An Introductory Guide to Bitcoin
Date: 30 September 2021

An investment in the Vault International Bitcoin Fund (VIBF) is a highly speculative investment. Bitcoin is a highly volatile asset. This means the VIBF will not be appropriate for all investors. You should read the disclosure material before investing. You should also seek advice from an independent financial adviser to help you make investment decisions.

Implemented Investment Solutions Limited is the issuer and manager of Vault Digital Funds (Scheme). For a Product Disclosure Statement please visit: www.iisolutions.co.nz or https://disclose-register.companiesoffice.govt.nz/

This paper has been prepared with help from the team at Easy Crypto (www.easycrypto.com/nz) with the purpose of helping people understand more about Bitcoin.

What is Bitcoin?

Bitcoin is a decentralized digital asset known as a cryptocurrency that is created and held virtually, facilitating peer-to-peer transactions without the need for traditional intermediaries such as banks.

Powered only by its users, Bitcoin is fully decentralized: just as no one owns the technology behind the internet or email, Bitcoin is collectively controlled by its users, investors, and developers around the world rather than a single entity.

What is a cryptocurrency?

Cryptocurrency is any system that uses cryptography as the framework to make internal payments, where funds are represented as entries in a decentralised distributed ledger.

In essence, cryptocurrency is digital money that can be used as a medium of exchange to buy and sell goods and services. Cryptocurrencies are stored in an account, called a crypto wallet – an account that operates and functions outside of bank systems.

Bitcoin was the first - and still largest - cryptocurrency, accounting for over 40% of the total market value.

According to CoinMarketCap, there are over 6,800 different cryptocurrencies, which includes other well-known cryptocurrencies such as Ethereum, Cardano and Ripple.

What is cryptography?

Put simply, cryptography is the technological means by which information and transactions are protected by using codes that can only be decrypted by the intended end-users.

History of Bitcoin

Bitcoin was first proposed in 2009 by an individual (or individuals) publishing under the pseudonym Satoshi Nakamoto as a means for creating a currency system operating independently of existing banks or financial institutions via an autonomous decentralized ledger system known as a blockchain.

The value of Bitcoin had relatively humble beginnings, only surpassing $1,000 USD in January of 2017, before peaking later in that same year. Its value has seen highs and lows over the years illustrating the high volatility associated with this pioneering digital asset. This volatility is highlighted by the price of Bitcoin ranging between US$10,440 and $64,863 over the past 12 months.

However, despite its volatility Bitcoin has recently seen adoption among some individuals and institutions who see potential for further growth in this asset.

Currently Bitcoin retains its reputation as the most popular digital asset for investors. Bitcoin also remains the largest cryptocurrency with a market value hovering around $780 Billion USD – placing it within the top 10 most-valuable traded assets in the world (Source: www.companiesmarketcap.com as at 29 September 2021).

How does Bitcoin work?

Bitcoin is a peer-to-peer payment system that runs independently of a central governing authority that would traditionally control the supply of currencies.

The flow of Bitcoin is controlled directly by its users; from one wallet address to another. The total supply is also hard-capped at 21 million coins, which provides Bitcoin with potential value attached to its scarcity.

Bitcoin miners

Bitcoin miners are members of the platform who independently verify and confirm the *blocks*, or transactions using high-performance computers – a process that involves solving an algorithm that will verify that transactions occurring on the blockchain are authentic. Miners are then rewarded Bitcoins for their mining efforts.

To understand how Bitcoin works it's important to understand the different components of the system:

Blockchain

Bitcoin is a digital currency that operates on a decentralized ledger system known as a blockchain. This blockchain acts as a shared public ledger where each transaction is referred to as a *block* and is *chained* to the open-source coding creating a record of each transaction. This blockchain technology paved the way for the emergence of other cryptocurrencies

Private and public keys

Using a cryptocurrency on a blockchain requires a digital signature consisting of a person's "public key" and "private key".

These keys are generated whenever a new wallet is created. An easy way to think about it is that the public key is a Post Office Box, and the private key is the key to the Post Office Box.

The public key is the address for payments, similar to an individual's bank account number. The private key is like an individual's password to this account.

Private and public keys allow owners to access their assets. The importance of keeping these keys secure cannot be overstated and private keys should never be shared.

How people store Bitcoins: cryptocurrency wallets

Just as you would store fiat (or government-controlled) currencies in wallets or banks, cryptocurrencies also benefit from safe storage.

Bitcoin and cryptocurrencies are stored in what is known as a cryptocurrency wallet. There are different types of crypto-wallets, some offering more features than others. There are two main types of crypto-wallets – software wallets (hot wallets) and hardware wallets (cold wallets) – each with different risks and benefits.

Software wallets
As its name suggests, software crypto-wallets take the form of applications or software that run on computers, tablets, or phones that are connected to the internet – hence the term hot wallets.

The main advantages of software wallets are their convenience, accessibility, and on-the-go trading. This makes them a popular choice for beginners.

The main drawback of hot wallets is the potential threat and susceptibility of hacks and/or data breaches. However, it is possible to fortify hot wallets by implementing strong passwords, two-factor authentication, and the use of safe browsing practices.

Hardware wallets
Hardware crypto-wallets, or cold wallets, store Bitcoin and digital assets on physical devices that are not connected to the internet.

These wallets provide an offline environment to authenticate and verify transactions – essentially eliminating the threat to potential hacks or malicious software from breaching user assets or credentials.

Typically, hardware wallets are considered the most-secure storage options for Bitcoins and other digital crypto assets. However, they do require a bit more knowledge and expertise to set up properly.

Do I need to use a software or hardware wallet if I invest in VIBF?
No. The VIBF is a PIE Fund. Investors can hold their investment in VIBF through an investment platform like InvestNow. Investors can also hold their units in VIBF directly, meaning they are recorded on the registry of the Fund. VIBF's exposure to Bitcoin is via underlying exchange-traded funds (ETFs) and funds backed by Bitcoin: each of these ETFs and funds have institutional-grade crypto-custody arrangements in place.

Pros and cons of Bitcoin

Pros

- **Fixed supply -** Due to the framework of its blockchain, there can only ever be 21 million Bitcoins in existence.
- **Transparency -** Enthusiasts claim that a fundamental aspect of Bitcoin is its inherent transparency. Virtually all information that pertains to its supply and record of transactions are publicly available on the blockchain for anyone to verify in real-time.
- **Transaction speeds -** Bitcoin is very fast. Currently, it takes an average of three days to send money across borders using banks, whereas it takes Bitcoin an average of 30 minutes or less. Other cryptocurrencies can be sent across the globe within a second, regardless of bank opening times.
- **Divisibility -** Bitcoin's are divisible, meaning you can split a single Bitcoin down to the 0.00000001. This smallest part of a Bitcoin is called a 'satoshi', and there are 100 million satoshis in a Bitcoin, in comparison to the 100 parts in a New Zealand Dollar. This is how you can purchase a coffee using a fraction of a Bitcoin.
- **Security -** Due to its decentralized nature, owners have full control over their transactions. Payments involving Bitcoin can be made without the need to include personal credentials tied to the transaction.
- **Peer-to-peer transaction freedom -** Bitcoin is not restricted to any country borders, bank holidays, or government bureaucracy. Anyone in the world can send and receive Bitcoins at any given time, as long as they have access to the internet.

Cons

- **Volatility -**There is no denying that Bitcoin has an inherent volatility that is caused by a number of factors including, but not limited to, the still relatively small circulation and number of institutions using Bitcoin. Therefore, business activities, large trading volume, and other small events can significantly affect the Bitcoin price
- **Acceptance -** While public interest in Bitcoin is gradually increasing, its adoption is still a work in progress. Many people are still unaware and thus it will take some time to gain the trust and acceptance of businesses.
- **Lack of regulation -** cryptocurrencies are currently unregulated by both the New Zealand and most other governments and central banks.

- **Third-party security risks -** as Bitcoin is a virtual, technology-based currency, it is vulnerable to cyberattacks and 'hacking', as well as fraud.
- **Permanent loss of Bitcoin -** one of Bitcoin's unique attributes is that individuals are generally responsible for its safekeeping without having to use a trusted third party. However, self-custody places the responsibility of security and the risk of loss on the individual; if an individual loses the private keys, the Bitcoin is irreversibly lost.

In addition to the pros and cons of investing in Bitcoin above, we recommend that you read the VIBF's Product Disclosure Statement and Other Material Information document that provides further information around the risks of investing in the VIBF.

How to buy Bitcoin if you want to invest in it directly?

Bitcoin can be bought and traded through cryptocurrency exchanges, such as Easy Crypto. Specialized Bitcoin ATMs are also another option where you can use your debit card or cash to buy Bitcoin.

Considerations for buying Bitcoin

For some, the prospect of investing in Bitcoin may seem daunting. While Bitcoin and cryptocurrency, in general, can be volatile assets, it is an alternative type of investment that could diversify your portfolio.

Common questions often asked for those interested in buying Bitcoin include the following:

Bitcoin and the VIBF

Bitcoin enthusiasts claim that the associated liquidity, transparency, and future prospects could make the cryptocurrency a good investment for those who can accept its inherent volatility. And as mentioned, Bitcoin's supply is hard-capped at 21 million coins – meaning the value is projected to continually increase as it gets closer to the maximum total supply.

As mentioned above, an investment in Bitcoin, or the Vault International Bitcoin Fund (VIBF), is highly speculative, giving access to an historically volatile digital asset.

Due to the underlying risks, investing in Bitcoin and the VIBF, will only suit those with a high-risk tolerance. Investors should be aware that the opportunity to make large returns also comes with the risk of making significant and permanent losses.

You should read the disclosure material before investing. You should also seek advice from an independent financial adviser to help you make investment decisions.

Implemented Investment Solutions Limited is the issuer and manager of Vault Digital Funds (Scheme). For a Product Disclosure Statement please visit: www.vaultdigitalfunds.com, www.iisolutions.co.nz, www.investnow.co.nz, or https://disclose-register.companiesoffice.govt.nz/.

Glossary

Blockchain
A digital ledger comprised of unchangeable, digitally recorded data in packages called blocks. Each block is "chained" to the next block using a cryptographic signature.

Crypto Asset
Special kinds of virtual currency tokens that reside on their own blockchains and represent an asset or utility.

Cryptocurrency
A cryptocurrency (or crypto) is a digital asset designed to work as a medium of exchange wherein individual coin ownership records are stored in a ledger existing in a form of computerized database.

Cryptocurrency Exchanges
Sometimes called digital currency exchanges, cryptocurrency are unregulated platforms that allow customers to trade cryptocurrencies for fiat money or other cryptocurrencies.

Cryptography
A method of protecting information, communications and/or processes by using codes that can only be decrypted by those who are intended to read and process them.

Decentralized
A network which does not have a single point of failure or breach-ability.

Digital Currency
A currency that exists only in digital form, as opposed to traditional fiat currency.

Exchange Traded Fund (ETF)
A security that tracks a basket of assets such as stocks, bonds, and cryptocurrencies but can be traded like a single share on a sharemarket or exchange.

Fiat
Derived from the Latin word meaning "it shall be", which refer to government-issued currency. The US and NZ dollars are examples of Fiat currency.

Ledger
This word can have multiple meanings within the crypto space. Used alone, Ledger is a brand of USB hardware digital wallet, which holds digital assets on its memory. The Bitcoin network and other crypto networks can also be described as "Digital Ledger's". A digital ledger is a record of transactions on the blockchain. For example a digital ledger of Bitcoin transactions. A digital ledger is a way to help describe the workings of the blockchain.

Miners
Miners, see “Mining” are a collective group of mining machines that work together to solve a mathematical problem while ensuring the blockchain network is true, decentralized, and immutable. Miners can also “Pool” their mining hash rate (the rate at which they solve computational problems) in order to get rewards faster, then split them according to the computational power they contributed to the pool.

Mining
Mining in the crypto world means processing transactions, encrypting network data, ensuring that transactions are true, comparing blocks, and the list goes on. But to simplify this mining crypto is using the computational power of your PC, Graphics card or ASIC machines (built specifically for mining) to solve mathematical problems in return for crypto rewards. This assists in the decentralization of said crypto and ensures the security and truth of the blockchain.

Peer to Peer (P2P)
A peer-to-peer (P2P) network structure as it relates to blockchain technology is generally considered decentralized and is designed to operate in the best interest of all parties involved, as opposed to benefitting mainly a single centralized entity.

Private Key / Secret Key
A personal key that serves as the counterpart for the Public Key to be used for decrypting information hashed with the public key.

Public Key
Used to send and receive transactions on a blockchain network. An address is an alphanumeric character string, which can also be represented as a scannable QR code.

Wallet
A cryptocurrency wallet is a device or service that stores users' public and private keys, allowing them to interact with various blockchains and to send and receive crypto assets.