MAERKI BAUMANN & CO. AG

PRIVATBANK

Cryptocurrencies - What exactly are they?

Finance Theme, January 2019

The turbulent performance of Bitcoin over the last year has brought this cryptocurrency to the attention of the wider public. But this currency has actually been around for almost ten years, and an estimated 1,600 other alternative currencies have also sprung up in the meantime. The question is often asked whether these constructs – which only exist in the form of digital code – can really be considered currencies at all in a way that bears comparison with the dollar, euro or yen. We will return to this question later in this article. First of all it is worth establishing what actually lies behind cryptocurrencies such as Bitcoin, Ether and Ripple.

These currency constructs are based on blockchain technology, which was developed back in 2008. This computer technology involves data being encrypted and simultaneously stored on many computers. Information on the owner and the transfer of ownership is likewise incorporated into the encryption process. With each transfer that takes place, the encrypted data is augmented. In order to prevent this information being falsified or retrospectively corrected, all data is amalgamated into an individual string of characters. This sequence of characters is termed a hash, as all data is broken up and commingled. A blockchain consists of a sequence of these hashes, which – although they can be read by everyone – can only be decrypted back into meaningful data by the owner of the decoding "key". Transferring a block to another party is only possible if the majority of computers confirm the accuracy of the character string. In other words, the code can hardly be manipulated.

Due to the decentralized construction of this technology, it is also possible for an exchange to take place between two strangers – there is no need for the two parties to know or trust each other. Trust in the system is ensured through the security of the coding, the incorruptibility of the system itself, and the sheer number of participants. A retroactive change to the blockchain, i.e. fraud, requires two things, which – given the current state of technological knowledge – can only be achieved with a disproportionately large amount of work. On the one hand, the coding of a blockchain needs to be decrypted and changed flawlessly without ownership of a private key. On the other, this change needs to be recorded on at least 51% of all the computers that form part of the network. Because only if a majority of all computers approve the transaction and determine it to be correct can a transfer take place. This technology can be used not just for cryptocurrencies, but for any kind of transfer of material or non-material valuables. For example, this technology is already widely used in the trading of diamonds.

This technology can be used not just for cryptocurrencies, but for any kind of transfer of material or non-material valuables.

The next question is precisely what value these currencies represent. Apart from cryptocurrencies issued by a country – such as the critically viewed Venezuelan Petro – these currencies are not backed by the financial strength of a sovereign state. In other words, when you trade a cryptocurrency you are also trusting that another party will accept it as a means of exchange against a traditional currency such as the franc, dollar, or euro.

How can cryptocurrencies be traded?

These currencies are traded on hundreds of Internet exchange platforms that exhibit varying degrees of trustworthiness. Moreover, depending on the exchange platform cryptocurrencies can also be swapped for one another, e.g. Ripple can be exchanged for Ether, while Bitcoins originally acquired with a traditional currency can be exchanged back into US dollars or yen. It is also possible to trade fractions of cryptocurrencies, as the currency units can be very easily broken down into smaller units. Similarly, it is also possible to sell back just a proportion of the originally purchased holding.

In order to open an account and purchase cryptocurrencies, an electronic wallet is required. A wallet in this sense of the word is a small program that can be installed on

a smartphone or computer and execute two tasks. First, it can be used to generate a private key, which is essential for the purposes of providing a signature for transactions and accessing your account. If this private key is lost, the valuables secured with it are also lost, as these can neither be decrypted nor transferred in the absence of the key. Secondly, the wallet serves as a repository for Ether, Bitcoin, and their like. So this really is a wallet in the truest sense of the word, as it is where virtual monetary units are stored until they are sold or used to pay for something.

How can cryptocurrencies be kept safe?
Wallet applications are typically free of charge, allowing the individual to store cryptocurrency assets independently of banks or exchanges, just like a private safe. The owner has access to this wallet at all times and anywhere in the world, which makes them particularly attractive for people who are moving around in insecure environments, e.g. refugees or residents of countries with no functioning legal system.

But in addition to the above, there are three other ways of holding cryptocurrencies, which differ by the level of security they offer. The least secure option is an account held with one of the many trading platforms or crypto exchanges. These accounts are known as "hot wallets". The security standards offered by these institutions differ greatly, as there is still practically no regulation in place for marketplaces of this kind. The repeated stories of Bitcoins being stolen almost always involve a successful attempt to hack into these exchanges, whereupon the thieves can then simply empty client accounts. A much more secure option is to have larger amounts stored by trustworthy cryptobrokers in their secure storage facilities. You can also, of course, store the cryptocurrencies in your private wallet or on your own computer or smartphone

An even greater level of security can be achieved with special devices that only create a connection with the computer or smartphone (and therefore the Internet) when they are required to do so. These are actually a kind of specially secured device such as an encryption box. In the jargon of the market, this is also known as a "cold store". The securest way of storing your personal holding of Ether, Ripple, or Bitcoin is still to print out the blockchain code and the private key and then deposit these in a steel safe.

The different ways in which you can store currency units also give rise to differences in speed of access. For the purposes of daily trading on an exchange, it makes sense to have a certain amount in an account held with an exchange or a broker. A few providers spontaneously separate the amounts held for trading from the larger holdings that are not currently required for daily trading. As it is rather more laborious to sell Bitcoins and private keys based in paper form or from a cold store, these forms of storage are more suited to larger amounts that the owner rarely needs to access.

How can cryptocurrencies be mined?
The security and the functioning of blockchains is hugely dependent on the number of computers that review transactions and determine them to be correct. This work – reviewing the transactions of third parties and storing the amended blockchains locally – requires considerable computer processing and storage capacity. In order to make this work worthwhile, participants can also create new currency units and then book these to their accounts as personal profit. This process is known as mining. In order to mine new Bitcoins, for example, it is necessary for the information block data to be encrypted into a hash. The reward for completing this kind of encryption process (currently) amounts to 12.5 bitcoins. Additional rules are incorporated into the algorithm, which makes the encryption process increasingly complicated as time goes by, and with every encryption that is successfully completed the reward is an ever-decreasing number of Bitcoins. For that reason, only large server farms are truly profitable when it comes to mining new Bitcoins.

That said, private individuals without dozens of computers at their disposal can still benefit from mining. Often it makes sense for several miners to work simultaneously on a single block, and the reward will then be shared proportionately. For this purpose, "mining pools" have been set up to ensure that mining revenues are more calculable and regular. However, membership of a mining pool comes at a cost, which reduces the return. The key factor in effective mining is the performance capability of the computer processors, as this is what determines the speed at which encryption takes place. The costs of the current generation of such chips, together with the electricity cost of running them, make small-scale mining only profitable to a limited degree.

How do the cryptocurrencies differ from one another?
The number of different currencies, tokens, coins, etc. that are based on blockchain technology is already enormous. Essentially these constructs can be broken down by category according to what they represent – as is done by the Swiss Federal Market Supervisory Authority, for example. Accordingly, a distinction can be made between constructs that represent assets (asset tokens), those that represent usage rights (e.g. memberships, utility tokens), and finally the pure payment tokens (e.g. Ether). Below we focus on the third of these groups.

Bitcoin is without question the best-known and most significant cryptocurrency. Thanks to its broad spread, it offers a high level of acceptance and a high level of liquidity (i.e. ease of trading). At the same time, however, this currency also attracts criminals and fraudsters who can exploit the experience of newcomers.

Ether is the name given to the currency based on the Ethereum platform, which uses a more developed and flexible form of blockchain technology. Ether's great advantage over Bitcoin is that additional conditions can be linked to the transfer of Ether by being directly integrated into the blockchain code. This process, which is known as a smart contract, accordingly facilitates a much greater range of possible applications than Bitcoin. In addition,

there is no maximum number of units stored in this code, which means that more Ether can continuously be created as required.

Ripple is a currency which does not have a decentralized structure involving different, independent computers. Instead mining is carried out centrally and authentication is the responsibility of the company Ripple Labs. This currency was primarily developed for banks with a view to simplifying and accelerating payment transactions.

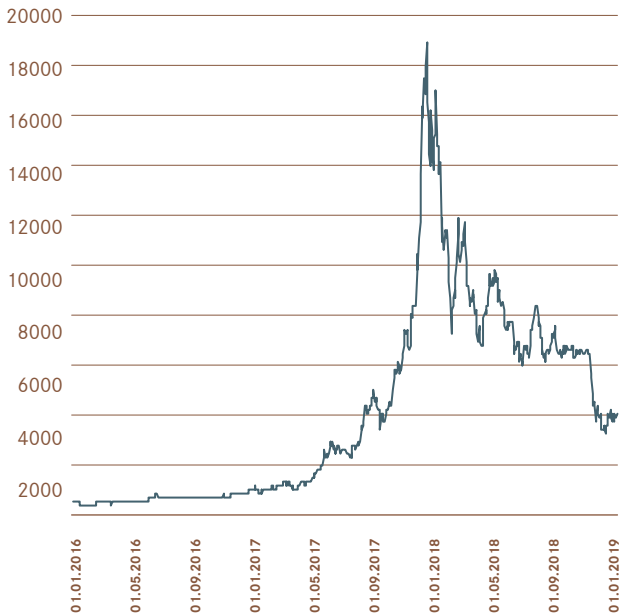
Litecoin is a spin-off ("fork") of Bitcoin. In other words, this currency is based on the same technology but offers significantly faster processing of transactions. To achieve this the currency uses the Lightning Network, which can process significantly more transactions than conventional networks. In addition, Litecoin is much cheaper to work with than Bitcoin.

Are there any alternatives to direct investments?
A number of investment products now exist (investment funds, structured products/certificates) that are suitable for less experienced investors in particular. These replicate the price performance either of individual currencies or of a defined basket of cryptocurrencies. This eliminates the trading and storage risk for the currencies, but attention must still be paid to the issuer's quality and investment policies. The products of known companies in Switzerland or neighbouring countries should be given preference.

Development of value: a rollercoaster
The price performance of cryptocurrencies in the past resembled a rollercoaster ride. There are a number of different reasons for these dramatic price movements, but none of them have anything to do with the usual factors that determine the market rates of traditional currencies. The price of a traditional currency is predominantly driven by current and expected interest rates in the corresponding currency area, anticipated economic developments, and – to a certain extent – political factors. Drivers of this kind are irrelevant to cryptocurrencies, as they are independent of economies and currency areas. For this reason, other price factors are at work here.

As with all goods, supply and demand are crucial for the market price. In the case of Bitcoin, it should be observed at this point that the maximum number of currency units is limited to just under 21 million. In other words, if demand rises and supply remains stable, the price will generally rise. No such limitation applies to other cryptocurrencies. Some experts believe that the usefulness and frequency of application of a cryptocurrency are important factors in its performance. Either way, if a currency is accepted as a means of payment and exchange in many spheres, this has a corresponding impact on its liquidity. From a short-term perspective, the newsflow relating to these new currencies is the greatest driver of prices. Reports of thefts of currency holdings, security problems on trading platforms, and the prohibition of initial coin offerings (a kind of securities issue based on blockchain technology) by individual countries can all put downward pressure on the price of a cryptocurrency. Additional factors here – just like in any market – include general market sentiment and expectations, as well as the market's assessment of other asset classes that could serve as investment alternatives.

Price development Bitcoin vs. USD



Source: Bloomberg

Thus there are many reasons why cryptocurrencies sustained sharp losses in the past year. A tightening-up of regulations on trading, ownership and mining in various countries has reduced the appeal of these currencies. Major investors took profits following the massive rise in 2017 or entered into bets on a fall in rates (short position). A further blow was dealt by the US supervisory authority's repeated refusal to allow cryptocurrency investment funds. And finally, many investors were unsettled when Bitcoin Cash was split off from Bitcoin.

Should I invest in cryptocurrencies?
The dynamism of the development of cryptocurrencies such as Bitcoin, Ether and Ripple peaked in 2017 and 2018 with the dramatic and erratic performance of various currencies, the massive increase in the number of initial coin offerings (ICOs) and regulatory responses in a number of countries. In the meantime, another form of blockchain-based financing has been created. Unlike ICOs, "security token offerings" (STO) embody a claim to the issuing company's earnings or assets. They thus offer investors more security than ICOs. At the same time, the legal status of cryptocurrencies and tokens resulting from ICOs has yet to be definitively clarified. For example, the pragmatic assessment of FINMA differs hugely from the current attitude of regulators in the US, namely that all cryptocurrencies should be viewed as securities. Whether or not cryptocurrencies will turn out to be long-term success stories cannot be judged from today‘s standpoint. Equally, however, we believe that cryptocurrencies are unlikely to disappear altogether. Rather, we are convinced that the regulated use of blockchain technology offers great opportunities for trading in assets that can be easily transferred via tokens.
We currently discern a certain amount of stabilization in

this area, both in the market and on the regulatory side. However, the approaches pursued by regulators are extremely divergent. Some countries are encouraging the development of these instruments through a benign regulatory framework that involves addressing the various outstanding legal questions (Switzerland, Japan, United Kingdom, Sweden). In other countries, the focus is on prohibiting the trading and mining of cryptocurrencies, while at the same time exploring the possibility of creating a state blockchain-based currency (China, South Korea, Russia).

The acceptance and custody of the funds generated through the mining and trading of cryptocurrencies continues to be overshadowed by all kinds of legal uncertainties for banks and investors alike, as there are no fixed rules laid down by the various national supervisory authorities. Due to the technical construction of cryptocurrencies, it should in principle be possible to furnish definitive proof of origin of such funds. However, this can be an extremely laborious process, depending on the scope of the relevant trading activity.

Maerki Baumann is keeping an eye on the development of these investment instruments and the corresponding progress on the regulatory side, without looking to gain exposure to this young asset class at the present time. This is true not just of direct investments in cryptocurrencies, but also investments in the necessary technology for the trading and custody of these instruments. We see cryptocurrencies as alternative investment instruments for which currently only limited empirical data and information to call upon (prices, volatility, trading volumes) is available. Maerki Baumann is generally prepared to accept funds generated through cryptocurrencies, be it through speculative transactions or in the form of payment received for services provided or from mining profits.

Generally speaking, however, we would advise against any major investment in cryptocurrencies at present. In our view, cryptocurrencies are unsuitable for long-term investments due to the uncertainties set out above. Only investors who are aware of all the risks associated with these investment instruments should consider allocating a limited proportion of their disposable assets to this asset class. We would currently advise all other investors to avoid a large exposure in this area. Maerki Baumann does not offer direct investments, but we are happy to support the evaluation of investment products.

Maerki Baumann does not issue recommendations regarding the quality of crypto exchanges and/or custody solutions (wallets), but we would be happy to provide interested clients with contact details for specialists in the area of blockchain technology and cryptocurrencies.

Editor: Milko G. Hensel, IT & Digitalisation
Editorial deadline: 9 January 2019

Maerki Baumann & Co. AG
Dreikönigstrasse 6, CH-8002 Zurich
T +41 44 286 25 25, info@maerki-baumann.ch
www.maerki-baumann.ch