Bitcoin Suisse AG
Grafenauweg 12
6300 Zug
Switzerland

September 2023

Special Risks of Crypto Assets

Contents

1. About this Brochure

1.1. With this brochure, Bitcoin Suisse AG ("**BTCS**") intends to provide its Clients with an introduction to the risks associated with Crypto Assets. This brochure contains an overview of various financial risks, including market, credit, and liquidity risks, as well as non-financial risks, including technical and operational risks, and legal and regulatory risks.

1.2. This brochure supplements and forms an integral part of the contractual relationship between Clients and BTCS and must be read in conjunction with the General Terms and Conditions of BTCS (the "**GTC**") and any other special agreements between Clients and BTCS, as applicable. BTCS reserves the right to adjust and amend this brochure at any time and to communicate such changes to Clients in accordance with the GTC. Unless otherwise defined herein or the context otherwise requires, all terms beginning with a capital letter shall have the same meaning as in the GTC.

2. General Risk Notice

2.1. This brochure can neither cover all available risks related to Crypto Assets nor provide an exhaustive account of all risks they entail. If available, it is advised to also rely on the information documents provided by issuers, distributors, financial services providers, trading counterparties, and other persons involved in the offering, distribution, trading, and other transactions related to Crypto Assets. Such information documents, including, but not limited to, prospectuses, key information sheets, white papers, factsheets, and other information sheets, contain detailed information on the risks and costs associated with a particular Crypto Asset, or a class of Crypto Assets.

2.2. The brochure "Risks Involved in Trading Financial Instruments" issued by the Swiss Bankers Association (SBA) may provide further information on Crypto Assets.

2.3. This brochure does not take account of Clients' individual financial, legal and tax situations. For comprehensive personal advice on your financial situation, please consult, if necessary, an investment advisor, tax, or legal expert.

2.4. **By trading, transacting, investing in, and/or holding Crypto Assets, Clients acknowledge and accept the risks described in this brochure. Clients understand that the materialization of such risks may result in a total loss of the investment and, potentially, additional losses exceeding the original investment, depending on the type of Crypto Asset and the specifics of the investment activity, if any, and the exposure.**

2.5. Clients who do not understand the information in this brochure should seek advice before making any investment or transaction in Crypto Assets. BTCS is under no obligation to inform the Client of the materialization or the possible materialization of any of the risks described herein or any other risks relating to Crypto Assets.

3. Definitions

3.1. **DLT**. The term "Distributed Ledger Technology" ("DLT") is a collective name for technologies that apply a distributed database architecture. This means that computers, also referred to as "nodes", distributed around the world maintain multiple, identical copies of the database and run a software to align and coordinate the database. For reference, the opposite of DLT would be one central server in a single location owned by one company or person.

Bitcoin Suisse AG
Grafenauweg 12
6300 Zug
Switzerland

3.2. **Blockchain**. Blockchain is a specific type of DLT. It describes the fact that data is recorded in blocks which are chained to each other by using cryptography. A block consists of transactions validated by the nodes in the network. Typically, when a block is produced, the block is "completed" (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 a chain or link between the blocks. New blocks are found and added to the chain by special nodes in the network, also referred to as "miners" or "validators".

3.3. **Permissionless, private and permissioned distributed ledgers**. Distributed ledgers can either be a permissionless (anyone with a node can participate), a private (a company or person builds its own distributed ledger for internal purposes) or a permissioned distributed ledger (possible to participate by invitation and verification of the participant). Permissionless distributed ledgers typically use public blockchains, meaning that all transactions between blockchain addresses are visible to the public. As the market capitalization of Crypto Assets can be attributed primarily to Crypto Assets issued on permissionless and public blockchains, this brochure mainly describes risks associated with such systems.

3.4. **Crypto Assets**. Crypto Assets are digital assets issued in a decentralized or centralized manner and transferred on a blockchain, or another cryptography-based distributed ledger.

4. Market Risks

4.1. **Market risks are risks that an investment or asset may lose its value partially or in whole.**

4.2. **Emerging market**. The market for Crypto Assets is still in an emerging and maturing phase which may be subject to elevated volatility and limited transparency and reliability, execution delays or failures, all of which may potentially result in losses or other adverse effects for clients. Investments in markets for Crypto Assets are often deemed riskier than in long standing and more mature markets. Furthermore, execution venues for Crypto Assets are typically open around the clock, seven days a week, 365 days a year. This means that the Crypto Assets are subject to constant market risks as trading never halts, possibly requiring constant monitoring by market participants.

4.3. **Difficulty to assign a fair value**. It can be difficult to determine the fair value of a Crypto Asset prior to the investment. Crypto Assets are often different from traditional assets in terms of their capital structure and cash flows which makes it difficult to apply traditional valuation models. Crypto Assets may not represent ownership or rights to cash flows, but instead often confer access rights to a blockchain-based service or application. In this case, it can be difficult to assess the value of the purchased Crypto Assets against the value of the service that the Crypto Asset can be used to pay with. This carries the risk of paying more for the Crypto Asset than it may be worth.

4.4. **High volatility**. The market value of Crypto Assets is often volatile. Some of the reasons for the volatility are the small market capitalizations compared to traditional capital markets, the risk of sudden regulatory changes, trend cycles and/or dependencies on the performance of the market for traditional investments.

4.5. **Connection to traditional financial instruments**. The value of Crypto Assets may rely on the market value of traditional financial instruments, such as tokenized stock or stablecoins pegged to a fiat currency. Such Crypto Assets may have the identical or a similar risk profile as the underlying, replicated, or mirrored traditional financial instrument, thus inheriting the market risks of traditional markets.

5. Credit Risks

5.1. **Credit risks are risks that a party to a transaction may be unable to meet its obligations toward its counterparty.**

5.2. **Issuer**. Crypto Assets often have no issuer in the traditional sense. As such, holding most Crypto Assets in self-custody does not carry traditional credit risk. Nonetheless, credit risk may be present in certain Crypto Assets especially in the form of issuer risk. Specifically, the issuer of a Crypto Asset may fail to deliver the assets to the purchaser, which means that the credit risk materializes.

5.3. **Traditional issuer**. For traditionally issued financial instruments, such as an exchange-traded financial product that replicates a basket of Crypto Assets, the counterparty risk may also involve the issuer risk of the respective financial instrument.

Bitcoin Suisse AG
Grafenauweg 12
6300 Zug
Switzerland

5.4. **Counterparty default**. When a client uses a service of a crypto service provider, such as a crypto custodian or execution venue, Crypto Assets may carry the default risk of the respective counterparty. Default risk is the possibility that a counterparty will not be able to fulfill their debt obligations. For example, execution venues may not be able to honor withdrawal or settlement requests from their clients. Furthermore, the occurrences of one or more counterparty defaults may have contagion effects on other crypto services providers and may thus negatively affect the entire market for Crypto Assets, resulting in the materialization of market and liquidity risks.

5.5. **No redemption**. Even if the Crypto Assets are delivered to the purchaser, there is no guarantee that the Crypto Assets can be redeemed against a fiat currency or a traditional financial instrument by exchanging them to the issuer or a third party.

6. Liquidity Risks

6.1. **Liquidity risks are risks that buying or selling an asset against fiat currency may have a price impact on the respective asset. If there is no price impact when buying or selling an asset, the asset holder is not exposed to any or only a low liquidity risk.**

6.2. **Immature market structure**. The markets for Crypto Assets are generally undercapitalized relative to traditional markets, as typically fewer market participants are active in these markets. The trading of Crypto Assets can be done at various types or execution venues, including, but not limited to, centralized exchanges, decentralized software-based platforms, and peer-to-peer marketplaces. The fragmentation of execution venues may lead to illiquidity, which in turn may cause price fluctuations in Crypto Assets, thus making the buying and selling of Crypto Assets difficult or even impossible for the asset holder.

7. Technical and Operational Risks

7.1. **Technical and operational risks are risks associated with the inadequacy or failure of procedures, humans, technology, and systems, or with external events.**

7.2. **Forks**. A blockchain fork describes an event which results in two conflicting versions of the original blockchain. There are many reasons for a fork, such as a change in the protocol code or an unplanned protocol code inconsistency due to a software bug. When there is a disagreement about a protocol upgrade, a blockchain network may split into two groups resulting in at least two different blockchains and networks. Following a fork, the Crypto Assets of the original blockchain will also exist on the new blockchain. In the event of a fork, there may be significant price fluctuations resulting in a temporary suspension of trading, cyber-attacks on the holders of Crypto Assets, or adverse effects on the functionality or convertibility which may result in a full or partial reduction of the value of the Crypto Assets involved.

7.3. **Replay attacks**. The occurrence of forks may lead to replay attacks carried out by third parties. Replay attacks take place when transactions in Crypto Assets on a recently forked blockchain are technically valid on both or multiple blockchains. Therefore, a third party may maliciously replicate a previous transaction made on the legacy blockchain on the new blockchain, resulting in the same number of units being transferred on the new blockchain as well.

7.4. **Loss of private keys**. Access to and use of a blockchain is based on public-key cryptography using a pair of private and public keys. Without the private key, a user cannot access the blockchain and therefore its Crypto Assets. Private keys can be stored on various media, such as on paper, software, or hardware wallets, or held with a crypto custodian. Theft, loss, destruction, hacking, or other reasons that render the private key no longer available or recognizable may result in the permanent loss of the corresponding Crypto Assets.

7.5. **Hacking**. Malicious third parties may use methods and means to gain access to private keys. For example, private keys, seed phrases, or relevant passwords that are communicated by e-mail or stored in a text file on an unprotected computer may be intercepted and read by third parties and used to control the blockchain address. This may lead to a total loss of the Crypto Assets.

Bitcoin Suisse AG
Grafenauweg 12
6300 Zug
Switzerland

7.6. **Hashing and encryption algorithms.** A hashing algorithm is a mathematical function that derives a unique text from input data in a consistent manner. Crypto Assets and their protocols may use non-standard, novel, outdated, or faulty hashing algorithms that may lead to vulnerabilities that affect the value of the Crypto Assets in question. Furthermore, protocols may use encryption algorithms that may prove faulty or outdated, or only provide weak protection against malicious third parties resulting in such algorithms being compromised. These risks may become particularly relevant as quantum computing capabilities increase.

7.7. **Use of incorrect blockchain addresses.** DLT transactions are sent to a blockchain address derived from the public key. If an incorrect address is used, it may be impossible to identify the sender or recipient and to reverse the transaction. Clients who intend to deposit Crypto Assets with a crypto services provider are advised to only use the blockchain addresses communicated to them.

7.8. **No possibility to reject funds**. When a transaction is made to a blockchain address, the owner of the address may not be able to refuse the transaction and thus may not prevent the receipt of Crypto Assets. This effectively implies the risks of receiving and holding Crypto Assets unwillingly.

7.9. **Third party dependency**. Execution and settlement of transactions in Crypto Assets may depend on the specifications of the relevant DLT, including the participation of third parties in the relevant network, such as miners or validators. Delays or failures to execute, process or settle transactions may potentially result in losses or other adverse effects for users of the network, such as waiting times when depositing with or withdrawing Crypto Assets from a crypto services provider.

7.10. **Inability to exercise rights and seize opportunities**. Crypto Assets may confer legal or actual rights and opportunities to their holders. Rights and opportunities may include the use as a means of payment or as a stake in Proof-of-Stake blockchain protocols, or the exercise of governance-related rights with respect to the development of a blockchain protocol. Depending on how and where the Crypto Assets are stored or used, the holder may not be able to exercise such rights or seize such opportunities.

7.11. **Consensus attacks**. A decentralized consensus is required to validate transactions and blocks and secure the blockchain. The validation may require computing power (Proof-of-Work), stake (Proof-of-Stake), or some other form of proof, depending on the applicable consensus mechanism. Therefore, it may be possible for a participant with significant computing power or stake to effectively manipulate the consensus mechanism. Such centralized power may result in various types of attacks, such as double-spending Crypto Assets or censoring transactions of third parties.

7.12. **Weaknesses in smart contracts**. The existence, functionality, and transferability of Crypto Assets may depend on smart contracts deployed on the blockchain. Smart contracts are based on computer code whose operation is triggered by a user or another smart contract. Interactions with smart contracts may often be very complex and mostly irreversible. The computer code may be faulty or hacked or may be changed by the deployer, or someone else, by updating or replacing existing smart contracts. The logic of smart contracts may be exploited by third parties, such as by manipulating off-chain price oracles that feed false data into a smart contract. The use of a smart contract potentially depends on the underlying network being available and not congested.

7.13. **Decentralized Finance (DeFi).** The use of DeFi applications, such as decentralized exchanges or borrowing platforms, may entail special risks, including, but not limited to, risks related to smart contracts, operational security, such as the use of admin keys by the developers, or someone else, to control a DeFi application, dependencies on other components and smart contracts of DeFi, the use of external (off-chain) data through oracles, increased illicit activities, and scalability issues.

7.14. **Weaknesses in open-source software**. Crypto Assets are typically based on open-source software that is freely accessible and may be copied, used, or modified by anyone at any time. While open-source software development may have many advantages, bugs, vulnerabilities and deliberately embedded malfunctions may exist and affect the security of Crypto Assets when holding or transacting in them. The development of open-source software may be discontinued at any time, which may also affect the long-term security of Crypto Assets.

Bitcoin Suisse AG
Grafenauweg 12
6300 Zug
Switzerland

7.15. **Staking lock-up periods**. Depending on the Proof-of-Stake blockchain protocol there may be lock-up periods during which users will not have access to the Crypto Assets they stake. This may result in the temporary illiquidity of such Crypto Assets. Clients of staking services providers may also be affected by lock-up periods when instructing such providers to stake their Crypto Assets.

7.16. **Slashing in staking**. Proof-of-Stake blockchain protocols may embed a "slashing mechanism" to prevent validator misconduct and thus to promote network stability and security. If a validator behaves dishonestly or otherwise violates the protocol rules, it may risk losing the staking rewards and/or a certain amount of the Crypto Assets staked in the protocol, potentially leading to a total loss of the Crypto Assets. Clients of staking services providers may also be affected by slashing when instructing such providers to stake their Crypto Assets.

7.17. **Data protection**. Users of permissionless blockchains should be aware that any transfer of Crypto Assets will be recorded in a public distributed transaction register and can therefore be viewed by third parties not involved in the transfer. Such information may be processed, exploited, or misused by third parties. It may be possible for third parties to reconstruct a relationship between a blockchain address and the identity of its owner.

8. Legal and Regulatory Risks

8.1. **Legal and regulatory risks are risks that uncertain legal treatment or change in current legislation may materially affect an investment or asset.**

8.2. **Legal uncertainties**. The legal and regulatory framework surrounding Crypto Assets may still be uncertain in many countries, and Crypto Assets may be subject to different legal and regulatory rules across those countries. In particular, it may be unclear under applicable laws who is entitled to what rights in relation to Crypto Assets, including ownership rights. The inconsistent treatment and potential legal measures expose holders of Crypto Assets as well as crypto services providers to the risks of non-compliance with applicable laws and/or non-enforceability of rights under such laws, which may ultimately affect the value of the Crypto Asset.

8.3. **No legal tender or inability to redeem**. Users should be aware that Crypto Assets, in particular payment tokens, may offer less legal certainty than traditional fiat currencies. There is typically no obligation to accept Crypto Assets as a means of payment, as they are not legal tender, and as they are not issued by a central bank or government. In addition, stablecoins issued by private market participants may not be redeemable in full or at all due to insufficient or illiquid backing.

8.4. **Changing legislation and supervisory practice**. The legal and regulatory landscape regarding Crypto Assets in and outside of Switzerland is constantly evolving and changing. Government authorities may within their jurisdiction classify or change existing classifications of Crypto Assets. This may result in a Crypto Asset being delisted from an execution venue or no longer being offered for trading by a crypto services provider, or in rights associated with Crypto Assets no longer being recognized by law. If countries prohibit or restrict trading and/or holding Crypto Assets, this may result in the inability to sell and/or hold such Crypto Assets, ultimately affecting their value.

8.5. **Classification**. Depending on the applicable laws and regulations, Crypto Assets may be classified differently and result in different rules being applicable to them, to holders of such Crypto Assets, or to services providers that offer them to their clients. Crypto service providers may classify or periodically reclassify Crypto Assets depending on the specific circumstances. This may result in them offering such Crypto Assets to their clients on a limited basis or not at all. This may be the case, in particular, if new circumstances cause the provider to reclassify a payment token as an asset token.

8.6. **Tokenization**. Where Crypto Assets are intended to constitute, embed, or represent legal rights and/or obligations, the legal effectiveness of such construct may be subject to differing rules in the potentially relevant jurisdictions, including the jurisdiction of the issuer or the holder of the relevant Crypto Asset. There is a risk that tokenization of the underlying rights and/or obligations and/or the transfer of such rights and/or obligations by transfer of a Crypto Asset may not be legally effective and that, consequently, the Crypto Assets may not include the expected rights and/or obligations, potentially resulting in a full or partial loss of value of the respective Crypto Assets.

Bitcoin Suisse AG
Grafenauweg 12
6300 Zug
Switzerland

8.7. **Bankruptcy treatment.** The treatment of Crypto Assets in the event of bankruptcy or a similar event is subject to special provisions under Swiss law. While recent legislation has improved legal certainty, it is still open how the new provisions will be applied in the event of bankruptcy of a crypto custodian in practice.

8.8. **Risk of abusive market conduct.** Traditional markets and trading venues are subject to a high degree of regulations that aim to promote fair and transparent markets. The market for Crypto Assets is still emerging and subject to a varying degree of regulation. As such, not all market participants observe standards that are comparable to the market conduct rules of traditional markets, which intend to prevent fraud, market manipulation and insider trading.

8.9. **Risk of fraudulent and other malicious behavior**. The market for Crypto Assets has shown to attract fraudulent and malicious actors that may target market participants in various ways, such as hacking their IT infrastructure, including wallet software, tricking them into revealing confidential information, misusing their credentials and identities, or pretending to do something that is not real or plausible.

8.10. **Poor transparency and investor protection.** Crypto Assets may not be listed on or admitted to trading at a regulated trading venue, and their issuers may not be required to disclose information relevant to investment or other decisions. Therefore, holders of Crypto Assets may not benefit from the same rules and regulations that apply to listed companies and/or in traditional markets for the purpose of protecting investors.

8.11. **Legal obligations**. Changing legal and regulatory frameworks may result in Crypto Assets or transactions being treated or classified differently by authorities in any jurisdiction at any given time. Depending on their domicile, users may have different legal obligations associated with holding, purchasing, or selling Crypto Assets or using certain services with respect to Crypto Assets. Such obligations may include legal and regulatory obligations, tax obligations or other requirements. Failure to comply may result in legal actions and sanctions, including criminal sanctions, or otherwise affect holders of Crypto Assets.

8.12. **Tainted assets**. Transactions in Crypto Assets on public blockchains can be traced back to previous blockchain addresses and through forensic investigations potentially to their owners. Crypto Assets that are attributable to criminal activities may thus be considered tainted by crypto services providers and/or authorities. As a result, Crypto Assets are at risk of being seized or at least made unusable by courts, which may affect the value of the relevant Crypto Assets.

8.13. **Supervisory measures:** Crypto Assets, their issuers or developers, users, execution venues, crypto services providers, or other parties involved in the industry may be subject to regulatory investigations, injunctions or other measures which may potentially result in a full or partial loss of the value of Crypto Assets or impact the ability to offer them to clients or otherwise affect holders of such assets. Such measures may also prevent, restrict, or prohibit users from trading and/or holding Crypto Assets.