Deloitte.

Assurance in a blockchain world

How you can prepare to address the risks

Introduction

As your organization begins to embark on a journey to develop and mature blockchain-related applications, it is important to consider and plan for risks. A quick search of the Internet reveals a series of risks that caused significant loss to various organizations. Blockchain and distributed ledgers are designed to help resolve a number of problems, one of the core areas being trust between entities. This has put trust at the heart of this revolution, thereby forcing the topic into boardroom discussions. Discussions related to risk are happening significantly sooner as a result of the negative media attention associated with cryptocurrencies. Similar to how the advent of the Internet led to an offspring of various new players, blockchain has already seen a similar rise in new market entrants. As blockchain, distributed ledgers, and cryptocurrencies continue going mainstream, stakeholders should consider their ability to mitigate the new risks that arise. These entities need to consider the risks associated with blockchain and which controls are relevant to mitigating those risks. In this paper, we'll explore the unique risks that come along with the technology and business models of these players, notably, the financial, technology, operational, and regulatory risks.

Key players

There are a number of blockchain-based companies who already are well established within the industry. The key players could be categorized into the following groups: Digital Asset Wallet Providers (W), Digital Asset Exchanges (E), Digital Asset Custodians (C), Cryptocurrency Payment Companies (P), and Utility Tokens (U).

Digital Asset Exchanges (E) and Digital Asset Wallet Providers (W)

As entities purchase or acquire publicly available digital assets using Digital Asset Exchanges, the exchange typically provides the customer with a wallet to store their newly acquired assets. While there are several wallet providers, it is important for entities to consider the risks associated with the security of the platform and the availability of the assets (see Table 1 for a list of associated risks). Entities have utilized a variety of mechanisms to assist customers in securing their assets, ranging from a simple username and password, to complex multi-factor authentication coupled with multi-signature wallets. Entities that store digital assets on exchanges should be asking a series of questions to their potential service provider prior to engaging in business. Some questions an entity might ask include:

- What percentage of the digital assets is stored in hot wallets versus cold wallets?
- How are digital assets going to be secured?
- What is the service provider's process to prevent misappropriation of assets?
- Are funds commingled with other customers?
- What happens if the service provider is hacked and loses a significant amount of digital assets?
- What controls does the service provider have in place to reconcile customer balances to protect blockchain data?

Digital Asset Custodians (C)

Similar to wallets, digital asset custodians provide an additional layer of services on top of standard wallet providers. Custodians have built out control environments that financial services institutions require in order to place trust and confidence in the solution. Custodians typically charge a service fee, which funds activities such as audit trails; automated business logic to set withdrawal limits; whitelisting IPs and blockchain addresses; third-party assurance reports; and built-in, role-based access. While the primary purpose of wallets is to act as a means of supporting transactions and to temporarily hold assets, custodian services are designed to act as storage of digital assets for longer periods of time. For this reason, security is of paramount importance to the custodians as compared

to the availability of services relative to digital assets exchanges. Examples of questions to consider include:

- What monitoring controls should the user entity implement related to usage of the custody service?
- How does the ledger work to ensure that the customer receives all transactional details associated with an account?
- If there is a theft by an internal or external actor, what assurances does the service organization provide?
- Which third-party certifications does the service provider have and what is the reputation of the organization providing the certification?

Cryptocurrency Payment Companies (P)

Cryptocurrency Payment Companies allow merchants to accept cryptocurrency as payment for the goods and services they sell. The merchants typically receive some form of fiat currency (i.e., USD) in exchange for a digital asset such as bitcoin. Given how quickly the digital assets are exchanged for USD, the risks related to processing of information are of much greater importance compared with the ongoing security and availability of digital assets. Examples of questions to consider include:

- What fees are charged by the service provider to process transactions?
- Who pays the blockchain miner fees associated with a transaction?
- Does the service provider have a dispute resolution process?
- Given the high congestion on the blockchain network, how quickly does the customer get access to USD funds?

Utility Tokens (U)

There are several other start-up entities that are using the Ethereum blockchain ERC-20 Utility Tokens (U), commonly known as Initial Coin Offerings (ICOs). It is important for enterprises to start considering the risks related to these tokens and services. Such tokens are commonly represented as units of service that can be purchased on a variety of digital assets exchanges. Historically, products have been developed prior to being sold in the marketplace. With the advent of crowdsourced funding, ICOs are one such mechanism sold to sponsor development of technology products. The tokens are not intended to be utilized as currency, but they do have a derived value based on the ability to trade them on exchanges. Entities planning to use such services or companies that are issuing tokens should address the key risks related to such tokens. Some questions to ask include:

- Has the issuer of the ICO documented all of the regulatory considerations with respect to issuance of these?
- Are these securities or not? How is the customer going to account for these tokens?
- What are the tax implications?
- What could go wrong related to the technology and ICO issuance?
- What are we doing to mitigate the risks related to theft during the issuance?

Blockchain risk considerations—responsibility of customers or service providers?

In addition to standard financial, technology, operational, and regulatory risks, blockchain and cryptocurrencies come with their unique set of risks and challenges. The table below is not an all-inclusive set of risks, but an illustrative set of topics from which entities can generate dialogue. The table also includes where the risks reside (e.g., at organizations providing the services to enterprises (service providers) or entities using such services for their business operations (customers)). It also specifies what risks apply to the above-listed service providers. For example, fluctuation in the market price of a digital asset isn't a significant risk of a custodian. Also note that risks are listed from the perspective of customers and not service providers (e.g., fraud risk for a customer's business includes risk of fraud at the entity, as well as at the service provider. Therefore, the customer needs to obtain assurance about their business and their service provider.)

Category	Enterprise risks (Entities using blockchain products/services)	Where do risks and related controls reside? ("Customer" and/or "Service Provider")	Relevant Service Providers (W,P,E,C,U)
Financial	**Fraud** Threat of fraudulent tokens	Customer Service Provider	W, E, C, U
	Market fluctuation Unregulated market; prone to price volatility	Customer	E, U
	Theft Loss of cryptocurrency/token due to cyberattacks, etc.	Customer Service Provider	W, P, E, C, U
	Embezzlement Loss of cryptocurrency/tokens due to misappropriation	Customer Service Provider	W, E, C, U
	Financial reporting risks Risk related to presentation of statements, cutoff, disclosure, etc.	Customer Service Provider	W, P, E, C, U
Technological/ Operational	**Information/cybersecurity** Manipulation of proof of work network, security of wallet	Customer Service Provider	W, P, E, C, U
	Traceability Reconciliation/tagging of blockchain transactions to internal ledgers	Customer Service Provider	W, P, E, C, U
	Slow transaction confirmation Delay in confirmation due to volume of transactions on blockchain	Service Provider	W, P, E, U
	Commingling of funds Use of concentration accounts, inadequate funds to fulfill customer transactions	Service Provider	W, E, C
	Irreversibility Immutability results in irreversible fraudulent/ erroneous transactions	Service Provider	W, P, E, C, U
	Key management Theft or loss of keys used for encryption and access to wallets	Service Provider	W, P, E, C, U
	Insufficient infrastructure and application controls Lack of standard IT controls such as segregation of duties, segmentation of network, application access, change management, etc.	Service Provider	W, P, E, C, U
	Governance framework Lack of governance framework, entity-level controls, oversight	Customer Service Provider	W, P, E, C, U
Regulatory	**Regulatory ambiguity** Unclear, evolving, and varying regulations across jurisdictions	Customer Service Provider	W, P, E, C, U
	Money laundering Lack of clarity on frameworks necessary in order to comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements around the world	Customer Service Provider	W, P, E, C, U
	Other illegal activities Use of cryptocurrency for terrorism financing, drug or human trafficking, illicit goods, etc.	Customer Service Provider	W, P, E, C, U

One solution: Third-Party Assurance reports

Entities utilizing any of the blockchain services referenced should be focused on these risks and consider what level of risk-mitigation assurance they would like. Given the volatility of the markets and increasing use of such digital assets, many customers are concerned about the availability of the services and access to their funds. While a majority of these risks reside at service providers, customers need to be aware of the same and plan to address them by identifying ways of evaluating controls at the service providers. There are a few different ways of evaluating risks and controls at the service providers. One way is for service providers to get a report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (Trust Services Criteria), also commonly referred to as a SOC 2 report. Given the nature of the technology and the lack of publicly available mature frameworks, it is incumbent upon the service provider to select a qualified service auditor. While not required, many service providers are starting with a controls readiness engagement and then plan to obtain Type 1 (report on management's description of a service organization's system and the suitability of the design of controls) and eventually a Type 2 (report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls). A control environment that effectively addresses the risks would consist of a combination of traditional controls and controls addressing blockchain-specific risks. Rapidly changing technology will continue to introduce new and unique risks in the environment and, therefore, customers and service providers alike will need to adapt and continue addressing such risks.

Contacts

Tim Davis
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 206 716 7593
timdavis@deloitte.com

Seth Joseph Connors
Senior Manager | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 313 394 5139
sconnors@deloitte.com

Soumabrata Dasgupta
Manager | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 206 716 6067
sodasgupta@deloitte.com

Yogeeta Raisinghani
Manager | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 206 716 6548
yoraisinghani@deloitte.com

Deloitte.