



KYC and Blockchain Onboarding Process for Banks

Abdelmageed Algamdi, Department of Computer and Information Systems, college of community. University of BISHA. Bisha. Saudi Arabia, Email: amofrh@ub.edu.sa

Interest in blockchain technology has grown significantly over the last decade, both technical and due to the many uses of this potentially revolutionary technology. This study examines the status of the much-discussed use of Blockchain technology in the context of client preparation and Know Your Customer (KYC) for banks. This systematic assessment acknowledges the emergence of technology and the critical role in reimagining KYC procedures for banks worldwide. This study presents a federation-based solution in response to the current growth in high-risk market situations, such as reconnaissance and security breaches affecting client data privacy. Yearly funds for KYC have increased, as have annual updates for high-risk customers. Regulators have also strengthened compliance checks beginning with client onboarding procedures and continuing with a slew of additional compliance standards to execute KYC. The importance of anti-money laundering investigation at the macroeconomic level, according to rules such as the Patriot Act and the Bank Secrecy Act, and at the microeconomic level via credit performance and operational risk management. The strict KYC requirements guarantee that banks comply with the need that each client establishes their legitimacy via evidence of identity and address and supporting documentation for the source of money. This article covers how to determine if banks really demand Blockchain for KYC and then analyses the benefits of using the technology if they do.

Key words: *KYC, Blockchain, Banks, Risk, Cost.*

1. Introduction

Blockchain technology had an early adoption phase with the emergence of cryptographic currency (Woodside, Augustine Jr, Giberson, & Management, 2017). While digital money had previously contained to centralized domains, such as government-issued money and centralized digital currencies, there was a period where digital money could be considered

"disruptive" (Kaplanov, 2012; Swan, 2015). Because of the technologies like digital currency, digital banking, and blockchain, all having a marked impact on the market (Buitenhek, 2016; Wang, 2021). Then, several associated expenses include more administration overhead, greater long-term ownership expenses, compatibility updates, several redundancies in place for disaster recovery, and an inescapable danger of data hacking by malevolent parties. When consumers were apprehensive about this, sustainability difficulties emerged, which attributed to the reluctance of top management and retail consumers to accept it. Various exciting ideas associated with digital money likewise met with varied attitudes and advocates (Oskamp & Schultz, 2005).

This groundbreaking work (Bitcoin: A Peer-to-Peer Electronic Cash System) by Nakamoto fully decentralized the notion of digital money, which he calls "money sitting on top of the existing financial system" in the introduction (Extance, 2015). This blockchain technology idea includes the network timestamping all transactions through a hashing process, becoming a chain of timestamped proofs of work (Ma, Ge, Zhou, & Applications, 2020; Namasudra, Deka, Johri, Hosseinpour, & Gandomi, 2021). The process cannot be modified without starting over with the proof of work. In recent years many have started arguing or doubting the actual benefits and adoption challenges of blockchain. Gartner's hype cycle suggests the 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. Many have formed a school of thought that suggests that blockchain technology needs a boost of disillusionment for investors who want to become super-rich in a short period (Kulkarni & Singh, 2017).

More recently, many people have begun questioning whether blockchain provides any significant advantages and whether it would ever catch on. According to Gartner's hype cycle, there has been a rapid surge of price stability and regulatory across several nations, which indicates that people's enthusiasm for blockchain has faded in the sphere of cryptocurrencies (Steinert & Leifer, 2010). Many have formulated a school of thinking that claims that blockchain technology requires a dose of disenchantment in order for investors to become ultra-wealthy in a short amount of time (Botsman, 2017). Crowdfunded projects also face regulatory scrutiny because of AML (anti-money laundering) (Blozinski, 2017).

If we have watched the rise and fall of cryptocurrencies over a decade, is it fair to argue that blockchain technology is without merit? Blockchain technology has not yet established itself as simply another craze (Chamberlain, 2019). The glimmer of hope has extinguished: Does information want to be decentralized now? It is time to look for something else to disturb. There are still many unanswered questions regarding technology. However, the most central question is whether we need a management think tank with more excellent capabilities to produce a more comprehensive array of concepts or improve our ability to develop a proof of concepts for various applications in different sectors. The assumption that the cryptocurrency bubble would eventually burst supported by one of the central premises of the blockchain

bubble theory. However, one of the theories is that the cryptocurrency bubble will burst (Shu, Zhu, & Applications, 2020).

Organizations have joined forces to raise money for any groundbreaking ideas implemented on the blockchain, and others are still deciding whether it's a good idea (Makridakis, Polemitis, Giaglis, Louca, & Applications, 2018). Some people have noticed the possible uses of blockchain, computer games, distributed ledgers in financial enterprises, supply chain logistics, decentralized voting, and many more applications. Furthermore, the second major drawback is that corporations, management think tanks, technical geeks, and legislators have not yet ceded control of blockchain technology (Cole, Stevenson, & Aitken, 2019). They are trying to decrease expenses while disrupting the status quo results in people accepting their current state and the challenges associated with centralized infrastructure.

This research has five parts: it begins with a review of the literature about blockchain technology, followed by an introduction, discussion, and an afterword, and then the last component consists of commentary on other papers on the issue. The topic of this section is how firms often struggle with implementing average KYC measures.

2. Blockchain in the real world discoveries

Creating KYC processes and processes presents several complications for banks. A basic technique often neglected in the course of designing a KYC framework. Complexity increases while developing a single KYC process that serves a diverse group of customers. One may request that folks produce their identity to regarded a genuine client. One smartphone app generates several problems when banks roll it out. There is not, is there? Do the banks make sure that the documents provided are genuine? The bank checks to see whether the ID indeed came from a government or credible source. A document submitted must be for the account holder whose account number provided. Complicating matters, the beneficial owner will likely not have the papers essential for KYC compliance.

They generally accepted identity papers viewed as secret documents in several nations. Customers are instructed to provide a certified, authentic copy of the document and are worried that the identity document copy is safe from theft or interference. The customers have to wait till the issue rectified before establishing an account. This used to take two days to create a business account. Because it might take weeks, maybe months, banks do not disclose definite timelines. Corporate clients are affected by these account opening delays, which may delay transactions that undermine the company's overall performance. Delays may generate considerable commercial challenges, especially for fledgling businesses that need to gain their partners' trust rapidly.

The amount of responsibility that the customers have while going through the KYC process grows. The more complicated the conditions need to be satisfied, the greater the challenge



becomes to create and maintain an account. While working on their KYC, compliance managers discover additional hurdles with which to contend. It might be the case for quite some time, as much time may be spent while waiting for customers to submit their information for KYC processing. Financial institutions must not go head-to-head with other industries for the same market segment. Many believe that the banking industry works inefficiently because it keeps its market captive and complies with strict Know Your Customer guidelines, which have fueled the belief that banks poorly managed. The only available choice for a consumer is to voice their unhappiness and hope that their problems are given more priority than the worries of other customers who have complained.

Even so, does the bank have a responsibility, or does the regulatory body? In all likelihood, they are both to blame. Regulators have implemented KYC standards that do not consider the many barriers that firms must overcome in putting them in place. Meanwhile, banks have to contend with constructing new systems, creating KYC (Know Your Customer) programs, and training customer service people to respond to many situations they may encounter as they go through the KYC (Know Your Customer) process. Both banks and regulators have found these shortcomings and are already trying to strengthen customer service.

Many banks are concerned about the added costs for their customers due to these limits, and as a result, some are pretty reluctant to implement them. Conversely, yet nonetheless, while making decisions about their clientele, they found themselves in a bind. When it comes to handling the current Coronavirus epidemic, should they invest time and money into building and maintaining a consumer-friendly KYC process, or are they risking damaging customer happiness by installing and administering a KYCT that takes little time to complete? Though official regulatory permission has provided, this product does not give a positive customer experience.

There is a great deal of worry amongst financial institutions because of the threat of losing their operating license should they fail a regulatory assessment. Any operating license, or its other kind of limit on conducting business, may damage a bank. It might mean the bank's customers lose money, devastate the company itself and any clients' businesses. As stated above, a period is probably granted for a bank to become compliant to avert this issue. Appropriate alterations are vital to particular consumers, who could not benefit from one that has not adequately stated. For all banks, the most important concern is making the services they provide less burdensome for their customers and maintaining the positive relationships they have with their customers. Even though several difficult and complex "global standards" programs are hard to establish with tricky and sophisticated procedures for internal employees and customers to follow, they tend to apply the rules to the extreme. As a result, they err on the side of caution. While avoiding a properly established KYC compliance program may result in fines and the danger of losing a banking operations license, it is a bad outcome no matter what course of action one chooses. Despite this, many rules have not implemented for financial institutions since doing so is not in anyone's best interest. We will not meet all of our customers' needs with compliance

programs universally identical yet made to accommodate clients in the particular range. When a bank has thousands or hundreds of thousands of accounts that may impact, there is no efficient, effective, or feasible way to examine each account holder on a case-by-case basis, within a reasonable period, or with the available resources.

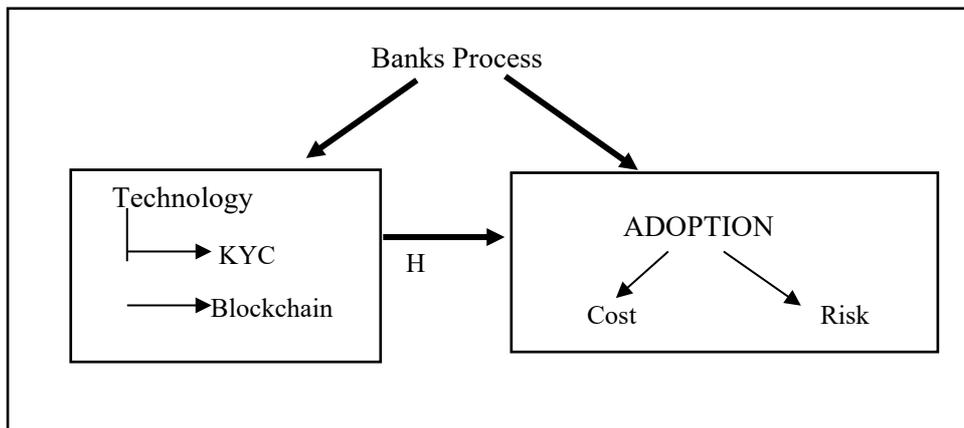


Figure 1. Blockchain research model

3. KYC (know your customer) impact on the banking industry

Any bank requires basic information such as a client's name, address, contact information, birth date, and location when onboarding a new client. Until this data obtained, no one bank can construct an account for anywhere in the world. Additional KYC (linking to financial resources, sources of wealth, individuals, and other criteria) is now necessary to examine the source of money, wealth, and other related variables.

- **Customer Identification:**

When high-risk characteristics linked with a client, the Customer Due Diligence (CDD) also performed to complete Enhanced Due Diligence (Lmater, Eddabbah, Elmoussaoui, & Boussaa). It necessitates further scrutiny from senior risk managers and head offices, who consulted to provide a final evaluation and approval.

- **Transaction & Trade Monitoring:**

Constant monitoring is in place after the consumers have onboarded and the accounts have opened. When any dubious transaction or a string of transactions identified, the audit process quickly initiates Several inspections and verifications conducted to ensure that the customer maintains within the boundaries of KYC standards and the declared source of money complies with KYC requirements. The account is flagged when a disparity is identified, which initiates a KYC review request. The results in a complete KYC to performed quickly.

- **Risk management:**

KYC (Know Your Customer) procedures take place as part of the onboarding process, and a reactive approach to risk management is in place at all times. A KYC refresh for each Standard Risk Customer occurs at least five to seven years following the first application. A refresh is planned for a medium risk client every three to five years, whereas, for a high-risk client, a refresh happens every year. This length holds the possibility of lapses and necessitates the use of reactive risk management to correct problems.

- **Policy Ambiguity:**

Banks worldwide adhere to policies prescribed by the country's authorities, and such policies are usually consistent with the legislation. These policy papers go into great depth on the criteria, but it is up to interpretation and evaluation after that. It is challenging to follow every one of the many customization requests due to the absence of standards.

- **Rigorous international regulations:**

In order to meet these heightened requirements, many cross-border rules are onerous and strict. International clients' tolerance limitations for change in permitted values are relatively limited. Moreover, the volume of changes to rules for consumers in two different countries is also relatively large. Every one of these things comes with an added maintenance burden for the banks.

- **Rising costs:**

A poll conducted by Thomson Reuters predicts that onboarding expenses have risen by a staggering 18% owing to KYC complexity, and these predictions show that the entire onboarding cost would be around 14% higher. New customers' onboarding period must be at least 26 days, and regular international clients should expect this process to take somewhat longer.

4. Blockchain and KYC in Banks?

We have many complex challenges ahead of us, which cannot be resolved by a single approach. Although the blockchain promises to manage over 75% of the issues discussed, it does not mean it can fulfil all of these functions. The test should examine the degree to which design principles, such as data sharing and control, governance standards, and scalability, have been used for KYC compliance. As well as the degree to which design principles can change as future complexity increases. To prove the appropriateness for use with blockchain technology, one must establish whether or not all of these screening tests have been satisfied.

- **Design Principles:**

The KYC process is dependent on the participants in the process to decide on how information is shared. Here, many design possibilities are possible. It is conceivable to implement a public blockchain accessible to participation and input from the general population. In the general case, public blockchains will be challenging to utilize for KYC (know your customer) reasons due to the data's sensitivity. However, if there is a requirement for the same, then this is undoubtedly an alternative. The private blockchain is available only to people who plan to use it and rigorously govern security and authentication regulations. The best design for a KYC requirement is the one shown above. This paper will provide detailed information on this design alternative. Not only is there the hybrid blockchain solution that searches for adding customers and prospects to the process, but there is also the hybrid blockchain alternative that also examines the use of customers and prospects as participants. While it is not necessary to do independent research on the viability of this design, it is not included in the scope of this work and should hence not further discussed.

- **Data Control:**

Features complementary to conventional banking services could include exchanging and accessing client data subject to various regulatory and data protection limitations. Besides that are standards set by the European Union to control data management, storage, and dissemination called the Global Data Protection Regulation (GDPR).

- **Governance Policies:**

According to the various regulations that the regulatory and compliance teams provide, a governing council should be in place to check that day-to-day activities are being carried out in conformity with the regulations. Any policy change will inevitably be accompanied by equivalent process changes and will need many stakeholders to agree on the strategy before being implemented. While it is vital to have governance rules in place for a blockchain, it is equally necessary to design those rules effectively. It is important to note that for many use cases, particularly when implementing a private blockchain, all nodes, users, peers, and validators must be adequately defined. Only sources you can trust should have access to the private blockchain, and their roles and functionalities' access permissions must be specified.

- **Blockchain technology:**

The potential scalability of blockchain technology is substantial and will support many transactions far beyond the KYC verification scalability demands during the next three years. The potential of blockchain blockchains has vastly grown with the advancement of the SHA256 algorithm, which has given birth to a whole new universe of possibility for cryptocurrencies in other areas. In addition, Christidis performed in-depth research on

blockchain mechanisms and confirmed that smart contracts scripts live on the blockchain, which allows the automation of multi-step operations. Through the intelligent contracts scripts, service providers can now freely and directly offer their services and resources to other service providers in the community, resulting in the development of a market of services where banks can utilize the workflows of their competitors to automate cumbersome processes. Accomplish the goals outlined in the introduction. One critical need is to create a purpose statement that summarizes the overall goal of the blockchain system, which is to simplify identity verification processes while limiting expenditures. Because the benefits above of a distributed, irreversible, transparent, and increased trust system are beyond the scope of this study, the possible benefits that a blockchain system may provide for healthcare systems must also be explored.

Although these first few framework considerations for designing blockchain applications are not comprehensive, they are a foundation for formulating a strategy for building blockchain applications while also outperforming regulatory compliance standards while also enhancing system efficiency.

5. Consortium Grid-Based Solution

The growing popularity of cryptocurrencies, especially Bitcoin, has helped spur growth in new blockchain projects. In addition, other noteworthy publications acknowledge the company's focus on decentralization and security; due to the stability of the blockchain, it has been surrounded by some hype for a decade, possibly due to its persistence. One of the primary reasons why information on a blockchain is considered "proof against tampering" is because of the ability of the SHA256 algorithm to construct a hash code, which is the unique key or ID for that block of information. Additionally, each block saves the previous block's hash value, which results in a whole chain produced. It is impossible to avoid changing the data when working with blockchains because all that data is interconnected. Changing the data in one block also requires adjusting the previous blocks' data.

KYC under the old paradigm places the responsibility on each financial institution to do their KYC. So, added to the other expenses, it creates an enormous burden for all the financial institutions. Thomson Reuters discovered that compliance budgets are increasing for most global banks. Their study discovered that more than one-third of these financial institutions intend to spend more than 15% of their compliance budget annually, while only one-fourth use outsourcing to cover all or part of their compliance operations.

In order to manage a consortium-wide KYC (Know Your Customer) model that leverages the blockchain, it is necessary to make a large number of KYC operations, which are accessible via the blockchain, accessible to other organizations as needed. If there are any modifications to KYC compliance rules, they just applied to a single site. This will allow for significant cost savings concerning installation and maintenance expenses. In the following example, the scenario projects a transaction where a client, who is also a consortium member, initiates a new



transaction with a financial institution member of the consortium. The relationship manager chooses to onboard the customer once the prospect has found it. The prospect automatically submits all of the paperwork required for KYC and CDD through a self-serve application form. The consumer will have to trust them since a unique number will generate, and this number will be kept and used as a future reference. Once the applicant has completed the application form and given the additional required documents. The data will be stored on the blockchain and made accessible to other consortium members. for example, to screen the application, a compliance and operations team will have to thoroughly study the form to verify that it meets company policy.

Due to the prior KYC processes have completed, there is a time limitation imposed on the current processes, which must check with the standards. The firm must move forward by obtaining a business account as soon as possible. If the KYC has completed any consortium partner in the allotted timeframe, the firm must have granted authorization by at least one of the consortia partners.

The clients grant the bank permission to access the encrypted file only if the key exchange verifies their authority. Only the relevant personal identifying information, which comes from the data file, is sent to the bank. That information then merged into the KYC system located in the back office. The moniker under which this model has most well recognized has been called "eKYC." Once the project completed, clients maintain control and ownership of their data. By doing this, they limit the possibility of errors and save on resources and costs. This treatment may be completed in seconds rather than days or weeks. It is in use and easily accessible at this time. The problem is determining the universal data format we should use and trusted to check and authenticate identity information. In order for banks to accept the eKYC form, they must confirm that the format of the data and the regulators' acceptance of the third-party certification organization are in agreement.

Banks and their clients spend much money in the process of doing KYC (know your customer). In the March 2017 report issued in April 2017, the European Banking Association's Crypto technologies Working Group has researched and provided an assessment on blockchain technology. Nevertheless, cash transfers enable banks to increase the simplicity of internal settings and client identification data. Opening up the ability to identify information expands on its already existing advantages. The advent of a single in-house source of truth regarding a customer's identification enables companies to reduce the delays caused by fragmented information. Customers who wish to enter into new connections with banks should undertake an acceptable level of screening for AML and due diligence. This case involves this particular instance. the access to secure data (KYC information exchange inside the financial sector or between banks and their subsidiaries) facilitated by facilitating the sharing of KYC information assists banks and affiliates in supplying unique goods, yet without the waste of duplicative efforts.



6. Conclusion

This research takes a deeper look at various use scenarios, which leads to an even better understanding of the overall implications of Blockchain technology. The processes now in place for KYC performed by Global Banks not only entail financial and operational overhead, but they also represent a large percentage of it. Adding the total time required to create new accounts and the total customer experience cited with it to the total overhead, including operations and administrative costs, means that when overheads included, the total time needed to create new accounts and the associated experience suffers. In particular, creating new accounts in international marketplaces has a considerable impact on the time it takes to do so. KYC intended to be the solution to the continuously rising compliance cost that financial institutions are facing. The private blockchain is considered an essential component in assisting it to become a reality. This alternative approach accommodates business-level customization and business clients' specific needs while simultaneously working to fight the ongoing complex anti-money laundering, terrorist funding, and black-money concerns. For this article to implemented on a broader scale, it is essential to acknowledge and include theoretical concepts and ideas. However, at the same time, a wide range of hurdles and issues must be resolved in order for the implementation to occur. While this is all well and good, bear in mind the powerful potential of blockchain technology, which is vital given the expectations associated with this design. This calls for diligence when reviewing the design, as well as concerns with consortium compliance.

Acknowledgements

The author would like to express their appreciation to the reviewers and editor for their valuable suggestions and comments.

Conflict of Interest

They have no conflict of interest.



REFERENCES

- Blozinski, P. (2017). *Bank Secrecy Act/Anti-Money Laundering Burden on US Financial Institutions*. Utica College,
- Botsman, R. (2017). *Who can you trust?: how technology brought us together—and why it could drive us apart*: Penguin UK.
- Buitenhek, M. J. J. o. D. B. (2016). Understanding and applying Blockchain technology in banking: Evolution or revolution? , *I(2)*, 111-119.
- Chamberlain, S. L. (2019). *Assessing the Merits of Blockchain Technology for Global Sustainable Development Initiatives*.
- Cole, R., Stevenson, M., & Aitken, J. J. S. C. M. A. I. J. (2019). Blockchain technology: implications for operations and supply chain management. <https://doi.org/10.1108/SCM-09-2018-0309>
- Extance, A. J. N. N. (2015). The future of cryptocurrencies: Bitcoin and beyond. *526(7571)*, 21. <https://doi.org/10.1038/526021>
- Kaplanov, N. J. L. C. L. R. (2012). Nerdy money: Bitcoin, the private digital currency, and the case against its regulation. *25*, 111. <https://doi.org/10.2139/ssrn.2115203>
- Kulkarni, V., & Singh, A. P. J. t. (2017). Sustainable KYC through Blockchain Technology in Global Banks. *6*, 18.
- Lmater, M. A., Eddabbah, M., Elmoussaoui, T., & Boussaa, S. (2021). Modelization of Covid-19 pandemic spreading: A machine learning forecasting with relaxation scenarios of countermeasures. *J Infect Public Health*, *14(4)*, 468-473. [doi:10.1016/j.jiph.2021.01.004](https://doi.org/10.1016/j.jiph.2021.01.004).
- Ma, G., Ge, C., Zhou, L. J. P.-t.-P. N., & Applications. (2020). Achieving reliable timestamp in the bitcoin platform. *13*, 2251-2259. <https://doi.org/10.1007/s12083-020-00905-6>
- Makridakis, S., Polemitis, A., Giaglis, G., Louca, S. J. A. I.-E. T., & Applications. (2018). Blockchain: the next breakthrough in the rapid progress of AI. 197-219. <https://doi.org/10.5772/intechopen.75668>
- Namasudra, S., Deka, G. C., Johri, P., Hosseinpour, M., & Gandomi, A. H. J. A. o. C. M. i. E. (2021). The revolution of Blockchain: State-of-the-art and research challenges. *28(3)*, 1497-1515. <https://doi.org/10.1007/s11831-020-09426-0>
- Oskamp, S., & Schultz, P. W. (2005). *Attitudes and opinions*: Psychology Press. <https://doi.org/10.4324/9781410611963>
- Shu, M., Zhu, W. J. P. A. S. M., & Applications, i. (2020). Real-time prediction of Bitcoin bubble crashes. *548*, 124477. <https://doi.org/10.1016/j.physa.2020.124477>
- Steinert, M., & Leifer, L. (2010). *Scrutinizing Gartner's hype cycle approach*. Paper presented at the Picmet 2010 technology management for global economic growth.
- Swan, M. (2015). *Blockchain: Blueprint for a new economy*: "O'Reilly Media, Inc."
- Wang, Q. (2021). *Is Virtual Currency a Standard Financial Bubble? Blockchain Industry Research*. Paper presented at the 2020 International Conference on Data Processing



International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 15, Issue 9, 2021

Techniques and Applications for Cyber-Physical Systems. https://doi.org/10.1007/978-981-16-1726-3_75

Woodside, J. M., Augustine Jr, F. K., Giberson, W. J. J. o. I. T., & Management, I. (2017).
Blockchain technology adoption status and strategies. *26*(2), 65-93.