Cryptocurrency

February 2023

ITSAP.00.650

Cryptocurrencies are **virtual assets** that use cryptography to protect and affirm their ownership. Units of cryptocurrency are called "coins", such as "Bitcoin" and "Ether", and their transactions are generally recorded on their respective blockchains. "Tokens" represent a certain value of "coins" and are used to buy some goods and services. Cryptocurrencies operate on peer-to-peer systems and are not managed by a central authority, such as a bank, government, or country. There are thousands of active cryptocurrencies in existence today, which makes their regulation difficult. The purchase, sale, transfer, and storage of cryptocurrencies are managed through traditional brokers, crypto exchanges, or individuals.

What is blockchain?

A blockchain is a decentralized, digitally distributed ledger that serves as a record of cryptocurrency transactions. Distributed ledgers are storage systems where data is added but cannot be removed. The data is stored at multiple points (or nodes) on a shared network, and often in the form of a blockchain.

Blockchains serve as records of cryptocurrency transactions. These transactions are recorded on blocks with cryptographic signatures and are irreversible. The ledger has many copies held by different entities in various locations, many of which will be involved in collectively validating the accuracy of the data in the new block before adding it to the chain. Once the block of transactions is verified and added to the chain, the information cannot be changed or tampered with.

Each block includes a confirmation of the previous block, strengthening the verification of the entire blockchain. Users must authenticate their transactions with cryptographic keys and may access their assets once their identity is verified.

Crypto mining

Apart from buying coins directly with other cryptocurrencies or legal tender, crypto mining can be another way to accumulate cryptocurrencies. Users with high powered computers or distributed computing capability compete to solve computationally intensive problems and verify currency transaction to add a new block to the chain. The reward is a share of the associated cryptocurrency. This process is known as **proof of work**. Not every cryptocurrency uses this method. Some may employ **proof of stake**, which is a method that randomly selects users to validate transactions.

You should know

Investing in cryptocurrency can be uncertain and comes with a variety of risks including:

- Fluctuations in pricing, due to a range of unpredictable factors like speculation and competition, can frequently impact the value of your cryptocurrency investment.
- Difficulties in liquidating assets as cash, and challenges using cryptocurrencies as many merchants in Canada do not accept them as payment.
- Lack of access to the same protections as fiat currency reduces the ability to submit complaints regarding transactions.
- A crypto wallet is an optional, tamper-resistant device for storing your transactions and credentials, such as your private key and password, If you lose or forget your crypto wallet password, it may be impossible to retrieve your assets.
- Institutions such as the Canada Deposit Insurance Corporation (CDIC) only provide deposit insurances for Canadian dollars and no federal or provincial deposit insurance plans cover cryptocurrency. The owner of digital assets has sole responsibility.
- Transactions are irreversible which creates issues if you do not receive your product or want to stop a payment.

AWARENESS SERIES

Cat. No. D97-1/00-650-2022E-PDF
ISBN 978-0-660-45916-5

What are the cyber security risks?

Phishing and scams

- Phishing attacks are a false representation of a legitimate company, such as a crypto trading platform. The goal is to obtain login credentials from users.
- Giveaway scams are also common, with threat actors posing as well-known investors or celebrities offering to help new investors grow their wealth.
- Threat actors may use a variety of crypto frauds such as fake trading platforms, Ponzi schemes, and tech support scams to deceive people and gain access to their crypto wallets.

Third-party services

- Crypto investors may use third-party applications to manage their digital assets. If a threat actor is able to gain access to the application, user account information will be compromised.

Crypto-malware and bots

- Threat actors use crypto-malware to engage in the unauthorized mining of cryptocurrency on a user's device. The malware is deployed through phishing attacks or malicious web ads that then use a device's resources to generate cryptocurrencies that can be traded or exchanged.
- Threat actors also engage in cryptojacking, which is stealing the private keys of a user's wallet and using them to gain access to their digital assets.
- Trading bots allow for automated trading actions and are commonly used by crypto investors. However, threat actors can make their malware appear as a trading bot program or software. Once users download the fake trading bot, their devices will be infected with malware.

Fraudulent trading platforms

- New trading platforms for investing and trading cryptocurrencies are emerging but they aren't all legitimate. In some cases, cryptocurrency companies initially seemed reputable but were later revealed to be fraudulent, multi-level marketing scams.

Mitigating the risks

Understanding the cyber security risks associated with cryptocurrency will help you protect against fraud, malware, and cyber attacks. There are several strategies you can use to mitigate risks and protect your digital wallet.

- Storing and encrypting private keys or login credentials on a purpose-built tamper-resistant physical device, to manage your cryptocurrency credentials and transactions.
- Using antivirus software, keeping software and operating systems up to date, and using strong passwords.
- Researching companies and their cryptocurrencies thoroughly before investing and keeping up with crypto news stories and announcements from reputable sources.
- Uninstalling unused software and monitoring your device and network activity for abnormalities.
- Ignoring unsolicited offers to invest in cryptocurrencies, as well as suspicious links and ads.
- Installing anti-crypto mining extensions and ad-blockers to protect your device.
- Ensuring that you secure third-party applications through measures such as allow and deny lists as well as separating personal and work data.

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**