TRADE REPUBLIC

Risk Information Crypto

There are very specific risks associated with the crypto business, which Trade Republic Bank GmbH (hereinafter "**Trade Republic**") first points out.

What are cryptocurrencies and how do they work?

"**Cryptocurrencies**" are a collective term for a range of virtual digital currencies. These are currently tradable as speculative assets in global financial markets. Examples of some of the major cryptocurrencies include Bitcoin, Ether, and Solana. The German Banking Act and the Markets in Crypto-Assets Regulation ("**MiCAR**") refer to "crypto-assets".

A significant difference between cryptocurrencies and traditional money, such as euros or dollars, is that virtual cryptocurrencies function independently of central banks or states. This is the case because it is not one (or a few parties) that decides on money supply and enforcement of property rights, but usually a decentralized network of many participants that coordinate the organization of the cryptocurrency. In this respect, cryptocurrencies do not have any "intrinsic" value, which, in the case of gold coins, for example, can be derived from the material value.

Whereas with traditional currencies it is usually the central banks that decide on the creation of new money and generate it, the creation of new "coins" (value units of the cryptocurrency) takes place directly in the encrypted, usually decentralized database of the cryptocurrency. In this database, all transactions and events are documented and stored - sealed in individual blocks - one by one. Since these blocks are usually linked together in the form of a chain to ensure that individual blocks cannot be subsequently changed, the database is also often called a "blockchain". A coin is nothing more and nothing less than a data record on this blockchain and thus a part of the program code of the blockchain. It is therefore nothing more and nothing less than lines of programming to which the market attaches a certain value.

The blockchain can therefore be thought of as the diary of the cryptocurrency, in which - publicly visible to all - pseudonymously stored who owned how many coins of the cryptocurrency at what time and where they were transferred to when.

"**Distributed Ledger Technology**" ("DLT") or simply "Distributed Ledger" is another common term for the described technology. We have chosen to use the more common term "blockchain". However, this is merely a synonym and refers to the same technological processes and the same associated risks.

In the blockchain, the legitimacy of individual events is also verified before they are irreversibly stored in the blockchain as new events. This verification is carried out for cryptocurrencies by means of various verification mechanisms. The most widespread is the so-called "**proof of work**" procedure, which is currently used for Bitcoin. In this mathematical procedure, at the end of which the blockchain is extended by a further block, all participants in the blockchain (the so-called "**miners**") work together to verify and document the information to be stored by solving a cryptographic puzzle. This requires significant IT computing power on the part of the miners. The participants who solve the puzzle first are allowed to add the respective new block to the blockchain and are rewarded with new units of cryptocurrency ("**Block Rewards**"). In the case of the cryptocurrency Bitcoin, the total amount of possible existing Bitcoins is limited (but not yet reached), while other cryptocurrencies do not (at least not yet) have such a limit (e.g. Ether). Alternative consensus protocols or verification mechanisms, e.g. "**Proof of Stake**" or "Delegated Proof of Stake", require significantly less IT computing power from the participants, as they reach a consensus on which participant may add the next block by means of a weighted random selection, in which in particular the duration of participation and the share of coins held, and not the computing power (as with Proof of Work), is decisive.

Nevertheless, even these consensus protocols may be susceptible to attacks that attempt to modify the blockchain. If they were to be successful there would be no alternative blockchain that backs up the transactions and hence the balances corresponding to the public keys and therefore all the crypto-assets could be lost.

Since the blockchain is not only extended by all participants/miners, but is also stored decentrally by all network participants, it is particularly difficult to manipulate the system, since once verified information can be confirmed by all participants and new information can be verified by all. Only when the majority of participants have verified a transaction is it irreversibly documented in the next block on the blockchain. This decentralized principle for verifying transactions, which is based on the elimination of central parties (such as banks or authorities), is also called the "**peer-to-peer**" principle.

Among other things, the blockchain also stores in anonymous (or pseudonymous) form which user owns how many and also which crypto values. For this purpose, each user has a kind of address under which his coins are "stored" and to which other participants can send further coins. This address is public and is also called "Public Key". You can compare the Public Key with a kind of account number. However, which participant has which public key - in order to

initiate transactions, for example - must be exchanged outside the blockchain. In addition to the public key, each participant also has a so-called "**Private Key**". This can be thought of as a password: It should be kept secret by the user and allows its holder to authorize transactions in the blockchain. Together, these two keys form the so-called "wallet", which is comparable to a digital wallet. However, this wallet does not store the cryptocurrencies, but only the keys necessary to access the cryptocurrencies. The wallet, and especially the Private Key, should be kept with extreme care, as a loss is irreversible and there is no possibility of recovery or reset (such as with a forgotten bank PIN).

Cryptocurrencies are not a substitute for money that can be used fungibly in the market. The acceptance of crypto-assets as a means of exchange is still very limited as there are only a few places that actually accept cryptocurrencies as a means of payment. In particular, there is no obligation to accept crypto assets.

Unlike well-known currencies, which are often backed by the economic power of a state, and unlike stocks, which are backed by the economic power of a company, this is not the case with cryptocurrencies. There are no underlying value-creating factors, a material value or a value established through decades of market acceptance. The price value is determined solely by supply and demand, the limited availability and the expectations of investors in the future price development. Significant price gains or losses can thus occur without it being apparent why this is happening at any given time.

Cryptocurrencies are therefore highly speculative financial instruments and every customer must be aware that he bears a significant risk here, up to the total risk of loss. In addition to the usual risks of financial investments, such as the price risk, there are also specific risks. Especially investments in early-stage projects involve a high level of risk, so it is necessary to properly understand their business model.

The technologies described herein are always evolving as such networks may have been created very recently, so they may not be sufficiently tested and there may be significant failures in their operation and security outside of Trade Republic’s control.

Volatility and 24-hour trading

Since there is not always a comprehensible relationship between economic data and price value and the main driver for the price development on the market is supply and demand, cryptocurrencies are usually very volatile. In this context, it should be noted that there are no mechanisms that ensure the correct formation of prices (as used, e.g., in regulated securities markets). The acceptance of the market participants with regard to the respective cryptocurrency is also decisive for the price development. This means that there can be significant price swings in one trading day and even in just one trading hour, even reaching double-digit percentages. A client can therefore easily suffer a large loss or profit on one trading day.

In addition, even small amounts of the respective cryptocurrency may be sufficient to trigger significant price movements, as cryptocurrencies are not always liquid. It cannot therefore be ruled out that attacks on cryptocurrencies will be carried out by third parties acting alone or together.

When speculating, the customer must therefore bear in mind that significant profits as well as losses can always occur, even at night or on Sundays and public holidays. This is because cryptocurrencies are usually traded around the clock and without interruption. This can lead to a cryptocurrency experiencing a significant change in value overnight while the customer is still asleep.

Liquidity

A financial instrument is liquid if trading in it is so brisk that you can always find a buyer or seller and you can therefore easily part with a financial instrument by selling it again. Bitcoin's liquidity is currently high, but this is not true for all cryptocurrencies. It can therefore come to situations that it is not possible to promptly part with cryptocurrencies by selling them or must accept significant price reductions.

Legal classification

The legal classification of cryptocurrencies has changed repeatedly in recent years. Most recently, the Markets in Crypto Assets Regulation (MiCAR) established a uniform legal framework across Europe.

German Crypto Market Supervision Act (KMAG) stipulates that, in the event of a crypto custodian's insolvency, the crypto assets held in custody belong to the customer, thereby protecting their rights.

Additionally, there may be a lack of clarity regarding the applicable legal system for cryptocurrencies. In the event of a conflict, this may have adverse effects on the legal position of the customer.

System operator risk

The existence and function of cryptocurrencies depends on certain entities / system operators (so-called "full nodes") maintaining the system by updating the blockchain. This happens without any central control or obligation. It cannot be ruled out that individual or all of these so-called full nodes will cease to operate a particular cryptocurrency and thus, if no replacement is found, the cryptocurrency will no longer be tradable. These full-nodes could also significantly increase the transaction costs for cryptocurrencies, making transactions uneconomical. Trade Republic would then have to decide whether and how to pass on any costs.

It is also conceivable that some of these system operators could merge, resulting in fewer control instances for a cryptocurrency, which would in turn make it more vulnerable to attacks from outside.

Trading partner risk / mistrade risk

Trade Republic has connected liquid trading partners. However, it can never be ruled out that the connected trading partner will suspend trading in the event of increased volatility in the market. This can lead to customers not being able to sell their cryptocurrencies while the trading suspension continues and thus suffer losses.

Trade Republic's current trading partners can be found in the "Information on Trading Venues" (available in the app under profile/settings/your documents/trading venue information).

Trade Republic as commission agent only passes on to the client what Trade Republic receives from the execution of the commission. Therefore, the client's contractual rights are also affected by these trading venue contracts.

In addition, the contracts contain special mistrading rules, the content of which the customer can access via the app (profile/settings/your documents/trading venue information).

No deposit protection

Crypto assets are not covered by client protection mechanisms such as the Deposit Guarantee Scheme or the Investor Guarantee Scheme.

Fork risk / Settlement risk

Cryptocurrencies are allocated through entries on the blockchain. This is done in a decentralised manner by various bodies. The blockchain is updated by different bodies. This can lead to the blockchain being updated in parallel in different strands. Example: Full node "A" simultaneously updates block XYZ of the Bitcoin blockchain with transaction data, while full node "B" updates other transactions in the same block. Later, the majority of entities that update the blockchain agree on which of the strands is the binding strand that will continue to be updated. The other strand is then called a fork and is no longer binding. If a transaction affecting the customer is on a fork, they have not received the cryptocurrency and may no longer receive it. There must then be a correction to the customer's transaction. This may also mean a reversal. With this in mind, it is also theoretically possible that even a transaction that took place a long time ago could be "eliminated" in this way. However, the market assumes that if only a few blocks are updated on the blockchain, a practically relevant "fork risk" no longer exists.

Cryptocurrencies also need to be settled. However, the settlement of these transactions can also take longer than with normal share transactions. As a rule, this is not the case, but here, too, it cannot be ruled out that difficulties may arise in the delivery of cryptocurrencies and/or payments. This may result in the corresponding transactions of a customer having to be reversed.

Regulatory risk

States sometimes look critically at cryptocurrencies because they are difficult to control. It is not impossible that a regulatory authority or a state will ban cryptocurrencies in whole or in part or regulate trading in them even more closely. This may have an adverse impact on customers, to the point that they may have to accept significant price discounts. Increased regulation can also lead to cryptocurrency falling in attractiveness to investors and prices falling. All of this can also occur if a foreign authority (or state) with the appropriate power regulates the cryptocurrency and urges all market participants worldwide to comply with this decision.

Software risks

Cryptocurrencies are based on software. Like any other software, there is never any guarantee that the software underlying the cryptocurrency is error-free. However, any errors may affect the cryptocurrencies held by the customer.

Risks of Crypto Transfers

Transfers of crypto assets involve specific risks. Due to the technical and operational characteristics of distributed ledger networks (blockchains), once executed, Crypto Transfers are irreversible. Transferred crypto assets therefore cannot be recovered. Customers are responsible for initiating Crypto Transfers with the utmost care – in particular by entering the correct wallet address and ensuring that both the type and amount of crypto asset to be transferred are entered correctly.

In addition, regulatory requirements apply to Crypto Transfers, which may oblige crypto asset service providers to collect certain data. In such cases, it is the customer's responsibility to provide this information promptly to enable the execution of the desired Crypto Transfer. Failure to provide the required data, or to do so in a timely manner, may result in delays in execution or even in the reversal of the intended Crypto Transfer.

Furthermore, network fees charged by the respective distributed ledger network (blockchain) apply to Crypto Transfers. Customers should review these fees carefully before initiating a transfer and be aware that such fees are to be borne by them, unless the crypto asset service provider covers them on the customer's behalf.

Risks of Crypto Staking

Crypto Staking involves specific risks. When staking, crypto assets are deposited within a network to validate transactions and earn rewards.

Staked crypto assets may, in exceptional cases, be subject to losses, in particular due to so-called slashing penalties. Slashing penalties occur when the participating network detects misconduct by the validator (e.g., double signing, inactivity, or technical misconfiguration). In such cases, a portion or even the entirety of the staked crypto assets may be confiscated or destroyed.

In addition, staked crypto assets are subject to lock-ups. This means that during the staking period, as well as during certain pre- and post-staking periods (so-called warm-up and cool-down periods), crypto assets cannot be transferred, sold, or otherwise disposed of. As a result, staked crypto assets may only be transferred or sold after a certain delay.