Assignment 2

**IT Technologies: Blockchain and Cryptocurrencies**

**What does it do?**

Blockchain is a revolutionary technology that was invented in 1991 as a way to timestamp digital documents to prevent backdating or tampering. Blockchain wasn’t commonly utilised until it was adapted by Satoshi Nakamoto in 2009 to run the first digital cryptocurrency, Bitcoin.

Blockchain is a backbone infrastructure which has distinct advantages over other technology by being incredibly secure, and it can be adapted for many different purposes. Blockchain is such a versatile infrastructure, it will enable advancements such as secure online voting systems for elections, health records, land and property records and banking.

The concept of cryptocurrency is to create a ledger (block) that records financial transactions of a digital currency. The ledger is decentralised, so that multiple nodes will have an identical copy of that ledger, so unauthorised changes are almost impossible. It does away with traditional intermediaries, who would have a central ledger which could be more easily tampered with and who would charge fees for transactions. By distributing the ledger, it ensures that there is no one central point of attack. This makes the blockchain incredibly secure and means that there are no middlemen, like banks, involved in the transfer of funds between two people.

A block is made every 10 minutes containing all the transactions a specific digital currency, comprised of the amount of the transaction, the two parties involved and their digital signatures. Thousands of mining computers (nodes) all over the world work to verify the transaction and signatures, and once they have reached consensus, they authenticate the block. The first computer to compute the data is rewarded with digital currency and adds the block to the chain. When the block is added to the chain, it joins to the hash of the previous block and it creates a hash ready to join to future blocks. The hash is unique to each block, as it is derived from the data within the block. The cryptographic hash is made of 256 bits, making it infeasible to re-calculate hashes in reverse. When a new block is added to the blockchain, every ledger is updated, and nodes check that the updated ledgers are all the same, and as long as 51% agree, they reach consensus. This prevents tampering and data corruption.

This is what makes blockchain so secure. Any changes to the data inside a block will ‘break’ the chain, as the hash will change and it won’t match the next block, invalidating them. If someone was to tamper with the data inside a block, they would need to calculate a new hash for each block, one for every 10 minutes, back until the start of the chain. A hacker would need to update at least 51% of the nodes simultaneously, making it very improbable.

To combat possible tampering, blockchain implemented the 10-minute timer called Proof-of-Work, which would slow a potential hacker by only allowing 1 hash change every 10 minutes.

One major advantage of this technology is the security of a digital signature, which assigns a ‘Shared key’ (or Public Key) and a ‘Secret Key’ to each person. The Secret key is used in conjuncture with the message or document contents to create a digital signature. The Public key can then be used to verify the authenticity of the signature. The signature itself is made of 256 bits, resulting in 2^256 possible combinations, making it almost impossible to calculate the secret key.

There a currently thousands of Cryptocurrencies using blockchain, and these are not affiliated or owned by a government or bank. The value of these cryptocurrencies’ changes based on trade, similarly to the stock market. This technology is available now and is open to any consumers to use.

**What is the likely impact?**

A potential impact of this technology is prosperity of poor and vulnerable people. The largest transfer of funds between developed nations and developing nations is remittance, at 600 Billion dollars a year. This is far more that corporate investment or foreign aid. People that work in developed countries and transfer money to their family members in developing nations often use companies such as Western Union, which charge 10% of the transaction and take 5-7 days to deliver. Utilising a cryptocurrency on Blockchain, this transaction can be close to instantaneous, with a fee as little as 2%. This will aid people who need that money to get to their family members, not ending up expanding the profits of large corporations, leading to the growth in prosperity of the poorest people in society.

The Australian stock exchange (ASX) is in the process of changing its infrastructure to blockchain, which will be implemented over the next few years. This will enable automated proxy-voting, and use smart contracts to automate business processes, making them more efficient.

There are many future possibilities with Blockchain, such as a voting system that can’t be tampered with. This could give hope to people in nations with corrupt governments to be able to vote with confidence in elections. It may also be possible for a government which has lost the faith of its people may gain back that trust with a fair election system.

Companies such as Airbnb and Uber are services that link people together and facilitate a transaction as the middleman. Blockchain can do most of the same functions as these companies who make extraordinary profits and using blockchain instead could cost less to consumers and grant higher earnings to workers.

Some Musicians are rejecting traditional music industry distribution, which has greatly diminished their profit from music sales, and are making their music available on a blockchain smart contract, which makes their music accessible to consumers. This ensures the payment reaches the musician directly. Jobs in music industry distribution for those who have made the most profit from sales will be affected by these smart contracts on blockchain, as will most middlemen or intermediaries in a lot of different industries.

Land titles is another area that would benefit from records being secured on a blockchain. As titles can be disputed, assets can be stripped from people whose records have been altered. Securing their future prosperity is possible through blockchain.

**How will this affect you?**

The impact this will have on my life is ensuring that records have not been tampered with, as blockchain can be used for any form of record keeping, such as medical records, financial transactions and taxation records. Blockchain can be used to trace ownership of assets. Money transfers can be done quickly and easily, and without exorbitant fees.

Smart contracts can be used on blockchain to conduct simple transactions such as music downloads, where the consumer can ensure that profits go directly to the artist who created the product. These can be used for any simple transaction and would allow artists to flourish in the commercial industry.

Another change would be if the world was to shift to a single, global currency. A global currency should be a cryptocurrency, as they are not owned by a for profit bank or government. This would do away with fluctuating exchange rates between different currencies, needing to change cash when travelling and would take the uncertainty out of price when buying items from other countries. This could eliminate the need for cash, which would have significant implications, but could make money more secure, as physical cash is untraceable.

Blockchain will enable more versatility in the future, and as more users experience the potential that blockchain has to offer, the more uses may be discovered.

**References**

Chinchilla, C., 2019. *White Paper - The Next Generation Smart Contract And Decentralized Application Platform*. [online] GitHub. Available at: <https://github.com/ethereum/wiki/wiki/White-Paper> [Accessed 10 April 2020].

Eyers, J., 2019. *How ASX's Blockchain Will Change Finance*. [online] Australian Financial Review. Available at: <https://www.afr.com/companies/financial-services/explained-how-asx-s-blockchain-will-change-finance-20191025-p534by> [Accessed 5 April 2020].

Harper, S. and Stornetta, W., 1991. *How To Time-Stamp A Digital Document*. [online] SpringerLink. Available at: <https://doi.org/10.1007/BF00196791> [Accessed 10 April 2020].

Harvard Business Review. 2020. *The Truth About Blockchain*. [online] Available at: <https://hbr.org/2017/01/the-truth-about-blockchain> [Accessed 10 April 2020].

Investopedia. 2020. *Block (Bitcoin Block)*. [online] Available at: <https://www.investopedia.com/terms/b/block-bitcoin-block.asp> [Accessed 10 April 2020].

Lantz, L., 2020. *The Blockchain Explained Simply*. [online] TedxHamburgSalon. Available at: <https://www.youtube.com/watch?v=KP\_hGPQVLpA> [Accessed 5 April 2020].

Nakamoto, S., n.d. [online] Bitcoin.org. Available at: <https://bitcoin.org/bitcoin.pdf> [Accessed 10 April 2020].

Savjee.be. 2017. *How Does A Blockchain Work*. [online] Available at: <https://www.savjee.be/videos/simply-explained/how-does-a-blockchain-work/> [Accessed 10 April 2020].

Tapscott, D., 2020. *How The Blockchain Is Changing Money And Business*. [online] Ted Talk. Available at: <https://www.youtube.com/watch?v=Pl8OlkkwRpc> [Accessed 3 April 2020].