

VIRTUAL MONEY TRADING OR INVESTMENT RISKS

Flightclup provides Software as a Service solutions for the cryptocurrency industry. There is a significant risk of loss associated with trading Virtual Currencies.

Virtual currency markets have several unique risks that traders and investors should be familiar with. These include but are not limited to the following.

Unique Features of Virtual Currencies. Virtual currencies are not legal tender in the United States, and many question whether they have any real value. The price of many virtual currencies depends on the agreement of the parties for a transaction. The risks associated with the unique characteristics of virtual currencies are explained.

Price fluctuation. The price of a virtual currency is based on the perceived value of the virtual currency and is subject to sensitivity changes that make these products highly volatile. Some virtual currencies experienced more than 20% daily price volatility. The risks associated with the extreme price volatility of virtual currencies and the possibility of rapid and significant price movements that could result in significant losses are explained.

Valuation and Liquidity. Virtual currencies can be traded through privately negotiated transactions and numerous virtual currency exchanges and brokers around the world. The absence of a central pricing source presents several valuation challenges. Additionally, dispersed liquidity can pose challenges for market participants trying to exit a position, especially during times of stress. Valuation and liquidity risks, procedures used in valuation of virtual currencies and related risks are explained.

Cyber security. The cybersecurity risks of virtual currencies and associated “wallets” or spot exchanges include hacking vulnerabilities and the risk of publicly distributed ledgers becoming immutable. A cybersecurity incident can result in a significant, immediate and irreversible loss for market participants trading virtual currencies. Even a minor cybersecurity incident in virtual currency is likely to cause downward price pressure on that product and potentially other virtual currencies. The cybersecurity risks associated with virtual currency transactions are explained.

Opaque Spot Market. Virtual currency balances are usually held as an address on the blockchain and accessed via private keys that can be held by a market participant or a custodian. Although virtual currency transactions are generally public on a blockchain or distributed ledger, the public address does not identify the controller, owner, or owner of the private key. Unlike bank and brokerage accounts, virtual currency exchanges and custodians holding virtual currencies do not always identify the owner. The opaque underlying or spot market creates asset verification challenges for market participants, regulators and auditors, and leads to increased risk of manipulation and fraud, including the potential for Ponzi schemes, bucket shops, and pump and dump schemes. The risks associated with the opaque nature of the underlying or spot virtual currency market are explained.

Virtual Currency Exchanges, Brokers and Custodians. Virtual currency exchanges and other brokers, custodians, and vendors used to facilitate virtual currency transactions are relatively new and largely unregulated in both the United States and many foreign jurisdictions. Virtual

currency exchanges often purchase virtual currencies for their own accounts on the public ledger and allocate positions to clients through internal bookkeeping entries while maintaining exclusive control of private keys. Under this structure, virtual currency exchanges collect large amounts of client funds for the purpose of buying and holding virtual currency on behalf of their clients.

The underlying opacity and lack of regulatory oversight of the spot market creates the risk that the virtual currency exchange may not be able to hold sufficient virtual currency and funds to meet its obligations, and this shortcoming may not be easily detected or discovered. In addition, many virtual currency exchanges have experienced significant outages, downtime and transaction processing delays and may have a higher level of operational risk than regulated futures or securities exchanges. If virtual currencies are traded or held through an exchange, broker or custodian, the risks associated with those transactions are disclosed.

Regulatory Landscape. Virtual currencies currently face an uncertain regulatory landscape in the United States and many foreign jurisdictions. In the United States, virtual currencies are not subject to federal regulatory oversight, but may be regulated by one or more state regulatory agencies. Additionally, many virtual currency derivatives are regulated by the CFTC and the SEC warned that many initial coin offerings would likely fall within the definition of a security and would be subject to US securities laws. One or more jurisdictions may adopt future laws, regulations or guidelines that affect virtual currency networks and their users. Such laws, regulations or guidelines may affect the price and acceptance of virtual currencies by users, merchants and service providers. The risks associated with the current regulatory environment for virtual currencies are explained.

Technology. The relatively new and rapidly evolving technology underlying virtual currencies brings unique risks. For example, a unique private key is required to access, use, or transfer virtual currency on a blockchain or distributed ledger. Loss, theft or destruction of the private key can result in an irreversible loss. The ability to join the forks could also have implications for investors. For example, a market participant holding a virtual currency position through a virtual currency exchange could be adversely affected if the exchange does not allow its customers to participate in a fork that creates a new product. The risks posed by this newly developing technology are explained.

Transaction fees. Many virtual currencies allow market participants to offer a fee to miners (i.e. parties that process transactions and record them on a blockchain or distributed ledger). While not required, a fee is usually required to ensure that a transaction is immediately recorded on a blockchain or distributed ledger. The amounts of these fees are subject to market forces and it is possible for wages to rise significantly during a stress period. Additionally, virtual currency exchanges, wallet providers, and other custodians can charge higher fees than custodians in many other financial markets. The impact of these transaction fees on performance should be understood by the participants.