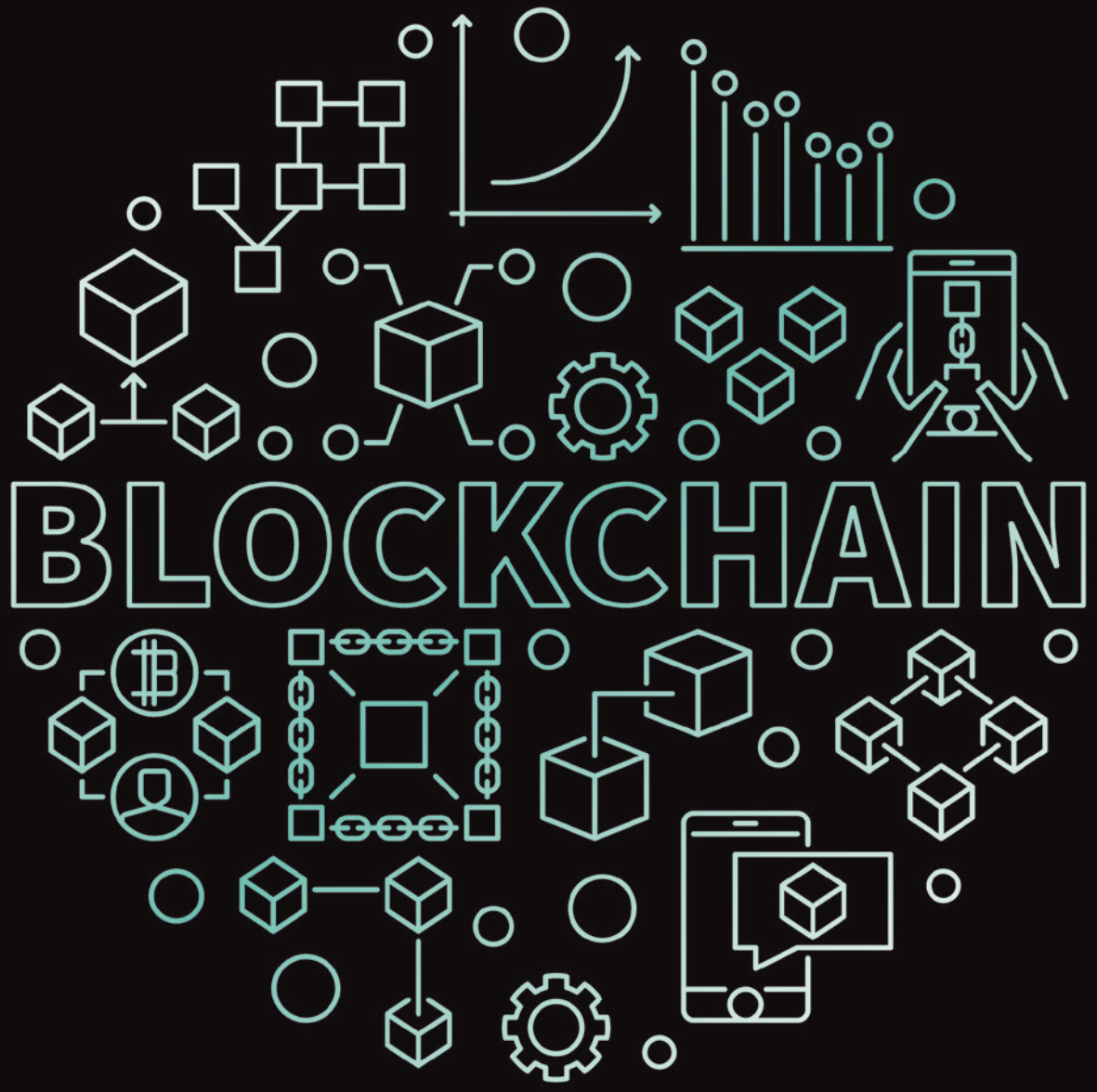
Deloitte.



Building trust in crypto exchanges

Can auditors help through necessary assurance services?

Deloitte Malta

Audit & Assurance

Introduction

Blockchain, the technology that underpins crypto currencies and initial coin offerings, was designed to "create trust" through its inherent properties that include immutability, consensus algorithm, non-repudiation, and encryption. However the general perception of blockchain and crypto assets may be somewhat less favourable such that there are serious trust issues that are inhibiting further expansion of use of the technology. Hacking events such as Mt Gox, the ICO scams such as Bitconnect Coin (BCC), and crypto related money laundering legal proceedings are leading to the erosion of investors' trust in the crypto ecosystem. In the traditional world of finance, it is the financial institutions that provide a degree of trust to ensure that people feel confident that their assets are safe; but what about crypto exchanges?

Regulation

Regulation is intended to play a pivotal role in advocating investors' trust, providing transparency, legal certainty and protection of the integrity of the crypto eco system. Increasingly, different government agencies are introducing new regulatory frameworks for the use of distributed ledger technology / blockchain networks or platforms. The primary aim is that of protecting consumers by setting the standards and rules that are deemed necessary to ensure that the objectives of the underlying technologies are met.

Under the new Maltese regulations, auditors are required to provide reasonable assurance to the competent authorities that the underlying technology is fit and proper for the purpose/s declared[1]. This assessment is commonly referred to as a Systems Audit. The related audit fieldwork and reporting are performed in accordance with the International Standard on Assurance Engagements (ISAE) 3000. Fundamental to the Systems Audit opinion is the extent to which the technology platform complies with the five basic trust principles; i.e. whether the systems and processes have the necessary controls to mitigate risks related to security, availability, processing integrity, confidentiality and privacy. The Systems Audit as mandated by the Maltese authorities spans across forty distinct applicable areas ranging from access control, vulnerabilities management, data retention, change management and risk management, amongst others.

From a crypto exchange perspective, analysing the root causes behind compromised exchanges, crypto fraud and money laundering, one finds a common factor i.e. inadequate or lack of internal controls. Although deemed a critical element, regulatory compliance in isolation is not enough, and a robust corporate governance regime is fundamental in addressing the difficult and complex issues around investors' protection and trust. Amongst the most thematic internal control weakness are poor cyber security programs, inadequate key/wallet management processes and weak due diligence procedures.

Cybersecurity

The large amount of money and crypto assets handled by crypto exchanges, make them highly attractive to hackers. Over the past few years, hacking incidents have translated to losses of investor funds thereby causing huge setbacks to further adoption and trust. Similarly, exchange unavailability or slow execution due to Distributed Denial of Service (DDOS) attacks also negatively impact the trust factor of an exchange.

Adopting an effective cybersecurity program is crucial to prevent and detect external attacks from malicious hackers. Having an adequate budget for cybersecurity is important, but how the program is organised and governed is more impactful than how much is spent relative to a company's overall IT budget or revenue[2].

In conjunction with an effective holistic cyber security program, Deloitte has developed a complementary detection technique that is typically referred to as "Transaction monitoring" – an exercise that reconciles the transactions recoded at the user wallets against the exchange balances and the transactions recorded by Deloitte's own node on the blockchain public ledger. In theory, transactions recorded on the exchange must equal the transactions recorded in the related Wallets as well as the transactions recorded by Deloitte's node on the blockchain. Any resultant discrepancies might indicate that someone has obtained unauthorised access to the exchange's wallet and potentially also performed malicious transactions.

Key management

Numerous blockchain bloggers or correspondents incorrectly claim that blockchain is rife with security flaws. To date, all the known incidents that led to various stakeholders losing their crypto assets are not deemed to be related to deficiencies in the blockchain technology, but are more likely to have resulted from vulnerabilities within the software used to manage/store cryptos (i.e. exchange soft wallets) or to fraud originating from unauthorised access to the private keys.

This suggests that crypto exchange's trust relies on proper private key management and the handling procedures surrounding access management. As custodians of the investors' assets, crypto exchanges need to ensure the confidentiality, integrity and availability of the operational private keys.

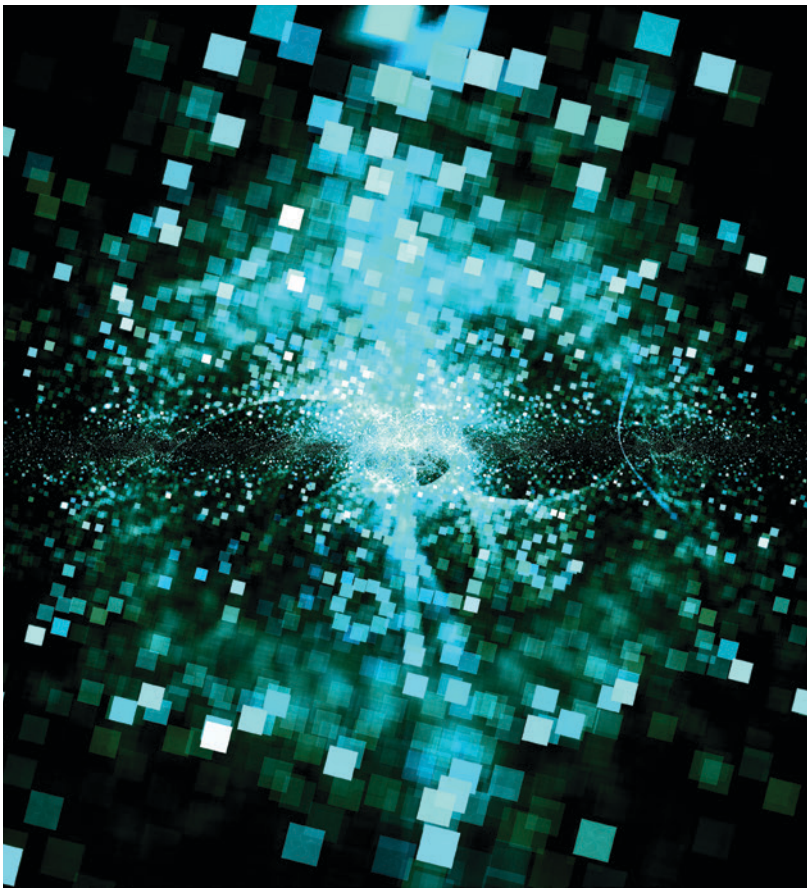
Most exchanges recognise these risks but have not yet found suitable solutions that are both effective and cost efficient. Deloitte have developed propositions that satisfies both these requirements, and which build upon its vast experience with key management in the payment industry. Secure key storage/escrow, fully managed service and cryptographic consultancy to provide a second opinion before launching the next-gen platform; are amongst the unique services being offered in this area.

Due diligence

Although many crypto exchanges do implement various degrees of KYC/AML procedures, it is perceived that more needs to be done around due diligence activities regarding the source of wealth/funds when conducting on boarding procedures.

Deloitte has developed an agreed upon procedure known as "Proof of origin" where, for each provided wallet address, all transactions related to the acquisition of crypto assets positions with fiat currency are verified for consistency with evidence in the form of cash transfer confirmation, bank wire confirmation, account information, loan agreements or similar documents from the various stakeholders, e.g. shareholders, banks, exchanges, brokers and custodians.

In the event that a particular crypto exchange is "named and shamed" for being used for money laundering, the consequences are far reaching and the possibilities of the institution bouncing back are somewhat limited. Consequently, adequate due diligence processes are key to manage and mitigate the related reputation risk.



Exchange convergence

In the first decade of 2000, we have witnessed the convergence of the telecommunication and media industries whereby services, content offerings, and means of communication were integrated under one core technology or ecosystem. Many telco providers started offering 4P services, namely telephony, mobile, internet and television. Financial institutions, and specifically stock exchanges, are bound to experience a similar transformation will it's only a matter of time when such entities will be hosting unified platforms where one can trade traditional financial assets (securities, shares of stock and bonds) as well as crypto assets (security tokens, equity tokens, utility tokens, cryptocurrencies and stablecoins).

Although exchange convergence will be mainly motivated by profitability and market expansion, investors are likely to profit from a host of benefits. Trust is one of these benefits, such that investors are more likely to trade with a known reputable entity rather than an unknown start-up.

Traditional exchanges offer the peace of mind that trading is performed in a legally binding, safe environment. Such reputations are earned over many years and numerous regulation updates. Having crypto exchanges collaborate with traditional stock exchanges, enables them to leverage on the compliance and regulatory expertise developed over the hundreds of years of trading traditional assets. As a result, such strategic alliances are thought to have a positive impact on the investors' protection and perception of trust; and generate trust in crypto transactions.

The 'blockchain island', as Malta has been referred to, is already experiencing the first wave of exchange convergence. In September 2018, crypto exchange giant Binance, Neufund (an equity fundraising platform based on blockchain) and and MSX (a subsidiary company of the Malta Stock Exchange) announced their collaboration which is aimed at creating the first regulated decentralised global stock exchange for listing and trading tokenised securities alongside crypto-assets.

Binance chief financial officer Wei Zhou was reported saying that "This partnership will allow Binance and MSE to host traditional financial assets on blockchain technology through security tokens"[3]. Although this collaboration does not as yet translate into a full exchange convergence model i.e. a common trading platform for traditional financial assets and crypto assets, the Binance, Neufund and MSX alliance is the first step in that direction.

In the foreseeable future, tokenisation of financial assets and other crypto assets are set to experience exponential growth. It is not envisaged that traditional financial assets based on fiat will be eradicated, exchange convergence is therefore seen as critical to provide a platform where FIAT and crypto assets coexist in an ecosystem that stimulates investor's trust.

Conclusion

Although The Economist has described the blockchain as "the trust machine", the control maturity of the off-the-chain components and processes (such as wallets, due diligence and cybersecurity) does not yet do justice to this definition. It is widely accepted that trust is the most valuable asset required to overturn a generally pessimistic view of crypto assets and exchanges alike. Typically, crypto exchanges lack the necessary resources to ascertain whether the related risks are being managed adequately within a robust internal control framework. Third party independent auditors are well positioned to bridge this gap and provide the necessary assurance services. The control procedures applicable to a crypto exchange are also highly specialised. The process to appoint a trusted auditor, must consider whether the provider not only delivers the regulatory compliance aspect but also that the certification is conducted by a reputable entity that can also therefore contribute to the entity achieving a higher trust factor.

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).

About the Author

Sandro Psaila holds the position of IT Audit Manager within the Audit & Assurance service line at Deloitte Malta. He has more than fifteen years' practical knowledge and experience in the IT/ Telecomms industry, most of which is in a role specialising in the fields of Internal IT Audit and Revenue Assurance.

References

1. https://mdia.gov.mt/wp-content/uploads/2018/09/MDIA-Guidelines-Chapter-1-Systems-Auditor-Guidelines_Public-Consultation.pdf
2. https://www2.deloitte.com/insights/us/en/industry/financial-services/state-of-cybersecurity-at-financial-institutions.html
3. https://blog.neufund.org/neufund-partners-with-malta-stock-exchange-and-binance-d01033e60402

Please contact Deloitte Malta Audit & Assurance for more information:

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

Michael Bianchi
Director - Financial Services Industry / Audit & Assurance
mibianchi@deloitte.com.mt

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

Deloitte
Deloitte Place
Mriehel Bypass
BKR 3000, Malta

Tel:+356 2343 2000

www.deloitte.com/mt/blockchain

Deloitte.