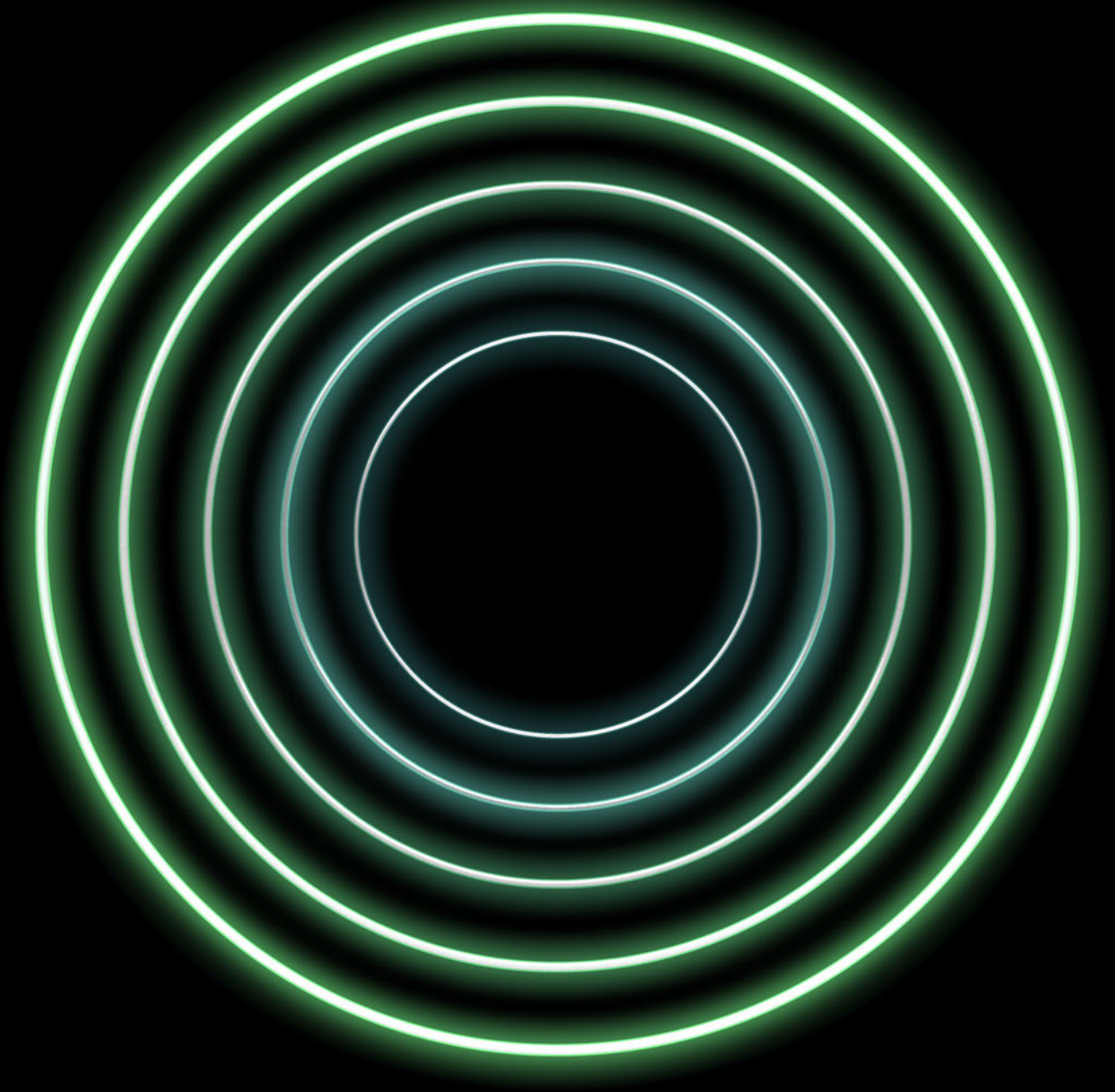
Deloitte.



ICO Audit & Assurance

Key considerations throughout the ICO lifecycle

Deloitte Malta

Audit & Assurance

What is an ICO?

2018 will be another record breaking year in the crypto space. In the first three months of 2018, Initial Coin Offerings (ICOs) raised more money than the whole of 2017. According to data collected by CoinDesk, at $6.3 billion, ICO funding in the first quarter is now 118 percent of the total for 2017[1].

If one Googles for the definition of an ICO, the most commonly returned definition would be that an ICO is an unregulated means by which funds are raised for a new cryptocurrency venture. According to Investopedia, ICOs are similar to Initial Public Offering (IPOs) whereby a stake of the start-up or company is sold to raise money for the entity's operations[2].

Other sources claim that ICO are used to bypass the rigorous capital-raising process in regulated environments.

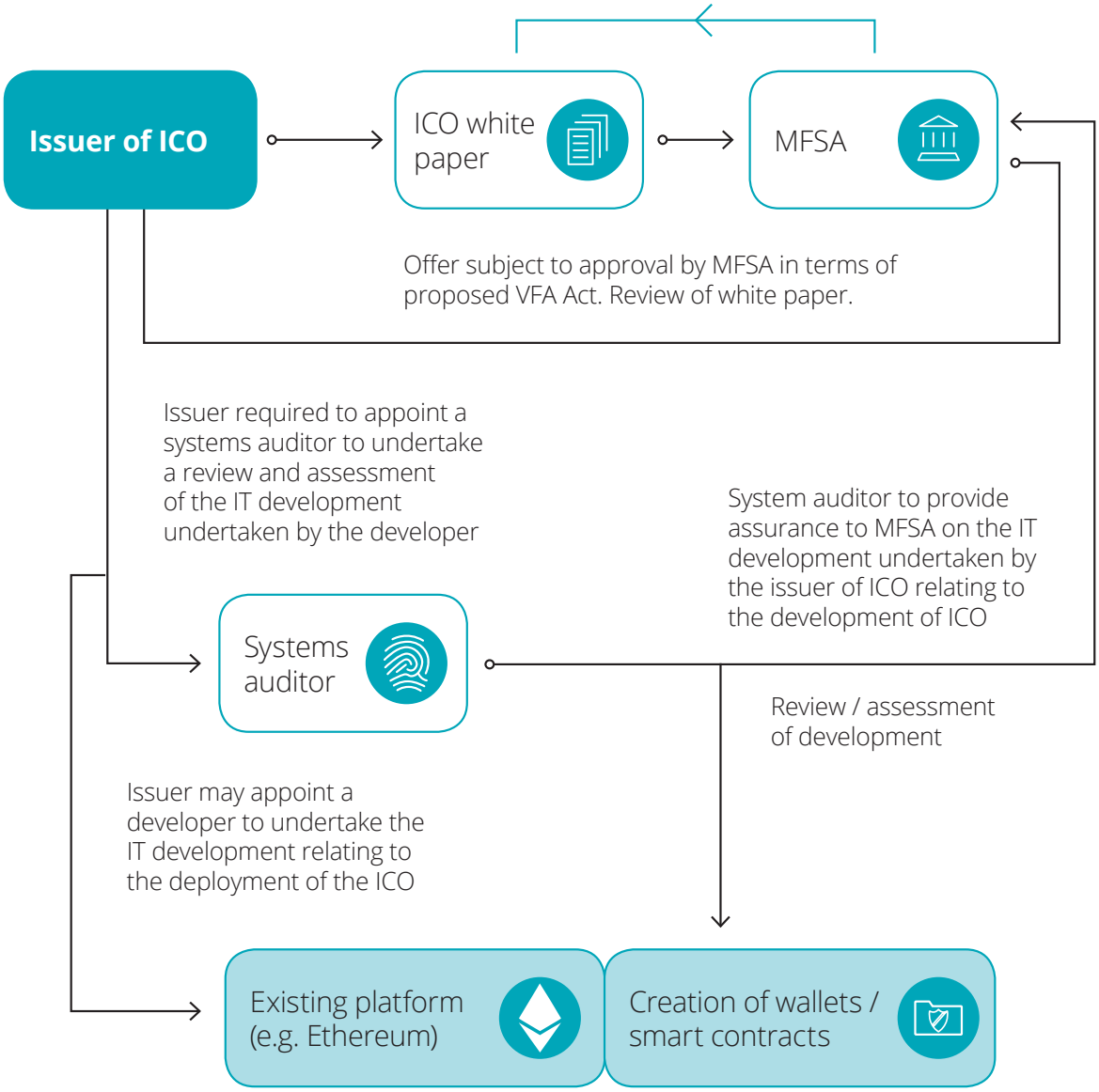
Different governments and authorities around the world have already acknowledged, or are seriously considering, the potential of ICOs as an innovative venture-funding model. Increasingly there are different degrees of ICO regulations and the "unregulated securities" tag that is often attributed to ICOs is fading away. Japan, Germany, Switzerland, Canada, UK and the US are amongst the countries where ICO regulation is available.

After a successful experience in building a reputation of the number one jurisdiction for online gaming; Malta now has the ambition of becoming the "**Blockchain Island**". In the realisation of this strategic objective, the Maltese Parliament approved three important bills on the 26th June 2018 that aim to create the right ecosystem where blockchain companies can flourish and prosper[3].

- Innovative Technology Arrangements and Services Act, 2018
- Virtual Financial Assets Act, 2018
- Malta Digital Innovation Authority Act, 2018

One of the proposed bills is the "Virtual Financial Assets" (VFA) and it intends to set out the framework for ICOs and the regulatory regime for the provision of certain services in relation to virtual currencies[4].

Following a preliminary analysis of the VFA Bill, it is clear that the auditors' function plays a central role in the proposed framework; especially in the processes related to the approval of an ICO.



Auditors are requested to provide the Malta Financial Services Authority (MFSA) the necessary assurances relating to the IT development undertaken by the issuer of the ICO. Within this article, the different stages that are required to provide the necessary assurances will be collectively referred to as the ICO Audit & Assurance IAA processes.

As devised in the VFA bill the key "ICO elements" to be considered in the IAA process are the ICO platform, the digital wallets and smart contracts. Put together, these ICO elements enable a person/investor to receive a token in exchange for another well-known digital currency like Ethereum. ICOs on the Ethereum network issue tokens to the investors via smart contracts.

As such, auditing these ICO Elements individually and in aggregation is crucial to provide the necessary assurances that information security and compliance are effective throughout the entire ICO lifecycle. The tests performed to assess these ICO elements need to address ICO specific risks such as technological risks process risks and regulatory risks.

Smart contracts

At their heart, smart contracts are simply codes - computer codes generated to efficiently mimic the real-world legal deals with executable command lines that makes them behave autonomously as if independent of human interferences[5]. These computer codes act as an intermediary between the ICO issuer and the investors without the need for a third party to overlook and manage the contract contents.

In a study by Deloitte, which identifies six control principles for financial services blockchains, it is recognised that improperly designed and implemented smart contracts can expose the underlying system to security vulnerabilities. As such, the auditing questions raised by the existence of this code on the blockchain may include[6]:

- Who approves changes to the shared codebase?
- How are access control lists within smart contracts administered?
- What determines the right to access smart contract functionality?
- Is this access control mechanism consistent across all smart contracts?
- What processes should be followed if private keys are misplaced or compromised?
- If oracles (off-chain data sources) are used, how is the integrity of the data they provide validated?

In conjunction with the above design of controls assessment, the code used for smart contracts needs to be audited through code review processes. This will ascertain that the smart contract is actually delivering what is being promised by the ICO issuer. Code reviews are highly specialised and expert skills and knowledge are required in order to be in a position to identify abnormal or vulnerable code segments.

Peer reviewed and verified smart contract templates are already available from the open source community and from established blockchain consortia such as the Enterprise Ethereum Alliance. These templates may be used in the design of the smart contract to minimise the risk of introducing new bugs or to serve as a baseline for the smart contract under test.

Assessing smart contracts for vulnerabilities is another key task in the smart contract assurance process. Auditors reviewing smart contracts need to ascertain that the smart contracts are resistant to different types of common vulnerabilities.

The auditor is to establish whether a vulnerability management program is in place to protect the components contributing to the ICO. The auditor is to assess whether the scope and frequency of periodic scans on the network perimeter are adequate and whether the process to investigate, prioritise, accept/mitigate and rectify the identified vulnerabilities is effective.

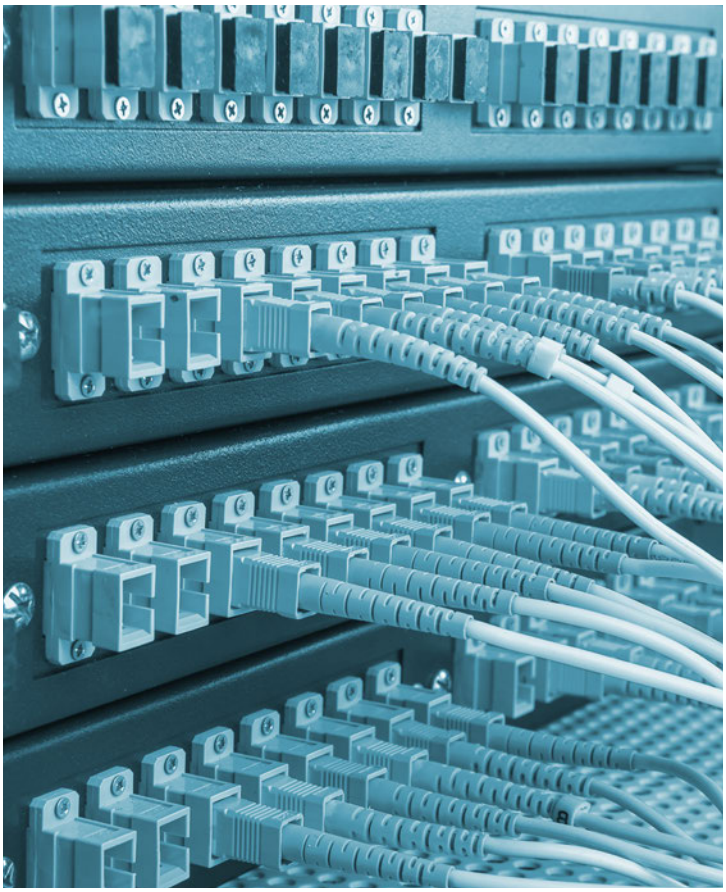
The International Standards Organisation is currently working on issuing a set of standards related with smart contracts. In particular the "ISO/NP TR 23455" which deals with the interactions between smart contracts in blockchain and distributed ledger technology systems; and the "ISO/NP TR 23245" which address the security risks and vulnerabilities of Blockchain applications are under development.

Off-chain components

The amount of data that can be stored on the smart contract is usually limited, thus making it important to decide which data (or meta-data) should be stored on-chain vs. off-chain. The latter also needs to be stored and secured in line with information security best practises.

The auditor is expected to also assess, from a security view point, the off-chain components related with the ICO. Typical examples are the site used to announce the ICO and to publish the contract address, slack, email and other messaging channels.

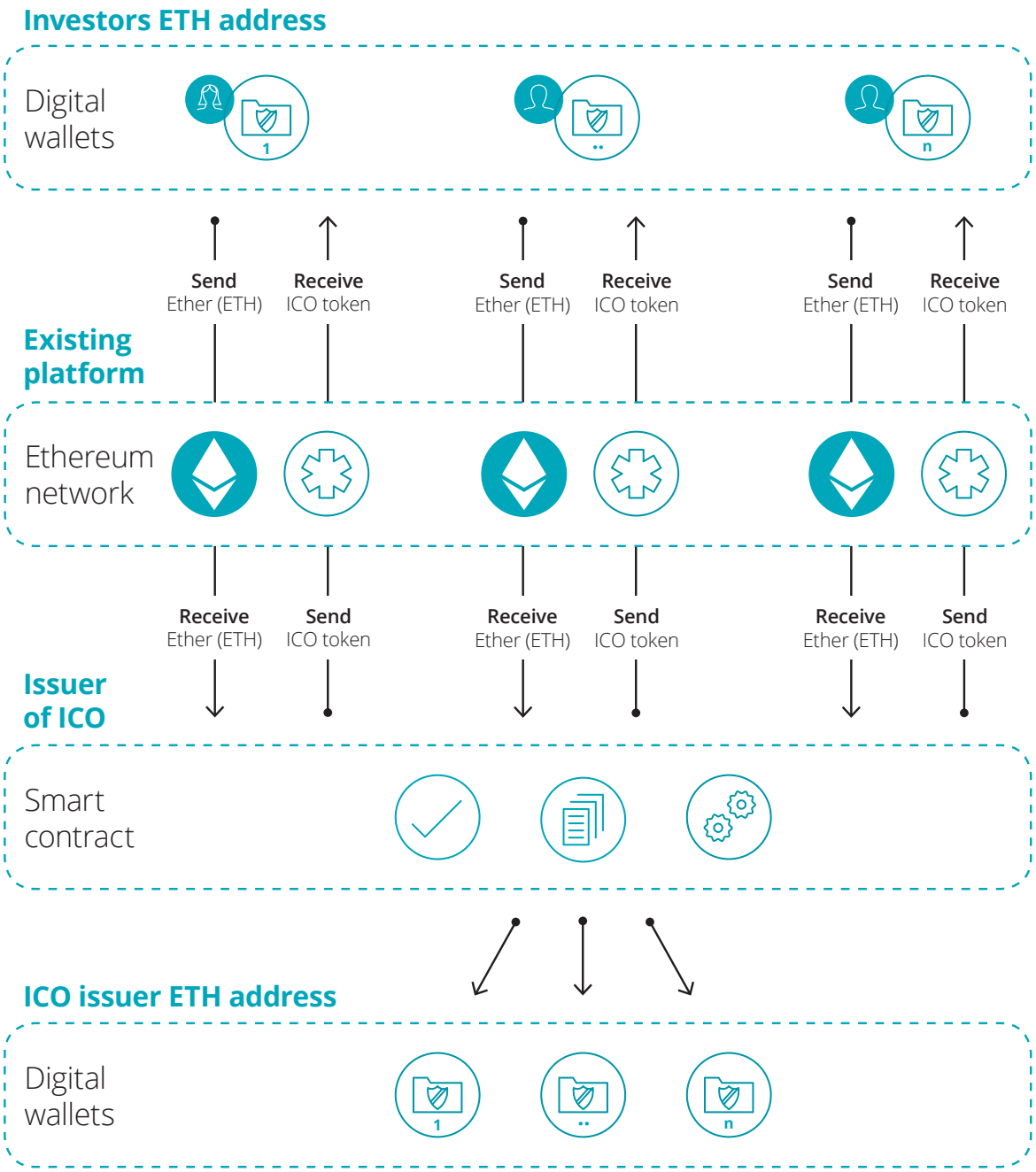
Against a backdrop of technology risks related with this space, especially the novelty of the ICO and underlying blockchain technology, secure communication becomes essential. This propels the demand for platforms that offer end-to-end encryption including off-chain components.



Digital wallets

Another element in the ICO IT environment is the digital wallet. One of the main functionalities of a digital wallet is to act as a repository of the private keys that are used to authorise the ICO actions on the blockchain.

Most ICO tokens (similar to shares in an IPO) are issued on Ethereum blockchain, consequently people who want to participate in the ICO need to have Ethereum virtual currencies and its digital wallet.



The vast majority of the ICOs that are in circulation require an Ethereum ERC20 compatible wallet. ERC20 has emerged as the current industry standard for implementing and issuing tokens.

An ICO is all about sending and receiving tokens. The private keys in the digital wallets are necessary for correct interaction with smart contracts to transfer and receive tokens. Consequently, from an audit perspective it is pertinent that the digital wallets at the ICO issuer are maintained securely and aligned to best industry practices.

In a previous article by Deloitte Malta, entitled 'Blockchain: A game changer for audit processes?"[7], it was mentioned that, in July 2017, an unknown hacker managed to steal nearly $32 million US dollars' worth of Ethereum. Following the necessary investigations, it resulted that the root cause of this fraud was not related to deficiencies in the blockchain technology but, rather, due to a vulnerability within the software that was used to manage Ethereum wallets.

This breach suggests that the digital wallets security is paramount for both the investors and the ICO issuers. For this reason, a security standard in the crypto space, commonly referred to as the Cryptocurrency Security Standard (CCSS), was introduced in 2014 to provide guidance in the secure management of any information system that handles and manages digital wallets as part of its business logic[8].

Assessing the ICO issuer practices for managing digital wallets against the CCSS is one way how regulatory regimes, ICO issuers and investors alike can obtain the necessary assurances that fraud risks related to digital wallets are addressed.

Technology platform

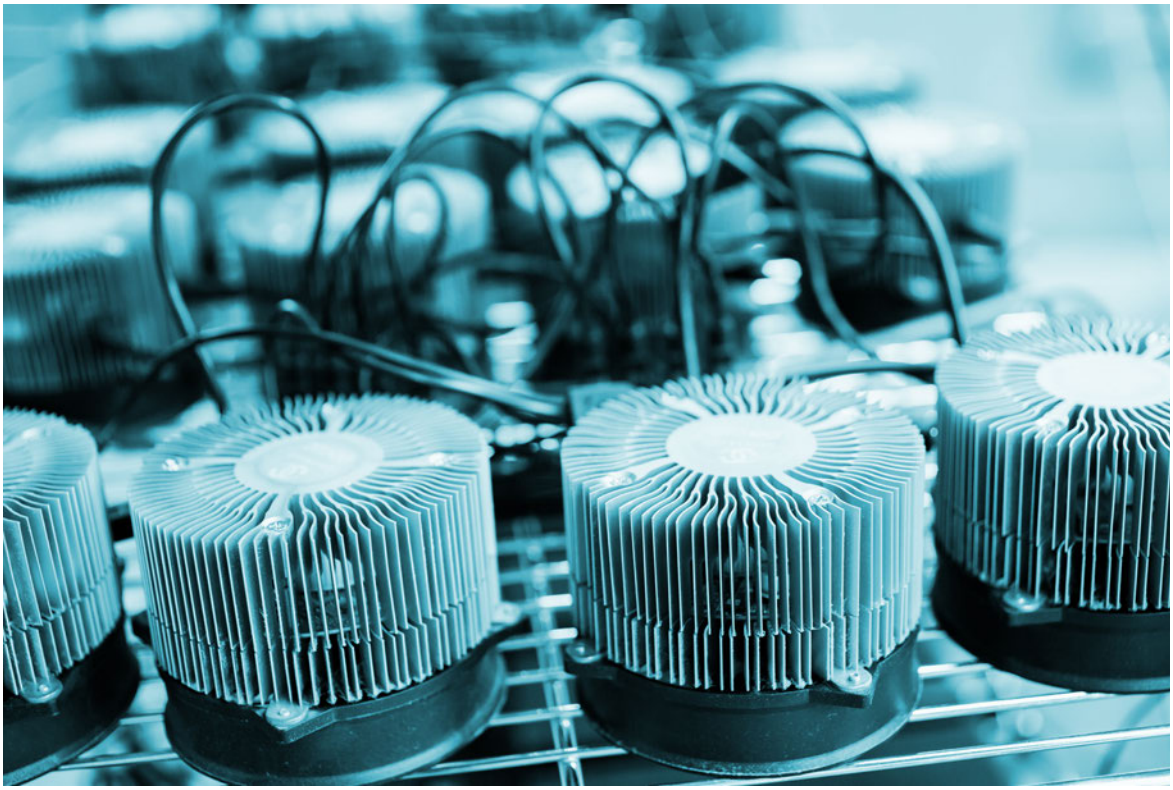
There are platforms whose entire purpose is to ease both the process of launching an ICO and investing in one. They work similarly to platforms that aggregate various crowdfunding projects and make it easy for contributors to find the necessary people who want to invest in their offering.

The Waves platform is one of the largest platforms around in terms of funds raised through crowdfunding. Waves allows anyone, for example a young startup, to set up digital tokens in mere minutes and at almost no cost. The tokens can then be listed on Waves' own exchange, where eager investors can find them easily and companies can secure the necessary funding[9].

In June 2017, the Waves platform reported the integration of the dollar payment gateway into the Lite Client, which allows users to replenish their wallet account in US dollars. It is only a matter of when rather than if, that other FIATs will be integrated to this and other similar platforms.

The auditors' responsibility in the ICO lifecycle is to assess the extent that the technology platform complies with one or more of the five basic trust principles; i.e. whether the systems and processes have the necessary controls to mitigate risks related with security, availability, processing integrity, confidentiality and privacy.

Once again, there is no need to reinvent the wheel in providing the necessary assurances; and the principles behind the SOC 2 or ISAE 3402 reports are fitting to meet the required assurance objectives.



KYC / AML processes

Know Your Customer (KYC) / Anti Money Laundering (AML) is a due diligence process which verifies the identity of customers and ascertains that the money being used for the particular transaction was acquired legitimately.

Whilst the national legislation for ICO is picking up, KYC/AML is a universal concept that's broadly understood in global finance. Consequently, voluntarily complying with KYC/AML regulations provides many advantages to the ICO issuers and its investors, even if they are not currently explicitly mandated to enact such process[10].

From an audit perspective, it is crucial that an independent assessment of the KYC/AML processes is performed to verify an appropriate KYC/AML program is in place. The New York Institute of Finance identifies the following four pillars for effective KYC/AML program[11].

1. The development of internal policies, procedures and controls;
2. Designation of a compliance officer;
3. An ongoing employee training program; and
4. An independent audit function to test programs.

The KYC/AML assurance process is a way to strengthen or improve a KYC/AML program and it should not be regarded as a regulatory burden. A well implemented KYC/AML processes provides the ICO offering and its participants a stamp of legitimacy with regulators and banks. They also enable the ICO issuers to reach a larger global audience and expand the number of jurisdictions in which the ICO offering can take place. Increasingly cryptocurrency exchanges are beginning to exclude tokens/coins that did not properly implement KYC/AML processes.

Deloitte assets in support of ICOs

The tasks involved in providing adequate ICO Auditing and Assurance are highly specialised and extreme caution must be exercised on appointing a trusted auditor.

Due to the breadth of Deloitte services and having already served a number of agreed upon procedures related to different ICO issuers and regulators worldwide, Deloitte is able to offer ICO issuers and regulatory regimes end-to-end support for the relevant aspects of the IAA process and activities.

Deloitte can support the ICO from an assurance perspective through the following services:

Pre and post ICO regulatory support
Work with ICO issuers and regulators to ensure proper status is maintained before and after an ICO. Whilst pre ICO is crucial in the attainment of the necessary licence and regulatory filings; post ICO processes are equally important to provide the necessary assurances that funds and tokens management is well planned and controlled.

Smart contract assurance
Provide assurance on smart contract code and language to ensure code is technically correct and the language is correct.

Digital wallets & key management assurance
Provide assurance on the security of an ICO's issuer held wallets.

ICO Platform assurance
Provide report on controls of service organisation(s) involved in on-chain (ICO Platform) and off-chain components.

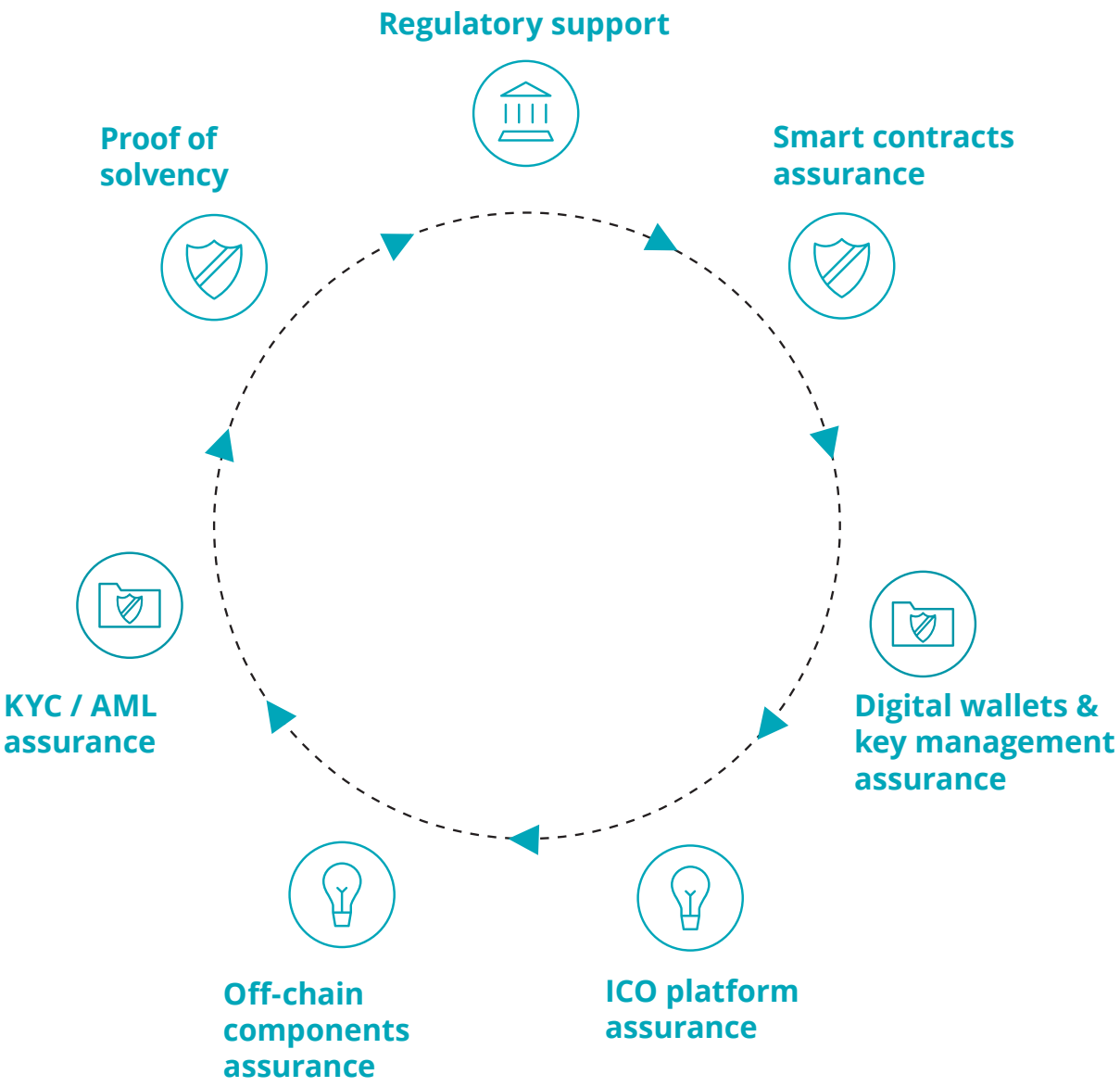
Off-chain components assurance
Provide internal controls reports for the Off-chain components that use, interact with, build, or provide blockchain related services.

KYC / AML assurance
Provide assurance services on KYC and AML issues for organisations ranging from banks to consortia.

- Custody confirmation.
- Traceability coins/ cryptos.

Proof of solvency
Provide validation, existence, and assurance services for digital assets that are representing physical assets on blockchains. Determine that there are sufficient reserves to cover the liabilities.

Deloitte assets in support of ICOs



Conclusion

Although ICOs are a relatively new phenomenon, they have quickly become a dominant topic of discussion within the blockchain community and the capital raised to date has reached astronomical figures.

Nonetheless, as things stand, a barrier that is stopping people from further investing in ICOs is the lack of regulation and trust in the ICO issuers. ICO Audit and Assurance services can provide meaningful information through which informed assessments and decisions can be made by the investors and regulators.

In adherence with the requirements driven by the International Standards on Auditing (ISAs), auditors are required to understand the specific risks to an entity's financial statements arising from IT. It is also mandated to establish how the entity is responding to these risks through implementation of IT controls.

A well planned IAA process that satisfies ISA requirements is crucial to shed light on ICO specific risks and to provide the added value of proposing alternatives on how the identified risks can be mitigated.

Deloitte is a global leader in providing multi-disciplinary blockchain advisory and technology delivery. It has over 1500 dedicated blockchain practices across audit & assurance, consulting, tax, corporate finance and risk advisory as well as dedicated blockchain centres of excellence in New York (Americas), Dublin (EMEA) and Hong Kong (Asia Pacific).

References

1. "$6.3 Billion: 2018 ICO Funding Has Passed 2017's Total" | Coindesk | "https://www.coindesk.com/6-3-billion-2018-ico-funding-already-outpaced-2017/ | April 2018
2. "Initial Coin Offering (ICO) Definition" | Investopedia | https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp#ixzz5FgHP5Ol3
3. http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29079&l=1
4. "Malta A Leader in DLT Regulation. Consultation Document" | The Parliamentary Secretary for Financial Services, Digital Economy and Innovation within the Office of the Prime Minister | February 2017
5. "What is smart contract and why is it needed for an ICO?" | Tokenguru | https://tokenguru.net/articles/what-is-smart-contract-and-why-is-it-needed-for-an-ico/
6. "Six Control Principles for Financial Services Blockchains" | Deloitte | Lory Kehoe, Paul Sin, Niamh O'Connell, Guilherme Campos, Eric Piscini and Eoin Connolly | October 2017
7. "Blockchain: A game changer for audit processes" | Deloitte Malta https://www2.deloitte.com/mt/en/pages/audit/articles/mt-blockchain-a-game-changer-for-audit.html | Sandro Psaila | September 2017
8. "Cryptocurrency Security Standard (CCSS)" | Deloitte Malta | Sandro Psaila | January 2018
9. "ICOs – The New IPOs?" | Deloitte | Dr. Dirk Siegel, Mirko Rene Gramatke, Jens Hermann Paulsen, Wanja Alexej Giessen, Mark Brosig, Sven Heinzelmann, Sawan Sathyanarayana Kumar| 2018
10. "What is a KYC/AML process and why it is important?" | Medium | Daneel Assistant https://medium.com/@daneel_project/daneel-ico-what-is-a-kyc-aml-process-and-why-it-is-important-e922d4f9b169 | January 2018
11. "Anti-money laundering : 5 Steps to conduct an audit" | New York Institute of Finance | https://www.nyif.com/articles/anti-money-laundering-audit-5-steps

Please contact Deloitte Malta Audit & Assurance for more information:

Sandro Psaila
IT Audit & Assurance Manager
spsaila@deloitte.com.mt

Antoine Fenech
Audit & Assurance Senior Manager
afenech@deloitte.com.mt

Michael Bianchi
Audit & Assurance Director
mibianchi@deloitte.com.mt

Sarah Curmi
Audit & Assurance Leader
scurmi@deloitte.com.mt

Deloitte
Deloitte Place
Mriehel Bypass
BKR 3000, Malta

Tel:+356 2343 2000

www.deloitte.com/mt/blockchain

Deloitte.