Risk Disclosure

Bitpanda Broker UK Ltd

Version 1.1.0, Dated 21 November 2025

Bitpanda places the utmost importance on protecting customers and customer assets through the implementation of robust risk management practices. Despite this, the use of the Bitpanda Platform, the making of Transactions, and investing in Crypto-Assets generally, carry significant risks, and a non-exhaustive list of these risks is set out in this Risk Disclosure. You must carefully assess whether investing in Crypto-Assets aligns with your risk tolerance, investment objectives, financial situation, and personal circumstances and you should only open an Account and conduct Transactions with Bitpanda if you understand and accept all of the risks. This Risk Disclosure should be read in conjunction with the User Agreement and the Product Terms, and your attention is drawn particularly to the E-Token Terms.

Don't invest unless you're prepared to lose all the money you invest. This is a high-risk investment and you should not expect to be protected if something goes wrong. Take 2 mins to learn more.

Bitpanda is registered with the Financial Conduct Authority as a cryptoasset business under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. This registration is for the purposes of anti-money laundering (AML) and countering the financing of terrorism (CFT) supervision only. The Financial Ombudsman Service or the Financial Services Compensation Scheme do not apply to the cryptoasset services carried on by Bitpanda.

Part A of this Risk Disclosure (*Class-specific Crypto-Asset Risk Warnings*) groups Crypto-Assets (which are Supported Assets) into categories based on their design and use and sets out some indicative risks applicable to each such category. Part B of this Risk Disclosure (*General Risks of Investment*) sets out some broad, indicative risks that are likely applicable to most Crypto-Assets.

This document is informational only. It is not intended to be investment, legal, tax, or accounting advice, and it is not tailored to your specific needs or circumstances. Before engaging in any Transactions with Bitpanda, you must conduct your own due diligence and, if you are in any doubt, you should obtain independent professional advice.

Capitalised expressions used throughout this Risk Disclosure are defined terms and have a certain meaning, as set out in the User Agreement or the Product Terms.

1 *Category A - Layer-1 Native Tokens (Protocol Tokens)*

1.1 Category A1 - Payments-focused Layer-1s

Description

1.1.1 These assets function as the native currency of a Layer-1 blockchain. They were created primarily to facilitate the transfer of value across a decentralised network without the need for intermediaries such as banks or payment processors. Users typically hold these assets to store value outside of the traditional financial system, hedge against inflation, or make peer-to-peer payments.

Risks

1.1.2 Volatility and Valuation Models. The value of these assets is not derived from traditional financial metrics such as revenue, dividends, cash flow, or interest rates. Unlike equities or bonds, there is no underlying balance sheet or earnings report to anchor the valuation. Instead, value depends heavily on network adoption, security hashrate, public perception, and speculative supply and demand dynamics. Consequently, prices can be extremely volatile and may react sharply to news cycles, macroeconomic shifts, regulatory announcements, or changes in investor sentiment. It is common for these assets to experience significant percentage fluctuations within a single trading day.

1.1.3 Consensus Mechanism Risks. Many payments-focused blockchains utilise a Proof-of-Work (PoW) consensus mechanism. While robust, these networks are susceptible to a '51% attack'. This occurs if a single malicious actor or a colluding group of miners gains control of more than half of the network's mining power. If successful, the attacker could disrupt the network, prevent new transactions from gaining confirmations, reverse transactions completed while they were in control, and double-spend tokens. Smaller PoW networks face a significantly higher probability of such attacks.

1.1.4 Scaling and Transaction Costs. These networks often prioritise security and decentralisation over transaction throughput. During periods of high global demand, the network's waiting area for unconfirmed transactions (mempool) may become congested. This results in a competitive fee market where users must pay increasingly higher fees to have their transactions prioritised by miners. This congestion can lead to significant delays in transaction processing times and a sharp increase in transaction fees. Users may find it prohibitively expensive or slow to move assets when they need them most, particularly during periods of market panic.

1.1.5 Environmental Impact and Regulatory Scrutiny. PoW networks consume vast amounts of electrical energy to secure the ledger. This high energy

consumption has led to criticism from environmental groups and policymakers. There is a tangible risk of regulatory crackdowns, carbon taxes, or outright bans on mining operations in various jurisdictions. Such regulatory interventions could destabilise the network by reducing the security hashrate or limiting the asset's integration with the traditional financial system and ESG-focused institutional investors.

1.1.6 Limited Upgradability. Due to their decentralised nature and reliance on broad consensus among thousands of independent node operators for protocol changes, these networks can be slow to upgrade. This rigidity may prevent the protocol from adapting to new technical threats or implementing desirable features found in newer, more agile blockchains. This could lead to a gradual loss of market share and value over time as users migrate to more technologically advanced alternatives.

1.1.7 Finality Risk. Transactions on PoW blockchains are probabilistic rather than deterministic. While a transaction may appear confirmed after being included in a block, there is always a theoretical risk of a 'chain reorganisation' where a competing chain with more accumulated proof-of-work becomes the definitive chain. This event could result in previously confirmed transactions being reversed or erased from the ledger.

1.2 **Category A2 - Smart Contract Layer-1s**

Description

1.2.1 These tokens are the native assets for programmable blockchains. Unlike payments-focused chains, these platforms act as 'world computers' that host decentralised applications (dApps), smart contracts, and other digital assets. The native token is used to pay for computation fees, known as 'gas', and to secure the network via staking. Users hold these tokens to interact with the ecosystem of applications, earn staking yields, or speculate on the growth of the platform's digital economy.

Risks

1.2.2 Gas fee volatility. The cost to transact on these networks is driven by the demand for block space and computational resources. During popular token launches, NFT mints, or periods of high network activity, gas fees can spike to extreme levels. The cost of the transaction fee may exceed the value of the assets you wish to move, and this effectively renders small balances illiquid during peak times.

1.2.3 Smart contract vulnerabilities. These platforms support complex programming, and this increases the 'attack surface' for hackers. While the Layer-1 blockchain consensus layer itself may be secure, the applications built on top of it often contain coding errors, logic bugs, or economic exploits. If you interact with these applications, you may lose your funds due to hacks, exploits, or unintended code execution.

1.2.4 Validator and staking risks. Most smart contract platforms use Proof-of-Stake (PoS) mechanisms. This requires network validators to lock up capital to secure the chain. If a validator behaves maliciously or suffers from technical downtime, the protocol may confiscate a portion of their staked funds. This penalty is known as 'slashing'. If you delegate your tokens to a validator that gets slashed, you may lose a portion of your investment principal.

1.2.5 Centralisation and governance. Some smart contract blockchains rely on a small number of validators or high hardware requirements to process transactions quickly. This creates a risk of centralisation where a few large entities could collude to censor transactions or halt the chain. Additionally, the governance of these protocols often favours large token holders (known as 'whales') or early investors. This means your ability as a retail investor to influence the direction of the platform or vote on critical protocol upgrades may be negligible.

1.3 Category A3 - Interoperability/IBC/Parachain Layer-1

Description

1.3.1 Tokens in this category belong to networks designed to connect distinct blockchains. They aim to create an 'internet of blockchains' where disparate networks can communicate and exchange data. The native token is typically utilised for network security, governance, and the facilitation of connections between different chains, which are often referred to as 'parachains' or 'zones'.

Risks

1.3.2 Ecosystem Dependency. The value of these tokens is not derived from a single application but from the collective success of the connected ecosystem. If the projects building on the network fail to gain traction, or if developers migrate to a competitor ecosystem, the value of the interoperability token may decline significantly. The network effect is the primary driver of value, and losing it can be fatal.

1.3.3 Bridge and Relay Risks. The core function of these networks is to bridge assets and data between chains. Cross-chain bridges are technically complex and have historically been prime targets for hackers due to the large liquidity pools they lock. A vulnerability in the central relay chain, the messaging protocol, or the bridge smart contracts could lead to a catastrophic failure across the entire connected network, resulting in the loss of bridged assets.

1.3.4 Inflationary Tokenomics. To incentivise security and connectivity, these protocols often issue high rewards to stakers to attract capital. This results in a high structural inflation rate for the token supply. If the demand for the token does not outpace the new supply entering the market from staking rewards, the price of the token may suffer chronic downward pressure over time.

1.3.5 Complexity of Security Models. These networks often employ 'shared security' or 'interchain security' models. These models are highly complex and largely untested at scale over long periods. A failure in the economic design of the shared security model could cascade failures across multiple connected blockchains simultaneously, and this could lead to a systemic collapse of the ecosystem.

2 *Category B - Layer-2 / Rollups / Appchains*

Description

2.1 Layer-2 networks, or 'rollups', are protocols built on top of a Layer-1 blockchain such as Ethereum. They are designed to process transactions off the main chain to increase speed and reduce costs while inheriting the security guarantees of the Layer-1. Users utilise Layer-2s to access decentralised finance (DeFi) and gaming applications with lower fees. Appchains are application-specific blockchains that may function similarly or as standalone chains with specific bridges.

Risks

2.2 Dependency on Layer-1. Layer-2 networks are entirely dependent on their underlying Layer-1 for finality and security. If the Layer-1 network suffers an outage, a reorganisation, or a censorship attack, the Layer-2 network will be directly affected. The Layer-2 cannot exist or secure funds without the liveness and security of the Layer-1.

2.3 Sequencer Centralisation. Many Layer-2s currently rely on a single centralised 'sequencer' to order and process transactions. This sequencer is often operated by the project development team and creates a single point of failure. If the sequencer goes offline, the network may halt and prevent you from transacting. If the operator acts maliciously, they could potentially censor your transactions or exploit the order of trades for profit (MEV). While many Layer-2s plan to decentralise their sequencers, this remains a future roadmap item rather than a current reality for many.

2.4 Bridge Security and Exit Timelines. To use a Layer-2, you must 'bridge' assets from the Layer-1. The smart contracts that hold these bridged assets are frequent targets for exploits. Additionally, moving funds back from a Layer-2 to the Layer-1 can be subject to long waiting periods. For 'optimistic rollups', this withdrawal period can last roughly seven days to allow for fraud proofs to be challenged. You may be unable to access your funds on the main chain during this time unless you use third-party liquidity providers, which introduce their own risks and fees.

2.5 Upgradeability and Key Controls. Many Layer-2 networks are still in an experimental phase and developers often retain 'admin keys' or 'multisig controls' that allow them to upgrade the smart contracts instantly. While this allows for quick bug fixes, it also means the team could theoretically alter the protocol in a way that compromises user funds without community consent or prior warning.

2.6 Data Availability Risks. Layer-2s must post transaction data to the Layer-1 to ensure security and state reconstruction. If the Layer-2 fails to post this data correctly, or if the data becomes unavailable due to technical failures, users may be unable to reconstruct the state of the Layer-2 and could lose access to their funds permanently.

3 Category C - Stablecoins

Description

3.1 Stablecoins are cryptoassets where the value is pegged to an underlying asset, such as a fiat currency, and reserves held in the pegged asset are used to maintain the stability of the stablecoin's value. They aim to maintain a 1:1 value with a specific fiat currency, such as the US Dollar, Euro, or Pound Sterling. They are widely used as a unit of account and a medium of exchange within the crypto ecosystem to preserve purchasing power during market downturns.

Risks

3.2 De-pegging Risk. The primary risk is that the token loses its 1:1 peg to the underlying fiat currency. This means the market price drops below the target value, such as trading at $0.90 instead of $1.00. This can happen if the market loses confidence in the issuer's solvency, if the issuer faces legal action, or if the mechanisms maintaining the peg fail.

3.3 Reserve Transparency and Quality. Stablecoin issuers publish reports on their reserves, but these are often 'attestations' rather than full, independent financial audits. There is a risk that the reserves are not fully backed 1:1, or that the reserves consist of assets that are illiquid, such as commercial paper or long-term bonds, rather than cash. If the issuer cannot sell assets quickly enough to meet a surge in redemption requests, the stablecoin may collapse.

3.4 Counterparty and Banking Risk. The fiat reserves are held in traditional banks. If the bank holding the reserves fails or becomes insolvent (as seen in the collapse of Silicon Valley Bank in 2023), the stablecoin issuer may lose access to the backing funds. Such an event could render the stablecoin partially unbacked and cause a permanent loss of value.

3.5 Regulatory Classification Risk. The UK regulatory regime for stablecoins is evolving. There is a risk that a specific stablecoin may not meet future UK regulatory standards for use in payments or custody. This could lead to the delisting of the stablecoin from the Bitpanda Platform.

3.6 Lack of Deposit Protection. Stablecoins are not fiat currency. They are not protected by the Financial Services Compensation Scheme (FSCS) in the UK or equivalent deposit insurance schemes. In the event of the issuer's insolvency, you would be an unsecured creditor and could lose your entire investment.

4 Category D - Memecoins

Description

4.1 Memecoins are cryptoassets inspired by internet memes, jokes, or social trends. They generally lack specific technical utility, a unique value proposition, or a serious roadmap for development. Instead, their value is driven almost exclusively by community engagement, social media hype, viral marketing, and celebrity endorsements. Users typically buy memecoins for purely speculative purposes, hoping for rapid price appreciation driven by online trends.

Risk

4.2 Extreme volatility and speculation. Memecoins are among the most volatile assets in the crypto market. They can experience massive price swings of thousands of percent in a short period but can crash just as quickly. Their value relies almost entirely on investor sentiment, attention, and 'hype cycles'. When the hype fades, prices often collapse and may never recover.

4.3 No intrinsic value. Unlike utility tokens or protocol tokens, memecoins rarely offer any product, service, or revenue stream. If the community leaves or the meme becomes outdated, the token has no fundamental floor price to support it. You should assume that the long-term value of any memecoin could effectively be zero.

4.4 Market manipulation and rug pulls. The memecoin market is rife with manipulation. Malicious actors may launch a token, pay influencers to promote it, and then sell their large holdings into the buying frenzy (a 'pump and dump'). Additionally, developers may withdraw all the liquidity from the trading pool, effectively stealing investor funds (a 'rug pull'). These scams are common and often leave investors with total losses.

4.5 Insider allocation and sniper bots. Many memecoins have unfair launch mechanics. Insiders or developers may use automated software ('sniper bots') to buy large portions of the supply the very second the token launches. These insiders then control the market and can dump their tokens on retail investors at any time, suppressing the price and extracting liquidity.

4.6 Liquidity traps. Memecoins often have very low liquidity. While the paper value of your holding may appear high, you may be unable to sell your position without crashing the price. This is often referred to as 'high slippage' or a lack of 'exit liquidity'.

4.7 Intellectual property risks. Many memecoins utilise copyrighted imagery or trademarks without permission. Legal action by the rights holders could force the project to shut down or rebrand, potentially leading to a total loss of value for token holders.

5 *Category E - Utility Tokens*

5.1 Category E1 - DeFi DEX/AMM Governance

Description

5.1.1 These tokens grant governance rights for Decentralised Exchanges (DEXs) or Automated Market Makers (AMMs). Holders can vote on protocol parameters, fee structures, and treasury spending.

Risks

5.1.2 Speculative Value and the 'Fee Switch'. The value of these tokens is often speculative. Many DEX tokens do not currently distribute protocol revenue to holders due to regulatory concerns regarding securities laws. Consequently, value often relies on the expectation that a 'fee switch' will be activated in the future to share revenue. There is no guarantee this will ever happen, meaning the token may hold no cash flow rights.

5.1.3 Smart Contract Vulnerabilities. DEXs handle massive volumes of assets and are high-value targets for hackers. A bug in the trading logic or the router contracts could allow attackers to drain liquidity pools, destroy confidence in the protocol, and crash the token price.

5.2 Category E2 - Defi Lending / Credit Governance

Description

5.2.1 These tokens govern decentralised lending protocols. These platforms allow users to lend assets to earn interest or borrow assets by providing collateral. The protocol uses smart contracts to automate interest rates and collateral management.

Risks

5.2.2 Bad debt and liquidation failure. Lending protocols rely on the liquidation of collateral to stay solvent. If the market crashes rapidly, the system may fail to liquidate collateral fast enough to cover the loans. This leads to 'bad debt' which can bankrupt the protocol. Governance token holders are often the backstop for this debt and could see their tokens diluted or sold off to cover losses.

5.2.3 Oracle dependency. Lending protocols require accurate real-time price feeds (oracles) to value collateral. If an oracle is manipulated or hacked, attackers can borrow more than they are allowed or trigger false liquidations.

5.3 Category E3 - DeFi Derivatives/Perps Governance

Description

5.3.1 These tokens relate to platforms offering leveraged trading, perpetual swaps, or options. Users hold these tokens to govern the platform, stake for fee discounts, or earn a share of the revenue.

Risks

5.3.2 Insurance fund depletion. Derivatives platforms use an insurance fund to cover trader profits that exceed the losses of other traders. In periods of extreme volatility, this fund can be depleted. If the fund runs dry, the protocol may fail, socialise losses among users, or suffer a collapse in the value of its native token.

5.3.3 Regulatory intensity. Derivatives trading is highly regulated in most jurisdictions. Decentralised derivatives platforms face significant legal risks regarding their operation, particularly concerning offering leverage to retail users.

5.4 Category E4 - Oracle/Data Networks

Description

5.4.1 Oracle tokens are used to pay for and secure the delivery of real-world data (such as price feeds) to the blockchain. Smart contracts cannot access the internet directly and need 'oracles' to feed them data.

Risks

5.4.2 Systemic risk. Oracles are critical infrastructure. If the network fails or provides bad data, it can cause catastrophic losses across hundreds of DeFi applications. While the oracle token itself might survive, the reputational damage from such an event could be irreversible.

5.4.3 Operator concentration. Despite being decentralised in theory, many oracle networks rely on a limited number of permissioned or 'whitelisted' node operators to ensure data quality. This introduces centralisation risks. If these operators collude or are compromised, the integrity of the data is at risk.

5.5 Category E5 - Infrastructure (storage/compute/indexing/DePIN)

Description

5.5.1 These tokens power Decentralised Physical Infrastructure Networks (DePIN). They facilitate marketplaces for resources like file storage, GPU computing power, or wireless coverage. The token acts as the medium of exchange between providers of the hardware and users of the service.

Risks

5.5.2 Supply and demand imbalance. The token economics of these projects rely on a balance between hardware providers (supply) and actual users (demand). Often, the supply of resources grows faster than the demand from paying customers. This can lead to an oversupply of the token as providers sell their earnings, suppressing the price permanently.

5.5.3 Technical barriers and competition. These networks compete directly with centralised giants like Amazon Web Services (AWS) or Google

Cloud. Decentralised alternatives are often slower, more complex to use, and technically demanding.

5.6 Category E6 - Gaming / Metaverse

Description

5.6.1 These tokens serve as in-game currencies, items, or governance shares for blockchain-based games and metaverse worlds. Players use them to buy assets, upgrade characters, or vote on game developments.

Risks

5.6.2 Hit-driven nature. The gaming industry is hit-driven. A game can be incredibly popular for a few months and then be abandoned by players for the next trend. The value of gaming tokens is tied 100% to the active player base. If players leave, the economy collapses.

5.6.3 Inflationary 'Play-to-Earn' mechanics. Many blockchain games issue tokens as rewards to players. This creates constant selling pressure. Unless there is a constant stream of new players buying the token to enter the game, the economy becomes unsustainable. This often results in a boom-and-bust cycle.

5.7 Category E7 -Centralised exchange/venue tokens

Description

5.7.1 These tokens are issued by centralised crypto exchanges. They typically offer benefits like trading fee discounts, higher staking rewards, or access to exclusive token sales on that specific platform.

Risks

5.7.2 Counterparty risk. The value of these tokens is inextricably linked to the reputation and financial health of the issuing company. If the exchange suffers a hack, regulatory shutdown, or insolvency, the token value will likely crash to zero. You are betting on the success of a single private company.

5.7.3 Utility changes. The issuing exchange retains full control over the token's utility. They can unilaterally change the fee discount rules, stop burn programmes, or alter the benefits at any time, potentially devaluing the token overnight.

5.8 Category E8 - RWA/Tokenisation Infrastructure

Description

5.8.1 Real-World Asset (RWA) tokens represent ownership or a claim to traditional assets which have been 'tokenised' on a blockchain.

Risks

5.8.2 Legal and custody complexity. The token is merely a digital receipt. The actual asset is held off-chain. The value of the token depends on the legal enforceability of the link between the token and the physical asset. If the custodian goes bankrupt or the legal structure is flawed, possessing the token may not guarantee you rights to the underlying asset.

5.8.3 Liquidity mismatch. While the token can be traded 24/7 on a blockchain, the underlying asset may be illiquid. If many users try to redeem their tokens for the underlying asset simultaneously, the issuer may be unable to sell the assets quickly enough. This can lead to redemption freezes.

5.9 **Category E9 - General Governance / Utility**

Description

5.9.1 This category encompasses tokens used for governance of Decentralised Autonomous Organisations (DAOs) or general utility within a specific project not covered by other categories.

Risks

5.9.2 Voter apathy and whale dominance. Governance is often dominated by a few large holders ('whales') or the founding team. Retail holders rarely have enough voting power to sway a decision. This can lead to voter apathy where the community disengages.

5.9.3 Lack of legal wrapper. Many DAOs operate without a formal legal entity. In the event of litigation or regulatory action, it is unclear who is liable.

PART B - GENERAL RISKS OF INVESTMENT

Every investment involves opportunities and risks. Investing in the Supported Assets offered on the Bitpanda Platform carries inherent risks. In extreme cases, the entire invested amount may be lost. You should carefully assess whether the products align with your risk tolerance, investment objectives, financial and tax situation, personal and legal circumstances, and other relevant considerations.

1 *Liquidity and Volatility Risks*

1.1 Volatility and price dynamics. The value of the Supported Assets available on the Bitpanda Platform is typically determined by their current market price. This market price can change rapidly, significantly, and unpredictably. Unlike traditional financial markets, Crypto-Asset markets operate 24 hours a day and 7 days a week. They generally do not have 'circuit breakers' or trading halts to stop price crashes. Consequently, the value of your Supported Assets may experience extreme volatility or decline to zero. Price changes can occur at any time, including outside of standard business hours.

1.2 Liquidity Risks. Not all Crypto-Assets are liquid assets. This means they cannot always be quickly and easily converted into cash or a cash-equivalent with minimal loss in value. There may be limited options to sell or exchange your Crypto-Assets for fiat currencies or other assets, especially during periods of market volatility, network congestion, or low trading activity. Demand for certain Crypto-Assets may decrease rapidly, and you may be forced to sell or exchange the Crypto-Asset at a price significantly lower than expected.

1.3 Specific Risks for Trade Only and Index Only E-Tokens. Certain E-Tokens classified as Trade Only E-Tokens cannot be withdrawn to an external wallet and can only be sold back on the Bitpanda Platform. This restricts your ability to move your assets to other venues where liquidity might be better or to self-custody the assets. Similarly, assets classified as Index Only E-Tokens are only available as part of an Index. They cannot be purchased, sold, or withdrawn individually. To exit a position in an Index Only E-Token, you must sell the entire Index or a portion of it.

1.4 Past Performance. Past performance of a certain Supported Asset is not a reliable indicator of future results. You should not rely on historical data to predict future growth, stability, or price movements.

2 *Regulatory Risk and Limited Protection*

2.1 Regulatory Uncertainty. The regulatory framework for Crypto-Assets in the UK and globally is evolving. It is possible that statutory or regulatory changes will have material effects on the current setup of the Bitpanda Platform. This may result in substantial modifications to any Supported Assets or the suspension of trading for specific assets. Bitpanda cannot guarantee that certain regulatory or legal changes will not result in the limitation, suspension, or termination of certain services on the Bitpanda Platform.

2.2 Limited Financial Compensation. Bitpanda is registered with the Financial Conduct Authority for the purposes of anti-money laundering (AML) and

countering the financing of terrorism (CFT) supervision only. The services provided to you by Bitpanda, and which are available on the Bitpanda Platform, are not within the scope of the jurisdiction of the Financial Ombudsman Service (FOS). E-Tokens and other funds held on the Bitpanda Platform are not subject to protection under the Financial Services Compensation Scheme (FSCS). This means that in the event of an adverse event affecting Bitpanda, such as insolvency, you will not be able to claim compensation under these schemes.

3 ***Operational and Structural Risks***

3.1 Internal Ledger. Bitpanda uses an Internal Ledger to record your ownership of E-Tokens, which are digital representations of the Supported Assets. While Bitpanda holds the underlying Crypto-Assets in custody, your interaction is with the E-Tokens on the Bitpanda Platform. The Internal Ledger structure means that your ability to transact depends entirely on the operational integrity of Bitpanda's internal systems and record-keeping.

3.2 Omnibus wallets. Your E-Tokens are held in commingled 'omnibus' wallets rather than segregated on-chain addresses unique to you. In the event of Bitpanda's insolvency, there is a risk that assets held in omnibus accounts may be treated as part of Bitpanda's general estate rather than as trust assets belonging to individual clients. This could result in delays in returning assets to you, or a loss of some or all of your assets if there is a shortfall. You may be treated as an unsecured creditor rather than a beneficiary with a proprietary claim to specific assets.

3.3 Banking rails. Bitpanda relies on third-party banking partners to process payments in Fiat Money. The appetite of banking institutions to service Crypto-Asset businesses can change rapidly. If Bitpanda loses access to these banking rails, you may be unable to deposit Funds or, more critically, unable to withdraw Funds from your Fiat Wallet for an extended period.

3.4 Operational Downtime. Bitpanda may need to perform maintenance on the Bitpanda Platform, or the Bitpanda Platform may suffer unscheduled downtime due to technical failures, cyber-attacks, or high traffic volume. During these periods, you may be unable to access your Account or trade Supported Assets. If this occurs during a period of high market volatility, you may be unable to sell your assets to prevent a loss or buy assets to capture a gain.

3.5 Delisting. Bitpanda may remove specific Supported Assets from the Bitpanda Platform at any time. This process is known as Delisting. Reasons for Delisting include compliance with applicable law, technological challenges, security concerns, or liquidity issues. If an asset is Delisted, you may be required to sell or withdraw your assets within a specific notice period. If you fail to do so, Bitpanda may be entitled to sell the assets on your behalf at the prevailing market price or take other measures as described in the E-Token Terms.

3.6 Irreversibility of Transactions. Transactions in Crypto-Assets are generally irreversible. Once you initiate a transfer of Crypto-Assets to a third party or an external wallet, you may not be able to recover the assets if you have made an error in the address, if you have selected the wrong network, or if the recipient

refuses to return them. Bitpanda cannot reverse a transaction that has been broadcast to the blockchain network.

3.7 Counterparty and Intermediary Risk. When providing certain services in connection with Supported Assets, Bitpanda may execute orders on behalf of the client or transmit an order for the client to a third party. This means Bitpanda might engage with a number of counterparties including financial counterparts, sub-custodians, liquidity providers, and external exchanges. Bitpanda has no control over the financial stability of counterparties that it interacts with as part of the crypto market infrastructure. In the event that a counterparty defaults, becomes insolvent, or suffers a technical failure, Bitpanda may be unable to retrieve or transfer Supported Assets held, potentially resulting in a full or partial loss.

4 *Technology and Security Risks*

4.1 Software Weakness and No Warranty. The technology of Crypto-Assets, the underlying software applications, and the smart contract systems are still in an early stage of development. They may be unproven and are often beyond Bitpanda's control. There is an inherent risk that the technology could contain weaknesses, vulnerabilities, or bugs. These defects can cause the complete loss of any Crypto-Assets. Many of these technologies are neither released by a software manufacturer nor certified by a central entity, meaning there may be no person or entity that could be held liable for such defects.

4.2 Device Security and Credentials. Failure to secure your own devices may lead to unauthorised access to your Account. If you do not activate two-factor authentication, any person with knowledge of your password and email address may be able to access your Account and remove assets. Bitpanda recommends that you always choose a strong, unique password and use 2FA.

4.3 Eliminating the Benefits of 2FA. The safety benefit of using 2FA is effectively eliminated if both factors can be accessed with the same credentials or the same device. For example, if you use an authenticator app on the same mobile phone you use to access the Bitpanda Platform, a compromise of that phone could compromise both factors.

4.4 Phishing and Social Engineering. SMS and email services are vulnerable to spoofing and phishing attacks. Phishing attacks often occur via SMS, email, search engines, ads in search engines, or other fraudulent links. While Bitpanda strongly recommends using 2FA, 2FA cannot prevent successful phishing or social engineering attacks if your credentials, including the second factor used for the 2FA, are disclosed in such an attack.

5 *Crypto-Asset Protocol, Development and Community Risks*

5.1 Imperfect Transaction Processing. Bitpanda uses 'Nodes' on each respective blockchain which scan each block for transactions, including both deposits and withdrawals. As soon as such a transaction is identified, it is taken into account in Bitpanda's systems. It is possible that a Node does not record a transaction and therefore does not feed it into Bitpanda's systems. This could result in

delays or failures in crediting deposits or processing withdrawals of Crypto-Assets.

5.2 Risk of Abandonment. The development of any Supported Asset might be abandoned for a number of reasons. These include lack of interest from the industry, community, or public, lack of funding, and lack of commercial success or prospects (for example, caused by competing projects). Certain Supported Assets may become subject to material changes to functionality up to and including the loss of all functionality.

5.3 Forks and Airdrops. The protocols of Crypto-Assets may be subject to forks that change the underlying blockchain protocol rules. Bitpanda is not obliged to support any specific fork. If Bitpanda decides not to support a fork, you may not receive the benefit of any new assets created by that fork. Furthermore, Bitpanda does not automatically support or distribute 'airdrops' (free distributions of new tokens). You may lose the opportunity to claim these assets if you hold your Crypto-Assets on the Bitpanda Platform rather than in a private wallet.

5.4 Blockchain Mining Attacks. Crypto-Assets may be susceptible to attacks on their underlying blockchain networks. These include, but are not limited to, double-spend attacks, majority mining power attacks (51% attacks), 'selfish-mining' attacks, and race condition attacks. These are mining or non-mining related attacks which are out of Bitpanda's influence and control.

5.5 Collateralisation Risk. Bitpanda does not take any responsibility for Supported Assets that are or claim to be collateralised with, backed by, or pegged to legal tender or any other underlying asset of any kind (for example, stablecoins). All actions in connection to such Supported Assets are in the sole responsibility of the issuer. There is a risk that the issuer may not hold sufficient reserves or may refuse redemption.

5.6 Execution Risks. The price of Crypto-Assets can fluctuate significantly within short periods of time due to various factors, including market demand, regulatory changes, and general market sentiment. Additionally, the execution of your trade may be delayed or not occur at all during periods of high volatility or low liquidity.

6 *Staking-specific Risks*

6.1 Reward Variability. Staking rewards are determined by the network and are not guaranteed. Factors such as protocol changes, validator performance, network conditions, and downtime may impact the reward rate. Past rewards are not indicative of future returns.

6.2 Liquidity Risk. Some staked Crypto-Assets are subject to a mandatory lock-up period during which they cannot be transferred or sold. Following the lock-up, an unbonding period applies. During this time, assets remain inaccessible until the network completes the release process. This timeframe varies by protocol and may be impacted by network conditions. During both periods, market fluctuations can affect the value of the staked assets.

6.3 Slashing Risk. Certain networks impose penalties, known as "slashing," on validators for downtime, improper behaviour, or protocol breaches. While rare, this may result in partial or total loss of staked assets. If slashing results from a network exploit, protocol error, or user actions, losses may not be recoverable.

6.4 Conflict of Interest in Staking. Bitpanda may stake E-Tokens held in custody on its own account and for its own benefit. Bitpanda retains any Staking Rewards generated from this activity unless explicitly shared with you under a specific product offering. This creates a potential conflict of interest between Bitpanda's commercial interests and its duty as a custodian. By agreeing to the E-Token Terms, you consent to this arrangement and waive any claim to rewards generated by Bitpanda on its own account.

7 *Tax and Currency Risks*

7.1 Tax Risks. The purchase, sale, exchange, and holding of Supported Assets may trigger tax consequences for you. Bitpanda may report information with respect to Transactions made by you to tax authorities to the extent such reporting is required by applicable law. You are responsible for complying with all national and international tax laws applicable to you.

7.2 Currency and Exchange Rate Risks. Many Crypto-Assets are traded globally in US Dollars (USD). If you fund your Account or trade in Pounds Sterling (GBP) or Euros (EUR), your investment return will be affected by the exchange rate between your local currency and the US Dollar. Even if the value of the Crypto-Asset remains stable in USD terms, a strengthening of your local currency against the USD could result in a loss when you convert your assets back to fiat currency.