The DLT Way to KYC & AML Regulations

Creating a more efficient and effective regulatory system in SEA

What's the buzz about DLT?

So you know Bitcoin and Ethereum. And you know they're related to blockchain but what's this new buzzword, DLT that's floating around? Briefly put, DLT or Distributed Ledger Technology is the overarching umbrella term to describe any system that distributes data across multiple sites to reduce the risk of central storage. It simply distributes information to multiple computers, not necessarily belonging to the same owners.

It was a term that was popularized after Bitcoin gained attention as the blockchain industry transitioned from digital currencies to its underlying technology and its applications. Since then, both blockchain and DLT applications have been conceptualized to be used in various industries. For instance, pilots in payments, securities and smart contracts are being conducted by banks and industry groups. Beyond financial applications, DLT was touted for numerous other applications such as in national digital identification and supply chains.

The underlying technology behind DLT

To understand the underlying technology behind DLT, we will need to get to the history of it, one which is very much closely linked to that of blockchain.

DLT had its earliest history in the Roman Empire.[1] The Romans created a banking system that allowed people to participate in transactions across other regions belonging to the empire. Further exploration of distributed ledger in the Roman Empire came in the form of paper checks, leading to enhancements in updating and recording transactions in a ledger (where records of transactions were written).

However, the use of distributed ledger faced a problem that later became known as the Byzantine Generals Problem[2]. Consider this situation. Multiple generals are leading their respective armies and are strategically positioned outside enemy territory. Generals must communicate with messengers to form a common agreement. But what if a corrupt general conspires against the others to prevent them from reaching a common goal?

In 1993, a protocol called Proof-of-Work was invented by Cynthia Dwork and Moni Naor.[3] Proof of work had solved this problem by deterring bad actors by requiring some form of work from the service requester (the generals). This had solved the problem of the bad actor in the use of a distributed ledger. This concept was then adapted for use in Bitcoin and was popularized in the 2008 Bitcoin whitepaper where Proof-Of-Work was used as Bitcoin's consensus protocol to solve the problem of double-spending which was then a huge obstacle to the use of digital currencies/electronic cash.

Bitcoin, the only fully functional blockchain-based DLT then, sparked off other blockchain-based cryptocurrencies such as Ethereum and Litecoin and a whole new DLT industry. This concept of blockchain was then extrapolated to make it more applicable on a broader and general scale, and thus DLT was born.
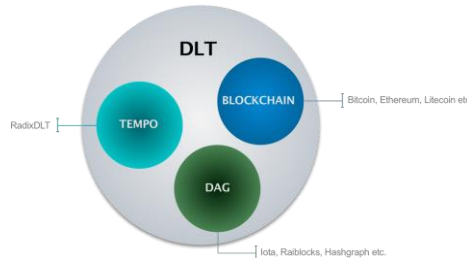
Source: Mango Research[4], 2018

There are several types of DLTs — blockchains, DAG (Directed Acrylic Graphs) and Tempo etc. Think of DLT as being the superset of blockchains and other DLT systems.

To be clear, it must be noted that there is no single, well-defined true technology behind DLT. If it is distributed and provides for a consensus algorithm to replicate the data across its nodes (users in the DLT network), it can be considered a DLT. If you're confused, just remember, all blockchains are DLTs but not all DLTs are blockchains.

DLT is simply a database that is shared, replicated, and synchronized among the members of a decentralized (not belonging to a central unit/person) network. The distributed ledger records the transactions, such as the exchange of assets or data, among the participants in the network.

Every member in this network functions as per consensus which they agree upon mutually without the interference of any third party like a governing body. Each record in the distributed ledger has a timestamp and unique cryptographic signature, thus making the ledger an auditable, immutable history of all transactions in the network. The characteristics of immutability, verifiability and cybersecurity resilience of DLT-based blockchains make it a suitable system for use in KYC and AML.

And to that, we get to the key discussion of this report, utilizing DLT-based blockchains and applying that to the field of Know-Your-Customer (KYC) and Anti-Money Laundering (AML).

What exactly is KYC & AML?

Anti-money Laundering or AML is a set of regulations designed to stop the practice of money laundering. Money launderers hide their actions through a series of steps that make it look like money coming from illegal sources was earned legitimately. AML regulations in the form of robust controls detect and deter the flow of such illicit funds through their financial systems.

KYC or Know-Your-Customer (KYC) are due diligence activities that financial institutions and other regulated companies must perform to know certain relevant information about their clients and customers. Such KYC controls would require conducting customer due diligence, determining their risk to commit money laundering, terrorism financing or identity theft and the continuous monitoring customers' transactions.

What's wrong with our current KYC & AML system?

Currently, KYC is conducted individually by financial institutions, requiring customers to provide the same information to different institutions. It is manual and paper-based, creating inefficiency. Resources are spent to validate these documents to determine the identity of the customer and the costs of adhering to KYC/AML regulations can go over $500 million for some major financial institutions, according to Thomson Reuters.[5]

Moreover, the same report found that customer onboarding time had rose by 22% just in 2016 and that was expected to increase further over the years with tighter regulations imposed by regulators. [6] Such a manual process also gives rise to inconsistent and not up-to-date information being collected by banks, making it an inefficient system for both consumers and banks.

To complicate matters, each country has their own KYC and AML requirements. Say, in our region of Southeast Asia (SEA), Thailand's KYC requirements of information required of a banking customer largely differs from that of Singapore where it is stricter. Due to this lack of standardization, complying to each request in a customized way is time consuming. To the financial institutions and fintech startups that operate across countries and regions, such differences can pose an obstacle to their growth and potential in those markets.

Despite the critical importance of these processes, KYC and AML at many financial institutions is extremely inefficient due to its time-consuming and labor-intensive manual processes, duplication of effort issues and risk of error.

Improving KYC & AML processes with DLT

These pain points have been sought to be addressed with institutions looking towards new technologies such as AI and cognitive technologies to automate such processes, and blockchain and DLT presents a compelling solution to this problem. Currently, there have been a few projects that have been undertaken to improve KYC & AML procedures efficiency and effectiveness through the use of DLT.

An aspiring case would be the Blockchain KYC Utility. It was envisioned in a proof-of-concept by a collaboration between a consortium of three banks in Singapore (HSBC, OCBC, Mitsubishi UFJ Financial Group) and KPMG and Bluzelle Networks as well as Info-communications Media Development Authority.[7] The Blockchain KYC Utility aims to reduce inefficiencies and duplication of effort in KYC information gathering between legal financial entities in Southeast Asia. The prototype of the Blockchain KYC platform was tested and the proof-of-concept was able to

demonstrate the utility's functionality, security, and scalability successfully.

To examine how exactly this Utility can improve KYC procedures, a break-down of the typical KYC requirements is necessary. We take the example of Singapore's requirements set by Accounting and Corporate Regulatory Authority for Singapore (ACRA)[8]. The general requirements are:

1. **Implement** clear internal procedures and policies to adhere to AML rules
2. **Assess** risk when acquiring a new customer
3. **Conduct** initial due diligence on customers if there are doubts on authenticity of identity of the customer
4. **Monitor** customers' transactions to ensure that they are in line with their known information
5. **Keep** and maintain a record of such information for regulatory reporting

The Blockchain KYC utility uses the model of a shared setup between a central entity like regulators and other entities such as banks. The central entity would take care of storing the details while the banks would plug into the system to access that information, creating an unified KYC platform.
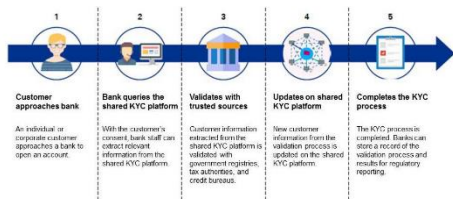
Source: OCBC Bank[9], 2017

To illustrate how this utility would work, we take the case of onboarding a new consumer banking customer.

(1) The customer approaches the bank to open an account.
(2) With their consent, the bank then taps on to the blockchain KYC platform to extract relevant information,
(3) This information is then validated with the relevant parties: government authorities and credit bureaus.
(4) The customer's updated and validated information would then be updated on the blockchain.
(5) The KYC process is complete, and banks store a record of the validation process and results for regulatory reporting.

Each new transaction of a customer monitored by any one of the participating member of the network can then be placed into the shared ledger which other institutions can rely on for the latest information about the customer.

Say, the customer then goes to the next bank and sign up for a new credit card, assuming the bank is part of the Blockchain KYC Utility network, the bank undergoes the same process and now extracts the most updated version of its information (previous bank's verified version).

Using this unified DLT-based blockchain, entities operating within the network can generate greater operational efficiency in requirements 2 to 5 of the typical KYC process. Customer onboarding time will be reduced, and banks can allocate more resources to the analyzing of data rather than collecting and verify the data received. Furthermore, suspicious activities can be more easily detected and highlighted to all network members where it would be flagged for further investigations in accordance to AML laws.

But, that's not all, using DLT solutions comes with additional benefits. Permissioned DLT offers immutability and verifiability while promoting higher security resilience over traditional centralized eKYC platform.

Blockchain KYC's Benefits Over Centralized eKYC Platforms

Firstly, it is **immutable and verifiable**, meaning that once information has been recorded on a blockchain, no one can change it. This prevents bad actors from manipulating or falsifying the data, ensuring the integrity of the data and providing an audit trail that is trustable for regulators to verify.

Second, this blockchain KYC Utility is **permissioned** — only approved entities can run nodes on the network where they can access/push information onto the network with legitimate authentication. This maintains the confidentiality of the data on the network and prevents tampering by third parties.

Third, it provides higher **security resilience** over traditional centralized eKYC platforms using cryptography in DLT-based blockchains. The access to the network is divided into 2 keys: public and private. The private key provides ownership authentication and the elimination of a need for sharing more personal information than necessary, providing more security. The public key then provides the access to the network to participate in events to retrieve/add/validate digital events on the network.

Implementation on A Global Level: R3 Corda

Beyond a regional level, such a compliance system can be implemented even on a global level. Enterprise blockchain software firm, R3 announced the completion of a KYC application trial built on their Corda blockchain platform where a total of 39 firms from 19 countries(the likes of BNP Paribas, SBI bank and Société Générale) participated in the trial.[10] Banks were able to request customers' KYC test data and customers were also able to update their information and approve or revoke access requests by banks. Like the Blockchain KYC Utility, the unified platform provided an up-to-date, immutable and validated customer information.

Opportunities of Combining Technologies

As the implementation is still nascent, further opportunities to combine this solution with other emerging technologies such as smart contracts or AI can be foreseen. For instance, a DLT utility

could be embedded with 'smart-contracts' with inbuilt algorithms that would allow financial institutions to directly parse data through an AML engine, automating the filtering of suspicious activities in accordance to AML regulations, providing even greater efficiency and lesser friction in the monitoring process (requirement 4 of the KYC).

We also foresee such a comprehensive DLT being used to standardize and kick off adoption of a global regulatory framework governing KYC and AML. Such frameworks could prove relevant in combatting KYC/AML issues spanning different countries. For instance, the Panama Papers investigations for tax fraud could have benefited from such a blockchain KYC platform.[11] Banks had a hard time handing KYC information as those information were dispersed over multiple banking systems. Regulators also could not confirm the veracity of the data. The trustability and standardization of KYC documents offered with a blockchain KYC registry would have enabled accurate and easy access to documents regulators required.

Challenges of Implementation

From a customer standpoint, customers may have privacy concerns over the sharing of their personal and financial data without their consent. However, this can be overcome with a digital approval layer added onto the blockchain such as using OTP to permit requests by banks.

On an international level, it must garner the cooperation and partly/mainly driven by the regulators. Regulators must then also converge on the standards of KYC & AML regulations to be adhered to by participating members of the network.

There is also the question of liability: who will be responsible should there be losses arising from errors or weaknesses. While blockchain and DLT systems themselves have proven to be secure and resilient. The participating banks(nodes) are prone to hacking threats, where if compromised can cause losses and damage to the integrity of such a system. In this case, who should be liable?

Where does this future lie?

Beyond the hype of cryptocurrencies, blockchain and DLT display a very promising use case in the field of KYC and AML. Current developments like the Blockchain KYC Utility in SEA and R3 Corda KYC trial looks promising.

However, a good DLT utility by itself does not automatically solve all the KYC/AML issues faced by financial institutions today. It must be coupled with a concerted effort and will by regulators globally to adopt and use the system. And if it proves successful, the idea of a self-sovereign identity where people manage their own personal information will become a reality.

We are hopeful that DLT & its blockchain spin-offs can deliver a more effective and efficient KYC/AML regulatory environment on the national, regional and global stage.

Contact: Gabriel Tan, Research Director
yhtan.2017@business.smu.edu.sg

Sources:

[1] Before Blockchain, There Was Distributed Ledger Technology (2018, September 6). Retrieved from https://medium.com/blockstreethq/before-blockchain-there-was-distributed-ledger-technology-319d0295f011

[2] The Byzantine Generals Problem (1982, July). Retrieved from https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf

[3] Pricing via Processing or Combatting Junk Mail. (n.d.). Retrieved from http://www.hashcash.org/papers/pvp.pdf

[4] Blockchain vs DLT. (2018, Feb 20). Retrieved from https://www.mangoresearch.co/blockchain-vs-distributed-ledger-technology-dlt/

[5] Callahan, J. (2018, July 10). Know Your Customer (KYC) Will Be A Great Thing When It Works. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/07/10/know-your-customer-kyc-will-be-a-great-thing-when-it-works/#dd3fecc8dbb9

[6] Cost of Compliance 2017 Report. (n.d.). Retrieved from https://risk.thomsonreuters.com/en/resources/special-report/cost-compliance-2017.html

[7] Could Blockchain be The Foundation of A Viable KYC Utility. (n.d.). Retrieved from https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/03/kpmg-blockchain-kyc-utility.pdf

[8] New KYC Regulations for Corporate Service Providers. (n.d.). Retrieved from https://www.startupdecisions.com.sg/singapore/company-law/acra-regulations-customer-kyc/

[9] OCBC Bank, HSBC and MUFG, together with the Infocomm Media Development Authority, complete proof-of-concept on ASEAN's first industry Know Your Customer blockchain (2017, October 3). Retrieved from https://www.ocbc.com/group/media/release/2017/ocbc-hsbc-mufg-kyc-blockchain.html

[10] 39 firms complete global trial of KYC on Corda blockchain platform (2018, June 28). Retrieved from https://www.r3.com/news/39-firms-complete-global-trial-of-kyc-on-corda-blockchain-platform/

[11] Distributed Ledger Technology and Blockchain (2017). Retrieved from http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf