BLOCKCHAIN

Posted on September 1, 2017

Category: CNPupdates

Date Published: 1 September 2017

Author: Quek Li Fei.

Introduction

In our previous articles (which can be accessed here and here), we introduced cryptocurrencies (with a focus on Bitcoin) and highlighted some legal, regulatory and tax issues relating to Bitcoin.
In this first article of a three-part series, we examine the technology underpinning Bitcoin (such technology known as blockchain) and how blockchain is currently used around the world in various industries including banking, finance, music, healthcare and supply chain. In the second article, we will discuss initial coin offerings ("**ICO**") – including the components of an ICO, a brief overview of the ICO process, the risks typically involved in an ICO and regulatory aspects of an ICO. The third and final article will cover the current tax and regulatory treatment of cryptocurrencies in Singapore and a few other major jurisdictions.

The blockchain technology

The blockchain is a decentralised and distributed ledger (or database) which is used to record transactions between two parties in a verifiable and permanent way. Being a decentralised and distributed database (i.e. storing data across the network as opposed to centrally) significantly reduces the risk of data hacking or corruption, and allows for better transparency and efficiency as the records are available to all users of the network.

Blockchain is the technology underpinning Bitcoin. It holds the transaction history of all Bitcoins in circulation and replaces the conventional trusted third party (i.e. banks) in a transaction. The following is the chronology of a Bitcoin transaction:

1. **Transaction request**: Person A wishes to send money (i.e. Bitcoin) to Person B.
2. **Block configuration:** the transaction is represented on the network as a "block".
3. **Broadcast:** this block is broadcasted to every party in the blockchain network.
4. **Mining:** where users in the network will verify and affirm the validity of the block/transaction (in exchange for crypto coins for each successful mining) before the same is added to the blockchain – hence fulfilling the role of the trusted third party.
5. **Addition to the blockchain:** The valid transaction block will then be added to the existing chain of blocks (i.e. past transactions), which then provides an indelible and transparent record of transactions.
6. **Completion of the transaction:** the Bitcoin is moved from Person A's account to Person B's account.

Advantages of blockchain

As can be seen, the blockchain and the mining process allow Bitcoin transactions to bypass the need for a third-party intermediary to verify or transfer ownership of the Bitcoin. In addition, blockchain technology presents the following advantages:

1. **Transparency:** The blockchain is run by a decentralised network of users, where transactions are broadcasted to everyone, ensuring transparency. Transactions are processed by all the users in the network creating a consensus mechanism such that every user creates the same shared system of record at the same time.
2. **Up-to-date:** The blockchain updates transactions in real-time. Each node in the network comes to the same conclusion, each updating the record independently, and instead of a master copy, the most accepted record becomes the de facto official record.
3. **Durability:** There is no single user or entity in charge or control of the blockchain.
4. **Verifiable:** All transactions are kept on a public ledger.
5. **Incorruptible:** Past transactions cannot be tampered with.

Blockchain has introduced a fundamentally new way of transacting and maintaining records online, for example, allowing people and banks to directly exchange money and assets like stocks and bonds, amongst other things, potentially without having to rely on a long chain of central authorities and expensive middlemen thus effectively dispensing with a need for a trusted party to facilitate the digital relationships.

Application of blockchain in various industries

Banking: Banks are looking at the blockchain technology to help disseminate "know-your-customer" compliance information more easily. This aims to resolve the issue faced by the current KYC procedure, namely that every time a new consumer goes to a bank, the customer is KYC vetted even though the customer has already been verified as a customer at another bank. In addition, International Business Machines Corp (IBM) is in the process of building a new blockchain that will be used by seven of Europe's largest banks to facilitate international trade for small and medium-sized enterprises. The seven banks are Deutsche Bank, HSBC, KBC, Natixis, Rabobank, Societe Generale and Unicredit.

Finance: In finance, the focus is on changing the systems currently being used by big Wall Street traders to buy and sell sophisticated assets like syndicated loans and corporate bonds. Resources are being channelled to create a new kind of blockchain to allow a more expedient trading of stocks in private companies, replacing the existing system in which private companies issue and trade shares using paper certificates, a process that means that even basic trades can take weeks to complete.

Music: In the music industry, Billboard has announced that several start-ups are trying to use a digital ledger like blockchain to help keep track of musical downloads and distribute royalties to artists without having to rely on a central record keeper.

Healthcare: In the healthcare sector, digital medical records in the United States are scattered across myriad hospitals, private practices, labs, pharmacies and private companies. Blockchain is being used to minimise this fragmentation, such that medical records can be more easily accessed and transferred across organisations, resulting in an improved healthcare system across the country.

Supply chain: The supply chain sector has identified blockchain technology as being able to help guarantee the authenticity of supplies, as the technology will allow more visibility through the monitoring of the movement of goods right from its source to its destination. As the origins of supplies can be traced, this results in increased accountability. An overall improvement in transparency and elimination of tampering is expected, resulting in safer food products on the shelves of supermarkets.

Glossary of common key terminology

Ether (ETH): the cryptocurrency used on the Ethereum blockchain; it can also be used to pay transaction fees and costs on the Ethereum network.

Ethereum: the world's second-largest cryptocurrency (second to Bitcoin) based on market capitalisation as at the date of this article.

Mining: the process of verifying and affirming the validity of the block/transaction (in exchange for crypto coins for each successful mining) before the same is added to the blockchain.

Smart contracts: self-executing and self-enforcing contracts which terms are recorded in a computer code

language (instead of legal language) and exist across the blockchain network. Allows trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism.

Token: what is secured behind the private keys inside a cryptocurrency wallet. There are two main types of tokens, namely:

1. "Intrinsic" or "native" or "built-in" tokens:
    - Examples include BTC (on the Bitcoin blockchain) and ETH (on Ethereum).
    - It is not pegged to or backed by any bank-issued currency.
2. Asset-backed tokens:
    - These are claims on an underlying asset (e.g. currency and precious metals) from a specific issuer.
    - Transactions of asset-backed tokens are passed along similarly like intrinsic tokens and are recorded on the blockchain.
    - To claim the underlying asset, the token is sent to the specific issuer, and the issuer sends the token-holder the underlying asset.

Wallet: the Bitcoin/cryptocurrency equivalent of a bank account. Key features include:

1. Similar functions to that of a bank: storage, withdrawal, transfers.
2. Stores the private keys that you need to access a Bitcoin address and spend the funds.
3. *Five main types of wallets: desktop, mobile, web, paper and hardware*