Crypto assets – what trustees and family offices need to know

Niklas JRM Schmidt

Introduction

In my practice of advising trustees and family offices on crypto assets I often encounter the following situation:

- There are younger beneficiaries who want investments to be made into crypto assets, an asset class which did not exist a decade ago, which has a low correlation with traditional assets, which is highly volatile and about which the beneficiaries are very enthusiastic.
- There are older trustees and board members who are administering a decades old structure, who have no idea what crypto is all about and who are therefore quite fearful of entering this brave new world.

In order to bridge this divide, education is paramount. The purpose of this article is to give a very high-level introduction to crypto assets and how to hold them. Readers are encouraged to attend one of the many courses offered on the internet in order to gain a deeper understanding.[1]

In the following, I will not be dealing with indirect investments into crypto, eg, by acquiring traditional securities which act as investment wrappers and for which custody works in the same manner as for stocks and bonds. More and more products of this type are becoming available. As one of many examples, the Open End Tracker Certificate IV on Bitcoin issued by Bank Vontobel AG in Zurich could be mentioned.[2]

Typology of crypto assets

General

A popular website lists nearly 13,000 crypto assets,[3] a bewildering menu which causes some initial consternation for the beginner. In this article, I will limit myself to the top two crypto assets, namely Bitcoin (the king of crypto) and Ether (the queen of crypto). When speaking of the top two crypto assets, I am referring to the market capitalisation. The market capitalisation of a crypto asset – similar to stocks – results from multiplying the circulating supply by its respective price. For example:[4]

- If around 18.9 million Bitcoins are in circulation and Bitcoin has a price of around US$38,700, then the market capitalisation of Bitcoin at that time is around US$731.4 billion.
- If around 119.8 million Ether are in circulation and Ether has a price of around US$2,600, then the market capitalisation of Ether at that time is around US$311.5 billion.

Of all crypto assets, Bitcoin (the king of crypto) has the largest and Ether (the queen of crypto) the second-largest market capitalisation.

Another interesting metric is market share – the market share of a crypto asset results from the ratio of its market capitalisation to the market capitalisation of all crypto assets. For example:

- If, as mentioned above, Bitcoin has a market capitalisation of around US$731.4 billion and all crypto assets together have a market capitalisation of around US$1,800 billion, then Bitcoin' s market share at the time is around 40.6%.
- If, as mentioned above, Ether has a market capitalisation of around US$311.5 billion and all crypto assets together have a market capitalisation of around US$1,800 billion, then Ether' s market share at the time is around 17.3%.

Thus, Bitcoin and Ether together have approximately 57.9% market share. By way of comparison, the next three crypto assets have market shares of 4.5%, 3.6% and 2.9%. Thus, for many investors new to the crypto space it could make sense to limit oneself initially to investments into Bitcoin and Ether, since these are by far the largest players. In the following I will attempt to briefly introduce these two.

Bitcoin

Bitcoin[5] is the original crypto asset and the most well-known. Bitcoin was originally conceived as electronic cash that can be sent directly from user to user without the need for intermediaries, with transactions being recorded in a decentralised database (ie, the blockchain). It is not yet considered as money, since its functionality as (i) a store of value; (ii) a medium of exchange; and (iii) a unit of account is still weak. Bitcoin has peculiar properties distinguishing it from traditional (ie, fiat) money:

- Fiat money is issued by a central bank. Bitcoins, on the other hand, are created by a decentralised network.
- Fiat money has a money supply based on a

Over time, Bitcoin' s purpose has somewhat morphed from digital cash to digital gold. As such, it does not have any real competitors in terms of brand and market share.

discretionary (political) decision. Bitcoin, on the other hand, has a money supply determined by an algorithm; it is therefore fairly easy to predict how many Bitcoins will be in circulation in a month, in a year or in a decade.

- Fiat money can be multiplied at will and (if things continue this way) may one day be worthless. Bitcoin, on the other hand, has an upper limit of 21 million, which acts as a protection against debasing.
- Fiat money cannot be transferred electronically without intermediaries (eg, banks, credit card companies, PayPal, Stripe, Apple Pay etc). Bitcoin, on the other hand, does not need intermediaries; everyone is their own bank and payments are made directly from one user's address to another user's address.
- Fiat money transactions intended by the transferor may ultimately not be carried out by the interposed intermediary, either for arbitrary or for legal reasons (eg, the application of money laundering regulations, sanctions or restrictions on the movement of capital). Bitcoins, on the other hand, are transmitted without intermediaries; nobody, therefore, can censor (ie, suppress) a planned transaction.
- Fiat money is normally held with banks, but opening a bank account can take a long time, among other things, due to the need to comply with legal provisions relating to money laundering and the financing of terrorism as well as the automatic exchange of information on financial accounts. Typically, many pages of forms need to be filled out. Finally, a bank can sometimes simply refuse to open a bank account. Bitcoins, on the other hand, are held directly by a user on an address;[6] the generation of a Bitcoin address (and the associated private key) is extremely simple and does not require the consent of third parties.
- Fiat money held with a bank can be lost due to attachment, expropriation or bankruptcy of the bank; in the latter case, sometimes a state deposit guarantee scheme gives some protection. Bitcoins, on the other hand, do not constitute claims against an intermediary; as long as the private key for a specific address is not disclosed, nobody can access the Bitcoins stored at this address. If you lose the private key, there is no deposit protection and that is the end of the story.
- Fiat money transfers recognise national borders – international transfers are slower and more expensive than domestic transfers. Bitcoin, on the other hand, is an electronic money system that makes no distinction between domestic and foreign recipients.
- Fiat money transfers are usually reversible – credit card payments can for example be reversed weeks later. Bitcoin, on the other hand, has – in principle – irreversible transactions. As soon as a transaction has been included in a block of the blockchain (ie, the decentralised transactional database), the process cannot normally be reversed.
- Fiat money is divisible to two decimal places (a hundredth). Bitcoins, on the other hand, are divisible to eight decimal places (a hundred millionth).

Over time, Bitcoin' s purpose has somewhat morphed from digital cash to digital gold. As such, it does not have any real competitors in terms of brand and market share. It is interesting to note that not only have well-known billionaires and hedge funds started dipping their toes into Bitcoin as an inflation hedge in turbulent times, but the number of public companies holding Bitcoins in their treasuries is steadily growing (eg, MicroStrategy Inc holds US$4.7 billion in Bitcoin and Tesla Inc holds US$1.9 billion in Bitcoin). Recently, even an accounting firm (KPMG Canada) disclosed purchasing Bitcoins.

Ether

Bitcoin, which I just described above, is a safe, efficient, resilient and decentralised system, which has been working for more than a decade without any downtime. It is, however, also simple, meaning that Bitcoins cannot be sent subject to a predefined condition being met – they can only be sent or not sent. This limitation led to the development of Ethereum, a blockchain-based computing platform, on which programs of arbitrary complexity can run in a decentralised manner. The advantages of such programs (so-called smart contracts) are:

- they do not run, and do not store their data, on a central server;

- they cannot be subsequently modified or interfered with;
- they can dispose over assets stored on the blockchain; and
- they can be reviewed by the public at large.

Smart contracts thus open up the possibility of making payment instructions conditional upon an external event occurring. While Bitcoin (ie, the platform) allows the unconditional transfer of Bitcoins (ie, the crypto asset), Ethereum (ie, the platform) allows the programmable transfer of Ether[7] (ie, the crypto asset).

Ether are a digital asset similar to Bitcoin, but they are also used to pay for the carrying out of transactions on the Ethereum blockchain. Similar to Bitcoins, Ether are transferred peer-to-peer without any intermediaries and are created by a decentralised network, with the money supply being based on an algorithm. In contrast to Bitcoins, there is no upper limit. Recent changes to the system have led to the regular 'burning' of Ether, which could offset the inherent inflationary tendency. Interestingly, Ethereum makes it possible to create other assets, so-called tokens. Such tokens basically work in the same manner as Ether.

Three of the most exciting developments on the Ethereum platform (which will drive demand for Ether) are currently:

- decentralised finance (DeFi) – the provision of lending, borrowing, derivatives trading and other financial services not by central intermediaries but through smart contracts;
- non-fungible tokens (NFTs) – tokens, which cannot be arbitrarily exchanged for other pieces of the same type, quantity and quality, but rather are unique and not divisible, with many use cases including in the world of art; and
- decentralised autonomous organisations (DAOs) – blockchain-based organisations for pursuing (commercial and non-commercial) projects.

Ethereum has many competitors offering smart contract infrastructures. As of now these, however, have quite low market caps. Whether they will make significant inroads or whether they will remain niche players remains to be seen.

Other crypto assets

A comparison of Bitcoin and Ether already shows that these are two completely different beasts (digital gold versus computing platform). In the following, I would like to introduce a few other crypto assets, with the goal of showing the immense breadth of this universe (the ticker symbols are mentioned in brackets):

- crypto currencies which serve as a means of payment, eg, Litecoin (LTC), Bitcoin Cash (BCH) or Dash (DASH);
- privacy coins, which are untraceable means of payment due to having no public ledger, eg, Monero (XMR), Zcash (ZEC) or Secret (SCRT);
- stablecoins, which are crypto assets pegged to the US dollar, eg, Tether (USDT), TrueUSD (TUSD), USD Coin (USDC), Pax Dollar (USDP), Gemini Dollar (GUSD), Dai (DAI) or Magic Internet Money (MIM);
- smart contract platforms which are competitors to Ethereum, eg, Avalanche (AVAX), Solana (SOL), Fantom (FTM) or Harmony (ONE);
- governance tokens of DeFi protocols, which promise dividends similar to shares, eg, Aave (AAVE), Curve DAO Token (CRV) or Sushi (SUSHI);
- tokens representing stocks, bonds or other financial instruments, eg, Mirrored Apple (mAAPL), Mirrored Goldman Sachs (mGS), Mirrored Starbucks (mSBUX) or Mirrored Tesla (mTSLA);
- tokens representing venture capital investments into start-ups, eg, Arweave (AR), Helium (HNT) or Livepeer (LPT);
- collectibles in the form of non-fungible tokens (NFTs), eg, Cryptopunks, Bored Ape Yacht Club or Art Blocks;
- works of art in the form of NFTs, which are mostly sold on decentralised marketplaces, eg, Mike Winkelmann's digital work of art "Everydays – The First 5000 Days", which was auctioned at Christie's for US$69 million;
- real estate in the metaverse, an immersive virtual world where people gather to socialise, play and work and which was familiarised through Mark Zuckerberg's announcement, eg, The Sandbox (SAND) or Decentraland (MANA);
- fan tokens issued by soccer clubs, which grant certain benefits to token holders, eg, Paris Saint-

Similar to Bitcoins, Ether are transferred peer-to-peer without any intermediaries and are created by a decentralised network, with the money supply being based on an algorithm.

Germain Fan Token (PSG), Manchester City Fan Token (CITY) or FC Barcelona Fan Token (BAR);
- meme coins, which are very speculative crypto assets, that have no commercial purpose, that often make fun of themselves, that typically cost a fraction of a dollar and whose price is driven through social media by meme lords such as Elon Musk, eg, Dogecoin (DOGE) or Shiba Inu (SHIB); and
- assets in 'play to earn' games which kept many families afloat during the pandemic in third-world countries, eg, Axie Infinity (AXS) or DeFi Kingdoms (JEWEL).

This is perhaps a good time to explain the distinction between coins and tokens:
- Coins are all crypto assets that have their own blockchain – eg, Bitcoin runs on the Bitcoin blockchain, Litecoin on the Litecoin blockchain and Monero on the Monero blockchain. Coins are immanent to a blockchain, ie, provided for from the beginning.
- Tokens are all crypto assets that do not run on their own blockchain – eg, Tether (USDT), Dai (DAI) and Aave (AAVE) all use the infrastructure of the Ethereum blockchain (which – as mentioned above – allows tokens to be issued). Tokens are not intrinsic to a blockchain, ie, they are not intended from the start and are only created later.

Regulatory concerns regarding crypto assets

A question mark for crypto assets is certainly regulation. Some (especially underdeveloped, Islamic and/or totalitarian) countries have declared crypto assets illegal and have banned them entirely. These are fairly extreme examples that would not work in more developed jurisdictions. Crypto assets are private property, which in most jurisdictions means that they fall within the scope of protection of the fundamental right to the inviolability of property. Bans on production, possession or transmission would constitute an interference with this fundamental right. In most countries, the existence of a public interest alone (eg, combating money laundering, terrorist financing or climate change) does not make the intervention constitutional; rather, a proportionality test is normally required. Similarly, a legislature cannot just ban the use of roads, airports, banks, the internet, the postal system, etc because these systems are also used by criminals.

Regarding the two major crypto assets described above, the following may be said:
- In the unlikely case that Bitcoin were banned in sophisticated jurisdictions (possibly because of its feature as an autonomous competitor to state-issued money or because of – vastly overblown – environmental concerns due to 'proof of work' mining), its price would probably fall in the short term. In the long term, however, one country's ban would make no difference at all. Rather, Bitcoin could conceivably become even more popular because more people would understand that this represents a monetary system completely autonomous from the state and unfazed by arbitrary government measures. In other words, only a worldwide ban of Bitcoin could make a dent in its price.
- I also do not see any grounds for a ban of Ethereum, this being a decentralised computing platform to run applications. No country would like to be seen as losing out on innovation. Environmental, social and governance (ESG) concerns also do not play out here, since Ethereum will be switching to environmentally benign 'proof of stake' in the very near future.

Apart from outright bans, other regulatory action regarding crypto assets seems possible:
- First, it is very likely that money laundering regulations proposed by the Financial Action Task Force (FATF) will be expanded worldwide. In the so-called 5th Anti-Money Laundering Directive, the EU has made the AML rules, which previously applied only to banks and other financial industry players, obligatory also for virtual asset service providers. The EU will soon be toughening up the applicable rules yet again.
- Second, it can be expected that regulators will be going after crypto assets which mimic

A question mark for crypto assets is certainly regulation. Some (especially underdeveloped, Islamic and/or totalitarian) countries have declared crypto assets illegal and have banned them entirely.

Addresses and the associated private keys are stored in a wallet, normally a computer program. This allows Bitcoins to be easily received and sent without having to enter lengthy letter/digit combinations.

traditional securities (so-called security tokens). It is clear that regulators want to see a level playing field between issuers of traditional securities (subject to the requirements of publishing prospectuses and of adhering to all sorts of conduct rules), on the one hand, and issuers of security tokens, on the other hand.
- Third, stablecoins will be regulated by legislators due to perceived (and in my view actually existing) risks in the areas of consumer protection, operational resilience of issuers and market stability. The EU has issued a draft proposal for a Markets in Crypto Assets Regulation (MiCAR), which aims to make the EU a regulatory first-mover in this field.
- Fourth, providers of certain crypto services such as brokers, exchanges, investment advisers etc will all become regulated in the near future. Currently, most of these operators are not subject to any regulatory regime at all. In the EU, MiCAR will add a raft of compliance requirements for such companies. A recently shelved amendment proposal would have banned services relating to 'proof of work' crypto assets.
- Fifth, DeFi will certainly attract more and more regulatory scrutiny. Projects that are not decentralised and/or pseudonymous enough can expect to be targeted by regulatory bodies.

None of this should in my view have an impact on an investor merely buying and holding Bitcoin and Ether for the long term.

Holding of crypto assets

Self-custody

Bitcoins (and this equally applies to other crypto assets such as Ether) are held in addresses, over which one disposes using the associated private key:
- An address is a combination of letters and digits, such as 1F9cZYh3ZB6gdF9mnzLgFn6yqnFvpP9iHn. Bitcoins are stored at an address. The address is thus comparable to the IBAN of a bank account (eg, AT843400000000062679) on which the euro are stored. An address can theoretically be disclosed to third parties (and must be disclosed if one wants to receive funds).
- A private key is a similarly long string, such as 5Kb8kLf9zgWQnogidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF. There is normally exactly one matching private key for each address. With the private key, one can dispose over the Bitcoins stored on the address. The private key is thus comparable to a PIN code (eg, 83puWz), with which one can dispose over the euro balance in a bank account. A private key must not be disclosed to anyone else; whoever knows the private key can make a Bitcoin payment from the address to which the private key belongs.

Addresses and the associated private keys are stored in a wallet, normally a computer program. This allows Bitcoins to be easily received and sent without having to enter lengthy letter/digit combinations. There are many different types of wallets: mobile wallets on a smartphone are most convenient (ie, one can at any time dispose over the Bitcoins on the smartphone), but not secure (ie, malware on the smartphone may steal the Bitcoins). Hardware wallets (USB drive-like devices) are very secure, but less convenient.

In essence, holding crypto assets (ie, basically bearer instruments) boils down to safely holding the private keys:
- If the private keys are lost (eg, hardware failure), then the crypto assets become irretrievable.
- If the private keys are obtained by an unauthorised internal (eg, employee) or external (eg, hacker) party, then that person has full access over the crypto assets.

External custodian

Self-custody of crypto assets most closely aligns with the mantra of getting rid of intermediaries. In the world of crypto, self-custody is generally seen as the safest way of owning crypto assets. Holding crypto assets via an external custodian is seen as inherently unsafe. After all, custodied crypto assets are held on addresses to which the custodian (and more importantly its officers and employees) has the

If a decision is taken not to self-custody crypto assets, but rather to use the services of an external custodian, it is of paramount importance to invest some effort into the selection of the right service provider.

private keys, opening up the above-mentioned possibilities of loss and theft. The typical slogan here is: "Not your keys, not your crypto".

However, self-custody – while being an ideal – is not for everybody. For example, for family offices or hedge funds holding larger positions in crypto assets, it is normally too dangerous to self-custody from an organisational and technical perspective.

Also, there has emerged a class of professional custodians using sophisticated internal control systems and technology in order to safeguard their clients' crypto assets. Typically, such custodians use so-called cold storage where private keys are not stored on computing equipment connected to the internet but on air-gapped devices. In addition, multi-signature wallets are utilised where several private keys are needed for signing-off a transaction.

These custodians often, but not always, also offer brokerage services, so that it is not necessary to involve an additional party for acquiring the crypto assets in the first place.

Selection of external custodian

If a decision is taken not to self-custody crypto assets, but rather to use the services of an external custodian, it is of paramount importance to invest some effort into the selection of the right service provider. There exists an ever-increasing number of firms offering the custody of crypto assets (sometimes including brokerage/exchange services). The following is a list of notable custodians, with whom I have been in touch in the past:

- Bank Frick & Co AG[8] in Liechtenstein;
- BitGo, Inc[9] in the United States;
- Coinbase Europe Limited[10] in Ireland;
- Fidelity Digital Asset Services, LLC[11] in the United States;
- Gemini Trust Company, LLC[12] in the United States;
- Maerki Baumann & Co AG[13] in Switzerland;
- SEBA Bank AG[14] in Switzerland; and
- Sygnum Bank AG[15] in Switzerland and Singapore.

Questions that I typically ask in the context of a due diligence when helping clients choose a custodian include the following:

- How long has this service provider been operating?
- Have there been any incidents with this service provider in the past?
- In which jurisdiction is this service provider based?
- Is this service provider subject to regulation and if yes to which?
- What amount of value is this service provider currently holding in custody?
- What type of insurance coverage exists for this service provider?
- What technical and organisational security measures does this service provider use?
- What kind of regular reporting on holdings is provided by this service provider?
- Are the crypto asset holdings, which are custodied by this service provider, regularly audited?
- Does this service provider also offer brokerage/exchange services?
- How does pricing work with this service provider?
- Does the service provider use general terms and conditions or bespoke agreements?
- What anti-money laundering documentation does this service provider require?

Typically, all custodians on a shortlist are contacted and asked to answer the questions above. The answers are then summarised in an easily readable table format, and a ranking is created based on a client's preferences. As a next step, a beauty contest is organised for the top three ranked service providers to present themselves. Finally, the contractual agreements provided by the winner of the beauty contest are reviewed and negotiated.

Summary

Crypto assets are an exciting new asset class that trustees and family offices need to know about. This article has attempted to give an overview of the two most important crypto assets, of how these should be custodied and what has to be taken into consideration when choosing a custodian.

Dr Niklas JRM Schmidt, TEP CBP is a partner at the Austrian law firm Wolf Theiss and can be reached at niklas.schmidt@wolftheiss.com. He has been involved in the crypto space since 2013 – as a researcher, as an investor and as a lawyer. In the latter capacity he has been advising family offices, foundations, trustees, wealthy individuals and banks on various topics related to crypto assets. In addition, Dr Schmidt is the author of the German language introductory book Kryptowährungen und Blockchains *(2019) and a co-editor of* Taxation of Crypto Assets *(2020), which covers the taxation of crypto assets in about 40 countries over nearly 800 pages. He is also one of the editors of an upcoming book summarising a conference he organised on legal aspects of crypto assets together with an Austrian university.*

1 The author is the founder of the WT Crypto Academy, an educational initiative for non-crypto natives over 16 hours (from zero to hero), where he has trained more than a thousand lawyers in the last few years. The details of the next event can be found at https://bit.ly/3sGtUwu. Many similar webinars are being offered by other institutions.
2 Product details may be found at https://derinet.vontobel.com/CH/EN/Product/CH0553378750. The International Securities Identification Number (ISIN) of this product is CH0553378750. Many other similar certificates are being offered on the market.
3 www.coingecko.com.
4 All numbers used in the following were current around the beginning of March 2022.
5 Bitcoin's ticker symbol is BTC.
6 See below on addresses and private keys.
7 Ether's ticker symbol is ETH.
8 www.bankfrick.li/en/services/blockchain-banking.
9 www.bitgo.com/services/custody/qualified-custody.
10 www.coinbase.com/custody.
11 www.fidelitydigitalassets.com/overview.
12 www.gemini.com/custody.
13 www.maerki-baumann.ch/de/blockchain-und-krypto-unternehmen.
14 www.seba.swiss/digital-custody-services.
15 www.sygnum.com/solutions/custody.