Are crypto currencies relevant for Corporate Treasury?

Corporate Treasury

Large companies such as Volkswagen, Bosch, BMW and Santander are jumping on the "crypto bandwagon" with cooperations and their own range of services. However, the current discussion about crypto currencies could not be more controversial – the medley of opinions ranges from bubble ready to burst to pyramid scheme to the revolution of the monetary system and the abolition of centralist structures. But how important are crypto currencies to corporate treasuries?

The "new digital currencies" have become known to the broad public at the latest since the enormous price jumps in 2017 and the introduction of exchange-traded derivatives (bitcoin futures). But let's start at the beginning. First of all, companies will not have to exchange their cash for Bitcoins and convert their entire payment operations to accommodate crypto currencies starting tomorrow. Nevertheless, in view of the constantly and rapidly changing expanding crypto universe, the present article aims to shed some light on the unknown. For all we know, some of the statements made here may already be obsolete in a few months. It is therefore crucial to take a differentiated and critical look at the developments to realize that the focus is not only on visionary projects such as the replacement of the prevailing monetary system. There are currently more than 1,500 different crypto currencies, with Bitcoin, Ripple, Ethereum and IOTA being four of the most important. Some of the goals of crypto currency supporters could not be further apart: from ideology-driven do-gooders to conmen who are riding the current hype wave and sensing fast wealth, to profit-oriented FinTechs who want to establish their services within the framework of the current financial system. This in turn means that not all crypto currencies are created equal. But first things first:

What is a "crypto currency"?

According to the European Banking Supervision (EBA), crypto or virtual currencies (VC) are defined as "...digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency. VCs are accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically". Therefore, the central differences between most crypto currencies and traditional paper money (fiat money) are by definition:

- that crypto currencies are created decentrally by the user community and that the total volume of the digital money supply is limited right from the start,
- and that by dispensing with central institutions and clearing houses, (global) payments via the Internet in real time and with virtually no transaction fees, are enabled in a simple and secure way across currency zones.

Trust is everything – distributed ledger approach as a protection against forgery

As is the case with "traditional money", a central feature of crypto currencies is the guaranteed protection against counterfeiting, thus preventing the multiple minting of individual monetary units. Most crypto currencies have in common that they are based on the distributed ledger approach (digital, distributed and, generally, in public trade repositories). The distributed ledger in turn uses blockchain technology. The term "blockchain" is defined as a continuously expandable chain of data records, called "blocks", which are linked together by cryptographic methods and executed and stored in a decentralized network (the distributed ledger). All transactions between parties are recorded transparently and saved with every detail in the distributed ledger. The network of the distributed ledger consists of a large number of computers that are connected to each other via the Internet. There is therefore no central entity to which information is transmitted. All information is known to all computers participating in the network. For example, if a transaction is executed between parties A and B, it is validated for its truthfulness based on the historical account balances and the transactions in the distributed ledger, and a new block containing information about the newly added transaction is appended to the blockchain, which is thus expanded accordingly. The data's integrity is ensured by so-called cryptographic, unique values that are archived and which are known to all participants in the network. They also define the unique irreversible sequence of the information blocks of the blockchain and thus maintain the historical sequence of the processed transactions.

Overview and objective of the (currently) most important crypto currencies

Bitcoin is one of the first crypto currencies and probably the best known. With more than USD 120 billion, Bitcoin currently has the highest market capitalization among the crypto currencies. Decentralized money creation takes place through so-called "mining". Network participants are rewarded with newly mined Bitcoins for making computing power available to process and validate Bitcoin transactions that have been made (bringing about a so-called consensus decision). Put simply, mining involves solving a mathematical task that can be solved only with very high processing power. However, it is quite easy to check the task's correctness afterwards. The miner who solves the task first makes his or her solution available to the other network participants. The other participants confirm the correctness of the solution. Afterwards, a new information block is appended to the blockchain for the correct result, which also contains the transactions that have been executed and now confirmed.
Bitcoin is being criticized because of the procedure described above that allows it to create money (coin) and process transactions. A major disadvantage of this procedure is the immense energy input required to solve the complex computational tasks. Electricity consumption for 2018 is estimated to be around 130 TWh, which is roughly equivalent to Argentina's electricity consumption. The settlement time of transactions is also comparatively slow. Depending on the fees paid, this can range from ten minutes to several hours.

So what does this all mean for Corporate Treasury? From a corporate and treasury point of view, Bitcoins are not necessarily that important. However, one of the few applications where it could make sense is the settlement of transactions in developing countries with a high rate of corruption and an unstable monetary system. For example, demand for Bitcoin in Zimbabwe has risen sharply due to hyperinflation. However, one of the essential ambitions of Bitcoin is to become a real alternative to the established monetary and financial system. But it still has a long way to go. In addition to numerous legal issues (liability, consumer protection, etc.), the fundamental characteristics of money (e.g. universal acceptance and obligation to accept as a means of payment, exchange and preservation of value) are not sufficiently given. Last but not least, state and central banks will not easily give up their monopoly on money creation. Added to this are the current technical and scaling problems that Bitcoin is suffering from. The bottom line is that Bitcoin is an ideological and technological leader among crypto currencies and demonstrates the fundamental technical feasibility of crypto currencies.

Ripple: Comparing Ripple and Bitcoin is like comparing apples and pears. The aim of the private company behind Ripple is not to replace the existing financial system, but to offer banks and payment providers (e.g. credit card providers) a payment transaction platform based on blockchain technology. The goal is to carry out cost-effective and secure (international) financial transactions in real time and much faster than, for example, than Bitcoin – four seconds per transaction, according to Ripple. Ripple thus sees itself in direct competition with SWIFT and its Global Payment Innovation Initiative (SWIFT GPI). Currently, industry giants such as Santander and SEB, as well as tech giants such as Google, are already part of the platform and involved as investors.

Ripple is not based on a publicly accessible distributed ledger and thus a public blockchain as in the case of Bitcoin, but on an internal blockchain, which is called an "enterprise blockchain" ledger. Furthermore, it is a kind of blockchain for bonds ("IOUs – I owe you"), that supports transactions for a variety of (fiat and crypto) currencies. Moreover, the process neither offers Bitcoin-style coin mining nor requires complex, energy-intensive computing operations to validate the performed transactions. Rather, the quantity of Ripple coins created at the beginning serves as a means of payment for transaction fees as well as a bridge currency for the exchange into other currencies for the platform participants. At Ripple, security is based on trust between participants, which are usually financial institutions, that deploy the bank-specific KYC and AML processes. As soon as two contracting parties issue promissory notes to each other, this is stored in the Ripple blockchain. Of particular importance here is that a constant consensus must be found in the network between all participants in a transaction. The Ripple system can only store liabilities, but cannot enforce them. It is therefore necessary for Ripple users to indicate which other user they trust, in what currency and up to what amount, to redeem the stored IOUs on request. If there is no direct trust relationship between sender and recipient, the network tries to identify a path of users, which enables sufficient trust to allow the payment to pass through. In this way, payments seep ("ripple") through the social graph of trust relationships. The register nets all these payments and individuals can then settle their net mutual debts outside the Ripple system. Ripple aims in particular to revolutionize international payment transactions and to compete with the Swift network. In today's traditional payment transaction environment, the processing of an (international) payment via Swift takes between two to four or even more days, as the payment has to pass through several fixed stations (usually four to six) in the correspondent bank network.

So what does this all mean for Corporate Treasury? Ripple's solution is a serious alternative to real-time payments at relatively favorable conditions. Ripple is currently in the beta phase with 75 banks and its success depends heavily on its adoption by the banking sector. However, other competitors are not asleep either and are ready to challenge the "supremacy" of the Swift network, such as among others the Linux Foundation's Hyperledger Project. The R3 consortium is one of the leading providers of blockchain-for-bank solutions. Last but not least, Swift itself is working hard to update its own network. It certainly cannot hurt to continue to keep a close eye on the development of the Ripple payment infrastructure.

Ethereum, in turn, serves primarily as a platform where two parties can enter into a contract (smart contracts) and should not be seen as a pure digital currency. These smart contracts are digital protocols that are intended to replace the analog, paper-based conclusion of contracts. The platform therefore serves to create, manage and exercise contracts, including any corresponding optional rights and clauses. The currency – called ether – is only used as an "insignificant means of payment" for transaction processing. As with Bitcoin, transactions are validated by consensus decision and the proof-of-work method.

So what does this all mean for Corporate Treasury? Potential applications for Ethereum Smart Contracts are manifold and are already being implemented by some companies. These range from logistics processes to the insurance business and financing issues (e.g. project or trade financing). In Treasury, for example, trade finance is a popular candidate. Here, Smart Contracts can solve the inherent trust problem in the context of the transfer of goods and automatically trigger associated payments as well as abolish paper-based processes.

IOTA is currently one of the most innovative crypto currencies. The objective of IOTA is to establish itself as the currency for the Internet of Things (IoT), i.e. for autonomous payments between machines and the related exchange of goods and services. In the future, for example, every car, parking meter or refrigerator would have its own account. The aim is to ensure extremely fast processing of mass (micro) payments without too much processing effort and costs. Recently, companies such as Volkswagen and Bosch announced cooperations with the IOTA Foundation. Compared to the crypto currencies presented above, IOTA would need a much higher transaction processing speed, for which the "conventional, sequentially executed blockchain technology" cannot be scaled sufficiently. IOTA focuses on a further development of the traditional blockchain approach, the so-called Tangle. Speaking from a purely mathematical viewpoint, it is a directed acyclic graph (DAG). Further, this method does not involve any miners. Each "user" (machine or object) must validate two other, randomly selected transactions in order to be able to execute its own transaction. Each participant thus directly contributes to consensus building in the network. In contrast to the conventional

blockchain, several transactions can be validated and executed in parallel in the IOTA Tangle. As a result, the IOTA network can handle more transactions simultaneously and faster than other crypto currencies.

So what does this all mean for Corporate Treasury? Unlike the previously mentioned crypto currencies, IOTA is still in the experimental stage and has yet to prove itself in practice. Once this proof has been provided, the application possibilities are manifold. The typical autonomous machine-to-machine payment process (e.g. between a car and a parking meter) often cited in connection with IOTA can also be applied, for example, to the (internal) production and (service) billing process for products in companies. This in turn has a similar effect on intercompany financing, i.e. the possible associated need for liquidity and the overall throughput time of the cash conversion cycle.

Conclusion

What needs to be done from a Corporate Treasury perspective now? It is becoming clear that the world of crypto currencies is proving to be very complex and the replacement of the established monetary system is not (at least not yet) under discussion. Rather, it can be seen that a "serious crypto community" is increasingly establishing itself. Its aim is to lead crypto currencies out of the shadowy niche existence that is highly speculative. From a corporate point of view, it is also evident that the focus should be on the technologies underlying the crypto currencies rather than the currency itself. Blockchain, smart contracts and Co. can help to make existing processes faster, more efficient and more cost-effective and minimize, ideally even eliminate, the associated risks of trust. Although some of these technologies are not yet mature enough and have yet to prove themselves, it is becoming clear that the developments outlined will have a significant impact on core treasury processes, such as payment transactions, cash & liquidity management, FX trading as well as financing and investment activities in the near future. So what should be done? The first step is to determine your own digital maturity level and to ensure that the potential of existing (Treasury) solutions is fully exploited today. Only then does it usually makes sense to think about the possible applications of new technologies. This situation should be assessed today rather than tomorrow. As this article makes clear, technology is developing rapidly and the gap to the status quo is constantly widening.

Payment operations befallen by e-crime – not again!

Corporate Treasury

The times when fraudsters sent e-mails in standardized or template-like texts in broken English or German are long past. The more aware companies have become regarding cybercrimes, the more complex the fraudster approaches have become.

"Hi Claudia, hope you are doing well! Has your daughter settled well at school? […]". If you received such an e-mail from your line manager, would you suspect it to be a scam? The times when fraudsters sent e-mails in standardized or template-like texts in broken English or German are long past. The more aware companies have become regarding cybercrimes, the more complex the fraudster approaches have become. Cybercrime has become very sophisticated, up to the point where you can buy "cybercrime-as-a-service". For instance, fraudsters can hire a fake call center in the dark web using crypto currencies, which is then used to confirm fake supplier accounts. Or fraudsters buy denial-of-service attacks as a service. The down time is meant to detract the company, thus obfuscating fraudulent payments. Because the attacked company is busy trying to fix the system, it loses valuable time necessary to identify the fraud and to contact the bank to stop the payments. This happened in a medium-sized company in Switzerland last year, where the damages totaled CHF 1.2 million by the time everything was counted.

However, as the latest KPMG study entitled "*Cybercrime at German companies 2017*" that surveyed a total of 504 companies showed that even better-known attack scenarios, such as the fake president scenario, remain wide spread: About a quarter of all companies that were aware of this type of scam had still fallen victim to it. Another quarter reported unsuccessful attempts in this regard. However, since many employees do not report unsuccessful attacks, the number of unreported cases is probably considerably higher. The study also shows that, despite the frequent presence of the topic in the media, more than half of the persons surveyed still were not familiar with the fake president scenario. Of course, this makes it very easy for criminals. After all, how can you protect yourself against something that you are not even aware of? Payment diversions are also widespread. Here, the fraudster tries to reroute payments to his own account using fake notifications regarding changed account information and similar techniques. Cyber criminals are also well equipped with remote access tools giving them access to victims' computers. Once they have access to the computer, they release fraudulent payments or get access to payment operations or treasury management systems that pass unnoticed. How does it work? Fraudsters get access by contacting employees by telephone and then pretending to be someone trustworthy, like a Microsoft support employee or someone working for the treasury management system provider. Using a severe security breach in the system as a pretext, they then help the company employee install the "remote maintenance tool". Once the employee has installed the malware, embezzlers can access the system remotely, spy on the employee and as soon as they have all the necessary information they can do all sorts of things, such as access the e-banking system and make fraudulent payments.

Getting personal

In order to maximize the likelihood of succeeding by using personalization, criminals use highly sophisticated techniques, such as social engineering and spear phishing. Staff involved in payment operations should also understand that fraudsters not only leverage information they obtained solely on the company's IT infrastructure. In order to individualize attacks as much as possible, criminals often gather all of the information available on the internet. Especially social networks, such as LinkedIn, XING, Facebook and Instagram are good targets for hackers. To begin with, hackers gather information on new positions that potential victims have recently started and which are revealed on LinkedIn and XING. The information thus gathered is then enriched with data gathered on private networks, such as Facebook and Instagram, which then allow the fraudster to prepare highly personalized e-mails as described at the beginning of this article. When it comes to social engineering, companies and their staff in key positions are spied on systematically and in great detail. This allows the fraudsters to appear as well-informed "insiders" when they move to attack their victims with scams such as the fake president or remote access tool attacks, making them easier to manipulate to do certain acts. Spear phishing is more specific than the very generic phishing attacks. With spear phishing, attackers send e-mails with very specific person-related or company-related content. For instance, the Head of Cash Management receives a fake e-mail that seems to be a newsletter from the treasury management system service provider that apparently offers a white paper for download. The chance of such an e-mail being more successful than a normal phishing e-mail trying to obtain the password for the person's PayPal account is enormous.

The 80/20 principle is no longer sufficient

Fraudsters have an easy game if companies do not have a complete overview of all bank accounts and payment operations processes. Moreover, significant risks arise due to an incomplete monitoring of the cash pool. The pareto principle (also known as the 80/20 rule) should never be applied in this case because both cash pools and payment operations are only as secure as their weakest link. Our discussions with cash managers often show that unintended cash outflows of less than EUR 1 million may not even register immediately and so can leave the company undetected. The list of security gaps in payment operations is long. For instance, we have remarked that often at Treasury departments, responsibilities have not been allocated to specific positions so that no one feels that a specific weak spot really belongs in their department. Moreover, we still see that databases and the exchange of data involving payment information are unencrypted. This makes it very easy for hackers to spy on or even manipulate data. Add to that a lax handling of access rights, weak bank account management, a high number of exception-to-policy cases that require manual processing and a too narrow view of the end-to-end process chain and the recipe for disaster is perfect as far as payment operations are concerned.

Keeping up with the criminals

The criminal energy that is expended on inventing new scams is considerable so it is better to anticipate rather than just react to incidents. Apart from processes and governance measures, companies should always update their IT landscape to use the latest technology. Modern techniques, such as process mining, allow the identification of weak spots and security gaps in workflows related to payment operations. Process mining is a special technique performed during process management. The idea is to create a profile of operational processes based on analyzed log files and movement files from the company's own IT environment. An ensuing comparison with the process documentation and the new requirements allows the recognition of weaknesses and identify where the system could be hardened. Recently, buzzwords such as blockchain and artificial intelligence have been making the rounds when it comes to risk mitigation in payment operations. However, before anything like that can be undertaken, it is important to first improve the status quo regarding centralization and standardization. The implementation of a payment operations platform is a way of creating the necessary conditions. By bundling payment operations, local banking solutions of individual entities are eliminated, which creates the necessary transparency to safeguard against embezzlers' attacks. Special software providers, such as TIS (Treasury Intelligence Solutions), Omikron, Ementexx or SAP, offer precisely such payment platforms that centralize all payment operations across an entire system and connect to external banks.

However, in the age of digitalization, there is lots more on offer. As already described, this is only the first step that will allow the use of the latest technologies and serves to prepare the data for further processing. Already today, companies have the possibility to identify defrauding attacks with the help of machine learning, thus thwarting such attacks. Analyzing mass data for unknown patterns therefore

helps identify "abnormal" payments and scrutinize these closer. As an alternative, payments could only be made based on rules (which are themselves based on factors such as payment amounts and recipients or user combinations and timing of release). Of course, such a process is only as good as the algorithms used, which base themselves on insights gathered from past damages. For instance, if a large payment is supposed to be made to a supplier that normally receives only payments of smaller amounts, this payment is stopped. The employee in charge of this payment is informed of it by the system and he/she can then release the payment if it is indeed correct or block it if it's fraudulent. So, while rules-based pattern recognition does an excellent job in recognizing patterns, this alone is not very effective in the detection of unknown patterns, in adapting to new fraud patterns and in dealing with the increasingly sophisticated techniques of fraudsters. This is the flagship discipline of new technologies. It will help companies considerably to keep abreast of the constant developments in e-crime.

Despite all the progress, Treasury should not leave aside traditional and trusted methods, such as reminding employees to be on the watch for any inconsistencies, clearly defining end-to-end processes in payment operations, implementing appropriate release processes and segregating duties as well as regularly reviewing systems and processes relevant to payment operations. These instruments form the foundation of secure payment operations and are supplemented by new technologies as they become available.

KPMG

IFRS 2

New aspects on the measurement and classification of share-based payments

Corporate Treasury

IASB resolved on 20 June 2016 to present its final adjustments to IFRS 2. All changes are mandatory and to be applied prospectively for reporting periods beginning on 1 January 2018.

The changes made to IFRS 2 heavily influence companies' valuing and recognizing of share-based payments in the financial statements. The adjustments are to bring clarity to aspects in the accounting standard that had not been clearly defined so far, thus reducing the complexity in regard to valuation and recognition.

The adjustments were made in three clearly delineated areas:

1. *The classification of share-based payment transactions with net settlement features*
   For agreements that foresee a net settlement (and thus the withholding of the tax burden for the employee in question) it had never been clearly defined what kind of impact the splitting between cash payment (direct payment of the taxes to the tax authorities) and the issue of equity instruments (remuneration of the employee) had on the classification of the payment. Such plans are regarded independent of the tax withholdings and will continue to be classified as equity settled.

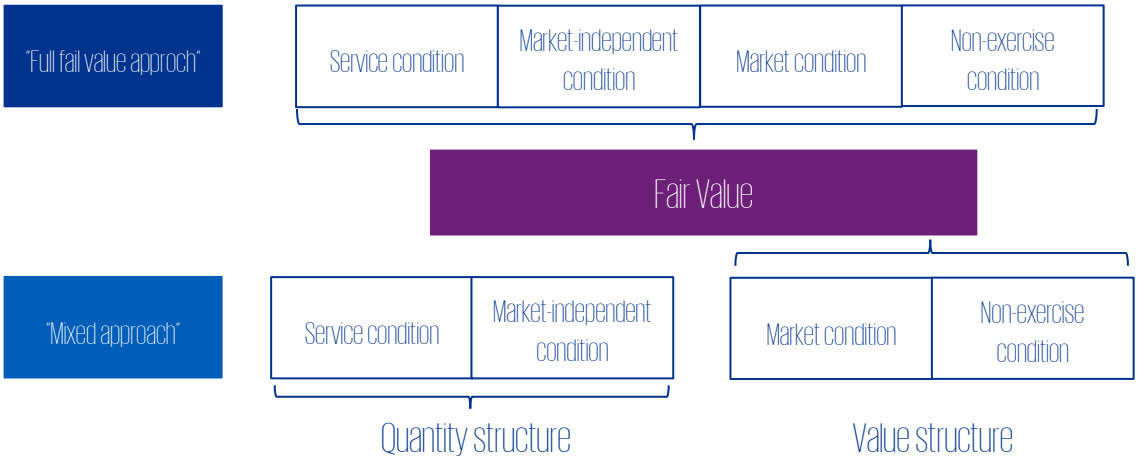
2. *Recognition of a modification of share-based payment transactions from cash-settled to equity-settled*
   These extensions complement IFRS 2 with accounting rules for a modification that changes the classification of payments from cash-settled to equity-settled. As a rule, an increase in equity is to be recognized on the day of the change, with a simultaneous derecognition of the provision for the planned cash-settled payments up to that date. Any difference has to be recognized as an expense or as income. Discrepancies could develop because of the different measurement times between the existing payments where cash settlement is used and the re-measurement of the payment using equity instruments (book values versus value as at the time of the modification) or because the vesting conditions have been modified further.

3. *Taking into account of the vesting conditions on the measurement of cash-settled share-based payments*
   The IASB defined how to recognize the different vesting conditions when measuring cash-settled payments. The valuation is now carried out in the same way as with equity instruments and will be considered in more detail later on.

Standardized measurement approach

This adjustment of IFRS 2 eliminates the possibility for companies to include all of the vesting options in the measurement of the fair value, the so-called full fair-value approach. Now, the mixed approach, where the employee's service and market-independent performance conditions are reflected (also called the modified grant date method) in the quantity is mandatory. Market conditions and non-

exercising of the option on the other hand are reflected in the fair value (see graph below). A significant difference between the two measurement approaches is that the mixed approach recognizes the payment only once it becomes likely that the employee fulfills all of the service and market-independent performance conditions by the end of his or her vesting period. In doing so, the concept of "likely" is defined with a "more likely than not" condition. When looking at it like this, a separation between values and quantities can therefore lead to deviating book values for the payment.



The reason for such a deviation is the different treatment of the components in the quantity of the mixed approach, where the vesting conditions have to be fully recognized as soon as the company deems the conditions likely to be fulfilled by the end of the vesting period (i.e. more than 50 percent likely). Contrary to this, the full fair value approach would also include these values or components, which would not be included in the mixed approach (i.e. those with a likelihood of less than 50 percent) and vice versa.

Conclusion

The changes made to IFRS 2 are to be applied prospectively, which means that there could be considerable changes as at 1 January 2018. Companies that are leaving their current measurement approach for cash-settled payments, i.e. the full fair-value approach for the mandatory mixed approach and that have follow new accounting principles. The consequences of the change in the measurement approach could have a significant impact on the previously used book value of the payment, depending on the parameters described above, and, accordingly, should be anticipated in a timely manner.