Blockchain-based Decentralized KYC (Know-Your-Customer)

Syed Azhar Hussain
University of Nicosia
Nicosia, Cyprus
qadria[at]gmail[dot]com

Zeeshan-ul-hassan Usmani
University of Nicosia
Nicosia, Cyprus
zusmani78[at]gmail[dot]com

***Abstract*— Know Your Customer (aka KYC) is the regulatory and compliance obligation for the conventional banking and financial system to capture customer information before onboarding and providing any financial services. In banks, KYC is embedded into the account opening forms, which mandate customers to provide accurate information and ideally update as soon as any change occurs in the KYC data. Similarly, other financial institutions such as stocks, Mutual Funds, Insurance companies, etc. also require KYC information from prospective customers. Primarily KYC helps financial institutions to prevent identity thefts, money laundering, terrorist financing, and profiling and eliminating the runaway creditors. Conventional banking and financial institutions spend a substantial part of customer acquisition costs of operating residents and isolated KYC databases and try to keep them updated and accurate. The overall cost of managing the silo KYC per customer increases because of a lack of transparencies, poor control, mistrust, and data duplication. Blockchain technology offers a solution to establish trust and transparency and provide a secure and publicly verifiable KYC. This paper presents a unique trust management platform based on self-sovereign and decentralizes Know-Your-Customer (DKYC) model to enhance customer privacy through consent-based access, featuring regulator governance and helping banks to use trusted and accurate customer data while reducing the customer acquisition costs.**

Keywords-Blockchain application; self-sovereign identity; trust system; know your customer (KYC); customer privacy.

I. INTRODUCTION

Blockchain is an emerging technology, a trust protocol, envisioned by Satoshi Nakamoto [1] with an extraordinary digital currency use case. In just a short span of 10 years, blockchain technology has disrupted every industry to establish trust and transparency through immutable provenance. The financial sector is facing many challenges, especially higher transaction costs [2] in trustless environments and eventually, all cost burdens shifted to end-customers. Additionally, banks pay huge sums to prevent fraud, but data breaches, leaks, and hacks [3] are fairly prevalent. This paper specifically examines the most important use case of financial sector i.e., "Know Your Customer" KYC (Figure 1), and addresses the key challenges it faces such as a high cost of managing the KYC per customer, increasing the unbanked customers [4], verification time, audit error and most importantly, the isolated centralized databases which do not talk to each other. This paper proposes a novel DKYC model, which is going to disrupt the current KYC implementations through distributed ledger technology and offers benefits such as lower transaction costs, with higher provenance, immutability, and transparency in transactions.

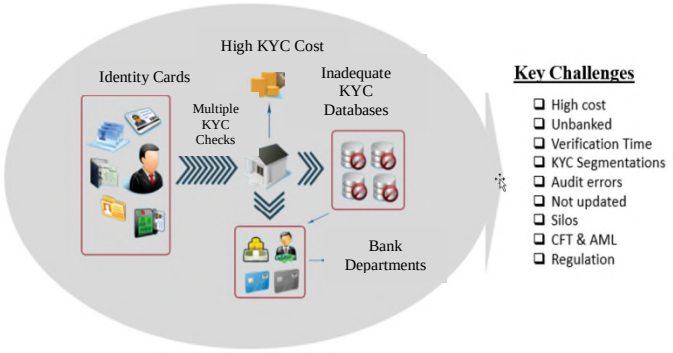

Figure 1. Know your customer

This paper is structured as follows; Sections I, II and III discuss the KYC challenges related to processes, implementations and regulatory implications in the financial sector. Sections IV and V explain our proposed model of distributed KYC (DKYC) solution. Section VI briefly highlights the viable incentive mechanisms, and Section VII summarizes the paper with key topics open for further study.

II. BACKGROUND ANALYSIS

In today's glo1bal economy, we live in a world where the users are in full control of their identity and are the sole authorizer to whom they may share their information. Know-Your-Customer has become pivotal in the digital world and large financial institutions need to identify ways to trust foreign banks and have more transparency into recipients' profile. Most financial institutions are sticking to the conventional procedures of KYC [4] which are inefficient and convey an unpleasant consumer interaction with the long and arduous process that KYC entails. Also, because of the involvement of many parties in the traditional KYC processes, it becomes prone to flaws and human errors and is very inefficient. Following are the key market dynamics and barriers of the KYC processes [5]:

- Despite dramatic increases in headcount and spend, KYC resource remains the greatest challenge to financial institutions

 ISBN: 978-1-61208-753-5

- The largest financial institutions ($10billion+ turnover) have seen average spend on KYC-related procedures increase from $142m in 2016 to $150m in 2017
- The number of financial institutions employees working on KYC adherence has rocketed from an average of 68 in 2016 to 307 in 2017
- Despite the rise in headcount, a third (34%) of financial institutions report that a lack of resources remains the biggest challenge in conducting KYC and customer because of diligence processes
- Financial institutions claim that on average it takes 26 days to onboard a new client, up from 24 days in our 2016 survey. However, corporate customers claim that on average it takes 32 days
- Financial institutions expect onboarding times to rise again by 12% in the next year

Many of the barriers can be eased with the adoption of state-of-the-art technology that can revolutionize this process both for the institution and the user. By using distributed ledger-based KYC [6], which can be shared by multiple banks, we are looking at a game-changing, innovative process that will reduce the burden of many processes and also provide more transparency and visibility let alone an enhanced user-friendly environment for KYC. We make identity verification secure and accessible on-demand.

Example KYC implementations using blockchain technology:

TABLE I. KYC IMPLEMENTATIONS

Company	Description
Argos Solution [7]	Argos provides KYC form submission and screening for errors and fraud cases. It also provides checkups on the customer lists with our AML global watch lists and targeted profile investigation and risk leveling. AML report publishing and Whitelist finalization. HQ in South Korea.
KYC-Chain [8]	A B2B managed workflow application that enables organizations to manage their KYC processes for individuals and corporates. It provides a solution to streamline the onboarding process for the customer. Review and process incoming KYC applications by streamlining workflow and automating the screening and verification process. HQ in Hong Kong.
Tradle [9]	KYC on blockchain provider. Aims to build a global trust provisioning network to give retail, wealth, SME and institutional customers of financial institutions access to capital and risk allocation. Uses pre-integrated vendor products such as biometrics, ID scanning, sanctions, and PEPs checkers. HQ in New York.
KYC Legal [10]	Provides blockchain KYC document verification through a mobile application, and verification of identity and documents with a KYC LEGAL agent. After verification into the blockchain, the user can use the stored data to verify identification for multi-purposes. The application is available for iOS and Android mobile devices. Provides B2B and B2C services. Offices in Berlin, San Francisco, and Moscow.
Confirm [11]	The company's platform uses algorithms and big data analysis to provide data on blockchain transactions and parties. It provides an AML Platform that offers anti-money laundering (AML) products for companies and financial institutions operating in the cryptocurrency ecosystem. Provides an end-to-end know your customer solution covering entities' activity in the crypto ecosystem. HQ in London, UK.

III. REGULATORY FRAMEWORKS

In this paper, have taken up the regulatory part to shed some light on how regulatory challenges affect the growth of DKYC based blockchain model. It is important to compare the traditional framework [2] with the perceived updated one across jurisdictions and the ways by which it makes compliance to allow decentralized growth. This will help us to form an adjustable framework that complies with all existing compliance models and can be changed regarding the jurisdiction in question.

A. Customer Case Studies

Because of the decentralized nature of our platform, it is difficult to formulate a common and adjustable framework, as different individuals and entities from different parts of the world will need separate frameworks for establishing KYC compliant infrastructure. An individual from the Eurozone in need of a GDPR compliant KYC/AML[12] framework cannot pass the legal hurdles with the local authorities when provided with an AML/CFT II framework established by the U.S. Regulatory Framework Act. Thus, there is a need for simplification of complexities of frameworks, as the traditional KYC model discourages knowledge transfer from one to another, limiting the exchange of value, information and ideas.

B. Frameworks

Most countries follow a similar KYC/AML framework [13], all taking its roots from either the European or the American standard of compliance. Most organizations have an inefficient system of asking for KYC/AML [6] documents separately, each time a new customer comes in. This model is flawed and inefficient as the same person might have to submit the same documents again and again with different entities throughout their lifetime, and inefficient on the business side and it brings in extra costs. By forming a common framework by which both sides can do away with this repetitive process, millions, if not billions can be saved in operating costs around the globe. 2015 saw a continued

 ISBN: 978-1-61208-753-5

rise in regulatory frameworks developed by governing bodies [14] with a key focus area for management, finance, registration, and authentication. Know Your Customer (KYC) and anti-money laundering regulations are becoming important to help businesses protect themselves from identity theft, money laundering and financing terrorism. Incidents like the one above, are all too common and the costs of complying with KYC's anti-corruption due diligence procedures are high.

According to the International Monetary Fund [15], incidents involving money laundering, compliance violations of KYC regulations, and other breaches are estimated to cost between two and five percent of the world's gross domestic product. The compliance with the regulatory frameworks (as illustrated in Figure 2) such as AML/CFT, Basel III, MiFID II, PSD2, GDPR is imperative for any KYC solution both at state and/or country level.

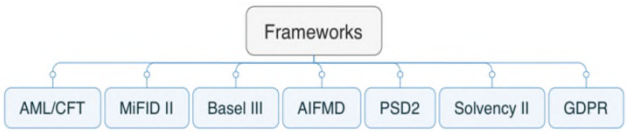

Figure 2. Regulatory Frameworks

The frameworks differ from area to area, depending on the perceived needs of the authorities to discourage unethical and unlawful practices. There are innumerable challenges when coming up with a common framework that is adjustable depending on the area and situation. Therefore, it is of utmost importance to show a robust KYC/AML framework with enough privacy, management, and oversight that ultimately understands and mitigates non-compliance and AML risks.

C. Other Compliance Costs

A financial institution spends on an average of about $50 million a year on KYC related expenses [16], with larger institutions going as high as $150 million dollars. Our aim is to propose a DKYC model to cut these costs that are associated with the tedious process of traditional KYC. The major cost that DKYC might incur is the registration with Governments of various countries. Each country has its own KYC norms that need undivided attention to detail as the subtle difference can lead to scrupulous outcomes. A research team will be necessary to go through the details of each country one by one to be thorough in all respects.

IV. DKYC Model

KYC forms (as depicted in Figure 3) are complex and contain lots of information related to the customer including Name, Birth Dates, Addresses, Income, etc. And as most of the information is dynamic in nature, the update process is very tedious and complex. In our study we have examined the data requirements of KYC, to understand the structured relationships and how it can be captured and reshaped through the DKYC model. There will be two different major segmentations, which hold and serve the Individuals KYC and Business KYC, and subsequently, both segments have different treatments.

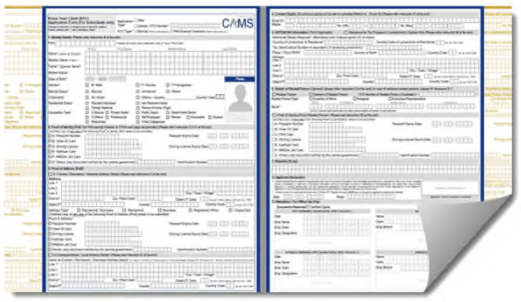

Figure 3. KYC Sample Form

Traditional KYC is based on the Pull mechanism where the customer information captured while onboarding the customer. DKYC supports both the Push (customer sending information to the service provider) and the Pull models (bank or service provider seeking an update on customer profile) with customer consent on what, where and whom he/she would like to share the information.

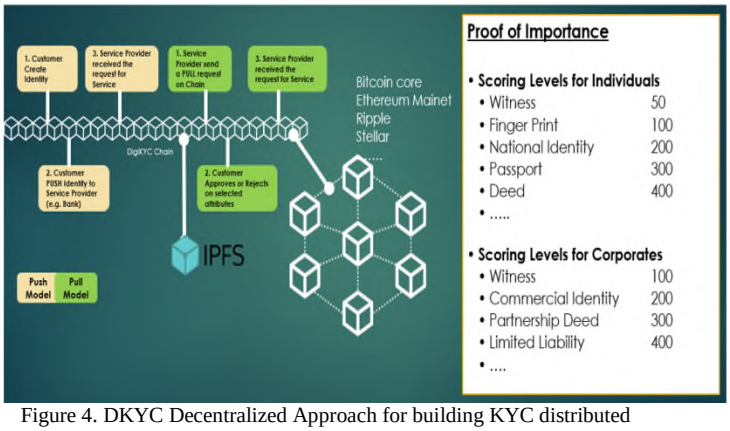

Figure 4. DKYC Decentralized Approach for building KYC distributed network

As illustrated in Figure 4, the typical scenario starts when a customer creates his/her identity on the chain and likes to push his/her information to the service provider for example to create a bank account. Bank will validate the request through the chain and start the customer onboarding. DKYC will be a public blockchain where anyone without geographical restriction joins the identity platform. We will apply Proof of Importance consensus algorithm to establish a scoring mechanism where existing conventional identities establishments e.g. Civilian Identities, Regulators, National Security Numbers, other private sector identities stores can also participate and part of the network to set the scoring. For example, from an Individuals segment, anyone can join the network by having the basic form of proof is "peer witnesses", however, the score is 50.

If the customer provides his fingerprint (which is unique in the world), his/her score in the DKYC chain will increase to 100. Similarly, if the customer provides the National Identity proof than his/her score will increase to 200. And A similar mechanism applies to a business establishment where

 ISBN: 978-1-61208-753-5

the score will increase based on the maturity of their proof of importance starting from peer witnesses to commercial identity, etc.

Now the service providers when they would like to pull identity of an Individual or Business, they will send the request and after the consent from the Individual/Business, the selected information will be shared with the service provider to complete his/her business transactions (e.g. creating an account). In our model, scoring sensitivity would be selected by the Service Provider (e.g. banks, stocks, etc.) depending on the Service to Offer. For example, bank open accounts with score 50 and lend when the score is greater than 150. In this way everyone either small or big and regardless of their income they can be part of the network and present the proof of identity.

V. SOLUTION ARCHITECTURE

As per the segmentation, there would be two different end-users of this DKYC Model one for retail/consumer referred to as DKYC Individual and another one for Business referred to as DKYC Business. On the DKYC public chain, every Individual or Business identities represented by the unique address which will be used in the chain for the business processes interactions and workflows.

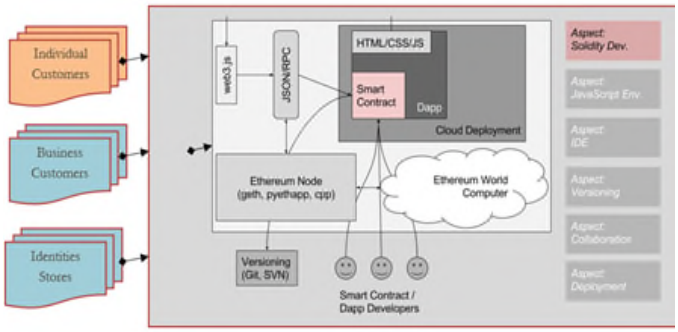

Figure 5. DKYC Solution Architecture

Proposed technology stack includes a hard-fork of the current Ethereum mainnet (development architecture illustrated in Figure 5) and adds customizations such as replacing the gas fee with the transaction-based fee which will be based on the transaction and paid by the requestor, with specific smart contracts to cover following high level use cases (listed in Table II). However, at the application layer, we will keep our development frameworks like the Ethereum development architecture (illustrated in Figure 5) where the community may use the existing platforms for dApp design, integrations, and developments. In a typical workflow, a customer will create his identity first time and pay the transaction fee for peer witnessing nodes, when the customer adds his/her fingerprint or national identity or passport, he or she will pay the verification node of civilian oracles node (onetime) and the record will be part of blockchain database. Moving forward for any network transaction the approving node will receive the benefits of service. Following are the list of Key Use Cases:

TABLE II. USE CASES

No.	Use Cases Name (Transactions Types)	Requestor
1	Customer Onboarding Use Case	Customer
2	Business Onboarding Use Case	Business
3	Verification Use Case	Any Entity
4	Risk Notifications Use Case	Customer or Business
5	Annual Profile Review Use Case	Customer or Business
6	Retire Record Use Case	Customer or Business
7	Activate Record Use Case	Customer or Business
8	Customer Consent Use Case	Customer or Business

VI. INCENTIVE MODELS

We have explored multiple incentivized business models, where CAPEX would be covered through seed funding or ICO. However, OPEX is incentivized by node subscriptions, network usage fee or extrinsic token-based fees. Figure 6 explains the key CAPEX and OPEX based models, which will be selected as per the applicable law in the jurisdiction. At the beginning of the project, CAPEX fundraising shall be done through Seed or ICO, whereas in OPEX several business model options are available such as collecting fees from nodes subscription, or charging a fee based on network usage and lastly we can also explore the applicability of fungible tokens.

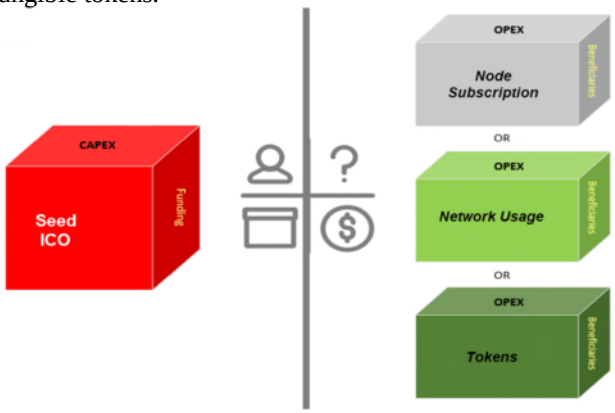

Figure 6. Incentive Approaches

VII. CONCLUSION

In our exploratory approach, we have tried to identify the core problems that current traditional KYCs databases are facing and how advances of blockchain could revolutionize the whole identity ecosystem (in trustless digital world) and bring the privacy control back to the end-users or end-customers where they will leverage the DKYC as decentralize, transparent, and trust-based know your customer. The open areas for research are; to address challenges such as fraud protection using artificial intelligence, creating the devices' identity, dApps application models, on-chain/off-chain oracles, performance and the blueprint for decentralized score-based KYC.

 ISBN: 978-1-61208-753-5

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System."

[2] KELVIN DICKENSON, "The Future of KYC – How Banks Are Adapting to Regulatory Complexity," Opus.com, 2018. [Online]. Available: https://www.opus.com/future-of-kyc/. [Accessed: 02-Sep-2019].

[3] LILY HAY NEWMAN, "How Hackers Pulled Off a $20 Million Mexican Bank Heist | WIRED," Wired.com, 2019. [Online]. Available: https://www.wired.com/story/mexico-bank-hack/. [Accessed: 02-Sep-2019].

[4] AFI, "KYC Innovations, Financial Inclusion and Integrity," no. March, pp. 1–103, 2019.

[5] Refinitiv, "KYC compliance: the rising challenge for financial institutions," p. 33, 2019.

[6] J. Parra Moyano and O. Ross, "KYC Optimization Using Distributed Ledger Technology," Bus. Inf. Syst. Eng., vol. 59, no. 6, pp. 411–423, 2017.

[7] "Product | Argos Solutions," Argos Solutions, 2019. [Online]. Available: https://argos-solutions.io/product/. [Accessed: 02-Sep-2019].

[8] KYC-Chain, "What is Know Your Customer (KYC) and how does it affect your business? - KYC-Chain," KYC-Chain, 2019. [Online]. Available: https://kyc-chain.com/what-is-know-your-customer-kyc-and-how-does-it-affect-your-business/. [Accessed: 02-Sep-2019].

[9] Tradle.io, "Tradle. Trust provisioning on blockchain.," Tradle.io, 2019. [Online]. Available: https://tradle.io/. [Accessed: 02-Sep-2019].

[10] KYC.Legal, "KYC - Blockchain user verification," KYC.legal, 2019. [Online]. Available: https://kyc.legal/faq-en. [Accessed: 02-Sep-2019].

[11] Coinfirm, "Coinfirm Reports," coinfirm, 2019. [Online]. Available: https://www.coinfirm.com/resources/coinfirm-reports. [Accessed: 02-Sep-2019].

[12] SUMSUB.COM, "5 Most Important AML Compliance Laws You Need In 2019 | SumSub.com," SUMSUB.com, 2019. [Online]. Available: https://sumsub.com/blog/aml-compliance-laws/. [Accessed: 02-Sep-2019].

[13] D. Mulligan, "Know Your Customer Regulations and the International Banking System: Towards a General Self-Regulatory Regime," Fordham Int. Law J., vol. 22, no. 5, pp. 2324-, 1998.

[14] International Telecommunications Union, Digital financial services: Regulating for financial inclusion - an ICT perspective. 2016, 2016.

[15] FATF, "Money Laundering - Financial Action Task Force (FATF)," FATF, 2019. [Online]. Available: https://www.fatf-gafi.org/faq/moneylaundering/. [Accessed: 02-Sep-2019].

[16] John Callahan, "Council Post: Know Your Customer (KYC) Will Be A Great Thing When It Works," Forbes, 2018. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2018/07/10/know-your-customer-kyc-will-be-a-great-thing-when-it-works/#47624be48dbb. [Accessed: 02-Sep-2019].

 ISBN: 978-1-61208-753-5