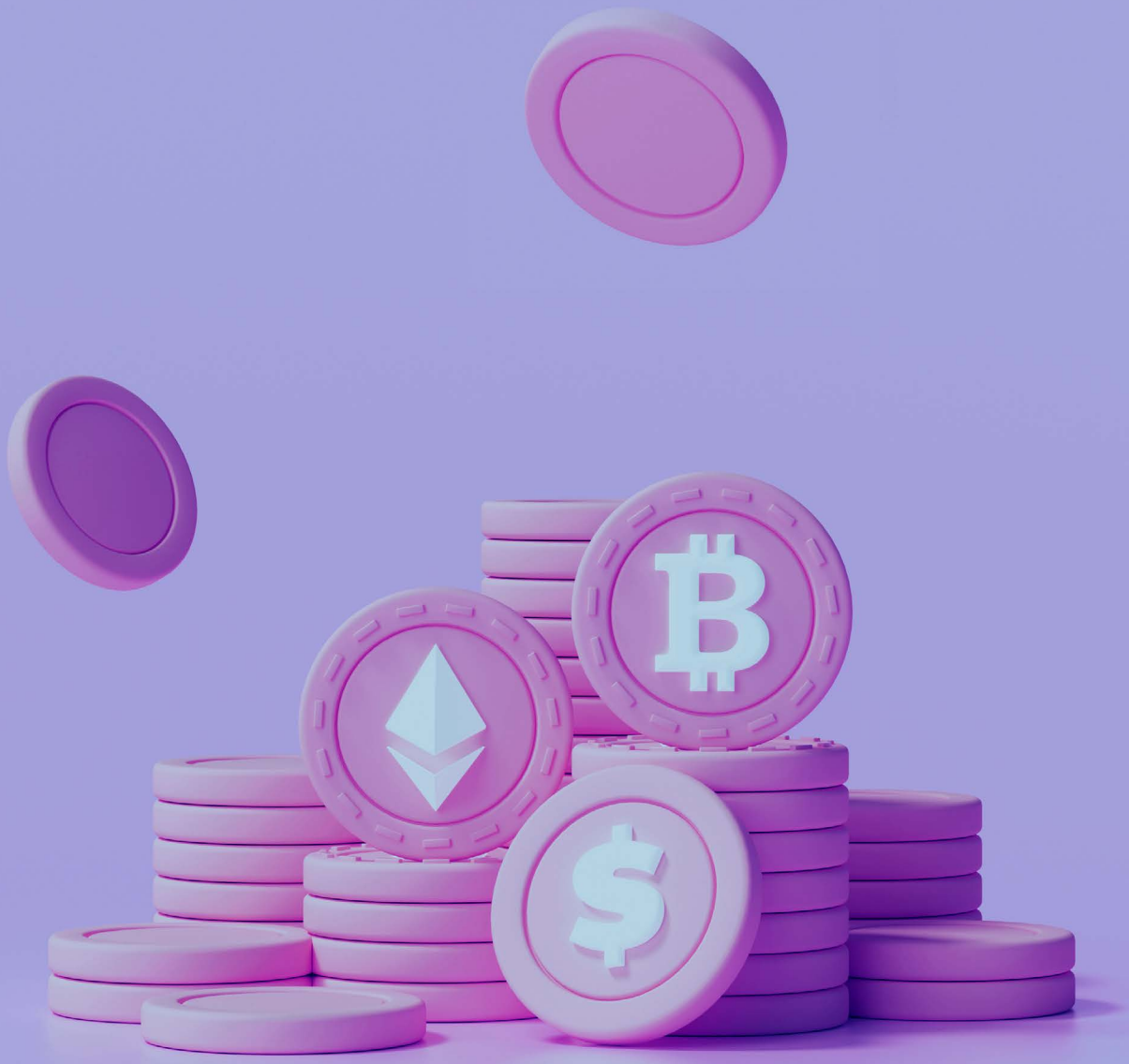
TREASURY EXCELLENCE AS STANDARD

MAY 2023



A treasurer's guide to opening a crypto wallet

Contents

Nothing in this guide can be construed as providing professional advice and as always, readers should make suitable enquiries of their professional advisers before they take any relevant action.

CIRCLE KPMG RAMPARTS

1 Purpose of guide and introduction

What do you do when your CFO asks you to open a cryptocurrency wallet? In response to guidance that was requested from the treasury community, the Association of Corporate Treasurers (ACT) has compiled this guide with contributions from Circle, KPMG and Ramparts to help treasurers work out their response.

While the idea of crypto may still seem new to many people and companies, it is almost 14 years since the Bitcoin network came into existence. Over time, the treasury community has watched with a mix of interest and scepticism as the ecosystem has grown exponentially. Stellar price rises followed by lightning crashes have all encouraged risk-averse treasurers in the belief that it is prudent to monitor developments from the side-lines – especially when there are plenty of other (and more pressing) treasury matters to deal with.

The ACT has followed the development of the crypto market and produced a series of webinars with the support of Copper.io and Arcalabs to share insights on the use of crypto – especially as a digital asset. The series can be found here. In addition, there has been a variety of articles in the print and online editions of *The Treasurer*.

In 2020/2021, there was some interest among treasurers but mainly those working for organisations operating in the digital space. Furthermore, some treasurers have become involved in this space through the growth in the market for NFTs (non-fungible tokens) and others through their business experimenting in the metaverse. However, during 2022 and 2023, there has been an increasing number of treasurers who approached the ACT for practical advice on opening and operating a crypto wallet – and many of these are traditional businesses with very limited activity in the digital economy. The range of use cases has been surprising and reflects the wide (and growing) interest and curiosity in the applications of cryptocurrencies and the digital ecosystem more broadly by different parts of the business and the growing maturity of market participants.

According to a study[1] conducted in July 2022, which sampled 2,000 retailers in the US, 75% said that they would accept a crypto or virtual asset as a means of payment within the next two years. However, with just over 50% of respondents

1. https://www2.deloitte.com/us/en/pages/consulting/articles/digital-currency-payments-merchant-adoption-survey.html

planning to convert digital currency into fiat (legal tender issued by a government, like the US dollar, the British pound and the euro) many of the retailers are not planning to actually own the crypto-asset (CA) that is used for payment. While this may change over time, in the short term, it seems that many businesses are simply looking to increase the range of channels in which they can receive payments.

It appears that CAs are highly correlated with the wider macro risk environment and, in particular, technology markets. This makes them attractive in a low-yield environment that has characterised much of the global macro environment in the 2010s. When macro conditions return to low inflation and interest rates we may see increased institutional interest in diversification into CAs, which may have an outsized positive response to such conditions. Likewise, the newer generation of family offices may also begin to take substantial positions in CAs during the next bull run.

Purpose of this guide

Given how quickly the market continues to evolve, with regulators and governments introducing new rules and guidelines, this guide has been developed to provide treasurers with a series of questions that will help them identify what type of wallet they need and some of the tax, accounting, and operational aspects that will require consideration. There are also links to professional organisations and market participants who will be able to address specific concerns and provide appropriate guidance. The guide includes a glossary of key terms in Appendix 1.

From an infrastructure perspective, there has been growing interest by major traditional finance custodians such as Fidelity and State Street. This makes it much easier for larger institutions to take substantial positions in the underlying assets, without all of the concerns about how to safely store private keys that are used to access non-custodial CA wallets. In addition, there are a wide range of custodians that have developed their services from within the CA sector and that offer CA custody.

Operating in the crypto ecosystem is not without a range of regulatory risks and a high-profile entry into the space may impact relationships with other key business partners (major banks have notably often been unsupportive of activities within this sector, even if the bank is not being asked to support the activity directly).

In addition, some activities (for example, those involving exchanging CAs for fiat, or CAs for other CAs) will require companies to be registered for anti-money laundering (AML) purposes as a Virtual Asset Service Provider in the UK or elsewhere. However, this does not mean they are authorised and supervised more widely to conduct those activities, as currently many of these activities do not

have an authorisation regime in the UK. The UK intends to extend the financial promotions regime to CA as part of the Financial Markets Services Bill. At present, the government has introduced an exemption to the Section 21 authorised persons definition, allowing for firms registered with the FCA under the Money Laundering Regime to be included in this definition.

The ACT would like to thank Circle, KPMG and Ramparts for supporting this important educational resource.

2 Questions for the business

Establishing business requirements

Treasurers are all too frequently aware of how simple questions from the C-suite are actually very complex. This is true of a request to create a crypto wallet (sometimes the request may incorrectly be for a crypto bank account).

As always, it is critical to understand the nature and purpose of the wallet and what management understands the requirements to be. Often, management will only have a vague idea of the purpose of the wallet and in order to deliver the right outcome, treasurers should invest time in understanding how the wallet would be used.

Key areas to understand include:

1. Strategy

Is the business clear about the use of the wallet? Will it be used as an asset on the balance sheet in order to diversify investment risk/generate additional returns? Or will it be used as a trading currency (similar to the familiar process of receiving payment in a foreign currency)?

Does the business see the use of CAs as a contingency feature to provide capability if it is required in the future?

Does the business have a clear strategy of how it sees the wallet being used? If not, it may be better looking for a suitable custodian that has the flexibility and capability of safely operating a wallet and enabling conversion with a wide range of fiat and cryptocurrencies.

Does the business plan to use Bitcoins, stablecoins or other CAs?

2. Types of activity

Will the wallet be used to:

- pay suppliers
- receive cryptocurrency from the sale of goods and services
- or both?

What volumes of inflows and outflows does the business forecast to transact in the short and medium term? Who is producing the forecasts and how reliable are the projected volumes? Does the forecast show the different currencies the business expects to transact in? Do you anticipate that sales will be large-value transactions, small-value transactions or some other variation? Do you anticipate seasonal activity will affect volumes?

3. Currency risk management

Does the business expect to buy and sell the same CA, or will one CA be used predominantly to pay suppliers and a range of other CAs received from customers?

What margins does the business anticipate the sales to generate and what will be the maximum volatility that the business can tolerate? Given this, what period do you anticipate holding any CAs for, or will they be converted to/from a fiat currency? If you plan to use a fiat currency, will this be US dollars or some other currency (such as your local/reporting currency)?

Do you plan to convert receipts to fiat:

- upon each receipt?
- once a certain threshold has been achieved?
- before period end reporting?

Depending on the approach taken to holding CAs, are you aware of the tax and accounting implications (see Sections 6 and 7 for more details)?

4. Pricing

How will the business set sales prices in the different trading CAs? Will it be based on a fiat price converted into a prevailing CA price?

Will prices be set for a period of time (weekly/monthly/quarterly)? If so, how will these prices be established? Will you use prices set by a particular exchange at a particular time?

5. Systems

Are your systems capable of holding prices of the differing CAs? How often can/will you want to update the system prices for the goods being sold? Does your reconciliation process need any adaptation?

3 Selecting an appropriate wallet

There are a number of different ways in which a business can choose to create and operate a wallet. Each comes with its own advantages and disadvantages, risks and opportunities.

Custody of digital assets is one of the foundational aspects of operating within the ecosystem and should be the first consideration for all organisations.

In the context of CAs, we define third-party custody as "the management of crypto-assets on behalf of others". A key decision is control vs beneficial ownership.[2] Control over the CAs will depend on who has access to the private key (see Appendix 1). Typically, one would not share the private key with a custodian but pass control over the CA. (Thus, for example, if one sends a crypto exchange 1 BTC to store, one does not send them the private key to one's wallet. Instead, control of that 1 BTC is transferred to the custodian – which is controlled by their private key – and one can continue to safely use one's wallet and private key for other transactions that the custodian has no control over.)

As ownership of CAs at the blockchain level is determined by who holds the private keys to these assets, they are far more important than a password could ever be. If a private key is lost or stolen the assets cannot be recovered even by their rightful owner (though as the industry matures insurance products will become available).

The generation of the private key, and many other operational factors such as how it is stored, who is authorised to access it, and who is responsible for its safekeeping, are critical decisions that need care.

As of today, we see two distinct types of CA management: custodial and non-custodial. Your adoption strategy as a treasurer should be centred on these two methods of handling digital assets:

- managing the handling of crypto payments yourself, via a self-custody solution, or
- outsourcing some or parts of the process to a third party.

2. https://blogs.orrick.com/blockchain/english-high-court-recognizes-cryptoassets-to-be-a-form-of-property-considerations-following-aa-v-persons-unknown/

Self-custody wallets

Self-custody occurs where there is no third party providing a service to manage a wallet holding CAs. Users access and safeguard their own CAs, giving them full control. The assets can be stored in hardware or software wallets. This option is typically only used by sophisticated users since the range of operational and security requirements to consider are significant (for example, is the source code for the wallet chosen public and publicly verified? Can you understand and manage the risks involved with storing private keys safely?).

Custodial wallets

Custodial wallet services offer varying levels of control. Some wallet providers have partial control over the asset, with the ability to execute, transfer, sign transactions, block or recover assets and private keys on behalf of a client with their instruction. However, they may not have full control to initiate a transaction on behalf of a client if the custodian does not have the client's private key in their possession to settle the transaction. In certain circumstances, the custodian could exercise full control.

The custodian creates redemption conditions around the safekeeping and release of CAs from a custodial account. Beneficial owners (clients) transfer digital assets into custodial accounts and declare which fiduciaries must initiate redemption requests. Fiduciaries approve redemption requests initiated by a beneficial owner. Beneficiaries receive CAs or fiat conversion of CAs from the custodian.

Custodians may provide services in addition to safekeeping or the holding of assets on behalf of others, which include, but are not limited to, reconciliation, settlement, corporate actions, maintaining bank accounts and fund management.

4 Identifying providers

There is a wide range of organisations that can provide the services that a treasurer will require in order to transact in CAs, and applying due diligence to those is key.

It is essential that treasurers consider the wider context, particularly how the normal fiat banking world and the crypto world interact. It is essential that where CAs are being used to buy goods and services they can be converted as needed into fiat currency. This conversion process requires good relationships with payment providers, banks and others that are comfortable with the activity and the compliance processes in place for those crypto transactions.

The regulatory environment continues to evolve with numerous developments that are focused on AML (FATF Guidance for a Risk Based Approach to Virtual Assets) and whether CAs should be treated as a payment tool or a financial instrument (for example, security).

A key area of persistent regulatory tension is the divergence between the self-custodied (decentralised) crypto community and the desire for increased regulatory oversight, and governmental control of CA transactions and participants.

Complex issues of personal autonomy, privacy, counterparty risk, control of the financial systems and taxation interact to make this a battleground between the more libertarian elements and the developers that believe 'code is law', and traditionally centralised governments, regulators and national banks. This divergence could lead to a situation soon whereby CAs that are outside of the normal financial services system (for example, self-custodied CAs) are not able to easily convert to fiat currency using regulated entities and channels.

Self-custody leverages the distributed ledger to reduce counterparty risk and place operational control into the hands of the user, however it comes with increased requirements to manage AML and Counter Terrorism Financing (CTF) risks. Many companies with limited operational know-how may choose to work with a crypto payment service provider so that AML/

CTF checks (as well as chain analysis checks for use of higher risk public crypto addresses) are conducted by that specialist provider, and the specialist provider may also provide a conversion to fiat service through their banking and payment providers. (The table in Appendix 2 highlights the novel risks and considerations that arise.)

Key questions you need to ask include:

- Are you or the chosen provider regulated?
  - If so, by whom and for what activities and in which jurisdictions?
- What type of wallet you want and if they can offer this?
- If they support the currencies you currently and plan to use?
- How do they connect to fiat currencies (both on-ramp and off-ramp)?
- What transparency do they offer over traceable and non-traceable assets (and the mixing of them)?
- If they offer chain analysis?
- If they can ensure clean traceable non-boxed assets?
- To what extent can they be connected to your existing IT infrastructure?
- In which jurisdictions can they operate?
- What level of recourse do they offer?
- What dispute mechanisms do they offer?

5 Internal governance

Treasurers will be familiar with their governance framework and the extent to which they have delegated authority to open bank accounts. They will need to check clearly if this extends to crypto wallets and what, if any, restrictions apply.

If there is no clear mandate, it will be important to consider what approvals would be required. It may be beneficial to seek separate approval of the different types of CAs available, as each will carry its own risks (and therefore require potentially different controls).

Key controls that will require to be documented and implemented are:

- Authority to open and close wallets
- Wallets only opened with specific providers regulated for AML (as a minimum) and, if possible, also authorised to do the proposed activities
- Only a certain type of wallet can be opened
- Authority and thresholds for transferring CAs to another wallet (including dual key access/multi-factor authentication (MFA))
- Access rights to wallet (read access, payment access, admin access, and so on)
- Regular reconciliations of the wallet and by whom
- Controls over mixing of traceable and non-traceable CAs
- AML on beneficiaries being paid and customers paying
- Cryptographic key management
- User access management
- Change management
- Privacy and compliance
- Insurance in the event of loss
- Periodic reporting
- Segregated accounts
- Third-party asset audits.

6 Accounting

As of January 2023, there is limited accounting and reporting guidance for digital assets. Existing guidance is principally from The IFRS Interpretations Committee (IFRIC), which had issued an agenda decision in June 2019, entitled Holdings of Cryptocurrencies. As the title suggests, the scope was limited to cryptocurrencies, which is a specific type of digital asset issued as a medium of exchange that does not entitle the holder to any real-world asset.

The June 2019 IFRIC guidance requires preparers to assess their business model or purpose for holding the cryptocurrency. The committee concluded that IAS 2 Inventories should be applied when cryptocurrencies are held for sale in the ordinary course of business. If that guidance is not applicable, then IAS 38 Intangible Assets would be applied.

Under IAS 2 Inventories, the preparer will present their digital assets as inventories measured at the lower of cost or net realisable value (NRV), unless the broker-trader measurement exemption applies. If the broker-trader exemption applies, then the inventories are measured at fair value, less cost, to sell with changes in fair value going through profit or loss. If the exemption does not apply, any write-downs of inventories measured at cost or NRV are recognised as an expense in the Statement of Profit or Loss. In order to qualify to take the accounting policy decision to apply the exemption, the entity will need to exercise judgement as to whether the inventories were principally acquired for the purpose of selling in the near future and generating a profit from fluctuations in price.

Under IAS 38 Intangible Assets, the cryptocurrencies being presented as intangible assets are measured at cost, less accumulated amortisation and impairment. If an 'active' market exists for the cryptocurrency, the preparer may select an accounting policy to measure the intangible asset at fair value, with changes in value generally going through other comprehensive income when in a revaluation surplus, or in profit or loss in the event of a reduction of value more than the previously recognised valuation surplus, or an increase in value that reverses previous amounts recognised through profit or loss. The entity may need to exercise significant judgement as to whether a market is 'active'. IFRS 13 fair value measurement only provides a definition of an active market as a "market in which transactions for the asset... take place with sufficient frequency and volume to provide pricing information on an ongoing basis", however, it does

not provide guidance on thresholds to determine sufficiency of frequency or volume.

There are different methods for identification of cost under both IAS 2 and IAS 38. Under IAS 2, when the inventories are measured at lower of cost or net realisable value, the cost of inventories must be assigned using either the first-in, first-out or weighted average cost formulas. Under IAS 38, the cost of the intangible asset is the cash paid or the fair value of any other consideration given; there is no accounting policy choice as to cost identification methodology.

Preparers must ensure their finance systems can enable the appropriate cost identification methodology as, depending on the standard applied, the Statement of Profit or Loss presentation of any changes in value will depend on accurate identification and assignment of cost.

For digital assets other than cryptocurrencies, preparers need to thoroughly understand the terms and conditions specific to each digital asset to identify the applicable accounting standard. For example, some stablecoins (a type of digital asset purportedly pegged to a fiat currency through reserving strategies) provide the holder with the right to redeem their token for a fixed amount of the underlying fiat currency. This entitlement may result in the token being in scope for IFRS 9 as a financial instrument. In other instances, preparers may need to develop accounting policies by using the hierarchy of accounting policy sources guidance in IAS 8.

In addition to understanding the terms and conditions of the specific digital asset, preparers should also understand the terms and conditions of their custody solution. If the entity is using a solution other than self-custody, they may be exposed to a securities lending like arrangement. If so, an analysis of control is required to determine the appropriate presentation of their asset. Similarly, if the preparer intends to use an intermediary payment service to allow customers to pay in digital assets, they should consider whether they will be entitled to receive a financial instrument or a digital asset.

Finally, when a customer promises consideration for goods or services in the form of digital assets, it is non-cash consideration and must be measured at fair value as per IFRS 15 revenue from contracts with customers. IFRS 15 does not provide specific guidance on the measurement date for non-cash consideration, therefore, an entity must exercise judgement in selecting the reference measurement date.

7 Taxation

Similar to the position in respect of accounting guidance, there is limited tax guidance for digital assets. There is no specific CA legislation, and the HMRC *Cryptoassets Manual* (which essentially applies existing legislation to these new asset types) itself starts by highlighting that HMRC's views may evolve further as the sector develops and that it may publish amended or supplementary guidance accordingly. Further, although titled the *Cryptoassets Manual*, as of January 2023, its scope only specifically covers exchange tokens intended to be used as a means of payment that do not entitle the holder to any real-world asset.

Although intended to be used as a means of payment, HMRC makes clear that it does not consider any of the current types of CAs to be money or currency. Entities should instead take into account all of their CA transactions as they would any other type of asset, and tax it accordingly. In general, the tax classification is largely expected to follow the accounting treatment. In practice, this means that entities are required to assess their purpose for holding the CA and then either:

- apply the normal rules for computing trading profits where the CA is being traded
- tax any CA under a specific regime such as the intangible fixed assets rules, or
- treat all (other) transactions involving CAs as disposals of capital assets subject to tax on the capital gain.

Where the CA was principally acquired for the purpose of selling in the near future, and generating a profit from fluctuations in price, then broker-traders holding CAs with changes in fair value going through profit or loss are likely to also be subject to tax volatility in their income statement, with tax gains and losses occurring in line with accounting gains and losses.

Where the CA is taxed under the intangible fixed assets regime, then profits and losses should generally be taxed or relieved in accordance with accounting principles. However, it is important to note that simply because the CA falls under IAS 38 Intangible Assets does not necessarily mean that it will be taxed as an intangible fixed asset for tax purposes. In order to be an intangible fixed asset, it must be held by the entity for use on a continuing basis.

Where the CA is taxed as a capital asset, then a taxable event arises only on disposal of the investment. Where the CA is being used as a means of payment,

this means that using the CA to pay for goods or services is a disposal. The usual tax rules on how to compute capital gains will apply, including the rules on pooling that average the cost basis of assets in different pools, and the rules that set out the expenses that are deductible in calculating the gains. As is the case for accounting considerations, it will be important for companies to have sound financial systems that can retain records of transactions throughout the year.

Furthermore, where the CA is custodied using a solution other than self-custody, it will be important to understand the terms and conditions of the custody solution and, in particular, whether the beneficial interest in the CA transfers with the legal interest. Where the entity retains beneficial ownership of the CA throughout, then no disposal has occurred and there is no taxable event for capital gains tax purposes. Where, however, as suggested above, an entity is potentially exposed to a securities lending like arrangement, this may be a disposal event subject to tax. This is a developing area, however, and in April 2022, HMRC launched a consultation to ascertain whether administrative burdens and costs could be reduced for taxpayers engaging in securities lending like arrangements involving CAs, and whether the tax treatment could be better aligned with the underlying economics of the transactions involved. This is pending a consultation response.

8 Opening a wallet

Generally providers will have a clear set of due diligence requirements that the treasurer will need to provide. Having these ready in advance will expediate the opening of a wallet. For many providers, the Know-Your-Customer (KYC)/ AML processes will essentially be the same as those followed by traditional banks. They will conduct extensive sanctions screening, evaluate risk scores and carry out ongoing monitoring for risky activities. Some providers may be Payment Card Industry (PCI) compliant and offer Systems and Organisation Controls (SOC) reports to back up their information security standards. It is important to choose a wallet provider that follows strict operating guidelines in order to comply with relevant laws, banking requirements, and card or payment associations' rules and policies.

At a minimum, one can expect the following:

- Government ID
- Tax ID/registration number
- An organisational chart or capitalisation table that shows shareholders
- Proof of physical address
- Incorporation or formation documents.

There is a wide range of wallet-like services available to corporate treasurers who want to begin transacting in CAs. Many wallets are standalone apps or basic browser extensions that can be set up in just a few minutes. But these require the safe storage of a confidential 'seed phrase' that serves as the wallet access key. Losing this seed phrase can mean permanent loss of CA stored in the wallet, making them less than ideal for custody of corporate funds. In addition, funding this type of wallet requires the setup of a separate account at a CA exchange where treasurers can exchange fiat currency for CAs to then send to the wallet.

As a more robust alternative, a number of providers are developing enterprise-grade account infrastructure with wide-ranging functionality and a user experience more like those found in traditional treasury portals. These enable treasurers to switch easily between fiat currencies and CAs. Providers may also be able to facilitate the minting of stablecoins like USDC and Euro Coin, plus payments and storage of these digital versions of US dollars and euros, along with Bitcoin, Ether and other major CAs. The key is determining your specific needs and then identifying an appropriate provider.

9 Operational considerations

Costs and maintenance

Given the wide range of digital currency wallets and accounts, accordingly, there is a wide range of cost and maintenance requirements. Many of the standalone wallet apps and browser extensions are free, but they lack access to critical corporate treasury functionality and 24/7 account management support. This choice can lead to a proliferation of providers to meet all treasury needs, resulting in slower operations and additive service fees.

Some providers offer a free account, while offering robust reporting, multi-user support and a merchant dashboard, alongside strong security protections. Extra valuable services that give the business an integrated treasury platform across both traditional and digital currency may be available for a fee.

If using third-party custodians, it is essential to check how they manage the risk of loss or theft of CAs (for example, insurance, transparent audits, segregation of client assets, and so on).

Timings

In addition to the significant investment in time in determining your requirements and undertaking the necessary due diligence, it will also be important to consider how long it will take to open a wallet, once you have identified suitable partner(s).

This may be further delayed by any discussions with professional advisers (such as auditors) and commercial banks who may wish to review your choices and readiness assessment. Given the sectoral reputation it would be prudent to build in significant contingency to any plans to open a wallet.

Appendix 1: Glossary of key terms

Term	Definition
Altcoin	A crypto-asset that is not Bitcoin.
BTC	Bitcoin
Crypto-asset (CA)	Cryptographically secured digital representations of value or contractual rights that use some type of distributed ledger technology (DLT) and can be transferred, stored or traded electronically.
Decentralised finance/DeFi	An umbrella term for the part of the crypto universe that is geared towards building a new, internet-native financial system, using blockchains to replace traditional intermediaries and trust mechanisms.
Private key	A sophisticated form of cryptography that represents ownership of a user's CAs and facilitates the use of CAs to transact. A private key is an integral aspect of CAs, including Bitcoin and altcoins, and helps to protect a user from theft and unauthorised access to their assets. (It is not an issue with traditional banking as one of the key roles of regulators is to ensure that monies held with authorised financial institutions are kept secure.) It is the key that is used to sign (authenticate) a transaction. Because of cryptographic technology, private keys cannot easily be derived from public keys and this enables the safe sharing of public CA addresses by participants and verification of transactions involving the public-private key pair.

Term	Definition
Public key	Public keys are derived from private keys and this enables verification of transactions because of this public-private key pairing. The blockchain validators (nodes) can check that the signer is the controller of those CAs on the blockchain.
Stablecoin	CAs whose value is pegged, or tied, to that of a real-world currency, commodity, or financial instrument.
Staking	The process of locking up cryptocurrencies to receive rewards/returns.
Wallet	A wallet is a tool used to store the private password (key) for accessing CAs on the blockchain and to share the public address for receiving CAs. Wallets do not actually hold CAs since CAs are on the blockchain network. The system of transfer and ownership relates entirely into having the private key to prove ownership of specified units on the blockchain. CAs are not therefore electronically sent between participants, instead proof of ownership is transferred electronically.

Appendix 2: Self custody vs third-party custody

The table below provides more detail when choosing between the two different custody models

Attribute	Self custody	Third-party custody
Control of your assets	**Yes:** Risk of loss/theft internalised (lack of in-house expertise).	**No:** Risk of loss/ theft externalised to an expert.
Counterparty risk (bankruptcy and cybersecurity)	**No:** Time to implement – acquire expertise either through external hire or in-house training.	**Yes:** Exposed to counterparty risk, however, can go to market immediately. Essential to check how the third party manages the risk of loss or theft of CAs (for example, insurance, transparent audits, segregation).
Cost	Capital expense	Operational expense
Leverage your own balance sheet	Yes	No
Access to liquidity	**Instant:** Operational flexibility – move funds 24/7 365 days a year from anywhere in the world.	**Can be slow:** Reliant on third-party systems, processes and downtime.

Attribute	Self custody	Third-party custody
Risk and compliance operations	Self-directed program (compliance/operations/ internal resources) gives flexibility, for example, choosing which customers you want on board based on the risk profile. However, requires better knowledge and tools for managing AML/CTF risks.	Outsourcing risk and compliance process can introduce new variables, such as standards around counterparties, approaches to regions and immature and dynamic regulated environment. However, third parties may be more experienced in managing AML/CTF risk.
Power to benefit from new models as they emerge (for example, DeFi and staking)	Yes	No
Payments and banking	Requires you to have a greater understanding of the banking and payment system interaction with CAs and more careful management of relationships with CA exchanges or over the counter (OTC) providers, payment companies or banks.	Often leverage the third party's relationships.
Integration with KYC/AML providers	Highly automatable and controllable.	Depends on third-party infrastructure.
Closed loop	**Flexible:** choose your own set up.	Depends on which third parties are used for which purposes (for example, storage vs conversion of CAs).

TREASURY EXCELLENCE AS STANDARD

The Association of Corporate Treasurers
150 Minories
London EC3N 1LS
+44 (0)20 7847 2540
treasurers.org
technical@treasurers.org

@actupdate
actupdate
treasurers.org
treasurersorg

CIRCLE

Lauren Granchelli
lauren.granchelli@circle.com
https://www.circle.com/en/solutions-for-exchanges-and-wallets

KPMG

Ian Taylor
Ian.Taylor@KPMG.co.uk
Phone: +44 (0)7713 751277
https://kpmg.com/uk/en/home.html

RAMPARTS

Peter Howitt
peterhowitt@ramparts.gi
Phone: +447899623127
www.ramparts.gi