THE FUTURE OF ENTITY DUE DILIGENCE

January 2018

KEITH FURST

Introduction

The world has gone through an incredible amount of technological transformation over the past ten years. While it may seem hard to imagine that change will continue at this pace, it's not only likely to continue, but it will accelerate. There are various functional areas within institutions that support global commerce, but some have been laggards in adopting new technology for a plethora of reasons.

Structural market trends will force organizations to innovate or they will be subject to consolidation, reduction of market share, and, in some circumstances, complete liquidation. Future proofing the entity due diligence process is one key functional area that should be part of an organization's overall innovation road map because of the impacts of trends such as: rising regulatory expectations, disruptive deregulation initiatives, emergence of novel risks, explosion of data, quantifiable successes in artificial intelligence (AI), and changing consumer expectations.

Entity due diligence continues to be a struggle for many financial institutions as regulatory requirements such as beneficial ownership continue to expand in breadth and depth. One of the fundamental struggles to resolve is the identification of the entity with the information used during the due diligence process which can be scattered across various data sources, manual to access and screen, and at times riddled with data quality issues.

The future of entity due diligence is not written in stone, but as will be argued later there is an opportunity to shape its future. The future of entity due diligence is not only about shaping its future, but also includes us, people, and the role we play in that future.

This paper will outline some of the key trends that will drive the transformations of the entity due diligence process and what the future could start to look like.

Modeling Possible Futures

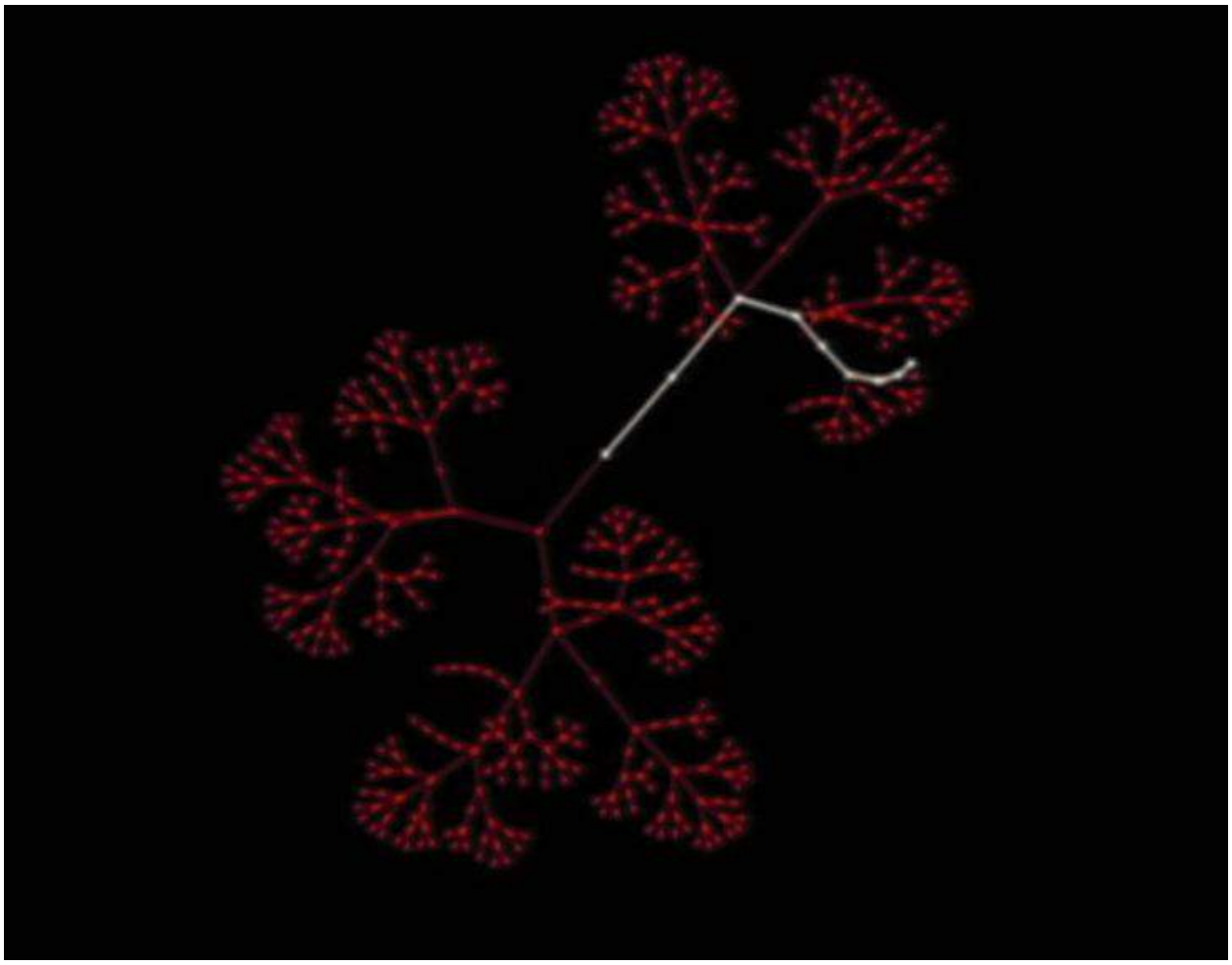
To understand the future entity of due diligence, we should attempt to understand, to a certain degree, some of the history which led up to its current state. While it would be impractical to document every historical incident which led up to the current legislative and institutional frameworks, it is useful to imagine entity due diligence as a result of actions and interactions among many distributed components of a complex adaptive systems (CAS).

The study of CAS or complexity science emerged out of a scientific movement where the goal was to understand and explain complex phenomena beyond what the traditional and reductionist scientific methods could offer. The movement's nerve center is the Santa Fe Institute in New Mexico, a transdisciplinary science and technology think tank, which was founded in 1984 by the late American chemist, George Cowan. Researchers at the institute believe they are building the foundational framework to understand the spontaneous and self-organizing dynamics of the world like never before. The institute's founder, Mr. Cowan, described the work they are doing as creating, "the sciences of the 21st century."

CAS are made up of a large number of components, sometimes referred to as agents, that interact and adapt. Agents within these systems adapt in and evolve with a changing environment over time.

CAS are complex by their very nature, meaning they are dynamic networks of interactions, and the behavior of the individual components doesn't necessarily mean the behavior of the whole can be predicted, or even understood. They are also adaptive so that the individual and collective behavior can self-organize based on small events or the interaction of many events. Another component of these systems is that emergent patterns begin to form which can be recognized. e.g. formation of cities

Another key element of CAS is that they are intractable. In other words, we can't jump into the future because we need to go through the steps. The white line in the image below shows the steps of a system from the past to the present, and the red dendrite like structures are other possible futures that could have happened, if a certain action was taken at a particular point in time.



Source: YouTube TEDxRotterdam - Igor Nikolic - Complex adaptive systems

These models suggest that no one knows everything, can predict everything, or is in total control of the system. Some entities have greater influence over the evolution of the system as a whole than others, but these models imply that everything can influence the system, even a single person.

The entity due diligence process involves many agents interacting and responding to one another which include, but are not limited to: financial institutions, companies, governments, corporate registries, formation agents, challenger firms, criminals, terrorists, and many more. By examining the complexity of the due diligence space, and how technology is constantly reforming agents relationships to one another, can firms, and people within those firms, help chart a course for the future of due diligence and their place within it?

The Evolution of Criminals and Terrorists and Reactions from Law Enforcement

The history of the anti-money laundering (AML) regime in the United States could be understood through the lens of a CAS. Before any AML legislation existed the US government prosecuted criminals such as Al Capone, for tax evasion as opposed to other crimes.

In 1970, the US passed the Banks Records and Foreign Transactions Reporting Act, known as the Bank Secrecy Act (BSA), to fight organized crime by requiring banks to do things such as report cash transactions over $10,000 to the Internal Revenue Service (IRS).
Another key development in the history of the AML regime was the prosecution of a New England bank for noncompliance with the BSA, another seemingly small event, had far reaching consequences as it prompted Congress to pass the Money Laundering Control Act of 1986 (MLCA).

But as we know today, the US government passed the BSA, but criminals and criminal organizations continue to evolve, as cash structuring or using money mules are common methods to avoid the reporting requirement.

Drug Cartels

Clearly, the rise of the Colombian and Mexican drug cartels in the 1970s and 80s show how agents of a CAS act and react to one another. In 1979, Colombian drug traffickers were killed in a shootout in broad daylight in Dadeland Miami mall. This event and many others clearly got the attention of US law enforcement and in 1982, the South Florida Drug Task force was formed with personnel from the Drug Enforcement Agency (DEA), Customs, Federal Bureau of Investigation (FBI), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Internal Revenue Service (IRS), Army, and Navy.

By the mid 1980s, as the South Florida Drug Task force started to succeed in reducing the flow of drugs into the US via South Florida, the Colombian cartels reacted and outsourced a lot of the transportation of cocaine to the US via Mexico with the help of marijuana smugglers.

Mexican drug cartels continue to evolve and innovate as they have reportedly used unmanned aerial vehicles (UAV), more commonly referred to as drones, to fly narcotics from Mexico over the southwest border to San Diego and even experimented with weaponizing drones with improvised explosive device (IED) equipped with a remote detonator.

9/11 and the Evolving Threat of Terrorism

The above examples pale in comparison to the impacts of the 9/11 terrorist attacks on the United States that killed almost 3,000 people and caused billions of dollars in property damage, economic volatility, cleanup costs, health problems for people living or working near the site, job loss, tax revenue loss, and many other cascading effects. Shortly after the 9/11 terror attacks, Congress passed the Patriot Act which was designed to combat terrorism, including its financing.

However, as the US and other countries have enacted laws to prevent the funding of terrorism, terrorists have reacted or evolved by opting to use legitimate funding sources such as government benefits, legitimate income, and small loans to launch low cost attacks. The French government estimated the November 2015 Paris attacks cost a maximum of 20,000 euros.

Vehicles have been used as ramming weapons in terror attacks in London, Berlin, Nice, Barcelona, and New York which simply amounted to the cost of fuel, and possibly a rental charge. This also points to the changing nature of the types of people who are engaging in these types of attacks that usually have a criminal background and are radicalized by content online as opposed to operating within a well financed and organized cell of a larger terror group.

But is it only the content online that radicalizes people or does most terrorist recruitment happen face-to-face? According to research by Washington University's Professor Ahmet S. Yahla, Ph.D., just over 10 percent of the 144 people charged with ISIS-related offenses in US courts were "radicalized online." Professor Yahla ran a program, in a Turkish city on the southern border with Syria, to intervene with school-aged children at risk for recruitment by terrorist organizations. Professor Yahla found that most families weren't aware that their children were being approached by terrorist recruiters and were open to intervening to ensure their children were not radicalized.

The Professor's assertion that most of terrorist recruitment happens face-to-face seems to make sense because we have all experienced the power of a personal referral. If, a person you like and trust makes a recommendation to you then you are much more likely to act on it, rather than be prompted to act through some passive media online. This also implies that networks of people exist, in countries where attacks take place, that believe in various terrorist ideologies, but not all of those believers take up arms.

Naturally, this leads to the idea that even if internet service providers (ISP) and social media companies could remove a lot of the terrorist propaganda online, it wouldn't stop so called 'lone wolf' terror attacks as the system would evolve and rely more on face-to-face recruitment as small communities of people with shared beliefs and values find ways to congregate.

However, this doesn't mean that laws such as the Patriot Act are not effective against preventing terrorism because they are without a doubt, they are creating barriers against large scale terror attacks, but terrorism and its agents are constantly evolving. While the Patriot Act and similar laws allow for broader surveillance powers by governments, terrorists know this and have reacted by using encrypted messenger applications such as the Telegram to communicate and spread propaganda.

All of this suggests that the fight against terrorism needs to be a multi-pronged approach including, but not limited to preventing terror groups access to the financial markets, intervening early with at-risk youth, tackling various socio-economic issues that could contribute to feelings of alienation of impressionable youth, and countering compelling social media delivered by ISIS through public private partnerships (PPP) by launching an ongoing and strategic counter-narrative.

Drivers of Regulation

The motivations for new regulations can come in many different forms such as combating terrorism, drug trafficking, money laundering, tax evasion, securities fraud, financial fraud, acts of foreign corruption, etc.. As discussed in the previous section, terrorism continues to evolve as there have been a growing number of low-cost of attacks which will keep it at the top of political agendas for years to come.

Data and technology are integral parts of what are driving new regulations on various fronts. The rise of smartphones, explosion of data, proliferation of the internet of things (IOT), and other sensor technology has fundamentally changed the speed at which data can be accessed, transferred, analyzed, and acted upon. There will be various regulatory rules examined later in this paper which, in one way or another, can be linked to technological transformations.

The most pressing example of how technological transformation can influence regulation can be observed with the Panama Papers data leak. While it could be argued that it was simply the actions of one person, or a group of people, the leak would only be possible if the technological framework was already in place to store, distribute, and analyze all of those documents rapidly and truly understand the implications of them.

Would the Panama Papers data leak even be possible in 1940?

Atomic Secrets Leak

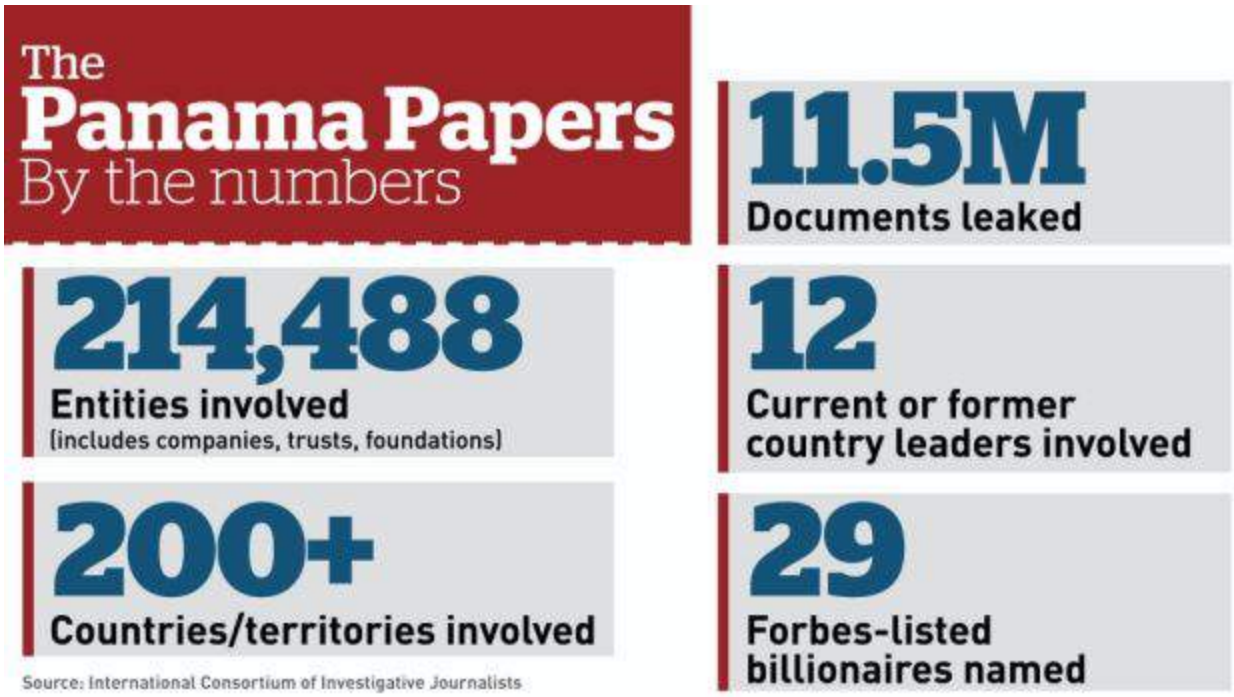
Maybe not on the scale of the Panama Papers, but data leaks are not something completely new as several Americans and Britons helped the Union of Soviet Socialist Republics (USSR) become a nuclear power faster than it could on its own, by leaking military secrets. Some scientists contend that the USSR and other countries would have obtained a nuclear bomb on their own, but the data leaks likely accelerated the process by 12 to 18 months or more.

Klaus Fuchs is commonly referred to as the most important atomic spy in history. Fuchs was born in Germany and was actively engaged in the politics of the time. Fuchs immigrated to England in 1933 and earned his PhD from the University of Bristol. Eventually, he was transferred to Los Alamos labs in the early 1940s where he began handing over important documents about the nuclear bomb's design and dimensions to the USSR. There were other spies giving nuclear secrets to the USSR with various motivations such as communist sympathies or thinking that the more countries that had access to nuclear technology would decrease the probability of nuclear war.

The amount of nuclear secrets leaked to the USSR may have not been that massive in terms of storage space if we imagine all of those documents being scanned as images or pdf files, but the implications of the USSR having that information during World War II was very serious. So, data leaks have not emerged out of nowhere, but the scale and speed at which information can be distributed is clearly very different today than it was 70 years ago. It's much easier to stick a Universal Serial Bus (USB) drive into a computer rather than trying to walk out of an office building with boxes full of files.

The Data Leak Heard Round the World

The Panama Papers had a tsunami effect on global regulations as it prompted countries around the world to re-evaluate their corporate registry requirements and the use of shell companies to hide beneficial ownership. The first news stories about the Panama Papers leak appeared on April 3, 2016 and just over a month later the US Financial Crimes Enforcement Network (FinCEN) issued the long awaiting Customer Due Diligence (CDD) final rule. The magnitude of the Panama Papers is revealed in the sheer volume of documents, entities, and high profile individuals involved as shown in the image below.



Source: International Consortium of Investigative Journalists

Data is a significant part of the driver for new regulation which stem from a wide range of activities including money laundering, corruption, human trafficking, tax evasion, etc. There are a wide variety of regulatory rules, which institutions had to prepare for across the globe, coming into full force into 2018 such as the Payment Services Directive (PSD2) in the European Union, the CDD final rule, the New York State Department of Financial Services (NYDFS) risk based banking rule, and others.

The impact of the Paradise papers is still yet to be fully realized, but it's fair to assume that it will contribute to the trend of increased regulation and scrutiny of the financial services industry. Whether or not there is an immense amount of explicit wrongdoing identified the public perception of offshore tax havens and shell companies continues to take on a negative light.

Based on current regulatory expectations for financial institutions and other structural and market trends such as the digital experience, new and evolving risks, increased competition, technological progress, growth of data, and the need to make better decisions and control costs the entity due diligence process will be drastically different than it is today for the financial services industry.

The Murder of a Journalist

The Panama Papers are still having cascading effects across the globe and one of the most tragic examples of this in 2017 was the assassination of the Maltese journalist, Daphne Caruana Galizia, by a car bomb. Mrs. Galizia was a harsh critic of Maltese political figures accusing some of corruption and international money laundering much of which was revealed by the Panama Papers. She also highlighted the links between Malta's online gaming industry and the mafia. The only other journalist killed in the EU during 2017 was Kim Wall who was allegedly killed and dismembered by the Danish inventor, Peter Madsen.

Source: https://www.theguardian.com/world/2017/oct/16/malta-car-bomb-kills-panama-papers-journalist

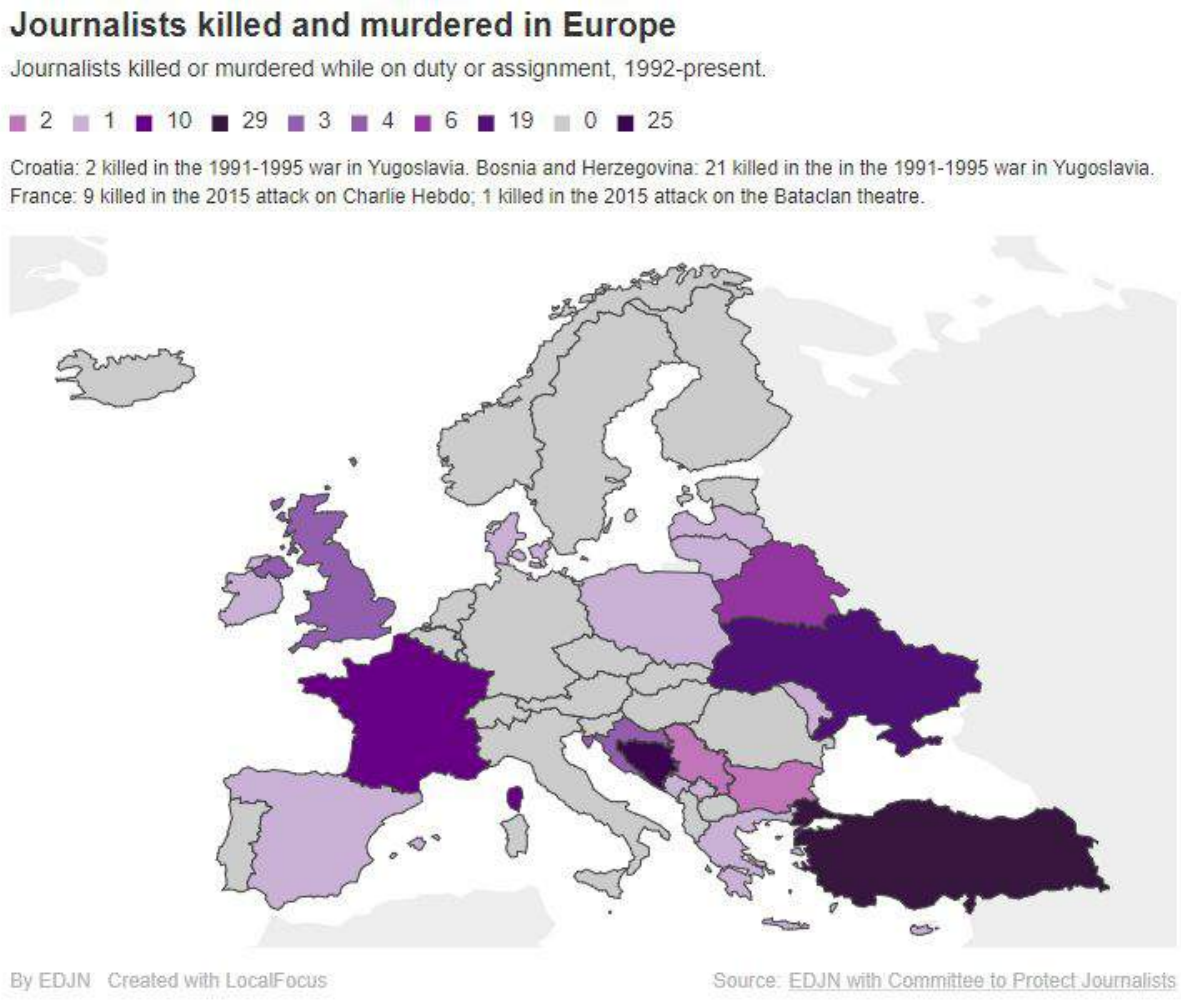
The difference between the murder of the two journalists, was that in the case of Mrs. Galizia, there is a strong indication that her reporting on corruption and money laundering could be the underlying motive for her death. However, the death of Mrs. Wall appears to be more random and unplanned event as the circumstances that led up to her death are still unclear.

According to the Committee to Protect Journalists (CPJ) there were 248 journalists killed since 1992 who reported on corruption and only 7 of them happened in the EU[1]. The top 5 countries

[1] 3 out of the 7 murders happened in Croatia, Cyprus and Lithuania before they were part of EU

for murdered journalists, who reported on corruption, since 1992 was the Philippines, Brazil, Colombia, Russia, and India totaling 34, 26, 24, 21, and 17 respectively.

Outside of reporting on corruption, one of the main drivers of murdered journalists in Europe since 1992 to the present was war and terrorism which makes the case of Mrs. Galizia, all the more shocking. The war in Yugoslavia created a high-risk reporting environment for journalists and left 23 of them dead. On January 7, 2015, two brothers marched into the Charlie Hebdo offices and massacred 12 people, 8 of them journalists, which was the worst attack against the Western media since 1992.



Source: http://www.voxeurop.eu/en/2017/freedom-press-5121523

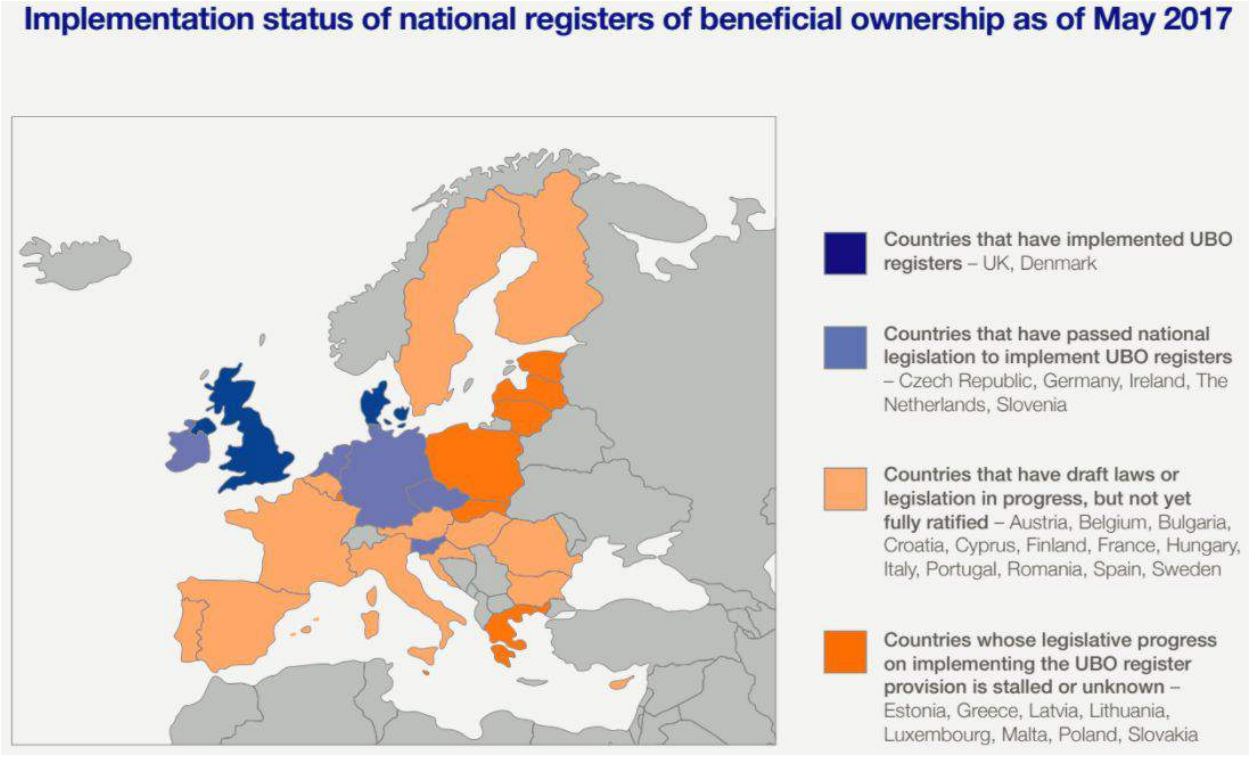
The worst attack against the media worldwide in recent memory occurred in the Philippines in 2009, when gunmen killed 32 journalists and 25 civilians in the Maguindanao province which is a predominantly Muslim region of Mindanao. Terrorism was the common factor that linked the

Charlie Hebdo attack and the Maguindanao massacre. However, there is another factor common factor that underlies the murder of Mrs. Galizia in Malta, the Charlie Hebdo journalists in France, and the reporters in the Philippines which is that terrorism and corruption can be linked to shell companies.

This is not to say that any of those specific attacks were explicitly linked to use the of shell companies, but there is a common theme that criminals, corrupt politicians, and terrorists use shell companies as a tool to hide their identities as exposed by the Panama Papers.

There is already action being taken by the European Parliament as it passed a motion in November 2017, stating that Malta's country police and judiciary "may be compromised." The murder of this journalist is extremely tragic and it could prompt more aggressive moves from the EU to get its member states up to regulatory standards, especially in the area of beneficial ownership.

It could be argued that the EU is only as strong as its weakest link, so can the EU accept its members exhibiting low standards of justice and law enforcement?



Source: Bureau Van Dijk - A Moody's Analytics Company

Regulations Coming into Force in 2018

There are three important financial service regulations coming into force in 2018 which are the CDD final rule in the United States, PSD2 in the European Union, and the NYDFS risk based banking rule in New York.

The CDD final rule was on the US legislative radar for some time, but it appears the Panama Papers expedited its approval. While the CDD final rule is a step in the right direction it does place additional burdens on financial institutions without addressing other issues such as specific states in the US still allowing companies to incorporate without collecting and verifying beneficial ownership.

The reported titled Global Shell Games: Testing Money Launderers' and Terrorist Financiers' Access to Shell Companies, stated that, "It is easier to obtain an untraceable shell company from incorporation services (though not law firms) in the US than in any other country, save Kenya." There are two bills that were introduced to the Senate and Congress which are supposed to address the weak state corporate formation laws and this will be discussed in a later section.

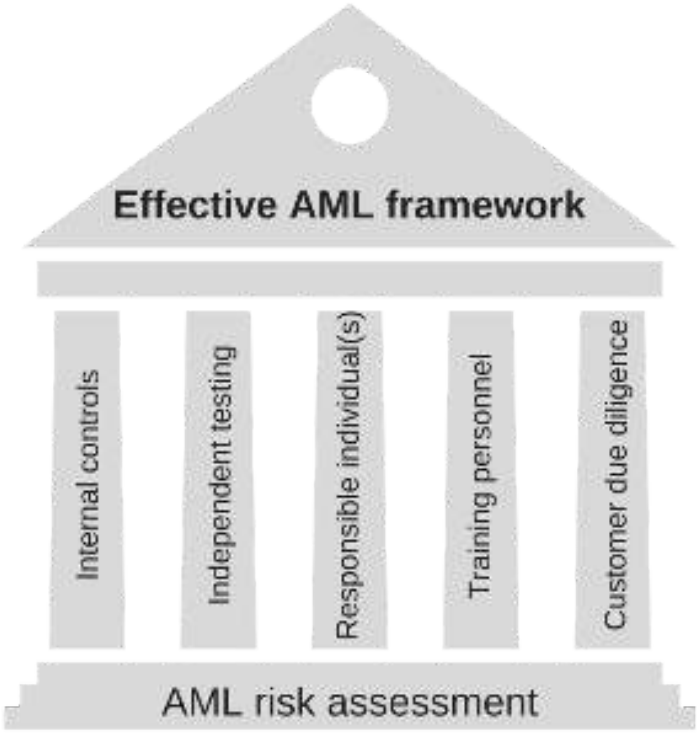
PSD2 is one of the most unique financial regulations because it is arguably one of the few instances where legislators adopted a proactive as opposed to reactive regulatory framework. The motivations for the regulation were to increase market competition, consumer protection, and the standardization of infrastructure in the payments sector by mandating banks create mechanisms for third party providers (TPP) to access customer's bank information. What's interesting about this regulation is that it will have a significant impact on the market, but there wasn't a discernible negative event which drove its adoption.

Instead the regulation is forward looking, as its supporters realized, quite astutely, that incredible amounts of change are on the horizon for the financial services sector due to technological disruptions. Since, EU regulators can see the future coming, to a certain degree, they have enacted legislation to help shape the future of payments with sensible regulations which will help increase standardization, security, and consumer protection.

The NYDFS risk based banking rule is also very interesting because it introduces more accountability on New York regulated financial institutions' senior leadership to certify the institution's AML program. The rule highlights that the reviews it conducted have identified many shortcomings in transaction monitoring and filtering programs and a lack of governance, oversight, and accountability.

Customer Due Diligence (CDD) Final Rule

In the US, the long awaited CDD final rule adds the fifth pillar to an effective AML program. In reality, many financial institutions have already integrated CDD into their overall AML program. The other four pillars of an effective AML framework, which are built upon an AML risk assessment, are: internal controls, independent testing, responsible individual(s), and training personnel.



Source: Data Derivatives

For example, in terms of transaction monitoring some banks would use the risk rating of a customer as another way to prioritize their alert queues. In other words, a customer which is perceived by the institution as being higher-risk would have their activity investigated first when compared to similar activity of a lower-risk client.

One of the major impacts to financial institutions in 2017 was the preparation to comply with the new beneficial owner requirements for the impending May 11, 2018 deadline. There were definitely challenges to comply with this new rule from an operational perspective, especially at large banks, because of the siloed structure of client onboarding and account opening processes. Banks can have dozens of onboarding and account opening systems and trying to

coordinate where the know your customer (KYC) process is for a particular customer, at a given point in time, and when the handoff to the next system happens, can be extremely challenging.

Also, the account opener certification created wrinkles in the operations process, and questions arose regarding how long a certification was active and if one certification could support multiple account openings.

Also, the CDD final rule is based on *trusting* the customer, but as discussed in a recent article, in the Journal of Financial Compliance (Volume 1 Number 2), by the Head of Financial Institutions & Advisory in North America for Bureau van Dijk - A Moody's Analytics Company, Anders Rodenberg, there are three inherent flaws of asking companies to self-submit beneficial ownership information which are:

1. lack of knowledge;
2. missing authority; and
3. no line of communication when changes happen.

While US banks would be in compliance with the rule if they simply collected beneficial ownership based on what their customers supplied, it may not accurate all of the time. This is why it would be prudent for a financial institution to collect beneficial ownership from the client, and also use a third party data source such as Bureau Van Dijk's Orbis as another method of coverage and verification.

If, there was a gap between what the customer provided and what Orbis has then it could be a factor to consider when determining which customers should undergo enhanced due diligence (EDD). Also, the more beneficial owners identified, either disclosed or uncovered, creates an opportunity to screen more individuals through adverse media, politically exposed persons (PEP), and sanctions lists. This allows for greater confidence in a institution's risk-based approach given the broad coverage.

Finally, financial institutions in the US and elsewhere should be monitoring global standards and consider that the CDD Final Rule or similar regulations could be amended from the trust doctrine to the trust and verify concept as detailed under the Fourth Anti Money Laundering Directive (AML4).

Sanctuary Corporate Formation States

There are two bills, aimed at addressing beneficial ownership gaps in the US, that were introduced to the Senate and Congress which are the True Incorporation Transparency for Law Enforcement (TITLE) Act (S. 1454) and the Corporate Transparency Act (H.R. 3089/S. 1717). Both proposals cite similar findings of how criminals can exploit weakness in state formation

laws. The TITLE Act specifically mentions the Russian arms dealer, Victor Bout, who used at least 12 companies in the US to, among other things, sell weapons to terrorist organizations trying to kill US citizens and government employees. Additionally, the TITLE Act refers to other major national security concerns such as Iran using a New York shell company to purchase a high-rise building in Manhattan and transferring millions of dollars back to Iran, an Office of Foreign Asset Control (OFAC) sanctioned country, until authorities found out and seized the building.

Both bills have reasonably good definitions of beneficial ownership and the requirements to collect identifiable information. Also, both bills allow up to $40 million dollars available for implementation costs with the new rules which will be funded by asset forfeiture funds accumulated from criminal prosecutions. There are common sense proposals in both bills such as exemptions for publicly traded companies, companies with a physical presence, minimum number of employees, and minimum annual revenue.

The one distinction between the two bills is that the TITLE Act requires states to comply with the bill, but it doesn't penalize states if they fail to comply. If, history is any guide then the TITLE Act could lead to a scenario similar to sanctuary cities, where local city governments fail to cooperate with federal immigration authorities.

If, the TITLE Act was adopted then how do we know that states such as Delaware will comply? Could the US could end up with 'sanctuary corporate formation states'?

The Corporate Transparency Act takes a slightly different approach where the states are not required to collect beneficial ownership, but if states are in noncompliance with the statue then companies incorporating in those states are required to file their beneficial ownership information with FinCEN. While it could be argued this bill is slightly better than the TITLE Act, its not clear how FinCEN will monitor and enforce companies out of compliance with this regulation.

The ideal scenario for the US would be that all states collect beneficial ownership in the same standardized fashion or in another extreme example, if some states fail to comply, then the federal government would take over the authority to form corporations and remove the rights from states. The latter scenario would not be ideal and would be very unlikely to get passed by the Congress and the Senate unless there were some extreme circumstances, possibly equivalent to another 9/11 terrorist attack tied to the use of shell companies in the US. There would be significant economic and social implications of such a change so it appears that beneficial ownership doesn't have enough political capital to initiate such a drastic move.

It also gets into the nuts and bolts of legal theory. Would the supremacy clause of the US constitution hold up or would states try to nullify federal law, arguing that it was unconstitutional?

Payment Services Directive (PSD2)

On October 8, 2015 the European Parliament adopted the European Commission's updated PSD2. The regulation is ushering in a new era of banking regulations which is positioned to increase consumer protection and security through innovation in the payments space. The idea is that consumers are the rightful owners of their data, both individuals and businesses, and not the banks. The regulation mandated that banks provide payment services to TPP via an application programming interface (API) by January 13, 2018.

Essentially, PSD2 will allow TPP to create customer centric and seamless interfaces on top's of banks operational infrastructure. On a daily basis individual and business customers interact with various social and messaging platforms such as Facebook, LinkedIn, WhatsApp, Skype, etc. This regulation will allow a whole array of TPP to enter the payments space accessing banking data of their loyal customer base and even initiate payments on the their behalf assuming the consumer already gave authorization to do so.

Consumers are demanding real time payments as many other parts of the digital experience is real time, so why should it be any different for payments? Financial institutions have made some progress in the payments space as evident by the successful launch and market penetration of Zelle backed by over 30 US banks. Zelle allows customers of participating banks to send money to another US customer, usually within minutes, with an email address or phone number.

The integration is rather seamless because Zelle, can be accessed through the customer's existing mobile banking application and a separate Zelle application doesn't have to be downloaded, but it's now being offered for customers of non-participating banks. It appears that the launch of Zelle, which required extensive collaboration of many leading US banks, was initiated by the risk, some challenger payment providers such as Venmo and Square Cash posed to the industry.

The European Parliament astutely realized that to encourage innovation and competition in the payments space, new rules would need to be enacted. The fact that PSD2 was initiated by the government actually strengthens cybersecurity as opposed to diluting it. The reason is that whether we like it or not, innovation will march on and new FinTech players will continue to emerge. Since, the European Parliament is taking a proactive role in the evolution of the payments space it allows the industry as a whole to think about best practices for security and authentication.

PSD2 is requiring strong customer authentication (SCA) which falls into three basic categories such as:

- Knowledge (e.g. something only the user knows)
- Possession (e.g. something only the user possesses)
- Inherence (e.g. something the user is)

The third category, inherence, opens up one of the most promising applications of artificial intelligence which is biometric authentication, but more specifically facial recognition. This will apply to both individual customers and entities because financial institutions may start to store biometric data of executives who are authorized to perform specific transactions. Biometrics and how it could impact entity due diligence will be discussed later in this paper.

New York State Department of Financial Services (NYDFS) Risk Based Banking Rule

The NYDFS risk based banking rule is requiring covered institutions to certify they are in compliance with the regulation by April 15, 2018. The rule is the first of its kind and identifies the key components of effective transaction monitoring and filtering programs. As mentioned earlier, this rule has highlighted the need for senior management to have greater governance, oversight, and accountability into the management of the transaction monitoring and sanctions screening programs of their institution.

Some of the requirements are straightforward and well known in the industry such as conducting a risk assessment and ensuring a robust KYC program is in place. However, this rule is unique in the sense, that it highlights very specific system, data, and validation requirements. Transaction and data mapping were highlighted as key activities which are specific to the implementation of transaction monitoring and sanctions screening systems.

The focus on data and sound quantitative methods are not new from a regulatory perspective, because many of the requirements in the NYDFS rule can be found in the Office of the Comptroller of the Currency's (OCC) paper, Supervisory Guidance on Model Risk Management. The OCC's paper has traditionally applied to market, credit, and operational risks such as ensuring the financial institution is managing its risk properly to ensure it has enough capital to satisfy reserve requirements and has conducted sufficient stress testing to ensure different market scenarios can be endured.

Many of the high dollar enforcement actions by the NYDFS have involved foreign banks and specifically cite the AML risk of correspondent banking. There have been several phases to the enforcement actions where some banks have actually engaged in systemic wire-stripping,

deleting or changing of payment instructions, to evade US sanctions. As large financial institutions have moved away from these practices the enforcement actions have cited deficiencies in other aspects of the institution's AML program.

This brings up back to a common theme of CAS. For anyone, who has worked with many aspects of an institution's AML program, it's complex. It's not only the systems which are supposed to screen for sanctions and monitor suspicious activity because there are other factors at play such as the interactions between interdepartmental staff, vendor management, emerging financial crime trends, new regulatory rules, staff attrition, siloed information technology (IT) systems, general technology trends, among other things.

In a sense, one interpretation of what the NYDFS rule says, at its essence, is that institutions need to do a better job at managing complexity. And to manage complexity effectively, in complex organizations, support is needed from senior leadership so requiring the annual certification does make sense.

Derisking and Hawala Networks

The interesting part of enforcement actions is that it has led to derisking of correspondent banking relationships by US and European banks to reduce the risk of severe financial penalties and reputational damage. According to a 2017 Accuity research report, Derisking and the demise of correspondent banking relationships, there has been a 25% decrease in global correspondent banking relationships largely due to strategies executed by US and European banks.

This has reportedly left a huge window of opportunity for other countries to move in, and China has been at the forefront by increasing its correspondent banking relationships by 3,355% between 2009 and 2016. The reduction in correspondent banking relationships increases the pressure for individuals and businesses in emerging markets to seek out alternative methods of finance which could increase the power of criminal groups and other nefarious actors offering shadow banking services. The Global Head of Strategic Affairs, Henry Balani opined on the consequences of derisking by stating, "Allowing de-risking to continue unfettered is like living in a world where some airports don't have the same levels of security screening – before long, the consequences will be disastrous for everyone."

There are informal money transfer systems outside the channels of traditional banking such as hawala in India, hundi in Pakistan, fei qian in China, padala in Philippines, hui kuan in Hong Kong, and phei kwan in Thailand. Hawala is an informal money transfer system that has been used for centuries in the Middle East and Asia, and facilitates money transfer without money movement through a network of trusted dealers, hawaladars. The origins of Hawala can be found in Islamic law (Sh'aria) and is referred in texts of Islamic jurisprudence in the early 8th

century, and is believed to have helped facilitate long distance trade. Today, hawala or hundi systems can be found in parallel with traditional banking systems in India and Pakistan.

According to a report issued by FinCEN, Hawala transactions have been linked to terrorism, narcotics trafficking, gambling, human trafficking, and other illegal activities. In John Cassara's book, Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement, he cites evidence has shown that funding for the 1998 US embassy bombing in Nairobi was through a hawala office in its infamous Eastleigh neighbourhood, an enclave for Somali immigrants.

In 2015 it was reported that across Spain, groups such as ISIS and the al-Qaeda-affiliated Nusra Front are funded through a network of 250 to 300 shops - such as butchers, supermarkets and phone call centres - run by mostly Pakistani brokers.

Could the decline of global correspondent banking relationships strengthen informal remittance systems such as Hawala because the average business or person in an impacted geographic area or industry has fewer options now?

This is not to say that US and European regulators should have not aggressively enforced financial institutions compliance failures, but they may need to reevaluate their strategies going forward to ensure the integrity of the global financial system without causing the unintended, and sometimes hard to predict, consequences of derisking. It's not only about ensuring the prevention of terrorist financing, but it's also about allowing access to the global financial system to law abiding businesses and citizens so they don't have to use shadow banking networks which can strengthen various aspects of black markets and criminal networks.

Correspondent banking became increasingly costly because the correspondent banks started to reach out to their customers (respondent banks) to get more information about their respondent banks' customers. The correspondent bank would contact the respondent bank through a request for information (RFI) to understand who the customer was and the nature of the transaction. This created a long and laborious process for correspondent banks to complete and the small revenues generated didn't justify the operational costs and compliance risks of serving high-risk jurisdictions and categories of customers.

One of the main components of the US Patriot Act was the customer identification program (CIP), but in the case of correspondent banks, how do they really know if the respondent banks are conducting effective due diligence on their own customers? While it wasn't the correspondent banks responsibility to verify the identity each and every one of the respondent bank's customers, during some AML investigations, at certain banks, it almost went to that length.

This brings up an interesting question about innovation in the correspondent banking space, and if there could be a way for respondent banks to verify their own customer's identity and somehow share it with their correspondent banks? A number of problems arise with this such as a data privacy, but there have been companies exploring this possibility to prove, to a certain extent, that respondent banks due diligence procedures are robust and accurate.

The Financial Action Task Force (FATF) has stated that, "de-risking can result in financial exclusion, less transparency and greater exposure to money laundering and terrorist financing risks." If punitive fines against financial institutions by regulators was a major contributor to the derisking phenomenon, then what is the role of regulators in supporting innovation to reverse the effects of derisking to ensure the integrity and transparency of the global financial system?

Regulatory Sandboxes

Regulatory sandboxes may be one of the key ingredients needed for compliance departments to innovate, especially in the financial services sector. Financial institutions are under severe scrutiny for money laundering infractions and the United States regulatory regime is notoriously punitive based on the amount of fines levied against institutions which failed to comply.

It was reported that HSBC Holdings engaged the artificial intelligence (AI) firm, Ayasdi, to help reduce the number of false positive alerts generated by the bank's transaction monitoring system. According to Ayasdi, during the pilot of the technology HSBC saw a 20% reduction in the number of investigations without losing any of the cases referred for additional scrutiny.

The bank's Chief Operating Officer Andy Maguire stated the following about the anti-money laundering investigation process:

"the whole industry has thrown a lot of bodies at it because that was the way it was being done"

HSBC is one of the world's largest banks which was fined $1.92 billion in 2012 by U.S. authorities for allowing cartels to launder drug money out of Mexico and for other compliance failures.

So, why would HSBC be one of the first banks to test out an unproven technology and vendor in an area with so much scrutiny and risk?

First, it's worth noting that the pilot took place in the United Kingdom and not the United States. While there are many factors at play in a bank's decision making process, clearly the regulatory sandbox offered by the United Kingdom's Financial Conduct Authority (FCA) could have been a key factor in piloting the new technology.

In November 2015, the FCA published a document titled the 'Regulatory Sandbox' which describes the sandbox and the regulator's need to support disruptive innovation. The origin of the regulatory sandbox goes beyond supporting innovation because the FCA perceives their role as critical to ensure the United Kingdom's economy is robust and remains relevant in an increasingly competitive global marketplace. The FCA's perception of their essential role in the continued growth and success of the United Kingdom's financial services sector is succinctly summarized below:

"To remain Europe's leading FinTech Hub, we have to ensure that we continue to be an attractive market with an appropriate regulatory framework."

The FCA is not the only regulatory regime to discuss the importance of innovation as government officials in other countries have publicly discussed technology as a means to advance various functions within the economy. On September 28, 2017, at the Institute of Singapore Chartered Accountants' Conference, the Deputy Prime Minister Of Singapore, Teo Chee Hean, made the following comments about the use of technology in the fight against transnational crime.

"We will increasingly have to use technology and data analytics (to strike) back at them, to detect and pursue transnational crime and money laundering, strengthen our regulatory framework enforcement approach, and collaborate more closely with our international counterparts…"

Mr. Teo's comments about transnational crime make sense because Singapore is arguably the safest country in Southeast Asia, and one of the safest countries in the world. Hence, Singapore's touchpoint with crime is at the transnational level, in the form of trade finance and other financial instruments through its extensive banking system.

Singapore also has its own regulatory sandbox and on November 7, 2017 just on the heels of Mr. Teo's comments, it was reported that OCBC engaged an AI firm which helped it reduce its transaction monitoring system alert volume by 35%.

It's not only financial institutions that are experimenting with AI to fight financial crime because the Australian Transaction Reports and Analysis Centre (AUSTRAC) collaborated with researchers at RMIT University in Melbourne to develop a system capable of detecting suspicious activity for large volumes of data.

Pauline Chou at AUSTRAC indicated that criminals are getting better at evading detection and the sheer transaction volume in Australia requires more advanced technology. Ms. Chou told

the New Scientist: "It's just become harder and harder for us to keep up with the volume and to have a clear conscience that we are actually on top of our data."

It's worth noting that the Australia supports its own innovation hub and sandbox to explore the prospects of fintech, but at the same time do a better job at combating financial crime, terrorist financing, and various forms of organized crime.

On October 26, 2016 the Office of the Office of the Comptroller of the Currency (OCC) announced it would created an innovation office to support responsible innovation. While several countries have embraced the notion of a regulatory sandbox, the United States regulators are preferring to use different terminology to ensure financial institutions are held responsible for their actions or lack thereof. The OCC Chief Innovation Officer Beth Knickerbocker was quoted as saying that the OCC prefers the term "bank pilot" as opposed to "regulatory sandbox," which could be misinterpreted as experimenting without consequences.

According to a paper published by Ernst and Young (EY), China has leapfrogged other countries in terms of fintech adoption rates which is mainly attributed to a regulatory framework that is conducive to innovation.

As discussed financial institutions are beginning to leverage AI to reduce false positive alerts from transaction monitoring systems and identify true suspicious activity. The same concept also applies to the future of entity due diligence. As new technology is developed to simplify and optimize the due diligence process, then organizations which operate within jurisdictions that support innovation will be more likely to be the early adopters and reap the benefits.

Digital Transformation

It's hard to imagine how to survive a day without our phones as they have become such integral parts of our daily lives. Being able to send an email, make a phone call, surf the internet, map directions, and watch a video all from one device that fits into our pockets is somewhat remarkable. At the same time its somewhat expected given computing power has doubled every two years according to Moore's law. It's not only mobile phones because we can see the digital transformation everywhere, even in the public sector which can be slow to adopt new technology.

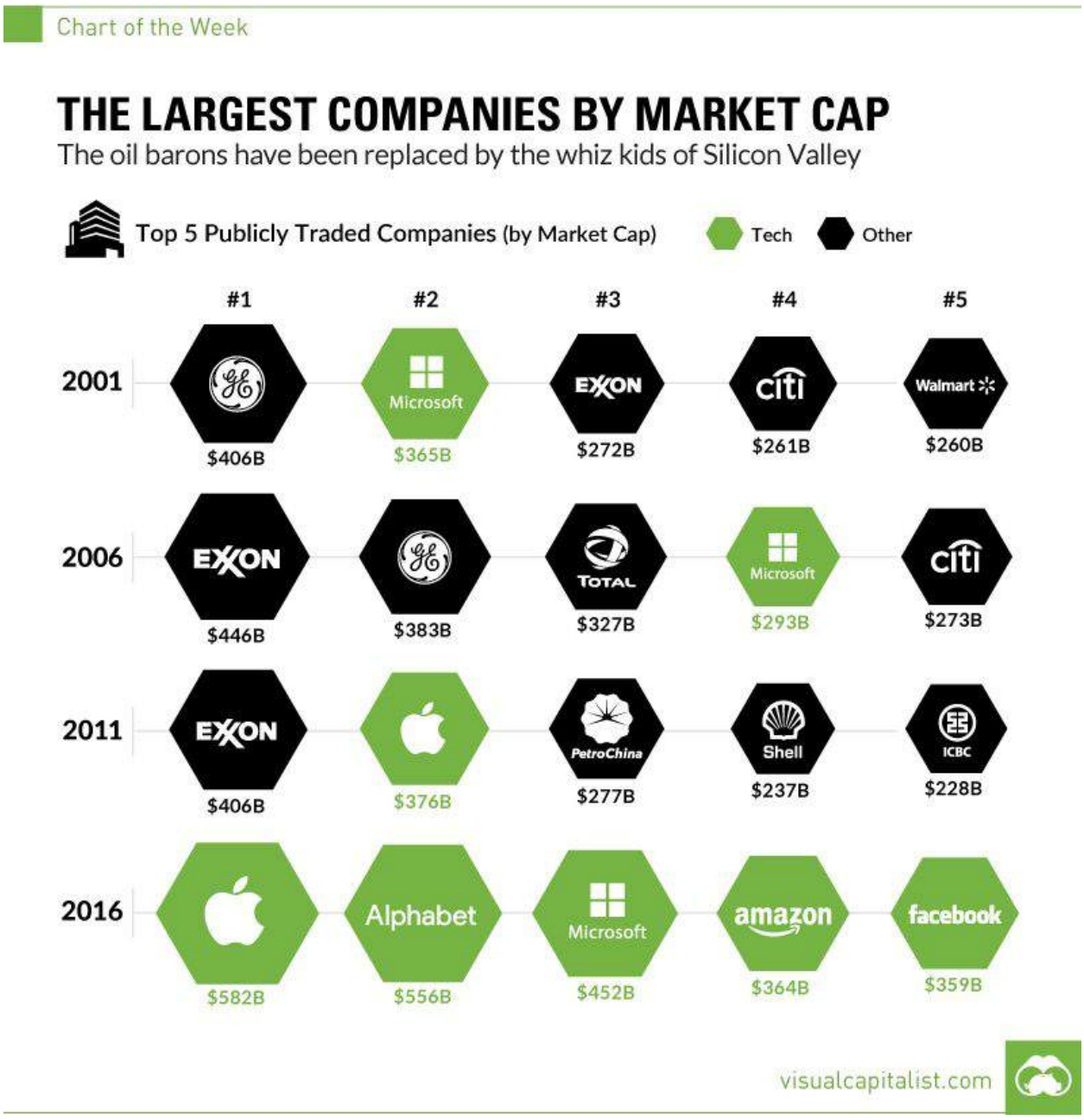
The Queens Midtown Tunnel that connects the boroughs of Queens and Manhattan in New York has converted to cashless tolling joining the ranks of other US cities in California, Utah, and Washington. Cashless tolling is a large upfront cost to implement the necessary systems to support the process and there are construction changes needed to renovate the infrastructure.

Also, other bridges have reported a spike in uncollected tolls and a loss in revenue after going cashless.

However, there are significant benefits such as reducing traffic congestion in the city which helps alleviate some of the air pollution from idling vehicles. Also, the staff needed to facilitate the collection, transportation, and computation of bills and coins is a high administrative cost for the city. This highlights concerns many people share, which is that automation and technological innovation in general will take jobs away from people, but legislators believe the advantages of cashless tolling outweigh the disadvantages in the long-term.

Similarly, as we go through various digital transformations as individuals, businesses need to follow suit or potentially be disrupted given that consumer expectations are evolving, or, at the very least, open to easier ways of doing things. Uber is a strong example, along with other assetless firms, of a company that leveraged technology to completely disrupt a market such as the taxi industry which has historically been fairly stagnant.

In 2001, 2006, and 2011, there was only one technology company, Microsoft or Apple, listed as one of the top 5 companies in the US by market capitalization. In 2016, only 5 years later, all 5 companies were technology companies which clearly shows the speed at which times have changed. The Economist published an article, “The world’s most valuable resource is no longer oil, but data,” which highlights that all 5 of those companies have created elaborate networks, based on physical devices, sensors or applications, to collect enormous amounts of data.



Source: http://www.visualcapitalist.com/chart-largest-companies-market-cap-15-years/

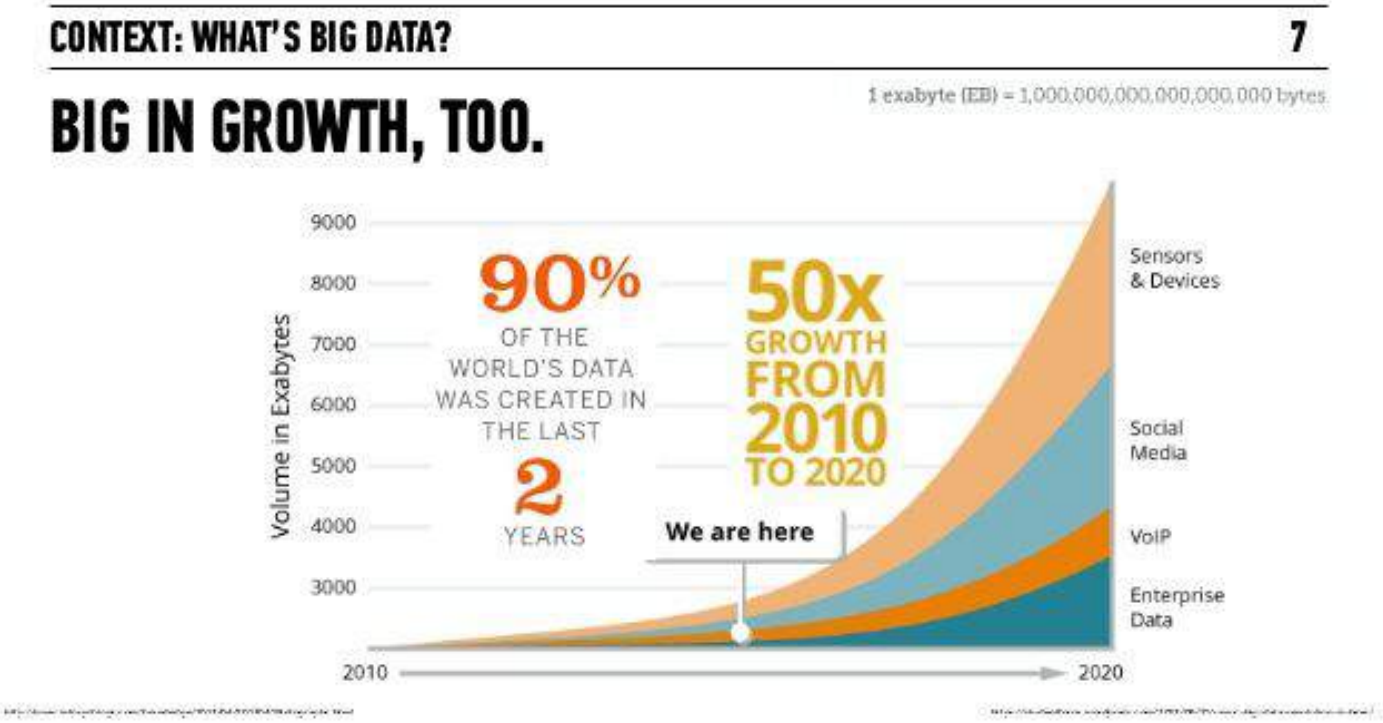
Google, a subsidiary of Alphabet, has a major source of its revenue that comes from advertising. The reason Google is able to deliver so much economic value is the massive amounts of data collected on users and leveraging advanced machine learning algorithms to make relevant and meaningful ad recommendations based on the user's preferences while surfing the internet. Google has fundamentally transformed the advertising industry because all of their metrics can be measured and tracked as opposed to traditional forms of advertising

media such as print, television, and radio which can be measured to a degree, but not to the extent to know if the user acted upon the ad or not.

The Rise of Alternative Data

The natural byproduct of governments, companies, and people going through these various forms of digital transformations is that it creates enormous amounts of data. According to research conducted by SINTEF ICT in 2013 it was estimated that 90% of the world's data has been created in the last two years.

Dr. Anasse Bari, a New York University professor, contends that the big data and deep learning are creating a new data paradigm on Wall Street. Dr. Bari explains that diverse data sets such as satellite images, people-counting sensors, container ships' positions, credit card transactional data, jobs and layoffs reports, cell phones, social media, news articles, tweets, and online search queries can all be used to make predictions about future financial valuations.



Source: https://www.promptcloud.com/blog/want-to-ensure-business-growth-via-big-data-augment-enterprise-data-with-web-data/

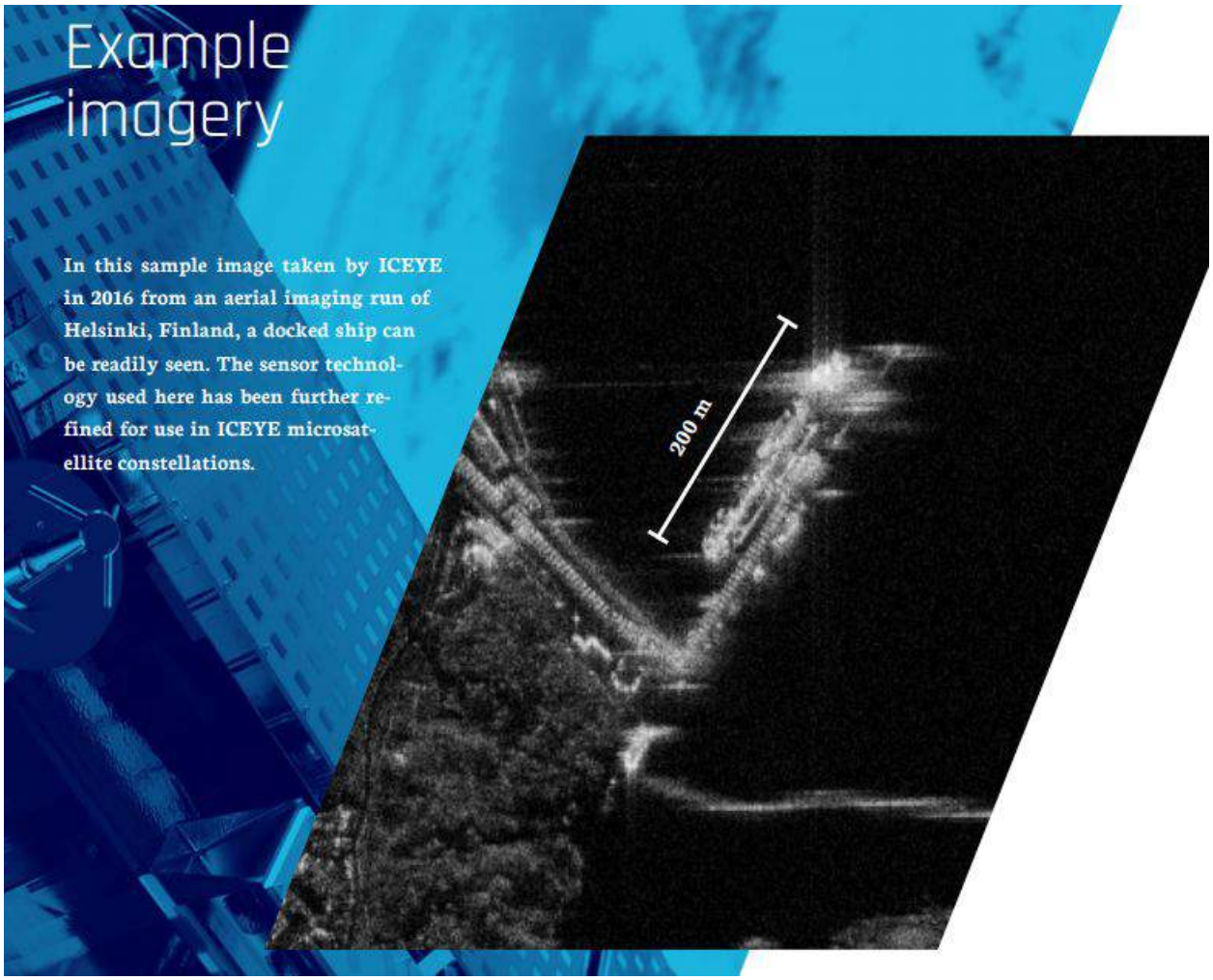
For example, data scientists can mine through satellite images of the parking lots of major retailers over a period of time to predict future sales. Professor Bari was part of a project that analyzed nighttime satellite images of the earth as a way to predict the gross domestic product

(GDP) per square kilometer. The theory was that the greater the amount of light in a given area would infer a higher GDP.

Many institutions have already incorporated social media as an alternative data source for AML and fraud investigations and even for merger and acquisitions (M&A) deals. During the analysis phase of a M&A deal, social media could be one of the data sources to leverage by conducting a sentiment analysis of the target company. Sentiment analysis is type of natural language processing (NLP) algorithm which can determine, among other things, how people feel about the company. Some of the insights that could be derived is that people love their products or have similar complaints of poor customer service which may have an impact on the final valuation.

Sentiment analysis can be a particularly powerful analysis method which was illustrated by an anecdote in James Surowiecki's book, The Wisdom of Crowds. The story was that in 1907 Francis Galton realized that when he averaged of all the guesses for people participating in the weight of an ox competition at a local fair, it was more accurate than individual guesses and even supposed cattle experts. The method was not without its flaws though, because if people were able to influence each other's responses then it could skew the accuracy of the results. However, it does point to the powerful insights that could be extracted from social media platforms which have large crowds.

Another potential area for alternative data in the financial services sector is a network of nano satellites that leverage synthetic-aperture radar technology that, among other things, track ships on Earth. ICEYE is a startup that has raised funding to launch a constellation of synthetic-aperture radar enabled satellites which can observe the Earth through clouds and darkness that traditional image satellites can't do.

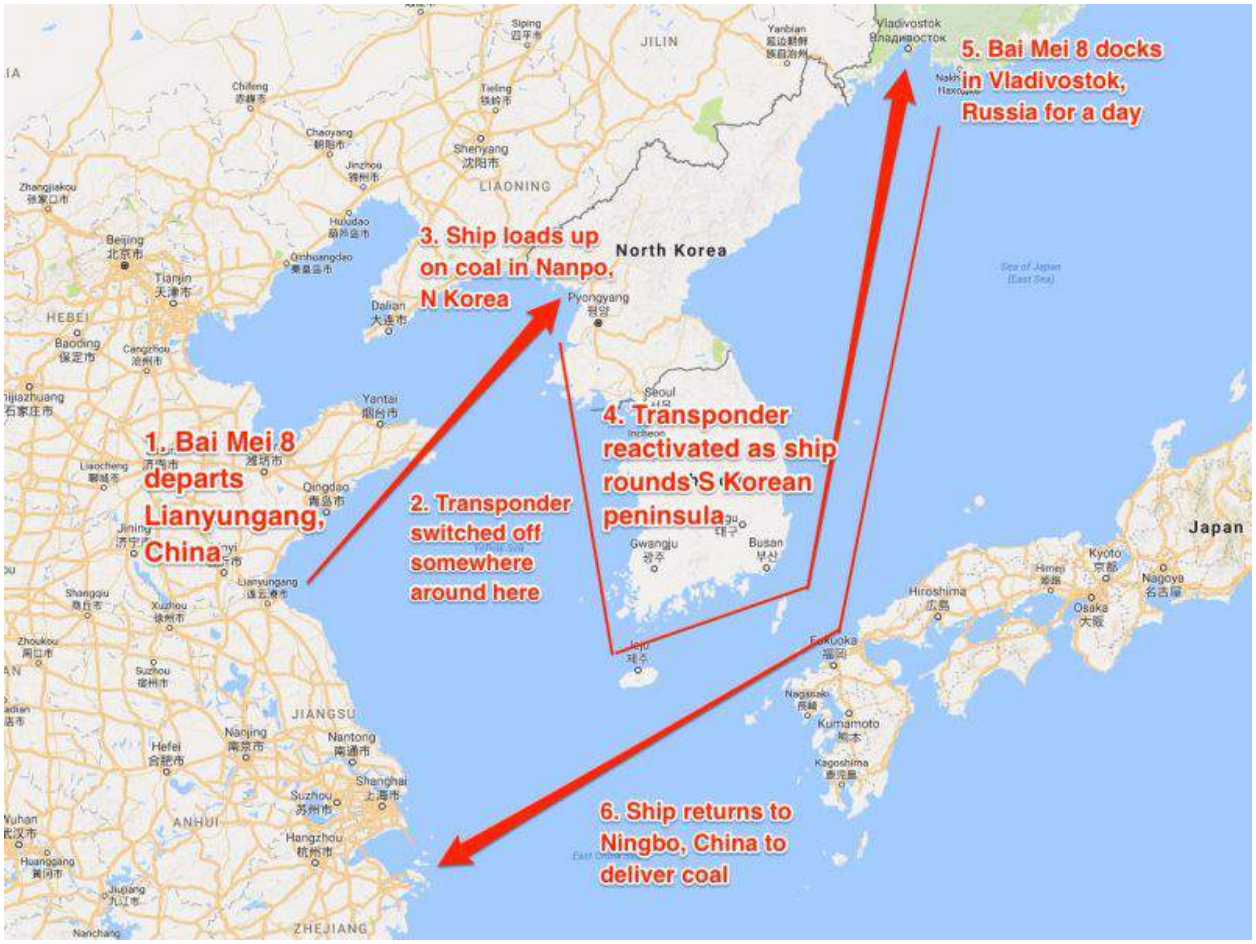


Source: ICEYE - Problem Solving in the Maritime Industry

Trade finance is one of the key components which facilitates international trade supported by financial institutions. One component of trade finance is that many goods travel from one country to another on vessels. North Korea's aggressive missile tests and nuclear ambitions are creating a volatile political environment and increasing the focus and exposure of sanctions risk. Financial institution don't want to be linked to vessels dealing with North Korea, but it can be hard to know, in some circumstances, for sure by limiting the due diligence process to traditional data sources.

Marshall Billingslea, the US Treasury Department's assistant secretary for terrorist financing, explained to the US House of Representatives Foreign Affairs Committee that ships turn off their transponders when approaching North Korea, stock up on commodities such as coal, then turn them back on as they sail around the Korean peninsula. The ships would then stop at a

Russian port to make it appear that the ships contents came from Russia, and then sail back to China. The other challenge is that North Korea doesn't have radar stations that feed into the international tracking systems. This type of satellite technology could be used by multiple stakeholders to help identify what vessels behave suspiciously near North Korea and could, to a certain extent, make sanctions more effective by applying pressure on noncompliant vessels.



Source: https://www.businessinsider.nl/north-korea-why-un-sanctions-not-working-2017-9/

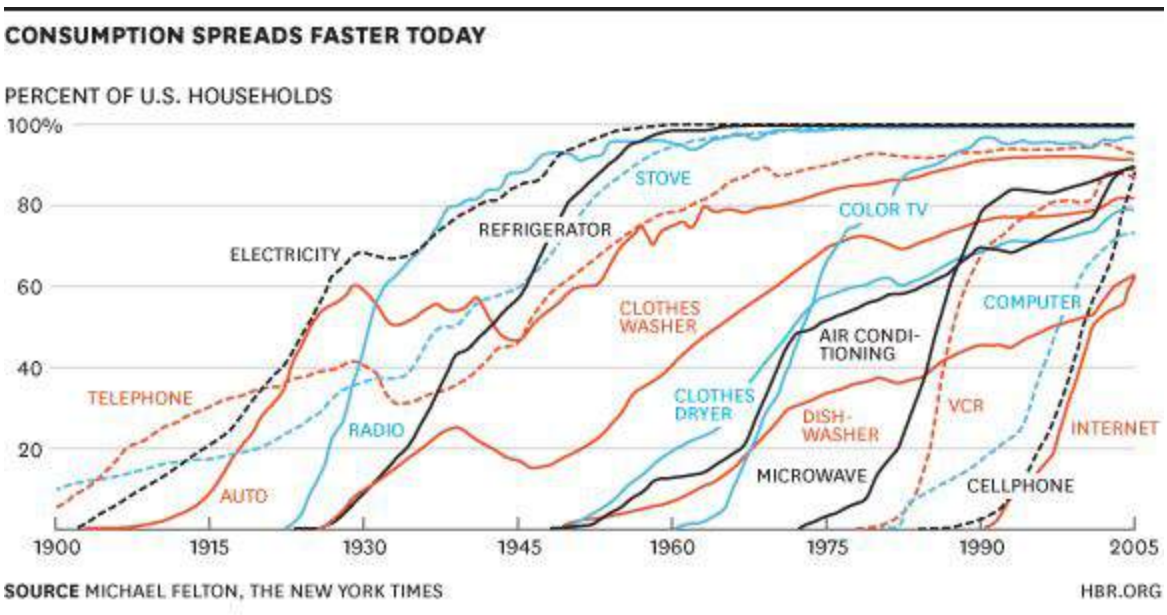
A recent report by the US research group C4ADS highlights another tactic that North Korea uses to evade sanctions, which is to create new webs of shell and front companies to continue operations. This sentiment is echoed in an October 13, 2017 report by Daniel Bethencourt of Association of Certified Anti-Money Laundering Specialists (ACAMS) MoneyLaundering.com North Korean front companies "use a series of perpetually evolving sanctions-evasion schemes" to continue its proliferation of a the nuclear weapons program.

Changing Consumer Expectations

The new paradigm for the customer experience is Disney World. For anyone who has travelled to Disney World recently, the MagicBand sets the bar for our expectations as consumers. The MagicBand is based on radio-frequency identification (RFID) technology and is shipped to your home for your upcoming trip and can be personalized with names, colors, and other designs for everyone in your party.

The MagicBand can be used to buy food and merchandise, enter your hotel room, lookup photos taken by Disney staff, and even enter your preselected rides. There are water rides at Disney so last thing you want is going on one of those and having your belongings get soaked. But the idea is to make the experience personalized, frictionless, and pleasurable. Since, companies are merely a group of individuals then as our individual expectations change so will our organizational ones, even if it happens, in some firms, at a slower pace.

The speed at which consumers are adopting new technologies has advanced rapidly when examining the historical penetration of other technologies such as the electricity, and the refrigerator. The adoption rate of the cell phone and internet exhibits a steeper incline in a shorter timeframe than earlier technologies as seen in the image below.



Source: https://hbr.org/2013/11/the-pace-of-technology-adoption-is-speeding-up

Bank in a Phone

While banks have had various levels of success with digital transformation, there is one that stands out from the rest of the pack. DBS bank launched Digibank in India in April 2016 and in Indonesia in August 2017 which is basically a bank in your phone. As a testament of the bank's success in August 2016, at a Talent Unleashed competition, DBS' chief innovation officer, Neal Cross, received the most disruptive Chief Innovation Officer (CIO)/ Chief Technology Officer (CTO) globally. Mr. Cross was judged by prominent figures business such as including Apple co-Founder Steve Wozniak and Virgin Group Founder, Sir Richard Branson.

Source: https://www.dbs.com/newsroom/DBS_Neal_Cross_recognised_as_the_most_disruptive_Chief_Innovation_Officer_globally

DBS' strategy with Digibank is succinctly summarized by its chief executive executive, Piyush Gupta, in the below quote:

"With digibank, we've built a bank that pulls together the power of biometrics, natural language, artificial intelligence and in-built security in one offering. We believe this mobile-led offering represents the future of banking."

While Digibank is targeted at the retail banking in emerging markets, it sets a clear precedent of what's to come in the future, even for institutional banking in the developed economies. For example, as the customer service chatbots functionality advances then they will begin to be deployed by banks as an option to serve large banking customers. While some customers will prefer to speak to an actual person, the fact that these chatbots are serving those same people in other sectors and businesses will drive the adoption for financial institutions because of changing customer behavior.

This has also has had profound effects on the financial services industry which, in some sense, is struggling to keep up with the fervent pace of the digitalisation across various aspects of its operations.

Self Service in Spades

Self-service machines are not something new as we have been interacting with automatic teller machines (ATM) for years. The first ATM appeared in Enfield, a suburb of London, on June 27, 1967 at a branch of Barclay's bank. An engineer, John Shepherd-Barron, at a printing company is believed to have come up with the cash vending machine idea and approached Barclay's about it.

The first ATMs were not very reliable and many people didn't like them, but banks continued to install them despite the lack of customer satisfaction. In the United Kingdom in the 1960s and 70s, there was growing pressure from the trade unions for banks to close on Saturdays. Hence, the executive leadership of banks seemed to think that ATMs were a good idea to appease the unions and customers and to reduce labor costs. This is another historical example of how different agents of a CAS act, react, and learn from each other and how automation was seen as a remedy for all those involved.

This brings up a number of points of about the transformative effect of new technology. First, ATMs are densely present in most major cities today and their transformative effect on us has become almost invisible. Second, it seems that most bank employees were not concerned about getting replaced by an ATM. How could they? It performed so poorly and couldn't do the same type of quality job as a human bank teller, at least at that time.

After society accepted ATMs as a part of banking, did we even notice as they got better?

Some pharmacies, in low traffic areas, today will only have one employee working in the front of the store acting like an air traffic controller, directing customers to self-service checkout systems. The self-service systems in most pharmacies today is similar to ATMs in the sense that they have predefined responses and can't learn or are not embedded with *intelligence*.

These self-service systems can only give feedback based on the user's physical interaction with the system usually via a touch screen as opposed to a customer's voice. Occasionally, the employee will intervene if the customer attempts to buy an age-restricted item, but many times it's possible to complete a transaction with no human interaction at all.

A similar transformation will continue to evolve in the entity due diligence space where the consumer, or the account opener, is directed to a system and guided through the onboarding process by a series of prompts. The self-service onboarding systems are already beginning to emerge by prompting customers to update their information based on policy timeframes, refreshing expired documents or reverifying information required for the bank to conduct its periodic review, if applicable. While this trend appears to be strongest in the retail banking market right now, it will certainly become the standard for commercial and wholesale banking in the future, it has to.

The Rise of Non-documentary Evidence

As discussed in previous sections consumer expectations are changing and the new customer experience model is Disney's MagicBand. Additionally, financial institutions can develop platforms to initiate their customer base to get more engaged in the due diligence process by refreshing their own documentation collected for regulatory purposes. However, as highlighted earlier regulatory expectations are likely to increase over time which means that offloading all of the heavy lifting to the client is not the best long-term strategy.

Hence, other activities need to be planned to reduce the amount of work the customer has to do on their own and continue to evolve the due diligence process so it becomes as seamless as possible. There are other factors at play as well such as the risk of losing customers to other more mature digital banks with better onboarding processes or even losing business to fintechs. Again, fintechs are taking advantage of the current regulatory environment which puts enormous regulatory pressure on depository institutions that creates an opportunity for them to offer snap-on financial products linked to a customer's bank account.

Another strategy that can be developed, in the US and other countries, for the due diligence process is to leverage non documentary methods of identification as described in the Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual.

The determination of what data could satisfy non documentary needs and when to require a potential client to supply the actual document could follow the risk-based approach. For example, if during onboarding the customer triggers the EDD process based on the institution's risk rating methodology then the physical documents could be requested. On the other hand, if

a potential customer is onboarded and is determined to be low-risk then this could allow for more flexibility when satisfying the policy requirements, including using non-documentary evidence..

As will be discussed later in this document there will be opportunities to leverage the advances in robotic process automation (RPA) and AI to further streamline the due diligence process by automating specific portions of it.

Emerging Risks

There are many emerging risks for financial institutions as the transformative effects of the digital age continue to shape and reshape the world, business, consumer expectations, risk management, etc. In the OCC's Semiannual Risk Perspective for Spring 2017 report, four key risk areas were highlighted including strategic, loosening credit underwriting standards, operational (cyber), and compliance.

The theme underlying all of these key areas was the influence of digitalisation which amplified the complex, evolving, and non-linear nature of risk. For example, while strategic risk and loosening credit underwriting standards were listed separately, one leads to the other. In other words, strategic risk was created by nonfinancial firms, including fintech firms, offering financial services to customers which forced banks to respond and adjust credit underwriting standards in an attempt to retain market share.

Cyber risk wasn't a result of the interactions between competitors, but something that arose out of the increased digitalisation of the modern world, including business processes. However, cyberattacks are successful because of the immense amount of human and financial capital invested into it by foreign governments and large networks of bad actors to ensure its continued success.

Financial Technology (Fintech)

Financial technology or fintech is not something new because innovation has always been a part of finance, but the what's emerging is that an increasing number of firms are offering services based on a fintech innovation directly to customers and are threatening the traditional financial institutions market share.

The modern day multi-purpose credit card has its roots in a 1949 dinner in New York City, when the businessman, Frank McNamara, forget his wallet so his wife had to pay the bill. In 1950, Mr. McNamara and his partner returned to the Major's Cabin Grill restaurant and paid the bill with a small cardboard card, now known as the Diner's Club Card. During the card's first year of

business, the membership grew to 10,000 cardholders and 28 participating restaurants and 2 hotels.

On February 8, 1971, the National Association of Securities Dealers (NASDAQ) began as the world's first electronic stock market, trading over 2,500 securities. In 1973, 239 banks from 15 countries formed the cooperative, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), to standardize the communication about cross-border payments. There were other companies which built risk management infrastructure or data services to serve the financial services sector such as Bloomberg and Mysis.

The difference between the major changes of the past and today, was that in the past innovation came from within, and if it did come from an external company it was designed to support the financial services sector as opposed to threaten its market dominance. Today, some fintechs are looking to make the financial services sector more efficient with better software, but other firms are looking to take market share by offering complementary financial service products directly to consumers.

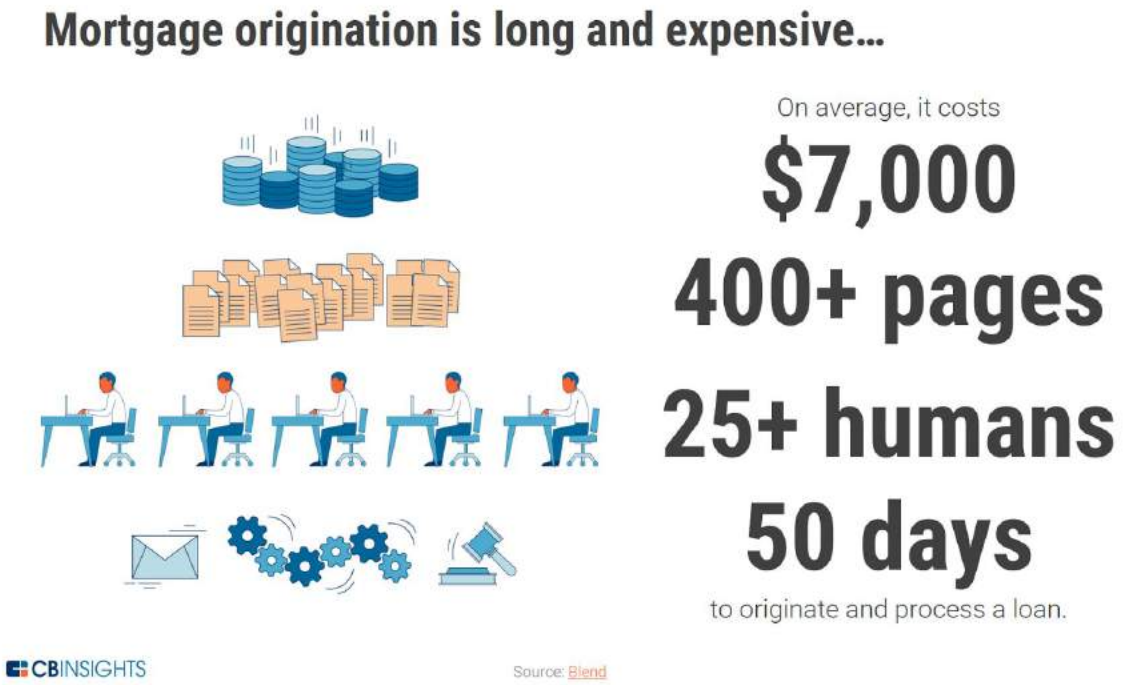
Arguably, the first signs that fintech could be in direct competition with the financial services sector was the emergence of Confinity, now PayPal, in 1998. Confinity was originally designed as a mobile payment platform for people using Palm Pilots and PDAs. The company was acquired by Ebay in 2002 to transform the business of payments. PayPal disrupted the sector by building a payments ecosystem to allow electronic funds transfer typically faster and cheaper than traditional paper checks and money orders.

The global financial crisis of 2008 was pivotal point in the history of fintech which laid the foundation for more challenger firms to begin entering the financial services space. The collapse of some major financial institutions such as Lehman Brothers, and the acquisition process to consolidate other major financial institutions in the US and Europe created negative public sentiment towards the industry and regulators demanded sweeping changes to ensure that type of crisis wouldn't happen again.

Given the sheer magnitude of the 2008 financial crisis, many institutions were so focused on remediation efforts and meeting new regulatory demands and innovation was not a top priority. However, at the same time there were significant technological advances in smartphones, big data, and machine learning which allowed for fintechs to disrupt the sector - as it laid stagnant for a few years - with consumers more open to digital alternatives.

One financial service that is ripe for disruption is the mortgage loan process which is extremely laborious and, according to CB Insights, costs an average of $7,000, contains more than 400 pages of documents, requires more than 25 workers, and takes roughly 50 days to complete.

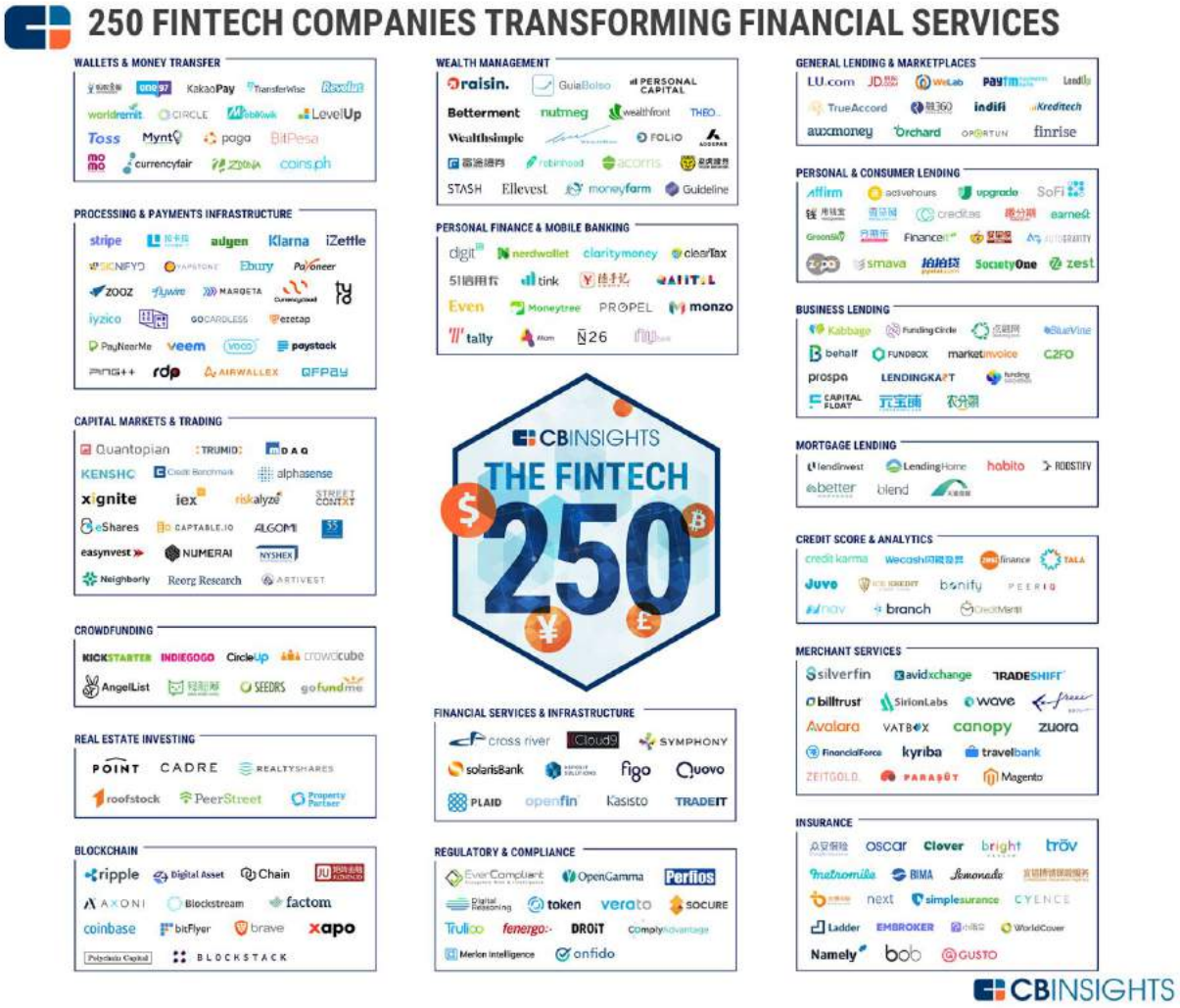
Clearly, this is a concern and consumers may opt for nontraditional online lenders to avoid the painful experience in traditional banking.



Source: https://www.cbinsights.com/research/mortgage-fintech-industry-primer/

According to a report by PricewaterhouseCoopers (PWC), large financial institutions across the world could lose 24 percent of their revenues to fintech firms over the next three to five years. Today, fintechs are focusing on a wide array of applications that can be categorised as consumer facing or institutional and includes services such as business and personal online lending, payment applications, mobile wallets, and robo advisors .

Some fintechs are marketing directly to consumers and taking advantage of the power of digital platforms and the current regulatory environment which puts enormous pressure on depository institutions. As discussed in the digital transformation section this creates an opportunity for fintechs to offer snap-on financial products linked to customer's bank account without the regulatory burden of being a bank. CB Insights created the graphic below to highlight 250 fintech startups transforming financial services.



Source: https://www.cbinsights.com/research/fintech-250-startups-most-promising/

Financial institutions are not only in competition with fintechs for market share because they are also in a fight for talent with technology companies more generally, given the impacts of the digital era. The CEO of Goldman Sachs hosted an event in September 2017 for 250 students at a New York public college which traditionally wouldn't have been on the prestigious firm's recruiting radar. However, Mr. Blankfein stated the following about Goldman's current outlook and modified talent sourcing strategy:

"It wasn't an act of kindness on my part, or generosity, or trying to create diversity; it was as pure selfish, naked self-interest, we wanted to really extend our net further because everybody's involved pretty much in a war for talent. And we compete against obviously all the other financial services firms, but we compete against all the technology firms."

Some financial institutions are taking an alternative approach, rather than competing directly or doing nothing, by either investing in or partnering with fintech companies, and fewer have acquired fintechs directly. According to data compiled by CB Insights, since 2012 Citi has invested in 25 fintechs and Goldman Sachs in 22, while fintech acquisitions have been less frequent. However, in October 2017 JP Morgan Chase agreed to acquire the fintech company, Wepay, for $220 million.

Model Risk

The OCC's paper, Supervisory Guidance on Model Risk Management, outlines an effective framework to manage model risk. The basic components for managing model risk can be broken into three parts which are:

- Model development, implementation, and use
- Model validation
- Governance, policies, and control

As the digital era changes the way financial products and services are offered, it also changes the way risk is evaluated and managed. Again, while these robust frameworks have historically applied to market, credit, and operational risk. However, there is clearly a place for due diligence in both third party risk management and AML programs.

The irony about model risk here is that while new technologies will help automate repetitive tasks and advanced algorithms will assess various risks more accurately, it will greatly increase the complexity of the governance and validation processes. To calculate risk more effectively more external data sources will be interrogated by more complex algorithms. This will increase the risk management surface area, and determining where potential issues occur could become more cumbersome to identify and remediate.

Another emerging technology trend is regulatory technology or regtech. Regtech's goal is to enable institutions to make better and more informed decisions about risk management and given them the capability to comply with regulations more efficiently and cost effectively. However, as discussed previously the threat posed by fintechs are putting pressure on financial institutions to loosen their credit underwriting procedures to avoid losing more market share. This trend will continue to drive the incorporation of more external data sources and more complex algorithms to arrive at more accurate assessments of risk, faster.

Financial institutions also have to deal with legacy IT systems which require data to flow through many toll gates before getting to the risk management systems. It's akin to trying to fit 'a square peg in a round hole' which can result in various data quality issues. While adopting new

technology can increase the overall complexity of the model risk management process, it could, at the same time, increase the framework's overall effectiveness, when implemented properly.

Cyber Risk

Cyberattacks have been called one of the greatest threats to the United States, even beyond the risks that a nuclear North Korea may pose. 2017 has been a blockbuster year for data breaches and no organization seems to be immune from the threat.

Some high profile data breaches in 2017 include, but are not limited to entities such as: IRS, Equifax, Gmail, Blue Cross Blue Shield / Anthem, U.S. Securities and Exchange Commission (SEC), Dun & Bradstreet, Yahoo, Uber, and Deloitte.

While the extent of the data breach varied for each organization, it's abundantly clear that cyberattacks are affecting a wide range of institutions in the public and private sector at an alarming rate.

The foreword to Daniel Wagner's book, "Virtual Terror: 21st Century Cyber Warfare," was written by Tom Ridge, the former Governor of Pennsylvania and First Secretary of the US Department of Homeland Security described the threat as follows:

"The Internet is an open system based on anonymity - it was not designed to be a secure communication platform. The ubiquity of the Internet is its strength, and its weakness. The Internet's malicious actors are known to all of us via disruption, sabotage, theft, and espionage. These digital trespassers are motivated, resourceful, focused, and often well financed. They eschew traditional battlefield strategy and tactics. They camouflage their identity and activity in the vast, open, and often undefended spaces of the Internet. Their reconnaissance capabilities are both varied and effective. They constantly probe for weaknesses, an authorized point of entry, and a crack in the defenses. They often use low-tech weapons to inflict damage, yet they are able to design and build high-tech weapons to overcome specific defenses and hit specific targets."

As institutions move more towards a complete end-to-end digital experience it will require them to monitor the digital footprint of their customers, counterparties, and service providers to ensure nothing has been compromised. Today, some internet marketplace companies maintain a list of internet protocol (IP) addresses, either on their own or with the help of a vendor, known to be compromised or associated with cyber crime groups to avoid fraudulent charges, account takeovers, and other forms of cyber attacks.

For example, if a credit card was issued by a bank in the US, but the IP address associated with the online transaction was coming from another country overseas it could increase the risk of fraud, assuming the individual was not travelling.

There have been cases of fraudsters impersonating an executive of an existing customer by calling up the wire room of a financial institution and requesting a high priority wire to be sent overseas. This is a low-tech form of fraud because the fraudster used social engineering to convince the bank's employee that they were a legitimate representative from the company. The fact that the fraudster had some much information regarding the bank's operations, customer's account, and the customer's organizational structure which made the scheme that much more believable.

This is another serious risk for business-to-business (B2B) commerce because with all of the data breaches happening, its relatively straightforward to gather or purchase the confidential information needed to conduct an effective B2B fraud.

Cybersecurity has become a core part of third party risk management as an potential business partner's cyber resiliency could impact the decision making process. The 2013 data breach of Target's systems which compromised 40 million credit and debit card numbers highlight the fact that in terms of entity due diligence, cyberattacks are a serious risk to third party risk management. Target's systems were reportedly compromised by first stealing the credentials of a Heating and Ventilation company (HVAC) in Pittsburgh. Target used computerized heating and ventilation systems and it was apparently more cost effective to allow remote access to its systems to a third party rather than hire a full time employee on-site.

The risks posed by cyberattacks are forcing organizations to rethink how they engage with customers and other businesses in their supply chain. The future of a robust entity due diligence process will have to include an assessment of cyber resiliency which could include cybersecurity insurance policies, but this industry is still in its infancy due to a lack of comprehensive standards when assessing cyber risk exposure. This is beginning to change in the US based on the NYDFS cybersecurity part 500 rule will require covered entities to submit a certification attesting to their compliance with the regulation beginning on February 15, 2018.

Technology and Innovation

The story of human history could be traced back to technological innovations that allowed for early humans to exert greater control over the environment to meet their needs or desires. The most basic technological innovation was the discovery and control of fire which allowed for warmth, protection, cooking, and led to many other innovations. Scientists found evidence at a

site in South Africa that Homo erectus was the first hominin to control fire around 1 million years ago.

If, we consider ideas as an invention or innovation then the next big shift in human history was the concept of agriculture and the domestication of animals which laid the foundation for civilization to flourish. Mesopotamia was the cradle of civilisation as no known evidence for an earlier civilization exists. Mesopotamia was a collection of cultures situated between the Tigris and Euphrates rivers, corresponding mostly to today's Iraq, to support irrigation and existed between 3300 BC – 750 BC. One theory also credits Mesopotamia with another revolutionary innovation, the wheel, based on the archaeologist, Sir Leonard Woolley, discovery of remains of two wheeled wagons at the site of the ancient city of Ur.

There is a difference between groundbreaking innovations and incremental improvements to existing products or processes. Historically, there has arguably been less innovation, in terms of volume, when comparing ancient civilizations to the modern societies of the 20th and 21st centuries. However, the discovery of fire, the invention of the wheel, paper, compass, and printing press had an extraordinary impact on social structures, evolution of culture, and value systems. For example, the wheel was a groundbreaking innovation because it rearranged social structures by revolutionizing travel, trade, agriculture, war, among other things.

One of the most groundbreaking innovations of the modern world was electricity because many other revolutionary technologies such as the radio, television, computer, and internet wouldn't be possible unless there was a way to power those devices. When analyzing the impact of technology on the future, it's worth imagining if the technology is a groundbreaking advancement of an incremental improvement.

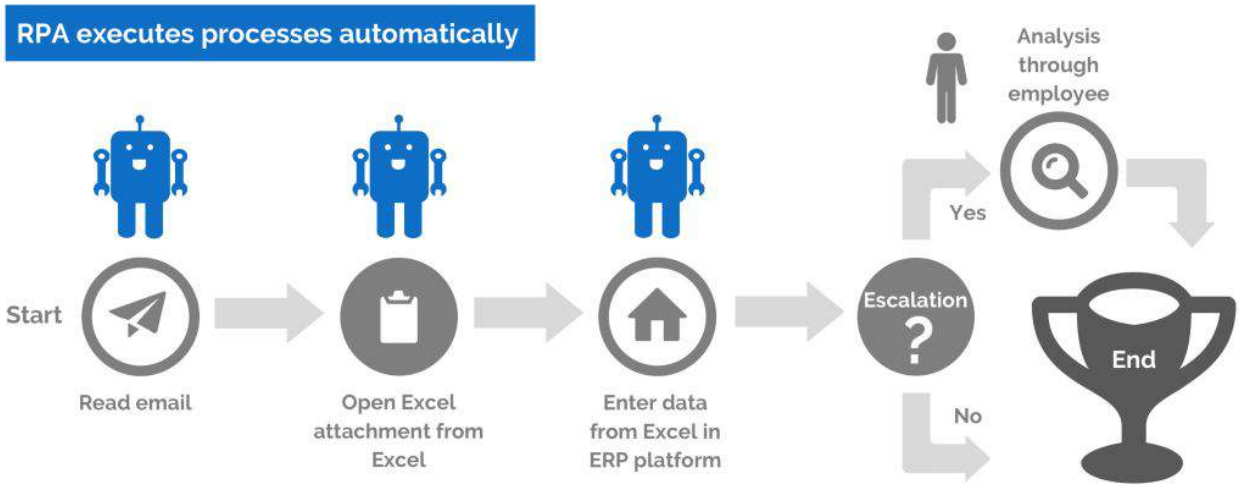
There are four key technology areas which will have a transformation effect, on different time horizons, on the future of entity due diligence which are robotic process automation (RPA), big data platforms, AI, and blockchain. The general trend of digitalisation will de-emphasise the need for specific aspects of the due diligence process such as collecting and processing data and customer interaction. Other new technologies such as blockchain will introduce the concept of shared work and consensys which will rearrange how transactions are conducted. This general trend will be amplified by other adoptions such as the integration of more alternative data sources, self-service systems, acceptance of non-documentary evidence, and more complex algorithms to reduce false positive alerts and the re-prioritisation of risk management queues.

Robotic Process Automation (RPA)

RPA is an important stepping stone in the evolution of the due diligence process, but it's more of an incremental improvement rather than a groundbreaking innovation. RPA is the application of technology that allows employees of an organization to program a 'robot' to complete repetitive and mundane tasks such as processing a transaction, transferring data from one application to another, transforming data, and triggering automated responses.

The entity due diligence process can be extremely cumbersome, especially the KYC process, because the workflow can include hundreds of keystrokes and mouse clicks. For example, the CIP and CDD components of the KYC process can include over 100 data points to complete for a legal entity. If, the entity is determined to be high-risk based on their business or product types products being used then the EDD process can include hundreds of data points. Depending on the policy of the institution, higher-risk customers will have to be reviewed periodically.

There are many aspects of the KYC workflow that are repetitive where RPA solutions can be designed to complete specific tasks in a queue. The below graphic shows a potential use case for RPA where the robot can complete different several tasks and transfer data between siloed applications. In this example, there is the potential for no human interaction, if an escalation to an employee is not needed.



Source: https://www.roboyo.de/en/robotic-process-automation/

The rising regulatory expectations and increased competition from fintechs are forcing financial institutions to explore different possibilities to increase efficiency, speed, and reduce costs. The types of RPA being implemented today are mainly rule based, meaning the process being automated is stable, predictable, and repeatable.

Big Data

One of the popular historical definitions of big data has been described in a META group report as data which exhibits the three 'V's - a large volume, of a wide variety, and can come into an organization at a velocity of high speeds or real time. The definition of big of data like many emerging technology trends is a moving target and there have been two other V's added to the historical definition. The fourth V is veracity, a byproduct of another V - variety, which refers to the trustworthiness or integrity of the data. The last V is value, which is simply the ability to turn data into value and actionable intelligence.

The last two V's of veracity and value most likely arose out of the need to address the real world challenges of implementing big data platforms and deriving real value from it. Data integrity is highlighted as a key component to ensure the success of big data initiatives. This also implies that simply storing massive amounts of varied information doesn't mean the organization is engaged in big data initiatives. The key to big data is the last V, value, because storing a lot of information has no intrinsic value unless insights can be extracted and acted upon quickly.

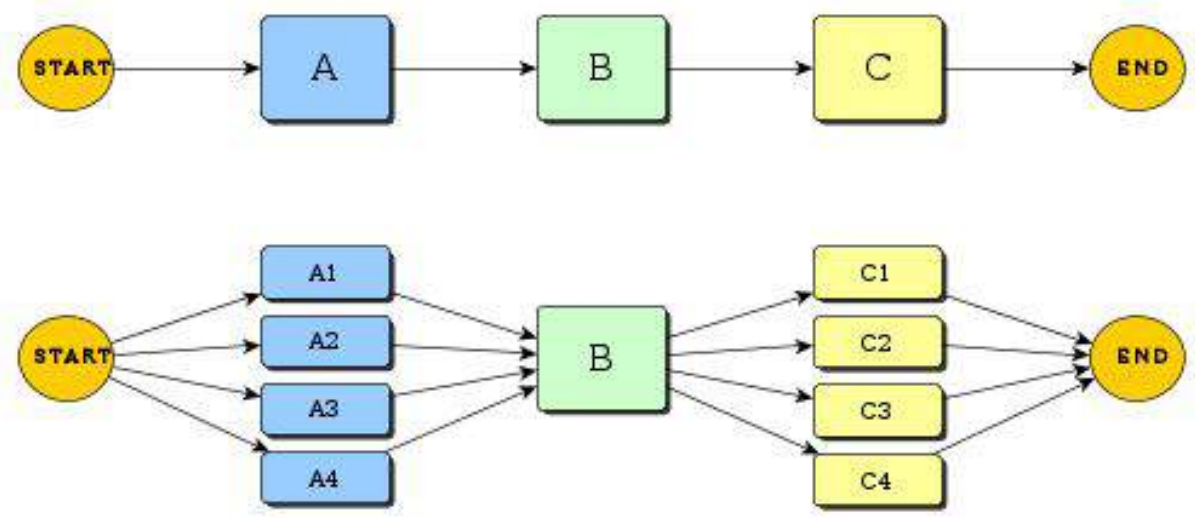
The concept of processing large amounts of data has a longer history, but the practical application of dealing with large semi-structured data sets emerged out of the internet search companies need to create an elegant solution of ranking millions of web pages efficiently. In 2004, when the internet included roughly 51 million websites, Google published a research paper about how they used a MapReduce modeling program to optimize the complex problem of parallelizing a computation across a networks of computers. Google's paper prompted Doug Cutting and Mike Cafarella to create Apache Hadoop in 2005 which is used as a big data platform by many organizations today.

The fundamental issue is that for big data problems, there is more data to process than what can be done on a single computer. Hence, the explosion of the internet created a need to optimize parallel processing to address the bottleneck issue encountered in the physical hardware limitations of using a single computer to process massive amounts of data.

Traditional computer programs have followed a serial computation workflow where an algorithm would be executed in steps - and after the completion of each step - it would proceed to the next step on a single computer. The explosion of the internet and the continued rise of alternative data has created the need to store, process, transfer, and analyze massive amounts of data or

what has been called ‘big data.’ Again, to put the growth of data in context, research conducted by SINTEF ICT in 2013 estimated that 90% of the world’s data has been created in the last two years.

The top graphic in the image below shows the traditional programming paradigm where algorithms follow a serial method of processing instructions one-by-one in a queue. The bottom graphic in the image below shows the enhanced programming paradigm which follows a parallel processing method where data (or the problem) is broken into discrete parts that can be processed concurrently on different machines, and the parts are recombined later in the process to arrive at the final result.



Source: http://xmipp.cnb.csic.es/twiki/bin/view/Xmipp/ParallelProgramming

While this is a fairly technical concept, it’s essential for everyone to understand especially for users of systems that support various business functions. For example, senior management of the compliance department in financial institutions are the users of various systems such as CDD, transaction monitoring, and sanctions screening to meet regulatory requirements.

The general trend is that big data and AI will transform all sectors and industries, but it's important to note that, parallel processing implies cloud computing. This essentially means that to process large amounts of data very fast, the algorithms must split the tasks over a network of computers which doesn’t necessarily mean the network of computers resides within the institution’s firewall.

Hence, institutions may need to send some of their data outside of their network to harness the power of big data through parallel computing. However, there is the possibility that institutions

will opt to implement advanced software within their own data centers and manage the parallel computing process themselves. However, others may opt to leverage cloud providers to scale up their computing capacity, but this raises questions such as, what data can be sent outside of the institution and what data can't? Also, does it need to be anonymised first?
The term big data is a bit of a misnomer because it's not all about the data at all. Big data is really about the ability to extract value for decision making, and one of the most effective ways to do this today is by leveraging the power of parallel processing.

The massive amounts of data generated by the digital revolution and the advances in parallel computing laid the framework for major successes in AI, which will be explored in the next section.

Artificial Intelligence (AI)

AI is one of the most exciting technological trends of our time where machines have 'learned' to recognize faces, classify objects in images, recommend advertisements that align with our preferences, understand and act on voice commands, drive cars autonomously, beat humans in chess back in 1997, and the notoriously complex game of go in 2017.

With all of these impressive feats, what exactly is AI? This is actually a complicated question, but one of the simplest definitions is that AI is the study of making computers great at tasks associated with human intelligence.

The term "artificial intelligence" was coined in a 1956 academic proposal for a 2 month study of how machines can simulate learning and intelligence which was submitted by John McCarthy (Dartmouth College), Marvin Minsky (Harvard University), Nathaniel Rochester (IBM), and Claude Shannon (Bell Telephone Laboratories). According to the proposal the goal of the workshop was, "An attempt will be made to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves."

While the term of AI first appeared in 1956, the interest in objects exhibiting intelligence has appeared throughout antiquity such as in the civilizations of ancient Egypt and Greece. In the Greek myths, Daedalus used quicksilver to put a voice in his statues, Hephaestus created automata for his workshop, and Talos was an artificial man of bronze.

The independent invention of calculus by Isaac Newton and Gottfried Leibniz was another precursor to AI because created the foundation for the idea that rational thought could be systemised or mechanised.

There were other precursors to AI such as research by the British physician, Richard Caton, who discovered the electrical nature of animal brains by recording impulses. Caton's work led to the research of physician, Hans Berger, who was the first to record human electroencephalograms (EEGs) in 1924. The discovery of the electrical nature of the brain inspired early work in the field of neural networks and cybernetics. The idea was that, if a brain was an electrical system, then a machine could be built to replicate it. To this end, the development of AI has been about, at its core, replicating human intelligence or biomimicry, but our definition of intelligence may need to be modified in the context of AI to avoid anthropomorphising it, and distorting its current capabilities and limitations.

Intelligence and Thinking

There seems to be some confusion around what AI can and can't do today, and this could partially stem from the use of the word intelligence. Intelligence is a nebulous concept because we could think of intelligence, in a narrow human sense, in terms of an intelligence quotient (IQ), as the ability to break down and solve complex problems quickly. Other interpretations of human intelligence think of it more broadly as a multitude of abilities, beyond book smarts, such as the ability to 'read people' or a type of emotional intelligence.

But intelligence is not limited to humans, even though humans clearly exhibit a special form of intelligence, as animals can communicate with one another, coordinate attacks on a prey, and save food for the future. It could even be argued that plants exhibit a form of intelligence, as its branches tend to grow away from darkness towards sunlight. The Sante Fe Institute President, David Krakauer, offered another definition of intelligence stating that, "is making hard problems easy."

In 1950 Alan Turing, one of the pioneers of computer science, proposed the idea of the imitation game to address the question of whether machines could think. The game, commonly referred to as the Turing test, was to have an evaluator review the written conversation between player A and B, and determine which player was human and computer. If, the computer was mistakenly taken for a human 30% or more of the time then the test was passed. In 2017, at an event hosted by the University of Reading, it was reported that a computer program, Eugene Goostman which simulates a 13-year-old Ukrainian boy, passed the Turing test.

While the Turing test is an important milestone to gauge the development and capabilities of AI, it doesn't actually show that machines think. This was even stated by Alan Turing himself, in the same paper that proposed the game, when he wrote:

"The original question, "Can machines think?" I believe to be too meaningless to deserve discussion."

In a discussion about thought, Noam Chomsky highlighted this sentence that Turing wrote in his paper to show that Turing was well aware of the limits of human language and the ridiculousness of the question itself. The phenomenon of thought is not well understood today, so for some to claim that passing the Turing test shows machines can think, presupposes we know what thought is, but we really don't understand it that well. Or as Noam Chomsky explained, saying machines can think is sort of like saying submarines can swim - you can say it - but it really doesn't make sense. However, this doesn't mean that computers don't exhibit forms of intelligence because clearly they do, but it does show the pitfalls of language and the need to carefully choose the words we use and in what context to achieve the highest level of understanding.

Limits of AI Today and Policies to Protect the Future

It's important to note that AI is highly domain specific today. For example, an AI can process human voice commands, but the same AI program wouldn't be able to drive a car autonomously or determine if an image had a cat in it. The only potential exception to this was demonstrated by AlphaGo created by Google's Deep Mind which beat a world champion at the ancient chinese, and notoriously complex, game go.

Despite the game's simple rules there are 10 to the power of 170 possible board configurations - making go a googol (10 to the power of 100) more complex than chess. Traditional approaches to have AI programs learn complex games have been to construct a search tree over all possible positions, but the sheer number of configurations make this method impossible. This is why the creators of AlphaGo used a search tree with deep neural networks with millions of neural-like connections mimicking the human brain.

In 1997, when IBM's Deep Blue beat a world champion at Chess there was a brute force mechanism to it, in terms of processing all of the potential scenarios and arriving at the optimal solution. Also, some of the highest economic value created by AI systems today such as targeted digital advertising required immense amounts of data beyond human cognition. So, in this sense, there are cases where AI exhibits greater intelligence than humans today in a very specific domain problem, but its the multitude of intellectual abilities, emotions, and the experience of the physical world that makes us human.

The media exacerbates fears that AI is positioned to take over the world, in some type of Terminator Skynet scenario, in the not too distant future. While there are serious serious social and economic implications to consider with the continued advancement of AI capabilities and applications, most leading academic experts agree that machines becoming sentient is not something that is likely in the near future. However, there have been leading figures in the technology world such as Elon Musk who have warned about the dangers of AI. Other leading

tech tycoons and intellectual figures such as Bill Gates and Stephen Hawking have expressed similar concerns.

There comments do point to the need for the regulation of AI to ensure power is not concentrated among a few companies and that policies are in place to address when people's jobs are displaced. A December 2017 report by the McKinsey Global Institute estimated that as many as 375 million workers globally (14 percent of the global workforce) will likely need to transition to new occupational categories and learn new skills, in the event of rapid automation adoption. While AI is just one technology which encompasses the wider automation trend, it does significantly contribute to the overall job displacement concerns over the next 12 years.

Many have discussed the idea of some type of universal income to support people who are displaced, and allow them the opportunity to study and gain skills relevant for the economies of the future.

Beyond the concern of income replacement, there are also concerns about activity replacement. If, people are truly displaced by AI, would they even want to study to gain new skills? Some have speculated that new jobs will be created by the AI revolution that haven't existed in the past, but can all of those jobs really be filled by the workers of today?

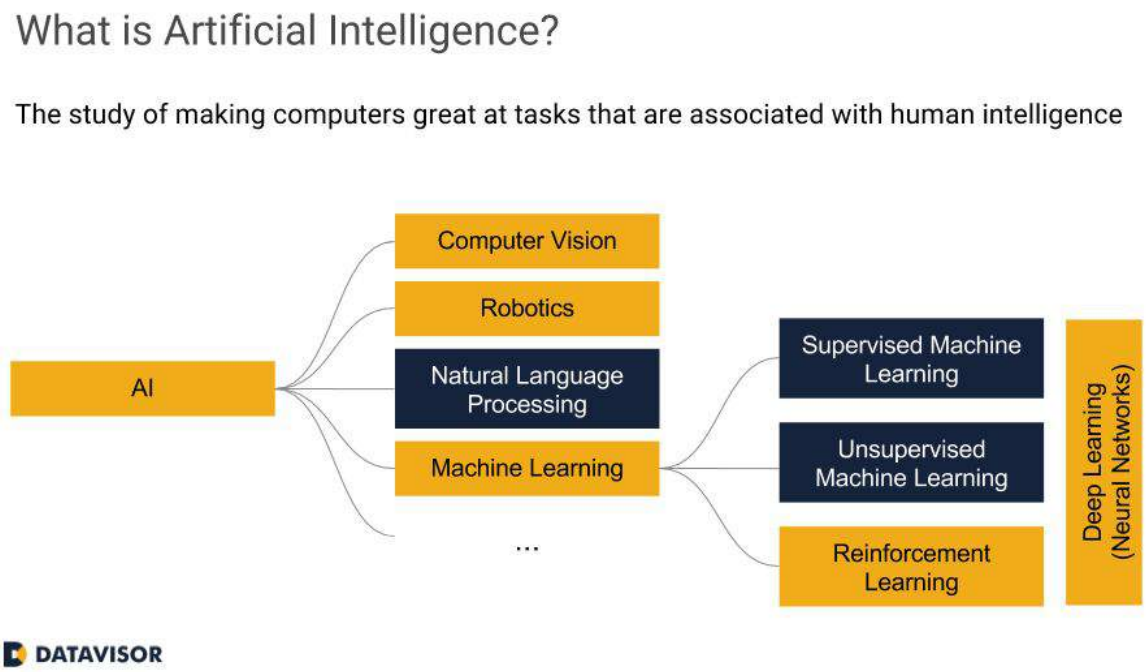
And perhaps more philosophically, if someone loses their job and has little prospect to replace it with another, then how will they spend those core 8-10 hours of each day that they typically spent working? Could we see a spike in drug use and civil disobedience? What policies will be in place to not only replace people's income, but also to fill people's schedule with relevant activities to ensure a person's dignity is intact?

Types of AI Today

One of the world's leading AI experts, Professor Andrew Ng, has stated during numerous talks and conferences that "AI is the new electricity." Professor Ng explained that electricity was an invention that impacted almost every industry such as transportation, medicine, agriculture, food storage, etc. In essence, Professor Ng is stating that just as electricity was a groundbreaking innovation that led to many other innovations, and AI is in the same revolutionary category.

There are three areas of AI which will likely have the most impact on the entity due diligence process over the next 10 years which are NLP, machine learning, and computer vision. There are also sub-categories of machine learning that could be used in a certain situations of the due diligence process and not in others. The image below shows the various fields of study of AI which includes several sub-categories of machine learning, some of which, are likely and not likely to be applied in various portions the due diligence process. Also, for specific problems

various types of AI need to be used at different points in the process to reach the optimal solution.

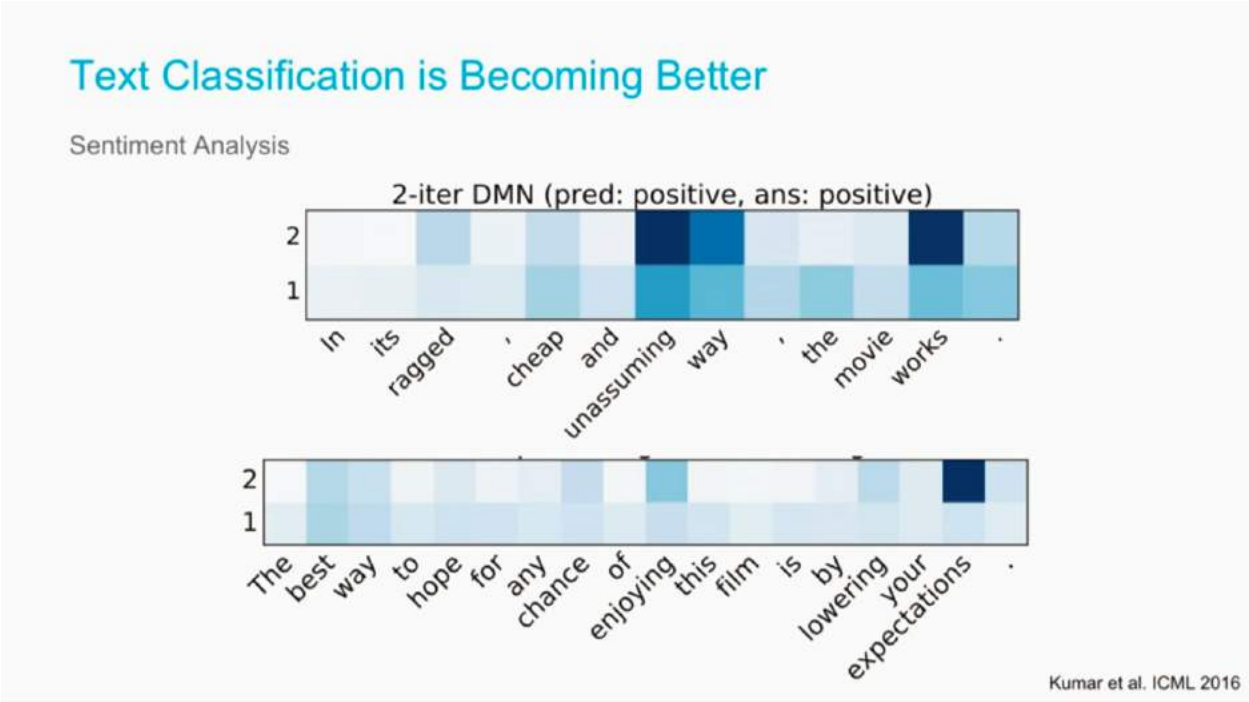


Source: https://www.datavisor.com/portfolio-items/webinar-practical-approaches-to-apply-machine-learning-to-aml/

NLP is the study of applying technology to process human language which includes, but is not limited to: sentence understanding, automatic question answering, machine translation, syntactic parsing and tagging, sentiment analysis, and models of text and visual scenes. Sentiment analysis has become increasingly accurate and more sophisticated as these algorithms have been fine tuned over time. For example, in 2011 it was observed that the mention of the actress, Anne Hathaway, appeared to influence the stock price of the Berkshire Hathaway stock.

This suggests that the type of NLP algorithms that executed automated trading strategies from analyzing news sentiment, were somewhat unsophisticated and crude by not being able to distinguish between an actress and a company with one matching word in their names. This brings up another key distinction about using AI for different purposes such as trading and due diligence. For hedge funds, its not about understanding how the algorithms works, its simply about profit and loss (P&L). If, the algorithm is profitable then understanding it becomes secondary, but in many aspects of the due diligence process understanding needs to come first and results later.

Today, sentiment analysis is becoming more sophisticated and the more advanced algorithms would not make the Anne Hathaway and Berkshire Hathaway mistake. As shown in the graphic below, there are single words in each sentence that suggest the overall sentiment is positive or negative, but the final word reveals the author's true feeling.



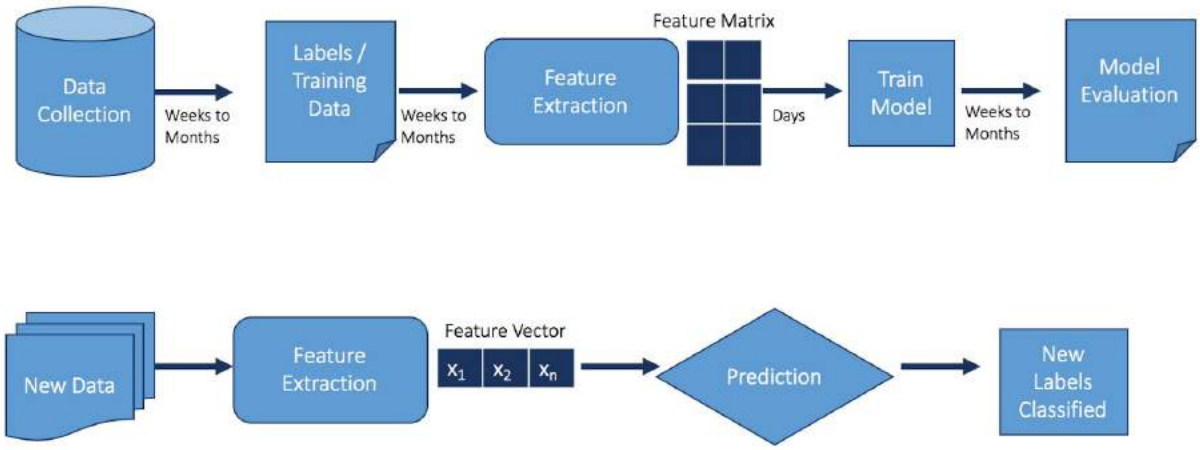
Source: Where AI is today and where it's going. | Richard Socher | TEDxSanFrancisco https://youtu.be/8cmx7V4oIR8

Machine learning can be broken into several categories such as supervised, unsupervised, reinforcement, neural networks, etc. As discussed previously supervised machine learning (SML) has brought a tremendous amount of economic value to the advertising industry by 'learning' internet users preferences based on their search and website browsing behavior and tailoring advertisements to meet their specific interests.

SML have several techniques such as decision trees, random forests, nearest neighbors, Support Vector Machines (SVM) and Naive Bayes which can solve complex computations with hundreds of variables (high-dimensional space). SML model require data to be labeled, meaning there is an input and its expected output is already predefined which works best when the problem is well understood and somewhat stable. As new data is introduced to the model, it can predict what the output should be based on how its has been trained which works for many, but not all scenarios.

The image below shows a high level flow of the SML process where the data collection, data training, feature extraction, model training, and model evaluation all make up core components

of the initial learning process. As new data is introduced predictions are made and labels classified based on the model's historical training.

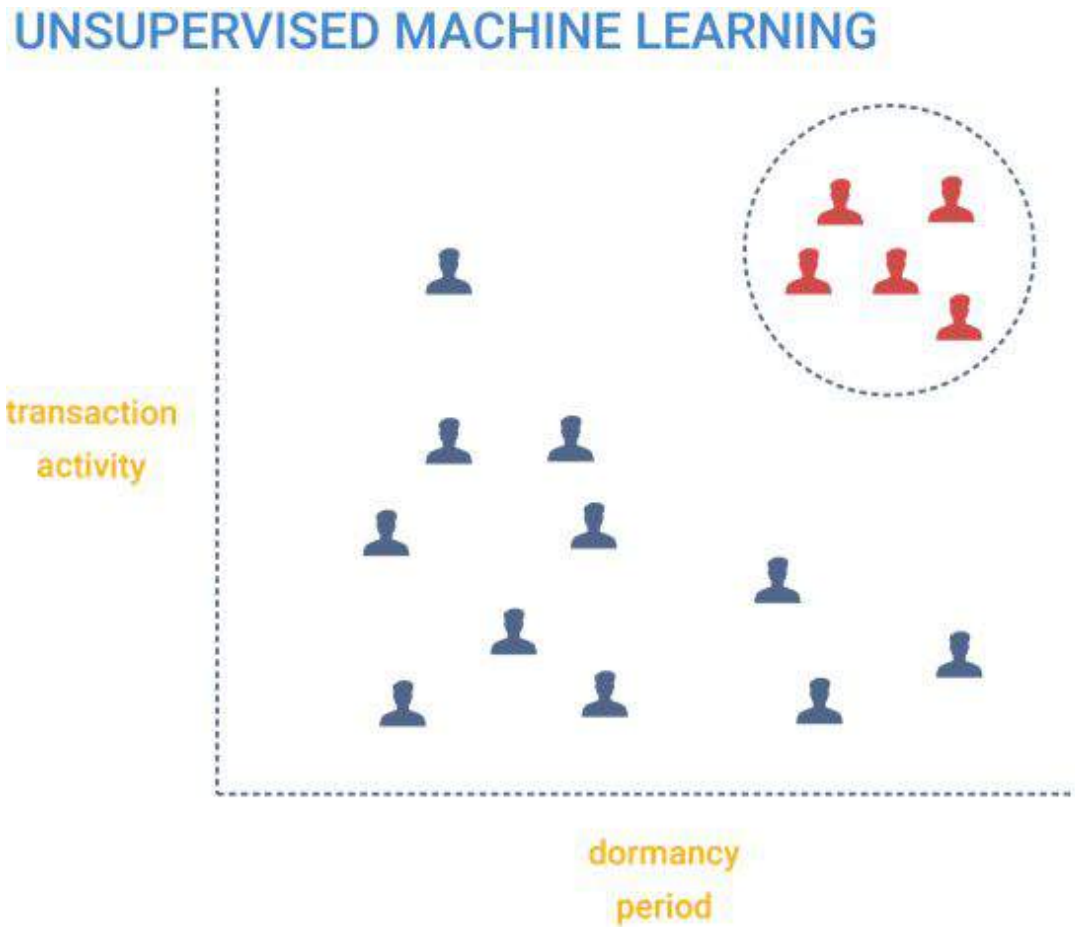


Source: https://www.datavisor.com/technical-posts/rules-engines-learning-models-and-beyond/

There are some limitations to SML such as dealing with new scenarios that are not part of the existing landscape. For example, new typologies can emerge in fraud and money laundering which didn't exist in the past or were unknown when the model was trained. Dealing with these unknown unknowns is one of the limitations of SML, which is why unsupervised machine learning (UML) is used to close the gap on CAS such as fraud and money laundering networks.

UML leverage techniques such as clustering and anomaly detection without prior knowledge of the input and expected output. In other words, no training data is needed for the algorithms to identify useful insights. UML can identity networks of bad actors acting similarly and hyper segment customers into categories which is important in the fraud prevention and AML space.

The below image represents a simple use case of UML in the fraud and AML space. It is common for bad actors wanting to commit fraud or launder money to let their accounts age before they start transacting as many institutions treat new accounts as higher-risk. Traditionally, rule based systems would be used to identify accounts older than X days conducting Y transactions over a time period Z. The problem with the naive rule based systems is that the hard-coded thresholds could miss suspicious behavior (false negatives) and tends to include non-suspicious behavior (false positives).



Source: https://www.datavisor.com/portfolio-items/aml-whitepaper/?portfolioID=6839

UML doesn't cling to thresholds and looks for patterns of behavior among clusters of entities. The use cases for entity due diligence will leverage both SML and UML for specific problems, but the overall process will most likely use a combination of both to achieve optimal results of the end goal of better entity risk management.

There are other exciting areas of AI such as robotics, but this area is not likely to have as much of an impact on the entity due diligence process in financial services when compared with other types of AI. In the Federal Financial Institutions Examination Council (FFIEC) manual, there is a reference to consider on-site visits as part of the due diligence process for cash-intensive businesses which could be potentially conducted by UAV in the future, but there are legal and technical limitations for these devices to operate completely autonomously today. As discussed in the rise of alternative data section, networks of nanosatellites could be used as another data source to verify if an entity is violating sanctions beyond what traditional trade documents show.

Similarly, UAVs could be used as another data source in the entity due diligence process, but the market needs time to mature because financial institutions are more likely to purchase the data showing images and video of locations and entities, as opposed to directly commissioning a UAV to check up on its prospect or customer. The UAV scenarios are more aligned to assessing the integrity of physical assets such as real estate for M&A or conducting audits in the retail and manufacturing sectors today. Other use cases for UAVs, commonly referred to as drones, are emerging to combat modern slavery and forced labour. In 2015, it was reported that Brazil would use drones with cameras to help combat forced labour with slave like conditions in rural areas.

According to the World Labour Organization at any given time in 2016, there are an estimated 40.3 million people in modern slavery and 24.9 in forced labour. Hence, drones have the ability for governments and companies to manage risk in their supply chain by holding their suppliers accountable for forced labour conditions by creating more capabilities to monitor activities of those companies remotely.

Politically Exposed Persons (PEPs) and Adverse Media Collection

NLP and types of machine learning are positioned to disrupt the way politically exposed persons (PEPs) and entities associated with adverse media are identified, curated, and verified. PEPs have been traditionally been identified, curated, and verified by human analysts who comb through various data sources to determine if a given person is a PEP. This approach has its limitations because there is a bottleneck to the amount of PEPs that can be verified because each analyst can only do X number of investigations each day. X number of investigations multiplied by Y number of analysts is the daily throughput for an organization verifying PEP data via a manual approach.

Another challenge to the manual approach is the timeliness of the data because the status of a PEP could change on a daily basis, and this may or may not be reflected immediately in the data set which organizations consume for their risk management programs. By merging the increased accuracy of NLP algorithms with SML which are provided feedback from analysts reviewing potential PEP and adverse media matches, the system can learn and improve over time.

Collective Learning through Data Sharing

This brings up another interesting point about the next generation of PEP and adverse media matching technology based on AI, which is the notion of collective learning. As described in the big data section the massive amounts of information produced by the internet created a scalability challenge for the internet search companies. This led to the extreme levels of parallel

processing, where a task was broken into parts, and worked on concurrently to vastly increase the throughput and speed to completion.

While the large internet search companies can support massive data centers, not all financial institutions would want to support the type of data centers required to get the most out of AI embedded technologies. Hence, its likely that certain aspects of the PEP screening and the adverse media process would be outsourced to cloud computing solutions. If, the same vendor is doing PEP and adverse media matching for different institutions on the same cloud vendor, then is there a way to share true positives and false positive matches, without violating data privacy regulations, from all of the participants? This way the algorithm can learn from the collective as opposed to be limiting the data to a particular organization's data set and searches? This also implies that the large banks will have better risk management algorithms in the future when compared to the smaller ones, simply from the fact of having more data.

The idea of sharing data among financial institutions is the holy grail of the KYC process because the same customer could be onboarded by 10 different banks and would have to replicate the procedure including the supply of all the relevant documentation, 10 separate times. The KYC utilities have attempted to address the duplicative nature of the KYC process, to a certain degree, by collecting specific information that can be reused by institutions. However, the KYC utilities tend to be specialized for specific types of KYC data, stronger in certain geographic locations, and collect information for a specific types of customers such as hedge funds, asset managers, financial institutions, and corporates.

Obviously, any type of customer data sharing leads to privacy concerns. However, some financial institutions may argue that cloud computing solutions are simply extensions of their own network, and their own data centers are no more or less secure than the cloud providers. Other institutions may opt to send out to the cloud all of the data which is not sensitive and do the last mile of matching, with sensitive customer data, on their own networks. Also, the algorithm could be designed in way where the data was not necessarily shared, but simply exposed to the algorithm itself, and not other banks, which could lessen the data privacy concerns. Data sharing without violating privacy regulations will be explored again in the blockchain section.

Due Diligence, Behavior, and Networks of Entities

Regulators commonly cite the 'risk-based approach' as an important litmus test for the health of an AML program. AI and the rise of big data is redrawing the lines of what the risk-based approach actually means. For instance, in some financial institutions today the customer risk rating process is overly reliant on a customer's static attributes such as operating in a high-risk jurisdiction, stating the intention of using specific high-risk financial products, operating a cash-intensive business, etc. However, the future of entity due diligence will likely focus more

on the actual transactional activity of the entity as opposed to simply relying on their static attributes.

For example, a customer could be identified as high-risk based on their demographic information, but their transactional activity is so minuscule that it 'should' automatically lower the risk score and scrutiny for that entity. Similarly, a customer which appears totally innocuous could be transacting in a way, which is associated with networks of suspicious actors. This is why there will be a blurring line between entity due diligence and transaction monitoring, because they are essentially two sides of the same coin and changes in one can influence the other.

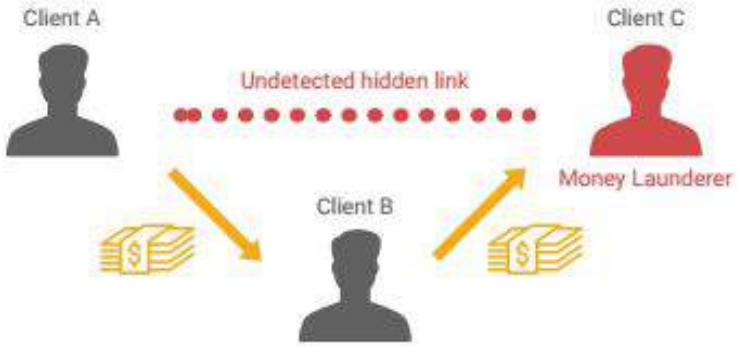
The other advantage that SML will bring to both the due diligence and transaction monitoring process is that it will be able to take thousand of disparate attributes to make more accurate predictions about risky customers and behavior. As discussed in an extended blog post, beneficial ownership can add crucial context to an AML investigation. For example, some of the data that institutions could have access to, but don't always leverage for customer risk rating are:

- Suspicious activity reports (SARs)
- Hidden links among transaction networks
- Entities linked to suspects who are PEPs
- Adverse media
- Section 314(a) of the USA Patriot Act 2001
- Section 314(b) of the same Act
- Subpoenas

Beneficial ownership data provides networks of legal entities and their beneficial owners to allow for sanctions, PEP, and adverse media screening. The SAR, 314(a), 314(b), and subpoena data helps add context to the customer's behavior and their associated network inside and outside the financial institution. If financial institutions can identify what customers are considered suspicious (labeled data) and supply their associated data then SML can make more accurate predictions about the risk future customers pose.

UML can take this process even further by clustering segments of customers together based on similar behavior derived from thousands of data points, and even identifying hidden links among bad actors as shown in the graphic below. For example, if a financial institutions filed a SAR against Client C then the investigation may or may not uncover the link between Client C and Client A, based on the movement of funds through Client B. This may be too much for a human investigator to try to uncover manually and that information may or may not be relevant for a

given investigation. UML can automatically identify these links and present the information to the investigator through a graphic interface to incorporate into their investigation seamlessly.



Source: DataVisor

Julian Wong, VP of Customer Success at DataVisor, says that “previously unknown cases of fraud and money laundering can be uncovered using UML by finding hidden linkages and correlations between bad actors and accounts. These results can in turn be used as labels to train SML models/algorithms and further increase coverage and improve precision. The combination of UML and SML offers companies better protection by catching known patterns of fraud while also casting a safety net to defend against never-seen-before fraud techniques.”

The Director of Content, Brian Monroe, for the Association of Certified Financial Crime Specialists (ACFCS) highlighted the evolving nature and intersection of fraudsters and money launderers in a recent article. Fraudsters collaborated with unscrupulous hosts and used stolen credit cards to book rental rooms online, where a portion of the proceeds was returned from the host to the fraudster. This merged fraud and money laundering typologies because the process of using the stolen credit cards was the fraud, and the return of funds from the host to the fraudster was the money laundering, which made the received funds appear legitimate. In summary, the interplay of UML and SML can address the evolving nature of CAS beyond what traditional rule based systems can offer.

Human Readable Reports

Another emerging area is the ability of various NLP and AI programs to create human readable reports from various data sources on the internet and other subscription based databases. For example, let’s say a user wanted a report about coal mining in Brazil, then a simple graphical interface will allow a user to enter information and a report will be produced by the algorithms behind the scenes. Primer, an AI company, is doing just that by making sense of the endless

information on the internet by summarizing important topics into a one page report with graphs, charts, and drill down options.

The same idea could be applied the entity due diligence space, where all public and private database information is feed into these types of algorithms to create a human readable report. There are third party companies willing to produce in depth due diligence reports on companies or individuals for a fee. These reports can be extremely detailed for a M&A deal or very basic for the screening needs of an individual customer opening a brokerage account. Regardless of whether a person or an algorithm creates the report, it still needs to be read, understood, and decisioned by a human.

The sanctions, PEP, and adverse media screening results could potentially be incorporated in these types of human readable reports in the future. Similarly, if any of the SML or UML algorithms identify suspicious activity it could provide drill down options. The only potential downside of this approach is the over reliance on these types reports to provide information, and could they potentially overemphasize specific data sources and miss important information a human investigator could have found on their own during the investigative process. This is why model validation and calibration will become such an important activities as AI technologies are embedded and deployed in regulatory compliance settings to ensure models don't exhibit systematic bias or other shortcomings.

Biometrics

Computer vision covers a wide area of applications, but biometrics and specifically facial recognition is beginning to make its way into financial services. Biometric authentication is the process of verifying an individual's identity by matching their fingerprint, retina, or face to pre-collected or pre-approved physiological identifiers. Facial recognition involves a number of different problems which are generally broken in parts and solved separately such as:

1. Identify faces in an image
2. Focus on the face, regardless of the direction, tilt, and lighting
3. Identify unique features of the face such as the width of the eyes and height of eyebrows
4. Compare unique features from face in image against database of all known faces to find match, and determine identity or unknown

Facial recognition software has advanced at a rapid pace where Chinese researchers reportedly created an algorithm that can recognize faces better than humans. Facebook's system (DeepFace) was tasked with comparing the faces from two images to determine if they were the same person and reached 97.35% accuracy when compared to the averaged accuracy of 97.53% for humans. Researchers describe the DeepFace system is based on a nine-layer deep neural network with a mind blogging 120 million parameters.

There are already organizations such as Thorn and Marinus Analytics tackling complex issues using facial recognition to fight child sex trafficking. Marinus Analytics has a released FaceSearch feature, powered by Amazon Web Services Rekognition platform, which allows law enforcement to upload a photo of a potential victim which is searched against internet sex advertisements to determine if the child has become a victim. It's logical that law enforcement have turned to the latest advanced in AI technology to fight child sex trafficking due to limited resources and the sheer volume missing children and online advertisements.

Despite the advances in the face recognition technology there are still limitations as represented by researchers in Vietnam, who reportedly fooled Apple's Face ID with a mask that cost $150. This suggests that fraud could decrease for a time by raising the cost to fool the software, but clearly the criminal underworld will react and could innovate by using 3D printers to create custom masks in the future.

Shaun Moore, one of the creators of TrueFace.AI, highlighted that some facial recognition technology can be 'spoofed', and can't tell the difference between a real face and photo. There are other concerns with the collection of biometric data for authentication purposes because of the prevalence of data breaches. If, a hacker gets access to your password it can be changed, but your retina, iris, and fingerprints are permanent. Facial recognition is probably the least invasive of all biometrics to collect given the prevalence of social and professional photos floating around cyberspace.

Financial institutions have been providing biometric options for account access as consumers seem to prefer it, over remembering a password. Traditionally, financial institutions have offered some access controls to a company's operating account by requiring two signatures from authorized account signers. However, this has been more of a symbolic act than a real control because most institutions didn't have ways to systematically validate all signatures. However, there could have been a dollar threshold assigned to a trigger a manual review of a check or wire by an analyst.

In the future, as part of the onboarding process, financial institutions could begin to offer the collection of biometrics for authorized account signers, beneficial owners, etc.. Then fund transfers or other transactions could be initiated and logged with the requestor's biometrics, which creates greater transparency and could reduce the prevalence of employee fraud. Financial institutions in the US, and many other countries, are required by law to collect and verify the name, address, and tax id of potential customers.

Could biometric data fall under the same category in the future?

If, institutions begin to collect biometric data on individuals and even beneficial owners for access control purposes, then the question becomes, what else can be done with the data?

What could develop over the next 10 to 30 years, is that adverse media is expanded to include alternative data such as faces as opposed to simply relying on textual references of an individual in a news article, court filing, PEP database, etc. As the facial recognition algorithms get better and processing speed continues to double every 18 months then searching for a face, could be similar to a google search today.

Sanctions lists could evolve to not only include textual information, but also a high resolution photograph of a sanctioned individual. Then violating sanctions will not be limited to what gets represented in trade documents and fund transfers, but simply being in the same photo as a sanctioned individual could lead to reporting by financial institutions and investigation by regulators.

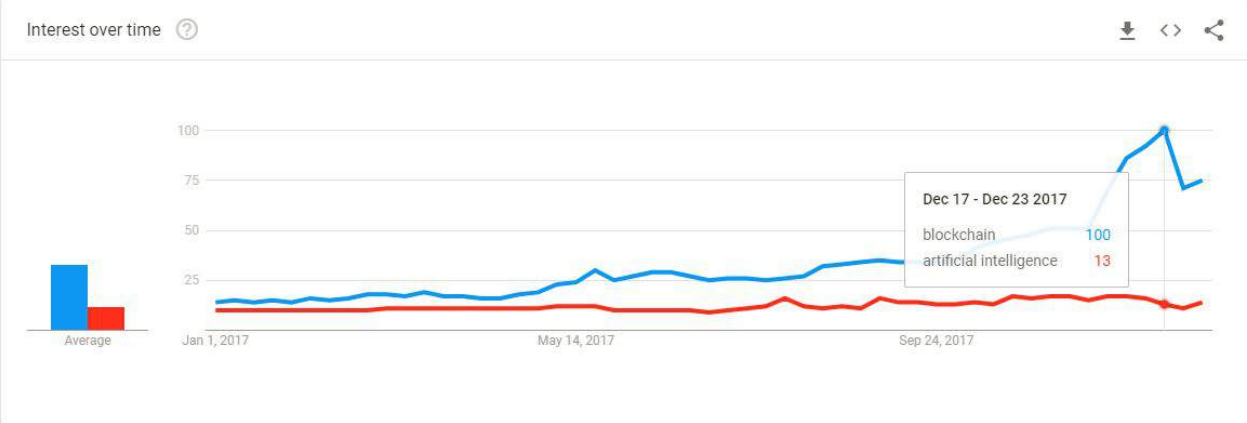
For example, if photos of the meeting between Joaquin "El Chapo" Guzman Loera, the OFAC sanctioned Drug Kingpin, Kate Del Castillo, and Sean Penn were leaked 30 years from now, then it could create an adverse media hit in the sanctions screening programs of the future, assuming photos of sanctioned individuals are indexed and compared against facial data of an institution's customer base, including beneficial owners acting on behalf of a company.

Source: http://abcnews.go.com/International/kate-del-castillo-describes-sean-penns-meeting-el/story?id=37729504

If, biometric data is used for screening purposes in the future, it could feed other emerging trends such as privacy and anonymity which can be offered by the darknet and other encrypted applications.

Blockchain

AI received an incredible of media coverage in 2017, but it was eclipsed by the interest in blockchain, the underlying technology powering the Bitcoin protocol. The real driver of interest in blockchain was the breakout year that Bitcoin had in 2017, and this drove people to search related terms such as blockchain to understand why the price kept increasing and what was behind it all.



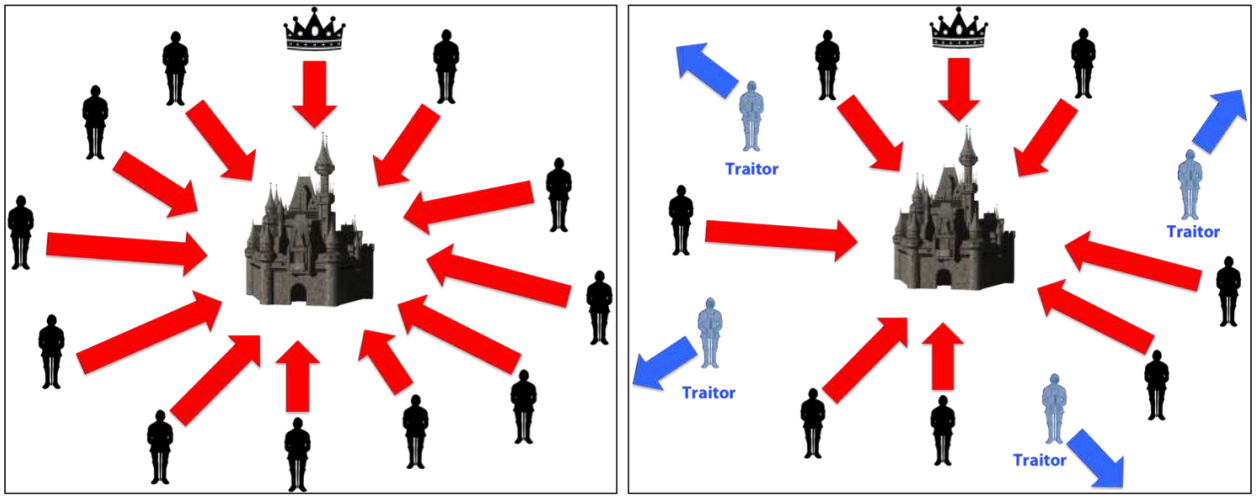
Source: Google Trends

At the most basic level, blockchain is form of mutualized record-keeping in a near irrevocable time-stamped ledger. To understand blockchain it's worth taking a closer look at the emergence of Bitcoin, which was the first successful implementation of the blockchain *idea*. It's useful to think of blockchain as an idea as opposed to a technology because this may make it more intelligible, to a certain degree.

Despite some attempts to separate blockchain from Bitcoin, it was the world's first decentralised cryptocurrency, Bitcoin, that propelled the idea of blockchain into the public consciousness. In October 2008, Satoshi Nakamoto, a pseudonym for a person or group of people, published a paper describing the how the Bitcoin protocol would allow for online payments without having to go through a trusted third party such as a financial institution. Bitcoin solved the problem of trustless consensus, because it provided a self-governing network through the innovative use of several different ideas such as proof of work (POW), cryptographic signatures, merkle chains, and peer-to-peer (P2P) networks.

The classic problem that Bitcoin solved is referred to as the 'Byzantine Generals Problem', which is a logical dilemma of trying to reach consensus described by Leslie Lamport, Robert Shosta, and Marshall Pease in an academic paper published in 1982. The goal of the paper was to highlight that reliable computer systems must be able to handle malfunctioning parts that give conflicting information to different parts of the system. This concept was expressed abstractly by thinking about the generals of the Byzantine army, waiting outside of an enemy city waiting to attack it.

Since the different groups under each general's command are dispersed over a wide geographic area, it makes centralized command difficult. Hence, the generals are forced to rely instructions to another through messengers so they can come to a consensus of when to attack the city, which will only be successful if the all generals strike at the same time. The problem is that the generals know their is a traitor among them, so how will they know the message they receive has not been tampered? If, different messages are sent to different generals then it will break down the cohesion of the army of how to act and when, and could cause the attack to fail.



Coordinated Attack Leading to Victory **Uncoordinated Attack Leading to Defeat**

Source: https://medium.com/@DebrajG/how-the-byzantine-general-sacked-the-castle-a-look-into-blockchain-370fe637502c

The same idea could apply to a P2P payment system which doesn't have any trusted third party validating the transactions. In a shared and distributed ledger, any payments (messages) to the ledger (coordinated attack time) must be trusted. But large distributed networks can have millions of users (generals) so how can the payments made through an open ledger system be trusted with no third party facilitating the activity? Blockchain essentially solves the Byzantine Generals Problem through an innovative combination of existing ideas including cryptography, P2P networks, and game theory.

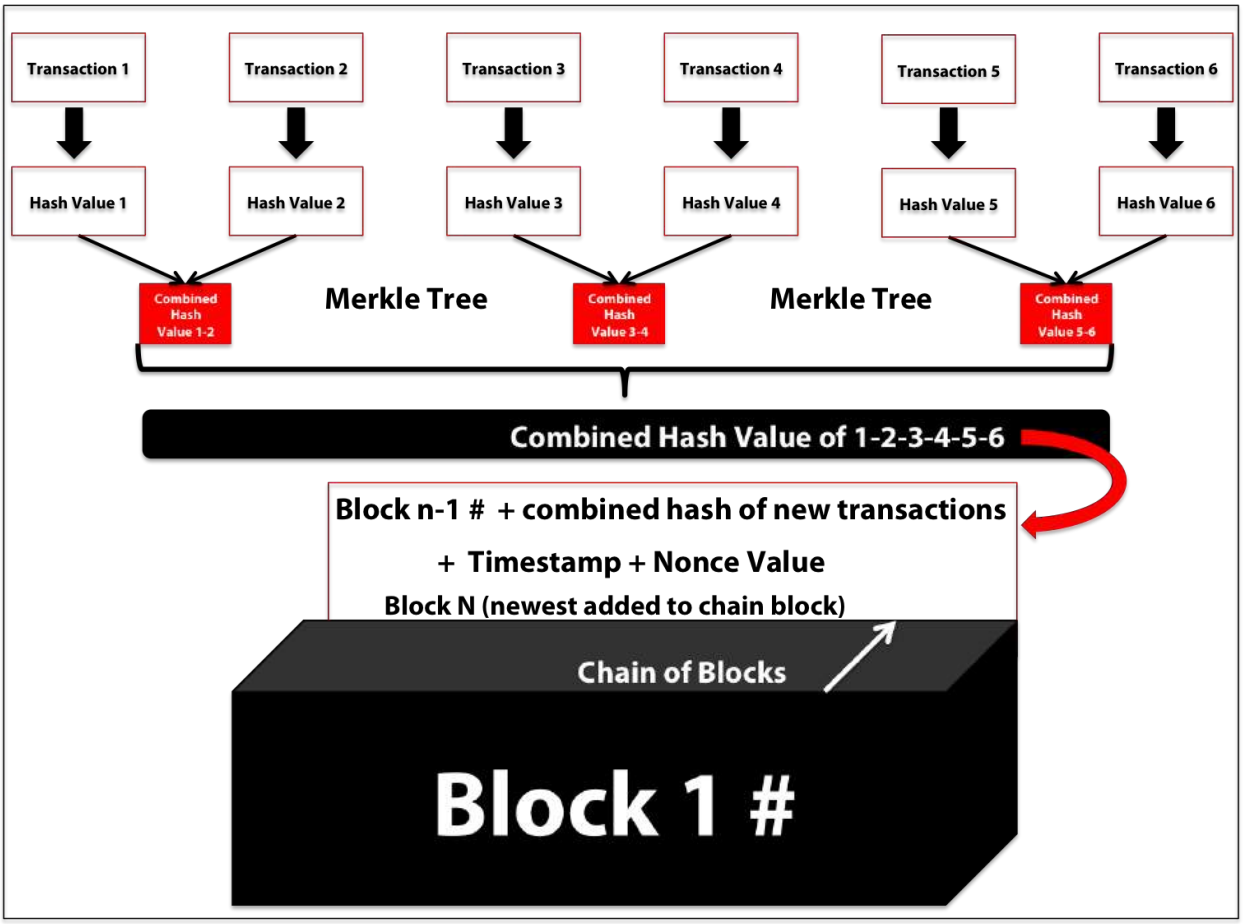
A Closer Look at Bitcoin

Again, Bitcoin is essentially a digital ledger of all transactions that have been recorded since its genesis and transactions are grouped together to form blocks which are cryptographically secured and linked to previous blocks in the blockchain (ledger). The Bitcoin ledger is distributed across a network of computers commonly referred to as nodes. In order for bitcoin transactions to complete successfully, all of the nodes on network must agree or reach *consensus* that the transaction is accurate and true. To conduct a bitcoin transaction, a person must have a bitcoin wallet that can read and initiate transactions on the ledger.

To move bitcoin from one wallet to another, the network of nodes will examine the transaction to verify its authenticity and ensure the bitcoin is available and prevent double-spending. Once, the individual transaction is determined to be authenticate it gets sent to a queue with other pending transactions that will form the next block in the blockchain. For transactions to be added to a block they must be approved by the network. The final approval is based on a computational puzzle (the proof-of-work) which is solved by specific nodes known as miners. Once a miner solves the proof-of-work for a pending block, the solution is sent to the network for verification. Once the solution is verified by the network, the block is added to the blockchain.

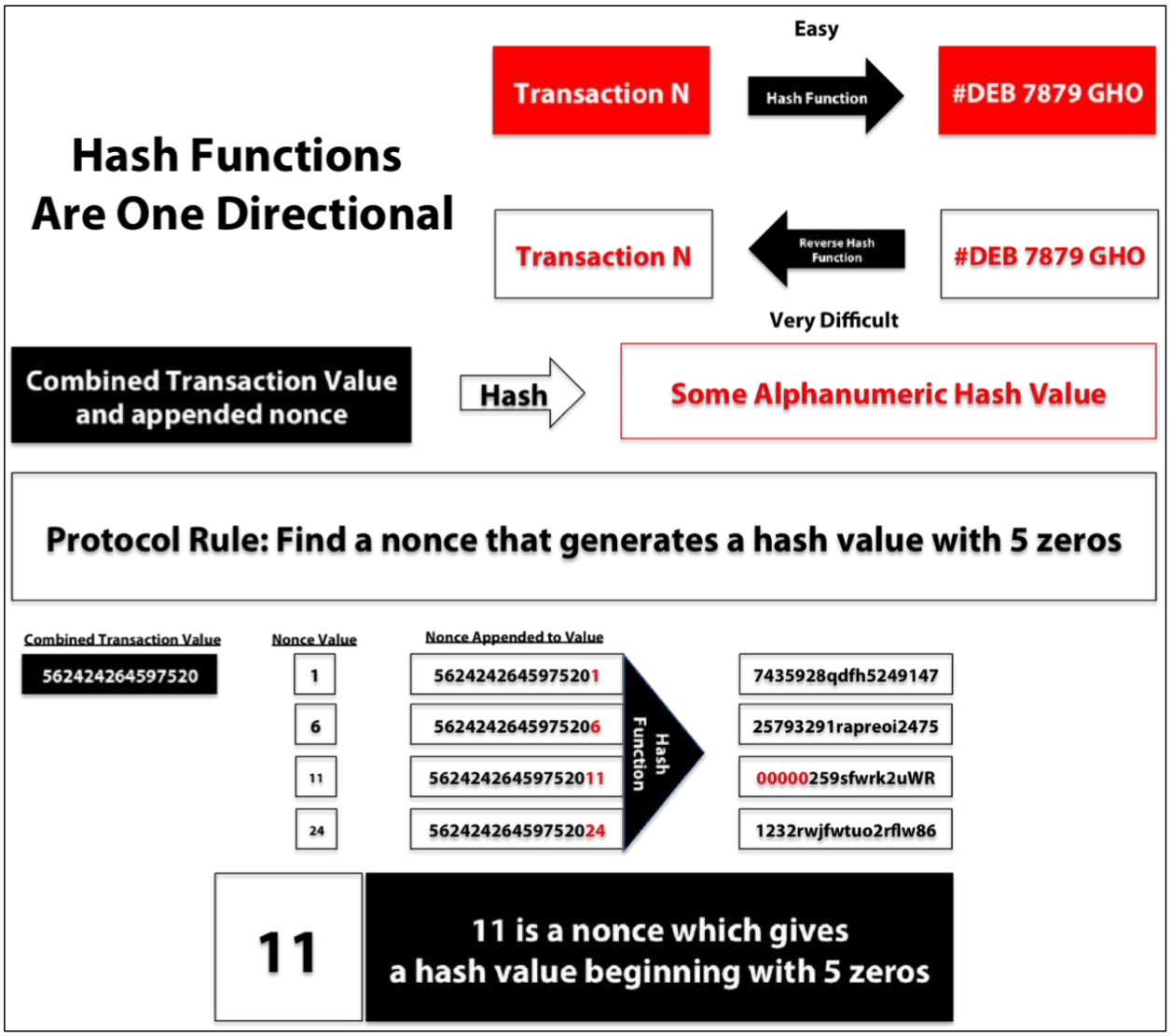
Bitcoin uses the Secure Hash Algorithm 2 (SHA-2) developed by the National Security Agency (NSA) to encrypt transactions. For example, if you wanted to send 1 bitcoin to your friend, then the transaction itself can be thought of as a string of characters which is put through a cryptographic hash function which generates a hash value. The interesting thing about hash functions is that they are nearly impossible to invert. In other words, it's nearly impossible to know what the input (transaction) was based on analyzing the hash function's output. Furthermore, if only one character of the input changes, then the hash function will create a completely different output.

After each pending transaction is put through the hash function, the individual generated hash values are routed through a merkle tree to form one hash value based on the combined hash values from all of the pending transactions that will form the new block. Then the computational puzzle is solved based on this newly defined character string based on the combined hash value from the pending transactions within the new block, the hash value from the previous block, a timestamp, and a cryptographic nonce.



Source: https://medium.com/@DebrajG/how-the-byzantine-general-sacked-the-castle-a-look-into-blockchain-370fe637502c

The cryptographic nonce is where part of game theory comes in because to solve the computational puzzle miners find a nonce value, which is made arbitrarily difficult, that produces the output which meet Bitcoin's protocol standards. The only way for the miner to solve the puzzle is by brute force through trial and error and a lot of computing resources. Miners are also incentivised to competing with other miners and being the first one to solve the puzzle, despite it being very difficult, because the winner is rewarded with bitcoins. The graphic below shows the goal of miners is to append a nonce value to the end of the combined hash value from the pending block and pass the concatenated value through the hash function again which produces another hash value with 5 leading zeros.



Source: https://medium.com/@DebrajG/how-the-byzantine-general-sacked-the-castle-a-look-into-blockchain-370fe637502c

Issues with Bitcoin

Bitcoin has proven that the interaction between core concepts such as cryptography, P2P networks, and game theory can be applied to create a functional system where consensus is possible without a trusted third party. In this sense Bitcoin has been a success because it has inspired a wave of investment and research into what else might be possible.

However, there are still fundamental issues with the current Bitcoin protocol, and the three major ones are scalability, sustainability, and money laundering. Bitcoin can only process between 3 to 7 transactions per second, based on an arbitrary limit of a 1 megabyte (MB) block size. How can Bitcoin be a viable medium to conduct transactions with an upper limit of 7

transactions per second? This is much lower than the scale of transactions that can be processed through Visa and PayPal infrastructures.

Bitcoin enthusiasts would argue that the block size could be increased if some of the nodes or members on the Bitcoin network agree to the new rules which is referred to as a hard fork. Ironically, for participants on the Bitcoin protocol, where consensus has been predefined and governed by mathematics, its really hard to come to consensus on Bitcoin outside of the protocol itself. Bitcoin cash is an example of a hard fork which occurred in August 2017 where some nodes will follow the new rules defined by the fork and other nodes will follow the old rules of Bitcoin. This essentially creates two blockchains with a common history, but are no longer connected and will create their own unique transaction histories going forward. Not all hard forks have been successful because the SegWit2x proposal was cancelled as supporters felt consensus was not reached among a wide enough user base of the Bitcoin community.

Another major concern with Bitcoin, and cryptocurrencies in general, is sustainability and because the computational puzzle which needs to be solved requires a lot of computing power. According to Digiconomist, it was estimated that the Bitcoin network uses more power than all of Ireland in one year. There are various energy sources for electricity, but fossil fuels still hold a majority of the share in the US. According to the Institute for Energy Research (IER), 41% of electricity is generated by coal and burning coal creates carbon dioxide which is something governments are trying to regulate.

Based on the estimated energy consumption of Bitcoin, it would take roughly 250 to 300 kilowatt hours to process one 1 bitcoin transaction. This would equate to powering the average US household for 8 days or burning 244 pounds of coal. Regulators may try to impose energy consumption standards on cryptocurrency transactions, similar to emission standards imposed on automobiles. However, the risk could be that artificially decreasing the difficulty of the computational puzzle, could make the protocol more vulnerable to a cyberattack.

The last major concern with Bitcoin is its connection to money laundering and crime. Ironically, it was exactly the criminal element which were the early adopters of Bitcoin, and this laid the foundation for its legitimacy as a medium for the transfer of value. Silk road was the first darknet market used primarily for selling illegal drugs, and was shut down by the FBI in 2013. The darknet has been built on top of the internet, which is only accessible through special tools such as Tor and by direct links, invitations or passwords to allow for anonymity for the website host and the user browsing the web. Some users use software like Tor to browse the web anonymously in countries where censorship of the internet is common such as in China and Iran. However, the darknet allowed for dark markets to emerge, but the one missing ingredient was a way to exchange value anonymously which Bitcoin solved, to a certain degree.

Silk road was very successful given that it had over 13,000 items for sale in October 2014, most of them drugs, that were categorized by types such as stimulants, opioids, precursors, etc. As a testament to Silk road's success, the US Department of Justice (DOJ) collected $48 million in proceeds from an auction where 144,336 confiscated bitcoins were sold. Bitcoin was a much more effective medium for conducting illicit transactions when it was not well known in the public mind.

For example, one of the main ways to buy Bitcoin today is to go through an exchange, and many exchanges perform some basic form of KYC procedures and may collect identification, addresses, etc. This will make it easier for law enforcement to piece together who is actually behind a given bitcoin transaction. However, it's still possible to purchase bitcoin anonymously, if someone can deal directly with a seller and circumvent the need to go through an exchange which will try to verify your identity.

Perhaps the leading indicator that Bitcoin will trend downward in 2018, and beyond, is that criminals, which laid the foundation for its mass adoption, are beginning to abandon it for more anonymous cryptocurrencies. Law enforcement is ringing the alarm bells to policy makers as can be seen by the testimony made to the Senate Judiciary Committee on modernising money laundering laws by Matthew Allen, ICE's special agent in charge of Homeland Security Investigations (HSI):

"HSI agents are increasingly encountering virtual currency, including more recent, anonymity enhancing cryptocurrencies (AECs), in the course of their investigations. AECs are designed to better obfuscate transaction information and are increasingly preferred by [transnational criminal organizations]."

Regardless of what happens to Bitcoin, bubble or not, and despite the rise in criminal dark markets, Bitcoin was the first successful implementation of a blockchain protocol that has inspired a lot of smart people to imagine what types of applications are possible. Hopefully this will lead positive social benefits and sustainable innovation.

First Digital Government Doubles down after Cyberattack

A recurring theme in this paper has been CAS and, more subtly, the interconnectedness of things. It's very interesting to see what prompted Estonia to digitise nearly its entire government, and how it earned the name, 'the most advanced digital society in the world', by Wired magazine. Estonia has historically been a battleground for various countries such as Denmark, Germany, Russia, Sweden, and Poland because of its important geographic position in the Baltics. During World War II, Nazi Germany launched their invasion of the USSR, which included Estonia, in 1941. Eventually, the Soviet army was able to push the Nazi troops out of Estonia by 1944, and reoccupy the country.

In 1947, after World War II had ended, the Soviet authorities introduced the Bronze Soldier which was supposed to represent the USSR's victory over the Nazis. Monuments being erected after the war was to be expected, and this is especially true for the USSR which suffered the most human casualties of any country. However, for ethnic Estonians the monument didn't represent liberation at all, and it was a solemn reminder of years of Soviet occupation and oppression. In 2007, the Estonian government decided to relocate the Bronze Soldier from the center of its capital to another site on the outskirts of the city.

The decision to move the monument created outrage from the Russian media outlets, and prompted two nights of protesting, rioting, and looting by Russian speakers. Then on April 27, 2007, Estonia was hit with a series of cyberattacks, some of which lasting weeks. The websites and online servers of different institutions across Estonia were taken down through denial of service type attacks, where servers are overwhelmed by a large number of artificially created online requests.

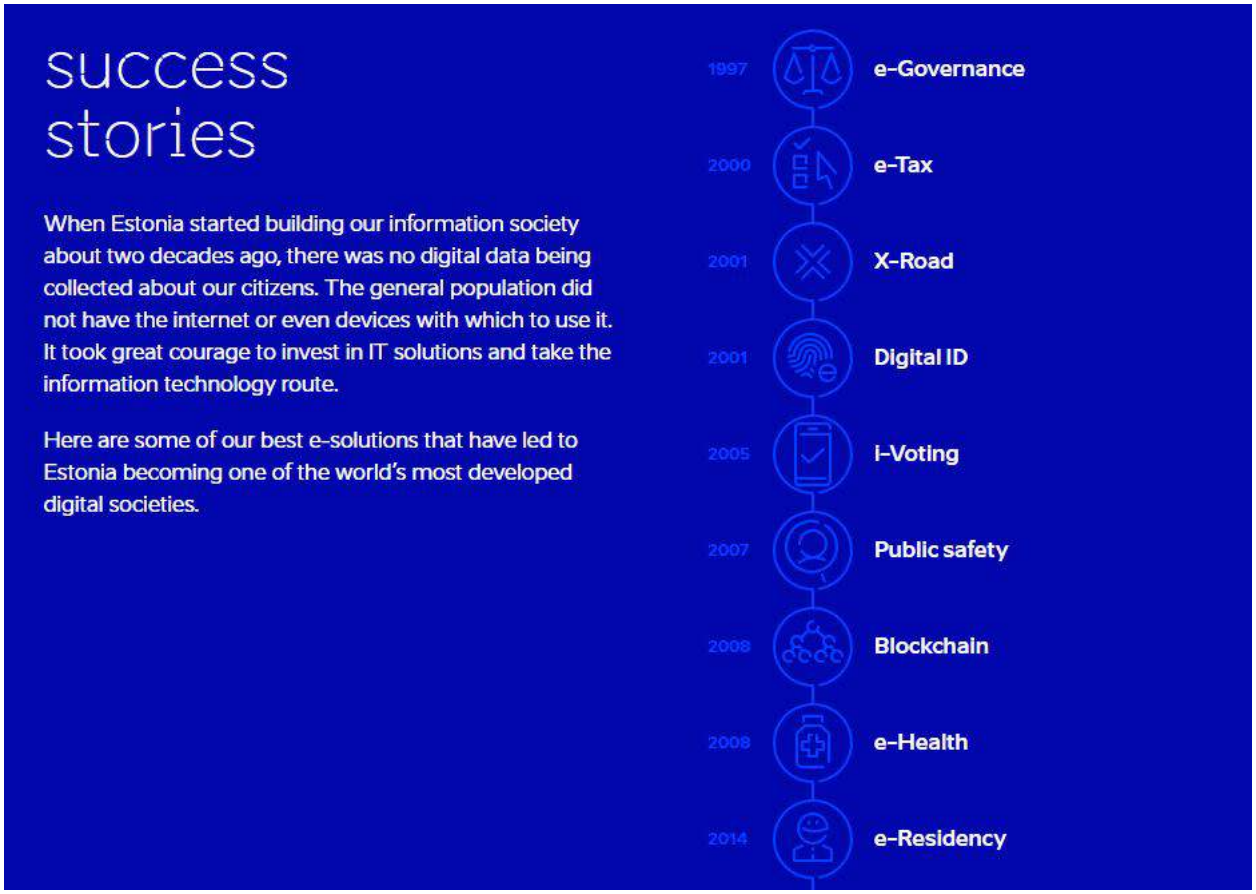
The result of the cyberattacks during that time period was that ATMs didn't work reliably, government employees had issues communicating via email, and newspapers and broadcasters couldn't get the news out. Liisa Past, a cyber-defence expert at Estonia's state Information System Authority, explained that "cyber aggression is a different type of kinetic warfare" which can be deployed with lower risk of creating tensions with Western powers and other Nato nations than traditional forms of warfare.

Russian aggression in Crimea resulted in more US sanctions, but cyber aggression didn't because it's not always easy to prove who was behind an attack. While Estonia strongly suspects the 2007 cyberattacks were coordinated by the Kremlin, it doesn't have any definitive proof. The US is beginning to see cyber aggression as a real geopolitical risk which can be mitigated, when the perpetrators are known, to a certain degree, through its cyber-related sanctions program which was launched on April 1, 2015.

Estonia had the advantage of being a young nation, when its gained its independence in 1991 and was not burdened by legacy IT systems because of its feeble digital infrastructure, a remnant of the Soviet era. The country's population, just over 1 million people, is much smaller compared to the majority of other nations in the world which makes it more nimble to change and reaching consensus among heterogeneous stakeholders.

These conditions and the 2007 cyberattack prompted Estonia to take steps to further secure its digital infrastructure by adopting radically new technology and become more cyber resilient. There were also economic considerations from the beginning of the country's independence because by becoming leaders in technological innovation, it would create greater economic opportunities for a country with few other growth options available.

The digital infrastructure that Estonia built is based on public key infrastructure (PKI) and eID system which leverages encryption technology and requires 2-factor identification for access. Information can be shared among different government agencies on a need to know basis and audit trails are kept what data is being accessed and by whom. Also, the cost savings and efficiency of having this system is profound because the data is decentralised and is not duplicated across various participating institutions, but simply accessed and used on demand. Blockchain was not part of Estonia's initial core digital infrastructure, but it began testing it in 2008 and put blockchain into production in 2012 for various use cases including national health, judicial, legislative, security, and commercial code systems. The below graphic shows shows key milestones in the digital evolution of Estonia.

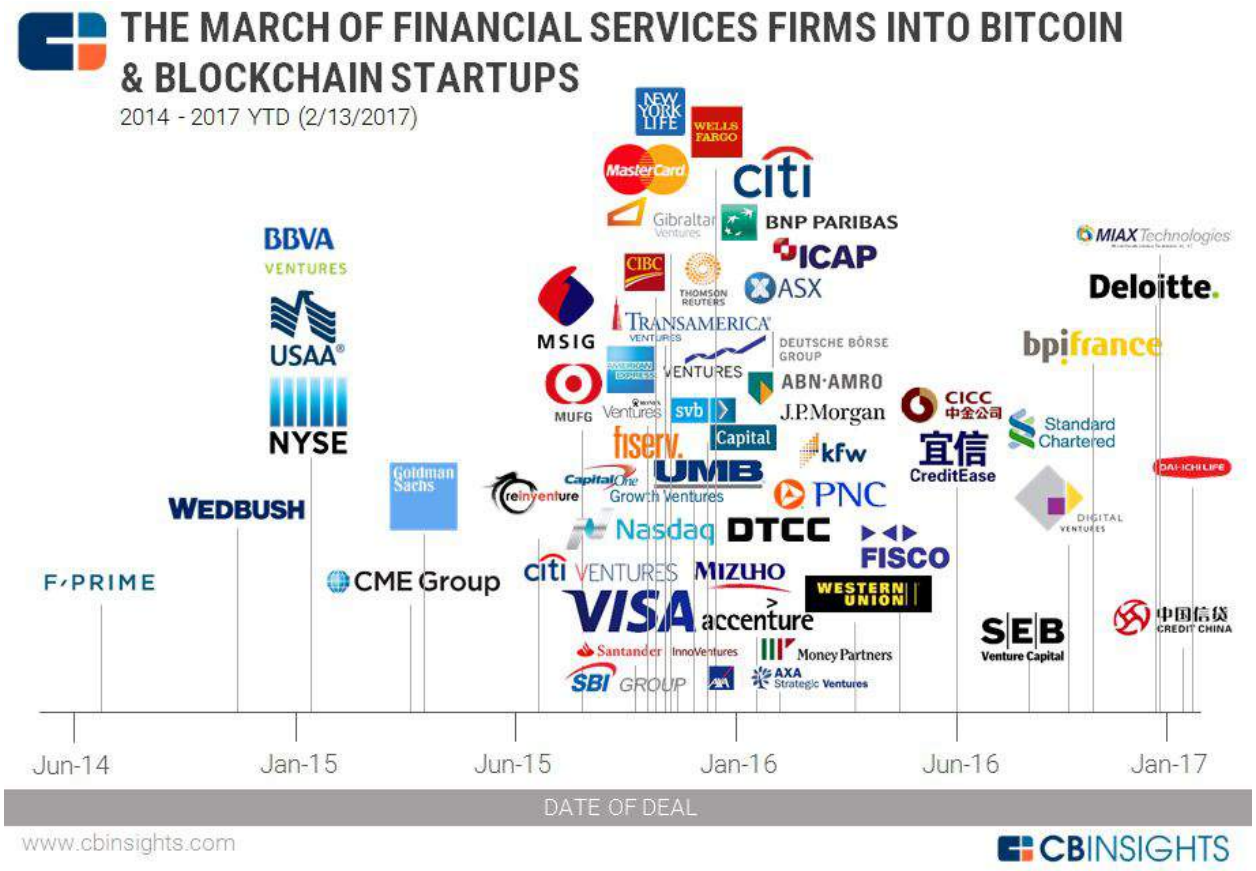


Source: https://e-estonia.com/

Blockchain in Financial Services

Financial services is one sector that has jumped on the blockchain bandwagon. This can be easily illustrated by the amount of investment in blockchain startups and banks participating in

blockchain related projects. There was a surge of participation in blockchain startups in 2015 and 2016, and still continues today, as seen in the graphic below.



Source: CB Insights

Large existing customer bases and the ability to cooperate with other financial institutions are distinct advantages that banks have over their fintech competitors. This ability to cooperate can be traced back to, among other things, the creation of SWIFT, where financial institutions had to agree on standard ways to communicate between one another, regarding payments and other types of financial transactions. This is an important distinction to make because the success of many of these blockchain projects require the group of participants reaching consensus on the rules that govern the system.

Based on the financial services history of coming up with standards to interact with one another, they are poised to be one of the groups of institutions that can derive tremendous economic value out of the new applications of blockchain. While one of the motivations to participate in blockchain related project there are also other benefits such as a better customer experience. There is also a clear distinction between the bitcoin blockchain, and the consortium blockchains

such as R3, Hyperledger, and the Enterprise Ethereum Alliance. The bitcoin blockchain is completely public and only requires the minimum system requirements, application download, and internet connection to participate, but the consortium blockchains are a hybrid because they are 'member-only' (not public) and are managed, to a certain degree, by a central authority. So it depends on how you define blockchain, but the consortium blockchains are probably better defined as a distributed ledger technology (DLT). In a 2016 white paper, The Depository Trust & Clearing Corporation (DTCC) defined DLT as having the following characteristics:

- A common shared version of the truth – every trusted member has a copy of the same history of all transactions in an asset.
- All data is encrypted in a common manner according to modern standards and can only be decrypted and inspected by the owner of the required keys to the data.
- The shared ledger, used by every trusted party in trading a particular asset, establishes a network and data standard that can be integrated with tools, workflows and asset management systems in a simplified, consistent manner.
- The transaction distribution model defines a paradigm for always-on, active:active processing, which is more resilient to local database corruption than existing hardware replication models.

There are many use cases for DLT including trade settlement, payment processing, trade finance, etc. It really comes down to the lack of transparency and interoperability between financial platforms within institutions themselves, and externally at other entities that creates spiraling cost and inefficiencies. Consider what SWIFT actually accomplished, it just allowed for the standardisation of message communication between participating members in the network. Each member has its own technology infrastructure and data storage facilities. So in essence, the data was duplicated across every member's infrastructure involved, at some point in the message chain. This is what Estonia did away with, the unnecessary duplication of data, by leveraging an interoperable digital platform where data was shared and accessed securely on demand.

Historically, SWIFT messages would have to be routed through multiple banks infrastructure, which was clunky, and if a payment did get hung up for compliance or some other reason, then there would be no transparency into where it sat within the collective processing queue. By sharing a distributed ledger, it will greatly increase processing times and reduce costs of old legacy systems, if consensus on the rules are reached and enough participants sign up to the same platform. As the technology matures and the consortium blockchains start to see some small incremental successes then there will be renewed interest in tackling large scale problems.

How Distributed Ledgers can Reinvent Due Diligence Forever

To understand how blockchain could fundamentally change entity due diligence forever, it's worth examining a pilot project dubbed Massive Autonomous Distributed Reconciliation platform (MADREC) which is trying to address the quality of counterparty data. The Markets in Financial Instruments Directive (MiFID) II is requiring the use of legal entity identifiers (LEIs) for all eligible entities. The Senior Product Manager of Gresham Tech, Steve Miller, explored the many use cases of blockchain in the financial services space in various blog posts. He stated the following in an email exchange about the MADREC project:

“This sounds to me like one of the first real-world use cases for distributed ledger technology (DLT) in this space – crystallising the idea that if firms A and B have already done the due diligence on Entity X, then firm C shouldn’t have to (if A, B and C are all contributors to the same ‘ledger’ of entity reference data). Nor should anyone be periodically reconciling their customer static/reference data against so-called ‘golden’ sources – because the single distributed chain *is* already the golden source by definition.”

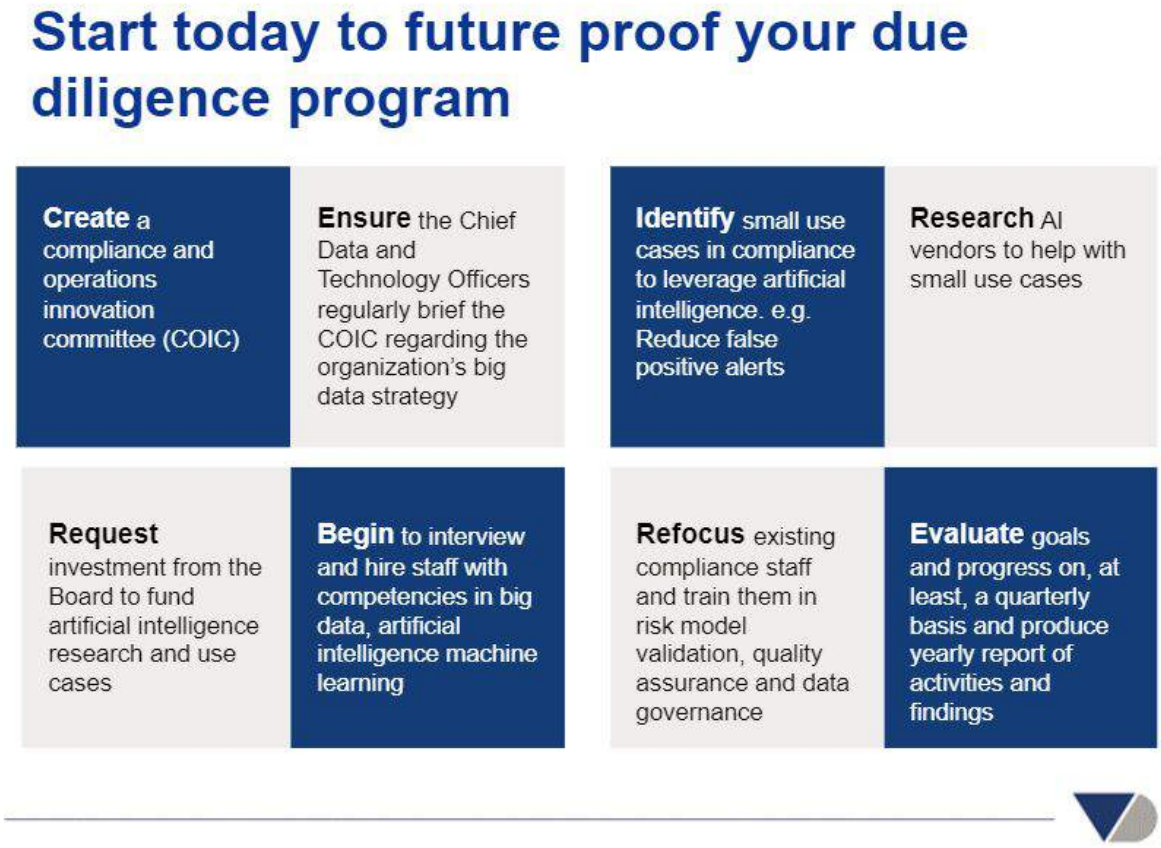
That about sums it up. This is how blockchain or DLT or whatever label you want to put on it, will change due diligence forever. Once, the due diligence for the same customer or entity can be shared among participants in the blockchain, then it removes the duplicative effort of the process. No longer would the client have to provide the same document, to several different banks. Just as the Bitcoin protocol removed the need for a trusted third party, financial institutions could remove the need for data utilities by distributing the workload and sharing the results. It’s interesting to see how slackers would be managed in this type of environment though. What happens when Bank A is not pulling its weight?

Clearly, there are major challenges to implementing a wide scale and comprehensive KYC DLT platform. It would also require that all legal entities have some type of universal identifier such as the LEI, beyond simply for derivatives trading. It’s not clear if the LEI could become the universal standard for all legal entities worldwide, and there would need to be consensus among governments and regulators that this sort of approach would be acceptable. Also, complex corporate structures and dynamic nature of beneficial ownership could throw another wrinkle into the mix.

Reaching consensus among homogeneous entities such as financial institutions is much easier than heterogeneous stakeholders that include governments, corporations, financial institutions, regulators, etc. As the founder of Bloqchain Science, Dean "Sakis" Karakitsos, once told me in a conversation, “the state of blockchain today, is like being in 1995 when the internet was taking off.”

Recommendations

At the end of the [Channeling big data through RegTech] webinar, 8 recommendations were listed, but only a few were explored briefly given time constraints. Each recommendation will be explored in more detail below, in the context of the points highlighted in this paper thus far.



Source: https://www.bvdinfo.com/en-gb/knowledge-base/webinars-on-demand

1. Create a compliance and operations innovation committee (COIC)

As discussed, there are multiple threats that financial institutions face on various fronts including rising consumer and regulatory expectations. This means banks have to transform their infrastructures to become completely integrated and digital which can satisfy the on-demand and near real time delivery of various requests. As regulatory expectations increase, so does

costs to comply since the underlying technology being used hasn't changed drastically changed in the last 10 years. Large institutions can be categorized as CAS in their own right, with conflicting priorities across business lines so a COIC is needed to drive change effectively.

As mentioned earlier, a December 2017 report by the McKinsey Global Institute estimated that as many as 375 million workers globally (14 percent of the global workforce) will likely need to transition to new occupational categories and learn new skills, in the event of rapid automation adoption. Hence, another key priority for any innovation committee needs to be enterprise policies on human resources.

Not all jobs can be tracked by utilization rates, but customer onboarding, fraud, and money laundering investigations are good job categories, where an employee's utilization percentage could be estimated, to a certain degree, given most of work is recorded in an investigation tool. So, an institution might estimate that the average utilization percentage within this department is 70%. If, the utilization percentage drops down to an average of 60%, then what will the institution do? There are several options such as:

- Reduce employee headcount to raise the group's total utilization percentage back to 70%
- Retain employees and reallocate the extra 10% of time gained among training, extra vacation time or maybe a 4 day work week

Institutions need to start thinking about how they will retain good employees for the long-term and how they can train people to learn to do completely new jobs. Also, European companies tend to offer more vacation time than ones is the US, so could increased efficiency and more time be given back to employees for a better work-life balance?

Also, it's important for institutions to have a utilization rate policy, whenever possible, and monitor compliance with it, so heads of business don't see automation as an opportunity to reduce headcounts disportionately. This could presumably be done in an effort to reduce the unit's costs and artificially inflate profits, which may lead to bigger bonuses for upper management.

2. Ensure the Chief Data and Technology Officers regularly brief the COIC regarding the organisation's big data strategy

This point assumes that one of the main objectives of the COIC is a big data strategy. And it should be. To get the most out of the latest advances in AI and machine learning then a big data platform on premise or in the cloud is a prerequisite for some of the intensive computing power algorithms.

Big data platforms offer other opportunities such as better master data management (MDM). Another way to think about these central repositories is that they are flexible, and don't need to adhere to a monolithic data model. They also offer the opportunity to manage the meaning of data as opposed to simply its movement. Once, an organization knows what data means then it can protect and value it.

The next step in the evolution of analytics is the reusability of data, similar to the idea of how SpaceX was able to reuse rockets. Elon Musk realized that one of the major costs of space exploration, was that rockets were throw away items. If, rockets could be fired into space multiple times then it drastically reduce the costs to explore space. It's essentially the same idea with data from different source systems, because today the same mortgage file could be sent to 10 different analytic systems, and would need to be shaped 10 different ways to fit within the data models of those systems. Once, analytic systems can take the data 'as is', then that will be the next phase in the evolution of analytics that will drastically reduce operational overhead costs.

3. Request investment from the Board to fund AI research and use cases

It won't be a surprise to anyone who worked on large scale enterprise projects, that support from the Board of Directors is essential to the success of the initiative. This support can take many forms such as financial, agenda based, etc. The Board also needs to support the idea that they could fund AI research internally, and the project fails to deliver anything of value, besides a learning experience. However, there needs to be mind shift that failure is not necessarily a bad thing, if the group learns from it and can document their findings for the next project to reference. It's the willingness to fail, learn from that failure, and to try again that will lead to the best possible use cases for new and cutting-edge technology such as AI.

4. Begin to interview and hire staff with competencies in big data, AI, and machine learning

Institutions will need to invest in projects, but also people to help proof-of-concepts (POC) in motion. Since, talent in big data, AI, machine learning is limited then the institution may need to consider hiring an expert in AI to help guide a select group of developers to learn how to develop different types of AI algorithms. This may seem odd that an institution would need to create a type of internal university, but completely relying on external consultants is not a viable option either.

There are other options available such as sending developers to AI bootcamps or short-term fellowships. The Data Incubator, founded by Tianhui Michael Li, offers a data science

fellowship specifically designed to train highly educated professionals, practicable and applicable quantitative skills that companies need.

The whole idea of work and training needs to be completely rethought as technology and automation are rewriting the rules for what work will be in the future. As companies send some of their existing developers to get trained as data scientists, they should offer education options to existing employees to learn to code. If there is high demand then decisions will have to be made whether its a meritocracy or maybe a random raffle.

5. Identify small use cases in compliance to leverage AI

Another thing that the COIC can help drive is to find real pain points for operations and compliance. What are some potential use cases for AI? One could be to hyper-segment, or cluster, groups of customers together based on many data attributes using UML for fraud, money laundering, or other reasons. Another pain point is false positive alerts in TMS, which could potentially be used with new technology. Also, false negatives could increase an institution's coverage by identifying instances that may be getting missed by existing algorithms.

6. Research AI vendors to help with small use cases

Since the AI vendor market is still growing, institutions can take advantage of this, by becoming early adopters and requesting specific functionality that some vendors may be willing to accommodate to get some POCs going.

7. Refocus existing compliance staff and train them on model validation, quality assurance, and data governance

As mentioned in the first point, technology and automation are likely displace millions of jobs, so institutions should do what they can to retain their existing employees. There would be a natural migration of investigators or client onboarding staff moving into quality assurance, model validation and data governance because they know what the process looks like from the inside. Obviously, they would need to learn some new concepts, but this goes back to a key idea of what the institutions want to define as learning, knowledge, and work.

If, there are enterprise standards established, and there should be, for core activities such as model validation then its reasonable to think that people can be trained to do this work. Furthermore, data governance is thought of as an activity for the IT department to deal with. This idea needs to change, and the tools need to be given to the business lines to manage the meaning of their own data. This is the whole point of effective challenge in model risk management.

There have been compliance failures that simply stem from the disconnect between compliance and technology and since compliance had no transparency into the black box, it allowed the problem to fester which exacerbated the consequences of when it was found. Allowing compliance to have some access to big data platforms, and the data's metadata or meaning will allow compliance executives to conduct a better effective challenge and protect themselves from professional liability.

8. Evaluate goals and progress on, at least, a quarterly basis and produce yearly report of activities and findings

The COIC should clearly define its objectives and timeline, and report on this regularly. But innovation implies that things may not always work the first time, so expectations need to get set in a way that values learning and progress as opposed to quantifiable economic results in the short-term. Also, the word 'failure' may need to be removed from an organization's vernacular for another type of phrase. So, when reporting about AI projects to the board, it shouldn't be said that our AI project failed, but something more to the effect of our hypothesis was incorrect and here is what we learned.

Board of directors will want to see quantifiable results so there could be metrics created to measure intangible assets such as AI knowledge within the firm. One way that regulators measure an institution's AML knowledge was to count the number of people it had on staff with anti-money laundering certifications. Similarly, the number of PhDs, individuals that went through AI fellowships, and number of failed and successful AI projects could all be potential inputs to help quantify an institution's intangible asset of AI knowledge.

Conclusion

If, we can accept the assertions made about CAS then we can conclude that the future of due diligence is unknown, but we can model some of its potential futures and guess where it could be going. However, what's more interesting is that if we buy into the idea of CAS then it suggests that all of the entities which make up the system including legislators, regulators, executives, employees, consultants, institutions, software firms, non-profit entities, and others in the supply chain can help shape its future by taking action and allowing the system to evolve to a better and more sustainable future.

Criminal networks are adapting rapidly in many ways such as with the use of drones to smuggle drugs or leveraging dark markets to sell stolen data. Also, the heightened risks associated with asymmetric terrorism and cyberwarfare suggest that institutions should double down on technological innovation, as Estonia did, quite impressively.

Regulatory expectations continue to evolve in scope, and some are disruptive and pose real strategic risks, such as PSD 2, to firms that don't go all in with its digital transformation initiatives.

The general trend is that, as AI matures in its ability to process massive amounts of data and is used for scenarios such as biometric identification, human readable report generation, more accurate risk classification, and other advanced NLP sentiment analysis then alternative data sources will continue to expand the scope of compliance screening programs, including entity due diligence. It will not be enough to simply trust what your customer tells you and to check what's available online in a limited number of data sources, as the physical world will come into play with the rise of alternative data such as networks of nano satellites that leverage synthetic-aperture radar technology.

Innovation is a key element that governments and legislators need to support, so the institutions which need to stay in compliance with rules and laws can be given some leeway to experiment. This doesn't mean that regulators shouldn't hold institutions accountability for governance failures, but the only way to push the industry forward and truly manage risk is to evolve and try new ways of doing things. However, even if an institution operates in a jurisdiction that doesn't offer regulatory sandboxes with safe harbour protections, it shouldn't stop the experimentation, which could happen in the background.

The most successful organizations of the future will be the ones that can manage and accelerate their perpetual transformation from one state to another seamlessly. The leading companies of the future will manage change, as if they are flying in an airplane that never lands and refuels in mid-air and when the transformation of the organization to its next state does occur everyone skydives out of the old plane, at different intervals, into the new plane that's also moving in mid-air. It's the organizations that land their plane to refuel and move people safely on the ground from one plane to another that will fall behind in the innovation game.

Institutions also need to seriously think about their human resource policies and use greater efficiencies and reduced costs as an opportunity to improve the quality of lives of their employees and to improve staff retention. Technological innovation will transform how organizations function, and similar education and training can transform what functions people can perform. So, education and training need to take a front row in the companies of the future and it can't be limited to an upper limit tax deductible reimbursement for getting a good grade in a graduate level course. Education needs to become a core part of the organization's long-term strategy and hiring too much talent outside of the firm could lead to a dilution of the firm's collective business knowledge and historical progression including challenges, successes, and failures.

In terms of the place of people in the future of entity due diligence, it should be acknowledged that logical reasoning and human intuition are still the crown jewels of the decision making and investigative process. The advances in technology, automation, and AI are all powerful tools which should be handled with care. This is why governance and oversight need to be implemented to continually assess the impacts of technological innovation on the workforce which should enhance an individual to make a better, more informative, and accurate decisions faster as opposed to marginalizing a person's logical reasoning and intuition. As with all power comes responsibility, and technological innovation discussed throughout this paper has great power to transform the future of entity due diligence for the better, if handled with care, and maybe, even make the world a little safer.