



# Sustainable KYC through Blockchain Technology in Global Banks

Vikrant KULKARNI\*, Awadhesh Pratap SINGH\*\*

## ARTICLE INFO

### Article history:

Accepted June 2019

Available online July 2019

### JEL Classification

E50, E58

### Keywords:

Blockchain, KYC, Banking, Total  
Cost of Ownership, Proactive Risk  
Management

## ABSTRACT

Blockchain has spiked a lot of interest in this decade both from technology perspective and also from the various applications of this potential disruptive technology. This paper performs a systematic review of the research and adoption progress of the much talked about Blockchain technology in the context of Customer Onboarding and KYC for Global Banks. This systematic review embraces the prominence of the peer-to-peer technology and the substantial role it can play in the complete revamp of the KYC processes for Global Banks world-wide. This paper proposes a design for consortium based solution in recent rise of risk events in global markets around reconnaissance and security breaches where the customer data privacy was compromised. The increasing annual budgets for KYC and Annual Refresh for high risk customers has become a norm in the light of terrorist attacks in 9/11 and others. The regulators also have increased the compliance checks for customer onboarding processes and then a plethora of other compliance rules to perform the regular ongoing Trigger Event KYC (change of address, change of source of funds and many more). The need for a check on AML at a macro-economic level aligned to regulations like Patriot Act, Bank Secrecy Act but also at a micro level by performing credit and operational risk management. Strict KYC norms make sure the banks and accountable executives adhere to the fact that every customer has to prove the legitimacy of their existence by submitting Proof of Identity and Proof of Address along with documents supporting Source of Wealth. This paper details on how to determine the need for Blockchain for KYC and then study the benefits of implementing Blockchain for KYC if the technology is indeed needed for the banking organization.

© 2019 EAI. All rights reserved.

## 1. Introduction

The overall rise of blockchain technology started with cryptographic currencies. Prior to this disruptive technology taking birth, the concept of digitalized money was always in a centralized manner governed by layers of security, encryption, firewalls and everything else that can maintain the privacy and secrecy associated with the value of digital money. This had its inherent issues of management overhead, higher costs of ownership, compatibility upgrades, added back-ups for disaster recovery and the unremitting risk of data hacking by miscreants. This led to sustainability issues and was always associated with a resistance in adoption by the senior managers and retail customers at large. Various enthralling schemes surrounding digital money also received mixed responses and supporters.

Nakamoto (2008) in his transformational paper "Bitcoin: A Peer-to-Peer Electronic Cash System" completely decentralized the concept of digital money and overcoming the shortfalls of centralized architecture. This blockchain technology concept involves the network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers.

In recent years many have started arguing or doubting the true benefits and adoption challenges of blockchain. Gartner's hype cycle suggests blockchain has lost its lustre in the field of cryptocurrency as there has been a sudden wave of price stabilization and regulatory tightening across many countries. There are many who have formed a school of thought which suggests that blockchain technology needs a boost of disillusionment for investors who want to become super rich in short span of time. Initial Coin Offerings are

\*, \*\*Institute of Management Technology Nagpur. E-mail address: [kulkarni.kulkarni@gmail.com](mailto:kulkarni.kulkarni@gmail.com).

also under the regulatory radar due to the issues around Anti-Money Laundering (AML) and terrorist financing.

If within a decade, we have seen cycles of both the rise and fall of cryptocurrency, is it justified to say the blockchain technology holds no ground? Is it too early to call blockchain technology as a 'just another fad'? Is the ray of hope to de-centralize information gone? Is it time to move on in search of some other disruptive innovation? Or, whilst many questions remain un-answered about the technology, the most prominent question is that whether we need a better management think tank or rather ability to create more proof of concepts for a myriad of applications in different sectors. The reason being the main thought that blockchain bubble is about to burst has two key shortcomings. The most critical one being that the apart from crypto-currency there has not been any other application that has been implemented in real use before 2017. The first beta version has only come out in 2017 and then the top 100 largest companies have started infusing money into it since then. There are some companies who have come together to crowd-fund any innovative implementations on block-chain and there some who are still evaluating the application. There has been quite an excitement seen around some of the applications like smart contracts, video games, distributed ledgers in financial firms, supply chain logistics, decentralized voting and many more. And the second shortcoming being that for blockchain technology to become an augmenting technology the organizations, management think tank, technology geeks or the policymakers have not yet surrendered control. The increasing focus on reducing costs and not having the will and intent towards disruptive innovation is making them accept status quo and suffer from the problems of centralized infrastructure.

This paper is divided into five parts: the first part reviews the crucial literature on the subject of blockchain technology. The second part focuses on the key challenges faced by organizations in trying to perform regular KYC. The third part discusses on the scenarios on when blockchain technology is a suitable choice. The fourth part of this paper draws the concluding observations. The fifth and the last section of this paper outlines the vital points on policy and decision making by the global banking organizations across the world.

## 2. Findings of key papers about different applications of blockchain in practice

S. No.	Year	Authors (year)	Blockchain Application	Major findings
1.	2008	<i>S Nakomoto;</i>	Bitcoin (Cryptocurrency )	<ul style="list-style-type: none"> <li>First paper to formally give a real life application of blockchain technology</li> </ul>
2	2015	<i>Kishigami et al.</i>	Content Distribution System	<ul style="list-style-type: none"> <li>Established the first of its kind blockchain based digital content distribution system</li> <li>Setup of Successful model of superdistribution concept which was theoretically established 30 years ago.</li> </ul>
3	2015	<i>A Walch</i>	Operational Risk Management	<ul style="list-style-type: none"> <li>Emphasized on the how blockchain can be a remarkable innovation for operational risk management</li> <li>Also studied the factors to remove inefficiencies and eliminate redundant costs.</li> </ul>
4	2015	<i>Fujimura et al.</i>	Rights Management System	<ul style="list-style-type: none"> <li>Accentuated on a concept of new rights management system</li> <li>Provided results from sample implementation</li> </ul>
5	2015	<i>Noizat</i>	Electronic Voting	<ul style="list-style-type: none"> <li>Looked to remove the issues of authenticity of voting in current voting system which impacted the confidence in voters and election organizers using blockchain technology.</li> </ul>
6	2017-18	<i>Beck Roman et al.; Moyano; Bhaskaran; Lootsma, Yvonne; Mougayar, William;</i>	KYC in Banking	<ul style="list-style-type: none"> <li>Substantiated the idea of using a single KYC verification for multiple financial institutions is an elegant and effective solution for an expensive burden for banks.</li> </ul>

### 3. Key Needs and Challenges in KYC faced by Banking Industry in today's world

**Customer Onboarding:** Onboarding a customer into any bank needs all the basic details such as name, address, contact, birth date, birth place. In absence of these details no account can be opened in any bank globally. Additional level of KYC is now mandated to review source of funds, source of wealth, connected individuals and much more.

**Customer Identification:** In cases where there are potential high risk factors associated to a customer then the Customer Due Diligence (CDD) is extended to perform Enhanced Due Diligence (EDD). This requires additional reviews and approvals from senior risk managers and head offices to review and approve.

**Transaction & Trade Monitoring:** Even after the customers are onboarded and the accounts are opened, a continuous monitoring is in place. Any doubtful transaction or a pattern of transactions immediately triggers a series of reports and checks to ensure the client is within the remits of KYC policies and the transactions are as per the declared source of funds. If there is any discrepancy found, a trigger KYC review request is started and it warrants a full KYC to be done immediately.

**Risk management:** All along the KYC processes after the customer is onboarded there is a reactive approach for Risk Management. For any Standard Risk Customer, a KYC refresh happens only after 5-7 years. For medium risk customer a refresh is scheduled every 3-5 years and for a high risk customer it is done annually. This duration has potential for lapses and then calls for a reactive risk management to fix things.

**Policy Ambiguity:** Every bank follows the policy in line with the regulations mandated by the authorities in the country which it operates. These policy documents detail out the requirements but then is subject to manual interpretation and reviews. Due to this lack of standardization, complying to each request in a customized way is time consuming.

**Rigorous international regulations:** Cross Border regulations are very rigorous and stringent. The tolerance limits for variation in permissible values is very low for international customers. Moreover, the frequency of change in policies for cross border customers is very high. All of this adds a maintenance overhead for the banks.

**Rising costs:** Thomson Reuters has projected in a survey, that due to hassle of KYC, onboarding costs have increased by a whopping 18% and they predict a further rise of 14%. Onboarding time for a new client is now a minimum of 26 days for international customers for a standard risk category.

### 4. Is Blockchain really fit for purpose of KYC in Global Banks?

All these challenges cannot be addressed by a single solution. However, blockchain technology claims to address 75% of the challenges listed above. Fitness for purpose test should validate design principles for KYC requirement, data sharing and control, governance policies and the scalability of technology to be able to cater to evolving complexities in the future. If all of these testing points are satisfied by blockchain technology then we can confirm the fitness for purpose.

**Design Principles:** Depending on which all parties are going to participate in KYC information sharing, a variety of design options are available. A public blockchain which is open for contribution and participation from everyone is possible. A public blockchain will be very rarely used for KYC purposes due to the sensitivity of the data, however if there is a need for the same then the option is certainly available. A private blockchain is open for only intended parties and is strictly managed by security and authentication rules. This is the most suitable design option for a KYC requirement. This paper will discuss in detail about this design option. There is also a hybrid blockchain option available worth exploring which can also look for including the customers or prospects becoming part of the process. A separate study is warranted for evaluating the feasibility of this design and hence is out of scope for further discussion in this paper.

**Data Sharing and Control:** In banking domain, sharing and accessing client data is subject to numerous regulatory and data privacy requirements. In addition to that there are Global Data Protection Regulation (GDPR) rules which govern the data handling, storage and distribution processes.

**Governance Policies:** Based on the various policies outlined by the regulatory and compliance teams there needs to be a thorough governance council setup to validate that the day-to-day functions are followed by abiding these policies. Any change in policy warrants a process change and needs a lot of stakeholders to provide sign-off before implementing it. With regards to blockchain, the Governance rules need to be the most crucial part of the design. Especially in cases where a private blockchain is setup, all the nodes, users, peers and validators need to be defined. Only the trusted sources should have access to the private blockchain and their roles and functionality accesses need to be defined.

**Technology Scalability:** Blockchain technology has a very high scalability potential and can easily surpass the KYC scalability requirements for next 25 years. SHA256 algorithm has increased the blockchain capability manifold for crypto-currencies and has created a new world of opportunities in all other domains. Additionally, Christidis has reviewed how blockchain mechanism works and also confirmed that the smart contracts-scripts that reside on the blockchain allow for the automation of multi-step processes: 1) facilitates the sharing of services and resources leading to the creation of a marketplace of services between banks and

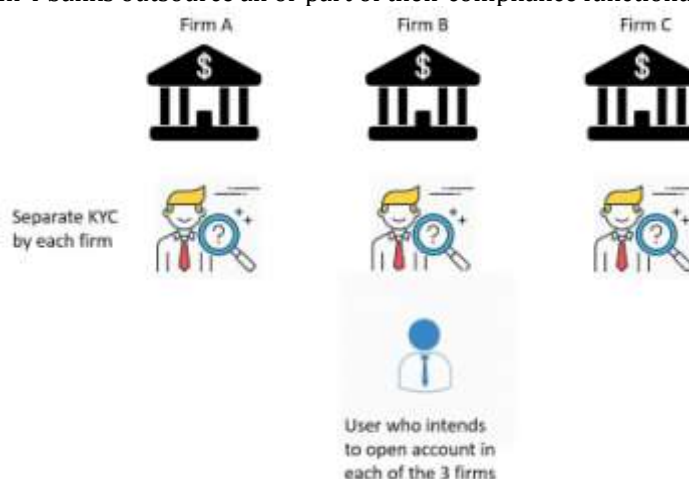
2) allows us to automate in a cryptographically verifiable manner several existing, time-consuming workflows. Although it may seem obvious, a critical issue that must be addressed is the definition of the ultimate goal of the blockchain to improve KYC processes and keep the costs at a minimum. Beyond the core benefits of a distributed, immutable, transparent, and higher trust system, the unique benefits a blockchain system can provide for healthcare processes over other existing technologies must also be assessed.

Though the above 'fit-for-purpose' blockchain framework considerations are not exhaustive, they form a basis for thinking about how blockchain can be designed in ways that have shared goals of improving KYC in a sustainable manner.

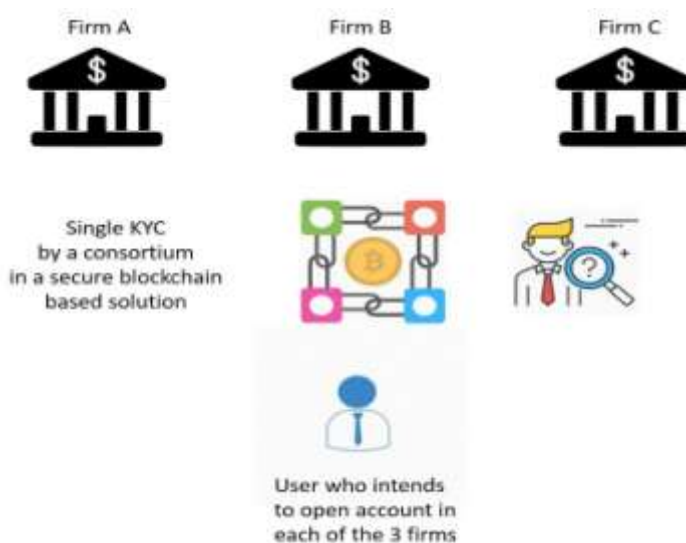
## 5. Design & Approach – Consortium Grid Based Solution

Blockchain has become highly popular with the advent of crypto-currency especially Bitcoin. It received many accolades for the key feature of decentralization and secure. The permanency factor associated with Blockchain has also attracted a lot of fanfare in the last decade. The reason why the information in a blockchain is tamper-proof is because of the ability of the SHA256 algorithm to generate a hash-code and that forms the unique key or ID for that block of information. Each block also holds the hash value of previous block and thereby a full chain is created. All the blocks are inter-linked and tampering data within any block will also need fixing the hash values of all the previous blocks in the chain.

Traditional KYC Model focuses on each financial institution must conduct its own KYC. This adds up tremendous overhead for all the financial institutions. As per Thomson Reuters report on cost of compliance in 2018, nearly 2 in 3 global banks expected an increase of more than 15% in their compliance budget on an annual basis and only 1 in 4 banks outsource all or part of their compliance functionality.



Blockchain based Consortium KYC Model focuses on consolidating the KYC operations jointly in a blockchain and then referenced by any firm as and when required. Any updates in the KYC compliance requirements will need to be done at a single place and thereby reduce the cost of implementation and maintenance in a significant manner.



The following scenario assumes a situation in which a customer conducts a new transaction with a financial institution participating in the consortium.

1. Once a prospect is identified and the relationship manager for Firm A decides to onboard a customer, all the documents required for KYC and CDD purposes for all the banks participating in the consortium will be uploaded by the prospect on a self-serve application form. A unique application number will be generated and shared with the prospect for future reference purposes.
2. This prospect's application form and the documents will be then maintained within the blockchain and accessible by all the consortium partners.
3. Firm A's compliance and operations teams will review the application i.e. perform screening, ID&V, KYC and a thorough check on the connected parties as well. These results of the review will also be sent to the blockchain and will be maintained there for audit purposes.
4. This customer's record will be updated with the latest KYC information by the Firm A on whenever there has been a change in address, contact details or any other key information.
5. If the prospect has also issued an account opening request with Firm B in future ( and Firm B is part of the consortium with Firm A ), then all the processes required to be completed by firm B can be avoided. Firm B just has to take care of "mitigation of impersonation fraud" (MoIF ) processes to ensure that it is the same customer who is requesting for the account opening.

There is a time factor associated to previous KYC processes which has to be verified with the guidelines. If the KYC has been completed by any consortium partner in the recent allowed timeframe, then the firm can directly move towards account opening.

## 6. Concluding Remarks

In this paper, we investigate the impact of Blockchain technology on varied areas of applications. Studying the current KYC procedures adopted by Global Banks, it is clear that these come with a lot of financial and procedural overhead. This overhead not only impacts the bottomline of the firm but also has a detrimental impact on the turnaround time to open new accounts and the overall customer experience associated with it, especially in cases of international customers. The blockchain based consortium KYC approach suggests that the private blockchain can be the true solution to address all the growing compliance costs for all the banks together. This solution not only renders benefits to individual firms but also helps a lot for the industry and nations as a whole to combat the growing challenges of Anti-Money Laundering, Terrorist Financing and Black Money. While this paper dwells into the theoretical design and approach, practical implications and challenges need to be looked into detail to make it an industry-wide adoption. Nevertheless, considering the high potential of blockchain technology, this design should be interpreted with caution and associated compliance risks should be evaluated by all the partners in the consortium.

## References

1. Beck, Roman, et al. "Blockchain technology in business and information systems research." (2017): 381-384.
2. Bhaskaran, Kumar, et al. "Double-blind consent-driven data sharing on blockchain." 2018 IEEE International Conference on Cloud Engineering (IC2E). IEEE, 2018.
3. Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and smart contracts for the internet of things." *Ieee Access* 4 (2016): 2292-2303.
4. Fujimura, Shigeru, et al. "BRIGHT: A concept for a decentralized rights management system based on blockchain." 2015 IEEE 5th International Conference on Consumer Electronics-Berlin (ICCE-Berlin). IEEE, 2015.
5. Kishigami, Junichi, et al. "The blockchain-based digital content distribution system." 2015 IEEE Fifth International Conference on Big Data and Cloud Computing. IEEE, 2015.
6. Lootsma, Yvonne. "Blockchain as the Newest Regtech Application—the Opportunity to Reduce the Burden of KYC for Financial Institutions." *Banking and Financial Services Policy Report* 36.8 (2017): 16-21.
7. Luu, Loi, et al. "Making smart contracts smarter." *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. ACM, 2016.
8. Mougayar, William. *The business blockchain: promise, practice, and application of the next Internet technology*. John Wiley & Sons, 2016.
9. Moyano, José Parra, and Omri Ross. "KYC optimization using distributed ledger technology." *Business & Information Systems Engineering* 59.6 (2017): 411-423.
10. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008)
11. Walch, Angela. "The bitcoin blockchain as financial market infrastructure: A consideration of operational risk." *NYUJ Legis. & Pub. Pol'y* 18 (2015): 837.