INTRODUCTION TO CRYPTOCURRENCIES

INTRODUCTION

This publication provides an introduction to cryptocurrencies that entities may possess or otherwise use when transacting with other parties. While the discussions below focus on bitcoin, the most popular cryptocurrency among entities, the information below also applies to other cryptocurrencies (e.g., Ethereum, Litecoin, etc.) developed using a similar technology (i.e. blockchain).

Entities adopt cryptocurrencies for various reasons, such as:

- For investment purposes
- To attract potential clients/customers (e.g., Generation Z)
- To raise funds directly from the public through an initial coin offering (ICO), as an alternative to traditional securities markets
- To increase their traded market value by developing a reputation of being innovative
- To provide cryptocurrency-related services to individuals or companies (e.g., cryptocurrency trading platform, clearing services, custody and software development)
- To obtain supplies and services from entities transacting in cryptocurrencies.

Cryptocurrencies and blockchain technology challenge the commonly accepted perception of an entity's books and records. The documentation when an entity transacts in cryptocurrencies like bitcoin is solely digital (e.g., encryption keys confirm transactions, asset ownership is presented as a wallet ID, multiple decentralised third-party confirmations are needed, and transaction parties are anonymous to each other). Consequently, an entity transacting in cryptocurrenices needs to implement different procedures and controls to ensure such transactions are appropriately authorised, completely and accurately recorded, and properly valued in accordance with the entity's financial reporting framework. An entity also needs to maintain adequate control over its cryptocurrency wallets to safeguard those assets.

The paragraphs below provide background information to help you understand how bitcoins and other cryptocurrencies work.

DIGITAL CURRENCY, CRYPTOCURRENCY AND BITCOIN

Digital currency is a type of money available only in digital form and kept in a digital wallet, resembling physical currencies but allowing instantaneous transactions and borderless ownership transfer. The money balance is recorded electronically in a digital wallet or another device either centralised (e.g., central bank issued digital base money), where there is a central point of control over the money supply, or decentralised, where control over the money supply can come from various sources (e.g., virtual currencies, cryptocurrencies).

IN THIS ISSUE

Cryptocurrency is a digital currency that exists in a hexadecimal format designed to work as a medium of exchange that uses asymmetric cryptography[1] to secure its transactions, to control the creation of additional units, and to verify the transfer of assets. The decentralised control of each cryptocurrency works through a blockchain technology, a distributed digital ledger in which transactions made in bitcoin or another cryptocurrency are recorded chronologically and publicly (i.e. public transaction database).

Bitcoin is the first cryptocurrency, created in 2009 and initially defined as a chain of digital signatures. The bitcoin network is a peer-to-peer network that runs on a distributed self-clearing ledger (i.e. blockchain). Units of currency that run on the bitcoin network are called bitcoins, which are used to store and transmit value among network participants. It has a limited and finite supply of 21 million bitcoins, and as of December 2017, approximately 17 million bitcoins were circulated worldwide.

The following discussion focuses on bitcoins but the principles may be applied, where relevant, to other cryptocurrencies that you transact or invest in.

Bitcoin balances are recorded in ledgers that are accessed through public and private keys. Public and private keys are long strings of numbers and letters linked through a mathematical encryption algorithm which created them (ECDSA is a cryptographic algorithm used by bitcoin).

- The public key, an identifier of 26-35 alphanumeric characters beginning with the number 1 or 3, known as a bitcoin public address, serves as the address of the ledger, which is published to the world and to which others may send bitcoins (comparable to a bank account number)
- The private key, a series of 64 letters and numbers (a 256-bit number), is a secret string used to authorise or 'sign' bitcoin transactions by the sender (comparable to an ATM PIN).

Bitcoin addresses are designed to be used only once for a single transaction; re-used addresses may interfere with the participant's privacy and security. For instance, whenever an address is re-used, the beneficiary can uncover information about the sender's identity.

1 Asymmetric cryptography uses public and private keys to encrypt and de-crypt data. The keys are large strings paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept secret; it is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.

TYPES OF BITCOIN WALLETS AVAILABLE

A bitcoin wallet is a software that saves the public key (bitcoin address) and private key. Bitcoin wallets facilitate sending and receiving bitcoins, give ownership to a bitcoin balance and record all transactions. You may choose to have different wallet types or more than one wallet as a result of security considerations, specific purpose wallets or diverse business activities. Each digital wallet has a unique wallet identifier (wallet ID), which is a string of 36 letters and numbers that is similar to a username you may use to access email or an application. To log into a wallet, you use a wallet ID, password, and if enabled, two-factor authentication. The wallet ID is different than a bitcoin address and cannot be used to send or receive bitcoins.

Common types of bitcoin wallets are:

Desktop wallet – Software installed on a desktop computer that enables the user to create a bitcoin address for sending and receiving bitcoins and stores the private key. A desktop wallet keeps the complete history of bitcoin transactions archived in blocks on the local hard drive.

Mobile wallet – Software installed on a smartphone that can carry out the same functions as a desktop wallet. In addition, a mobile wallet facilitates payments in physical stores by using NFC scanning of a QR code[2].

Web wallet – An online wallet managed by a third-party and accessible through a browser. Transaction history and keys are kept at the service provider; the user can back up the wallet at their email address or on a local hard disk.

Hardware wallet – An electronic device built for the sole purpose of securing bitcoins, it is kept offline and only connected to the web to perform bitcoin transactions.

Paper wallet – Printed paper usually in QR code which contains the public key and private key.

Entities usually use desktop, mobile or web wallets for current payments, which can be compared to current bank accounts. Hardware or paper wallets are often used for maintaining larger amounts for a longer period, which can be compared to longer term bank deposits.

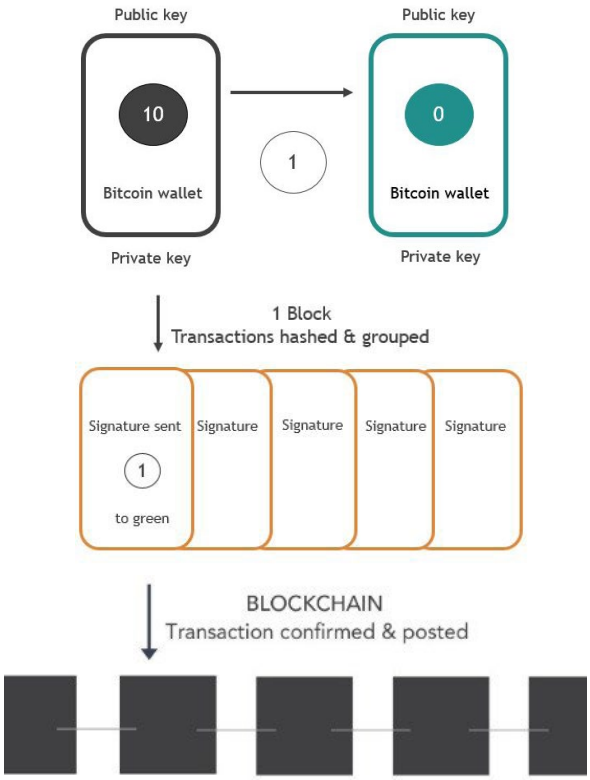
2 A Two-dimensional barcode machine-readable optical label that contains information about the item to which it is attached (an example of QR code is:)

UNDERSTANDING BITCOIN TRANSACTIONS

A bitcoin transaction is a piece of data signed by the private key sent to a public key / bitcoin address through the public blockchain protocol over the web, containing an amount of bitcoin. If valid, it transfers ownership and ends up in a blockchain block. The bitcoin amount is sent to a public address and locked to the receiving address associated with the wallet. Transfer of bitcoin is possible only from funds previously received and currently present in a digital wallet.

When a sender sends bitcoin, a bitcoin transaction is created by the sender's wallet and broadcast to the network. Bitcoin nodes[3] on the network will relay and rebroadcast the transaction, and if the transaction is valid, the nodes will include it in a blockchain block, usually within ten minutes. At this point, the receiver can see the transaction amount in their wallet.

The signed transaction is hashed[4] and grouped with multiple other similar transactions into a block, along with all the corresponding transactional data (i.e. block ID, timestamp). Blockchain data is published once the block is hashed, and it is permanently published to the blockchain.



3 A node is a computer connected to the bitcoin network. It supports the network through validation and relaying of transactions while receiving a copy of the full blockchain itself.

4 A hash algorithm turns an arbitrarily-large amount of data into a fixed-length hash and acts like a wax seal on the bitcoin transaction since the same hash will always result from the same data, but modifying the data by even one bit will completely change the hash.

RISK IDENTIFICATION AND ESTABLISHING INTERNAL CONTROLS

Cryptocurrencies are at an early stage in their development and the way they work is complicated. New cryptocurrencies are becoming available all the time, with different features and processes. If you wish to transact in cryptocurrencies, you need to invest time and/or hire consultants to ensure you understand how they work and the risks you may be undertaking.

Entities who use bitcoin or other cryptocurrencies are exposed to internal business risks (e.g., loss of bitcoin wallet, invalid transfers or fraud) and external business risks (e.g., cyberattack, new government regulations, and high volatility in valuation). These business risks are higher as your use of cryptocurrencies in your operations increases.

You need to identify the degree of risk your entity is exposed to and establish adequate internal controls relating to cryptocurrency processes and safeguarding. The appropriate mix of internal controls will include IT controls and manual controls over relevant business processes.

There are two primary operating models related to cryptocurrency transactions:

- Outsource the wallet custody and clearing process to a third-party company which converts the amount from cryptocurrency to the local currency in real-time, and after the cryptocurrency is received, it transfers the funds directly to your bank account in your local currency.
- Manage your own digital wallet, which is usually installed in the local network, and internally monitor and report on the cryptocurrency transactions.

You also need to consider how cryptocurrency transactions interface with your other accounting applications. The digital wallets used to hold and perform cryptocurrency transactions may be completely separated from your other accounting applications and require manual entry of such transactions. In other cases, transactions and invoices may be transferred automatically from the point of sale (POS) application or the digital wallet directly to your general ledger.

The nature of risks and the processes and controls needed in these situations is different as illustrated in the table below.

RISKS	
Outsourced wallet custody and clearing	**Internally managed digital wallet**
The service provider's creditability and stability are key business risks to evaluate. Since transactions are automatically converted to local currency and transferred to your bank account (net of provision) soon after they occur, in case of a cyber attack at the service provider, losses are expected to be relatively low. The service provider maintains your wallet ID which is linked to your company details and your bank account data, so security of those items is at risk.	Security and other operative risks are retained by you, such as: • Loss of a wallet (i.e. accidental erasure, malware attack or other circumstance) • Loss of the wallet's access credentials (i.e. username or password), preventing access to the cryptocurrency • Unauthorized fund transfer by a person who holds the access credentials • Recording unconfirmed cryptocurrency transactions in the accounting system • The wallet ID is likely linked to an email account, without additional identification details.

POSSIBLE PROCESSES AND CONTROLS	
Outsourced wallet custody and clearing	**Internally managed digital wallet**
General	
Evaluate the risks arising from the agreement with the service provider.	Identify the type of digital wallets you are using and assign responsibility to particular personnel for this process.
Logical access controls	
• Validate that only authorized employees have access to the online services • Review logical access controls (e.g., authentication) to the online services • Review that two-factor authentication is implemented (i.e. one-time PIN or token) • Verify that passwords and usernames are not saved in the browser.	• Establish policies for how the digital wallets are registered (e.g., company email or private mail) • Determine who possesses the credentials for authenticating to the wallet (wallet ID, password, access to registered email, recovery words, etc.) • Determine if two-factor authentication is to be used • Establish access rights and validate that access is restricted to only authorized personnel • Ensure that a hardware wallet (if used) is stored in a secure safe and protected by PIN code • Determine from which devices access to the wallet is allowed (e.g., PC, smartphones or tablets) • Set policies related to a robust password and that passwords are replaced periodically • Establish policies on multiple signatures where relevant • Verify compliance with all the policies and controls established.

Outsourced wallet custody and clearing	Internally managed digital wallet
Program changes	
• Ensure your agreement with the service provider regulates software maintenance • Monitor the list of incidents and cryptocurrency losses and their status/resolution • Establish controls related to changes in parameters or configuration settings (i.e. bank account, dates, commission).	• Understand the types of digital wallets in use and ascertain if the version is updated periodically • Determine if you want to implement Adblock, real-time antivirus monitoring, and determine if all patches have been installed on equipment where the wallets reside • Monitor the list of incidents and cryptocurrency losses and their status/resolution.
Data processing management	
• Establish controls over the data transfer process to the accounting application • Perform periodic reconciliations between the service provider's reports and the accounting application.	• Establish policies on using a different bitcoin address for every transaction • Establish controls over the recording of cryptocurrency transactions in the accounting system • Perform periodic reconciliations between the digital wallet and the accounting application • Establish controls related to the invoicing process and money requests received (i.e. include details about the service or products, including the invoice number, and that the invoice is linked to the dedicated public address) • Verify compliance with all the policies and controls established.
Other	
• Determine if the service provider has implemented security controls to prevent exposure of your information or stealing of cryptocurrencies.	• Establish policies related to backup of wallets and that they are kept offline • Review that the firewall is configured adequately to eliminate unwanted network access • Verify that passwords and usernames are not saved in the browser • Perform periodic vulnerability scans.

CONCLUSION

Using bitcoins or other cryptocurrencies in your business activities may provide unique opportunities to your business, but it also comes with some unique risks. It is essential that you understand those risks and establish appropriate processes and controls to mitigate those risks.

If you have questions relating to this topic, contact your local BDO office for assistance.

GLOBAL CONTACT:
AUDIT@BDO.GLOBAL