Chapter 2
A Survey of KYC/AML for Cryptocurrencies Transactions

Suzana M. B. M. Moreno
Brazilian Development Bank, Brazil

Jean-Marc Seigneur
University of Geneva, Switzerland

Gueorgui Gotzev
Kohler Gotzev, S.àr.l. - Avocats à la Cour, Luxembourg

ABSTRACT

KYC (know your customer) and AML (anti-money laundering) practices have been designed and implemented in traditional financial transactions for some years now. However, it has been complicated to find a balance between business efficiency, innovations, financial inclusion, and compliance, both in the specification of what should be done and in the implementation of a risk-based approach that satisfies the required specification during real business operation. This chapter presents a survey of traditional practices to KYC/AML, highlighting a subset of existing challenges in these practices, taking into consideration the innovation of cryptocurrencies transactions and related innovations, such as digital identity, and the financial inclusion of unbanked people without identity papers. The authors finish this chapter by discussing existing solutions to these challenges both by adopting new KYC/AML practices and by using innovative technological solutions.

INTRODUCTION

A financial system consists of institutional units and markets that interact, typically in a sophisticated manner, for the purpose of mobilizing funds for investment, and providing facilities, including payment systems, for the financing of commercial activity (*The OECD Glossary of Statistical Terms*, n.d.). The sources of national or international money transactions in a financial system may come from legitimate or illegal economic activities. Money laundering is the process of making money generated by criminal

DOI: 10.4018/978-1-7998-5728-0.ch002

activity appearing lawful by using the financial system. The United Nations Office on Drugs and Crime estimated in 2013 that between 2% to 5% of global gross domestic product (GDP) per year is a result of money laundering and less than 1%, probably around 0.2%, is seized and frozen (UNODC, 2011). Besides, other crimes like tax evasion, sanctions evasion, frauds, and terrorism financing may also happen in the financial system.

Advances in financial information and technology enable money to move around the world quickly. These advances bring benefits to society and help to prevent nefarious purposes, but they also introduce new types of risks. For example, the use of the Internet made financial systems more efficient. At the same time, it also introduced new kinds of crimes, i.e., cybercrimes such as attacks on online banking or credit card frauds.

After analyzing its 2018 statistics (*Shaping the Future of Payments*, 2019), the Bank for International Settlements (BIS) concluded that domestic payments are becoming more convenient, instantaneous and ubiquitous because of innovation in the financial industry and their adoption by consumers. At the same time, BIS concluded that the use of cash is still significant. Still, it is increasingly seen as a way to store value rather than making payments.

Blockchain (Nakamoto, 2008) is a foundational technology able to cause substantial changes in many sectors, including the financial one. Cryptocurrencies enable fast, global reach, peer-to-peer transactions with different levels of anonymization. These innovations can undoubtedly create new or more efficient business models with many benefits to society. Still, they may also be used to conduct illegal activities like dark market payments and digital transfer of money associated with malware and ransomware attacks. According to ChainAnalysis (Chainanalysis, 2020), illicit transactions still make up a small share of all cryptocurrency activity at just 1.1% at the time of writing. However, the report also states that nearly all dark market commerce, from illegal drugs to weapons and sensitive personal information, is transacted in cryptocurrencies. ChainAnalysis estimates that the total cryptocurrencies sent and received by illicit entities summed up to more than $10 billion in 2019.

Before converting cryptocurrencies involved in crimes into fiat money that can be used in real life, it is necessary to hide their origins with money laundering. Unfortunately, there are sophisticated solutions to help criminals to achieve their goal, which imposes new challenges to regulators. Some examples are mixers, chain hopping, privacy coins, and anonymous peer-to-peer exchanges (Chainanalysis, 2020).

At the same time, many countries in the world have tried to enforce the identification of the payers and payees as well as of the source of the transferred money to protect the international financial system from misuse. These countries have even tried to force other countries to do so to prevent criminals or terrorists from seeking out and exploiting jurisdictions with weak or no supervision.

Nowadays, there are national and inter-governmental initiatives focused on minimizing the risk of criminal activities in the financial system.

This paper discusses past and current practices of KYC (Know Your Customer) and AML (Anti-Money Laundering). It explores the new challenges introduced by cryptocurrencies transactions and possible future practices. The remainder of this chapter is structured as follows. Section 2 presents essential concepts and the current KYC/AML practices in traditional financial institutions. Section 3 discusses the issues in these current practices of KYC/AML. In Section 4, we discuss our potential solutions and recommendations. Finally, Section 5 presents our future work and concludes this survey.