ESSEC
BUSINESS SCHOOL

Cyber and Financial service industries

Public regulation and business cyber compliance to improve resilience towards blockchains disruptor risks

Camille Madec – Msc in Management
June 2016

Introduction

In order to stay competitive, financial industry must seize the opportunities of the on-going technological disruption, and particularly with the recent so-called blockchain innovation when some argue that this new technology has the potential to replace banks as financial intermediaries for transfer and exchanges of money. In this transitional context, financial sector could face new cyber-security risks, with sophisticated attacks, which eventually call for a renewed regulation framework. Here the financial sector means banks, insurers, asset managers, and advisory firms.

Blockchain can be defined as *"a peer-to-peer operated public digital ledger that records all transactions executed for a particular asset (…) "The Blockchain maintains this record across a network of computers, and anyone on the network can access the ledger. Blockchain is 'decentralised' meaning people on the network maintain the ledger, requiring no central or third party intermediary involvement." "Users known as 'miners' use specialised software to look for these time stamped 'blocks', verify their accuracy using a special algorithm, and add the block to the chain. The chain maintains chronological order for all blocks added because of these time-stamps."* [1]

Hence, Blockchain, well known through the so-called bit coin, could open much more perspective and should guaranty security and the validation of all the exchange of data.

In addition to open room for new business opportunities, this new technology could disrupt the legal conception of privacy, intellectual property right, and presents some issues regarding financial institution accountability given the new associated risks.

As a consequence while financial institutions have been under strengths by the new regulatory requirements in the aftermath of the 2008 financial crisis, they might see their accountability rises again to address cybersecurity risks and associated prejudices related to blockchain innovation.

Cyber security is a burning issue in the international agenda. The G7 made cyber-security a priority and have established the "G7 Principles and Actions on Cyber"[2]. This issue is also considered in Asia, for instance, a new Cyber-security Act will be tabled in the Singapore Parliament next year that will also "empower the Singapore Cyber Security Agency to manage cyber incidents and raise the standard of cybersecurity providers in Singapore."[3]

---

[1] Piper Alderman, « Blockchain –emerging legal issues », Lexology, Global, october 12 2015, http://www.lexology.com/library/detail.aspx?g=6e5a942e-94ea-4891-a07c-a9d96343dc95

[2] http://www.mofa.go.jp/files/000160279.pdf

[3] http://globalcompliancenews.com/new-cybersecurity-laws-in-the-works-20160601/?utm_source=wysija&utm_medium=email&utm_campaign=weeklynewsletter

More over, international regulators are particularly vigilant as regard technological innovations. On the one hand, regulators watch the use of consumer data made by financial institutions, as an example, EBA is currently consulting on that issue [4] in order to "identifies risks and benefits for consumers and financial institutions, as well as for financial integrity in general". Regulators such as the SFC[5] in Hong Kong, AMF in France and FCA in the UK, have established new Fin-tech contact points in order to work with financial institutions to address those issues. On the other hand, they started to fine financial institutions for misrepresentation of data security practices. For instance, the SEC has fined $1M Morgan Stanley[6] in order to "settle charges related to its failures to protect customer information, some of which was hacked and offered for sale online".

As a consequence, given the current development we cannot exclude the risk that financial institutions could eventually be fined in the future for eventual impact on customers given cyber security attacks related to blockchain.

This paper explains how business compliance to new cyber regulatory framework is a strategic issue for financial institutions. It presents the financial institutions specific data profile and linked eventual collateral damages. It highlights blockchain innovation opportunities and associated new cybercrime challenges. It describes the current European regulatory framework and legal accountability scenarios. It then finally supports the hypothesis of cyber compliance as a corporate competitive advantage and maps out some elements of potential recommendations to strengthen cybersecurity resilience.

This paper comes from my participation of the management course "Applied Cybersecurity Strategy for Managers". The course aimed to provide an understanding of information security challenges and overview of strategic best practices regarding governance and crisis management. Particularly, I have been able to understand the innovativeness of cybercriminals. I thank for the information and knowledge shared that particularly have inspired this work.

This paper has also grown out of my current experience as a compliance officer for BNP Paribas Global in the area of Clients Interest Protection that has stressed the strategic dimension of compliance for corporate world.

[4] http://www.eba.europa.eu/-/eba-seeks-views-on-the-use-of-consumer-data-by-financial-institutions
[5] http://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=16PR19
[6] http://www.sec.gov/news/pressrelease/2016-112.html

How Blockchain redefines cyber security: a brief overview

Examples of blockchain business opportunities

Blockchain is the technology many believe will be the key to the future of banking. The digitalisation of financial service opens room for new opportunity such as to propose new kind of consumer's experience as well as the use of new technologies and improve business data analysis.[7] The ACPR, the French banking and insurance regulatory authority, has recently classified the opportunities and risks linked to the Fintech[8] such as the new services for uses, better resilience versus the difficulty to establish effective supervision, the risks of regulation dumping and regarding clients interest protection such as data misuse and security. The French Central Bank is currently studying blockchain in cooperation with two start-ups, the "Labo Blockchain" and "Blockchain France".

In that context, blockchain is a true financial service disruption, according to Piper Alderman "Blockchain can perform the intermediating function in a cheaper and more secure way, and disrupt the role of Banks."[9] According to the lawyer Alain Bensoussan[10], blockchain allows decentralization, anonymity as well as security, traceability and reduces costs. In a nutshell, Blockchain allows faster and more effective transaction, as well as it reduces transaction costs.

Hence, leading bank wants to seize that financial service opportunity. They are currently working on blockchain project with financial innovation firm, R3 CEV. The objective is that the project delivers a "more efficient and cost-effective international settlement network and possibly eliminate the need to rely on central bank"[11]. R3 CEV has announced that 40 peer banks, including HSBC, Citigroup, and BNP Paribas, started an initiative to test new kind of transaction through blockchain. This consortium is the most important ever organized to test this new technology.

Another example of blockchain's smart output is the so-called "smart contract" this innovation would allow automatic execution for standardized contracts such as loans or corporate issuance of bonds, without central compensation. Notably, blockchain is opening a new wave of innovation for Legaltech. Other major areas for applying blockchain technology include: smart assets, clearing and settlement, payments, digital identity.

---

[7] Frédéric Visnovsky, Secrétaire général adjoint ACPR, « Les banques face à trois défits », Mai 2016 (p.13).
[8] Idem
[9] Piper Alderman, « Blockchain –emerging legal issues », Lexology, Global, october 12 2015, http://www.lexology.com/library/detail.aspx?g=6e5a942e-94ea-4891-a07c-a9d96343dc95
[10] Olivier Hielle, La technologie Blockchain : une révolution aux nombreux problèmes juridiques, Dalloz actualité (31 mai 2016).
[11] [11] Piper Alderman, « Blockchain –emerging legal issues », Lexology, Global, october 12 2015, http://www.lexology.com/library/detail.aspx?g=6e5a942e-94ea-4891-a07c-a9d96343dc95

Another example is the new cryptographic decentralized money, Elthereum, is the second cryptographic money after Bitcoin. It is evaluated at 688 millions of dollars today.

According to FTI consulting [12] recent study "UK banking and investment institutions are most knowledgeable about bitcoin technology blochain", the study, which targeted 772 respondents in the banking and investment sector from the UK, Germany, South Africa, Australia, Hong Kong, Singapore and the US, found almost two-thirds of respondents were aware of blockchain technology and a quarter is knowledgeable about it.

Blockchain and cyber security risks

There is no consensus about whether blockchain could increase cyber security risks. The degree of security of the network could possibly determine the "the speed and extent of acceptance of blockchain technology within the global financial services community."[13]

In March 2015, Interpol conducted a research[14] to identify new cyber threats unleashed by blockchain. According to the experts *"the design of the blockchain means there is the possibility of malware being injected and permanently hosted with no methods currently available to wipe this data. This could affect 'cyber hygiene' as well as the sharing of child sexual abuse images where the blockchain could become a safe haven for hosting such data."* Further, according to the research, *"it could also enable crime scenarios in the future such as the deployment of modular malware, a reshaping of the distribution of zero-day attacks, as well as the creation of illegal underground marketplaces dealing in private keys which would allow access to this data."* Has a conclusion, INTERPOL communicated about its challenge to *"spread awareness amongst the public and law enforcement"*.

The issue of cyber-security for financial institutions is very strategic. Firstly, as these institutions rely on customer confidence they are particularly vulnerable to data loss and fraud. Secondly, banks represent a key sector for national security. Thirdly they are exposed to credit crisis given their role to finance economy. Lastly, data protection is a key challenge given financial security legal requirements.

[12] City Am – Article 07/03/2016
[13] Hunton & Williams "Blockchain, cybersecurity and global finance" https://www.hunton.com/files/News/289469d8-826a-4f2b-ae48-df04b4c0acae/Presentation/NewsAttachment/3abe4d02-0d61-4276-9831-ea3ce3f225f9/blockchain-cybersecurity-and-global-finance.pdf
[14] « INTERPOL cybe research identifies malware threat to virtual currencies » 26 march 2015 http://www.interpol.int/News-and-media/News/2015/N2015-033

Fraud is the majority of cyber incident in Financial sector today (extortion, identity theft and other kind of crimes targeting individual customers or employees[15]. However, firms are exposed to larger risks such as data theft, system disruption and damage.

System failure is an incident affecting lot of financial institutions aiming at unleashing a failure of the payments system or a failure of the national infrastructure upon which rely the financial sector. This can of scenario would be very costly, for instance, the IFM has estimated the planned shutdown of the Greek economy to represents 7% of Greek GDP[16]

Further more, the risks are very high given that cyber crime motivation varies a lot (spying, terrorism, hacktivism, enrichment). In case or cyber attacks, financial institutions face specific risks such as: operational, reputation, criminal litigation, fines from regulators, eventual client losses and financial losses.

Therefore, financial institutions Corporate Security Department have to foresee new cyber risk that could threaten their firms in case of blockchain development. This is even more essential as the regulatory and legal framework addressing blockchain is under development and not established so far. Hence, financial institutions cannot anticipate what would exactly be their degree of accountability in case of cyber attacks related to blockchain.

Blockchain regulatory framework and legal challenges

Cyber security and New Technology European legal framework

In Europe, there is already a legal framework aimed to address cyber-security risks. The European directive for network and information security has implemented a cyber-security strategy for member states with the legal obligation to adopt a security strategy and create a national authority in charge of those issues with sufficient resources. Particularly, this authority should be notified for every security incident.

Further, as cyber-security attacks are a threat for personal data, we can also mention existing European regulation on personal data. The protection of personal data and the respect of private life, are fundamental rights under European law under article 7 and 8 of the European Union Fundamental Rights Charter (articles 7 and 8). There is a specific European regulatory authority for personal data protection, and every Member States has established a national

[15] « Cyber and the City, Making the UK financial and professional services sector more resilient to cyber attack » May 2016. TheCityUK, Marsh.
[16] Idem

regulator in charge of those issues. These legal requirements were also supposed to increase consumers' trust in online services.

Fintech, that integrated the market through online payment service, have been regulated with the directive related to payment service (DSP 2) defining new rules to protect consumers while implementing a biding legal framework.

The general trend is that those legal obligations tend to increase legal requirement and strengthen sanctions. What is more, personal accountability for managers tends to be increased.

As cryptographic signatures in electronic documents made necessary a worldwide wave of legal reform, blockchain challenges current legal framework. It is possible that existing legal frameworks are insufficient, and that new regulations would need to be developed.

Blockchain governance and regulation challenges

While Fintech had integrated the payment market through online payment with a specific European legislation, the is now legal recognition of virtual money and no specific reglementation dedicated to blockchain given the few application of this technology today. As we focus on cyber security attacks we will not pursue a deep dive in legal issues regarding smart contracts, intellectual property right but rather privacy and decentralized organization accountability [17].

On the one hand, blockchain innovation presents legal issues that will need to be addressed in order to establish who is responsible in case of cyber risks hypothesis particularly because "management" is conducted automatically with blockchain. On the other hand, as Blockchain is not yet a mainstream technology, the regulation needs to be balanced in order to foster innovation.

According to Pascal Bouvier, "the legal framework is incompatible with a technology where unknown actors would settle transactions, where the transaction settled would represent a security exogenous to the technology and where the technology could not deliver 100% of ownership"[18].

The recognition of this new technology is very new. For instance, in France, the new article L. 223-22 of the financial and monetary code seems to legalize in a specific area the use of "dispositif d'enregistrement électronique partagé" a direct reference to Blockchain according to Alain Besoussan. The French Parliament had also organized a conference about the subject last spring, which stresses that the subject made its entrance in the political agenda.

---

[17] Piper Alderman, « Blockchain –emerging legal issues », Lexology, Global, october 12 2015, http://www.lexology.com/library/detail.aspx?g=6e5a942e-94ea-4891-a07c-a9d96343dc95

[18] Pascal Bouvier, "Distributed Ledgers Part II: Clearing, Settlements & Legal frameworks" 10 août 2015 : https://www.linkedin.com/pulse/distributed-ledgers-part-ii-clearing-settlements-pascal-bouvier-cfa?trk=mp-reader-card

Existing regulatory frameworks will also need to evolve to address issues of taxation, national security, and money laundering since Blockchain can seamlessly facilitate cross-border transfers. Hence, another difficulty will be related to the international dimension of blockchain that makes hard to implement a national regulation. As an example, after the signature of the Judicial Redress Act by Obama Administration, the signature of the agreement between the European Union and the United States has been a result of a very long negotiation process in order to address the issue of data sovereignty.

As regard cyber security risks, on of the core legal challenge will be the accountability issue. As Blockchain is grounded on anonymity the question is who would be accountable for the actions pursued? Should it be the users, the Blockchain owner, or software engineer?
Regulation will address the issue of blockchain governance. According to Hubert de Vauplane[19], "the more the Blockchain is open and public, less the Blockchain is governed", "while in a private Blockchain, the governance is managed by the institution" as regard" access conditions, working, secyrity and legal approval of transactions". Where as in the public Blockchain, there is no other rules that Blockchain, or in other words "Code is Law" to quote US legal expert Lawrence Lessing. First issue: who is the block chain user? Two situations must be addressed depending if the Blockchain is private or public. Unlike public blockchain, the private blockchain - even though grounded in a public source code - is protected by intellectual property rights in favour of the organism that manages it, but still exposed to cyber security risks.

Moreover, a new contractual documentation provided by financial institutions and disclosure duty could be necessary when consumers may simply not understand the information on how their data may be used through this new technology.

Lastly, even though government claims to give priority to the offensive against cyber criminals, with for example in the UK the recent creation of the National Cyber Security Centre; regulators will probably face difficulties to implement those sanctions. Indeed, it is very hard to identify the author of such intrusion and to establish enough proof. Further more, it will be hard to quantify the prejudice and to make an exact assessment of reputational damages and information losses. Therefore, financial institution will probably be accountable towards customers as regard eventual cyber security failures.

However, in addition to regulation fining power, financial institutions must take into account that in common law country, and specifically in the US the class action represents a high risk to take into consideration. Indeed, Cyber security issues could be a new area of claim in the future years.

[19] Hubert de Vauplane, la Blockchain et la loi, Alternatives économiques (14 février 2016) http://alternatives-economiques.fr/blogs/vauplane/

How financial industry can step forward on the issue: compliance to strengthen cyber resilience

Cyber resilience as a competitive advantage

The introduction of Blockchain innovations in Financial institutions business model makes necessary to redefine the problem of cyber security in those groups, as the threats could be different or new. Indeed, with blockchain new information technology systems failures could appear.

Even though blockchain legal framework is not yet established neither at the international or European level, financial institutions could anticipate compliance challenges in order to strengthen blockchain cyber resilience. A dedicated cyber security road map could be a competitive advantage for firms that aim to integrate blockchain innovations in their business models by creating high entry barriers with high security standards.

During 10 May 2016 City Week Conference, Will Brandon Chief Information Security Officer of the Bank of England had stressed some of key priorities regarding cyber security plan such as "culture training", "leadership from the top (and not just from the IT department)", to conclude "that will mean, among other things, clear policies and standards, good management information, and a sensible approach to compliance".

Cyber compliance road map

Freshfields Partner Klaus Beucher, who advises multinationals on cyber security issues, says there is a set of steps that companies must take to protect themselves with:

- Risk assessment: map the data, look at technical infrastructure, to look at everything from IP protection to the obligation under data privacy and employment law
- Ensure you have effective data governance policies in place
- Draw up a crisis plan and practise it
- Finally, all should be done in partnership with the board in order to determine who is accountable for data security

In My 2016, TheCityUK made a study "Cyber and the City" with recommendation to improve financial sector cyber attack resilience[20]. According to John McFarlane, Barclays Chairman, a "systemic risk" is upon financial institutions as cyber crime is a real danger.Among the key recommendations of the "board cyber check-list" were :

- *"The main cyber thrats he firm have been identified and sized*
- *"There is an action plan to improve defence and response to these threats"*
- *"Data assets are mapped and actions to secure them are clear"*
- *"Supplier, customer, employee and infrastructure cyber risks are being managed"*
- *"The plan includes independent testing against a recognised framework"*
- *"The risk appetite statement provides control of cyber concentration risk"*
- *"Insurance has been tested for its cyber coverage and counter-party risk"*
- *"Preparations have been made to respond to a successful attack"*
- *"Cyber insights are being shared and gained from peers"*
- *"Regular Board review material is provided to confirm status on the above"*

Hence, the methodolgy to strengthen compliance and cyber resilience seems to be well established and consensual. However, even if firms are aware of the cyber threat, actions against it are still in progress. Hence the so colled blockchain business revolution for Financial Institution will need to be developed through compliance framework in order to broaden and redefine actions to avoid new cyber security risks.

[20] « Cyber and the City, Making the UK financial and professional services sector more resilient to cyber attack » May 2016. TheCityUK, Marsh.