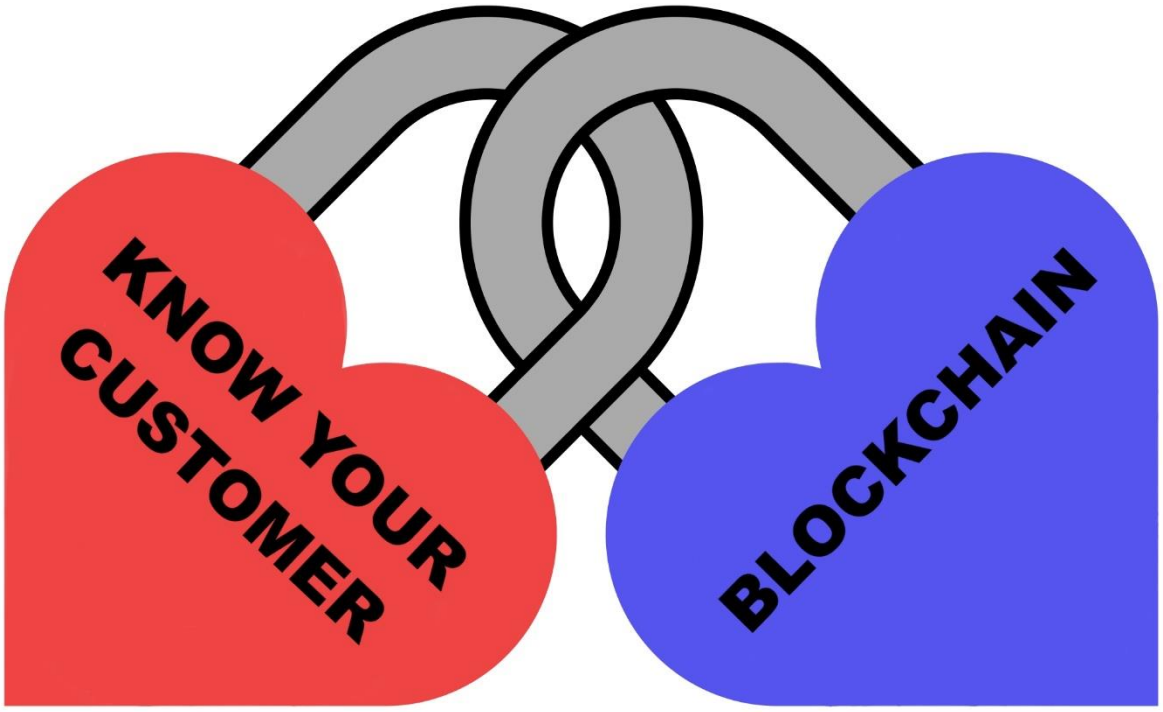

Could this be the perfect marriage?

ACTENSA GROUP

YOUR TRANSFORMATION PARTNER

24/01/2018

Table of Contents

Introduction

Know Your Customer and Blockchain, could this be the perfect marriage? The first date in Singapore is over, was that the first step towards a perfect marriage or like so many business and technology partnerships, will this relationship end in unfulfilled promises and broken dreams?

In this article I will assess the compatibility of KYC and Blockchain to determine whether Blockchain or a similar technology has the potential to digitally transform the way KYC is performed by banks and financial institutions. I will begin with an overview of the 'state of play' play for both KYC and Blockchain including key factors for consideration. Once this baseline is established I will look at how these factors create business challenges for organisations that are required to perform KYC.

To support the assessment of compatibility between KYC and Blockchain, a hypothetical KYC 'platform' underpinned by Blockchain will be outlined based on current industry research and development efforts in this domain. To assess the compatibility of KYC and Blockchain the hypothetical KYC Platform will be evaluated against 3 key tenets of Digital Transformation to determine whether fulfils these requirements. Finally, I'll outline how the theoretical KYC platform would address the identified business challenges and offer my closing thoughts on the future of KYC and Blockchain.

Key Concepts and Terminology

Know Your Customer

For the purposes of this article I will define KYC in a broad sense as a set of regulations, guidelines, policies, and processes that aim to prevent banks and financial institutions from being used, intentionally or unintentionally, by criminal or terrorist organisations. KYC enables banks and financial institutions to better understand their customers and their associated financial dealings.

KYC currently has a high level of focus globally within the banking and finance sector and has increased in both breadth and depth throughout its history. The current regulatory framework is complicated and made up of a combination of country and regional specific measures such as Dodd-Frank Act, FATCA, and MiFID II.

Meeting the regulatory requirements is difficult, particularly for regional or global organisations. While several new regulations such as FinCEN and the 5th EU Money Laundering Directive are about to come into force, many organisations are struggling to comply with previous regulations that are more than a decade old [1].

Estimates vary on the cost of KYC compliance vary but Thomson Reuters estimates "financial firms' average costs to meet their obligations are $60 million, some are spending up to $500 million on compliance with KYC and Customer Due Diligence (CDD)" [2]. It is also estimated that the global spending on AML (a subset of KYC) compliance alone amounted to $10 billion in 2014 [3].

A significant additional factor is the cost of noncompliance. For example, in 2015 two Nordic banks were fined for non-compliance. At the time, the largest fine possible, 5.7 million USD, was issued to one of the banks, Nordea. Changes to Swedish financial regulations mean a similar infringement today could cost an organisation up to 10% of their revenue or possibly their operating license [4]. Ability to achieve and maintain compliance is not just a challenge locally in the Nordics, globally financial organisations are struggling to stay compliant with KYC regulations for several reasons including understanding or interpretation of the regulations, technology requirements and sourcing qualified human resources.

At a technology or systems layer the existing approach to KYC is heavily fragmented and siloed. Many of the solutions available today are proprietary with limited integration between different KYC systems and an organisations internal systems. Whilst there are centralised repositories such as SWIFT and KYC.com these still hold individual organisations customer data in propriety systems with limited sharing between them. As there are no consolidated registries of customers, each bank or financial institution is performing their KYC process individually for each one of their customers. As an example, a business with accounts across three different banks will need to provide essentially the same information three times to complete KYC process for each bank. Once the process is complete, that KYC data may need to be stored and updated in three disparate systems. Adding to the problem is the fact that most organisations are struggling to achieve greater levels of automation that would ease human resource dependencies.

From the example above, it is logical to derive that the current approach to KYC is not particularly customer friendly, some reports suggest the KYC process can delay onboarding customers as it can take 30 to 50 days to complete to a satisfactory level [3]. Another survey of corporate customers found that 89 percent had not had a good KYC experience, and 13 percent had changed their financial institution relationship as a result [2].

Blockchain

It is important to clearly distinguish between Blockchain and Bitcoin:

- **Blockchain** a form of Distributed Ledger Technology (DLT**).**
- **Bitcoin** is a type of digital or crypto currency.

Bitcoin utilises Blockchain as a ledger for transactions however Blockchain exists as a separate, standalone technology that can be applied to a variety of business cases. For the purposes of this article I am referring only to Blockchain, not Bitcoin.

Also, it is important to note that whilst Blockchain is currently the most prominent implementation of DLT in the media, it is not the only form of DLT currently being used. However, it has become synonymous with DLT in a similar way to ‘Hoover’ and vacuum cleaners or Swish and mobile payments. In this article I will use Blockchain as the primary example of an appropriate DLT.

Blockchain, is it real or is it hype? There are enough industry experts and commentators who agree that blockchain will be a transformational technology that I believe the most relevant question is not if but when will Blockchain’s use become mainstream, in the way other technologies such as cloud computing and smartphones have already become. Respected research company Gartner currently places Blockchain towards the end of the ‘peak of inflated expectations’ in their hype cycle, see Figure 1 below, and estimates that it will reach the plateau of productivity (mainstream adoption) in 5 to 10 years [5].

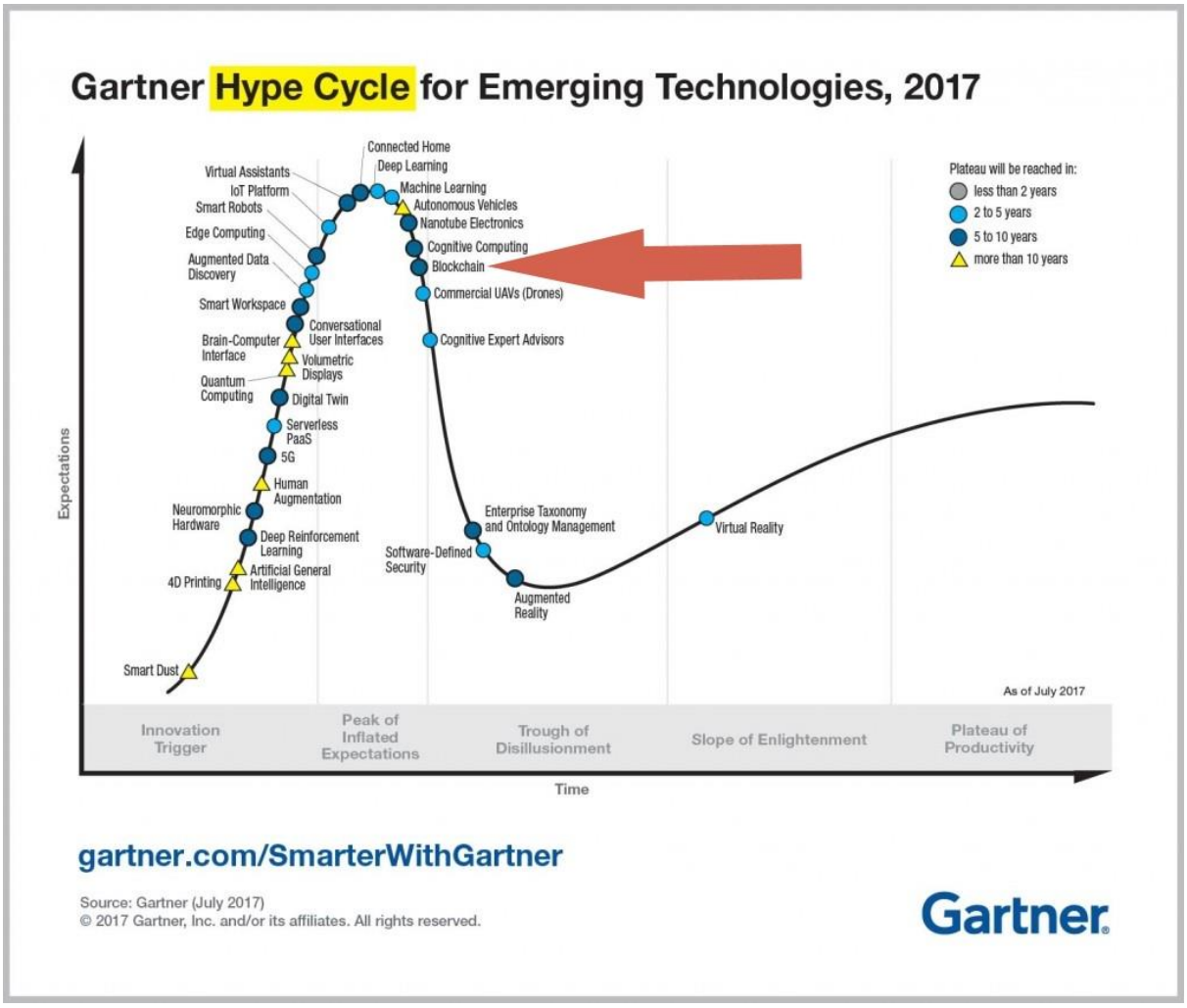

Figure 1 - Gartner's hype cycle of emerging technologies [5]

To clarify mainstream adoption a little further, the innovation diffusion curve will be used to define the beginning of mainstream adoption as the junction between the end of adoption by the 'Early Majority' and beginning of adoption by the 'Late Majority', or 50% market share, see Figure 2.

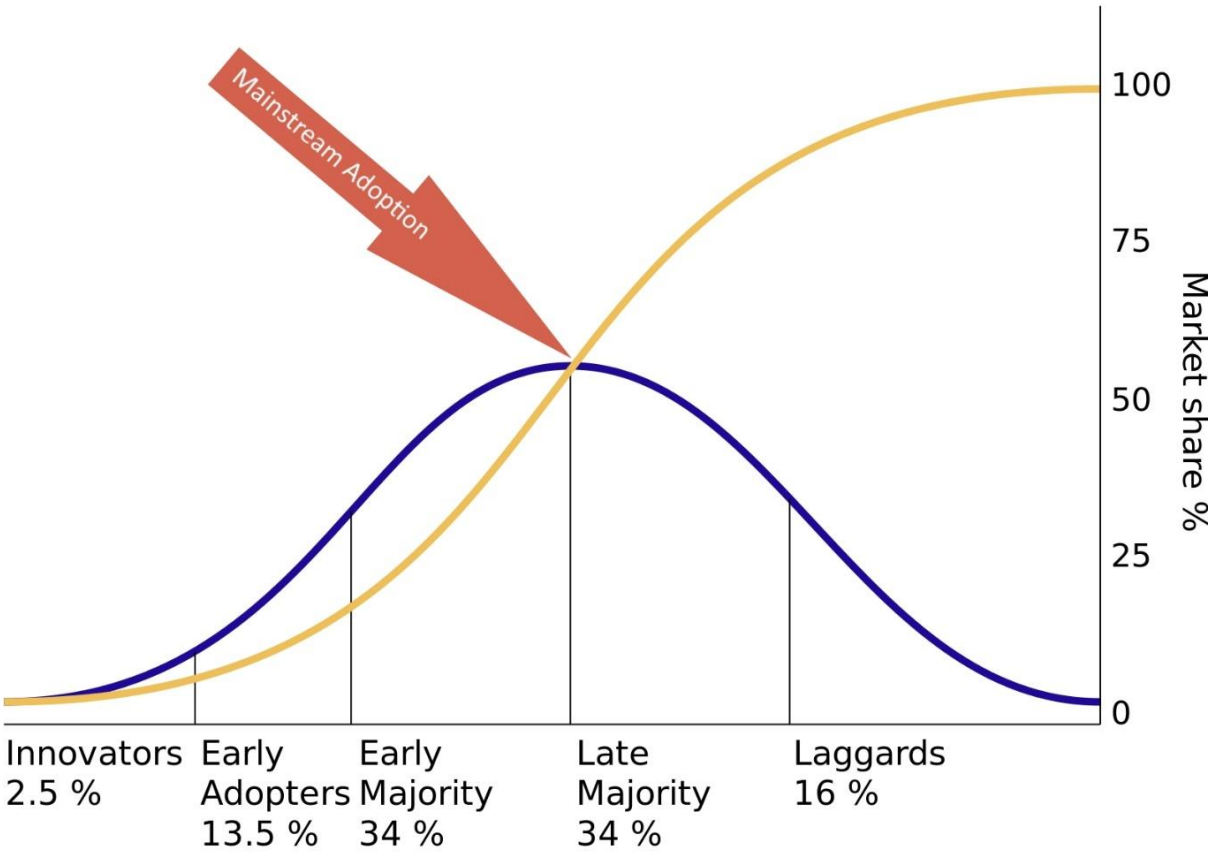

Figure 2 - Diffusion Curve

Will blockchain take 5-10 years to achieve mainstream adoption? Personally, I think it will be closer to 5 years than 10 years. There is a definite trend that shows technologies are achieving mainstream adoption faster today than ever before [6]. There are also a number of accelerators that are relevant to blockchain which will drive adoption.

- The network effect - blockchain's benefits will increase exponentially as more people use the technology as a common framework for different business cases.
- Cybercrime - future security breaches of centralised data repositories housing customer information resulting in financial penalties and/or reputational damage.
- Globalisation - although perhaps slowing in the current political climate, the drive towards globalisation and initiatives such as the United Nations 2030 Sustainable Development Goal of providing legal identity for everyone on the planet.

As the benefits Blockchain increase exponentially so too will adoption, resulting in a compression of the time axis in the innovation diffusion curve and ultimately faster mainstream adoption

Whilst there are many KYC solutions already utilising Blockchain, many of them follow the current siloed and propriety approach to KYC and therefore may only offer incremental gains in the future. What I believe to be the most interesting development of KYC and Blockchain at present is the recent completion of a Proof of Concept(POC) for a Banking KYC Shared-Services Utility in Singapore underpinned by Blockchain [7]. I will explore this model in detail later in the article but further detail on the Singapore POC can be found here and here.

Supporting Frameworks and Concepts

- Banks and Financial Institutions – this term will be used to cover traditional banks and financial institutions but will also include any other type of organisations whose operations are subject to KYC.
- Distributed Ledger Technology (DLT) – "In its simplest form, a distributed ledger is a database held and updated independently by each participant (or node) in a large network. The distribution is unique: records are not communicated to various nodes by a central authority but are instead independently constructed and held by every node. That is, every single node on the network processes every transaction, coming to its own conclusions and then voting on those conclusions to make certain the majority agree with the conclusions. "[8].
- Technological Debt – Higher levels of technological debt increase the cost of maintaining technology systems and reduce the performance and agility of business processes that rely on those technologies. All organisations carry a level of technological debt, the challenge is to minimise the amount of debt. Technical debt is generally increased through the result of either successful implementation of sub-optimal technology solutions or sub-optimal implementation of good technology systems.
- Value chain – is a set of activities that an organisation operating in a specific industry performs to deliver a valuable product or service to the market.

Figure 3 - Generic Value Chain

- Porter's Five Forces - is a model named after Michael Porter that identifies and analyses the five key forces that influence rivalry or competition within an industry.

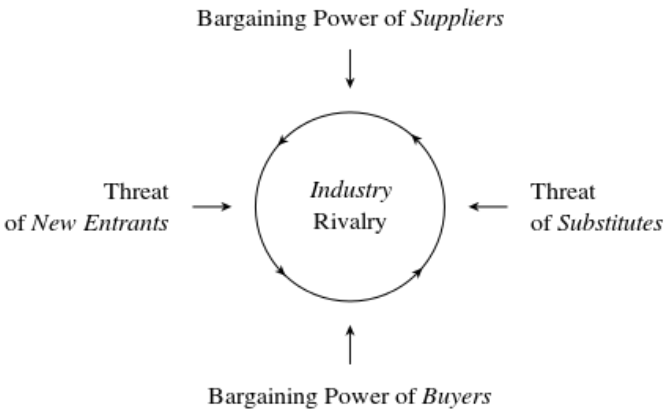

Figure 4 - Porter's Five Forces

Business Challenges

To understand the business impact the current challenges with KYC are providing I have grouped them into four distinct areas:

- **Increased operating costs,** related to compliance with KYC regulatory requirements. As an example, many organisations are having to recruit more staff to manage and achieve compliance, in addition technology infrastructure and software costs for associated systems must also be considered. With the current trend of increasing KYC regulation [8] there is no sign of relief soon. Factoring in the additional cost of noncompliance creates the risk that KYC costs could prove terminal to some banks and financial institutions in a market that is facing intense competition from new entrants such as innovative fintech's and lower barriers to entry through open banking initiatives and globalisation.
- **Reputational damage,** from public regulatory breaches. Two prominent Nordic banks that were fined by the Financial Supervisory Authority (FSA) in 2015 experienced share price decreases as a direct result. In another example all four major Swedish banks were associated with a Russian Money Laundering case earlier this year impacting their reputation.
- **Poor customer experience,** leading to loss of customers. Large established banks have traditionally managed to retain customers due to high switching costs and high barriers to entry for competitors. Open banking initiatives currently in varying levels of implementation throughout the world, will make it easier for customers to switch banks and lower the barriers to entry for new competitors. Within these changing market dynamics, customer retention through a high-quality customer experience will be critical to remain competitive.
- **Increased Technological Debt,** due to the current fragmented approach to many KYC technology solutions and lack of integration. Many banks and financial institutions agility is restricted by their ability to perform KYC for customers in a timely manner.

KYC and Blockchain

What would a perfect union of KYC and Blockchain look like and would such a marriage have the capability to solve some or all the challenges associated with KYC?

Setting the scene

One utopian view of KYC involves a single global distributed ledger that contains a single digital record for every person or business entity in the world. The digital record would contain all relevant data (or attributes) associated with the entity and the ledger would contain an immutable history of the entity's financial transactions. The owner of the record, including data and transactions associated with it, would be the person or business entity, not the platform owner or operator. Authorised parties such as government departments and for this example, authorised banks and financial institutions, would be able to add/update/remove data to a record only with the entity's explicit permission. The model would contain a trust system that facilitated sharing of data between:

- Government departments and person or businesses entities.
- Persons or businesses entities and authorised parties.
- Government departments and authorised parties.
- Multiple authorised parties.

The trust model in combination with the data and transaction integrity provided by Blockchain would allow the KYC process to be greatly simplified. Each record would be built up over time using an additive process for data and transactions, begun at birth (for a person) or start-up (for a business) and continuing uninterrupted until close. New data would be added to the record once and shared as few or many times as required. Integration with government systems of record would be key to establishing the baseline record, including data such as birthdate, personnummer or social security number, company number, address and tax details. To access products and services from another authorised party the person or business entity would only need to perform a check box type activity to share the required data and transactions with the new authorised party rather than having to supply the full set of data and transactions over and ever again for each new product or service request. In certain situations, a person or business entity may need to add additional required data to their record and share accordingly. The model would be usable across a wide range of business cases including but not limited to KYC and could even provide a foundation for the United Nations 2030 Sustainable Development Goal of providing legal identity for everyone on the planet.

The more realistic goal is a version of above in which, a country or region implements their own distributed ledger technology platform that contains records for every person or business entity within that region or country. This is a similar model that a consortium of banks and technology providers, led by the Singaporean government, have just completed a POC for. Ideally each region or country would apply an open source approach to development of their platform and adhere to a set of global standards that allowed interoperability and portability of records between regions and countries without compromising security and operability even if the platform was built on different underlying blockchain technologies. For the remainder of the article I will refer to such a platform as 'Know Your Customer Blockchain' (KYCBC) [9] [10] [11].

From a technology systems and process perspective the move to a single KYCBC platform which reduces the number of times KYC is performed for each customer should yield significant cost benefits from today's approach of operating and maintaining multiple fragmented KYC systems and processes. The KYCBC would become a shared services platform for banks and financial institutions at a regional or country level. While it is hard to predict a cost model at this stage, the reduction in duplication of technology systems and redundant process in combination with integration improvements and economies of scale, should yield considerable efficiency gains.

The question now becomes could a marriage of KYC and Blockchain in the form of a KYCBC platform, digitally transform KYC from a support activity to a primary activity in the value chain for banks and financial institutions?

To help answer this question we must first define Digital Transformation, as the term has become generalised and misused in many instances. For this article I will use the following definition to provide the required focus.

“every successful digital transformation has the following three elements:

1. A new customer experience.
2. A new business model.
3. A new value creation model.” [12]

To determine the feasibility of the KYCBC platform to digitally transform KYC, I will evaluate it against the three elements defined above.

A New Customer Experience

To evaluate this element, I will define a scenario as follows. In this scenario it is assumed that each customer (person or business) has a single record for which they are authoritative, as per the previous explanation of the KYCBC. It is also assumed that they can easily add or remove data to their record themselves through an intuitive interface such as a smartphone or desktop application.

Scenario, a customer is opening their first bank account and the bank they have chosen (Bank 1) has asked them to provide supporting data with their application to meet the bank’s KYC requirements. The customer provides the required information by first adding any missing data to their personal record through the application, either by entering an ID or Customer Number directly, for institutions and organisations integrated into the KYCBC platform already. For non-integrated systems the customer could attach electronic documents or photograph\scan physical supporting documents into the application. The customer would then provide Bank 1 with authorisation to access the requested data. Once authorised, Bank 1 would perform its own validation of the data in line with its KYC requirements and stamp their approval on the person’s record. If at a later stage the customer applied for a loan or bank account with another bank (Bank 2), assuming both banks were part of the trust model, Bank 2 could use the KYC approval from Bank 1 as explicit KYC approval for their KYC requirements, if Bank 2 required additional data from the customer they could submit a request only for the additional data and once this was supplied and validated, add their respective KYC stamp of approval for the new data to the customers personal record. This scenario can be extrapolated further for different types of banks or financial institutions and various products or services.

If the KYCBC platform were able to support this scenario then it would qualify as a new customer experience. The POC in Singapore also achieved a new customer experience with the time required to open a bank account online reduced by as much as 80% using a platform similar in principle to the proposed KYCBC [13].

A New Business Model

Utilising the scenario outlined above, potential for a new business model has also been created. In the current environment all banks and financial institutions are responsible for meeting KYC regulations individually, either by performing KYC activities themselves or where relationships with other banks exist, accepting the other banks KYC assessment. Regardless of whether the bank

performs the KYC process itself or 'trusts' another bank to perform the KYC process, each bank retains full responsibility and hence risk for their own customers within their applicable KYC compliance framework.

Expanding on the scenario above, what if Bank 1 had the opportunity to share their KYC stamp of approval for use by Bank 2 and other banks or financial institutions? A new business model could be created whereby banks were able generate revenue by licensing their KYC stamp of approval to other banks and financial institutions. Expanding further, for Bank 2 performing KYC, assuming a form of market equilibrium is achieved, they could pay less for the KYC 'license' from Bank 1 than if they were to perform the KYC process themselves. The additional benefit for the Bank 2 is that Bank 1, through the licensing activity, would retain full responsibility for KYC compliance, thus reducing Bank 2's risk exposure.

This new business model could even result in new entrants to the market that existed only to perform KYC activities and then license their approval stamps to the banks and financial institutions, not actually providing any financial products or services themselves. This would allow banks the option to fully outsource the KYC process and focus on their core business if they chose to.

A New Value Creation Model

There are two ways in which the KYCBC platform could facilitate a new value creation model;

Banks and financial institutions could use the revenue generated through selling 'licenses' for KYC approval to offset the cost of performing KYC. The resultant savings could be invested into research and development of new or optimisation of existing, products and services. Alternatively, the resultant savings could be reinvested into further optimisation of KYC to reduce financial penalties and reputational damage associated with regulatory failings or breaches. Both these options would create new shareholder value.

Comparing the current customer experience to the new customer experience, a new value creation model can be seen whereby the customer is empowered with ownership and authorisation rights for their data. The customer's burden of maintaining and providing their data to satisfy a bank or other institutions KYC requirements is significantly reduced. The KYCBC platform provides value to the customer in the form of a single repository for easily storing, updating and sharing their financial data and history.

Conclusion

In this article I have questioned the likely success of a marriage between KYC and Blockchain. Despite some industry analysis suggesting mainstream adoption of Blockchain is still some way off, 5-10 years, there is strong evidence, especially from the successful POC in Singapore, to suggest that the adoption of Blockchain, for KYC purposes at least, could be closer to 5 years than 10.

Having identified current challenges faced by organisations performing KYC I articulated numerous ways in which the envisaged KYCBC platform would decrease or remove those challenges. The KYCBC platform would achieve this through introduction of new customer experiences, business models and value creation models to evolve KYC into a new fully digitalised and optimised state. This is reinforced by comparing the benefits of the proposed KYCBC platform with the identified challenges:

- **Increased operating costs –** the new business model proposes an opportunity to both reduce costs through new revenue streams for performing KYC approvals and implementing a more efficient shared services approach to the underlying KYC technology platform.
- **Reputational damage –** the improved efficiency of a regional or country scale KYCBC platform offers to free up resources within banks and financial institutions. These resources can be refocused to ensure tighter regulatory compliance. Additionally, by implementing a smaller number of larger scale integrated KYCBC platforms at the country or region layer, the duplication of data, gaps in data and integration constraints for current KYC systems are reduced. This in turn reduces the opportunities for exploitation of financial services by criminal elements.
- **Poor customer experience –** through digital transformation the customer experience is improved and new customer value is created. New business models provide opportunities for new market entrants. More competitors within a market is typically beneficial for customers either through increased innovation of products and services, increased focus on customer retention or simply more competitive pricing.
- **Increased Technical Debt** – Whilst the ownership and operating model for such a KYCBC is difficult to predict, it would most likely follow a shared services approach and be consortium led initially, like the POC in Singapore. Then if the platform was adapted across a wide range use cases moving towards the utopian view of global system of record for all people and businesses, it may need to be transitioned to a country or regional level of government for management. However, in both these cases for the individual bank or financial institution the overall level of technical debt would be reduced through improved systems integration and a reduction in the need for owning their own dedicated KYC systems and processes.

In summary, after a successful first date in Singapore I believe it's fair to say KYC and Blockchain are definitely 'in a relationship'. There will be many twists and turns without doubt, not least the issue of who would own, operate and regulate a country or regional KYC platform underpinned by Blockchain. Will this relationship become the perfect marriage, it's hard to be sure, perhaps in today's world a strong mutually beneficial relationship is enough?

About the Author – Benjamin Peacock

I am a Business Architect with strong depth and breadth of skills and knowledge across the leading technologies of today. My consulting experience features a diverse range of customers across the UK, Australia and the Nordics. Of my 16 years professional experience I have spent almost 6 years working with leading financial institutions in the UK and Australia.

The key qualities I bring to our Actensa clients are:

- A passion for driving solution orientated outcomes that deliver tangible value to the end customer.
- Deep understanding of a diverse range of technologies and the business benefits they deliver across the entire value chain.
- Effective communication and engagement with a wide group of stakeholders from senior managers to technical specialists.
- A structured and analytical approach to problem solving and task execution.
- Experience in building and leading high performing teams.

I enjoy driving positive change that brings real value to customers, employees or an entire organisation. It doesn't matter how small or large, simple or complex the project required to achieve that change is, the satisfaction of achieving it is what motivates me to come to work each day and be the best consultant to my clients that I can be.

References

[1] J. Dumphy, “Fenergo,” [Online]. Available: https://www.fenergo.com/assets/files/Fenergo_KYC_and_AML_Client_Reviews.pdf?mkt_tok=eyJpIjoiWTJOa1pEZGtZakV4WWpBdyIsInQiOiJFcFY1WTJLc3RMYXdtdm9hVFQ3M2xuNmdaZjlNRVwvT2FZdDhSRW5Db01MUTg1a1wvUG5ialQyT1ZXeTZwUmxPc1UreVJvanNrMVlNNCs3UXRSNXd2Z0FDNFZPYWZhaXhTNXd. [Accessed 8 January 2018].

[2] T. Reuters, “Thomson Reuters,” 9 May 2016. [Online]. Available: https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html. [Accessed 10 January 2018].

[3] “Finextra,” 30 March 2017. [Online]. Available: https://www.finextra.com/blogposting/13903/kyc-and-blockchain. [Accessed 10 January 2018].

[4] “Reuters,” 19 May 2015. [Online]. Available: https://www.reuters.com/article/nordea-bank-handelsbanken-fsa/update-1-nordea-handelsbanken-fined-over-money-laundering-breaches-idUSL5N0YA1MS20150519. [Accessed 10 January 2018].

[5] K. Panetta, “Gartner,” 15 August 2017. [Online]. Available: https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/. [Accessed 10 January 2018].

[6] R. G. McGrath, “Harvard Business Review,” 25 November 2013. [Online]. Available: https://hbr.org/2013/11/the-pace-of-technology-adoption-is-speeding-up. [Accessed 10 January 2018].

[7] “Fintechnews,” 3 January 2018. [Online]. Available: http://fintechnews.sg/14420/blockchain/ibm-completes-poc-blockchain-based-shared-kyc-deutsche-bank-hsbc-mufg-cargill-ibm-treasuries/. [Accessed 10 January 2018].

[8] “PWC,” January 2016. [Online]. Available: https://www.google.se/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiqg7epjNLYAhUBZ1AKHWBDDXgQFggzMAA&url=https%3A%2F%2Fwww.pwc.com%2Fgx%2Fen%2Ffinancial-services%2Fpublications%2Fassets%2Fpwc-anti-money-laundering-2016.pdf&usg=AOvVaw. [Accessed 11 January 2018].

[9] S. Cantillon, “Medium,” 3 November 2016. [Online]. Available: https://medium.com/marino-software/blockchain-and-identity-revolutionising-kyc-for-financial-institutions-96f4bd8e508f. [Accessed 8 January 2018].

[10] “Fintechnews,” 3 October 2017. [Online]. Available: http://fintechnews.sg/12468/fintech/first-industry-know-customer-blockchain/. [Accessed 8 January 2018].

[11] R. Kastelein, “BlockchainNews,” 20 November 2017. [Online]. Available: http://www.the-blockchain.com/2017/11/20/ibm-completes-poc-blockchain-based-shared-kyc-deutsche-bank-hsbc-mufg-cargill-ibm-treasuries/. [Accessed 6 January 2018].

[12] J. Becher, “Digitalist Magazine,” 17 September 2017. [Online]. Available: http://www.digitalistmag.com/digital-economy/2015/09/17/avoid-digital-washing-recognize-true-digital-transformation-03456177. [Accessed 11 January 2018].

[13] “Open Gov,” 15 November 2017. [Online]. Available: https://www.opengovasia.com/articles/mas-working-closely-with-local-and-foreign-banks-to-explore-a-banking-kyc-shared-services-utility. [Accessed 11 January 2018].

[14] N. Bauerle, “Coindesk,” [Online]. Available: https://www.coindesk.com/information/what-is-a-distributed-ledger/. [Accessed 10 January 2018].