Investing in crypto

There are over 19,000 different cryptocurrencies, including stablecoins, that have been generated and made available for sale and trading on various exchanges. Bearing in mind the various warnings that governments, such as those in the UK, Israel, the United States, and Singapore, have issued regarding investment in digital assets – including specific warnings about scams and the advertising restrictions on crypto advertisements to the general public that have been enacted in the UK, Spain, and Singapore.

We have set out some basic due diligence steps when investing in cryptocurrencies. Of course, where necessary, professional advice should be sought.

- Mode of investment: Most purchases of cryptocurrencies will be from exchanges. Then, upon payment, the cryptocurrencies will be sent to a hot wallet, typically hosted by the exchange. In some cases, the cryptocurrencies are obtained directly from the token generation event in a process called the initial coin offering. However, there is a class of cryptocurrency transactions that use cold or unhosted wallets where the technical assistance and transaction mechanism of an exchange will not be available. In this case, extra care should be taken, as discussed below.
- Research: Conduct thorough research on the cryptocurrency. Read and understand its business model and tokenomics, and check out the background of the key team. The website, the white paper, and the accompanying contractual documentation should set out clearly and consistently the entities involved with the cryptocurrency.
- Whether the cryptocurrency is listed: Although not conclusive, a listed cryptocurrency indicates that there is a ready market should you need to liquidate. If the exchange is reputable, it will also have done some level of basic due diligence.
- Security measures: Cybersecurity hacking incidents such as those relating to Solana, Harmony, and Axie Infinity have given rise to the term cryptojacking. A significant investment requires that some due diligence be carried out on the cybersecurity measures employed by the token issuer or platform as crypto companies have been targeted by hackers.
- Anti-money laundering/know your client (AML/KYC): Transactions involving regulated wallets will already have AML and KYC features built in. For transactions involving unhosted wallets, AML and KYC measures will be necessary – especially for significant transactions. In the EU, the proposed transaction floor for required reporting is €1,000. In all transactions, the source of funds must be determined in order to ensure that the cryptos being transferred are not the proceeds of criminal activity.

A final note on significant unhosted wallet crypto transactions – in order to ensure that the transaction is executed smoothly and with reasonable levels of privacy for the parties, practice has evolved to includes measures and techniques such as zero knowledge proof (where information is exchanged to validate the transaction with high probability without revealing confidential data such as wallet addresses), proof of coin (the crypto equivalent of proof of funds), and the Satoshi test (to demonstrate control over a specific address).

Author

Bryan Tan
Partner
Singapore
bryan.tan@reedsmith.com