DIGITAL CUSTODY

EVOLUTION

ALFASEC RESEARCH REPORT

AlfaSec Advisors Pte. Ltd.
20 Collyer Quay #09-01
Singapore, 049319
M (+65) 9738 7590
Marketing@alfa-sec.com

INTRODUCTION

The growth of digital assets and their increased usage as an investment opportunity had initially been met with great skepticism but now are undoubtedly becoming more important as potential investments for asset managers. This relates to crypto currencies but also other assets such as security tokens.

With simplicity we often try to explain the concept. A standard explanation is to compare the custody of digital asset to a standalone vault full of gold which can only be accessed by one key. Whoever has the key owns the gold. This may be simple but not entirely accurate - unfortunately, the devil is always in the detail.

A digital asset is comparable to a bearer instrument – the ownership passes not with a bearer document but with the exchange of unique keys. Like a bearer document, if the keys fall into wrong hands or are lost (destroyed) the asset is mainly irrecoverable.

Here we look at some of the potential implications for those who wish to act as a custodian to these investors and how these assets differ to traditional custodian functions.

WHAT DOES IT TAKE TO OWN A DIGITAL ASSET?

It is not easy to find a common acceptable definition of Digital Assets however if we look to the International Monetary Fund (IMF) they have provided a statement as follows:

" A digital asset is a representation of value made possible by advances in cryptography and distributed ledger technology. They are denominated in their own defined units of value and can be transferred peer to peer without the use of an intermediary."

An investor in a digital asset on a public blockchain basically has a distributed ledger entry that is secured by technology and computer code which makes it hard to tamper with and censorship resistant. Its access is secured by a two-pass code combination:

- Private Code (or key) is a string of numbers or alphanumeric codes that were randomly composed by the initiator of the transaction (at the time a wallet was set up). The assets attached to this private key would be unrecoverable when the key is lost (at least for several public blockchains)
- Public Code (or key) is a second key created using the aforementioned private key however made public and can be known by many individuals. The Public code is used as an address to identify the parties in the network.

Once an investor has purchased a digital asset, they basically have a few options with regards to custody. The primary option to date is that the investor himself will keep the keys and execute the transaction on a proprietary basis. The alternative would be to allow a third party (custodian) to manage these codes on behalf of the investor. A third potential option would be to use an Exchange – where the exchange holds the private keys, and the investor has access to a share (via a digital wallet) of what could be a co-mingled pool of digital assets. In practice, this set up is more complex given key sharing and other forms of hybrid models.

The risk associated with holding assets on public blockchains is significant as should the key get lost or a cyber attack steal those keys the asset is irrecoverable. There is no central governance so the risk to loss is huge and despite potential insurance policies (many are still emerging in this space) the custody challenge is not to be underestimated.

Custody is amongst the largest factors, that will enable institutional investors to further develop and invest in Digital Assets. The ability for a Custodian to provide a safe environment, trusted by Institutional investors who demand that their assets are safe and secure over the long term is paramount. Solutions need to be scalable and not dependent upon layers of controls that sacrifice volumes and security.

Solving the challenges in the institutional custody capability will be a key driver to allow scale into the market and ultimately drive the inevitable growth of this new asset class.

How are Digital assets (Crypto) Different to Traditional Custody?

A traditional custodian would be holding assets for clients in omnibus or segregated accounts, enabling transactions on those assets, processing entitlements, and reporting the assets to the client. There may also be a question of valuation which is a separate category of challenges. Here are some of the key digital custody differentiators:

- Public blockchain networks do not have a concept of nominee holdings since a holder of a private key is able to spend or mange the asset. This will mean that for each digital asset the Investor may need a separate account with those exchanges on top of the custodian employed unless they trade through a prime broker, in which case that responsibility or risk is with the prime broker. This clearly challenges the benefits that the industry has attempted to reap over the years through so called fungible securities and "omnibus holding" that concentrate positions in one account for all investors.

- The different crypto asset are traded on different exchanges. This clearly adds to the proliferation of vendors who need to be approved and managed as part of the industry's best practice. Each exchange will also have its own procedures around the movement of assets. Each exchange will also have separate access points either via an API or standalone proprietary web enabled input screens that need to be activated to see and move assets. These screens then have user rights and passwords all of which also needs administration.

- The movement of traditional assets is via a Client instruction that is authenticated at the CSD or Custodian. The intermediary then moves assets as instructed. The authentication of the instruction is done via signatures or standard industry security codes. Instructions can be one to many to save time. If a problem arises parties intervening can often fix the problem by adjusting the delivery or receipt requirements. With a digital asset the only authentication within the Blockchain network is the Private key. If that key gets lost or stolen the asset is gone.

- This brings up a new challenge namely how best to store all these private codes for the individual assets. There is no traditional custody concept that easily applies to private keys. If these are lost or stolen the asset is lost and mainly irrecoverable. Keeping these keys is a major feature of digital assets. It is also amongst the biggest headaches. Keep the keys on the main servers of the institution they become vulnerable to insider fraud and cyber-attack. If the keys are kept offline (or cold storage) they become difficult to access. Today's asset management regulation provides for a custodian's strict liability for the loss of assets depending on the market model – digital asset thus creates a new scale in liability and certainly a new contractual condition.

- Cyber Security is a challenge with traditional assets – but tends to magnify many times when we think about the private key storage. A potential weakness of an Exchange Wallet is that they are vulnerable by virtue of existence – a place that provides huge temptation to attack in the hope of gaining access to many private keys.

- In traditional settlement we are familiar with the concept of Delivery or Receipt against Payment (DVP/RVP) and we use that concept to net positions where possible to reduce intraday and potentially overnight funding requirements. This concept is not in broad use when it comes to digital assets. The release and capture of assets is an independent function – that may rest on a process that provide close to or near DVP. In effect its either cash before delivery or free delivery.

- Due Diligence and certification of traditional custody assets takes place through tried and tested methods that have been adopted over many years. Internal independent reviews and external audits provide institutional investors with some security that good oversight and applicable procedures are in place to secure assets under custody. These need to be re-written to accommodate crypto assets and create a similar high standard that institutional investor can rely on to judge best process amongst provides. It will also be aa critical aspect of competitive review to allow institutional investors to do due diligence and understand in depth the processes and controls to keep institutional assets safe.

- Last but by no means least the question of regulation comes up. A digital asset can be many things. It can be a currency; it could be a security or represent some form of commodity. In fact, it can be many more things. In addition, digital assets today, are often managed via national rules and regulations, yet the beneficial owners

of those assets are often in cross board jurisdiction. Another important issue arises in that who regulates these assets and which of the current regulations apply to digital assets in any one country?

INVESTOR ADVANTAGES THAT FAVOR THE USE OF CUSTODIANS

As these digital assets grow in number, scale and size clearly the investor will want to see ways to outsource these tasks to a reliable third party. They are clearly more challenging that traditional assets, which much greater risk attached but Custodians have traditionally been good at accumulating inefficiency and gradually creating standards and simplicity. It's part of their DNA. It is also going to be a bigger part of their future – as these positions will continue to evolve and grow to meaningful size.

Custodians are practiced at creating the environment to talk to investors, market infrastructure, regulators, and counterparties in order to create the rules and process that will allow this asset class to gain greater acceptance. This in turn helps investors as they do not single handily have that scope and hence custodians can play a large roll.

The web based and online nature of these assets creates a huge challenge around systems security and cyber risk. Custodians have substantial expertise and IT capability to explore and find solutions that protect assets from undesirable events.

The opportunity is there to participate in a huge growth sector that clearly is looking for asset security – as always with custody is it is a product for "the brave of heart".

FUTURE is about substantial CHANGE.

Custody and the associated asset servicing functions are currently undergoing substantial transformation. T2S in Europe, MIFID and EMIR all have brought huge change. In Asia we see reforms across countries such as stock / bond connect in China and the 2025 ASEAN Blueprint and capital markets vision. On the technology front we see substantial changes where automation and AI are transforming processing. Digital Custody will further streamline many functions – arguably creating greater concentration of function and removing the need for physical presence. All this will lead to substantial HR dislocation, continued industry operational and clerical redundancies.