THE FUTURE OF THE WESTERN CAPE AGRICULTURAL SECTOR IN THE CONTEXT OF THE 4TH INDUSTRIAL REVOLUTION

Review: Blockchain

October 2017

USB
University of Stellenbosch Business School

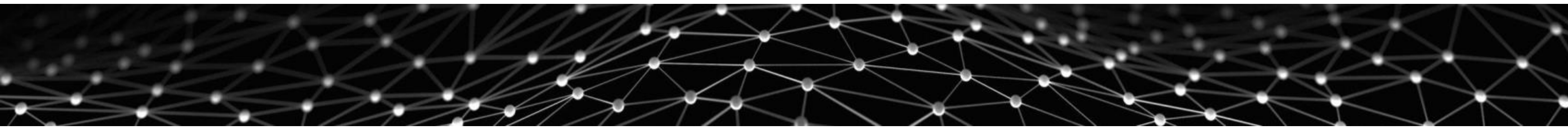

Table of Contents

1. What is Blockchain?

Introduction

Blockchain is a term used to describe distributed ledger technology (DLT), which is, in essence, the opposite of having a centralised record keeping system, where a trusted third party is used to provide the 'true version' of recorded history. A blockchain is a decentralised, peer to peer network. Blockchain was originally developed for the Bitcoin use case by the person, or group of people, going by the pseudonym, Satoshi Nakamoto.

Perhaps the easiest way to understand blockchain, at a high level, is to imagine a spreadsheet which is distributed across thousands of computers connected via the internet. No single, centralised, copy of this exists for a hacker to corrupt. All the holders of the spreadsheets then receive potential amendments from other users of the spreadsheet by broadcasts sent out to the network. Each holder checks that the amendments are valid, based on the previous confirmed entries in the spreadsheet, and then adds it to the record if it meets the criteria. In this way, a distributed ledger is maintained. Computers connected to the blockchain network, running the associated software are called nodes. These are the computers that validate transactions.

Information held on a blockchain exists as a shared, and continually reconciled, database. This is a way of using the network that has obvious benefits. The blockchain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralised version of this information exists for a hacker to compromise. Hosted by thousands of computers simultaneously, its data is accessible to anyone on the internet[1]. There are many use cases, which are discussed below, where blockchain creates efficiencies that are not possible in centralised systems.

How does blockchain work?

While it would be difficult to concisely explain the intricacies of how a distributed ledger works. This review will attempt to give a brief description of how the network fits together and maintains itself over time, by using the Bitcoin example. For technical details about DLT, see the appendix for links to resources.

Transactions

To understand how Bitcoin (and other blockchains function), it is helpful to start with a transaction and follow how it moves through the network to eventually be recorded, permanently, in the blockchain.

Firstly, to send and receive Bitcoin, an electronic wallet is needed. A wallet is a program which manages a person's addresses (the equivalent of a bank account number) using corresponding private keys to authorise transactions from those addresses (much like you use your password to authorise a bank transfer). The software is connected to the Bitcoin network and is able to send and receive broadcasts from that network. In this way it initiates transactions and updates its knowledge of the balances in the addresses when transactions are sent to those addresses.

Bitcoin, like other digital representations of value, is not tangible, and there is no single location containing a Bitcoin. Even your wallet does not contain Bitcoins. A Bitcoin is simply an unspent output of a previous transaction sent to an address. All your wallet holds is your private keys and facilitates your interaction with the network. Bitcoin exists on the blockchain as the sum of input transactions minus the sum of output transactions . You do not even need a computer to hold your private keys. If you knew your address and private key by memory, you would still be able to receive Bitcoin to that address. However, you would need a computer to send those coins.

When a user, let's call her Alice, wants to send Bitcoin to another person, Bob, she must use her wallet to broadcast this transaction to the entire network. If the transaction is valid it will be permitted into the pool of transactions waiting to be processed. The validating nodes (miners) on the network will add hers, and many other transactions, into a block and attempt to find what is called a proof-of-work. This is a computationally intensive solution to a mathematical problem. When the block has been found, it is broadcast to the network and if the majority of nodes accept that the proof is valid, which is easily verified (although not easy to create), it will be added to the blockchain (consensus version of the history of transactions). Due to this process of validation taking approximately 10 minutes, Bitcoin transactions are not instant. After the block has been added to the blockchain, the transaction is complete and can be independently verified by Bob, who can look up his address in the blockchain and see that Alice has sent him Bitcoin.

While we have used Bitcoin as an example here, there are many other blockchains which use different currencies, such as Litecoin, Ripple, and Ethereum, to name a few. Furthermore, the units of value need not be money. The ledger tokens are simply units of account for the purpose of maintaining the ledger. Other information such as text or images and other data can be stored on a blockchain instead of simply transactional information.

Mining

Mining is the term used to describe the process of coin creation on the Bitcoin network. Much like gold is mined by expending resources to remove it from the ground. Bitcoin is mined by validating transactions on the network, expending CPU time and electricity, and finding a proof-of-work. When a new block is found, included in that block is a reward of new Bitcoin allocated to an address controlled by the miner.

Nodes on the network, called miners, compete to mine blocks by using specialised computers to solve for the next proof-of-work first. They do this through a process called hashing. Hashing entails processing the transactions combined with the previous block's hash and a random variable through a cryptographic algorithm. The output of this process is a hash, which is a unique fixed length string of characters representing all the information passed through the hash function. This process also ensures that each transaction is timestamped and joined to the history of previous transactions in a way which is computationally impractical to tamper with. In this way there is a true version of the history of the order of transactions. The node that first solves the proof will add that block to its local version of the blockchain and then broadcast this to the network, if the other nodes on the network agree that this is a valid block, they will abandon the block they were working on and accept that chain as the latest version of the blockchain. They will start mining the next block to add to that chain. If it is not valid, they will reject the block and continue looking for the proof-of-work. The miner that produced the invalid block would thus have wasted computing resources in trying to append an invalid block to the chain.

Security

Due to each block being inextricably linked to all previous blocks through the hashes, Bitcoin is tamper resistant. To change a block in the history of the chain would involve having to redo all the proof-of-work from that time in history onwards and then having to mine blocks faster than the rest of the network can, so that your dishonest version of the chain is the longest chain and thus accepted as the true version.

The longest chain should be the valid chain, because the longer a chain is, the more computing power was needed to produce chain. If a chain is the longest, it stands to reason that the majority of nodes, by computing power, accept that as the true history of the chain (as they have committed resources to mining on it). Assuming that at least half of the mining power is honest, that chain will be valid. In the Bitcoin network, double spending a coin (changing the history), would entail having more than 50% of the computing power linked to the network. This would be very expensive to achieve, and any wealth gained would likely be eradicated by undermining the security of the network. It would also most likely be more profitable to use that mining power to accumulate Bitcoin through validly mining coins faster than anyone else can.

It is through both the computationally impracticality of corrupting the ledger as well as the lack of incentive to do so, that the integrity of distributed ledgers are secured.

2. Why is blockchain important now?

Blockchain technology and its adoption are incredibly important developments in the way we record anything of value. It is a way to create trust without having to trust anyone. Before blockchain technology, there was no way for two parties to send value to each other, via the internet, without using a third party intermediary that they trusted[2]. Peer-to-peer transactions were only possible with a cash transfer in person. Bitcoin changed this, and created a true internet currency that is not able to be manipulated by any central bank or practically, by any person. It created an open source and efficient system to securely record anything of value, from money to land ownership. The emergence of a record keeping system as robust as the internet itself, is pivotable and enables a new level of freedom from intermediaries and control. Blockchain will create a new level of accountability and transparency that will reduce fraud, corruption and even poverty.

Blockchain has created a new internet, the internet of value. Blockchain applications such as cryptocurrencies, tokenisation, distributed title registries and crowdfunding, will undoubtedly change the way the world interacts, stores information and even computes. The technology is still very immature and many of the most valuable use-cases have yet to be discovered. Much like we could not foresee the incredible value the internet unlocked in the 80s, we do not know how blockchain will be used in 30 years time.

3. What are the applications of Blockchain today?

There are many applications of the blockchain, not all of which will be able to be discussed here. Some of the important applications of blockchain are mentioned now.

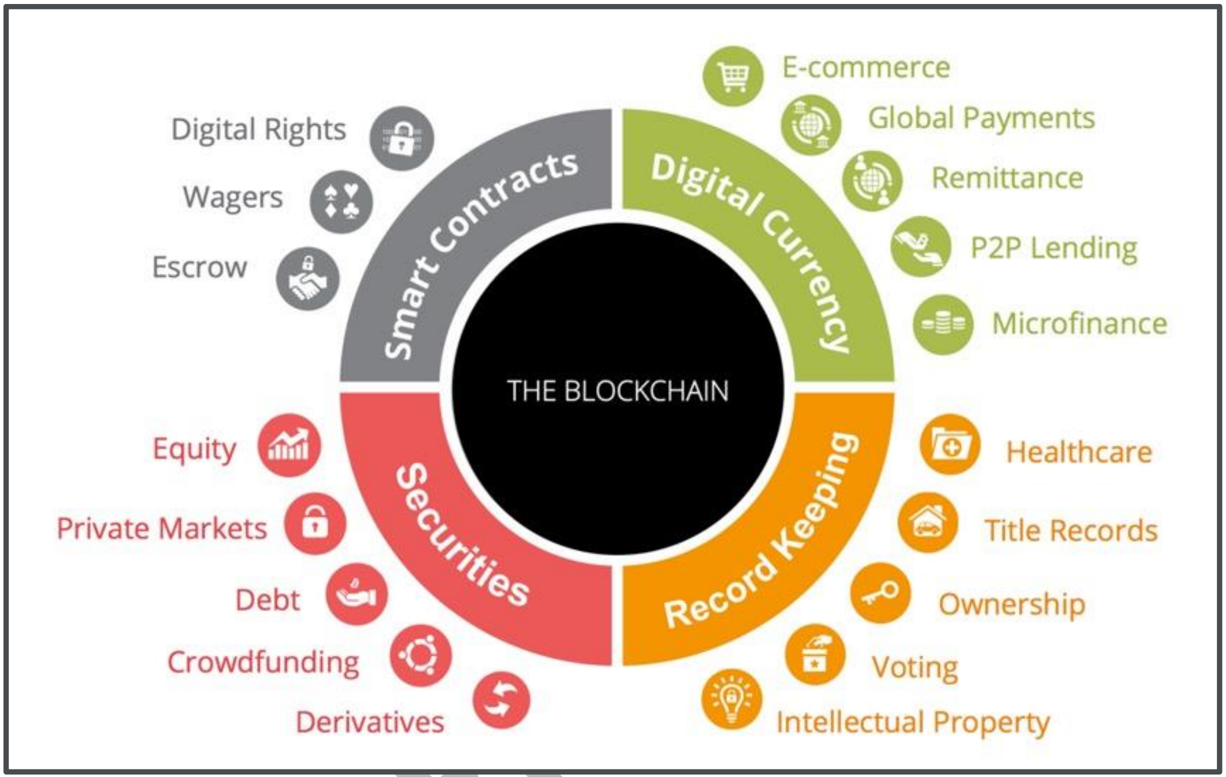

Figure 1: Applications of blockchain technology.
Source: https://datafloq.com/read/what-is-the-blockchain-and-why-is-it-so-important/2270.

Smart Contracts

Smart contracts are agreements, which are converted into computer code, and then written into a blockchain. Once the code is in the blockchain, it cannot be changed, much like a transaction cannot be reversed. Parties to this contract can carry out their obligations by sending tokens (such as Bitcoin or ether) to the contract. The contract code will then be run on the network, in a decentralised fashion, by the node which validates that transaction. The code will output the results of the agreement, for instance the issue of a security like a share or another cryptocurrency and the payment to the issuer. Any kind of agreement that could be fulfilled digitally, could theoretically be done through a smart contract[3].

An example of a smart contract use-case on a large scale would be a voting contract for a country. Citizens could send a voting token, which would be issued to all registered voters, to the contract representing the party or leader they have chosen. The contracts would aggregate the votes and determine the winner in a publically accountable fashion as the code and the vote record would be public. The anonymity of voters could easily be preserved through token mixing or zero-knowledge proofs.

Initial Coin Offerings

While the current use of smart contracts, in practise, has been limited. The theoretical uses are numerous. The most popular use of smart contracts has been to launch new currencies which power new blockchains. This process of offering a new coin for sale is called an initial coin offering (ICO). There has been an incredible amount of money raised for blockchain projects through this method,[4] with over US$2.3B being raised to date. It is an extremely easy way to raise funds from investors all over the world in a crowd funded manner. However, there have been many legal concerns over the nature of the offerings and whether the issuing of the tokens amounts to the issuing of a security.

This new means of raising funds has taken the market by storm, and small 10 person development teams have been able to raise unprecedented amounts of money, publically. Without blockchain this would not be possible for such a small operation, as the traditional IPO process would need to be followed.

An example of a recent ICO which raised in excess of US$200M, is the Tezos blockchain project, which aims to be a self-amending cryptographic ledger that functions in a similar manner to the Ethereum blockchain. It would form a platform for development of decentralised applications (programs which run on the blockchain) and smart contracts as well as value transfer. Tezos' advantage, is that its protocol can be updated in a very orderly fashion. The same is not true for other blockchains which need to undergo a fairly risky process to update the underlying software of the network.[5]

Digital Currency

This application was used as the foundation for the explanation of the technology, however, a few insights about why cryptocurrencies are important will now be presented.

There are many cryptocurrencies such as Bitcoin, Dash and Litecoin and a few more on the way, such as Nimiq[6]. These currencies can be used as any other currency, however, they have some important differences.

One of the key properties that gives Bitcoin value is that it has a certain money supply and growth rate. There will only ever be 21 million Bitcoin (divisible into smaller units up to $1/10^8$). As of October 2017, there are approximately 16.5m Bitcoin in circulation and this amount is growing at 12.5 Bitcoin per 10mins (the block time). This surety of the amount of money is not present in fiat currency which can be created at the will of the central authority. This provides surety that inflation would not be artificially driven through money creation.

While cryptocurrencies are generally not anonymous due to the full history of addresses being public, some have been created which are extremely difficult, if not impossible, to trace, e.g. Monero.

Cryptocurrencies can be transferred more easily than fiat currencies. International payments are no more difficult than local payments, as no exchange needs to be done between banks. So long as the recipient is prepared to receive the cryptocurrency in question, the payment can occur in seconds, as opposed to days for banks. Payments can also take place at any time of the day or week as the blockchain is never offline.

Most cryptocurrencies have values which are determined by supply and demand on exchanges (such as Kraken). These are highly volatile, with prices being known to fluctuate in excess of 200% in a day for some smaller coins. However, there are currencies which attempt to peg themselves to the value of other assets, such as the US Dollar. Tether is a controversial currency which does this.

Other Applications

- Blockchain can be used for file storage (see Filecoin), whereby users pay in tokens to have their files stored securely and privately on the blockchain.
- Prediction markets are another use. The prediction market application Augur makes share offerings on the outcome of real-world events. Participants can earn money by buying into the correct prediction. The more shares purchased in the correct outcome, the higher the payout will be.
- Protection and marketing of intellectual property: Mycelia uses the blockchain to create a peer-to-peer music distribution system. Founded by the UK singer-songwriter Imogen Heap, Mycelia enables musicians to sell songs directly to audiences, as well as license samples to producers and divvy up royalties to songwriters and musicians — all of these functions being automated by smart contracts[7].
- Decentralised computing, where users can pay to have code executed on the blockchain. Golem is a project which creates a marketplace for idle computing power which is powered by blockchain technology[8].

Applications within agriculture

An agricultural use-case for blockchain centres around supply chain tracking, in a transparent and publically verifiable way. This would entail holding records of how a product moves down the supply chain on a blockchain. Consumers could audit the chain themselves to see if the products they are consuming come from where the manufacturer says they do, by looking up the product code. An organisation that does this for the general case is Skuchain.[9] However, there are agricultural specific versions which allow consumers to verify that food is organic or GMO free based on the upstream supply chain that it came from, for example, Provenance[10].

4. What is the Future of Blockchain?

Blockchain is still a very immature technology and it is expanding at a remarkable rate. However, there are some key developments that seem to be on the horizon and toward which blockchain is moving.

Decentralised Exchanges

At the moment, cryptocurrencies may be decentralised but in order to trade them, a middleman is needed, an exchange. Thus, all the vulnerabilities associated with centralised systems present themselves again. Exchanges are repeatedly hacked, like Mt Gox and Bitfinex, as a result, despite the security of the currencies themselves, this single point of failure rendered the system weak.

Decentralised exchanges would enable buyers and sellers to find each other, but never need to deposit coins in the exchange, as the transfers would take place peer-to-peer. Atomic swaps allow for this. Atomic swaps will allow cross chain or currency exchanges without the need for a third party, by using hash time-locked contracts (HTLCs). These are a type of escrow contract which leverages the lightning network to allow both parties to do an exchange without fear that the other party will default.

Off-chain Transactions

Transaction fees (an incentive to have your transaction included in the next block to be mined) are increasing on many blockchains as the demand for transactions increase. A way to make transactions both instant, and significantly cheaper, would be to use payment channels between users that keep track of the net amount owed between users during a given time period. The net amount owed is then settled on chain at the end of the period. The lightning network makes this possible using smart contracts (HTLCs)[11] in much that same way that banks do at the end of a trading day, where transactions are aggregated and the net difference between banks is settled.

Sharing economy

As the internet of things becomes more prominent and the number of connected devices and things increases, we can expect to see more sharing of assets powered by smart contracts on the blockchain. For example, if your house was fully connected to the internet. You could set up a smart contract to rent your house out, that would release a private key to open your door once payment has been made by the renter. The smart contract could then be used to charge the renter for use of electricity, water and internet use.

The sharing of excess storage and computing power will become more commonplace and decentralised computing could become a new form of supercomputing.

5. Blockchain Application Life Cycle

Blockchain is advancing very rapidly but is still in an innovation and early adoption phase. The current application to agriculture in the Western Cape is limited. Cryptocurrencies may well gain traction, particularly in the developing world, and this would lead to usage in agriculture sales and in the machine to machine economy.

6. Business Eco-System View

There is a rapidly growing ecosystem in South Africa from a business perspective. Whilst Bitcoin adoption in South Africans is high relative to the rest of the world’s per capita adoption, the companies with expertise in blockchain adoption are only starting to build expertise. Companies such as SovTech Software, (based in Johannesberg) have built applications for blockchain and have expertise in the field from a technical perspective. South African businesses such as UBU have also launched their own tokens and there are a handful of others who have also done so. South African banks and consultancies are experimenting with blockchain adoption and have made progress in the field.

7. Potential Economic, Social, Ecological and Political Developments and Impacts

Blockchain will have major consequences on all of the above factors. A full discussion of this impact would involve a study of its own but there are certain impacts which are obvious and pressing. Should a cryptocurrency such as Bitcoin gain worldwide adoption, the threat to a small currency like the Rand could be significant. A move to Bitcoin would reduce demand for the Rand, decreasing its value against other world currencies. This would be positive for agricultural exporters but would probably have a net-negative effect on the economy. Anonymous currencies, such as Monero pose a threat from a money laundering perspective as funds can be moved without any insight into the owners of those funds. There is a risk to farmers who transact in cryptocurrency from a reporting perspective also, as taxation rules are yet to be defined for blockchain transactions. The tracking of funds moving in and out of the country on the blockchain poses a threat to the SARB and also to businesses from a compliance perspective.

The beneficiary of blockchain is the end user, who is able to transact far cheaper than before. But the technology is disruptive to the likes of the banks and other intermediaries whose businesses will be eroded by blockchain. Decentralised ledgers allow for rules-based currencies as opposed to currencies essentially controlled by rulers. This is particularly beneficial for developing nations whose currencies are subject to the whims of dictators. Countries such as Zimbabwe and Venezuela would be obvious beneficiaries of cryptocurrency. The ease of trade between different nations through blockchain is an important factor to consider from a farming perspective, particularly with regards to the amount of produce exported from the Western Cape.

Technical Appendix

For a more technical understanding of how blockchain works please see the sections below and the links to content provided.

Foundation:

To understand blockchain, a basic understanding of a few concepts is required:

- Public and private key cryptography: This type of cryptography uses two keys, one key to encrypt: the public key and another to decrypt, the private key. In a blockchain ecosystem, there are key pairs which are defined as the public address of an 'account', combined with a mathematically linked private key, which is used to sign transactions in order to authorise them. The holder of a Bitcoin private key, is the owner of the balance associated with that account.
- A computer algorithm called a hash function, is used to create a fixed length string of characters, called a hash, that represents whatever information was passed through the algorithm, uniquely. There could, practically, only ever be one hash of a given set of information. Thus, the hash can be used to represent that information, and if any of the input information where to change, the hash would be completely different. An

example of a hash process would be the following (using the SHA-256 algorithm[12], the same as Bitcoin uses):

Input: “blockchain will change the way we think about money”

↓

Hash function: SHA-256

↓

Hash:

BCB54906D08DD2E076899FA7048F51D62D490D2DB28F4310076C07F3F11EC3C3

Changing the input by one word to: “blockchain will **not** change the way we think about money”, results in a completely different, but same length, hash:

↓

1015DA637B78613DBD461AE77C4F265E77938B6EA7CFD9FFBE8C8A890779046B

- Peer-to-peer networks: this is the concept where all nodes (end points of the network) are connected to each other and all information is stored across the nodes in the network, instead of all information passing through a central point, which would be a typical client-server setup.

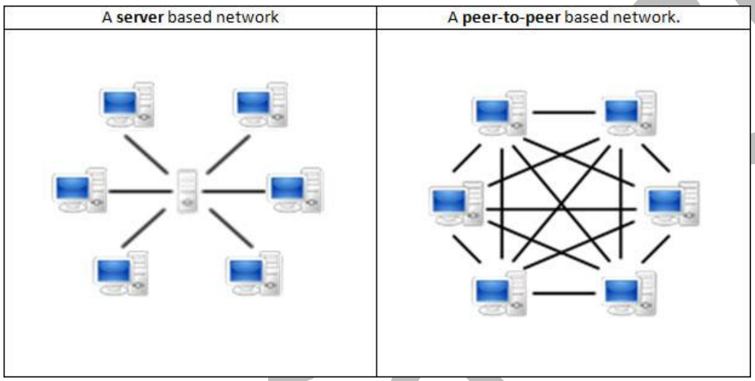

Figure 1: Centralised vs a decentralised network

Source: https://www.gigatribe.com/en/help-p2p-intro.

For more:

- Kahn Academy: https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/Bitcoin/v/Bitcoin-what-is-it
- Bitcoin Wiki: https://en.Bitcoin.it/wiki/Main_Page
- Bitcoin White Paper: https://Bitcoin.org/Bitcoin.pdf
- Tezos White Paper: https://www.tezos.com/static/papers/position_paper.pdf
- Nimiq White Paper: https://medium.com/nimiq-network/nimiq-a-peer-to-peer-payment-protocol-native-to-the-web-ffd324bb084
- Lightning Network: https://lightning.network/

[1] Blockgeeks. 2016. *What is Blockchain technology? A step-by-step guide for beginners.* [Online] Available: https://blockgeeks.com/guides/what-is-blockchain-technology/ [Accessed: 29 October 2017].

[2] Blockgeeks. 2016. *What is Blockchain technology? A step-by-step guide for beginners.* [Online] Available: https://blockgeeks.com/guides/what-is-blockchain-technology/ [Accessed: 29 October 2017].

[3] BlockGeeks. 2016. *Smart contracts: The Blockchain technology that will replace lawyers.* [Online] Available: https://blockgeeks.com/guides/smart-contracts/ [Accessed: 29 October 2017].

[4] Barnett, C. 2017. *Inside the Meteoric Rise of ICOs.* [Online] Available: https://www.forbes.com/sites/chancebarnett/2017/09/23/inside-the-meteoric-rise-of-icos/#51a2377b5670 [Accessed: 25 October 2017].

[5] Tezos. 2017. *Technology.* [Online] Available: https://www.tezos.com/technology [Accessed: 27 October 2017].

[6] Nimiq. 2017. *Unleashing the Blockchain*. [Online] Available: https://nimiq.com/ [Accessed: 2 November 217].

[7] Mycelia for Music. 2017. *A think + do tank*. [Online] Available: http://myceliaformusic.org/ [Accessed: 27 October 2017].

[8] Golem Network. 2017. *Golem: The worldwide supercomputer*. [Online] Available: https://golem.network/ [Accessed: 27 October 2017].

[9] Skuchain. 2017. *Turn information into capital*.[Online] Available: http://www.skuchain.com/ [Accessed 29 October 2017].

[10] Provenance. 2017. *Provenance.* [Online] Available: https://www.provenance.org/how-it-works#producers [Accessed: 27 October 2017].

[11] Lightnight Network. Undated. *Transactions for the future.* [Online] Available: https://lightning.network/ Accessed: 2 November 2017].

[12] Password Generator. 2017. *SHA256 Hash Generator.* [Online] Available: http://passwordsgenerator.net/sha256-hash-generator/ [Accessed: 2 November 2017].