
Risk Disclosure

You should not trade or invest in Virtual Assets unless you fully understand the highly speculative nature, complexity, and risk inherent in the transactions you enter into, and your exposure to financial loss. Only persons with adequate understanding of the economic, legal, and other risks associated with Virtual Assets, and who are willing to assume such risks, should trade in Virtual Assets.

We set out below the risks of trading Virtual Assets and of the use of the services provided by Matrix Limited (“**Matrix**”). Note that there may be additional risks that we have not foreseen or identified as part of this risk disclosure statement. You should carefully assess whether your financial situation and risk tolerance is suitable for trading in Virtual Assets. Matrix does not provide trade recommendations, investment advice or financial advisory services.

The risks described below may result in the loss of Virtual Assets, a decrease in or loss of all value for Virtual Assets, an inability to access or transfer Virtual Assets, an inability to trade Virtual Assets, an inability to receive financial benefits available to other Virtual Asset holders, and other financial losses to you.

I. General risks associated with Virtual Assets

- 1) **Total loss** - A Virtual Asset may lose all of its value, and subsequently you may lose any fund invested in such Virtual Asset and losses may occur over a short period of time.
- 2) **Not a legal tender or backed by a government** - Virtual Assets are not a legal tender and are not backed by any government.
- 3) **Complexity** - The features, functions, characteristics, operation, use and other properties of any Virtual Asset and the software, networks, protocols, systems, and other technology (including, if applicable, any blockchain) used to administer, create, issue, transfer, cancel, use or transact in any Virtual Asset may be complex, technical or difficult to understand or evaluate.
- 4) **Valuation and market/price** - The price of Virtual Assets traded on an exchange is derived based on the market data and price information on the exchange. Such market data and price information may be different from the information available on other exchanges given the fact that Virtual Assets can be traded on other exchange platforms. Prices can and do fluctuate at any given time. Due to such price fluctuations, the value of your investment in Virtual Assets may decrease at any given moment. Virtual Assets may be subject to large swings in value and may even become worthless. Trading activity in a particular Virtual Asset traded on another exchange could affect the price of that Virtual Asset on Matrix’s online trading platform.
- 5) **Volatility** - The price of Virtual Assets can be subject to large fluctuations (whether in a Virtual Asset/fiat pairing or Virtual Asset/Virtual Asset pairing). The price of a Virtual Asset can be volatile, unpredictable, and inconsistent. Sudden shifts in prices are possible at any given moment and could result in significant loss.
- 6) **Liquidity** - Markets for Virtual Assets can at times become “illiquid,” which means there can be a scarcity of persons who are willing to trade at any one time. Thinly traded or illiquid markets have potential increased risk of loss because Virtual Assets can experience high volatility of prices and in such markets market participants may find it impossible to liquidate market positions except at very unfavorable prices. There is no guarantee that the markets for any Virtual Asset will be liquid or permit you to establish or liquidate Virtual Assets positions when you want, or at favorable prices.
- 7) **Irrational market forces** - Virtual Assets are probably susceptible to irrational loss of confidence or market forces (e.g. as a result of any misleading statements or rumors), which could cause a collapse in the demand relative to supply without a reason anchored in reality. Many Virtual Assets have no underlying value other than the trust the holder of such Virtual Assets places in them. References to "market

capitalisation" in connection to Virtual Assets should not be confused with the intrinsic value of other assets, such as equities, which are valued and whose market capitalisation depends on the intrinsic value of the legal entity which they represent a share in i.e. the value of the underlying assets and liabilities of a corporation.

- 8) **Financial crime risk** - Virtual Assets provide a higher degree of anonymity for their holders and makes it more difficult to trace them compared to conventional assets, which can lead to an increased risk of Virtual Assets being used for, or being connected to, financial crime (which includes (i) fraud or dishonesty; (ii) money laundering such as the handling of proceeds of crime; (iii) the financing of terrorism; or (iv) dealing with sanctioned persons or breaching economic sanctions).
- 9) **Cyber-attack risks** - The non-tangible nature of Virtual Assets and their heavy reliance on technology may make them subject to an increased risk of cyber-attack and theft. However, Matrix does have an insurance policy for theft of Virtual Assets held in Cold Storage which should help mitigate the risk for Matrix's clients. Virtual Assets are susceptible to specific types of cyber-attacks as a result of their network architecture. For example, Bitcoin and Ethereum rely on a Proof-of-Work consensus mechanism, in which a distributed network of computers (known as miners) complete complex mathematical problems in order to validate and record transactions. Theoretically, a malicious actor could gain control of >50% of the network computing power (known as a 51% attack) to rewrite transactions or create fake ones in order to steal assets from exchanges and other service providers. Polkadot relies on a Proof of Stake consensus mechanism, in a which a set number of node operators (known as validators) post collateral in order to validate and record transactions. A validator will lose some or all of its collateral if it behaves maliciously or carelessly. Theoretically, a validator or group of validators could post enough collateral to control the validation and recording of transactions. While these kinds of attacks are theoretically possible, they require significant capital to be carried out successfully.
- 10) **Technology risks** - Trust and confidence may collapse in a Virtual Asset such as Bitcoin because of, but not limited to, unexpected changes imposed by the software developers or others, changes introduced by the relevant authority or regulator, the creation of superior competing alternative Virtual Assets, or a deflationary or inflationary spiral. Confidence may also collapse because of technical problems: if the anonymity of the system is compromised, if money is lost or stolen, or if hackers or governments are able to prevent any transactions from settling. There may be no mechanism for the recovery of lost or stolen Virtual Assets. Any Virtual Asset or technology may change or otherwise cease to operate as expected due to a change made to the underlying technology, a change made using features or functions built into the underlying technology or a change resulting from an attack. These changes may include, without limitation, a "fork" or "rollback" of a Virtual Asset or blockchain. Finally, due to their nature, technological difficulties experienced by Matrix may prevent access or use of Virtual Assets.
- 11) **Irreversible transactions** - Each Virtual Asset has its unique deposit address. If an exchange user accidentally deposits any other Virtual Assets into the address, those Virtual Assets would be lost forever and cannot be recovered. Likewise, if an exchange user accidentally types in a wrong withdrawal address, once the withdrawal request is processed and the transaction is completed from the Exchange's end (once the Virtual Asset leaves Matrix's wallet system), the transaction is irreversible, and the withdrawn amount cannot be retrieved by the exchange user. Finally, and for the same reason, Virtual Assets which are stolen as a result of a cyber-attack, as well as Virtual Assets where the private keys are lost, destroyed or stolen, may not be recoverable.
- 12) **Acceptance as payment** - There is no assurance that a counterparty who accepts a Virtual Asset as payment today will continue to do so in the future. Changes to laws and regulations might prevent a counterparty from accepting a Virtual Asset as payment. Virtual Assets not being a "legal tender", a counterparty could refuse to accept them as a means of payment.
- 13) **No central bank or other official support** - There is no central bank that can take corrective measures to

protect the value of Virtual Assets in a crisis. Virtual Assets are only backed by technology and mutual trust, and therefore rely heavily on the technology and economic model its community and developers have built. Any changes in the core logics of these could result in a collapse of its price and value.

- 14) Unregulated Virtual Asset-related activity** Fiat Pairs listed on Matrix lie outside the regulatory remit of the Financial Services Regulatory Authority (“FSRA”) (e.g. holding Virtual Assets with external wallet providers, trading of fiat pairs such as USDC/USD) and may be subject to no or limited regulation, and therefore may pose a higher degree of risk. While the trading of fiat pairs is not subject to FSRA oversight for market abuse purposes, it will still be subject to fair and orderly trading requirements as well as other checks and controls required by Matrix.
- 15) Regulatory risk** - Regulatory changes or actions by the FSRA, or any other regulator or relevant authority, may adversely affect the access to, use, transfer, exchange, or value of Virtual Assets.
- 16) Tax risk** - Virtual Assets gains are typically subject to tax, depending on the client’s country of residence, and may impact a client’s tax footprint or optimization. If you have any further tax concerns pertaining to Virtual Assets you are best advised to visit the relevant country’s tax website or consult your own financial, investment, tax, or legal adviser.

II. Risks associated with Matrix products and services

- 1) Trade execution risk** - Matrix may perform additional reviews or monitoring of a client’s onboarding or any Virtual Asset trade and transaction request which might require, among other things, requesting additional documentation during such review or monitoring. This additional review or monitoring, which may be required for compliance reasons, may delay trading, and therefore could potentially cause a client to miss out on a trade opportunity or expected profit.
- 2) Internet trading risks** - There are risks associated with Matrix’s technology service providers which enable its clients to trade on its exchange. Although Matrix carefully chooses its providers and the solutions it uses, Matrix’s clients would still be exposed to risks which include, but are not limited to, the failure of hardware, software and hacking through internet connection. Clients may experience communication failures, disruptions, errors, distortions, or delays when trading due to network failure from the client’s end, which might result in losses.
- 3) Risks of cyber-attack**

Website Phishing Risk

Attackers may host a similar website which has a similar domain name as the Matrix website. By sending phishing emails or chat messages, attackers may induce clients to access the phishing website where they would input their password or disclose other sensitive information, which could then be used by the attackers.

Official Account Phishing Risk

Attackers may create accounts with the same nickname and avatar as Matrix employees on websites, social media pages or chat rooms. With these fake accounts, attackers may induce clients to disclose their passwords or other sensitive information.

"Remote Hacking" Risk

Clients can expose their computer or mobile device to remote hacking by unconsciously downloading viruses from the internet or other connecting devices. Hackers can then access and control a client’s device without the client being aware. In this case, a hacker might login to and operate a client’s trading account. If a hacker has obtained enough information for him to pass all security measures on the Matrix online trading platform, and the system is tricked into considering the attacker as the legitimate client, the attacker would be able to transfer all funds or Virtual Assets in the client’s account to other addresses.

-
- 4) **Weak User Password/"Brute force" attack risk** - Users sometimes use weak passwords to protect their Exchange accounts. Attackers may attempt to login to the Matrix online trading platform by attempting to guess a client's password through trial and error, by enumerating weak or common passwords, or by using username password combinations leaked from other websites.
 - 5) **"Hard Forking" risk** - A "hard fork" results in a Virtual Asset forked from the original one. Accepting the original Virtual Asset does not mean Matrix automatically accepts any new Virtual Asset that is forked from the original accepted one. In such case, clients will not be able to trade the forked Virtual Asset and need to withdraw it to other addresses for further action. During this time the price of the forked Virtual Asset might decrease.
 - 6) **Regulatory risk** - Matrix may be subject to supervisory or enforcement action by the FSRA which may result in suspension of trading on the Matrix online trading platform or in clients being unable to have control or access over their Virtual Assets for a period of time. This could eventually impact the value of Virtual Assets.

7) **Risks associated with Block Trades**

Block Trades ("**Block Trades**") on Matrix' exchange are trades in Virtual Assets that are above a certain minimum volume, and which are negotiated outside the exchange between certain eligible users and intermediaries (Liquidity Providers who are not subject to pre-funding requirements), and are subsequently notified to exchange users.

Settlement risk

Block Trades may pose some risks of settlement failure which are mitigated by Matrix's establishment of the Default Risk Guarantee which serves to honor any failed Block Trade resulting from a Liquidity Provider failing to settle a Block Trade.

Volatility risk

Although Block Trades are conducted with specialized Liquidity Providers who would normally initiate such large trades carefully so as not to trigger a volatile rise or fall in the price of a Virtual Asset (such as splitting a large "Iceberg Order" into smaller trades) or create a misleading impression as to the trading of a Virtual Asset, there is always a risk that such Block Trades might affect the prices of the Virtual Asset being traded by causing panic trading or causing traders to potentially bid up the Virtual Asset. When this is done on purpose, it may amount to market abuse.

Liquidity Provider's loss risk

Liquidity Providers who initiate Block Trades usually do so with the expectation of getting a price discount on a Virtual Asset's exchange-quoted price. In certain circumstances, the discount margin is so low that Liquidity Providers risk losing money when they later sell the Virtual Assets they acquired through a Block Trade.

Insider dealing risk

Parties to a Block Trade are required to keep the details of a Block Trade confidential, in the same way they would for insider information, since these can potentially affect the price of a Virtual Asset once disclosed to the public. However, the risk of such details leaking cannot be fully mitigated, causing persons holding such information to trade in the relevant Virtual Asset on the basis of confidential Block Trade information which is not available to the public.

Market abuse risk

A scenario of market abuse which can lead to the volatility of a Virtual Asset is where the ultimate beneficial owner on both sides of a Block Trade is the same, and the Block Trade is entered into to generate a false impression of liquidity or trading activity in a particular Virtual Asset or to impact its pricing.

Although Matrix carries on strict customer due diligence on all exchange users including those eligible to participate in Block Trades and on the Liquidity Providers, the risk of common ultimate beneficial ownership is effectively occulted or hidden cannot be fully mitigated.

III. Risks associated with specific types of Virtual Assets

While Matrix endeavors to assess, approve and only list Virtual Assets that comply with its stringent assessment criteria, there may be risks which specific Virtual Assets have that Clients should be aware of when trading them. This list is not exhaustive and may change as the technology evolves.

a) Virtual Assets:

- 1) **Bitcoin (BTC)** – Bitcoin, created in 2009, is considered by many as the original, most popular, and widely traded cryptocurrency. However, its utility has not yet been fully defined. It was originally designed as a peer-to-peer payment system. But slow transactions times, high transaction costs and high energy consumption have limited adoption for this purpose. It is sometimes utilized as a non-sovereign store of value (“digital gold”) or as a hedge against inflation, but these use cases are not yet fully developed. . The Bitcoin network seldom implements upgrades or new features, which may limit the scalability of the network over time. Clients should also be aware that Satoshi Nakamoto, which is the pseudonym used to refer to the individual or group of individuals who created BTC, holds a substantial proportion of BTC’s total supply, and if these holdings were to be liquidated on the open market, could increase the volatility of BTC prices significantly.
- 2) **Ethereum (ETH)** – Ethereum, created in 2013, is a decentralized, blockchain that also features smart contract functionality which when deployed, runs automatically to facilitate transactions or exchanges of assets of value. In relying on a Proof of Work consensus mechanism, Ethereum prioritizes network security and transaction finality over throughput. As a result, the Ethereum network suffers from congestion and/or high transaction fees at times. While this does not put assets at risk, it may lead to delays or higher than normal costs in completing transfers and transactions. From time to time, Ethereum upgrades the underlying blockchain software through what is known as a non-contentious hard fork. Technology risks may increase during an upgrade as a result of a bug or if a significant number of network participants do not adopt the latest version of the software. Also, Ethereum plans to migrate to a Proof of Stake consensus mechanism, which is designed to maintain security while increasing throughput. The migration may increase technology risks or volatility of prices. Smart contracts are self-operating, tamper proof and designed to execute specific actions once certain conditions are met. However, this also means that any human error or exploitable bug in the smart contract code cannot be reversed once executed.
- 3) **Litecoin (LTC)** – Litecoin, created in 2011, has a long track record, enjoys strong network effects and high liquidity due to its close ties with BTC, and positions itself as a faster and cheaper alternative to BTC. However, its use case remains limited as it cannot match the Store of Value properties of BTC, nor the speed and speed of stablecoins as a medium of exchange. Development of the LTC project has also stagnated in recent times.
- 4) **Bitcoin Cash (BCH)** – Bitcoin Cash arose out of a hard fork on BTC in 2017 due to the potential problems that BTC faced in terms of network scalability, rising transaction fees, and the inability to conduct micro transactions. However, the larger block size of the BCH network is less secure and more centralized than the BTC network. While BCH is the largest and most successful fork of BTC, the success of BCH is highly dependent on certain stakeholders who hold a large proportion of the BCH supply and thus possess great influence over the BCH project.
- 5) **Ripple (XRP)** – Ripple, established since 2012, is similarly characterized by a relatively high concentration of shares/tokens allocated to certain groups of stakeholders such as the founders. For example, Ripple directly holds about 6% of the total supply of XRPs, and this amount is not considered by Ripple as part of

the circulating supply. Ripple also holds in escrow accounts a substantial proportion of the total supply of XRP which is being released back to Ripple at a rate of 1 billion XRP per month to manage the supply predictability of XRP. The issue of higher concentration of shares may mean that a project may suddenly become controlled by a particular group of stakeholders. **XRP has also been subjected to regulatory scrutiny in the US, and the outcome of these investigations may have an impact on its liquidity, volatility, and its performance.** Deposits of XRP also requires the submission of TAG by the Client as a proof of deposit, without which there may be difficulty for Matrix to ascertain the true ownership of the assets that are deposited into the system.

- 6) **Stellar (XLM)** – Stellar was established in 2014 and faces a similar issue of high concentration whereby the Stellar Foundation holds a large proportion of the total supply of XLMs. This creates a high centralization risk for the project. **The current regulatory scrutiny of XRP in the US creates a cause for concern for the regulatory future of XLM.** Deposits of XLM also requires the submission of Reference / Memo IDs by the Client as a proof of deposit, without which there may be difficulty for Matrix to ascertain the true ownership of the assets that are deposited into the system.

b) Stablecoins:

In addition to all risks mentioned above, Matrix would like to also highlight the additional risks that are related to Stablecoins. It should be noted that Stablecoins when paired with Fiat Currency, they will be treated by Matrix as Fiat-Fiat Pairs as defined in Matrix's Market Rulebook.

- 1) **USD Coin (USDC)** – USDC was launched in 2018 and is issued by the Centre Consortium, with its current members consisting of Circle Financial and Coinbase. USDC is designed to be pegged to the US Dollar and collateralized with 1 USD in reserve for every 1 USDC issued. However, it must be noted that USDC is not subject to deposit insurance protection and also not regulated, and the presence of that USD collateral does not mean that any USDC trade is guaranteed. Beginning in 2020, Centre made several changes to improve the security and transparency of USDC, including moving from a fractional reserve to a full reserve, and providing monthly publicly available financial reports on assets held in reserve. However, USDC falls outside of current banking regulations, so its reports, and disclosures are voluntary. There is a possibility that the assets held in reserve are not what is reported, or that sufficient USD may not be available for redemption during times of extremely high demand. There have been occasions when the price of USDC has gone above and below USD \$1 during times of high market volatility. USDC is also supported by multiple blockchain protocols. Withdrawing the same Virtual Asset, on different protocols, can have different impacts on lag times and withdrawal costs, which may affect the final performance and results for the Client.