Introduction

It’s not often that we get to live through a technological revolution as significant as the Internet. And by many accounts, a similar revolution is happening today: the birth of a digital asset class known as cryptocurrencies, or more broadly, cryptoassets.

Cryptoassets are digital assets in which cryptographic techniques are used to regulate the generation of units of the asset and to verify their transfer between parties via a blockchain without a central party. Different cryptoassets have different features, behaviors and uses; while some behave as a commodity or a form of payment, others behave more akin to a security.

In 2009, there was only one cryptoasset in the market – bitcoin. Today, more than 1,500 cryptoassets exist, with many more created monthly. The market capitalization of these cryptoassets has grown tremendously as well. As of year-end 2017, the market capitalization for all cryptoassets was an astounding $573 billion, which equates to growth of over 3,237% in the course of one year.¹ Cryptoassets, it seems, are getting too big to ignore.

With this exponential growth comes many novel challenges. Financial institutions are accustomed to servicing traditional assets, such as equities, bonds and physical assets, like gold. Many of the skill sets required to service these traditional assets, however, are difficult to apply to cryptoassets, which exist in a purely digital form and typically as a form of bearer instrument.

To date, the players enabling the market for cryptoassets have been primarily FinTech startups. But as the market is maturing and the industry user base is growing, customers are looking to traditional financial institutions to provide access to this asset class. As firms assess opportunities, we would like to highlight some key considerations that may be faced and ways these challenges can potentially be mitigated.

¹ https://coinmarketcap.com/historical/20171231/
Key management challenges

One of the greatest challenges in managing cryptoassets is the management of the cryptographic keys that govern the transaction process. Transfers of cryptoassets are controlled using a cryptographic technique known as digital signatures. Assets are sent from one blockchain address to another by “signing” a transaction using what is known as the private key — usually represented as a string of numbers and letters that acts like a password, or a key to a vault. While this makes sending cryptoassets straightforward, it opens up considerable security considerations: that is, the assets are only as secure as the private key that controls them. If a malicious party accesses the private key, they have total control over the underlying assets in the address controlled by the private key. If the private key is lost, there is no way of accessing the assets and they will be forever inaccessible.

For this reason, storing, operating and backing up the keys are crucial, and each of these procedures has its own unique considerations.

Storing keys

Key storage typically comes in two forms: hot storage and cold storage. Hot storage refers to safekeeping private keys on a device that has access to the internet, while cold storage refers to a device that is offline, or not accessible via the internet. The challenge is in determining the optimal tradeoff between accessibility and security.

An asset whose private key sits in hot storage, for example, is easy to move from one account to another as transactions can be instantly signed and sent. The tradeoff, however, is that the asset is also less secure, since it’s potentially open to attackers via the same connection. Cold storage suffers from the opposite tradeoff. Since it’s disconnected from the internet, moving assets out of cold storage can be cumbersome and time consuming, yet safer and more secure. It is worth noting, however, that assets can be sent to an address whose keys are in cold storage, without needing to take the keys out of cold storage.

Determining the proportion of assets held in hot storage vs. cold storage will depend on each institution's activity profile. For example, hedge funds that trade frequently may want to have more assets in hot storage. Custodians providing services to high-net-worth individuals, however, may want to place the majority of assets in cold storage for long-term safekeeping.

Key operations

Since sending transactions requires access to private keys, establishing an operational process for securely managing cryptocurrency transactions can be technically complex. In particular, an organization should establish a secure environment with appropriate controls that do not allow any one individual – or group of conspiring individuals – to access funds in an unauthorized way.

A number of technologies can be leveraged to implement this. Multisignature addresses, for example, are addresses that require two or more private keys to send transactions: much like cosigners on a bank account. In this way, no single operator has full control over the assets.

The operational model may differ as well, depending on the services being provided and level of security desired. For example, an operational structure that allows consumers to manage their cryptoassets directly — that is, full control to send and receive their assets across the blockchain — requires a very different structure to a model that only permits buying and selling activity, akin to commodity trading. While the former may provide more facilities for consumers, providing direct access to the assets may have security and regulatory issues that are more complex than a simple buy/sell facility.

Key backup

As a loss of a private key means a loss of assets, backups are critical. Secure enterprise backup solutions typically fall into two categories: hardware secure modules (HSMs), and physical backups.

HSMs are hardware devices specifically designed to securely generate and store keys, typically for enterprise-grade key management solutions. The benefits of HSMs is that they can be configured to store the private keys without ever revealing them outside of the device, which is a significant security advantage.

The second type of key backup solution is storing private keys on a physical material, such as steel or paper. While the solution may seem archaic at first, physical backups have one key strength over HSMs: they are immune to electromagnetic attacks. To further protect against exposing the private key on physical devices, key backups may be split into multiple pieces using a cryptographic technique known as sharding and sent to secure locations over the world. This technique enhances security, requiring the key to be reconstructed from the shards in order to be used.
Product challenges

Cryptoassets as an asset class face some unique challenges in how they behave due to their being based on public blockchains. Through a rather technical process, these public blockchains can be either copied, creating entirely new assets that can be claimed by owners of the original cryptoassets (called an “airdrop”) or may split in two, duplicating the original cryptoasset (called a “fork”).²

Airdrops and forks can be arbitrarily performed by anyone, and consequently the primary challenges with airdrops and forks are twofold. First, how do you determine which airdrop or fork to support? Second, is your infrastructure set up to hold multiple different cryptoassets, which will inevitably be the result of an airdrop or a fork?

As part of developing a cryptoasset product – especially one that will custody customer assets – companies need to decide what criteria have to be met in order for an airdrop/fork to be onboarded onto the product. Not accepting any forks or airdrops may not be acceptable if a fork or airdrop turns out to have market value. On the other hand, as anyone can create a fork or an airdrop, it would be impractical to accept all, as establishing operational processes and infrastructure to handle this would become cumbersome very quickly.

Financial crime challenges

Financial crime is top of mind for regulatory and reputational risk purposes. Fortunately, vendor products for most popular digital assets such as bitcoin and litecoin are available to facilitate the monitoring for illegal activity. Using this type of monitoring software can detect many types of financial crime activity, however, typologies for such activity differ significantly from those found in more traditional financial instruments.

Consequently, certain activity is difficult to monitor. Due to the nature of blockchains, it is difficult to determine if a cryptoasset sent from one address to another is in breach of sanctions, as no physical location is associated with the transfer. Due to these sort of complexities, some institutions are choosing to limit activity to buying and selling of cryptoassets, rather than enabling transfers between arbitrary parties.

Capture the opportunities, but do it right

In a rapidly changing financial world where technology is quickly bearing down on the industry, it would be amiss to not consider the potential of this new asset class. As interest increases among traditional financial institutions, we are seeing organizations establish infrastructure to claim key market positions in the emerging ecosystem.

We recommend our clients determine their cryptoasset strategy by asking themselves a number of questions. First, what are your business's core competencies, and how may these be applicable to cryptoassets? For example, your clients may be expecting fund administration, custody or management of such assets in the future: will you be able to provide the function?

Second, how strategic a position do you wish to take in the market, and is there an opportunity to capture adjacent markets to your core competencies? For example, there may be a market opportunity for fund administrators or asset managers to expand into custody services. Taking on such roles, however, will typically require your organization to establish new functions and hire unique skill sets.

Third, considering your desired strategic positioning, what is your appetite for risk, and how do you manage? It is unlikely that the first step toward your strategic position will be the final state: how do you best leverage current technology and vendors in your product road map?

Finally, how do you design your product in the most scalable, secure way using industry leading practices and ensuring you have the right skill sets for long-term success?

Technology now will not be the same as technology in the future. With increasing technical advancements in the cryptocurrency space, it is highly likely that this is just the beginning of a new financial ecosystem. Understanding how this technology works and building institutional expertise will certainly benefit the organization as it evolves. Managing cryptoassets is complex and requires different technology and operations than most financial institutions are used to: however, as with most things, where there is complexity, there is opportunity to be captured.

² For more information on forks, please see https://www.coindesk.com/short-guide-bitcoin-forks-explained/
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2018 Ernst & Young LLP.
All Rights Reserved.

1809-2901887
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com

Contacts

Eli Stern
Ernst & Young LLP
Americas Financial Services Advisory
Blockchain Leader
eli.stern@ey.com

JB Rambaud
Ernst & Young LLP
Principal
jb.rambaud@ey.com

Charles Smith
Ernst & Young LLP
Executive Director
charles.smith@ey.com

David Loffredo
Ernst & Young LLP
Principal
david.loffredo@ey.com

Natasha Wheatley
Ernst & Young LLP
Executive Director
natasha.wheatley@ey.com