Introduction

Digital currencies are becoming increasingly popular among users to purchase goods and services globally, to transfer to another person, for personal use or to hold as an investment. While there are some benefits associated with digital currencies, there are a variety of risks associated with them. Users of digital currencies can, therefore, become vulnerable to fraudulent or any other criminal behaviour as they may be less circumspect than usual when faced with the promise of high-return investment opportunities.

Note: In South Africa, there is no recourse for those who invest in digital currencies.

1. What is a digital currency and how does it work?

A cryptocurrency is a digital or virtual currency that is underpinned by blockchain technology. A cryptocurrency is difficult to counterfeit because of this security feature and the complex blockchain technology. A defining feature of a cryptocurrency is its organic nature. Members of the virtual community agree to accept digital currency units as a representation of value in the same way that currency is accepted. In contrast to traditional currencies, digital currencies operate without the authority of central banks and are therefore not regulated. The unregulated nature of digital currencies (generally) exposes end-users to risks. One of the greatest risks for end-users trading in digital currencies is the potential to incur sizeable financial losses. This is due to the price volatility inherent in digital currencies as demand and supply (price) are controlled by individuals and could fluctuate wildly. Furthermore, digital currencies could be vulnerable to operational risks. A cyber-attack could potentially wipe out the total value of the digital currency.

The anonymous nature of cryptocurrency transactions makes them well-suited for a host of criminal activities, such as money laundering and tax evasion.

Bitcoin's is an example of a cryptocurrency that has led do to a number of competing cryptocurrencies, such as:

- Litecoin
- Namecoin
- PPCoin
- Ethereum

1.1 Cryptocurrency pros and cons

Cryptocurrencies make it easier to transfer funds between two parties in a transaction; these transfers are facilitated through the use of public and private keys for security purposes. These fund transfers are done with minimal processing fees, allowing users to avoid the steep fees charged by most banks and financial institutions for electronic funds transfers (EFT's).

Central to the genius of Bitcoin is the blockchain it uses to store an online ledger of all the transactions that have ever been conducted using Bitcoin's, providing a data structure for this ledger that is exposed to a limited threat from hackers and can be copied across all computers running Bitcoin software. Many experts see this blockchain as having important uses in technologies, such as online voting, crowd-funding and major financial institutions.

However, because cryptocurrencies are virtual and do not have a central repository, a digital cryptocurrency balance can be wiped out by a computer crash if a backup copy of the holdings does not exist. Since prices are based on supply and demand, the rate at which a cryptocurrency can be exchanged for another currency can fluctuate widely. For example, today one Bitcoin may be worth R5,000, and next week it may be worth R50,000, then the following week it may be worth R3,000.
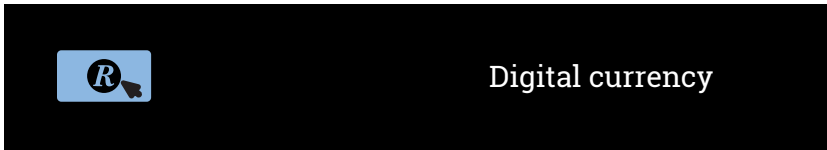
Cryptocurrencies are not immune to the threat of hacking. In Bitcoin's short history, the company has been subject to over 40 thefts, including a few that exceeded a billion dollars in value. Still, many observers look at cryptocurrencies as hope that a currency can exist that preserves value, facilitates exchange, is more transportable than hard metals, and is outside the influence of central banks and governments.

Note: In South Africa, if you invest in cryptocurrency you will have no recourse should you lose your money.

1.2   How it works?

The following process is followed:

- Someone requests a transaction for example online by visiting a digital currency website.
- The requested transaction is broadcast to a peer-to-peer (P2P) network consisting of computers known as nodes
- The network nodes validate the transactions and the user's status using known algorithms
- A verified transaction can involve cryptocurrency contracts, records or other information
- Once verified, the transaction is combined with other transactions to create a new block of data for the ledger for the investor
- The new block is then added to the existing blockchain, in a way that is permanent and unalterable
- The transaction is complete