Special Risks of Digital Assets

November 2020

Information to clients of financial service providers

Bitcoin Suisse

Content

About this Brochure

With the evolvement of distributed ledger technology, digital assets, new markets and participants, it becomes relevant to provide information on these topics and the associated risks.
The aim of this brochure is to inform persons or entities that have engaged themselves in this new market either by themselves or by choosing a financial service provider specialized in digital assets.

The first chapter of this brochure gives a brief introduction to distributed ledger technology ("DLT"), blockchain and digital assets characterized by utilizing DLT. The second chapter identifies various financial risks (risks related to markets, credit and liquidity). Lastly, the third chapter describes non-financial risks (technical- and operational risks along with legal- and regulatory risks).

This brochure has margin navigation or each chapter is concluded with a "Caution" section which highlights and summarizes the described risk in a brief, accessible manner and explains how the risk can be mitigated.

The information provided in this brochure is for general informational purposes only and should not be considered exhaustive. The reader is therefore encouraged to obtain professional advice before making any investment in digital assets.

We hope that this brochure is informative and useful for you. Suggestions and feedback are welcome to the authors.

Kindest regards,
Bitcoin Suisse AG

1. Introduction

1.1 Distributed Ledger Technology and Blockchain

DLT

The terms “Distributed Ledger Technology” (“DLT”) and “blockchain” are often used interchangeably. However, this is imprecise, and differentiation must be made. (see illustration 1 below for terminology overview)

DLT is a collective term for technologies that apply a distributed database architecture.
This means that each computer around the world maintain multiple, identical copies of the database and run a software to align and coordinate this. At the time of writing, there is by way of example 7618 nodes spread across 100 countries on the Bitcoin network[1].
For reference, the opposite of this would be one, central server in a single location owned by one company or person.

Public, private or permissioned

Distributed ledgers can either be public (anyone with a node can participate), private (a company or person builds its own distributed ledger for internal purposes) or permissioned (possible to participate by invitation and verification of the participant).

As the market capitalization of digital assets can be attributed primarily to digital assets issued on public distributed ledgers, this brochure mainly describes risks associated with these.

Blockchain is a specific type of distributed ledger technology.

Blockchain

The term “blockchain” simply describes that data is recorded in blocks which are chained to each other by using cryptography.
In detail, this means that a block consists of validated transactions. Once a block is full of transactions, the block is closed (or “hashed”) by using a cryptographic hash function which contains the data of all the transactions in the block, and a reference to the previous block thus creating the chain or link between the blocks.
New blocks are found and added to the chain by the nodes in the network. Once found, the block can be filled with new transactions, hashed and the cycle repeats.

[1] Source: https://bitnodes.io/. Reachable nodes as of Monday, September 7, 2020

Transaction example

By way of example, a Bitcoin blockchain transaction is completed in the following manner:

1) New transaction requests are sent to all nodes in the network. A node is a computer that is connected to the Bitcoin blockchain by running the required software.

2) From these transactions, "mining" nodes ("miners", a fraction of all nodes) construct blocks and try to solve a puzzle known as "Proof of Work". This solution is a number ("nonce") that is repeatedly guessed until the block conforms with Bitcoin's rules.

3) If the new block candidate is accepted by other nodes (which it will be if the solution is correct and all transactions are valid*), the block is added to the Bitcoin blockchain.

4) The transactions within this new block are now confirmed, and miners begin searching for the next block.

*an invalid transaction would, for example:
spend coins that have already been spent
contain an invalid digital signature

DDBMS:
A type of database management system.

DLT:
A ledger-database which records data changes (A transaction from Person A to Person B can be considered as a data change).

Blockchain:
The data is recorded in blocks, which are organized chronologically in a "chain". Bitcoin and Ethereum uses blockchain.

Public:
Any person or entity can participate.

Private:
E.g. a company's own blockchain.

Permission:
Participation after verification and authentication of the participant.

Caution

The distributed ledger on which your digital assets are registered and transferred is not operated by your bank, broker, or other central institution and thus outside the control of these. All interactions with a distributed ledger are at the sole risk and responsibility of the user.

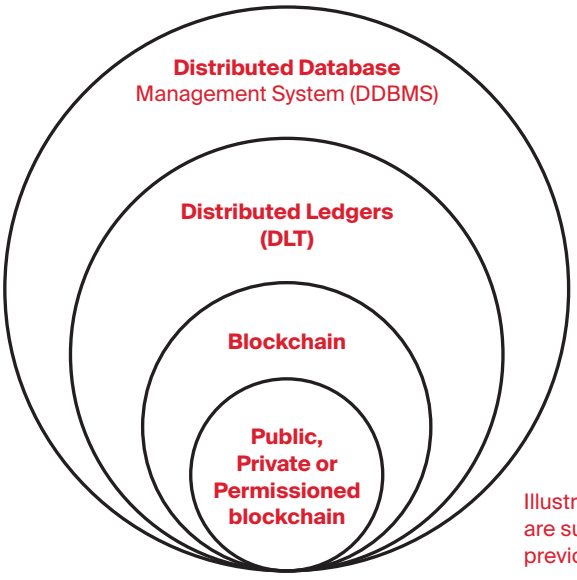

Illustration 1: All circles are sub-categories of the previous, larger circle.

[2] Adapted from: Satoshi Nakamoto, 2008, Bitcoin: A Peer-to-Peer Electronic Cash System, page 3.
See also https://github.com/bitcoin/bitcoin

1.2 Digital Assets

What are digital assets?

Digital assets are an evolving, non-uniform asset class characterized by the use of DLT where the holder can control the asset by means of cryptographic methods.

Digital asset is a general description and can be used both for already existing, traditional assets that are registered on a distributed ledger and for assets that are solely issued and existing on a distributed ledger.

Digital assets and cryptocurrencies

Digital assets may constitute native units of value issued and transferred on a specific blockchain. These do not include or represent any claim against an issuer or any third party. Where such units are intended or used for payment purposes and do not qualify as a security or financial instrument, they are sometimes referred to as payments tokens or cryptocurrencies.

For simplicity, only the term digital asset is used throughout this brochure.

"Substance over form"

Where digital assets constitute, embody, incorporate or represent securities or forms of financial instruments, the risks associated with them in their traditional form remains associated also in their representation of a digital asset.

General information regarding risks in securities trading can be found in the brochure Risks Involved in Trading Financial Instruments issued by Swiss Bankers Association (SBA).

Caution

The risks associated with financial instruments in their traditional form remain notwithstanding the use of DLT. Therefore, additional, risks may be added when registering financial instruments on a distributed ledger.

2. Financial Risks

2.1 Market Risk

What is market risk?

Market risk is the risk of an investment losing its value partially or in whole due to changes in the market.

What are the risks?

The following risks are examples of risk in the market that may affect the investment in digital assets.

Difficult to assign a fair value

It can be difficult to determine the fair value of a digital asset prior to the investment. For example, when buying shares in a company, certain models can be used for assessing the fair value. Digital assets are often different in terms of their capital structure which makes it difficult to apply traditional valuation models. Furthermore, certain digital assets do not represent ownership, but instead confer digital access rights to a service or application. In this case, it can be difficult to assess the value of the purchased digital assets against the value of the service that the digital asset can be used to pay with. This implies the risk of paying more for the digital asset than it might be worth.

High volatility

The market value of digital assets is often volatile. Some of the reasons for the volatility are the small market capitalization compared to traditional capital markets, the risk of sudden regulatory changes, trend-cycles or the performance of the market for traditional investments.

Emerging market

The market for digital assets is still in an emerging and maturing phase. Investment in these markets are often deemed riskier than in long standing and more mature markets.

Derivative of a regulated instrument

Digital assets can also be issued to derive their value from the market value of traditional financial instruments. In this case, the digital assets indirectly benefit from the regulation and protection of the underlying.
However, the digital assets can still be structured to track their value of the underlying either linearly or non-linearly.
For example, a digital asset can represent the value 1:1 of a stock traded on a traditional regulated market, or it can represent an option offering leverage, thus inheriting the risk of the traditional market as well.

Regulation

The legal framework surrounding digital assets is still uncertain in many countries and so far, digital assets have seen to be regulated differently across countries. This non-uniform treatment and new, potential legal measures exposes digital assets and its investors to the risks of non-compliance with law and restricted trade- and transferability which ultimately affect the value of the digital assets and can lead to penalties or fines. For more information on legal and regulatory risks, see section 3.2. below.

Fraud or insider trading

Traditional markets and trading venues are subject to a high degree of regulations that aim to promote a fair and transparent market. As outlined above, the market for digital assets is still emerging and subject to a varying or non-existing regulation. As such, not all market participants offer the safeguards of traditional markets to prevent market abuse (i.e. fraud, market manipulation or insider trading).

Market opening hours

Traditional financial service providers have limited opening hours. For example, the New York Stock Exchange is open from 9:30 to 16:00 (UTC -5) from Monday to Friday and other exchanges have very similar opening hours. Digital asset exchanges are often open around the clock seven days a week. This means that the digital assets are subject to a constant market risk as trading never halts.

Caution

Market risk is a very pronounced risk factor in digital assets. Traditionally hedging becomes more relevant, and the investor must be willing to assume the above listed risks.

2.2 Credit Risk

What is credit risk?

Credit risk is the risk that a party to a transaction may be unable to meet its obligations.

What are the risks?

There are various potential counterparties when trading digital assets. Even an autonomous piece of code can be the direct counterparty to a trade in digital assets. In the following, various counterparties and their associated risks are outlined. This list is not exhaustive.

Issuer risks as credit risk

A form of credit risk is that the issuer of a digital asset cannot deliver the purchased digital asset. As the issuance of digital assets can be done with simple software (or even autonomous) some issuances take place with limited or without any legal supervision.

No redemption

Even if the digital assets are delivered to the investor, there is no guarantee that the digital assets can be redeemed against cash by selling it back to the issuer or to a third party, see also liquidity risk in section 2.3 below.

Traditional issuers

For traditionally issued financial instruments (such as an ETF) which track digital assets (Bitcoin and/or ETH), the counterparty risk shifts from the underlying digital asset itself to the issuer of the financial instrument.

Bank and brokers

For buying and selling digital assets in the secondary market through financial service providers, an individual counterparty assessment is applicable when the service provider acts on a principal basis, meaning the investor trades directly against the service provider.

Smart contract

A smart contract is an interactive agreement based on code. For example, a smart contract can be coded to send out digital asset A (e.g. DAI) if a user sends in digital asset B (e.g. ETH). This way, funds can be exchanged without the need of a middleman/intermediary other than the autonomous smart contract. However, since the smart contract relies solely on the underlying code, the interaction with the smart contract cannot be ensured to be bug-free. For the investor, this means that the counterparty risk is the risk of the underlying code of the smart contract which can be difficult to assess. Furthermore, transactions to the smart contract cannot be reversed or rectified even if proven to be faulty.

Caution

Credit risk is present in digital assets, especially in the form of issuer risk. It must be noted that issuers and the issuance itself is not always subject to investor protection rules.
Issuer risks can be decreased by investing in a traditional financial instrument covering digital assets issued by a regulated entity subject to adequate supervision.

2.3 Liquidity Risk

What is liquidity?

An asset is considered to be liquid when it is possible to easily sell it against cash with no or little impact on the price. To achieve this, the marketplace must have many and highly capitalized buyers.

What is liquidity risk?

Per contra, an asset is illiquid when it is difficult to find buyers and the asset must be sold at a reduced price or cannot be sold at all. The investor is then exposed to liquidity risk.

Trading venues

The market for digital assets is – relative to traditional markets – undercapitalized and has fewer buyers. Furthermore, the trading of digital assets can be done at various venues such as:

- centralized exchanges, or
- decentralized exchanges (autonomous, ownerless, smart contract and internet website-based exchange), or
- peer-to-peer

Caution

These various exchange venues can result in illiquidity thus making the selling of digital assets difficult or even impossible. Illiquidity can also result in rapid price fluctuations.
The risk of illiquidity is more pronounced in the digital assets market than in traditional financial markets. This can make it difficult for the investor to sell or reduce his digital asset exposure.

3. Non-financial Risks

3.1 Technical and operational Risk

What is it?

Technical and operational risks are risks associated with inadequate procedures, technology, or systems.

What are the risks?

The following section outlines risks that should be noted when having digital assets and interacting with a distributed ledger.

Fork

A blockchain fork describes an event which splits a new blockchain from the original one by modifying the source code. Usually a modification or update of the source code is accepted by all participants. When there is a disagreement, the network infrastructure can be divided into two groups using two different blockchains. Digital assets registered on the original blockchain will be credited on both the original and new blockchain.
In the event of a fork, there may be significant price fluctuations resulting in a temporary suspension of trading.

Technological innovations

The functionality of digital assets relies on computing technology. Innovations, particularly in the field of cryptography or quantum computing, may make existing technology obsolete, affecting demand and thus market value.

Storage

Access to the distributed ledger network is through a public and a private key. Without these, access to the network and therefore to the digital asset is impossible. Keys can be stored on various media such as paper wallets or ledgers or in a physical vault.
Theft, loss, destruction, hacking or other reasons for the private key not to be recognizable any more can result in not being able to access the digital assets.

Transactions

Transactions on a distributed ledger network are sent to an address determined by the public key. If a wrong public key is used, it will be impossible to identify the recipient and to reverse the transaction. There may also be delays in the execution of transactions as the transfer of digital assets is subject to verification and other processes involving third parties.

When a transaction is made to an address, the receiving address cannot refuse the transaction. Therefore, the owner of the address has no control over the funds that are sent to the address, nor over their origin. This effectively implies the risks of holding digital assets unwillingly.

Open-source software

Digital assets are based on open-source software that is freely accessible and may be copied, used or modified at any time. There is thus an increased risk of bugs and vulnerabilities, and also deliberately embedded malfunctions. The discontinuation of such open-source software is always possible and might expose digital assets to vulnerabilities, programming errors and threats from fraud, theft and attacks.

Smart contracts

The functionality of an asset, i.e. its creation, transfer, trading etc., depends on the smart contract used. Smart contracts are computer code that interact with a distributed ledger network. The interaction is often very complex and mostly irreversible. The computer code may be faulty or hacked or may be changed by the issuer. The execution of a smart contract depends on the underlying network being powered and available.

Hacking

Access to digital assets requires a private key. Transactions sent to the public key can be deciphered using the private key, which is only known to the recipient. Hackers try to gain access to these keys in order to control the address. For example, keys that have been communicated by email or stored in a text file on an unprotected computer can be read by hackers and used to control the blockchain address. This can lead to a total loss of the digital assets.

Attacks

A decentralized consensus is necessary to validate transactions and the validation requires computing capacity. Therefore, it is possible for a participant with significant computing capacity to effectively centralize the consensus and thus manipulate it. For example, making it possible to verify or process a false transaction for its own benefit at the loss of others. The risk of such a majority attack decreases with the increased computing capacity dedicated to validating.

Due to the mathematical foundation of the crypto technology, there are also various other forms of attacks, like collision attacks, dusting attacks or censorship attacks.

Caution

The technological design of DLT and the applications utilizing it comes with a variety of risks. It is important and advisable to not only consider the financial aspects of an investment in digital assets but also the technological handling of the investment.

3.2 Legal and regulatory Risk

What are legal risks?

Legal and regulatory risk is the risk of uncertain legal treatment or change in current legislation which may materially impact the holder of the affected asset.

What are the risks?

As regulatory framework may change, there is the risk of digital assets or transactions being treated or classified differently.

Varying regulations

Government authorities may within their jurisdiction classify or change existing classifications of digital assets. This could for example result in a digital asset being delisted from an exchange or not being traded by a broker or that rights associated with a digital asset are not recognized by law.

Exercising of rights

Rights associated with a digital asset (for example voting on matters related to the issuer of the digital asset) are not guaranteed to be exercisable if the digital asset is stored with a bank, broker, or custodian.

Current classification approach

In different jurisdictions the classification of digital assets has become a regulatory standard (often called "token classification"). In Switzerland tokens are classified based on the underlying economic function:[3]

Payment tokens:
Payment tokens are tokens which are intended to be used, now or in the future, as a means of payment for acquiring goods or services or as a means of money or value transfer.

Utility tokens:
Utility tokens are tokens which are intended to provide access digitally to an application or service by means of a blockchain-based infrastructure.

Asset tokens:
Asset tokens represent assets such as a debt or equity claim on the issuer. Asset tokens promise, for example, a share in future company earnings or future capital flows. In terms of their economic function, therefore, these tokens are analogous to equities, bonds or derivatives. Tokens which enable physical assets to be traded on the blockchain also fall into this category.

[3] See FINMA ICO Guidelines, Section 3.1.

Impact of token classification

The individual token classifications are not mutually exclusive. In this case the token is called hybrid token and as a result the legal and regulatory requirements need to be applied cumulatively.

Based on the token classification, which due to the lack of internationally recognized classification schemes need to be performed independently by each jurisdiction, the regulatory treatment may differ. This includes that certain asset tokens may only be issued or traded if the necessary licenses are in place.

Tainted assets

Digital assets can usually be traced back to previous addresses and potentially its owner. Digital assets that are traceable to criminal activities may thus be considered tainted. The treatment of tainted digital assets may vary between jurisdictions.

Caution

Clients should be aware that digital assets offer less legal security than fiat money since regulations are constantly developed and evolving. In addition, there is no obligation to accept digital assets as a payment due to the lack of acceptance as a legal tender. If countries prohibit or restrict trading in digital assets, this can mean, in addition to a massive loss in value, that the digital assets can no longer be resold to third parties. Clients should ensure that investing in the given product is compliant with the relevant local regulation.