a prevention method. Eliminating the risk of human errors will never happen, and the expectations should be aligned with reality. Individuals inside an organization are the most vulnerable link and should be treated like everything else in risk management. Be familiar with the vulnerabilities, the risk tolerance and have a response ready if something occurs.
Build a strong morale and don’t punish errors

A strong morale inside an organization often leads to the employees appreciating their job more. Making them feel that they are a part of something, instead of just a corporate worker, will boost their eagerness to avoid threats. This happens both consciously and sub-consciously. Management should also remember not to punish human errors too harshly. Social engineering is in fact often conducted in new founded and sophisticated manners. And if errors are punished too hard, it can lead to the employees not being willing to report when they potentially have made an error. This can lead to the damage becoming far worse. (SecurityIntelligence 2018). Pleefeger et al.’s hypothesis is that if the employees are taught the importance of behaving responsibly, are given time to learn the computer systems and are trusted to behave satisfactory in terms of cyber security policies, it can lead to better cybercrime prevention.

Deterrence methods are frequently used to get the employees to follow security protocol (McBride et al.). Deterrence theory suggests that if the sanctions are severe and certain, it will lead to that the employees won’t engage in activities that aren’t allowed (Akers, 1990). The effect deterrence methods have on employees are based on an individual’s rationality and morality. An individual’s perception of the sanctions being too harsh, can lead to negative effects with respect to cyber security (McBride et al. 2012).

Constant education

Educating and making the employees aware of potential threats is key when it comes to cyber security. By educating the employees, they will learn how to recognize common social engineering techniques, how their private cyber behaviour like lax password management and risky handling of company files can put the company at risk. And finally, different response methods against intrusions. For this all to be accomplished, constant education needs to take place. The landscape of the cyber criminals is constantly shifting, new methods of exploiting vulnerabilities are founded. Therefore, the education should follow the same pattern, it should be ongoing. In order to get the employees to learn as much as possible, the education should be versatile. Both practical and informative education should be provided. The result from the practical exercises should indicate how the education methods can be adjusted (Conteh et al. 2016). The best way according to Luo et al. (2007) to prevent ransomware attacks is to show what implications risky cyber behaviour lead to in terms of loss of stock value or loss of important customers. When the employees understand the real-life implications it can lead to, the chances of them taking precautions increases. The awareness training should also begin directly from the employment. By doing so, the organization will automatically shift the employee’s mindset in terms of how cyber security should be prioritized (Simpson, 2017).

In his research article, McBride et al. describes three levels of cyber security training. The first two levels are similar and is referred to as the status quo-levels where generic training protocols are used with only a few individual differences acknowledged. The third level represents a potential future approach to cyber security training. The training protocol both incorporates personality factors and in which way individuals perceive security threats and potential sanctions. By using the results of McBride et al.’s study, it can help organizations to develop employee profiles based on their perception of threat, sanctions and their personality traits. Customized training would then be created for all employee profiles to specifically target the individual’s need when it comes to cyber security training. The information needed would be obtained by letting the employees answer a questionnaire that would evaluate both their personal factors as well as the situational factors.
Security Policy

The organization should establish a well-made security policy. Both technical policies as well as policies that focus on the individual perspective should be included. To make the security policy as hard-hitting as possible, it must be promoted from the company’s top management tier, embed all company’s processes and back it up with awareness training (Zurkus, 2016).

One of the most important aspects of the security policy is a clearly defined line of conduct, how things are supposed to be done. The employees should understand the course of action when sharing any kind of information inside the company. If something is asked to be done outside this procedure, it’s a red flag. In this case, the employer should simply ask its’ manager about it, if given the green light, the demanded information can be shared. Social engineers are also specialists at making the target feel pressured in to making decisions, this is also seen as a red flag.

If the employees don’t follow the security policy, it is useless. Therefore, organizations are required to actively check that the policies are adhered to. This is done by actively monitoring the employees. Such control methods can include analysing network logs, re-confirm employees’ authentication and to carry out made up social engineering attempts on its’ employees. In whatever it concerns when it comes to learning, people learn from their mistakes. For that reason, it’s so important to conduct these controlled tests. People will most likely feel somewhat of embarrassment for falling victim, and results in them being more alert next time they are asked to share information (Conteh et al. 2016).

When developing the internal policies with respect to cybercrime prevention, Pfleeger et al. (2012) suggests that there are areas of behavioural science that should be taken into account. Previous research on behavioural science shows that individuals tend to perceive and act differently in specific situations. By understanding these concepts and acting accordingly, organizations give themselves the chance to get more protected. For organizations to be able to change the beliefs and behavioural patterns, cognitive dissonance should be something every organizations should be aware of. An example is, the system would point out when an employee is acting stupidly in terms of risky cyber behaviour and make them aware of it. This would lead to a feeling of discomfort, and to get rid of the dissonance, the employee would have to be forced to change its’ cyber behaviour.

Understanding bias is also something useful when trying to promote a change in behaviours. Three biases that Pfleeger et al. presents are, Status Quo Bias, Optimist Bias Control Bias. Status Quo Bias shows how individuals usually stick to their current behaviour if they’re not given a convincing incentive to do so. To reduce this, systems should be able to create incentives to detect threats and act on them, aswell as providing feedback of their actions. Optimist Bias is when employees are underestimating the risk of anything occurring. This often leads the employees to avoid security measures. Control Bias describes when individuals think they can control an uncontrollable situation. Since they think they have control over the risks, employees are less likely to use preventive care measures (Pfleeger et al. 2012).

Technical Guidance

For the behavioural changes to have any impact, a multi-layered technical system must be in place. To keep the data protected, the organization needs well designed software that are installed on every device. Software’s such as; Intrusion Prevention Systems (IPS), Virtual Private Networks (VPN) and Intrusion Detection Systems (IDS). The employers should also have good spyware and antivirus software installed on their private devices (Conteh et al. 2016). Leon (2008) promotes organizations to use password management software programs to
securely handle all network passwords. The software does this by encrypting and randomizing the passwords, leading to a drastic decrease in password thefts.

**Future prevention of cybercrime**

Firstly, as cybercrime is evolving, and we are moving towards an even more digital work environment, the best way to prevent cybercrime in the future is to give up information about how these different cybercrimes in the past have occurred. All affected parties should release information about the crimes committed to the society and the business community to give more transparency regarding these issues. The conclusion is, that this would work like an “opensource” community or in other words a free service where all businesses and other parties could protect themselves by checking past breaches and how others were breached. Abraham S. et al. (2010) also talks about a synergy between governments, ISPs (internet service providers) and end users to reduce future and current issues related to cybercrime.

Secondly, another issue to deal with is the constant maintenance of cyber security. The businesses/governments can’t assume that the security is unbreachable or think that it is enough to have the latest security software’s. It was David Bernstein president of The Bernstein Agency that said, “For every lock, there is someone out there trying to pick it or break in..”. This highlights even more that these “security officers” of the entities needs to stay pessimistic, constantly maintain and test the system to prevent future problems and discover weak links.

Thirdly, education awareness of employees and end users is one of the key factors to prevent cybercrime. It is important to see that all employees know the risks and ways of cybercrime to minimalize the risk of getting targeted by cybercrime attackers. This was already verified by Fadi A. Aloul (2012) in his article that “While organizations expand their use of advanced security technology and continuously train their security professionals, very little is used to increase the security awareness among the normal users, making them the weakest link in any organisation.”. So what Fadi A. Aloul (2012) means is that the pressure should not only be put on the “security officers” but also on the normal employee to get more coverage. These cybercrime educations could be done by having a monthly or quarterly workshop discussing new issues regarding cybersecurity and security breaches that is connected to that department and other related issues.
Figure 3. The Figure 3 is taken from Conteh, N. Y., & Schmick, P. J. (2016). “Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks” (figure 3), but the figure design has been changed by the authors.

The above figure from Conteh et al. (2016) article is a good example that shows which entities that are targeted regarding social engineering attacks. The biggest targets are new employees, clients & customers and IT professionals. This strengthen the view on future prevention of cybercrime which is discussed above, that businesses need to educate their employees, both new and old and of course do maintenance on current security systems.

**Conclusion**

The main conclusion in this paper is that we need to change the way we look at cybercrime and realize that it is spreading and getting more and more common. The ways and motives of committing cybercrime are various but social engineering is one of the most common ways and the motives behind this can be different depending on the attacker. In this article we have identified 3 main motives behind cybercrime:

1. Financial gain
2. Political agenda
3. Intellectual challenge

Behavioral science is one of the most important pillars after computer science regarding cybercrime and in many cases, it is not that the cybercrime itself is extremely sophisticated, but it is due to human errors and lack of education the cyber attacker can accomplish his intents. The main measures against social engineering was discussed from Conteh et al. (2016) article and five measures were discovered:
In Das Sumanjits and Nayak Tapaswinis (2013) article they present a quote from Valerie McNiven, who is a U.S. Treasury Advisor and she indicates that the revenue from illegal drugs ($105 Billion) were less than, revenue from cybercrime and this was already in 2013. As we see an increasing trend in cybercrime we need to open our eyes and grab these issues when it is still possible. A combination of security information flow, education awareness and constant maintenance of security systems is a crucial and a good way of future and current cybercrime prevention for businesses and other end users.

Future guidance and outlook regarding this topic are that business owners and governments should invest in education of current and new employees regarding cybercrime. When employees are educated in issues regarding cybercrime the employers eliminate many problems that are connected to social behavior and cybercrime, e.g. human errors.

References


TechTarget. Worms. Available: https://searchsecurity.techtarget.com/definition/worm