OGCIO Primer: Blockchain, Distributed Ledgers and Cryptocurrencies

and what has this to do with Bitcoin?

This primer is intended to give a brief and basic overview of blockchain, distributed ledger technology and cryptocurrencies (such as bitcoin). It is not intended to be exhaustive and does not go deep into the technology details.

Traditional Ledgers

Traditionally, asset and transaction information was stored within physical books or ledgers to independently reference previous actions internally and externally. Ledger entries typically record transactions that involve the transfer of an asset from one party to another. As technologies advanced, physical books were translated into digital ledgers.

A trusted third party, an intermediary, holds these ledgers and ensures that they are up-to-date. For example, banks use ledgers to maintain records of account transactions, and governments use them to keep records of land ownership.

These ledgers are centralised – there is an intermediary, trusted by all users, who has total control over the system. In addition, how the ledger and its data function is not fully visible to its users. Digitisation has made these traditional ledgers faster and easier to use, but they remain centralised and opaque.

Blockchain

Blockchain is an alternative computing approach that uses distributed and decentralised computing networks to offer (potentially) greater levels of security and lower costs than traditional models. A blockchain is a continuously growing list of electronic records, called blocks, which are linked and secured using cryptography (i.e. by transforming data into formats that cannot be recognised by unauthorised users). A block is similar to records being collated on a single sheet of paper. Each block is added as the latest link on a long 'chain' of historic transactions. The blockchain is a trusted record of transactions among parties.

Blockchain offers the same record-keeping functionality as traditional ledgers but without a centralised structure (intermediary). How can it be certain that a transaction is legitimate when there is no central authority to check it? Blockchain technology offers a way for untrusted parties to reach agreement ("consensus") on a common digital history. This is achieved by decentralising control of the ledger. The ledger is maintained collaboratively by a decentralised network of computers. This approach is generically referred to as **Distributed Ledger Technology**. A distributed ledger is set of records that can be shared across a network of multiple sites. All participants within a network can have their own identical copy of the ledger. The security and accuracy of the ledger are maintained cryptographically.

A blockchain is a type of distributed ledger. It avoids one centralised location and the need for intermediaries to perform transactions. It has been designed to replicate data among participants in real time, ensuring all parties operate off a copy of the same ledger at all times. Adding a new block to the chain means updating the ledger that is held by all users. The transactions are immutably recorded across all parties, using cryptographic trust and assurance mechanisms. Users only accept a new block when it has been verified that all of its transactions are valid. If a discrepancy is found, the block is rejected. Otherwise, the block is added and will remain there as a permanent public record.

Cryptocurrencies

There are several possible application areas of blockchain technology, currencies being just one. **Bitcoin** is an online equivalent of cash and is the most well-known of many virtual currencies – referred to as **cryptocurrencies** – implemented via a blockchain. Others include Ethereum, Litecoin, and Dash.

Bitcoin is a decentralised, public ledger using blockchain technology. There is no trusted third party controlling the Bitcoin blockchain. Instead, anyone can read it, write to it, and hold a copy. The Bitcoin blockchain tracks a single asset: bitcoin. The blockchain has rules, one of which states that there will only ever be 21 million bitcoin. All participants must agree to Bitcoin's rules in order to use it. But how does Bitcoin establish consensus among untrusted parties? It does this by incentivising Bitcoin participants, known as "miners", to verify each transaction and compete to add it into a block with other transactions. Miners are required to solve a mathematical puzzle requiring a lot of computational power before being able to add a block to the chain of prior blocks. Others in the network check the miner's work and once verified, the block is added to the blockchain. The miner receives a reward, paid in bitcoin.

End users are removed from this level of detail when buying or spending bitcoin. Bitcoin, or more usually small fractions of bitcoin, are generally bought via a third-party service (bitcoin wallet service) and spent at online businesses (limited choice currently) that accept them for payment. Bitcoin can be sent to anyone with a Bitcoin wallet and can be sold through the wallet service.

Finally

Bitcoin is Blockchain's best-known, most used and highest-impact application. However, the potential impact of Blockchain and Distributed Ledger Technology generally, is seen as much greater and wider than virtual currencies. These technologies can provide new ways of guaranteeing ownership and provenance for goods and intellectual property. Blockchain technologies offer a fundamental departure from current transaction and record-keeping mechanisms. For public services, areas often suggested include land transactions, patents, intellectual property rights, identity management and voting procedures. However, blockchain technologies are relatively new and are evolving and progressing at a rapid pace. The technologies would not yet be seen as enterprise ready. There are concerns around scale, scope, performance, efficiency, and operational manageability. That said, many business and government organisations have begun experimenting and examining the potential use of this technology to provide new applications and tools to deliver services.

February 2018.

Further Reading

- How does the Blockchain Work? (2017) https://medium.com/blockchain-review/how-does-the-blockchain-work-for-dummies-explained-simply-9f94d386e093
- EU Blockchain Observatory and Forum (2018) http://europa.eu/rapid/press-release_IP-18-521_en.htm
- Practical Blockchain: A Gartner Trend Insight Report (2017 – requires subscription) https://www.gartner.com/document/3628617
- How blockchain technology could change our lives – European Parliament Think Tank (2017) http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_IDA%282017%29581948
- The future of financial infrastructure – WEF (2016) http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf (World Economic Forum)