Risk Disclosure Statement

Understand the risks before you invest.

DOCUMENT	EFFECTIVE	VERSION	ISSUED BY
Risk Disclosure Statement	**July 2026**	**v2026.1**	**Universal Quantum**

This Risk Disclosure Statement sets out the principal risks of using Universal Quantum and of investing in digital assets through our Investment Plans. It does not describe every possible risk. Digital-asset investment is unsuitable for many investors. Read this statement in full before you deposit any funds. If any part is unclear, seek independent professional advice before you proceed.

1. 1. Purpose of this statement

The purpose of this statement is to help you understand, in plain language, the risks of using the Platform and of committing funds to an Investment Plan. It should be read alongside our Terms of Service, our Privacy Policy, and our AML and KYC Policy. It is written for a general audience and does not take account of your personal circumstances.

2. 2. Not financial advice

Nothing on the Platform — including product pages, marketing content, projected returns, plan descriptions, blog posts, live-chat responses and support replies — constitutes financial, investment, legal or tax advice. All content is general information. Your decision to invest is your own. Consider seeking independent, qualified advice before you deposit funds, particularly if you are unfamiliar with digital-asset markets or if your investment would represent a material share of your net worth.

3. 3. Nature of digital-asset investing

Digital assets such as XRP, Solana (SOL), TRON (TRX), Bitcoin, Ethereum, BNB and USDT are relatively new, highly technical and market-sensitive instruments. Their design, supply, custody and market structure differ from traditional financial products such as shares, bonds and bank deposits. Some are more established than others; all remain subject to novel legal, technical and market risks.

4. 4. Volatility & market risk

Digital-asset prices are highly volatile. Prices can move materially, in either direction, over short periods. Sudden, large moves can be triggered by macroeconomic news, on-chain events, exchange failures, changes in liquidity, sentiment, protocol changes or regulatory action. Even short-duration Investment Plans can be exposed to significant price swings during the plan term.

5. 5. No guaranteed returns

The daily and total return figures shown on the Platform are **targets and illustrations**. They are based on our own strategies and assumptions and are not guarantees. Actual results depend on market conditions, strategy performance, network fees and other factors outside our control.

> High advertised returns carry high risk. A stated daily return does not guarantee that any specific amount will be earned or that your capital will be preserved. Past performance is not a reliable indicator of future results.

6. 6. Risk of total loss

You may lose some or all of the funds you commit to an Investment Plan. Circumstances that could cause loss include severe market drawdowns, protocol or smart-contract failure, custodial incidents, prolonged network outages, exchange defaults, regulatory action, fraud, cyber-attack and operational failure. Only invest funds you can afford to hold and, if necessary, lose in full.

7. 7. Concentration risk

Placing a large portion of your net worth into a single Investment Plan, a single asset or a single strategy concentrates your exposure to that asset or strategy. Diversification across assets, strategies and time can help manage this risk but does not eliminate it. Consider what proportion of your total capital is exposed to digital assets and to the Platform specifically.

8. 8. Liquidity & withdrawal timing

Amounts committed to an Investment Plan are locked until maturity. Between deposit and maturity you cannot withdraw the principal, and you should treat funds committed to a plan as not immediately accessible.

Withdrawals from your Available Balance are typically settled on-chain within twenty-four (24) hours but can take longer during periods of high demand, network congestion, or where compliance review is required. On-chain transactions are also subject to network fees and confirmation times set by the underlying blockchain.

9. 9. Custodial & counterparty risk

Funds deposited to the Platform are held under our custody until returned to you. Custody carries inherent counterparty risk — for example, in the event of an insolvency, an incident affecting our custody arrangements, or a failure of an upstream service provider. We take reasonable steps to mitigate these risks, but they cannot be eliminated. You should consider the impact on you if we were unable to return funds when you expected them.

10. 10. Smart-contract & protocol risk

Some strategies interact with smart contracts or decentralised protocols. Smart-contract code can contain bugs; protocols can be forked, upgraded or abandoned; oracle feeds can be manipulated; validator or staking arrangements can slash or under-perform. Any of these can affect the returns of an affected strategy, and in the worst case can lead to loss of the funds allocated to that strategy.

11. 11. Network & on-chain risk

Deposits and withdrawals rely on the underlying blockchain networks. Networks may experience congestion, temporary halts, chain reorganisations, or contentious hard forks. Transactions sent to the wrong address, on the wrong network, or in the wrong asset generally cannot be recovered. You are responsible for the accuracy of every address you provide.

12. 12. Regulatory risk

The regulatory treatment of digital assets, custody and yield-generating products varies by jurisdiction and is changing rapidly. New laws, regulator guidance or enforcement action could restrict, tax, license or prohibit activities related to the Platform in your country. You are responsible for ensuring that your participation is lawful where you live, and for any consequences of a change in the law.

13. 13. Tax risk

Deposits, returns, reinvestments and withdrawals may be taxable events in your jurisdiction. Tax rules for digital assets vary widely and can change with little notice. You are solely responsible for calculating and paying any tax that applies to your activity, and for keeping the records required by your local tax authority. We do not provide tax advice.

14. 14. Cyber & security risk

The Platform, its providers and its users are targets for cyber-attackers. Even with strong controls in place, there is residual risk of unauthorised access, credential theft, phishing, malware, denial-of-service attacks and other cyber events. Protect yourself: use a strong, unique password, enable two-factor authentication, keep devices and browsers up to date, treat unsolicited messages with suspicion, and only sign in from devices you trust.

15. 15. Fraud & scam risk

Impersonators frequently target investors on messaging apps, social media and email. We will never ask you for your password, your wallet keys, remote access to your device, or fees to release your funds. If someone contacts you claiming to be from Universal Quantum and asks for any of these, it is not us. Report the incident through the contact page and do not respond.

16. 16. Third-party & service-provider risk

The Platform relies on third-party services (for example hosting, transactional email, live-chat, blockchain data feeds and translation). A failure or compromise of any of these could affect availability of the Platform. We monitor and vet third parties but cannot fully eliminate this risk.

17. 17. Force majeure

Events outside our reasonable control — including natural disasters, war, pandemics, blockchain-network outages, government action and infrastructure failure — may delay or prevent us performing our obligations. In such cases we will restore service as soon as it is reasonably possible to do so.

18. 18. Suitability & personal responsibility

Digital-asset investment is not suitable for every investor. Before you deposit, consider your financial position, your objectives, your appetite for risk, your investment horizon, your knowledge, and your ability to bear a loss of the amount invested. If in doubt, take independent professional advice from someone qualified to advise you in your jurisdiction.

19. 19. Diversification & sizing

As a general principle, avoid committing money you cannot afford to hold, avoid concentrating too much of your net worth in a single asset or strategy, and consider staging deposits over time rather than in a single lump sum. Reinvestment increases the principal at risk; monitor exposure as balances grow.

20. 20. Continuous monitoring

Keep an eye on your Account. Review your deposits, returns, active plans and withdrawal history regularly. Update your contact details so that important notifications reach you. Act quickly if something looks wrong or if a message from us asks you to review recent activity.

21. 21. Your acknowledgement

By using the Platform you confirm that you have read and understood this Risk Disclosure Statement, that you understand the risks described, that you have considered your own circumstances, and that you accept full responsibility for your investment decisions.

22. 22. Detailed additional risks

Staking & validator risk. Some Investment Plans involve delegating to validators or staking to networks. Validator misbehaviour, extended downtime, or protocol-imposed slashing can reduce returns and, in some cases, cause loss of a portion of the staked principal. Un-staking may be subject to protocol-imposed lock-up or unbonding periods that delay withdrawal.

Oracle & data-feed risk. Some strategies rely on external price or data feeds ("oracles") to determine the value of assets, to trigger trades, or to calculate returns. Oracle failure, manipulation or delay can cause a strategy to behave in unexpected ways, including realising losses or paying incorrect returns.

Exchange & trading-venue risk. Where a strategy trades on centralised exchanges or decentralised venues, the credit and operational risk of those venues affects the strategy. Exchanges have historically halted withdrawals, been hacked, or become insolvent with limited or no recovery for their customers.

Bridge & wrapped-asset risk. Moving assets between blockchains via bridges, or holding wrapped versions of assets, introduces additional smart-contract risk and dependency on the bridge operator. Bridges have been repeatedly targeted by attackers and have suffered material losses.

Insurance & compensation. Digital-asset holdings are generally not covered by traditional deposit-insurance schemes, and there is no guarantee that any custody, network or exchange incident will be made good by insurance or by a public compensation scheme. Do not assume that a loss will be recoverable.

Behavioural & emotional risk. Sharp price moves, social-media coverage and impersonation attempts can create pressure to make hasty decisions. Take time to review any request before acting on it, particularly requests from anyone claiming to be part of our team, and particularly requests to move funds, share credentials, or install software.

Impersonation & phishing. Attackers frequently create fake websites, look-alike domain names, cloned social-media accounts and lookalike emails to trick investors. Always check the address bar, avoid clicking links from unverified sources, and access the Platform by typing our address directly or using a bookmark you created yourself.

Device & browser hygiene. Keep the device and browser you use to access the Platform up to date. Do not install extensions or software from untrusted sources. Consider using a dedicated browser profile for financial activity. If a device is lost or stolen, sign out of all sessions and change your password immediately.

Recovery limitations. Certain events are irreversible. Once a withdrawal transaction has been broadcast to the network, or once funds have been sent to an incorrect address, recovery is generally not possible. Take time to verify address details before you confirm any transaction.

Timing & market hours. Digital-asset markets operate continuously. You should not assume that we or anyone else can respond to a request outside our stated support hours or that market conditions will be similar to those at the time you initiated a request.

Rate & feed limitations. Prices displayed on the Platform are indicative and may be delayed or approximated. Executable rates at the time of a specific transaction may differ. Use displayed rates for orientation, not for trading against.

Documentation risk. Read the plan description, the Terms and this statement before you deposit. Ask questions if anything is unclear. Once you deposit, you are treated as having accepted the terms of the plan as described at the time you deposited.

23. 23. Glossary

Digital Asset — A digital token supported for deposits or withdrawals on the Platform.

Investment Plan — A managed digital-asset strategy offered on the Platform, with a stated daily return and a fixed term.

TXID — Transaction hash: the unique identifier of an on-chain transaction, used to match your deposit to your Account.

Available Balance — The sum of funds credited to your Account that are not currently locked in an active plan.

Maturity — The point at which an Investment Plan ends and your principal is returned on top of the accrued returns.

Slashing — A protocol-imposed penalty deducted from a validator (and its delegators) for misbehaviour, such as being offline or double-signing.

Oracle — A service that supplies external data (typically prices) to a smart contract.

Bridge — A protocol that moves assets between different blockchains.

Wrapped asset — A token representing a native asset from a different chain (for example wrapped Bitcoin on Ethereum).

Custody — Holding assets on behalf of another person; carries counterparty risk.

Force majeure — Events outside reasonable control (natural disaster, war, government action, infrastructure failure) that delay or prevent performance.

Volatility — The tendency of a price to move materially over short periods.

24. 24. Where to get help

Questions about anything in this statement can be raised through the contact page or by emailing **support@universalquantum.net**. If you believe you have been the victim of fraud, contact us immediately and, where appropriate, report the incident to your local authorities.