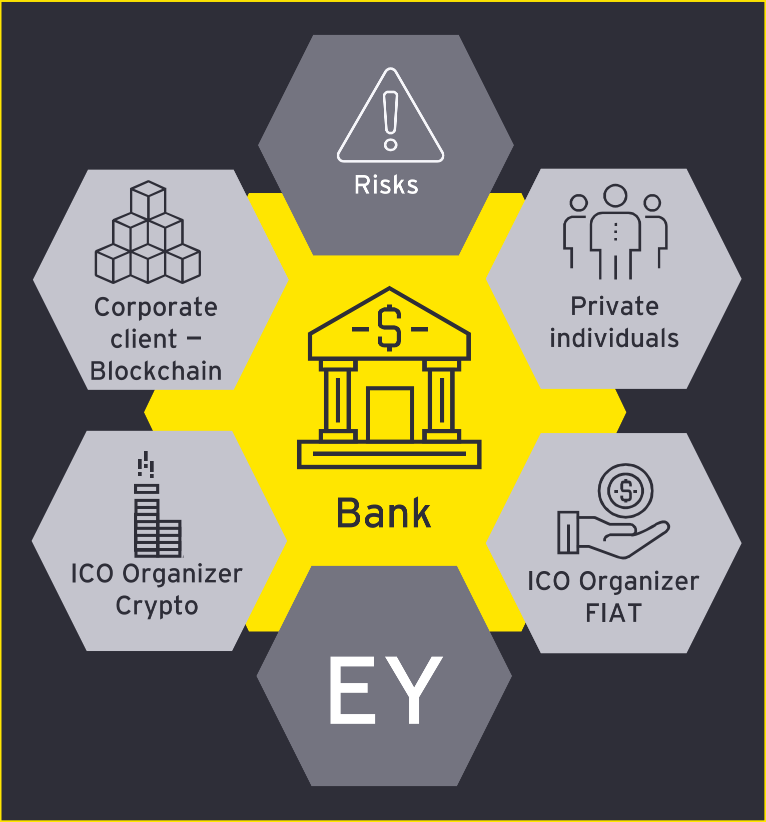
Cryptocurrencies

AML due diligence requirements from a Swiss banking perspective

September 2019

Contents

Legend



See also abbreviations on page 28

	Bank/Financial intermediary
	Corporate clients involved in Blockchain technology
	Crypto-exchange
	Due diligence
EY	EY (role and support)
	ICO organizer financing with cryptocurrencies
	ICO organizer financing with FIAT currencies
	Investor
	Legislation
	Peer-to-Peer
	Private individuals with funds from cryptocurrencies
	Risks
	Token
	Wallet provider

1 Introduction

1. Introduction

The dynamic evolution of cryptocurrency related business activities presents increased anti-money laundering (AML) risks to compliance departments at Swiss banks.

What is the concern?

- Switzerland recognizes that Blockchain and cryptocurrencies have considerable potential for innovation and enhanced efficiency both in the financial sector and in other sectors of the economy.
- Funds raised from TGEs/ICOs/STOs, speculative cryptocurrency investments or from mining successes are increasingly growing, together with the popularity of cryptocurrencies.
- Clearly, Blockchain companies as well as private crypto-investors are an interesting new client segment for Swiss banks.
- As Switzerland becomes an attractive hub for Blockchain startups, a growing number of these pay bills, salaries and social security fees using FIAT currency, which requires a bank account with a Swiss bank.
- However, despite the crypto-friendly regulatory framework, many Swiss banks are still unwilling to offer bank accounts to the new client segment.
- Opening an account poses various challenges for banks. As cryptocurrencies have been allowed to exist largely outside the regulated financial system while growing in market size and adoption, they have given rise to new risks and opened new means by which undetected criminal activity can be facilitated. There is a risk that cryptocurrencies could be misused for money laundering and terrorist financing. The vulnerabilities relate primarily to the difficulty of identifying the beneficial owners of cryptocurrencies in individual wallets. Therefore, banks have to perform strict due diligence processes before accepting new clients.
- Despite the concerns, banks can pursue a cooperative strategy with the cryptocurrency industry to support the Swiss vision of a "crypto nation".

Swiss banks are onboarding crypto-clients

- While some banks are still hesitant, others are already onboarding cryptocurrency clients under the condition that strict legal and regulatory requirements are fully complied with.
- The worlds of cryptocurrencies and traditional finance have been brought closer together by different Swiss banks, which recently either enabled:
  - The storage and trade of cryptocurrencies on behalf of their clients
  - The opening of bank accounts for private individuals or companies involved in Blockchain technology and cryptocurrencies
- It is expected that more banks will follow to facilitate opening bank accounts and handling cryptocurrency investments on behalf of their clients as a new asset class to achieve an additional portfolio diversification.

This brochure shall help Swiss banks manage their individual and corporate clients that are involved in the cryptocurrency industry. This will enable them to properly open a bank account and monitor cryptocurrency-related activities.

Find out how EY may support you in order to cope with the AML challenges ahead.

2 New players – old risks

2. New players – old risks

Although cryptocurrencies are relatively new, AML risks in payments or alternative remittance are not. From a regulatory point of view, many of the risks associated with cryptocurrencies echo those presented by new financial products and technologies of the past: untested business models, potential for abuse and fraud, lack of clear understanding on how cryptocurrency transactions work and the underlying uncertainty of a rapidly evolving regulatory environment.

Risks associated with cryptocurrencies

Risks inherent in the technology

- Transaction anonymity and difficult identification of beneficial owners
- Security vulnerabilities in the underlying technology
- Threats in connection with the novelty effect and users' inexperience
- Malware and ransomware

Risks of fraudulent use

- Means of payment for illegal goods and services
- Laundering of illegally acquired cryptocurrencies or FIAT
- Terrorist financing

How anonymous are cryptocurrencies?

Cryptocurrencies (e.g., Bitcoin) are designed to allow their users to send and receive payments with an adequate level of privacy. However, contrary to popular belief, Bitcoin is not anonymous. Bitcoin is more pseudonymous than anonymous. The use of Bitcoin leaves extensive public records and provides less anonymity than cash transactions. The public ledger readily provides anyone looking for it with detailed information about both the nature (such as time, values, recipient and sender public keys) and the context (the full history of who owned the Bitcoin before and after a transaction) of every transaction ever made.

Privacy coins

However, there are also cryptocurrencies that are untraceable. A privacy coin is a type of cryptocurrency that is cryptographically obscuring the link between a transaction and the public wallet addresses of the involved parties. Therefore, privacy coins have the potential for criminal activity as they could ultimately be exchanged back to primary cryptocurrencies which would then be exchanged for FIAT currency, completing the process of turning dirty money into clean money.

Mixer (or tumbler)

Mixers provide a mechanism of breaking down cryptocurrencies into many fragments and mixing those fragments with other fragments of other clients with the intention to confuse to trail back the "tainted" source of the cryptocurrency. The equivalent in the traditional financial world be using bank accounts in certain offshore jurisdictions to launder "soiled" FIAT money.

For more details see Interdepartmental coordinating group on combating money laundering and the financing of terrorism, Risk of money laundering and financing of terrorism by crypto assets and crowdfunding, dated October 2018.

2. New players – old risks (contd)

It is complex to assess the risk of money laundering and terrorist financing where cryptocurrencies are involved. The threat associated with cryptocurrencies is real and proven. Nevertheless, only a low number of money laundering cases using cryptocurrencies have been detected in Switzerland to date. Also no case of terrorist financing using cryptocurrencies has been recorded (cf. Federal Council report, Legal framework for distributed ledger technology and Blockchain in Switzerland, p.135).

There are a number of transversal challenges that, regardless of the use case, are going to be present, and need to be addressed and monitored when entering into the cryptocurrency space. The acceptance of sale proceeds of cryptocurrencies must always be determined on a case by case basis while taking specific risk factors into consideration.

Risk-based approach

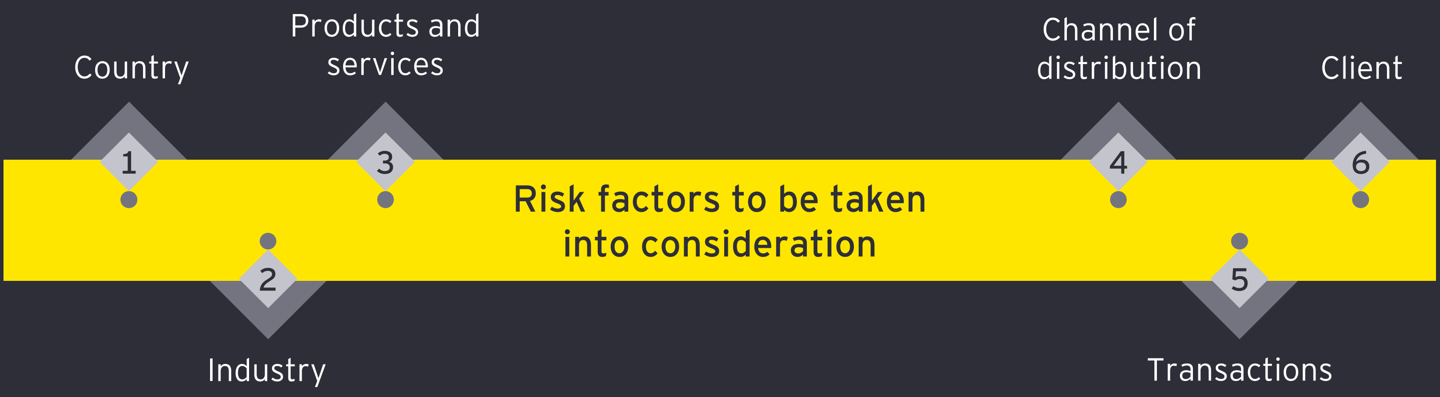
- The extent of the due diligence requirements are assessed based on the given risk situation.

Risk assessment

- The bank has to perform an accurate assessment of its inherent and residual risks and must have a meticulous insight into their counterparties, i.e., not only cryptocurrency exchanges, but also corporate clients that accept cryptocurrencies as means of payment and store of value.
- Monitoring the source, destination and value of funds through accounts is an important aspect of ongoing due diligence, especially where the potential source of funds could be the proceeds of a crime.

Risk mitigation

- Detailed and complete risk assessment
- Definition of risk appetite, e.g., not accepting cryptocurrencies/sales proceeds that are not transparent by intent
- Consistent framework for determining the bank's specific risk factors and risk management parameters
- Documentation of risk assessment, framework, risk factors-logic/derivation etc
- Periodic review/update of the client data
- Sound transaction monitoring system and a proper due diligence and documentation of generated alerts


Risk factors to be taken into consideration

3 Due diligence for corporate clients

3. Due diligence for corporate clients

Opening of corporate bank accounts

- The opening of corporate bank accounts for Blockchain companies has been a challenge in practice both for such companies and banks. The Swiss Federal Department of Finance convened a round table in the summer of 2018 and the Swiss Bankers Association (SBA) has extensively dealt with the issue in a working group involving the Crypto Valley Association. As a result, the SBA has developed Guidelines that are intended to assist banks in opening bank accounts for Blockchain companies.

- The SBA Guidelines list Blockchain-specific elements within the scope of the established KYC process and also set specific expectations for the issuer of tokens. Pursuant to the SBA Guidelines a company must demonstrate that it is operative in Switzerland and has a local substance (e.g., offices, personnel).

- The guidelines do not define binding minimum standards. Bank-specific instructions issued by SBA members take precedence. Each bank is responsible for its own business activities, which leaves room for banks to define and implement a due diligence framework regarding crypto-currencies.

- Corporate bank accounts are an essential infrastructure service and banks have an interest in doing business in this fast-growing area. At the same time, there is no obligation for Swiss banks to offer bank accounts to Blockchain companies. The integrity and reputation of the Swiss financial market must remain a top priority for all market participants.

- In August 2019, the SBA published updated Guidelines, which were updated both in terms of terminology and content. The updated Guidelines are in particular intended to support member banks in their discussions with companies that have links to distributed ledger technology (DLT) and assist with risk management in their business dealings.

> Banks can pursue a cooperative strategy with the cryptocurrency industry to support the Swiss vision of a “crypto nation”

3. Due diligence for corporate clients (contd)

Banks need to take a differentiated approach to account opening, depending on the nature of the involvement that the company has with Blockchain technology. Companies have to be categorized based on the type of corporate financing. The highest standards shall apply to the documentation for companies that finance an ICO via cryptocurrencies.

What is an Initial Coin Offering?

An Initial Coin Offering ("ICO"), Token Generating Event ("TGE") or Security Token Offering ("STO") is the issuing of digital, transferable, unique information and/or functional units (coins or tokens) by a company ("ICO organizer" or "Token Issuer") to a participant ("Investor"). This way of crowdfunding is mostly used by start-ups to bypass the stricter regulated traditional ways of capital raising. On 16 February 2018 FINMA published a guidance paper clarifying how ICOs are treated from a legal and regulatory point of view.

Blockchain companies without an ICO

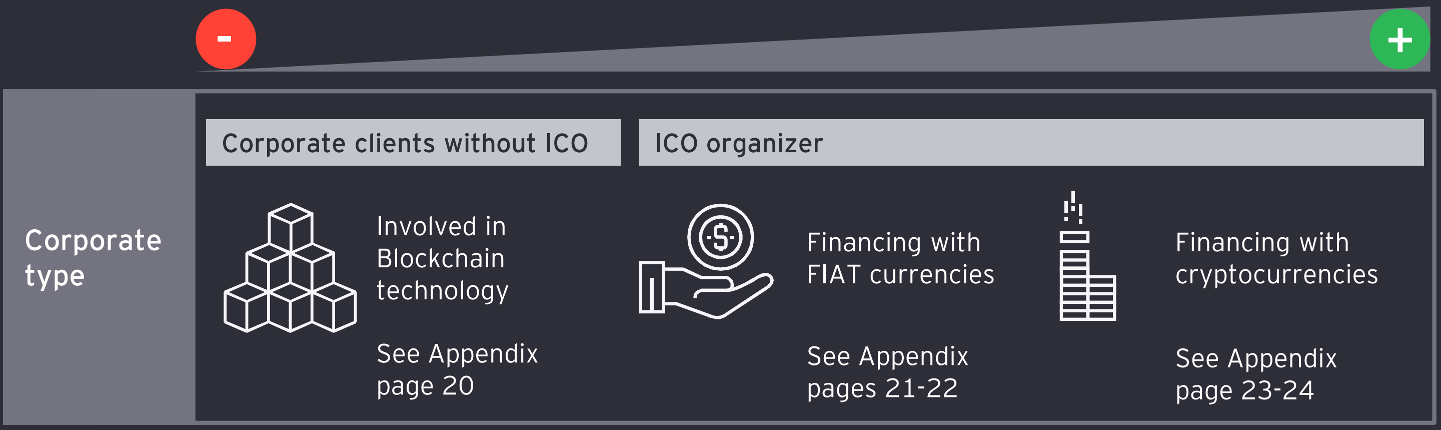
- Companies whose business model has links to Blockchain but do not use Blockchain technology to raise capital should not be treated any differently than other companies wanting to open an account. The usual, strict legal regulations that govern account opening should apply.
- Companies have a duty to cooperate in the opening of banking relationships. They need to be able to demonstrate that they are aware of and adhere to all regulations applicable to their business model. This includes the ability to show a meaningful business plan as well as adequate processes and resources.

Blockchain companies with an ICO

- Companies that raise capital by issuing tokens using Blockchain technology can do so in the form of FIAT or cryptocurrencies.
- For companies that are raising cryptocurrencies, higher and additional requirements should be imposed, whether or not the companies are subject to AMLA. The guidelines recommend that the ICO organizer should apply the relevant Swiss standards on KYC and AML when accepting cryptocurrencies in an ICO. It is also proposed that the acceptance of cryptocurrencies under ICOs should be treated in the same way as a cash transaction as a minimum.

EY has defined CDD checks for the different corporate types outlining the required actions

Intensity of due diligence requirements for the different types of corporate clients


-
+
Corporate type
Corporate clients without ICO
ICO organizer
Involved in Blockchain technology
See Appendix page 20
Financing with FIAT currencies
See Appendix pages 21-22
Financing with cryptocurrencies
See Appendix page 23-24

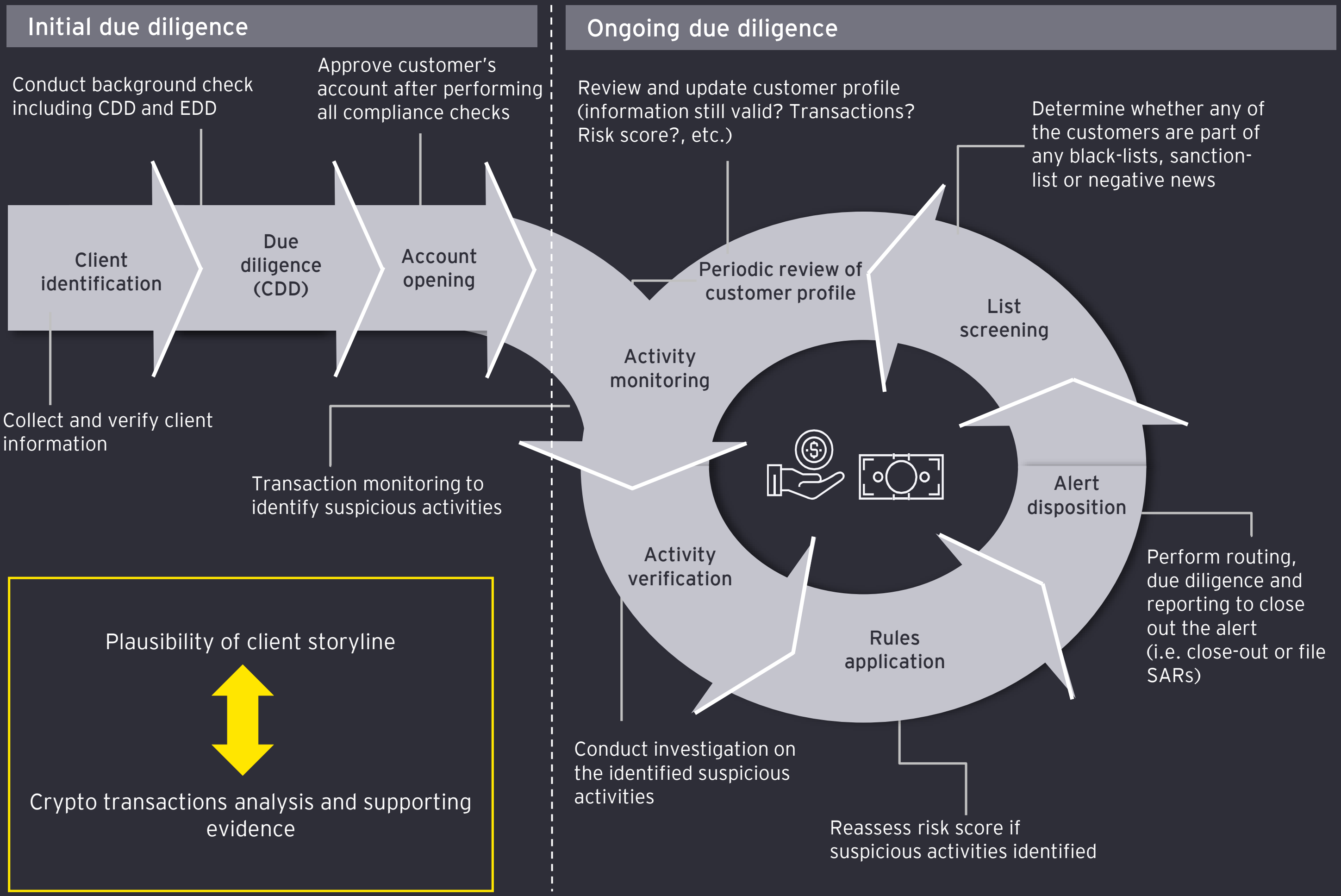
4 Due diligence for individuals

4. Due diligence for individuals

- With the rising popularity of cryptocurrencies, banks are more and more confronted with prospects or existing clients who intend to bring their cryptocurrency sale proceeds to the bank.
- Due to this market need, banks and other financial intermediaries are required to assess the corresponding risks, amend their service offering as well as processes and controls to mitigate potential risks:
  - All clients of a bank are subject to CDD measures. It encompasses knowledge, understanding and information obtained on clients before starting a banking relationship and throughout the lifecycle of the same. This includes verification of the wealth accumulation, negative media search and transaction analysis.

- Swiss AML regulation does not prohibit the acceptance of sale proceeds of cryptocurrencies in general. Nevertheless, the principle of the risk based approach will have to be adhered to. Therefore, the bank has to adapt its due diligence procedures depending on the underlying risk.
- A clear classification, the right approach and a proper implementation of the appropriate measures are crucial for minimizing the rising risks:
  - By law, there are no specific due diligence requirements for clients linked to the cryptocurrency/Blockchain world.
  - Risk-based approach
  - What are the identified risks linked to the client and cryptocurrencies and which mitigating-measures can be taken?

Due diligence lifecycle



Initial due diligence
Ongoing due diligence
Conduct background check including CDD and EDD
Approve customer's account after performing all compliance checks
Client identification
Due diligence (CDD)
Account opening
Collect and verify client information
Transaction monitoring to identify suspicious activities
Review and update customer profile (information still valid? Transactions? Risk score?, etc.)
Determine whether any of the customers are part of any black-lists, sanction-list or negative news
Periodic review of customer profile
List screening
Activity monitoring
Alert disposition
Activity verification
Rules application
Perform routing, due diligence and reporting to close out the alert (i.e. close-out or file SARs)
Conduct investigation on the identified suspicious activities
Reassess risk score if suspicious activities identified
Plausibility of client storyline
Crypto transactions analysis and supporting evidence

The due diligence checklist for corporate clients (see page 20 et seq.) applies to individuals by analogy.

5 EY services, tools and contacts

5. EY services, tools and contacts

Blockchainand cryptocurrencies pose challenges for an effective regulatory compliance from different angles: people, process and technology. Examples of how EY can help you approach these three key areas are shown below:

	People	Process	Technology
Current pain points and challenges	▶ **Public perception** ▶ Mainstream awareness of the use of cryptocurrencies and DLT/Blockchain ▶ Association with negative undertones ▶ **Lack of expertise**	▶ **Privacy and security** ▶ Visible transactions ▶ **Regulatory concerns** ▶ Money laundering, terrorist financing and fraud risks ▶ Lack of standardized monitoring processes	▶ **High initial cost** ▶ **Integration with legacy systems** ▶ **Lack of available compliance systems** ▶ Need for customized, scalable solutions and tools ▶ Advanced analytics
EY			
Strategy to comply	▶ Clarity on applicable regulatory laws ▶ Gap-assessments and corresponding amendments of internal guidelines and standards ▶ Creation and management of trainings for relevant stakeholders and employees	▶ Clarity on money laundering typologies ▶ Customized AML program and enhanced processes to support the bank's AML program (incl. cybersecurity and costumer protection) ▶ Transaction monitoring/alert review ▶ Application security ▶ Anti-fraud	▶ Customized compliance technologies such as: ▶ KYC and associated EDD functionality ▶ Implementation of various EY digital solutions and tools ▶ In-house transaction monitoring and case management tools ▶ **Leverage innovative tech to streamline processes such as** ▶ Natural language processing ▶ Robotics/automation

5. EY services, tools and contacts

Introduction into the EY Blockchain Analyzer

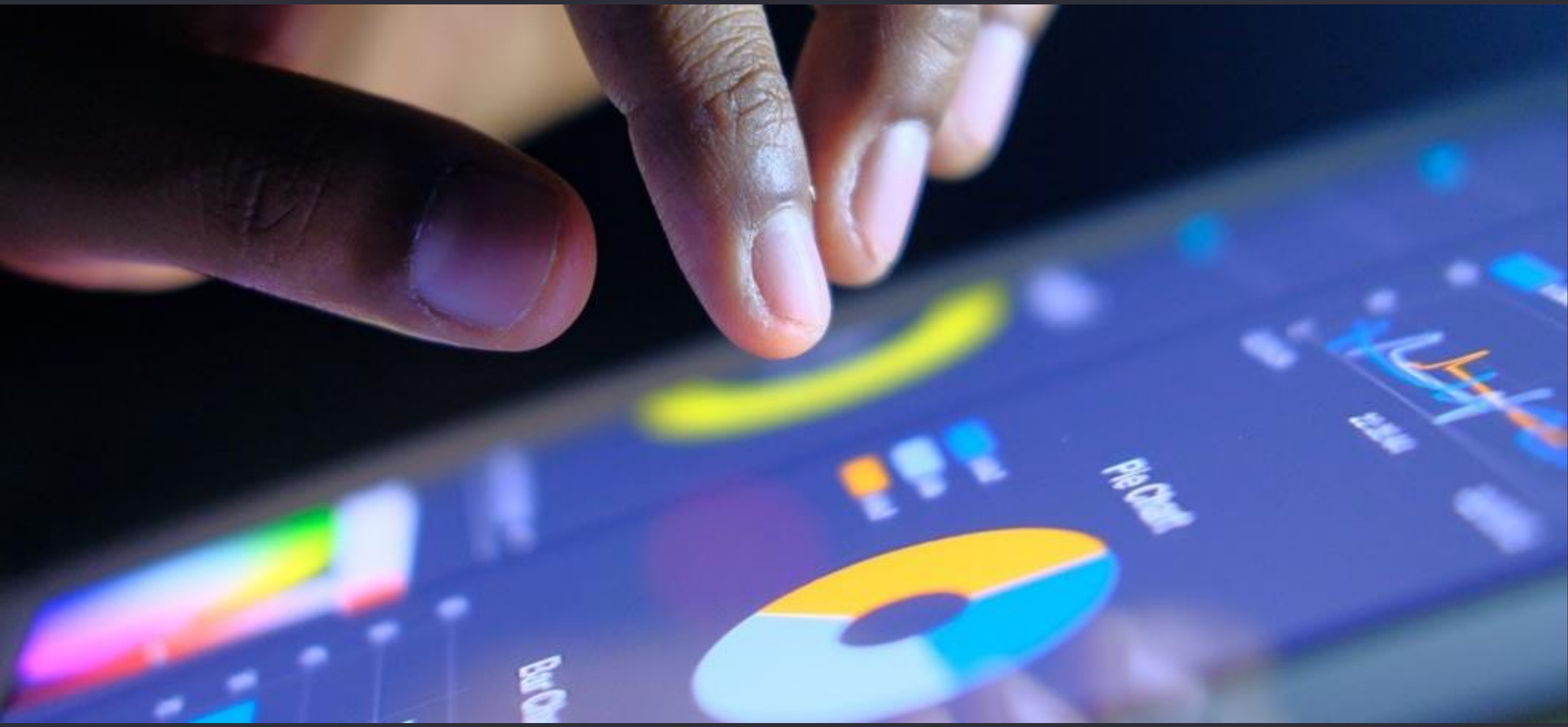
The first generation of the EY Blockchain Analyzer was designed to facilitate EY audit teams in gathering an organization's entire transaction data from multiple blockchain ledgers, to reconcile that data to EY client books and records and to perform enhanced analytics, including trend analysis and identification of outliers.

After a major upgrade, a second generation of the EY Blockchain Analyzer is now available globally for EY teams and all clients as a business application that is accessible anytime and helps enable financial reporting, forensic investigations, transaction monitoring and tax calculations.

The EY Blockchain Analyzer supports analysis of zero-knowledge proof (ZKP) private transactions on the public Ethereum blockchain, as well as the Bitcoin, Bitcoin Cash, Ethereum, Ethereum Classic and Litecoin public blockchains. EY Blockchain Analyzer also supports private Ethereum, Quorum and Hyperledger blockchains.

Tangible benefits

Some companies, like cryptocurrency exchange platforms, need to manage 20,000 to 50,000 cryptocurrency wallets on an ongoing basis with a transaction volume in the region of 100,000 per month. Although some tests could be performed manually on a sample of cryptocurrency transactions by using commercially-available solutions, the EY Blockchain Analyzer enables testing 100% of the transactions in a more efficient way, thanks to the deep data analysis and a quicker visualization of red flags.



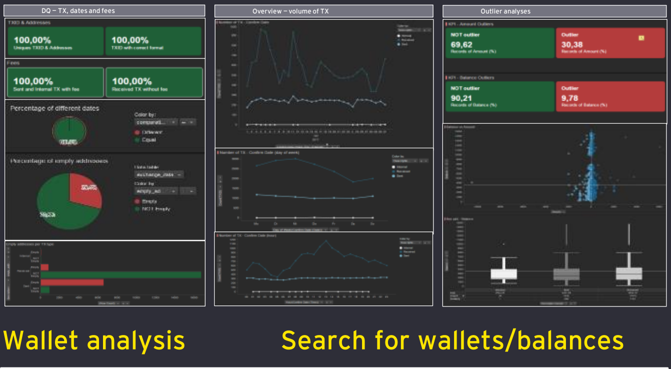
5. EY services, tools and contacts

How does the EY Blockchain Analyzer work?

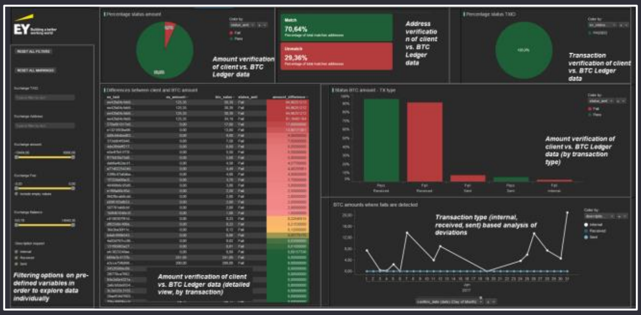
Reliable tool

The tool relies on a Blockchain node that holds a copy of the entire Blockchain ledger, from where the data is extracted by using the EY proprietary Blockchain ledger exporter into big data analytics, to perform e.g., audit certification/procedures and reconciliations on 100% of client transactions in a matter of seconds.

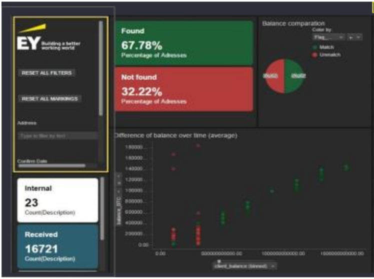
Data quality and descriptive analytics: understanding the client data and verifying the quality



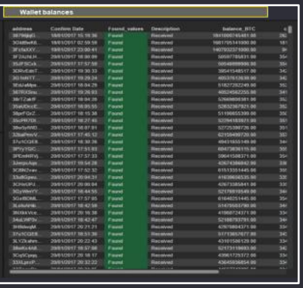
Transaction analysis


Match
70,64%
Unmatch
29,36%
Address verification of client vs. BTC Ledger data
Amount verification of client vs. BTC Ledger data
Transaction verification of client vs. BTC Ledger data
Amount verification of client vs. BTC Ledger data (by transaction type)
Transaction type (internal, received, sent) based analysis of deviations
Filtering options on pre-defined variables in order to explore data individually
Amount verification of client vs. BTC Ledger data (detailed view, by transaction)

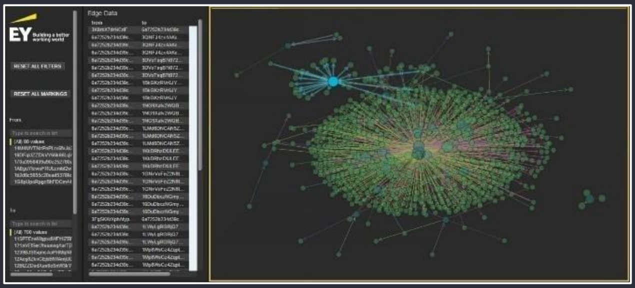
Wallet analysis



Search for wallets/balances

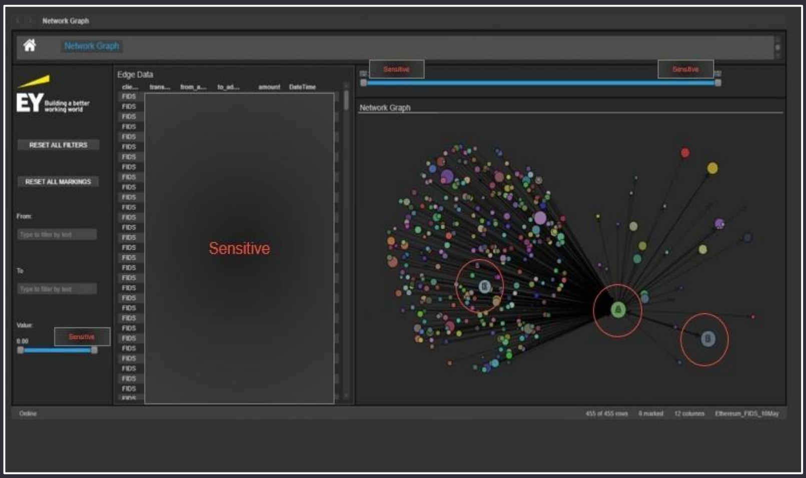


Pattern analysis



Fraud investigation use case

A client had two cryptocurrency wallets that had been compromised. Leveraging the EY Blockchain Analyzer, the engagement team and the client were able to visualize where and when the transactions took place and which wallets were involved. The team then “tagged” the compromised wallets for continued monitoring as the investigation evolved.



Thanks to some innovative features, the EY Blockchain Analyzer can also support Blockchain/crypto fraud investigations.

- Visualization
- Search, highlight and track transactions
- Reconciliation of ledgers
- Select groups of transactions
- Custom labelling and wallet profiling

5. EY services, tools and contacts

Multidisciplinary team

Our multidisciplinary team focuses on helping clients to improve their performance and manage their risks more effectively. This is particularly important in a challenging and uncertain business environment, with escalating competition.

01 Legal, Regulatory and Compliance

- Supporting in the implementation of your crypto business plan
- Establishing/strengthening of AML/CTF governance framework: policy framework, internal control system and functions
- Implementing applicable local and international securities laws, financial and data protection laws
- Advising on cross border regulatory considerations
- Leveraging deep contacts with FINMA
- Organizing staff training to raise awareness in all AML/CTF and cryptocurrency/Blockchain matters
- Regulating cryptocurrency exchanges
- Advising on reliable service providers in Switzerland to work with
- Benchmarking of policies, procedure and controls
- Conducting gap analysis on KYC/AML
- Outsourcing of internal audit, legal and compliance function

02 Assurance

- Testing of AML governance framework with focus on cryptocurrency readiness
- Transaction monitoring
- Providing external audits/certifications, in particular, regarding AML or financial statements
- Reviewing controls and audits/certifications regarding crypto funds
- Reporting of cryptocurrencies (i.e., Capital Adequacy)
- Accounting of cryptocurrencies RRV-FINMA/IFRS-Aspect

03 Advisory

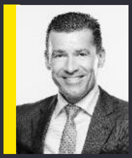
- Identification and analysis of the viability of Blockchain use cases including a strategic and technical analysis
- Defining Target Operating Model and Strategy for Blockchain business models
- Assessing competitive landscape and product strategy
- Engineering consortium ecosystem including the assessment of potential partners and its incentives
- Assessing risk and control including cyber risks, technology and process risks to facilitate an efficient crypto client onboarding
- Establishing audit readiness support ensuring compliance with your auditing teams, local and global regulations

04 Technology

- Providing the Blockchain Analyzer as a service to track the path of cryptocurrencies

5. EY services, tools and contacts

Legal, Regulatory and Compliance



Philippe Zimmermann

Partner, EY Switzerland Ltd.
Tel: +41 58 286 32 19
Email: philippe.zimmermann@ch.ey.com

Christian Röthlin

Partner, EY Switzerland Ltd.
Tel: +41 58 286 35 38
Email: christian.roethlin@ch.ey.com

Darko Stefanoski

Partner, EY Switzerland Ltd.
Tel: +41 58 286 37 08
Email: darko.stefanoski@ch.ey.com

Orkan Sahin

Manager, EY Switzerland Ltd.
Tel: +41 58 286 42 88
Email: orkan.sahin@ch.ey.com

Assurance, Advisory and Technology

Philipp Müller

Partner, EY Switzerland Ltd.
Assurance
Tel: +41 58 286 36 86
Email: philipp.mueller@ch.ey.com

Philipp de Boer

Partner, EY Switzerland Ltd.
Assurance
Tel: +41 58 286 3633
Email: philipp.deboer@ch.ey.com

Urs Palmieri

Associate Partner, EY Switzerland Ltd.
Advisory
Tel: +41 58 286 3951
Email: urs.palmieri@ch.ey.com

Robert Hirt

Director, EY Switzerland Ltd.
Technology
Tel: +41 58 286 8193
Email: robert.hirt@ch.ey.com

Craig Farrell

Assistant Director, EY Switzerland Ltd.
Technology
Tel: +44 20 7197 7752
Email: craig.farell@uk.ey.com

Eric Sebbagh

Senior Manager, EY Switzerland Ltd.
Advisory
Tel: +41 58 286 49 83
Email: eric.sebbagh@ch.ey.com

Joby Jose

Assistant Manager, EY Switzerland Ltd.
Assurance, Technology
Tel: +41 58 285 4901
Email: joby.jose@ch.ey.com

Appendix

Due diligence for corporate clients checklist

Additional checks that banks should complete when opening a bank account for corporate clients involved in Blockchain technology but without ICO:

	Required check	Description	Key actions
1	Blockchain or DLT involvement	▶ Specific description of the areas of involvement	▶ Review conceptual documentation of the Blockchain or DLT use case, the key features of the products or services to be developed, and the potential business implications. ▶ Assess involvement in sensitive industries, risk countries or other risk factors.
2	Description of the business model	▶ Conclusive and comprehensible description based on reliable documentation ▶ Description of the expected payment flows ▶ Description of the planned operational set-up in national/business language ▶ Identification of the legal form	▶ Review business plan and validate budgets and forecasts (provisional balance sheet, profit and loss account, etc.) and assumptions. ▶ Review internal organization, roles and responsibilities in articles of association, by-laws and other internal regulations. ▶ Review company structure (organizational chart of the company/group). ▶ Review ownership structure of the company (including breakdown of internal and external ownership, the name of the company's legal and beneficial owners and their percentage of ownership, as well as their role within the company, roles with other companies/organizations and details of partnerships, etc.).
3	Exclusion of the domiciliary company	▶ The company shall demonstrate that it is operative (CDB 16) and has a local substance. ▶ For the establishment of a new company: The company shall disclose its intentions, purpose and expected current revenue and expenses.	▶ Review documentation, certificates and attestations with respect to the legal entity set-up. ▶ Review documents and employment contracts of key personnel evidencing an operative activity.
4	Regulatory responsibilities	▶ The company shall have a dedicated contact partner for all compliance, regulatory and legal issues. In particular, it shall have: ▶ Knowledge of the relevant rules/regulations ▶ A clear description of how the company implements the relevant rules/regulations	▶ Legal assessment: ▶ Whether any licenses/authorizations are required for the planned business activities. ▶ What type of business activities are covered by the intended licenses/authorizations.

Due diligence for corporate clients checklist (contd)

Additional checks that banks should complete when opening a bank account for

ICO organizer raising FIAT currencies

	Required check	Description	Key actions
1	Use of funds	▶ Prior to launching an ICO, the ICO organizer shall demonstrate the existence of the project which is to be financed and that the funds being deposited into the account stem from the ICO and will subsequently be used for the stated purpose. ▶ The ICO organizer shall provide the bank with its final terms and conditions of the ICO.	▶ Review the budgetary allocation to ensure that the funds raised through the ICO are sufficient to cover the costs.
2	Liquidity planning	▶ The ICO organizer shall notify the bank at which the account is held prior to the launch of the ICO about: ▶ The breakdown of funds ▶ The amounts and frequency at which the funds will be transferred to the bank at which the account is held. ▶ Repayment patterns if the target amount is not reached.	▶ Monitor inflows/outflows of the account (e.g., volume, number of transactions, purpose of transactions, expected number of transactions per month, average size of transactions, maximum transaction amount, minimum transaction amount).
3	Handling risk under foreign law	▶ An ICO organizer shall establish relevant guidelines. It shall implement measures to exclude ICO participants from countries in accordance with the bank's internal rules. ▶ The ICO organizer shall provide the bank with this information upon request.	▶ Review cross-border manuals outlining: ▶ Regulations relating to financial activities ▶ Practice of the relevant local authorities ▶ Rules on marketing, negotiation and performance/execution of cross-border investment services ▶ Review implemented measures or documents, which confirm implementation.
4	AMLA subordination	▶ The bank shall initially assume that the ICO organizer is subject to AMLA. AMLA subordination is exclusively based on the FINMA guidelines for ICOs (dated 16 February 2018 incl. its supplement dated 11 September 2019). If the ICO organizer is not subject to AMLA, it must demonstrate this. ▶ In case of doubt, it must in particular produce a subordination enquiry answered by FINMA. ▶ The ICO organizer shall produce the following proof in case of an AMLA subordination: ▶ Name of the SRO and confirmation of SRO membership or evidence of DSFI affiliation ▶ In case of delegation: name of the financial intermediary and confirmation of delegation ▶ Complete documentation in accordance with the internal compliance rules of the bank.	▶ Check SRO affiliation or delegation or evidence that ICO organizer is not subject to AMLA. ▶ Establish a solid AML governance framework (i.e. policy framework, internal control system and functions). ▶ Ensure staff training and awareness program in all AML matters.

Due diligence for corporate clients checklist (contd)

	Required check	Description	Key actions
5	Tokens	▶ Detailed description of the tokens to be issued and their current status (market maturity, issue date). ▶ The token documentation, which usually takes the form of a white paper, represents an essential component of the bank's due diligence. Therefore, it must be provided to the bank as soon as possible.	▶ Review technical standards, e.g., ERC 20, technology used. ▶ Review functionalities of the token. ▶ Review token sale agreements, terms and conditions.
6	Duties under the ICO	▶ Legal obligations are based on the AMLA. ▶ At the bank's request, the ICO organizer shall demonstrate that the current use of funds corresponds with the stated purpose. ▶ At the bank's request, the ICO organizer shall demonstrate that the restrictions for foreign participants have been upheld. ▶ As a rule, any measure to create transparency with regard to the change of ownership (tokens) after the completion of the ICO reduces risk and is welcomed by the bank.	▶ Review ICO terms and conditions as well as the use of funds (e.g., % for ICO team, advisors, platform development, operational costs etc.). ▶ Review KYC/AML documentation. ▶ Review agreement with third party service provider (KYC/AML).

Due diligence for corporate clients checklist (contd)

Additional checks that banks should complete when opening a bank account for

ICO organizer raising cryptocurrencies

	Required check	Description	Key actions
1	Obtaining information about the ICO Investor	▸ Information about every Investor, which must be collected by the ICO organizer, is generally derived from the requirements of the applicable rules (e.g., SRO rules, FINMA circular 2016/07 on video and online identification). ▸ The ICO organizer must register each Investor regardless of the subscription amount and record the name, address (including country), date of birth, nationalities and place of birth. ▸ Regardless of the AMLA subordination of the ICO organizer, it is expected that the Investor is identified pursuant to the AMLA/AMLO-FINMA/CDB from a subscription amount of at least CHF 15,000. Any further measures to increase transparency serve to reduce risk, in particular in view of potential violations of sanctions. The information collected in the identification process also contains all relevant wallet addresses that the ICO Investor uses when making capital contributions. ▸ The raising of payment tokens is subject to the AMLA. In accordance with FINMA practice, a simplified identification duty applies up to a threshold value of CHF 3,000 in accordance with Art. 12, para. 2 (d) AMLO-FINMA by means of a simple copy of an identification document. Here, the name, address, date of birth, beneficial owner/authority holder, e-mail and telephone number must be recorded in writing. The information also includes all relevant wallet addresses that the ICO Investor uses when making capital contributions.	▸ Keep KYC/AML documentation in line with bank's standards/requirements. ▸ Establish automated data gathering and validation processes as well as geographic risk control mechanisms.

Due diligence for corporate clients checklist (contd)

	Required check	Description	Key actions
2	Use of risk databases	▶ The ICO organizer shall reconcile Investors with risk databases customary for the industry (in PEP and terrorism and sanction lists). ▶ The reconciliation shall be provided to the bank together with the internal guidelines on the monitoring of PEPs and sanctioned clients.	▶ Use KYC/AML combining cutting edge filtering technology with comprehensive global screening (sanctions, watch lists, PEPs and adverse media). ▶ Integrate search API and automated batch functionality into existing systems. ▶ Keep KYC/AML documentation in line with bank's standards/requirements. ▶ Use wallet analysis tools.
3	Background check (source of funds) and risk assessment of the wallet addresses used for participation in the ICO (AML)	▶ It is generally recommended that the ICO organizer takes a risk-based approach to the background checks (i.e., a systematic and complete tracing of the source of the funds in the Blockchain has so far not been required). In special cases or instances of specific suspicion it is recommended to carry out a thorough check by means of a wallet analysis or additional documentation (e.g., additional due diligence instead of a pure database reconciliation in case of high investment amounts or domicile in a risk country). ▶ A thorough check by the ICO organizer is always recommended for subscriptions that exceed CHF 100,000 (individual or cumulative). This thorough check includes documented reconciliation of wallet addresses and ICO Investors. ▶ The bank may request information about the Investors prior to the receipt of funds and, should it have its own specific suspicions, request the ICO organizer to carry out further clarifications (e.g., receipt of specific wallet analyses).	
4	Quality certification of the KYC/AML check	▶ Regardless of an AMLA subordination, it is recommended that KYC/AML checks be carried out in accordance with the applicable standards and in accordance with the FATF Recommendations 9 – 21. ▶ An ICO organizer that is not subject to the AMLA may either engage a financial intermediary or a company specialized in AMLA compliance for this purpose. ▶ The results shall be disclosed to the bank. The results shall also document compliance with internal company PEP guidelines.	

FATF Guidance for a risk-based approach

FATF Guidance for a risk-based approach for virtual assets and virtual asset service providers

With regard to the application of the risk-based approach (RBA), the FATF Guidance examines how the virtual assets ("VA's") and virtual asset service providers ("VASPs") fall within the scope of the FATF recommendations. The following specifications of certain recommendations support a risk-based approach. Nonetheless, the FATF Guidance is non-binding and does not overrule the purview of national authorities.

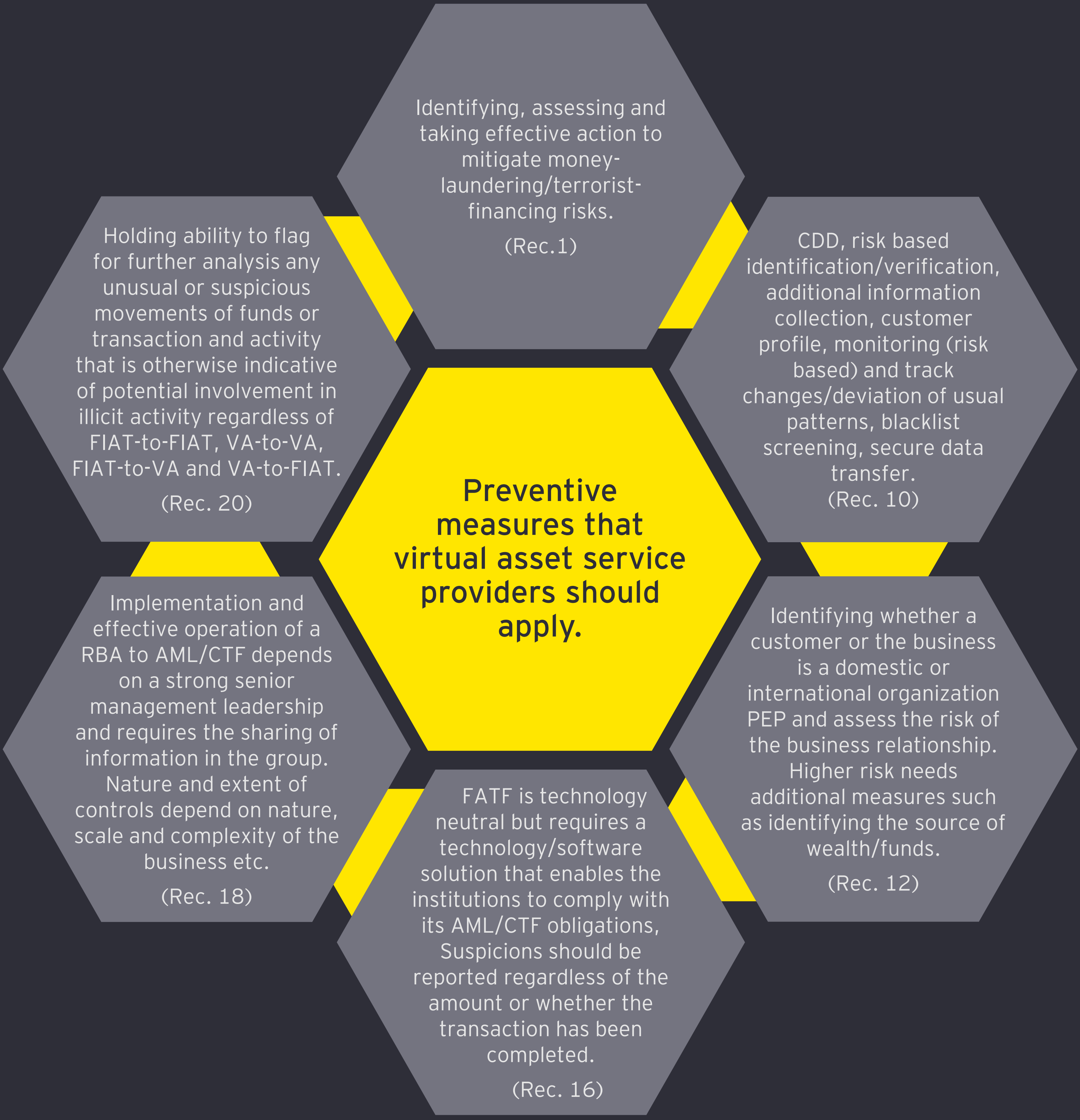
Financial Action Task Force (FATF)

- In June 2019, the FATF published a guidance on virtual assets ("FATF Guidance") which clarifies the application of the requirements for VA's and VASPs with regard to the application of the RBA. The FATF Guidance includes the following corner stones:
  - Countries should identify, assess, and understand the money laundering and terrorist financing risk emerging from virtual assets activities and activities or operations of VASPs .
  - VASPs should be required to be licensed or registered.
  - Countries should ensure that VASPs are subject to adequate regulation and supervision or monitoring for AML and terrorist financing.
  - Countries should ensure that there is a range of effective, proportionate and dissuasive sanctions (criminal, civil or administrative).
  - The occasional transactions designated threshold above which VASPs are required to conduct Client Due Diligence ("CDD") is USD/EUR 1,000.

Switzerland

- In its report of December 2018, the Federal Council stated that the AML framework in Switzerland is currently sufficiently technology-neutral to also cover activities related to cryptocurrencies and ICOs to a large extent. The activities of most players in the crypto space already qualify as financial intermediary activity and are therefore subject to the AMLA. As Switzerland is a FATF member, the FATF guidance will also have an impact on upcoming Swiss regulations.
- FINMA has already called on all Swiss financial intermediaries to take the FATF recommendations into account in their risk management strategies. It has also requested recognized self-regulatory organizations to inform their members.

FATF Guidance for a risk-based approach (contd)



Preventive measures that virtual asset service providers should apply.

Identifying, assessing and taking effective action to mitigate money-laundering/terrorist-financing risks.

(Rec.1)

CDD, risk based identification/verification, additional information collection, customer profile, monitoring (risk based) and track changes/deviation of usual patterns, blacklist screening, secure data transfer.

(Rec. 10)

Identifying whether a customer or the business is a domestic or international organization PEP and assess the risk of the business relationship. Higher risk needs additional measures such as identifying the source of wealth/funds.

(Rec. 12)

FATF is technology neutral but requires a technology/software solution that enables the institutions to comply with its AML/CTF obligations, Suspicions should be reported regardless of the amount or whether the transaction has been completed.

(Rec. 16)

Implementation and effective operation of a RBA to AML/CTF depends on a strong senior management leadership and requires the sharing of information in the group. Nature and extent of controls depend on nature, scale and complexity of the business etc.

(Rec. 18)

Holding ability to flag for further analysis any unusual or suspicious movements of funds or transaction and activity that is otherwise indicative of potential involvement in illicit activity regardless of FIAT-to-FIAT, VA-to-VA, FIAT-to-VA and VA-to-FIAT.

(Rec. 20)

Bibliography

Bundesrat, Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwab (13.3687) und Weibel (13.4070) vom 25. Juni 2014, https://www.news.admin.ch/NSBSubscriber/mes-sage/attachments/35361.pdf

ESMA, Advice on Initial Coin Offerings and Crypto-Assets of 9 January 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

European Parliament, Virtual currencies and terrorist financing: assessing the risks and evaluating responses, May 2018, http://www.europarl.europa.eu/Reg-Data/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf;

European Parliament, Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion, July 2018, http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

Federal Council, Legal framework for distributed ledger technology and Blockchain in Switzerland of 7 December 2018, https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-73398.html

FATF, National Money Laundering and Terrorist Financing Risk Assessment, 2013, http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf.

FATF, Virtual currencies. Key definitions and potential AML/CFT risks, Juni 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

FATF, Virtual currencies. Guidance for a risk-based approach, 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

FATF, Virtual assets and virtual asset service providers, Guidance for a risk-based approach, June 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

FINMA, ICO guidelines, 16 February 2018, https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

FINMA, Supplement to the ICO guidelines, 11 September 2019, https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-stable-coins.pdf?la=en

FINMA, Press release of 19 September 2017, https://www.finma.ch/de/news/2017/09/20170919-mm-coin-anbieter/.

FINMA, Press release of 26 July 2018, https://www.finma.ch/de/news/2018/07/20180726-mm-envion/

FINMA, Press release of 27 March 2019, https://www.finma.ch/en/news/2019/03/20190327---mm---envion/

Interdepartemental coordinating group on combating money laundering and the financing of terrorism, Risk of money laundering and financing of terrorism by crypto assets and crowdfunding, dated October 2018. Available at: www.admin.ch > Documentation > Media releases > Press release of 14 December 2018 (as at 14 December 2018).

Interdepartemental coordinating group on combating money laundering and the financing of terrorism, Report on the use of cash and its risks of abuse for money laundering and financing of terrorism in Switzerland, available at: www.admin.ch > Documentation > Media releases > Press release of 18 December 2018.

SBA guidelines on corporate bank accounts for blockchain companies of 20 August 2019, https://www.swissbanking.org/library/richtlinien/leitfaden-der-sbvg-zur-eroeffnung-von-firmenkonti-fuer-blockchain-unternehmen/sbvg_leitfaden_kontoeroeffnung_d.pdf/@@download/file/SBVg_Leitfaden-Kontoeroeffnung_DE.pdf

Bank for International Settlements (BIS), Statement on crypto-assets, March 2019, https://www.bis.org/publ/bcbs_nl21.htm

Abbreviations

AML	Anti Money Laundering
AMLA	Federal Act of 10 October 1997 on Combating Money Laundering and the Financing of Terrorism in the Financial Sector (Anti-Money Laundering Act; SR 955.0)
AMLO	Ordinance of 11 November 2015 on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Ordinance; SR 955.01)
AMLO-FINMA	Ordinance of the Swiss Financial Market Supervisory Authority of 3 June 2015 on the Prevention of Money Laundering and the Financing of Terrorism (FINMA Anti-Money Laundering Ordinance; SR 955.033.0)
API	Application Programming Interface
Art.	Article
BankA	Federal Act of 8 November 1934 on Banks and Savings Banks (Banking Act; SR 952.0)
BankO	Ordinance of 30 April 2014 on Banks and Savings Banks (Banking Ordinance, SR 952.02)
BBl	Federal Gazette
Blockchain	A Blockchain is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a merkle tree root hash).
BTC	Bitcoin
CDB	Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence
CDD	Client Due Diligence
CTF	Counter Terrorist Financing
DLT	Distributed-Ledger-Technology
ECJ	European Court of Justice
EDD	Enhanced Due Diligence
ERC20	Technical standard used for smart contracts on the Ethereum Blockchain for implementing tokens. ERC stands for Ethereum Request for Comment, and 20 is the number that was assigned to this request.
ESMA	European Securities and Markets Authority
EU	European Union
FCC	Financial Crime Compliance
FATF	Financial Action Task Force on Money Laundering
Federal Council Report	Federal Council report "Legal basis for distributed ledger technology and Blockchain in Switzerland", dated 14 December 2018
FINMA	Swiss Financial Market Authority
FINMA-RRV	Circular 2008/2 «Accounting – banks»
Genesis Block	The first block on the Blockchain, also known as «Block 0»
ICO/TGE/STO	Initial Coin Offering/Token Generating Event/Security Token Offering
IFRS	International Financial Reporting Standards
KYC	Know Your Customer
Mixer (or tumbler)	Service to make purchases and transactions of cryptocurrency untraceable and therefore anonymize the origin
PEP	Politically Exposed Person
Proof of work	A piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements
RBA	Risk-based approach
SAR	Suspicious Activity Report
SBA	Swiss Bankers Association
SBA Guidelines	SBA guidelines on opening corporate accounts for Blockchain companies
SME	Small and Medium-sized Entities
SRO	Self-regulatory organization

EY | Assurance | Tax | Transactions | Advisory

About the global EY organization
The global EY organization is a leader in assurance, tax, transaction and advisory services. We leverage our experience, knowledge and services to help build trust and confidence in the capital markets and in economies all over the world. We are ideally equipped for this task — with well trained employees, strong teams, excellent services and outstanding client relations. Our global purpose is to drive progress and make a difference by building a better working world — for our people, for our clients and for our communities.

The global EY organization refers to all member firms of Ernst & Young Global Limited (EYG). Each EYG member firm is a separate legal entity and has no liability for another such entity's acts or omissions. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information, please visit www.ey.com.

EY's organization is represented in Switzerland by Ernst & Young Ltd, Basel, with 10 offices across Switzerland, and in Liechtenstein by Ernst & Young AG, Vaduz. In this publication, "EY" and "we" refer to Ernst & Young Ltd, Basel, a member firm of Ernst & Young Global Limited.

CDS0055087
ED None

This presentation contains information in summary form and is therefore intended for general guidance only. Although prepared with utmost care this publication is not intended to be a substitute for detailed research or professional advice. Therefore, by reading this publication, you agree that no liability for correctness, completeness and/or currentness will be assumed. It is solely the responsibility of the readers to decide whether and in what form the information made available is relevant for their purposes. Neither Ernst & Young Ltd nor any other member of the global EY organization accepts any responsibility. On any specific matter, reference should be made to the appropriate advisor.

ey.com/ch