A Survey of KYC/AML for Cryptocurrencies Transactions

Mesquita Borba Maranhao M, Suzana; Seigneur, Jean-Marc; Gotzev, Gueorgui

How to cite

MESQUITA BORBA MARANHAO M, Suzana, SEIGNEUR, Jean-Marc, GOTZEV, Gueorgui. A Survey of KYC/AML for Cryptocurrencies Transactions. In: Handbook of research on cyber crime and information privacy. Maria Manuela Cruz-Cunha and Nuno Mateus-Coelho (Ed.). Hershey : Information Sci Refer IGI, 2021. p. 21–42. doi: 10.4018/978-1-7998-5728-0.ch002

This publication URL: https://archive-ouverte.unige.ch/unige:150576
Publication DOI: 10.4018/978-1-7998-5728-0.ch002

A Survey of KYC/AML for Cryptocurrencies Transactions

Suzana Maranhão Moreno,
Brazilian Development Bank, Brazil

Jean-Marc Seigneur,
University of Geneva & Reputaction, Switzerland & France

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. We finish this chapter by discussing existing solutions to these challenges both by adopting new KYC/AML practices and by using innovative technological solutions.

Keywords: Compliance, Financial Industry, Cryptocurrency, Blockchain, Virtual Assets, Virtual Asset Service Provider, KYC, AML, Identification, FATF, Financial Inclusion.

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 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.

BACKGROUND

This section introduces essential concepts like KYC, AML, FATF, and digital identity. It also presents current KYC/AML practices in traditional financial institutions. Finally, it gives the details of a standard cryptocurrency transaction.

KYC (Know Your Customer)

KYC is a process to identify and continuously verify customers during the business relationship with a financial institution with a primary goal to comply with a set of regulatory requirements.

The data collected from a client in a KYC process may vary a lot depending on the financial institution, the regulations that the financial institution must comply with, and the risks involved in the relationship with the client. Two examples of data that is usually associated with KYC are proof of identification (ID) and proof of address. Moreover, as part of the KYC process, the ID proof may be used to check that the client does not belong to any list of sanctions or that the client is not a Politically Exposed Person (PEP). The process of KYC might also include the monitoring of client actions during the business relationship to continuously collect sources of risks of financial crimes. Corporate KYC (also called as KYB – Know your Business) should involve analysis in the business itself and on its owners, being all of them or the main ones. In both cases, individual or corporate, the financial institution may need to recheck some client data after some business events or periodically.

In some cases, KYC follows a tiered approach, in which higher-risks clients require more effort on identification and verifications. For example, a bank may create levels of KYC based on how much money a client may transact or how much money the client may withdraw in one day. In this case, lower limits of daily transactions are associated with lower risks to regulations and, as a consequence, lower KYC requirements.

KYC is essential to regulation since financial institutions need to prevent crimes like identity theft and other crimes. A failure to implement safe requirements may result in possible fines, sanctions, and reputational damage to the financial institution. KYC also brings benefits to the institution itself because it helps to prevent fraud and losses resulting from illegal funds and transactions. The process of KYC may use physical or digital channels, sometimes called eKYC. As in other domains, digital channels may help to lower costs and increase efficiency and traceability.

AML (Anti-Money Laundering)

Criminals need to find a way to control their illicit funds without attracting attention to the underlying activity or the persons involved. Therefore they seek to create a plausible explanation about how the money was earned. Money laundering consists of the actions that criminals carry out to disguise their illegal money origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardizing their source (*FATF-GAFI - Financial Action Task Force*, n.d.).

It is familiar to breakdown the money laundering in three phases. The first one is called placement: it is when the illegal money enters in the financial system. It can happen, for example, by making small deposits

in different accounts or by buying monetary instruments. The goal of the second phase, called layering, is to give the money a lawful appearance by using conversions and movements. For example, the funds can be moved to jurisdictions that do not co-operate in anti-money laundering investigations. The criminal may also spread the amount of money by transferring parts of it to banks in several jurisdictions. In the digital world, it may involve converting between fiat money and cryptocurrencies as well as between one cryptocurrency into another. The first and second phases may be intertwined in some situations. For example, the criminal may fake the payments from unreal clients in a legal business that deals with many cash payments. In this case, the work to give a lawful appearance to the money happened before it enters in the financial system. Integration is the name of the third stage: when the criminal can spend the money in the real economy. It is the time when the criminal can buy goods or services and invest in new businesses.

Money laundering is considered a crime because it rewards criminals. Fighting money laundering is a way to prevent criminal organizations from profiting. Considering how money laundering works, criminals can exploit jurisdictions with fragile controls and with difficulties in preventing or detecting the crime. Governments should provide the necessary tools to the authorities charged with combating the problem and regulate the private sector to ensure cooperation. But it is not enough: international cooperation is fundamental to harmonize the national initiatives and ensure inter-country collaboration to deal with these global criminal activities.

Anti-money laundering is a set of laws, regulations, and procedures intended to prevent money laundering and maintain secure financial institutions.

FATF (Financial Action Task Force)

The Financial Action Task Force (*FATF-GAFI - Financial Action Task Force*, n.d.) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The body was established in 1989 by the Ministers of its member jurisdictions and has nowadays the support from more than 200 jurisdictions.

The FATF has developed a series of recommendations that are recognized as the international standard for combating money laundering and other related financial crimes. They form the basis for a coordinated response to these threats to the integrity of the financial system and work to stimulate the necessary political will to promote national legislative and regulatory reforms in these areas, which includes:

- establishing powers and responsibilities for the competent authorities;
- enhancing the transparency and availability of beneficial ownership information of legal persons and arrangements;
- facilitating international cooperation.

FATF recommendations include preventive measures that apply to traditional financial systems, virtual asset service providers (which are called VASP), and designated non-financial businesses and professions (like casinos, real estate agents, dealers in precious stones, and others). Countries should promote measures to make these recommendations a reality in the public and private sectors.

Because countries have diverse legal, financial, administrative, and operational frameworks, they cannot all take identical measures to follow FATF recommendations. There is room for flexibility to the country's reality when applying these recommendations. FATF suggests a risk-based approach (RBA), which means that countries, competent authorities, and banks should identify, assess, and understand the money laundering and terrorist financing risk to which they are exposed, and take the appropriate mitigation measures corresponding to the level of risk. The risk-based approach is central to the effective implementation because it allows the prioritization of resources to the most critical cases.

FATF monitors the progress of its members in implementing necessary measures and, in cooperation with other international stakeholders, works to identify national-level vulnerabilities.

It is essential to highlight that FATF 40 recommendations (FATF, 2019) do not mention the term KYC. Instead, the document defines the term Customer Due Diligence (CDD) in Recommendation 10. The authors assume that the CDD practices are similar to KYC but applied in the context of AML. For example, according to FATF, CDD should be performed when establishing business relations; carrying out occasional transactions; there is a suspicion of money laundering or terrorist financing; or the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

Digital Identity

Many human activities require personal identification, for example, to create a bank account, to study in a university, to buy an apartment, to travel abroad… Governments usually identify their citizens issuing official documents printed on papers, e.g., birth certificate, social security number, driver license, electoral id, passport…

With the development of digital services, there is also the need to identify online users remotely. There are many ways to create a digital identity. The first one is to create a simple account on a Website with a username, email and password, which leads to a proliferation of users and passwords. New solutions to manage this complexity are then created, such as passwords managers. Another way is to use an online identity provider to represent the user identity in other online services. A third way is to use an official digital identity issued by the government, like the Aadhaar service provided by the Unique Identification Authority of India (*UIDAI*, n.d.). A final way consists of using asymmetric encryption technology to link a digital signature to a real identity. In general, it uses digital certificates issued by a certified authority, like X.509 (*X.509 : Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certificate Frameworks*, n.d., p. 509). A certified authority may be more or less trusted depending on if it is accredited to operate in a specific jurisdiction and it follows a particular regulation. A regulation example that uses the concept of digital certificates is the Electronic Identification and Trust Services Regulation – eIDAS (*EIDAS-Ecosystem*, n.d.) used in the European Union.

Most solutions only use digital information, but a few also use physical information. To get an Aadhaar ID, the citizens have to visit a specific center, present their documents, and some of their biometrics are collected. Some certified authorities may also require that they visit a physical place to receive the certificate. The additional information about the person collected in the real world contributes to increasing the level of trust in the identity, by linking the real identity with the online identity.

A digital identity may also be assigned to legal entities, for example, by creating an online account for the legal entity or by getting a digital certificate issued to the legal entity to prove the ownership of a Website via HTTPS.

Traditional Practices of KYC/AML

Banks and other financial institutions need to comply with their national and regional regulation to be allowed to operate. They also need to comply with their partners' regulatory requirements to do business together. The average bank spends around US$48 million per year. In the US alone, banks are spending more than US$25 billion a year on AML compliance (*Combating Financial Crime - KPMG Global*, 2019).

If the institution needs to comply with laws that follow FATF regulation, it will need to apply the preventive measures described by FATF (FATF, 2019) following the risk-based approach described in recommendation 1. Examples of variables that impact the risk are: (a) jurisdiction(s) involved in the transaction, (b) the total amount of the transaction, (c) purpose and intended nature of the business relationship involved in the transaction. The practices, which are most relevant to the subject of this chapter, are related to FATF recommendations 10, 14, 15, and 16 because they are directly impacted by the cryptocurrency innovation.

Recommendation 10 describes when financial institutions should be required to undertake customer due diligence and what measures should be taken. It includes the identification and verification of the customer, the identification and reasonable measures to verify the beneficial owner, the verification if any part of the transaction is a Politically Exposed Person (PEP) or if he/she is part of any sanction list, information on the purpose and intended nature of the business relationship with ongoing re-evaluation. Depending on the risk assigned to the transaction, it may also include additional information about the customer, e.g. source of funds or volume of assets, as well as about the relationship and others.

It is interesting to note that, according to FATF, there is no enforcement to use official documents when performing a compliant CDD. This flexibility is advantageous in at least two scenarios. The first one is financial inclusion because unbanked in under developed countries may not have the necessary documents. The second scenario is to enable the use of new payment methods (NPM) on a global scale without asking the provider the complex task of ongoing verification of documents issued by different countries.

Recommendation 14 states that natural or legal persons that provide money or value transfer services (MVTS) should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance. FATF recommendation 15 is detailed in the section below on solutions and recommendations. FATF recommendation 16 indicates that, if a wire transfer meet some criteria, for example, it is a cross border wire transfer higher than USD/EUR1000, financial institutions should include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.

It is worth to mention here the importance of the SWIFT system (*SWIFT - The Global Provider of Secure Financial Messaging Services*, n.d.) because it can be used to exchange these messages in a payment chain. SWIFT's messaging services are used by more than 11 000 financial institutions in more than 200 countries and territories around the world. It carries over five billion financial messages a year. Through SWIFT,

banks, custodians, investment institutions, central banks, market infrastructures, and corporate clients can connect with one another, exchanging structured electronic messages to perform common business processes, such as making payments or settling trades.

In addition to the main recommendations, the FATF issued a report in 2010 about money laundering using NPM (FATF, 2010) like prepaid cards, Internet payment systems, and mobile payment systems. The report discusses how anonymity, high negotiability, and utility of funds, as well as global access to cash through automated teller machines (ATMs) are parts of the major factors that make NPMs attractive to money launderers. One mitigation of such risks is the value limits on transaction amounts or limits on frequency in the use of these payments. To the best of our knowledge, there is no standard limit defined in FATF for NPM or even for regular cash withdrawal using ATMs. Therefore, each country and financial institution must set its limits considering its risk-based approach.

Basic Cryptocurrency Transaction

The first cryptocurrency based on a blockchain is Bitcoin (BTC), proposed by Satoshi Nakamoto (Nakamoto, 2008) whose real-world identity is unknown. Blockchain technology is part of Distributed Ledger Technologies (DLT).

A blockchain may be seen as a decentralized public ledger, which is maintained by lots of entities decentralized over the world in a peer-to-peer way. An attack-resistant consensus algorithm (Gray et al., 2006; J.-M. Seigneur, 2005b) must be used to synchronize the state of the ledger among all those remote entities. There are four main types of consensus algorithms used in DLTs:

1. The first one is based on Proof-of-Work (PoW) where some peers run a full node that spends energy to solve computationally intensive problems called mining. Nobody can control the ledger if it has less than 50% of the mining power, which is a very costly attack at the time of writing. Each time a peer finds the solution to one of these problems, the peer is eligible to insert valid transactions into a new block and propagate this new block to other peers. The next block is linked to the previous block because it must contain the hash of the hashed content of the previous block. Thus, all blocks are linked together. Thus, it would be even more expensive to succeed in changing the content of older blocks.
2. The second type of conventional consensus algorithm used in blockchains is based on a variant of Byzantine Fault Tolerance (BFT) (Lamport et al., 1982; Yin et al., 2019). However, BFT-based blockchains aren't fully decentralized because they usually require choosing a few peers acting as generals in the peer-to-peer system, which resists to attacks up to less than one-third of compromised/faulty generals.
3. Due to the energy cost of PoW blockchain, several blockchains try to use a variant of Proof-of-Stake (PoS) where the entities who stake more coins have more chances to become the next validator and earn the fees associated to the new transactions to be validated. If the validator has cheated, then the coins at stakes may be lost. For example, Ethereum (Buterin & others, 2013), one of the significant decentralized application development platform (Ethereum Project, n.d.), has tried to move from PoW to PoS for several years and hasn't yet done so at the time of writing, partly due

to the uncertainty of PoS attack-resistance. The attack-resistance of PoS, as in any decentralized trust system where multiple virtual identities can be created at will (Jean-Marc. Seigneur et al., 2005), is difficult to estimate because there are many different types of attack scenarios: Sybil attack (Douceur, 2002), collusions/cartels…

4. Finally, there are DLT systems not based on blockchains, which are then very different than a blockchain. Instead of being based on a blockchain, the DLT may use a Directed Acyclic Graph (DAG). IOTA (Popov, 2016) has been one of the significant DLT based on a DAG. IOTA attack-resistance has been challenged several times (Narula, 2017; Wright, 2020), and it still relies on a centralized coordinator at the time of writing. Another major DAG is Hedera Hashgraph (Baird, 2016), which is governed by a consortium (J.-M. Seigneur, 2005a) of well-known and diverse big companies and organizations around the world.

Anyway, in most of these DLT, the accounts of the real-world users aren't formally linked to their real-world identity but to an account identifier acting as a pseudonym (J.-M. Seigneur, 2005b). Because the ledger is most of the time public, the transactions aren't anonymous: each transaction is linked to the pseudonyms accounts involved in the transaction. Chaum proposed the first attempt for untraceable digital payments based on blind signatures (Chaum, 1983), but some components were still centralized. More recently, he has tried with colleagues to merge blockchain (Chaum et al., 2016; Praxxis, n.d.). Several cryptocurrencies have also been created with anonymization techniques to guarantee anonymity such as Monero, ZCash, or Dash, but regulators over the world have put pressure on the exchanges to delist these anonymous cryptocurrencies (Buntix, 2018).

Blockchains, thanks to reaching consensus and synchronizing to the same state among all peers, assuming their level of attack-resistance isn't reached, e.g., 51% in Pow and one third in BFT, succeed in protecting against double-spending of the same cryptocurrency coins or amount from one account. Besides, thanks to asymmetric cryptography, which is used by all the DLT surveyed above, it is not possible for an attacker to forge transactions from one account to another because the attacker doesn't have the private key to sign the transactions. Once a master node or general receives a transaction to be inserted in the blockchain, it checks if the signature is valid or not. If not, the transaction is discarded. When a keypair is generated by an asymmetric cryptography algorithm (Gardner, 1977), the user obtains a private key, which is used to sign transactions and must be kept secret, and a public key, which is used to generate a short identifier for the account and can be shown publicly to receive funds on that account. Although quantum computing may break some asymmetric encryption algorithms (Perlner & Cooper, 2009), a few are still considered safe at the time of writing. Different hashing algorithms exist to derive a short name, called generally a hash, from a public key (Bakhtiari et al., 1995). A short name is easier to pass to others. However, it is still not considered as user-friendly because the list of characters means nothing, and it is easy to make a mistake when writing down this list of characters. Copy and paste or the scan of a QRCode are recommended if available. Some blockchain companies also try to provide a decentralized name service, similar to the Internet DNS transforming challenging to remember IP addresses to domain names, and in the case of blockchains transforming blockchain addresses to easy to remember domains names, e.g., (*Ethereum Name Service*, n.d.; *Unstoppable Domains*, n.d.). The problem with such decentralized name services to reach mass adoption is that they must convince all browsers and crypto-wallets to use their system.

PROBLEMS IN CURRENT PRACTICES OF KYC/AML

A crucial issue regarding KYC/AML in cryptocurrencies transactions is that users can create their accounts by just running the asymmetric encryption algorithm on their local computer. Traditionally, banks are required to create an account, and they can enforce KYC/AML before the account is created. In the best case, the account, which has been created by the user with the asymmetric encryption algorithm, is based on a public blockchain without anonymization techniques. In this case, each transaction between accounts can be tracked. However, as said above, the real-world identity isn't known. All users don't know how to use asymmetric algorithms, but several cryptocurrencies wallet applications exist to make the process very easy via a few clicks on the wallet graphical user interface (GUI), for example, My Ether Wallet (*MyEtherWallet.Com*, n.d.).

Once a cryptocurrency account is created, there is still the issue of the initial allocation of coins and amounts to these accounts. In Bitcoin, the miners who find the solution to the current problem have the right to build the new block and propagate it to the other peers. In the process, the transactions fees and a mining reward are gained by the miner. There are only 21 million Bitcoins in total. Thus, at some stage, only the transaction fees may remain. The miners account, once it has been rewarded with Bitcoins, can then sell their Bitcoins to other users and sign transactions to transfer those Bitcoins to the buyers accounts. Ethereum initial token allocation is a mix between mining fees/rewards and initial coin offering (ICO) (Venegas, 2017).

An ICO is run at the beginning of a new project, which proposes to create a new cryptocurrency and sell an amount of this new cryptocurrency coins for other cryptocurrencies or fiat money (USD, EUR…) (Jean-Marc Seigneur et al., 2017). The sale of the new cryptocurrencies coins is usually limited to a short period of time to attract potential investors who may otherwise wait to buy those cryptocurrencies coins. The project may communicate that the raised funds will be used for development, but many projects haven't done what they promised due to poor operations or they even scammed the investors (Zetzsche et al., 2017). Some ICO investors haven't received any cryptocurrencies because there was no automated mechanism in place to force the cryptocurrencies creators to send them the correct amount of bought cryptocurrencies. Other ICOs have used automated mechanisms to deliver the correct amount of cryptocurrencies based on the sent cryptocurrencies. Those automated mechanisms are often called "smart contracts" (Szabo, 1997). Initial ICOs, such as Ethereum's one, didn't enforce KYC, not even speaking about AML. At the end of 2017, regulatory pressure was higher, and KYC started to become part of most ICOs. However, KYC quality of most of these ICOs may not have been sufficient because most of them were just providing a way to upload the photo of an identity document, which also created risks of identity documents leaks due to poor security management by the ICOs creators.

To further facilitates mass access to cryptocurrencies and their trading, online cryptocurrencies exchanges have been created (Janze & Gvozdevskiy, 2017). The user can easily create an account on a Website and then buy cryptocurrencies via credit cards or bank transfers to the exchange bank accounts. The users may also send their cryptocurrencies to their account on the cryptocurrency exchange. Unfortunately, in this case, the cryptocurrency exchange is generally the owner of the private key associated with the user's account on the exchange Website. If the cryptocurrency exchange is hacked or disappears, the users lose their cryptocurrencies. Several cryptocurrency exchanges have been hacked in the past (Chohan, 2018). For example, the Mt. Gox cryptocurrency exchange that handled around 70% of Bitcoin transactions in 2014 closed after being hacked. Again, initially, the cryptocurrencies exchange didn't carry out proper KYC

checks. At the time of writing, there are still several exchanges that do not enforce KYC appropriately concerning FATF recommendations. For example, Binance (*Bitcoin Exchange | Cryptocurrency Exchange*, n.d.) is the cryptocurrency exchange with a large part of the cryptocurrencies transactions, but only requires KYC above 2 BTC withdrawal per day and has been hacked in 2019 (Ćirić & Ivanišević, 2018).

Regarding the issue of private keys owned by the cryptocurrencies exchanges, a new generation, called decentralized exchanges (DEX), has been created. The first DEX iterations were slow, difficult to use, and with low liquidity, but next iterations are improving. Nash (Nash | Trade. Pay. Invest., n.d.), for example, is even a DEX regulated in the EU, with KYC/AML and user-friendly interfaces. Nash liquidity is still low, though. One reason may be that its users have to pass a mandatory KYC. Other examples are Binance DEX or Komodo DEX (*Komodo - An Open, Composable Smart Chain Platform*, n.d.), which is even working as a smartphone application (Decentralized Exchanges, 2019). It may be harder to sue cryptocurrencies DEX for lack of KYC/AML because they do not own the private keys and are only a layer to facilitate transactions. If the DEX is provided as a Website or a mobile application on an official applications store, their liability is more important than if they only offer an open-source, peer-to-peer software that can be run locally by users. When they support a service on a Website or via an application connected to their servers, they are responsible for the provided service, which cannot exist without the Website or the mobile application available on the applications store. A final way for users to exchange crypto-currencies is via Over The Counter (OTC) transactions (Nezamaikin & Zbirovskaya, 2019). There are different types of OTC solutions via an OTC facilitating desk acting as an escrow or directly between the seller and buyer, which may be risky. On the one hand, the payer may not pay after receiving the cryptocurrencies or use fake or laundered money. On the other hand, the buyer may not receive the cryptocurrencies after payment. There is also the issue of finding potential buyers and sellers. It is the reason that OTC Website listings have appeared, such as LocalBitcoins (*LocalBitcoins.Com: Fastest and Easiest Way to Buy and Sell Bitcoins*, n.d.). On Paxful (*Buy Bitcoin Instantly | Paxful*, n.d.), Bitcoins may also be purchased or sold thanks to gift cards. Generally, most retail OTC users do not spend time and money checking KYC/AML if they are not forced too. A final way to withdraw Bitcoins anonymously in exchange of cash is to use crypto ATMs. For example, in Switzerland, at time of writing, it is still possible to buy or withdraw Bitcoins up to 5000 CHF per transaction without KYC with Bity crypto ATMs (*Bitcoin and Cryptocurrency ATMs in Switzerland*, n.d.).

Financial Inclusion

2.5 billion people, half of the world adult population, lack a bank account. These are low income, rural, migrant, and undocumented persons who have been underserved or excluded from the formal financial sector. Financial inclusion is a way of ensuring access to appropriate financial products and services at an affordable cost, fairly and transparently and subject to adequate regulation in line with the FATF recommendations (FATF et al., 2013).

Financial inclusion and an effective AML regime can and should be complementary national policy objectives with mutually supportive policy goals. If carefully designed, measures, which ensure that more clients use formal financial services, increase the reach and effectiveness of the AML controls (Bester et

al., 2008). If those measures are not carefully designed, AML measures can negatively affect access to, and use of, financial services (Isern & Koker, 2009)

FATF stated that underserved clients represent a very heterogeneous category with very different risk profiles in different jurisdictions. As a consequence, they cannot be classified as lower risk clients solely on the basis that they are low-income individuals. A typical risk of these clients is that they can act as a straw man, facilitating the use of their account to third-party illegal actions. On the other hand, there is an explicit example of a low-risk scenario in FATF recommendation: "financial products or services that provide appropriately defined and limited services to certain types of customers, to increase access for financial inclusion purposes" (FATF et al., 2013).

Rigid CDD requirements that insist on government-issued identification documents, adopted by some countries or financial institutions, have acted as barriers to disadvantaged populations obtaining access to the formal financial system (FATF et al., 2013). Research from the World Bank determined the following barriers together with the following percentual of non-account holders reporting each barrier as a reason for not having an account: not enough money (30%), too expensive (25%), family members already have an account (23%), too far away (20%), lack of necessary documentation (18%), lack of trust (13%) and religious reason (5%). In Sub-Saharan Africa, for example, documentation requirements potentially reduce the share of adults with a bank account by up to 23% (Demirgüç-Kunt & Klapper, 2012). It means that new solutions, more affordable, more accessible – perhaps by using digital channels - and that minimize the need for formal documents seem to be valuable to financial inclusion.

Privacy Issues

KYC/AML practices need to store, process and share data to calculate the risk degree of a client or a transaction. The overall result of these practices is that the collected data in one organization can be distributed to many financial and government institutions for future processing and evaluation.

According to Hughes (Hughes, n.d.), there are varying degrees of privacy protections offered by different countries. Some countries provide little to no protection, while others provide complex, comprehensive privacy schemes. The type of data being protected, along with the definitions of data type, can also vary too. In some countries, data privacy protections are explicitly spelled out by statute. In other ones, data privacy protections are derived from their general constitutional privacy guarantees.

Even if we consider these differences, there is no doubt that there is personally identifying information (PII) involved in KYC/AML because there is the collection of proof of identity of people. In this sense, there is a conflict with the privacy laws, which call for minimizing the collection and processing of personal data. One could argue that these practices are considered as "important reasons of public interest". Still, it is not clear how to deal with it even in GDPR (General Data Protection Regulation – Official Legal Text, n.d.), a mature European privacy law (Shainski, 2019).

The design of KYC/AML practices should consider possible privacy requirements of the applied jurisdictions, like protecting the data for unintended use, informing how the user data would be processed in addition to the purpose of the data collection and acquiring the user consent when processing and transferring their information. A fault in data privacy may result in fines and reputational damage. However,

in most countries, financial law is considered as above privacy law. For example, in the European Union, even if the users ask that their cryptocurrency exchange account is deleted as their right to be forgotten as mentioned in the GDPR, the cryptocurrency exchange is likely to keep the details of the cryptocurrency account for several years because the financial law asks them to do so.

SOLUTIONS AND RECOMMENDATIONS

New KYC and AML practices are emerging due to the development and use of new technologies. Regional, national, and multi-national laws, regulations, and recommendations need to keep up with technological development. First issued in 1990, the FATF Recommendations have been revised a few times to ensure that they remain up to date and relevant and that they are of universal application. In this section, we survey the potential solutions and recommendations proposed by others and us.

Identification – new solutions and FATF guidance

As discussed in the above background section, traditional identity solutions combine digital information with additional information about a person collected in the real world to increase the level of trust in the identity. New identity solutions try to overcome the difficulty of collecting physical information via face-to-face contact by using digital channels only. Digital channels offer a faster, more convenient, and affordable way to identify. These new ID solutions collect physical information about a person, usually via the use of a cellphone, to aggregate extra information in the digital identity to increase its level of trust. The information is collected by using selfies, videos, biometrics, and liveness checks and video identification services, which sometimes includes an online meeting with a team of identification specialists.

The second type of innovation is related to how identity data is stored. The vast majority of ID solutions are centralized. The issue of this approach is that the custodians are subject to privacy laws, and the storage becomes an attractive target for attacks, which could lead to data breaches. On the other side, there are new decentralized solutions linked to the concept of self-sovereign identity (SSI). SSI enables a person to create her/his own identity using a decentralized infrastructure in which third parties can assign attestations on it to prove something about the person. For instance, it can prove that the person is older than 18 years without revealing his/her real age or any other information. Using SSI, the person does not need to trust a third-party to manage his/her data but assumes the responsibility to manage it by himself/herself, which in general also leads to more complicated user experience in business solutions.

Considering the advances of digital identity in the last years, the FATF recently released guidance (*Guidance on Digital Identity*, 2020) to clarify how digital ID systems can be used to conduct some aspects of CDD under FATF Recommendation 10. The guidance clarifies that non-face-to-face customer-identification and transactions that rely on reliable, independent digital ID systems with appropriate risk mitigation measures in place, may reach a standard level of risk, and may even be lower-risk. Some digital ID solutions may be authorized by governments for use in CDD, for example, see the Aadhaar solution in India (UIDAI, n.d.) and the idNow (*IDnow - The Fastest Way to Verify Your Customer's Identity*, n.d.) solution in the EU. If the solution is not authorized, it is necessary to know the robustness and assurance(s)

level(s) of the digital ID system and evaluate if the solution provides a sufficient assurance level for the associated money laundering and terrorist financing risk situation considering the risk-based approach of the institution. Some examples of other ID systems are Trulioo (*Trulioo*, n.d.) and onfido (*ONFIDO | Document ID & Facial Biometrics Verification SaaS*, n.d.). Finally, Sovrin (*Sovrin*, n.d.), WDIA (*WDIA – Worldwide Digital Identification Association*, n.d.), and the self-sovereign system developed by the European Blockchain Services Infrastructure (*EBSI*, n.d.) are examples of SSI. Civic (*Civic Wallet—Digital wallet for money and cryptocurrency*, n.d.) has been the first ICO successfully raising funds for SSI. Still, it has failed to deliver its full solution so far. DIF (*DIF - Decentralized Identity Foundation*, n.d.) is an association with most of the major stakeholders in the DID (Decentralized Identity) field aim at establishing an open ecosystem for decentralized identity and ensuring interoperability. One may also mention the ID2020 Digital Identity Alliance (*ID2020 | Digital Identity Alliance*, n.d.).

We are working on being able to reuse KYC and AML from one provider to another provider. Our idea is to standardize, through the ITU working groups dealing with blockchains, DLT and digital currencies, new sufficient fields in extended X509 digital certificates required to show that KYC and AML have successfully been passed recently in another provider. For example, after a user would successfully pass KYC and AML at a Swiss bank, the Swiss bank would date, sign, and give a digital certificate to the user. The user could store it and use it as a proof of KYC and AML at another bank, or for a remote transaction. The BlockPass (*Identity for a Connected World*, n.d.) mobile app already stores locally in the user's smartphone-related digital proofs in JSON format.

VASP - new FATF rules

In October 2018, the FATF Recommendations were amended in order to (i) adopt two new glossary definitions related to "virtual asset" (VA) and "virtual asset service provider" (VASP) and (ii) update its Recommendation 15 in order to clarify the application of FATF standards to VA activities and VASPs and ensure a regulatory level playing field globally. Furthermore, the amendments clarified that the FATF standards apply to both virtual-to-virtual and virtual-to-fiat transactions and interactions involving VAs.

In June 2019, the FATF adopted (i) an Interpretative Note to Recommendation 15 (INR. 15), which clarified how FATF standards should be applied to VA activities and operations and VASPs; supervision or monitoring of VASPs for AML/CFT (Combatting the Financing of Terrorism); licensing and registration; preventive measures, such as CDD, recordkeeping and suspicious transaction reporting (STR); sanctions and enforcement measures and international co-operation, and (ii) a Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

The FATF defines a VASP as any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

1. Exchange between VAs and fiat currencies;
2. Exchange between one or more forms of VAs;
3. Transfer of VAs; and

4. Safekeeping and/or administration of VAs or instruments enabling control over VAs;
5. Participation in and provision of financial services related to an issuer's offer and/or sale of a VA.

Based on the above definition, VAPSs include cryptocurrency exchanges and transfer services, some cryptocurrency wallet providers and many other business models such as cryptocurrency escrow services, brokerage and advanced trading services.

According to the FATF, if a VASP provides a cryptocurrency trading platform, which only represents a forum where users can post their buy/sell bids/offers, but then they trade and conclude the transaction amongst themselves outside the platform then the latter does not constitute a VASP. This is similar to a peer-to-peer exchange platform where any seller and any buyer may locate one another through a bulletin board and then move to another location outside the network to execute the contemplated trade transaction between themselves directly.

According to FATF Recommendations, VASPs are required for any transaction exceeding the designated USD/EUR 1,000 threshold to perform CDD measures for all customers, including identifying their customer and verifying the customer identity using reliable, independent source documents, data or information, identifying the beneficial owner; understanding and obtaining information on the purpose and intended nature of business relationship; and conducting an ongoing due diligence on the relationship and scrutiny of transactions. VASPs should obtain and verify the customer identification/verification information, which includes information on the customer's name and further identifiers such as physical address, date of birth, and a unique national identifier number (e.g., national identity number or passport number). Additionally, non-core identity information, could include, for example, an IP address with an associated time stamp; geo-location data; device identifiers; crypto wallet addresses; and transaction hashes.

INR. 15, paragraph 7(b) requires VASPs and other obliged entities such as financial institutions, involved in cryptocurrency transfers to also comply with Recommendation 16 of the FATF Recommendations, including to obtain, hold, and transmit required originator and beneficiary information in order to identify and report suspicious transactions, monitor the availability of information, take freezing actions, and prohibit transactions with designated persons and entities.

The ordering/beneficiary VASP involved in a cryptocurrency transfer shall obtain and hold required and accurate originator and beneficiary information: (i) originator's name (i.e., the sending customer); (ii) originator's account number where such an account is used to process the transaction (e.g., the VA wallet); (iii) originator's physical (geographical) address, or national identity number, or customer identification number (i.e., not a transaction number) that uniquely identifies the originator to the ordering institution, or date and place of birth; (iv) beneficiary's name; and (v) beneficiary account number where such an account is used to process the transaction (e.g., the VA wallet) It is not necessary for the information to be attached directly to the cryptocurrency transfer itself. The information can be submitted either directly or indirectly, as set forth in INR. 15 and need not be communicated as part of, or incorporated into, the transfer on the blockchain or other DLT. The aforementioned requirements are commonly designated as the "Travel Rule".

Several industry consortiums are currently working on a technological solution to solve the challenges induced by the compliance with the Travel Rule. Amongst the leading ones are:

- OpenVASP, which is an international consortium of VASPs defining a protocol that facilitates robust compliance with Travel Rule for VASPs, solely based on a set of principles, independently of the jurisdiction or the virtual asset and without membership or registration with a centralized third-party (*Open Vasp – An Open Protocol to Implement FATF's Travel Rule for Virtual Assets*, n.d.);
- the Travel Rule Information Sharing Architecture called TRISA (*Trisa.Io Travel Rule Compliance – FATF Guidance*, n.d.), which aims to enable compliance with the FATF and FinCEN Travel Rules for cryptocurrency transaction identity information without modifying the core blockchain protocols, and without incurring increased transaction costs or modifying virtual currency peer-to-peer transaction flows.

Although Japan is the fist FATF country that is undergoing an evaluation of its Travel Rule, the FATF is anticipating that such compliance shall not be effective before 2021.

Unbanked issues, biometric KYC examples

As discussed above, unbanked need financial solutions that are more affordable, more accessible, and with alternative approaches to the use of formal documents during KYC/CDD checks. The following paragraphs describe five recommendations considering these three requirements.

The first recommendation is to apply a "progressive" KYC/CDD approach, respecting a risk-based approach, whereby low transaction/payment/balance limits could reduce money laundering vulnerability. For example, in case of a low threshold for transactions, a limited number of transactions per period, and no cross-border, the overall money laundering risk is reduced. Thus, simplified measures may be sufficient (FATF et al., 2013).

The second recommendation is to offer products and services using new channels. Digital channels for financial transactions can lower costs by as much as 90% compared to similar transactions conducted in physical branches of financial service providers (Grossman, 2017). As a result, digital financial service providers (both banks and non-banks) can offer financial services profitably in areas where bank branches and ATMs are not viable to consumers who have historically been unprofitable to serve.

The remaining three recommendations are related to KYC. A service provider may rely on a broader range of acceptable identification means, for examplem expired foreign IDs, consular documents, or other records that undocumented people can typically acquire in the host country (bills, tax certificate, healthcare document, etc.). A significant drawback to this flexibility is that these acceptable alternative IDs are more challenging to verify and, in general, more susceptible to fraud and abuse (FATF et al., 2013).

The use of new solutions to digital identification and verification is the fourth recommendation. These systems may improve reliability, security, privacy, convenience, and efficiency. It is especially useful when the digital ID system is authorized by the government for use in CDD and when it supports many options for collecting user's information like biometric KYC (France & Selormey, 2009) and trusted information based on social reputation. One interesting scenario is to provide a very limited account to an unbanked via digital channels. The proof of identification may be less formal, but it is essential to check that the account

is really used by the original unbanked person, and not by a criminal third-party. Digital solutions with biometric help to assure that, protecting the financial system.

The last recommendation is to design new solutions that use alternative means instead of official personal documents during KYC. For example, instead of requiring a document to prove the address, a new solution would enable an individual or organization trustee to vouch for the applicant as a form of identity evidence. A second approach would be that the applicant periodically exposes his/her geographic coordinates from where this person sleeps.

Hardened crypto wallets for affordable offline transactions

In mid-2019, Facebook has unveiled a consortium called Libra (*Libra | A New Global Payment System*, n.d.) to create a new cryptocurrency based on a basket of fiat currencies to stabilize its price, in contrast to most other cryptocurrencies like Bitcoin that have a very volatile price. A cryptocurrency, which tries to have a stable price, is often called a stablecoin (Jean-Marc Seigneur et al., 2017). The Libra consortium was initially composed of major American companies such as Paypal, Visa, Mastercard or Uber. The fact that the Libra stablecoin could rapidly be used by all the customers of Facebook, potentially 2 billion users, made several countries and regulators worried. They quickly raised concerns about the risks of such a large-scale project and forced Facebook to put Libra in standby.

Although Facebook crypto wallet implementation, called Calibra, would comply to KYC and AML, the high-level design of Libra wasn't forcing mandatory KYC and AML. It wasn't enforced by default to be able to onboard users from underdeveloped countries, who may have a smartphone but no official identity papers. It is commendable to try to onboard unbanked into Libra, but lots of unbanked cannot afford a phone, not speaking of paying monthly mobile data subscriptions. Poor, unbanked users may also be in disconnected environments such as the desert or the jungle, which are too harsh for fragile smartphones.

To further extend the use of cryptocurrencies, a new generation of secure hardware crypto wallet has been patented by Reputaction (Jean-Marc Seigneur, 2019). Hardware crypto wallets (*Hardware Wallet - State-of-the-Art Security for Crypto Assets*, n.d.) are much cheaper than smartphones and could be hardened to become waterproof and shock-resistant. Unbanked could, therefore, afford a hardened crypto wallet. However, there is still the issue of being online at the time of the on-chain cryptocurrency transaction. Hence, they would have to pay data subscription that they, again, cannot afford. Some solutions have been proposed for off-chain cryptocurrency transactions like Bitcoin Lightning (Poon & Dryja, 2015). However, before any transaction, they require the creation of a first bi-directional channel between the buyer and the seller, which may not be the case if they have never met before. Even if Bitcoin Lightning payments can be routed through many sequential channels, a full path may not exist.

Furthermore, Bitcoin Lightning requires watchers to avoid that the counterparty misbehaves by publishing an old channel state to the blockchain. It is the reason that Reputaction's solution doesn't rely on Bitcoin Lightning or similar layer-2 solutions, but on modified hardened crypto wallets. Before the owners want to use their hardened crypto wallet offline, they must transfer cryptocurrencies on-chain into their hardened crypto wallet addresses. Then, they can use these cryptocurrencies to transact offline with other users also equipped with hardened crypto wallets. The main modification compared to a standard hardware crypto wallet is that the owners will never be able to see or extract the private keys of their hardened crypto wallets

receiving addresses. They will only be able to transfer the cryptocurrencies on these addresses managed by the hardened crypto wallet to other external addresses once they are back online on-chain. Cryptocurrencies transferred from one user to a second user can be transferred to a third user by the second user, but the first user has lost such right after the first transfer. The first user could regain this right if the current owner of the transferred cryptocurrencies transfers them again to the first user.

Regarding KYC and AML, because such transactions happen offline off-chain, they cannot be checked in real-time with up-to-date online information. Although Reputaction's patented technical solution may work without any KYC and AML checks, Reputaction can enforce, at the hardened crypto wallet software level, an additional KYC and AML check based on recent KYC and AML digital certificate, as mentioned above in this chapter, that would have been stored before going offline. In addition to a KYC and AML check, another offline check based on computed trust, risk, and reputation (Jean-Marc Seigneur et al., 2015) is even possible.

FUTURE RESEARCH DIRECTIONS AND CONCLUSIONS

In this chapter, we have first discussed how traditional KYC/AML solutions are challenged by new technologies, in particular, cryptocurrencies transactions. We detailed the problems associated with real use cases of cryptocurrencies, financial inclusion, and new privacy laws. Then we have given a number of solutions and recommendations to address these challenges.

We intend to focus our research in proposing alternative ways, primarily based on technical means, to comply with KYC/AML regulation and empower poor unbanked with decentralized finance services.

We observed that new KYC/AML regulations are trying to keep the principles used in traditional financial systems. Unfortunately, there are many details to consider when dealing with cryptocurrencies. We have not covered the issue of cryptocurrencies and blockchains that have anonymization features (zero-knowledge proofs, mixers, tumblers…), which is left for future work.

REFERENCES

Baird, L. (2016). *Hashgraph consensus: Fair, fast, byzantine fault tolerance*. Swirlds Tech Report.

Bakhtiari, S., Safavi-Naini, R., & Pieprzyk, J. (1995). *Cryptographic hash functions: A survey*. Citeseer.

Bester, H., Chamberlain, D., Koker, L., Hougaard, C., Short, R., Smith, A., & Walker, R. (2008). *Implementing FATF Standards in Developing Countries and Financial Inclusion: Findings and Guidelines | FinDev Gateway*.

https://www.findevgateway.org/paper/2008/02/implementing-fatf-standards-developing-countries-and-financial-inclusion-findings-and

Bitcoin and Cryptocurrency ATMs in Switzerland. (n.d.). Bity. Retrieved April 1, 2020, from https://bity.com/products/crypto-atms/

Bitcoin Exchange | Cryptocurrency Exchange. (n.d.). Binance. Retrieved April 1, 2020, from https://www.binance.com

Buntix, J. (2018). Coincheck Removes Monero, Dash, and Zcash Due to "Risks." *The Merkle*. https://themerkle.com/coincheck-removes-monero-dash-and-zcash-due-to-risks/

Buterin, V., & others. (2013). *Ethereum white paper*. Ethereum Foundation. https://ethereum.org/

Buy bitcoin instantly | Paxful. (n.d.). Retrieved March 14, 2020, from https://paxful.com/

Chainanalysis. (2020). *The 2020 State of Crypto Crime*. https://go.chainalysis.com/2020-Crypto-Crime-Report.html

Chaum, D. (1983). Blind signatures for untraceable payments. *Advances in Cryptology*, 199–203.

Chaum, D., Javani, F., Kate, A., Krasnova, A., de Ruiter, J., Sherman, A. T., & Das, D. (2016). cMix: Anonymization by high-performance scalable mixing. *USENIX Security*.

Chohan, U. W. (2018). The Problems of Cryptocurrency Thefts and Exchange Shutdowns. *Available at SSRN 3131702*.

Ćirić, Z., & Ivanišević, S. (2018). BLOCKCHAIN AND TOURISM DEVELOPMENT: CASE OF MALTA. *MODERN MANAGEMENT TOOLS AND ECONOMY OF TOURISM SECTOR IN PRESENT ERA*, 565.

Combating financial crime—KPMG Global. (2019, March 19). KPMG. https://home.kpmg/xx/en/home/insights/2019/03/combating-financial-crime-fs.html

Decentralized Exchanges: The Top 8 DEXs Compared. (2019, October 29). Komodo. https://komodoplatform.com/decentralized-exchange/

Demirgüç-Kunt, A., & Klapper, L. F. (2012). *Measuring Financial Inclusion: The Global Findex Database* (SSRN Scholarly Paper ID 2043012). Social Science Research Network. https://papers.ssrn.com/abstract=2043012

DIF - Decentralized Identity Foundation. (n.d.). Retrieved March 30, 2020, from https://identity.foundation/#wgs

Douceur, J. R. (2002). *The Sybil Attack*. http://research.microsoft.com/sn/farsite/IPTPS2002.pdf

EBSI. (n.d.). Retrieved February 26, 2020, from https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI

EIDAS-Ecosystem. (n.d.). Retrieved March 13, 2020, from https://www.eid.as

Ethereum Name Service. (n.d.). Retrieved March 30, 2020, from https://ens.domains/

Ethereum Project. (n.d.). Retrieved March 29, 2018, from https://ethereum.org/

FATF. (2010). *Money Laundering Using New Payment Methods*. https://www.fatf-gafi.org/documents/documents/moneylaunderingusingnewpaymentmethods.html

FATF. (2019). *The FATF Recommendations*. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

FATF, APG, & World Bank. (2013). *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion*. FATF, APG, World Bank. http://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf

FATF-GAFI - Financial Action Task Force. (n.d.). Retrieved February 24, 2020, from https://www.fatf-gafi.org/

France, F., & Selormey, D. (2009). Biometrics improving financial accessibility. *Biometric Technology Today, 2009*(7), 10–11.

Gardner, M. (1977). A new kind of cipher that would take millions of years to break. *Scientific American, 237*(8), 120–124.

General Data Protection Regulation – Official Legal Text. (n.d.). General Data Protection Regulation (GDPR). Retrieved February 26, 2020, from https://gdpr-info.eu/

Gray, E., Jensen, C., O'Connell, P., Weber, S., Seigneur, J.-M., & Chen, Y. (2006). Trust evolution policies for security in collaborative ad hoc applications. *Electronic Notes in Theoretical Computer Science, 157*(3), 95–111.

Grossman, J. (2017). *Executive Summary of ITU Focus Group Digital Financial Services Outputs*. ITU.

Guidance on Digital Identity (p. 105). (2020). http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf

Hardware Wallet—State-of-the-art security for crypto assets. (n.d.). Ledger. Retrieved March 31, 2020, from https://www.ledger.com/

Hughes, J. R. (n.d.). *The Importance of Incorporating Data Privacy into Anti-Money Laundering and Anti-Corruption Compliance Programs*. 14. https://www.acams.org/aml-white-paper-data-privacy-anti-corruption-regulations/

ID2020 | Digital Identity Alliance. (n.d.). ID2020. Retrieved June 22, 2020, from http://id2020.org/

Identity for a Connected World. (n.d.). Blockpass. Retrieved March 30, 2020, from https://www.blockpass.org/

IDnow—The fastest way to verify your customer's identity. (n.d.). IDnow. Retrieved March 13, 2020, from https://www.idnow.io/

Isern, J., & Koker, L. (2009). *AML/CFT: Strengthening Financial Inclusion and Integrity*. https://www.cgap.org/research/publication/amlcft-strengthening-financial-inclusion-and-integrity

Janze, C., & Gvozdevskiy, I. (2017). *What Drives the Competition of Cryptocurrency Exchanges? Examining the Role of the Market and Community*.

Komodo—An Open, Composable Smart Chain Platform. (n.d.). Komodo. Retrieved April 1, 2020, from https://komodoplatform.com/

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, *4*(3), 382–401.

Libra | A New Global Payment System. (n.d.). Libra.Org. Retrieved March 31, 2020, from https://libra.org/en-US/

LocalBitcoins.com: Fastest and easiest way to buy and sell bitcoins. (n.d.). Retrieved March 14, 2020, from https://localbitcoins.com/

MyEtherWallet.com: Your Key to Ethereum. (n.d.). MyEtherWallet.Com: Your Key to Ethereum. Retrieved April 1, 2020, from https://www.myetherwallet.com

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*.

Narula, N. (2017, September 7). Cryptographic vulnerabilities in IOTA. *Neha Narula*. https://medium.com/@neha/cryptographic-vulnerabilities-in-iota-9a6a9ddc4367

Nash | Trade. Pay. Invest. (n.d.). Retrieved March 14, 2020, from https://nash.io/

Nezamaikin, V. N., & Zbirovskaya, E. P. (2019, June). *Contemporary Challenges of OTC Trading in Digital Assets*. 2nd International Conference on Economy, Management and Entrepreneurship (ICOEME 2019). https://doi.org/10.2991/icoeme-19.2019.23

ONFIDO | Document ID & Facial Biometrics Verification SaaS. (n.d.). Onfido Identity Verification. Retrieved February 26, 2020, from https://onfido.com/

Open Vasp – An Open Protocol to Implement FATF's Travel Rule for Virtual Assets. (n.d.). Retrieved March 15, 2020, from https://www.openvasp.org/

Perlner, R. A., & Cooper, D. A. (2009). Quantum resistant public key cryptography: A survey. *Proceedings of the 8th Symposium on Identity and Trust on the Internet*, 85–93.

Poon, J., & Dryja, T. (2015). The bitcoin lightning network: Scalable off-chain instant payments. *Technical Report (Draft)*. https://www.weusecoins.com/assets/pdf/library/Lightning%20Network%20Whitepaper.pdf

Popov, S. (2016). The tangle. *Cit. On*, 131.

Praxxis. (n.d.). Retrieved March 9, 2020, from https://praxxis.io/

Seigneur, Jean-Marc. (2019). *Système sécurisé de transactions entre terminaux* (World Intellectual Property Organization Patent No. WO2019145620A1). https://patents.google.com/patent/WO2019145620A1/en/

Seigneur, Jean-Marc, Ballester Lafuente, C., Titi, X., & Guislain, J. (2015). OPPRIM: Opportunity-enabled risk management for trust and risk-aware asset access decision-making. *University of Geneva Technical Report*.

Seigneur, Jean-Marc, D'Hautefort, H., & Ballocchi, G. (2017). *Use case of linking a managed basket of fiat currencies to crypto-tokens*. First Meeting of the ITU Focus Group on

Digital Currency including Digital Fiat Currency. https://archive-ouverte.unige.ch/unige:97657

Seigneur, Jean-Marc., Gray, Alan., & Jensen, C. Damsgaard. (2005). *Trust Transfer: Encouraging Self-Recommendations without Sybil Attack. Proceedings of the Third International Conference on Trust Management*. http://www.cs.tcd.ie/Jean-Marc.Seigneur/publications/trusttransfer.pdf

Seigneur, J.-M. (2005a). Decentralized Identity for the Digital Business Ecosystem. *ERCIM News*. http://www.ercim.org/publication/Ercim_News/enw63/seigneur.html

Seigneur, J.-M. (2005b). *Trust, Security and Privacy in Global Computing* [Ph.D. Thesis, Trinity College Dublin]. https://www.cs.tcd.ie/publications/tech-reports/reports.06/TCD-CS-2006-02.pdf

Shainski, R. (2019, November 20). *For Banks, Data Privacy and Anti-Money Laundering Don't Have to Be Incompatible*. CPO Magazine. https://www.cpomagazine.com/data-privacy/for-banks-data-privacy-and-anti-money-laundering-dont-have-to-be-incompatible/

*Shaping the future of payments**. (2019, November 4). https://www.bis.org/statistics/payment_stats/commentary1911.htm

Sovrin. (n.d.). Sovrin. Retrieved February 26, 2020, from https://sovrin.org/

SWIFT - The global provider of secure financial messaging services. (n.d.). SWIFT. Retrieved February 26, 2020, from https://www.swift.com/node/7746

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, *2*(9).

The OECD Glossary of Statistical Terms. (n.d.). Retrieved February 24, 2020, from https://stats.oecd.org/glossary/

Trisa.io Travel Rule Compliance – FATF guidance. (n.d.). Retrieved March 15, 2020, from https://trisa.io/

Trulioo: Global Identity Verification Service. (n.d.). Trulioo: Global Identity Verification. Retrieved February 26, 2020, from https://www.trulioo.com/

UIDAI. (n.d.). Unique Identification Authority of India | Government of India. Retrieved February 26, 2020, from https://uidai.gov.in/

UNODC. (2011). *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes*. https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf

Unstoppable Domains. (n.d.). Retrieved March 30, 2020, from https://unstoppabledomains.com/

Venegas, P. (2017). Initial coin offering (ICO) risk, value and cost in blockchain trustless crypto markets. *Value and Cost in Blockchain Trustless Crypto Markets (August 1, 2017)*.

WDIA – Worldwide Digital Identification Association. (n.d.). Retrieved March 30, 2020, from https://wdia.org/

Wright, T. (2020). *Iota Network Relaunched Following Trinity Wallet Theft | Cointelegraph*. https://cointelegraph.com/news/iota-network-relaunched-following-trinity-wallet-theft

X.509 : Information technology—Open Systems Interconnection—The Directory: Public-key and attribute certificate frameworks. (n.d.). Retrieved March 30, 2020, from https://www.itu.int/rec/T-REC-X.509/en

Yin, M., Malkhi, D., Reiter, M. K., Gueta, G. G., & Abraham, I. (2019). Hotstuff: Bft consensus with linearity and responsiveness. *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing*, 347–356.

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Föhr, L. (2017). The ICO Gold Rush: It's a scam, it's a bubble, it's a super challenge for regulators. *University of Luxembourg Law Working Paper*, *11*, 17–83.

KEY TERMS AND DEFINITIONS

Asymmetric cryptography: a crypthography system whereby the user owns a key pair. The private key must remain private to sign and decrypt. The public key can be made public to be able to identify the user, most often based on a hash of the public key, and encrypt information for the owner.

Blockchain: a distributed ledger among a large number of peers that is secured by a chain of information blocks linked together via the hash of the previous block and synchronized thanks to a consensus algorithm.

Cryptocurrency: a digital representation of value that is owned and secured using asymmetric cryptography and blockchain to ensure its authenticity and prevent modification or tampering without the owner's consent as well as forbidding the owner to double-spend.

Customer Due Diligence (CDD): the process to identify and continuously verify customers during the business relationship with a financial institution or with other designated non-financial businesses and professions.

Know Your Customer (KYC): the process to identify and continuously verify customers during the business relationship with a (financial or non-financial) institution with a primary goal to comply with a set of regulatory requirements.

Anti-Money Laundering (AML): the process to continuously try to forbid identified customers to launder money.

Virtual Asset Service Provider (VASP): any natural or legal person who, as a business, conducts activities or operations with virtual assets, e.g., cryptocurrencies or crypto-tokens, for or on behalf of another natural or legal person.

Travel Rule: The requirement of VASPs to exchange information about senders and receivers of cryptocurrency transactions when executing a transaction on behalf of a user.

ENDNOTES

The authors do not endorse any solution cited in the text of this chapter.