Project 60: ‘Evaluating the feasibility of Blockchain applications’

University: Cardiff University School of Computer Science and Informatics

Degree: BSc Business Information Systems

Module Title: One Semester Individual Project

Module Code: CM3203

Credits: 40

Year: 2017-2018

Author: Fadi Zoghbi

Student ID: 1444076

Supervisor: George Theodorakopoulos

Moderator: Philipp Reinecke

Date Submitted: 11/5/2018

Abstract:

Blockchain is a disruptive technology that since its emergence to the world in 2009 as the infrastructure that supports Bitcoin Peer-to-Peer electronic cash system has influenced significantly the industrial world and prevailed as topic of discussion for commercialisation by large corporations and technology enthusiasts.

The main objective of this project is to assess the feasibility of Blockchain applications by conducting an in depth literature study. In order to accomplish this objective, the report will describe the fundamental principles of Blockchain technology and cryptocurrencies. Then it discusses the different types of distributed ledger technology as well as their similarities and differences. The paper continues by introducing the reader to the successful real life Blockchain applications and their respective characteristics. Further, a variety of future uses of the technology in various industries is suggested followed by the attributes of tasks that can benefit from a DLT implementation. Finally the report finishes with a conclusion regarding the discoveries that have been made.

Acknowledgments

First and foremost, I have to thank my project supervisor, Mr George Theodorakopoulo. Although I was not familiar with Blockchain technology and the project proved quite challenging for me he worked to the best of his ability to inspire me and assist me whenever I needed it. Without his encouragement, guidance and dedicated involvement in every step throughout the process, this report would have never been accomplished. It was a pleasure working with someone who consistently motivated me to get the best out of this project despite all the obstacles. His support and counselling were crucial to the completion of this project. I would like to thank you very much for your support and understanding over the last academic year.

Getting through my dissertation required more than academic support and I have many people to thank for listening to and giving advices to any hindrances that occurred. I cannot begin to express my gratitude and appreciation for their continuous support during my time at University, especially in the final year. Specifically, *Nikolaos Stergiou*, *Panagiotis Delphinis* and *John Christou* consistently encouraged and helped me at times I needed it most.

Most importantly none of this could have happened without my family. My parents who offered their support through Skype calls every week trying to encourage me to keep working hard and my sisters who consistently tried to motivate me every time I felt like quitting. My family has not only helped me achieve the best I can during the past three years in University but also provided me with support and belief in my capabilities. This dissertation stands as proof to your unconditional love and encouragement.

Contents

1. Introduction:

The ‘Blockchain technology’ (often referred as ‘Blockchain’) is one of the most prominent emerging technologies nowadays. Businesspeople and governments recognise its potential and label it as a “fascinating”, “innovative” and “disruptive” technology [1]. Basically, it is a digital and decentralised ledger that records all the transactions that have ever happened in its network. Best known as an immutable database that runs underneath cryptocurrencies like Bitcoin and Ethereum, it is expected to play a vital role in every industry as businesses are interested in the technology’s assurance of implementing a trustless consensus to validate transactions. Commonly, financial transactions are guaranteed by financial institutions, payment providers or a credit card company (e.g. Banks, PayPal and Visa) because people do not trust each other. Thus, they have to depend on reliable individual third parties as an assurance that the transaction of money will be successful. The problem with the current system of how transactions are happening is that people have to pay a small fee to the bank in case they want to transfer money the same day or even receive charges up to 3% for foreign transactions (e.g. make purchases while abroad, charge for currency conversion) [2]. Blockchain can overcome these forced intermediary fees by automating the process, reducing costs by removing the middleman (i.e. Banks, PayPal) by enforcing smart contracts, which act as trusted intermediaries between unknown parties in the network. The objective of Blockchain technology is to create a decentralised environment where no third party is in control of the transactions and data. More information regarding technical properties and processes of Blockchain (e.g. consensus mechanism, smart contracts, cryptocurrency, and decentralized system) will be discussed shortly, further in the report. Experts, consider the technology to become so influential in the next years that they regard it as a new “type” of Internet, one that stores and verify information about every asset, device, individual and introducing new technological capabilities across various industry fields such as finance, healthcare, supply chain management (SCM), electronic voting, Internet of Things (IoT) and many more [3]. Consequently, it is obvious that Blockchain is not only the foundation of cryptocurrency exchanges and its future uses are yet to unfold.

The primary aim of this project is to clarify what type of applications can realistically benefit from the implementation of Blockchain technology. To achieve this end-goal the following objectives have been set:

1) Understand and describe Blockchain technology from a non-technical viewpoint.
2) Identify the different kinds of Blockchain (e.g. public, private and hybrid) and display their similarities and differences.
3) Define Blockchain properties and its limitations.
4) Discover successful Blockchain applications and outline their characteristics.

   -Due to the vast number of Blockchain applications I will portray the three most mainstream and well-known applications and industry fields (e.g. Bitcoin, Smart Contracts, Supply Chain Management) where Blockchain applications can be impactful as well as their characteristics [4].

5) Suggest future implementations of applications supported by Blockchain technology.
6) Highlight the characteristics of tasks that would benefit from Blockchain.

In essence, the report examines how feasible is the implementation of Blockchain technology in various applications which potentially, can change in a genuine way, how businesses operate across the globe. This project, aims to be conducive in the education of, investors and individuals with no prior technical knowledge, who are fascinated by the capability of this emerging technology by outlining its properties, benefits as well as its limitations in order to have a thorough point of view to be in a position to judge objectively the potential of the technology and whether it is, the greatest innovation after the invention of the Internet.

In conclusion, through this dissertation I aspire to provide a comprehensive literature review on this revolutionary technology, information regarding current and future applications based on the Blockchain technology along with the key characteristics of tasks that could utilise the technology to its maximum potential.

1.1. Project Structure:

The dissertation starts with the introduction stating the importance and uniqueness of Blockchain technology as well as the areas where it can be applied. The following section will prepare the reader for the project with all the important background information regarding the Blockchain technology of Bitcoin, several of its technical terms and properties and a description of three other well-known Blockchain platforms, Ethereum, Hyperledger Fabric and Corda. In addition, in section 2 I will also explain the different types of Blockchain technology as well as their similarities and differences. Also, information regarding the distributed ledger technology, the type of technology Blockchain is based on and examples of DLT applications will be provided too. Furthermore, I will briefly describe Bitcoin, a peer to peer (P2P) version of electronic cash system based on Blockchain technology as it is the first and most well-known Blockchain application as well as its importance in the financial ecosystem. In Section 3 I will identify and describe successful Blockchain applications that can change radically how operations in certain industry fields (such as Finance and SCM) are carried out. Further, I will discuss the distinctive characteristics of the applications that were described in section 3. Following in section 4 future uses of Blockchain applications will be suggested, that could have a notable impact in the business world (e.g. electronic voting, recording of personal data, music/entertainment rights and asset management). Additionally, in section 5 I will highlight the characteristics of tasks that could potentially benefit from the technology of Blockchain. Finally, in section 6, I will conclude this dissertation with vital information for the reader regarding the revolutionary capability of Blockchain.

1.2. Approach:

Due to the theoretical nature of the dissertation, the objectives and aims of the project which were stated in the introduction will be accomplished by means of literature study. Throughout the duration of the project (12-15 weeks) an extensive research has been conducted on Blockchain technology, the successful applications based on the said technology and industry fields where the technology can be utilised. The research was carried out on the basis of articles, online papers, white papers (e.g. *Bitcoin: A Peer-to Peer Electronic Cash System* by Satoshi Nakamoto, January 2009), eBooks (e.g. *Blockchain: Blueprint for a new Economy* by Melanie Swan, 2015) and eLibraries (e.g. SSRN). The current approach was chosen because the aim of the report is to evaluate the practicability of Blockchain technology in applications of diverse industries. With the purpose of providing evidence regarding the potential of the technology, a detailed research had to take place with respect to, the properties of the technology and how it could be beneficial in the various industries around the world. Therefore, conducting a literature review is the most suitable approach to complete this dissertation and support the objectives of the project with concrete concepts and suggestions.

2. Background:

In a technologically evolving world new technologies and systems are being produced constantly. One of the many emerging technologies that have surfaced is “Blockchain technology” also declared as “block chain” or “Blockchain”, which is an electronic, distributed, decentralised, shared and cryptographically secure ledger designed to verify and record transactions chronologically. It is suggested by many that Blockchain technology is the greatest invention after the Internet (1993) [5]. It has the potential to change dramatically the way humans communicate, trade and work with each other as well as applications related to Artificial Intelligence (AI), IoT and technology in general. The figure below illustrates how the technology evolved over the years.

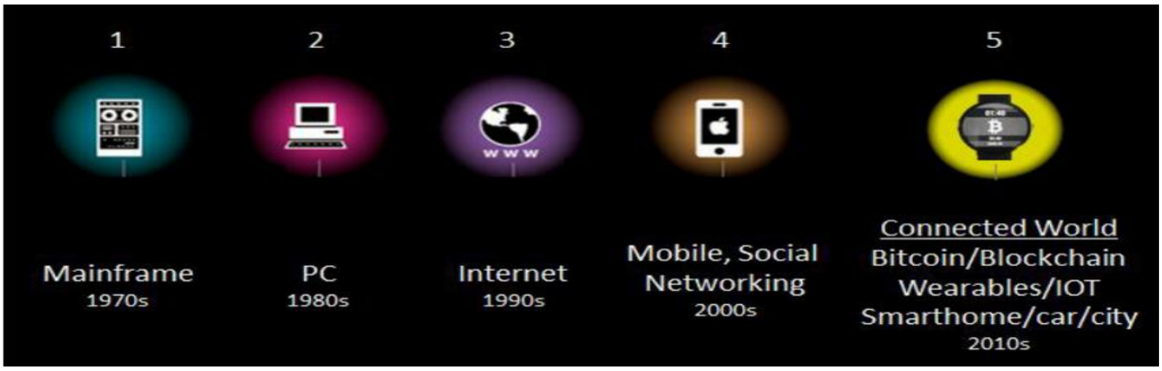

Figure 1: Innovative technologies which changed the world.

[22] Melanie Swan, February 2015, “Blockchain: Blueprint for a New Economy”. [Online]. Available: http://www.allitebooks.in/blockchain-blueprint-new-economy/ [Cited 1stMay, 2018]

2.1. Cryptocurrencies and Bitcoin:

2.1.1. Bitcoin and its significance:

Blockchain technology was first introduced to the world in 2009 by an unknown individual or group of people by the pseudonym ‘Satoshi Nakamoto’, who published a white paper called *‘Bitcoin: A Peer-to-Peer Electronic Cash System’*. Blockchain is the fundamental technology on which Bitcoin is built upon. It was created as the underlying architecture and database for executing and storing transactions of the digital cryptocurrency bitcoin. For clarity purposes, throughout the report the term bitcoin refers to the digital cryptocurrency while Bitcoin implies the system. In simple terms, Bitcoin is a peer-to-peer (P2P) digital cash system which allows transactions and payments between unrelated parties in an untrusted network like the Internet without the involvement of a trusted card provider (e.g. PayPal) or centralised institutions (e.g. Banks). The system allows payments using bitcoins, a type of digital currency called ‘cryptocurrency’.

Bitcoin is regarded as a revolutionary invention because transactions within the system are executed in a different way from current conventional money transactions through financial institutions. Nowadays, people rely on trusted third party organisations like banks, who act as a guarantor between two unrelated, trustless parties that the transactions will be carried out successfully without the possibility of tampering the data or fraudulent actions happening. These organisations ensure that the payer will indeed transfer the money to the recipient and the recipient is assured that the money will move into his account. Simply put, the banks act as a verifier when two mistrusting parties around the world who do not trust each want to transfer money with each other. However, this service comes with a cost. Financial institutions and brokers usually enforce charges or commonly called ‘transaction costs’ to buyers and sellers as a payment for their role. Moreover, there are transaction costs when purchasing or selling real estate which include agent’s commission and government fees [6]. Although the prevalent system of money transactions works well there are certain problems that can be avoided. For example, financial institutions charge additional costs to the customers in case of a disagreement between two parties during a transaction [7]. Consequently, these trusted third parties need to solve the controversy since people rely on them for the transaction to be successful. Moreover, an additional problem of having a middleman in order to carry out transactions due to trust issues is that the money and personal information are stored in the servers of the central authority. Therefore, data breach of information or even losing the money which are stored there is likely to happen since cyber-criminals only need to focus only one place to attack with the objective to access the confidential and private data of customers. Disastrously, these attacks such as the South Korea bank hack (2013), JP Morgan data breach (2014) and the Distributed Denial of Service (DDoS) on Bank of America (2012) [8] would not have been carried out, if the data and information were cryptographically stored in a decentralised electronic system like Bitcoin utilising the Blockchain technology rather than being stored centrally. Below a visual representation of blocks in Bitcoin’s Blockchain is provided as an assistance in order understand its architecture. The structure and contents of each block will be explained thoroughly in *section 2.1.4.2* (Mining Process).

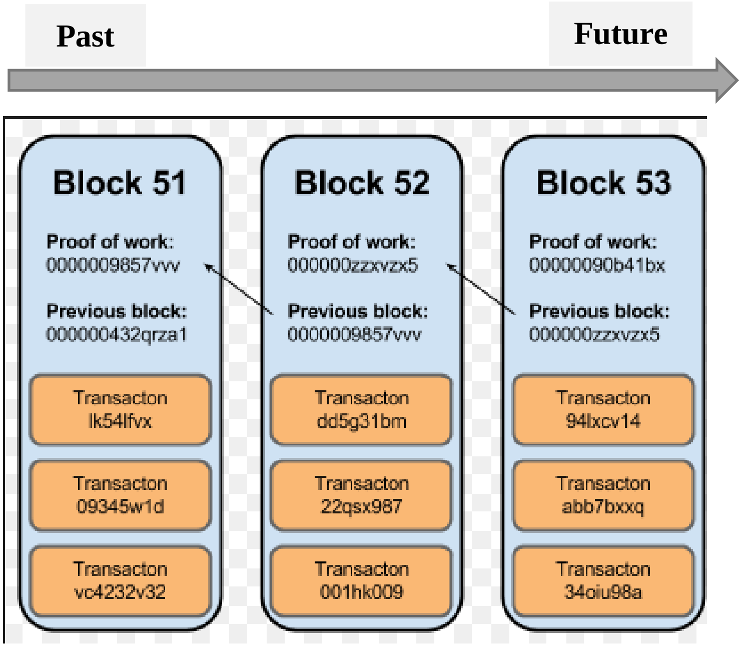

Figure 2: Connected blocks in Bitcoin’s Blockchain

2.1.2. Double Spending Problem:

Until the release of Bitcoin, electronic money transactions could happen only through trusted third party financial institutions to counter a major problem that occurs during the transaction process if it is carried out digitally. The problem goes by the name ‘Double Spending’. In particular, if two individuals who do not know each other want to initiate a transaction of money between each other without being supported by a trusted entity (e.g. banks) there is a possibility one of them to act unfairly. There is no counter measure to prevent the criminal from copying and sending the same amount of digital money to two separate individuals [30]. For example if Bob acts unlawfully he could send the same $5 to both Alice and Joe. This is possible because digital money can be replicated as many times as the individual wants if there are no counter measures in place. That way he could pay unrelated people with the same amount of money over and over again. Because of this problem people were forced to exchange money digitally through banks since the bank carries out the transactions with legitimacy and authenticity. They act as a validator to Joe (receiver) that Bob indeed sent $5 from his accounts and now are under Joe’s possession. That way people can trade funds with each other being assured of the genuineness of the transactions under the supervision of trusted third parties. In the past central authorities like banks, acted like ledgers by keeping a record of each individuals funds in order to prevent duplication. However, Bitcoin is the first electronic system that eliminates the ‘Double Spending’ problem as well as the necessity to carry out transactions through trustworthy centralised authorities. The preventative mechanism that is utilised by Bitcoin is called ‘Proof of Work’. Every transaction is validated by miners who certify the validity of the transaction. Once it is confirmed the transaction is stored in a block and then added to the blockchain. Since transactions in Bitcoin Protocol are irreversible there is no possibility of the ‘Double Spending’ problem to occur. Therefore one cannot spend the same amount of money or bitcoins repeatedly since upon the completion of the first transaction that the fraudster initiated then the money automatically withdraw from his wallet. Thus he cannot “spend” that amount to another person as he does no longer own them. The Bitcoin’s eradication of ‘Double Spend’ problem resulted in the viability of digital transactions without the compulsory participation of a centralised authority.

2.1.3. How Bitcoin works:

2.1.3.1. Bitcoin Components:

In order to be able to make transactions with bitcoins one need to install a Bitcoin wallet which encrypts and maintains the bitcoin balance in their personal computer or smartphone. Also it automatically generate the user’s bitcoin address which is used every time a transaction of funds take place. In addition every user has a Wallet ID (or Wallet Identifier) which is different from the Bitcoin address used for transactions [9]. The Wallet ID is a string of numbers and letters, similar to the username you would use to access your E-mail or social media accounts (e.g. Facebook). Its purpose, is to allow the user to connect to his wallet by using his Wallet ID, password and any type of Two Factor Authorisation he agreed to. In contrast, bitcoin address differentiates from the Walled ID because it is a single-use identifier generated automatically from your wallet every time you initiate a transaction. In the Bitcoin P2P electronic cash system people use different addresses to send and receive funds as an extra security measure. The components that are necessary to carry out transactions in Bitcoin system are listed below:

- **Private Key:** a 64 character sequence of arbitrary letters and numbers. It is a cryptographic key used by the user for the purpose of sending money from his wallet to another user's wallet. It is unique for every person and needs to be kept secret by all means. Every transaction is digitally signed with the private key for the purposes of security.
- **Public Key:** is the distinctive identifier of the user's cryptocurrency wallet and must be known to the public.
- **Address:** is a single use identifier which people will use in order to send bitcoins to your wallet. It is automatically generated for every transaction and is used only for the specific transaction taking place.

2.1.3.2. Mining Process:

Bitcoin runs on a decentralised P2P network. This means that the network consists of unrelated nodes (computers) which share information regarding validated transactions stored in 'blocks', to other nodes thus everyone in the network is aware of the updated state of the ledger. Since, there is no central authority in the Bitcoin protocol, the participants in the network must reach to an agreement regarding which transactions are legitimate in order to be put in a block and later in the Blockchain. Because of the lack of a trusted third party, which everyone would rely on with respect to the validity of the transactions (e.g. similarly to how people trust banks) a procedure needs to be implemented. This consensus mechanism is called 'Proof of Work' and will be explained in detail below. Primarily, as the bitcoins neither have a physical entity due to their digital nature nor are printed by governments or financial institutions like money, they need to be generated. Currently there are approximately 17 million bitcoins in circulation in the Bitcoin ecosystem and around 4 million bitcoins are expected to be generated until the threshold of 21 million is accomplished [11]. Once, this limit is reached no more bitcoins are going to be generated. The process of generating bitcoins is called 'mining' and requires certain special nodes, connected to the network to compete with each other to find a solution to a complex mathematical enigma[10]. Specifically people who are involved in the mining process also known as 'miners', create blocks which contain data of validated transactions and subsequently add them to the Blockchain (hence the name of the technology, 'chain of blocks'). One can see transactions being uploaded in real time at *blockchain.info*. The reward for their effort is 12.5 bitcoins at the time of writing and these bitcoins are generated from the pool of the remaining 4 million bitcoins. Specifically, miners download mining software and run it on their powerful computers to find the answer to the puzzle. Precisely, the puzzle that needs to be solved require miners to guess randomly a number ('nonce') which if it's linked to the data of the block and passed through a 'hash function', generates a number within a certain range (0 - 4,294,967,296) [10]. A hash-function is a mathematical process that transforms an input to an unreadable sequence of characters, which is called output. As an input one can use a single word or even a long text and if the user hash the input the hashing algorithm will produce a sequence of random letters and numbers of specific length (64-characters long)[12]. This is called 'hash-digest' or simply 'digest'. What makes hash function important is that no matter how many times you hash a specific input it will produce the same output. If the user changes the input even in the slightest way possible (e.g. deleting a comma or a letter) and run the hash algorithm the resulted output will be completely different. This randomness make it unachievable to predict the output. In the case of Bitcoin the input to the hash function are the output of the hashed recent transactions that need to be confirmed and logged in the block, the hash of the previous block as well as a nonce (a random number used once). Even if an attacker managed to modify a block he would have to modify the next block as well because the hash of the tampered block would be different from the hash that is stored in the next block [12]. So realistically an attacker needs to tamper the whole chain of blocks which altogether contain all the transactions that have ever happened in the Bitcoin ecosystem, a task virtually impossible. This is why the transactions in Bitcoin are considered tamper-proof, because modifying the data stored in the blocks is unfeasible. Further, in order for the miners to find the desired number (nonce), they have to guess arbitrarily for a certain period of time (on average 10 minutes) [13] because the hash function prevents miners from predicting the nonce. In addition sometimes, there is a possibility that more than one nonce produce the desired result or even none. In that case miners continue their efforts with a different block configuration until they succeed. Once, a miner finally finds the desired number or 'Proof of Work' [14] because he has proof that he has invested substantial computing power and time to solve the puzzle, he broadcasts to the rest of the network his succession so that the rest of the miners will assess the validity of that specific block and continue their efforts for the creation of the next block. Additionally, once a block is confirmed and added to the chain a difficulty target is generated for the next block [31]. A new block of data will be appended in the Blockchain only after the nodes in the network reach consensus with regard to the legitimacy of the transactions. Then in order for a new block to be generated, miners participate again in the race of assembling a block that outputs a hash value equal or lower than the target number created by the previous block. Typically this target number is a complicated hexadecimal number with many zeros in the beginning [44]. Due to the great number of miners, the reward in the form of bitcoins is not definite and depends on the computing power of the miner's hardware, since the faster the hardware is, the more calculations can be executed and the greater the chances are for the solution to be found. Further the process of how transactions are carried out will be explained in the next paragraph.

2.1.3.3. How Bitcoin transactions work:

As explained above, the bitcoins of a user are safely stored in his digital Bitcoin Wallet, a computer program which handles the transactions. The eWallet automatically generates a unique private key, public key. Additionally, in order for the Bitcoin address to be generated, the public key is transformed through encryption protocols (e.g. SHA-256 hashing algorithm) and the output of the hashing process is the Bitcoin address of the user [22]. The Bitcoin address can be compared to an email address. Anyone who has your email address can send you an email. Similarly, anyone who has your Bitcoin address can send you bitcoins. Every time the user initiates a transaction, whether to receive or send funds the bitcoins are being verified by a digital signature called 'public-private key cryptography' and consequently sent from one wallet to another [15]. I will illustrate an example of how transactions are executed in the Bitcoin ecosystem. In the paradigm, Alice does not have prior technical knowledge regarding Blockchain technology and Bitcoin but is interested in trying it because her friend Bob suggested it. Bob helps her create her own Bitcoin Wallet in order to initiate a transaction between each other to show Alice how the system works. For this reason, Bob accesses his wallet with the purpose of sending 10$ to Alice which is equivalent to 0.0010 bitcoins at the time of writing [16]. Then, Bob types in the input field Alice's bitcoin address which represents her wallet and the amount of bitcoins he wants to transfer to her. Once, Bob press 'send' on his wallet, he announces to the network that he would like to move his bitcoins, thus a transaction is initiated which upon completion will transfer 0.0010 bitcoins to Alice's bitcoin address withdrawing the bitcoins from Bob's wallet. Simultaneously, before the transaction happen Bob 'signs' digitally the transaction with his private key which states to the network that he is authorizing the transaction. Additionally, the process of signing with his private key ensures by mathematical proof that the amount of bitcoins he wants to send derive from his wallet since the private key of a wallet is only known to the respective owner. Moreover, the digital signature act as a means of prevention to any alteration an attacker would attempt. Shortly, after the transaction initiated, it is appointed to a "waiting list" of transactions which are pending (unconfirmed) and need to be verified from the other nodes (i.e. miners) in order to be logged in a block. For the transactions to be confirmed miners need to ascertain the legitimacy of the transaction and examine if the amount of bitcoins that the payer wants to send are available (i.e. A payer cannot send more bitcoins than he already has in his wallet) and consequently add it in a block. The process of their work is called 'Proof of Work' because they provide their powerful computers to produce a piece of data (costly and time consuming) which satisfies certain conditions as mentioned above (i.e. they examine if Bob's public and private keys are capable of accessing his wallet). This process takes approximately 10 minutes and upon completion a new block is created and broadcasted to the rest of the networks to assess their validity. If the other nodes reach to a consensus that the block is indeed legitimate the transactions within the block are considered genuine and ready to be completed. Which in our case means if the transaction that Bob initiated with Alice, ends up in a newly created block then their transaction was successful and Alice will be able to see that her wallet balance is 0.0010 bitcoins now. The figure below illustrates how a transaction in the Bitcoin ecosystem works:

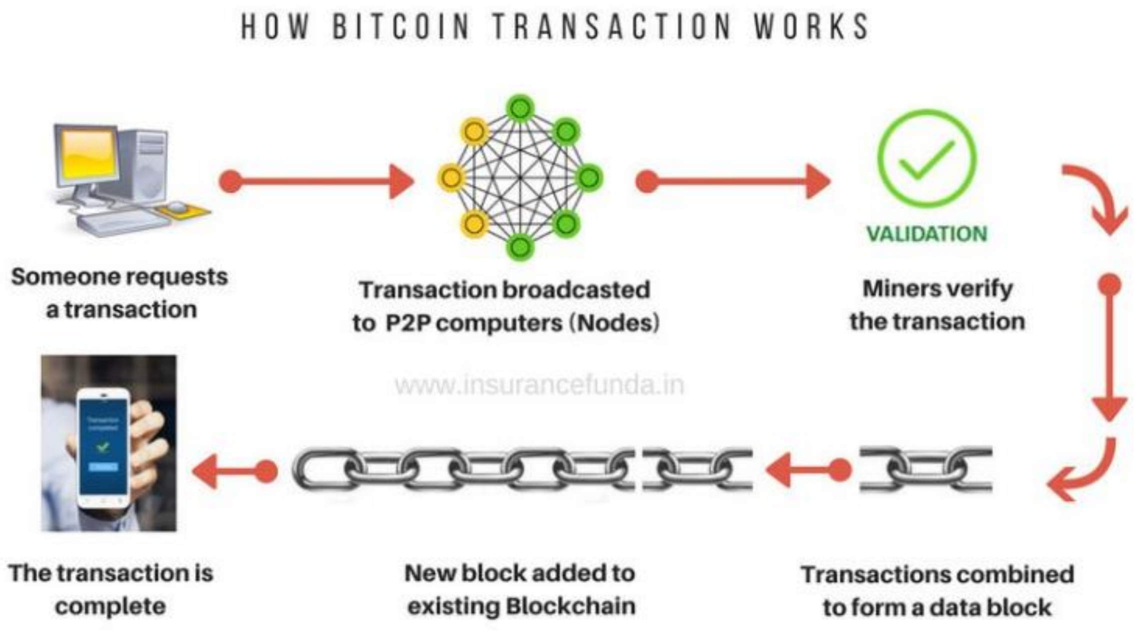
HOW BITCOIN TRANSACTION WORKS
Someone requests a transaction
Transaction broadcasted to P2P computers (Nodes)
VALIDATION
Miners verify the transaction
www.insurancefunda.in
The transaction is complete
New block added to existing Blockchain
Transactions combined to form a data block

Figure 3: The procedure of a Bitcoin transaction.

[23] Anish L J, "Bitcoin and other Cryptocurrencies-all you need to know", INSURANCE FUNDA, 2ndJune 2017, Available: http://insurancefunda.in/bitcoin-cryptocurrency/ [Cited 1stMay, 2018]

2.1.4. What is Cryptocurrency?

With the emergence of Bitcoin P2P decentralised cash system and Blockchain technology in the recent years, a new concept came to light by the name of 'Cryptocurrency'. It first was introduced to the world in 2009 along the release of Bitcoin [7]. Although the cryptocurrency has been in existence for almost 9 years it was not known by the larger part of the society. People were not interested in it because they were either confused of how a digital currency can compete the well-established physical currency (e.g. Dollars, Euro, and Yen) which is used across the globe or were reluctant of the capabilities of the new concept. However, in 2017 it was observed a notable increase in the value of cryptocurrencies, which escalated from a market capitalization of 17.7$ to 613$ billion [17]. This rise in the value of cryptocurrency is a result of the following three reasons:

1. One of the reasons why the market cap of cryptocurrencies rose so rapidly is because various countries realised the potential of the digital currency thus initiated the process of legalising bitcoins. Noteworthy, examples are Japan, in 2017 started to accept legally bitcoins as payments with 'Bic Camera' being the leading company in accepting cryptocoins [18]. Likewise, Australia has started regulating the currency since 2017 making bitcoin payments legal in July of the same year.
2. The appearance of Blockchain technology, the distributed and decentralised ledger, which is the underlying technology of Bitcoin and digital currencies has intrigued the majority of people. Due to its properties and mechanisms (PoW and irreversible transactions), which do not allow any modification or alteration of transactions as well as the remarkable security measures that provides due to cryptography, drew the interest of not only market investors who consisted the majority of people involved in trading bitcoins so far, but the general public, people with no technical knowledge necessarily of the technology. This resulted in an increase of demand for the cryptocurrencies and especially bitcoin. As stated above in the *Mining Process* section the number of bitcoins that will be produced is finite (21 million). Therefore, the total value of bitcoins in circulation will increase since higher demand along with limited supply of coins consequently lead to increase of the currency's value [19]. As expected the increase in value of bitcoin resulted in alternative cryptocurrencies or 'altcoins' (e.g. Ethereum, Ripple and Litecoin) to be regarded as 'attractive' for investment hence the rise of the total cryptocurrency market cap.
3. Mining difficulty is considered as a critical factor which affects the value of the cryptocurrencies. It is intentionally premeditated to be resource-exhaustive and laborious so the number of blocks (144) [20] mined daily remains steady [21]. If a crypto coin can be mined effortlessly that means a large quantity of coins will be available in short time which will affect its price negatively since it can be achieved by the majority of people. However, a coin which is significantly hard and time-consuming to mine results in a generation of coins at a steady and slow rate. Due to the difficulty of the process (also known as mining or Proof of Work) in blockchains where the mechanism of consensus is required, like the one which underlies Bitcoin system the value of the coin mined (i.e. bitcoin) will rise in value gradually as the PoW increases in complexity. Specifically, since the mining process will become

harder the miner will have to spend more money to update the computing power of his hardware and the costs of electricity. Therefore, it is expected that bitcoins will increase in value in order to be worth it to involve in the mining process. If the rewards of mining bitcoins were less than the costs which result from mining (electricity, time-consuming) then the majority of miners would not engage in this process anymore.

In the Bitcoin protocol the funds that are being transacted from one wallet to another are called bitcoins. These funds exist exclusively in a digital form unlike the tangible money or commonly referred as 'Fiat Money' people use on a regular basis [24]. Fiat money and cryptocurrencies differ significantly from each other. First of all, fiat money are supported by a government and can be found in tangible form like dollars, euros or in intangible form, by being transacted electronically through a financial institution (e.g. banks, credit card providers). In contrast, cryptocurrencies are not backed up by any government or central bank and its value derive from the common acceptance of a large number of individuals. In essence, the more people regard digital currencies as valuable asset the higher their value will rise. Likewise, it is a completely decentralised and universal currency that anyone can use for the purposes of buying goods and services. In conjunction with recent bank scandals and collapses, cryptocurrencies started being appealing to the general public. The most well-established and known cryptocurrency is bitcoin. It was the first instance of cryptocoin that was mentioned in Satoshi's Nakamoto white paper, "Bitcoin: A Peer-to-Peer Electronic Cash system" [7]. On 3rd January 2009 the first block (also known as Genesis Block or Block 0) of Blockchain technology was mined by Satoshi Nakamoto and generated fifty bitcoins [46]. Ever since, many big companies showed interest in the bitcoin and started adopting it. One of the first was the widely known computer company Dell [23]. Following the footsteps of Dell, more companies started accepting bitcoins as a means of payment which led to the rapid rise of the market value of bitcoin. Currently the total value of bitcoin cryptocurrency is 153,524,900,575$ billion which is equivalent to approximately 17 million bitcoins [25]. However, other types of cryptocurrencies started emerging after the successful launch of Bitcoin which people refer to as 'altcoins' (alternative cryptocurrencies). Specifically, the word 'altcoin' is an abbreviation of "alternative bitcoin" therefore people imply every cryptocurrency except bitcoin when they mention altcoins [26]. Noteworthy, altcoins are Ether (the coin of Euthereum technology), Dogecoin, Litecoin, Ripple and up-and-coming NEO and Stellar (XLM) [27]. Finally, potential investors and companies should consider carefully before investing in altcoins since digital currencies are highly-volatile because they luck certain regulations fiat money have [28]. Even an investment in bitcoin, the dominant cryptocurrency since its release is deemed risky [29]. Therefore, it is advised to trade bitcoins with money that they can afford to lose.

2.2. Blockchain technology:

Bitcoin protocol was one of the most alluring technological innovation of the past ten years, with a societal impact as well as causing disruption in the finance industry and specifically in the operation of the economic services. However, all of this would never have happened without the underlying technology upon which Bitcoin system is built, the Blockchain technology. The term Blockchain alludes to a chain of immutable blocks being connected by the consensus mechanism ‘Proof of Work’ [33]. This revolutionary technology, is the infrastructure that underpins Bitcoin protocol and ensures transactions are transparent and permanent [32]. Blockchain technology along with Bitcoin system have provided the capability to unrelated mistrusting parties to carry out financial transactions while offering a transparent and tamper-proof storage of these transactions [7]. Alongside this, it is capable to wipe out the entity with the most crucial role in the financial and societal ecosystem, the middleman. It is possible, for the reason that the technology grants power to the people, to transfer digital data and wealth to others, through a secure, and immutable network. Additionally, digital currencies that cannot be controlled by central authorities or governments, like bitcoin can be generated within its decentralised network. Furthermore, it supports the development of electronic contracts (smart contracts), which are self-executed once certain conditions have been met. Lastly, it introduces a new concept in the technological world which goes by the name ‘smart property’, which is essentially digital property (e.g. car, house, smartphone). The idea that physical things have technology embedded in them is not unfamiliar. Until recently the uses of IoT were for the purposes of collecting information and data thus people did not have much power over them [38]. Albeit, smart property contracts shift the potential of smart property one step further. By implementing in them, the decentralised Blockchain technology the control people have over them increases rapidly. In essence participants in the network, can carry out between each other, transactions of these electronic assets. Its properties such as data-integrity and transparency as well as irreversible transactions contributed to obtaining plenty of attention from various industries (e.g. healthcare, SCM, asset management) aside from corporate giants and financial institutions. Characteristically, in 2016 International Business Machines (IBM) Corporation, fascinated by the technology started engaging in the development of blockchain with the aim to shape it ready for business. The corporation in order to achieve its goal provided 44,000 lines of code to the Linux Foundation’s open source Hyperledger Project to help developers comfortably build secure distributed ledgers for commercial use of the blockchain technology, which can be used to exchange products of value [34]. Following the footsteps of IBM Corporation several banks showed interest in the technology as well. Specially, JPMorgan, Royal Bank of Scotland and UBS participated in an alliance conducted by an enterprise software firm by the name R3 to develop ‘Corda’, a blockchain platform for businesses [35]. Furthermore, Wal-Mart stores Inc. and Visa Inc., utilise the technology to improve the efficiency of supply chain, accelerate transactions and store data records [36]. It could be said with certainty that the Blockchain technology has been of interest to all these corporations and tech giants because of its properties and its potential to change entirely how people interact with each other on a personal and business level within the society. Visual representation of smart contracts:

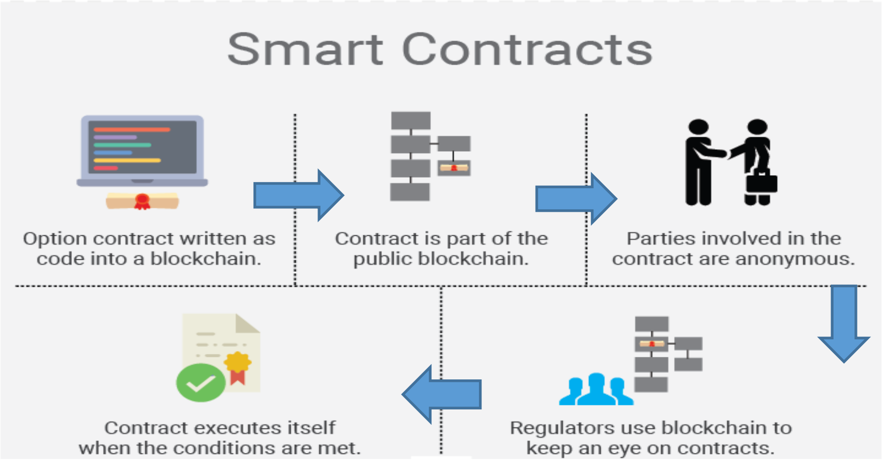
Smart Contracts
Option contract written as code into a blockchain.
Contract is part of the public blockchain.
Parties involved in the contract are anonymous.
Regulators use blockchain to keep an eye on contracts.
Contract executes itself when the conditions are met.

Figure 4: How smart contracts work.

2.2.1. Technical terms:

For the purpose of better understanding several key technical concepts of Blockchain technology, several of its fundamental principles will be defined below:

- ***Distributed Network:*** Depending on the type of Blockchain (public or private) organisations and individuals connect to the distributed network of Blockchain through their computers (nodes) which communicate with each other creating a Peer-to-Peer environment.
- ***Node:*** The distributed network of Blockchain technology consists of numerous electronic devices (e.g. computers, smartphones) or also referred to as 'nodes' [45]. Each node in the ecosystem is capable of receiving or initiating transactions through the advantageous P2P protocol of Blockchain.
- ***Consensus:*** Is the process that ensures each node in the decentralised network of the technology agrees on the state of the ledger. It is designed to ensure reliability between mistrusting entities.
- ***Block:*** Nodes collect and store confirmed transactions into a structure called 'blocks'. Each block is connected chronologically ordered with each other, forming a chain and contains a reference (hash) to the immediately preceding block, a nonce and the hash of the transactions stored inside the block. Typically a block in the Bitcoin's Blockchain contains a certain number of transactions because of its limited size (1 megabyte).
- ***Smart Contracts:*** They are similar to common physical contracts (e.g. a contract for paying rent) but in a digital form. Essentially, they are pieces of computer code, capable of monitoring, executing and enforcing an agreement (e.g. automatically withdraw bitcoins from the wallet of the payer every 1st of a new month to pay the rent).
- ***Blockchain:*** Every block in the network contains a reference of the previous block, thus forming a chronologically ordered chain. Hence the name "Block-chain".
- ***Validation of Transactions:*** Participants in the Blockchain initiate transaction by sending them to nodes connected to the network who distribute them to the remaining nodes in the network in order to reach to a consensus (agreement).

- ***Digital Signature:*** In simple terms, it is the digital equivalent of real life signatures. People use them in order to show that they have approved a document or a transaction. Specifically, in a more technical detail, it is a mathematical technique used to validate the integrity and legitimacy of a digital message or document. Moreover it is intended to solve the problem of tampering and imitating in digital communications and transactions. In Bitcoin's ecosystem its purpose is to verify that someone is who they say they are. Every transaction in Bitcoin protocol is digitally signed with the sender's private key, ensuring that only the owner of the account (wallet) can send money from it.

2.2.2. Advantages of public Blockchain technology:

Blockchain is not a new technology rather a composition of various technologies. It is built from a combination of five technological elements: 1) Public-Private Key Cryptography or Asymmetric Cryptography, 2) P2P Network, 3) Platform (distributed consensus network), 4) Hashing, 5) Proof of Work consensus mechanism. Utilising those five components allow the creation of different type of Blockchains (Ethereum, Hyperledger, Metaverse and NEM) by selecting different methods and mechanisms suited to the purpose of the intended Blockchain (e.g. Ethereum uses 'Proof of Stake' consensus mechanism in opposition to Bitcoin's 'Proof of Work') [37]. However the first Blockchain that was produced is the Bitcoin's Blockchain. Below the advantages of Bitcoin's Blockchain are listed in order to provide a clearer insight why the technology is so appealing to the business world.

Disintermediation:

This is a core concept and benefit of Blockchain technology. It is designed to be distributed and synchronised across networks, which can be remarkably beneficial for businesses and multi-organisations like supply chain management and financial syndicates. Additionally, it eliminates the need for a middleman due to the inherit consensus mechanism, thus making transactions faster. Furthermore, each participant in the network has access to the complete information and state of ledger. There is no single entity that controls the information of data.

1) **Easier for management:** Since every transaction is added to a public digital ledger which is copied to the computers of all participants and is updated every time a new transaction is confirmed, there is no wasted time for the purpose of coordination that occurs with multiple ledgers.
2) **New capabilities for ownership:** Distributed ledgers provide new opportunities and capabilities to people regarding the ownership and provenance of smart property.

Immutability of the data:

In the decentralised network of Blockchain technology, if a transaction is carried out, verified, validated and consequently stored in a block within the Blockchain it cannot be reversed. Additionally it cannot be modified or hid due to the PoW mechanism implemented in the technology. Therefore, every transaction from the first block that was mined on 3rd January in 2009 [39] until now is recorded and visible in the chain. Any participant in the network can see from where and when every piece of data ever recorded in the Blockchain has been sent.

Distributed Consensus Mechanism (Proof of Work):

Before a transaction is carried out between two parties, it must be assessed whether it is legitimate and subsequently confirmed from the participants of the network. These people are called miners and confirm transactions through the process of mining where they utilise the Proof of Work consensus mechanism of Blockchain. They must compete in a race to solve complex mathematical puzzles which require great amount of computing and electrical power to be solved. Through this process, everyone in the network is confident that the transactions are valid because immense amount of work has been done in order for the transaction to be confirmed. For that reason there is no possibility of fraudulent activities within the network.

Encryption:

Each block in the Blockchain is heavily encrypted by the use of Public-Private Key Cryptography. Every user has a public key, which is his address from where he receives and sends funds and a private key which is unique to every user and must be kept secret. The use of private key is for the purpose of signing the transaction he wants to commence in order to prove that he has access to the funds he wants to send. In addition, the encryption contributes in the preservation of security and distinctiveness of each block.

Transparency:

Public Blockchains are shared, which means anyone can participate in the network as long as he has a computer. Additionally, everyone can view every transaction that was confirmed by the miners since it is not possible to hide certified transactions.

Chronological order:

Every transaction that is confirmed, its details are stored in a block alongside with the timestamp that happened. That way the chain of blocks is historically ordered from the latest (first mined block) to earliest date (latest mined block). This attribute prevents fraudsters from malicious attacks on a block since they would have to rewrite the data that comes afterward entirely.

Peer to Peer Transmission:

In Blockchain technology every transaction is taking place between the network’s participants in place of a central server. In essence, every node stores and relays information to the other nodes. Because of this the state of the digital ledger is quickly transmitted and updated to every node in the network.

Trusted:

The network's distributed and decentralised nature of the technology requires the participating nodes to come to a consensus, which consequently allow mistrusting parties to carry out transactions between each other in a secure environment that otherwise would not be able to happen without the monitorship of a trusted third party.

Availability:

In Blockchain system, redundancy is provided by means of replication across the nodes. That way there is no risk in loss of records or coordination problems between participants about the state of the ledger because there is not a single node crucial for the state of ledger for the whole network. Moreover, because of the distributed network of Blockchain, there is not a central point of failure like the centralised databases where if an attacker manage to access the database he can modify or delete any data stored inside.

2.2.3. Disadvantages of public Blockchain:

Despite the significant benefits and notable societal impact, Blockchain technology encounters certain challenges. They are as follow:

Tremendous energy consumption:

Every node in the network participates in the 'consensus' process in order to maintain the legitimacy of transactions. Despite its tremendous profits such as fault-tolerance and ensuring the data stored in the blocks is unalterable and permanently saved, it is a very uneconomical and energy-exhaustive procedure. Specifically the consensus mechanism requires a lot of electricity and computational effort to be achieved in contrast to the considerably less energy consumption for maintenance of a single ledger in a centralised database [42].

Slower performance:

Because of the distributed nature, Blockchain technology is slower than a common centralised database since all the nodes connected to the network need to update their copy of ledger every time a new block is mined compared to the much faster update of the single ledger in centralised databases.

Complexity:

Blockchain technology is quite complex for a person to understand, without any technical knowledge of DLT and cryptography. Therefore, it will take a lot of time and effort in order for the technology to be adopted and used by the general public.

Security concerns:

One of the most crucial security issues that can happen in the network of Blockchain technology is referred to as '51% attack'. Specifically, in the distributed ledger system, nodes (computers) must reach to an agreement so every participant can be confident about the legitimacy of the transactions. If more than half of the network computers (at least 51%) work collaboratively, they can interfere with the process of recording blocks since they would control the majority of the network's computing power [43]. In addition they can even change the financial history of the chain entirely. As a result bitcoin mining pools in the network are closely tracked by the other participants to ensure no entity has so much control over the network.

Scalability: In Bitcoin's Blockchain, a block is mined on average every 10 minutes while in Ethereum's Blockchain it takes 12-14 seconds [47]. Furthermore, the amount of transactions that can be processed is very low. For example, Visa can process 50,000 transactions per second while Bitcoin's and Ethereum Blockchain seven and fifteen transactions per second respectively [48]. As a result it is obvious that Blockchain technology is not ready yet for daily commercial use on a large scale.

Privacy: Most Blockchains utilise distributed ledger technology which provides total transparency in the system. Unfortunately, enabling data to be viewed and accessed by anyone in the network is not always useful. For certain Blockchain applications privacy confidentiality is necessary.

Implementation: A major problem of Blockchain in order to utilise its technology, is the necessity of enforcing changes or complete replacement of existing systems and procedures within a business [67]. This is because of the way it works and its decentralised nature. Additionally, the solutions it offers are radically unrelated to the way current systems and procedures work. Hence, businesses and companies that are willing to adopt the technology need to carefully plan the conversion from their prevalent systems and technologies to the implementation of Blockchain technology.

2.2.4. Distributed Ledger Technology (DLT):

Distributed Ledger Technology refers to the ability of users to store and access information and records associated with digital assets (smart property, ownership) in a shared cryptographically encrypted database that operates without being monitored by a central authentication system. In particular, a distributed ledger system (DLS) is based on DLT a broader term to describe technologies that distribute records of information [40], which is essentially a database that is spread across the independent participating nodes (computers) of the system. Further, DLS can be classified in three categories: public (permission-less), private (permissioned) and hybrid (a combination of a private and public DLS). The mentioned types of DLS will be explained in detail in *section 2.2.4*. What separates apart DLS from common centralised databases is the fact that there is no central authority maintaining the ledger. Each node in the network is responsible for the preservation of the ledger by recording every update that changes its previous state. Once an update happens the nodes participate in a process called 'consensus'. Basically, they interact with each other to reach an agreement about the state of the ledger. When they successfully agree the whole ledger is updated and a copy is stored in every node of the network. That way every participant in the system is able to see the latest block or transactions that have been confirmed without a single node having a copy of the previous ledger's state. Another feature of DLT is Blockchain technology is the first fully functional DLS that utilises DLT, which allows users to record transactions and transfer assets (money, smart property) and ownership (healthcare records, personal identity) peer-to-peer without a central authority regulating the process, a characteristic of centralised databases. However DLT does not have to be decentralised or public and can exist in various forms such as hybrid and private. An example of a hybrid Blockchain utilising the DLT is 'XDC', developed by a Singaporean company called XinFin [41]. In addition, noteworthy private Blockchains are 'Corda', an open-source Blockchain-based project for recording and processing financial agreements intended for B2B, 'quorom', created by JPMorgan financial institution and 'Hyperledger' invented by The Linux Foundation to create inter-professional Blockchain technologies [41]. In summary, DLT has the potential to radically change how transactions between business-to-business (B2B), business-to-consumer (B2C) and P2P in our society are carried out by improving their resilience, transparency, efficiency and reliability.

2.2.4.1. Examples of Distributed Ledger Technology instances:

In this paragraph various samples of DLT will be briefly described. Bitcoin system was the first implementation of DLT and has been explained extensively in *section 2.1*, therefore it will not be included in this section.

- ***Ethereum:*** In 2013 the concept of Ethereum was described in a white paper by its creator called Vitalik Buterin and publicly announced in January 2014 [50]. Ethereum is a Blockchain based open source distributed computing platform. Ethereum utilises the Blockchain technology in a different way from Bitcoin's system. Specifically, its network is not used to carry out transactions or to store data but to create smart contracts and Distributed Autonomous Applications (DApps) [49]. Essentially, it allows the creation of applications that are executed automatically when specific conditions are met. It is similar to Bitcoin, because it allows the creation of digital payment systems that are independent of any central authority. However, it is more flexible than Bitcoin protocol, because users can not only transfer money between each other (its cryptocurrency is called 'Ether'), they can create 'smart contracts' as well. These contracts are created through it's inherit programming language called 'Solidity'. The Ethereum platform operates differently from Bitcoin protocol, for example it utilises a consensus mechanism called 'Proof of Stake' rather the 'Proof of Work', the one Bitcoin uses. It is regarded by many experts as a disruptive technology with the analogous potential of Bitcoin to change not only how the Internet works but also revolutionize multiple services and industries [50].
- ***IBM Blockchain-Hyperledger Fabric:*** In 2015 The Linux Foundation announced the creation of Hyperledger project. IBM released it's Blockchain on 20th March 2017, which is based on the open source Hyperledger Fabric, a project developed from The Linux Foundation [51]. It is a private (permissioned) Blockchain system that utilises numerous Blockchain technologies frameworks such as: Fabric, Burrow, Iroha, INDY and Sawtooth Lake [52]. In essence, it is an open source collaborative effort to develop cross-industry Blockchain technologies hosted by The Linux Foundation with partners from various industries like finance, banking, IoT, supply chains and manufacturing. What separates apart Hyperledger from common Blockchains is its privacy. In the system all transactions are encrypted and only relevant people-businesses in the network are allowed to decrypt that information, thus identities and transaction details are concealed from unauthorised third parties. This is why the specific Blockchain is widely used for interactions between businesses and consortiums. Furthermore, contrary to Bitcoin's 'Proof of Work' mechanism,

Hyperledger utilises a different consensus mechanism termed as ‘Byzantine Fault Tolerant (PBFT) algorithm [5]. As a result, in Hyperledger’s Blockchain there is no cryptocurrency as consensus is not reached through the process of mining like in Bitcoin.

- ***Corda:*** is a decentralised distributed ledger that provides API’s and codes for companies in order to help them build Blockchain applications [53]. It is developed by R3 CEV, an enterprise software firm with a network of over 200 banks and financial institutions [54] and is described as a private (permissioned) blockchain with a focus on financial applications for businesses. It allows the creation of distributed apps known as ‘Cordapps’ and immutable records for financial purposes as well. Moreover, smart contracts can be generated and executed in Corda’s Blockchain, however they are written in Java unlike Ethereum’s Solidity programming language. What set apart Corda’s Blockchain is that there is no consensus mechanism or cryptocurrency unlike Bitcoin’s and Ethereum’s Blockchains. It uses an infrastructure called “Notary” for chronologically ordering and validating transactions [55]. Eventually, the ultimate objective of Corda Blockchain is to eradicate the costly fees that occur in business transactions by eliminating the business intermediaries. Finally, because it focuses only in the financial industry, its architecture is much simpler than Ethereum’s and Hyperledger’s. As a result, it is considered safer and more efficient compared to other business-oriented Blockchains.

2.2.5. Types of Blockchains:

As mentioned in the above section (2.2.4) there are various types of a distributed ledger system. The distributed ledger systems can be open (permission-less) or private (permissioned). For example the distributed ledger system that undergirds Bitcoin's and Ethereum's Blockchain is a public type DLS while the DL of Corda and Hyperledger Fabric is private. In this section I will describe the diverse types of existent distributed ledgers as well as their differences. An illustration of the different types of networks is provided beneath.

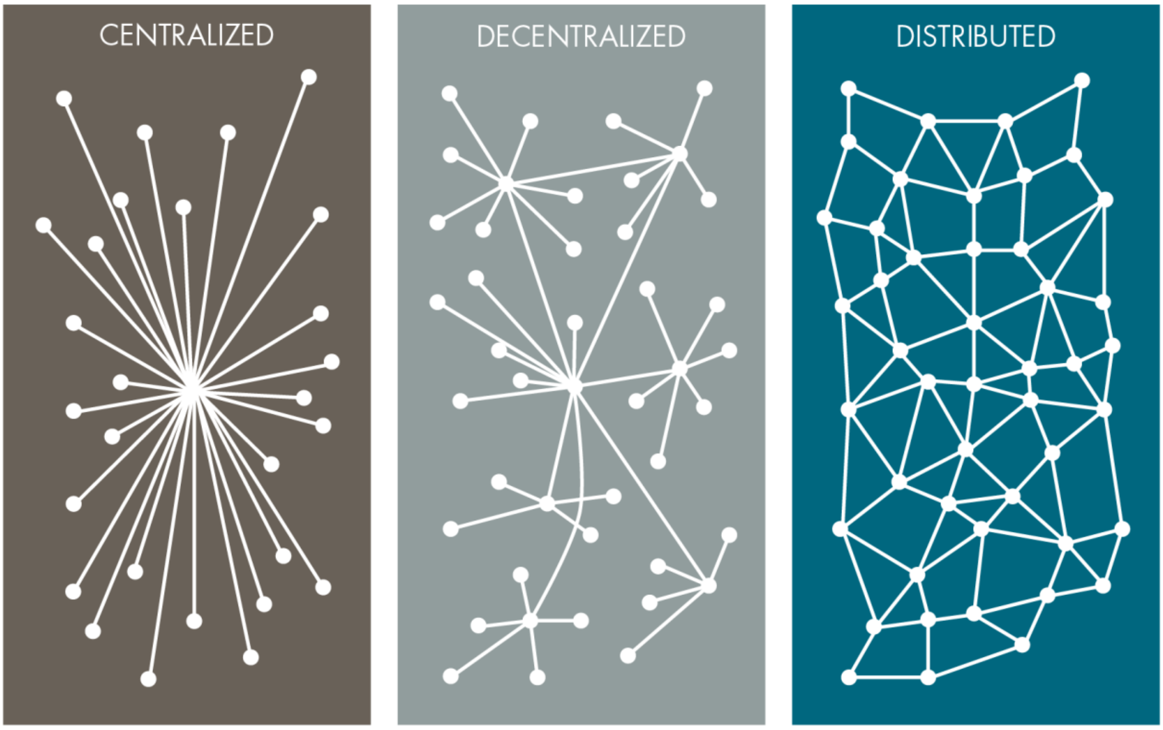

Figure 5: Different types of network.

The centralised type of network is commonly used for the operation of a single company or institution (e.g. banks), where the administrator is in total control of the database/ledger. A decentralised network is used in the public (permission-less) Blockchains like Bitcoin and Ethereum where any individual around the world with a computer can participate. Finally, the distributed network is a combination of a private and public type of network also known as hybrid/federated. It is similar to the decentralised network however all the participants are known and trustworthy. An example of such network is Corda and Hyperledger Fabric Blockchains. The following arguments are suggested in order to choose the most suitable type of network [60]:

Select:

- Centralised network: if scaling and fast growth is not a concern.
- Decentralised network: if a scalar problem needs to be solved quickly.
- Distributed: if you are solving a scaling problem and individual supporters are available.

Permission-less (Public) Blockchains:

Bitcoin and Ethereum are the most well-known examples of a permission-less type Blockchain. This indicates that their DLS is public, thus allowing anyone from the world to be part of its decentralised network, without the need for approval from an entity. The only requirement for a user, in order to be able to join the network and carry out transactions with the other participants, is a computer, also known as node. Because of the lack of a central entity each participant has a copy of the entire ledger stored in his computer. Therefore, every user that is part of the network has access to all the transactions that have been carried out in the ledger. It is suggested that a public or permission-less Blockchain should be used when unknown mistrusting entities want to interact with each other without a trusted central authority monitoring their transactions [56].

Permissioned (Enterprise) Blockchains: Permissioned Blockchains can be classified into two categories. Fully private and private-public or hybrid Blockchains. Despite the substantial importance of public Blockchain, which is accessible by anyone thus making it suitable for a large variety of applications, there are certain applications where the information regarding the transactions of the participating parties must remain private and invisible to the general public. Such applications are: financial transactions, medical records exchange and transport of merchandise (supply chain management).

- **Private Blockchain:** This type of Blockchain is suitable for use within an individual organisation (e.g. Bank, Organisation) and the participants are normally internal users. Only the participating users are capable of appending blocks in the chain as well as accessing the information. Usually, these users are preselected by the owner or administrator of the ledger to join the network and usually sets the ledger rules. Since, they are all trusted entities there is no possibility of a fraudulent incident occurring within the network. However, private Blockchains are more susceptible to attacks unlike public Blockchains because the consensus mechanism in place (typically a voting process) is much lighter than PoW, due to the fact that all participants are considered trustworthy. Notable private Blockchains are Multichain and MONAX [57].
- **Consortium Blockchain:** A federated or consortium Blockchain operates under the leadership of a group. Similarly, to private Blockchains they do not allow anyone to participate in the process of verifying transactions in their network. Moreover, a consortium or hybrid Blockchain ensures that every transaction is private but must still be verified by the majority of the participants. The consensus process implemented in this type of Blockchain is managed by a certain number of nodes [57]. For example a federated Blockchain could consist of ten financial institutions. Each institution represents a node in the network and if at least six out of ten nodes agree about the validity of a block and sign it, then it is appended in the chain. While the state of the ledger gives equal rights to every participant regarding viewing, and approving a block, the identity of the transacting parties is not visible to all the participants in the network [59]. Noteworthy, example of a hybrid Blockchain is Corda, developed by R3 CEV company.

	Characteristics of different types of Blockchain		
	Public Blockchain (No central authority)	**Private Blockchain** (Single organisation)	**Consortium Blockchain** (Multiple organisations)
Participants	Permission-less ▪ Anonymous	Permissioned ▪ Known and trusted individuals	Permissioned ▪ Known and trusted individuals
Level of trust	Not necessary	Necessary	Necessary
Consensus Mechanisms	*Proof of Work, Proof of Stake* ▪ Energy (Computational power, Electrical consumption) labour	*Voting or multi-party consensus algorithm (BFT)* ▪ Low energy consumption, ▪ Faster	*Voting or multi-party consensus algorithm (BFT)* ▪ Low energy consumption, ▪ Faster
Transaction Approval Frequency	*Long* Average: 10 min (can be longer)	*Short* 100x millisecond (one tenth of a second)	*Short* 100x millisecond (one tenth of a second)
Access to data	Open read/verify	Permissioned read/verify	Permissioned read/verify
Asset	Cryptocurrency (e.g. bitcoin, Ether)	Any type of asset	Any type of asset
Ownership	No entity in control	Owner/Administrator of the ledger	Owner/Administrator of the ledger

Centralisation/Intention	Decentralised/Peer-to-Peer	Semi centralised/ Single business	Semi-centralised/Business-to-Business
Examples	Bitcoin, Ethereum	Multichain, MONAX	Hyperledger Fabric, Corda

Table 1 Sources: [61] and [62]

3. Successful Blockchain applications and their characteristics:

Blockchain is a technological innovation that brought to the society more than just Bitcoin. It is capable of transforming the society thoroughly by increasing efficiency and trust over multiple areas of the economy. Subsequently, many software developers, technology enthusiasts as well as world renowned entrepreneurs were fascinated by the potential of this developing technology. Specifically, Sir Richard Branson, the founder of Virgin Group along with credible companies with international prestige like IBM and Microsoft support the technology and acknowledge its potentiality [63]. As a result, many small and medium-sized enterprises (SME) and large organisations from various industries started adopting and implementing the technology to streamline the processes within their constitutions. In addition, technology supporters and developers begun developing decentralised applications (DApps) via Ethereum platform, an equally emerging and disruptive Blockchain. As a consequence of this rise in the interest and acquisition in business processes of Blockchain technology, there are numerous applications in existence [65]. Therefore in this section the four most conventional and well-documented Blockchain-based applications will be described in conjunction with their characteristics.

3.1. Digital Currencies:

One of the earliest applications for Blockchain technology has been digital currencies related applications, like Bitcoin. Initially, detailed in a white paper called “Bitcoin: A Peer-to-Peer Electronic Cash System” published by Satoshi Nakamoto in 2009, the system relies on the decentralised nature of its undergirding technology known as Blockchain in conjunction with its enhanced security due to cryptographic algorithms in order to set up its own digital currency (bitcoin) or commonly referred as cryptocurrency (the term cryptocurrency derives from the process of cryptography, that is required for security purposes [66]). Because Bitcoin protocol is completely decentralised its currency is generated within the system by the participants of the network unlike fiat money like Euro, Dollar and Yen which are issued and controlled by governments and banks. Therefore, bitcoin is entirely undependable to governments and centralised financial institutions, withdrawing the control from central entities and “passing” it to the community. Bitcoin system has been covered in detail in the previous sections therefore there is no need to explain it further in this paragraph.

3.1.1. Bitcoin related applications:

Several applications that are related to the Bitcoin protocol and digital cryptocurrencies are the following:

Fold: is an evolving application that allows its users to spend bitcoins on real life items. Several large companies that have partnered with the app is Starbucks, Target and Whole Food where you can pay with bitcoins to purchase their products [81]. Users insert the amount of bitcoins they want to send and the application generates a barcode. Then, the store scans the barcode and the bitcoins are transferred from the customer to the company in a fast and secure way.

Earn.com: A creative smartphone application developed by the previously titled 21 Inc. [83], a manufacturer of bitcoin mining hardware that rewards its users with bitcoins if they answer the questions set out by the app correctly [82]. However, in order to earn an adequate amount of bitcoins one must have sufficient knowledge with respect to cryptocurrencies. In essence, users contact the public profiles of experts in the field of Blockchain technology and cryptocurrency market to ask for advice or have their queries answered without revealing any personal information. Eventually it is an innovative application that rewards experts with bitcoins and simultaneously assist people with little or no technical knowledge understand in depth the emerging Blockchain technology.

Gliph: is another mobile application founded in 2012 by Nicholas S. Asch and Rob Banagale [85] that serves as a messaging application while also allowing users to initiate financial transactions, typically bitcoins with other enlisted users [84]. Registered users can send cryptographically encrypted messages with each other in a safe and secure environment. Moreover the application is supported by two of the most famous Bitcoins wallets providers, Coinbase (largest bitcoin wallet in the United States) and Blockchain.info (favourite wallet among Bitcoin supporters) [86]. Users can either create a new wallet or use an existing one to transfer bitcoins to their friends. All the bitcoins are sent, received and consequently stored within the wallets of the mentioned providers because Gliph does not have its own bitcoin wallet. However it allows its users to connect an existing wallet to their Gliph accounts or create (and attach) a new wallet to the respective account. By merging a messaging service and financial transaction system in one application, Gliph application unquestionably stand out from the current applications in the market.

3.1.2. Characteristics of Bitcoin protocol:

Decentralisation: When Satoshi Nakamoto created Bitcoin, his main objective was to eliminate the existence of the middleman (banks, goverments) in order to develop a system of financial transactions, completely independent from central authorities. This means that there is no limit in bitcoins transactions (one could potentially transfer hundreds of bitcoins worth millions in fiat money in a single payment without any inconvenience and delays), there is no possibility of having your account blocked (as in financial institutions), it is not affected by the market conditions or regulatory issues and people are in complete control of their own money and digital assets [68]. It was designed to allow any individual around the world to connect to the network using his computer or smartphone and be able to initiate transactions (send/receive bitcoins, transfer ownership of smart property via the use of smart contracts) with other participants in the network. Any machine that mines bitcoins and processes transactions, is part of Bitcoin's decentralised network. These machines or commonly called as nodes, work collaboratively to ensure the integrity and legitimacy of the transactions via consensus mechanisms (PoW, PoS) that are carried out in the system.

Availability: As stated above each node in Bitcoin's Blockchain collaborates with the other nodes as part of the network. Thus, even if a node disconnects or is unable to perform its activities successfully, the operation of the network is not interrupted at all because the remaining nodes will continue. Furthermore, users can initiate transactions even on banks and public Holidays, dates when financial institutions and trusted third parties are not available which as a result caused inconvenience to people with regard to money transactions.

Availability is one of the major benefits of Bitcoin P2P transaction system apart from its capability to allow anyone to become part of the network due to the decentralised nature of Blockchain. In addition, another drawback is that the operation of centralised institutions is vulnerable to a financial crisis since it would cause a meltdown which would negatively affect the money held in a person's bank account. Further, due to the fact that all information and records are stored in a central database, in case of a successful cyber-attack, the records would be susceptible to modification, extraction and even deletion. This is why bitcoins are much safer than money deposited at the bank, because they are not only available 24/7 and secure by means of cryptography and encryption algorithms.

Simple to set up: Unlike setting up a bank account, which is a lengthy process because of the credit checks and paper work that is required, in the Bitcoin system a user can create a digital address in seconds without having to provide any papers to prove his identity or financial status. As soon as he set up his Bitcoin address, he can start transferring and receiving bitcoins.

Anonymity: As it was already mentioned Bitcoin's Blockchain is public (permission-less) and consequently fully transparent. This means that if Bob and Alice initiates a transaction both of their addresses will be known to each other. Therefore Bob could track all the transactions that Alice has ever carried out by carefully inspecting the chain of blocks. He would know the day and time she received or sent bitcoins as well as approximately evaluate how many funds she has in her wallet. However, there is a counteraction to this process. Typically users in Bitcoin system can achieve anonymity by creating and using multiple addresses for each transaction or generating a new address for a transaction of big value. By having multiple addresses a user can hide his identity, so if Alice created a different address for her next transaction there would be no way for Bob, to track down her transactions from that address since he is not aware it belongs to Alice. Therefore, as an additional security measure, experts advise people to create multiple addresses if they have a large amount of bitcoins in a single address or simply want to stay anonymous [69].

Fast transactions and diminutive fees: A user who is part of the Bitcoin's Blockchain can send money from anywhere to anywhere within a matter of minutes (average ten minutes) in a fast and secure way unlike intercontinental transactions through banks that require at least two business days to be completed. Within that time period of 10 minutes the transaction is being verified by the network and once it is confirmed, the transaction is successful. Furthermore, transactions Moreover, there are no substantial transaction fees with regard to international payments for which a person would have to pay approximately $45-50 if he initiated the transaction through a financial institution (bank, credit card provider) [70]. Nonetheless, transaction fees still exist in Bitcoin but they cost roughly 15-50 cents, a microscopic amount of money.

Divisibility: Bitcoin cryptocurrency can be parted into 8 decimal places and can be further extended if the need arise. Its smallest unit of bitcoin is called 'satoshi' (1 satoshi = 0.000000001 BTC) [71]. Since the maximum number of bitcoins that will ever exist is 21 million, in order to deal with the increasing goods and services, existing bitcoins should be split into smaller amounts. Additionally, bitcoin's characteristic of divisibility empowers people to carry out micro-transactions (e.g. buy coffee) using bitcoins on a daily basis.

Non repudiation: Since every Bitcoin transaction is irreversible that means if a transaction is confirmed, stored in a block and consequently appended in the Blockchain then the recipient cannot claim that the sender did not send the bitcoins.

Transparency and neutrality: Bitcoin system is based on a public (permission-less) Blockchain, which means that any individual who is part of the network can initiate transactions, verify transactions (also known as miners) and inspect the entire history of transactions. Essentially, every single transaction as well as every bit of information stored in the chain of blocks is available for anyone to see. However, the Bitcoin system is heavily encrypted by means of cryptography therefore no human or computer can alter its records. Even if it was possible such fraudulent action would be observed very soon. Moreover, because of its decentralised nature no entity will be in total control of the Blockchain. For these reasons Bitcoin system is neutral and transparent.

Portability: One of the unique characteristics of money is portability. Considering bitcoin has digital form, in effect any amount of money from $0.1 to $1 billion can be stored online or carried on a flash drive. In addition, bitcoins can be transferred within minutes to a recipient anyplace around the world as long as both parties are online.

Traceability: implies that all transactions on Blockchain are trackable by the participants of the decentralised network. Reason for that is that every transaction that is carried out and consequently stored in a block, along with the information related to the settlement the timestamp of the transaction is stored in the block as well. Therefore, because of the chronological order of Blockchain users can view all the transactions that have ever happened from the very first block (Genesis Block) to the most recent that was attached.

3.2. Smart Contracts:

Even though Blockchain technology was developed to assist cryptocurrency transactions in the Bitcoin protocol, software developers quickly realised the potential of this disruptive technology and started creating and implementing 'self-executing' smart contracts. In simple terms, they are similar to declarations and legal contracts people have to sign when they buy a new property (car, house), mortgage, receive a loan or when they want to ensure the related parties will honour an agreement (e.g. If someone lends money to another individual, he should sign a legal document/agreement stating that he will repay the money on the agreed date). With that said smart contracts essentially are contracts in a digital form that are self-executed when the specified conditions in the contract are met while operating in a transparent and conflict-free way. Technically, they are programmable (i.e. it is computer code) contracts which are inserted in the Blockchain and enforce themselves under the right conditions. It works on the basis of: If the event X happens then do Y. Specifically, the smart contract code assists, authenticates and executes appeasement of a transaction or agreement. At greater length, a distributed-based smart contract work as follows: It allows the involved parties of a transaction to consent to the terms and conditions of the transaction, comprising the self-regulating payments under the right conditions. These conditions are written in computer code and accordingly the code is utilised in order to determine the rules and legal consequences along the same line established legal contracts do. Similarly to legal documents such consequences might be payments, benefits of various kinds (e.g. clarity of P2P or B2B relationships, avoidance of disputes between the involved parties) as well as legal punishments [72]. Lastly, the contract is stored on the immutable ledger of Blockchain which allows to the involving parties to view and monitor it. Although Bitcoin protocol facilitates the use of smart contracts, Ethereum's Blockchain was the leading "application" of Blockchain technology that permitted the development and use of any type of contract [56]. The platform was built to allow the development of self-enforcing smart contracts and decentralised applications (DApps) for numerous purposes and various industries. The implementation of smart contracts in Blockchain is necessary because of its immutable decentralised nature. However, smart contracts are not a new technological innovation despite the fact they became popular after the creation of the Ethereum Project platform where they could be utilised to its maximum potential by any individual around the world. The concept was first conceived in 1993 by a computer scientist and cryptographer by the name of Nick Szabo, by using a vending machine to illustrate the idea of a smart contract [75]. Similarly, to a vending machine when a person wants to buy a soft drink he inserts the required amount of money (e.g. $1), then the machine checks if the right amount of money has been deposited and if the condition is met it releases the drink to the payer. In essence, a vending machine has the rules of transaction programmed in it, so if a user does not offer the right amount of money the conditions of the transactions are not fulfilled therefore the drink is not delivered. If on the other hand, the payer inserts more money than it is required, the drink will be given along with the extra money. It is obvious that there is no possibility of a misinterpretation in these automatic transactions provided the code within the digital agreement is correct. This proves, that as long as the right conditions are met the transaction will always be legitimate and successful. Moreover, automatic vending machines not only reduced the transaction costs but also extended their assistance by providing twenty-four-seven (24/7) availability to the people. This resulted, in an increase of convenience for people who could buy goods whenever they wanted and did not rely on the opening times of retail shops. Moreover, the transaction fees one would pay to a kiosk for the same item that can be found in a vending machine are much greater. Hence, another benefit of automation of transactions is the decrease of the fees when purchasing goods. Analogously, smart contracts offer these benefits as well since a vending machine can be considered as a primitive type of smart contract. As mentioned above, a smart contract is nothing more than a written code, so if someone had access to the code within a contract he would be able to change the conditions under which it is executed. This is why smart contracts are developed and stored in a Blockchain because altering a smart contract that is appended in the chain is an unfeasible task. One could say smart contracts are a form of decentralised automation of tasks and arrangements. Because of their automatic executional nature, smart contracts eliminate the need for trusted parties such as lawyers, banks and governmental bodies when a transaction between two parties must be carried out. Moreover, they drastically decrease the transaction fees which one would pay to a third party to ensure the smooth execution of a transaction or agreement. In addition, according to Capgemini paper titled 'Smart Contracts in Financial Services: Getting from Hype to Reality', "consumers can potentially expect savings of $480 to $960 per loan" and financial institutions could "cut costs in the range of $3 billion to $11 billion annually" by reducing processing costs in the origination process in US and European markets [73]. The purpose of a smart contract is to ratify the relationships between people, corporations and the assets they own [74]. As previously explained, the conditions and commitments set in a smart contract are capable of being executed automatically by the network of computers connected to the Blockchain as expeditiously as the involving parties satisfy the conditions detailed in the contract. Below illustrations of how transactions are carried out without and with smart contracts are presented respectively.

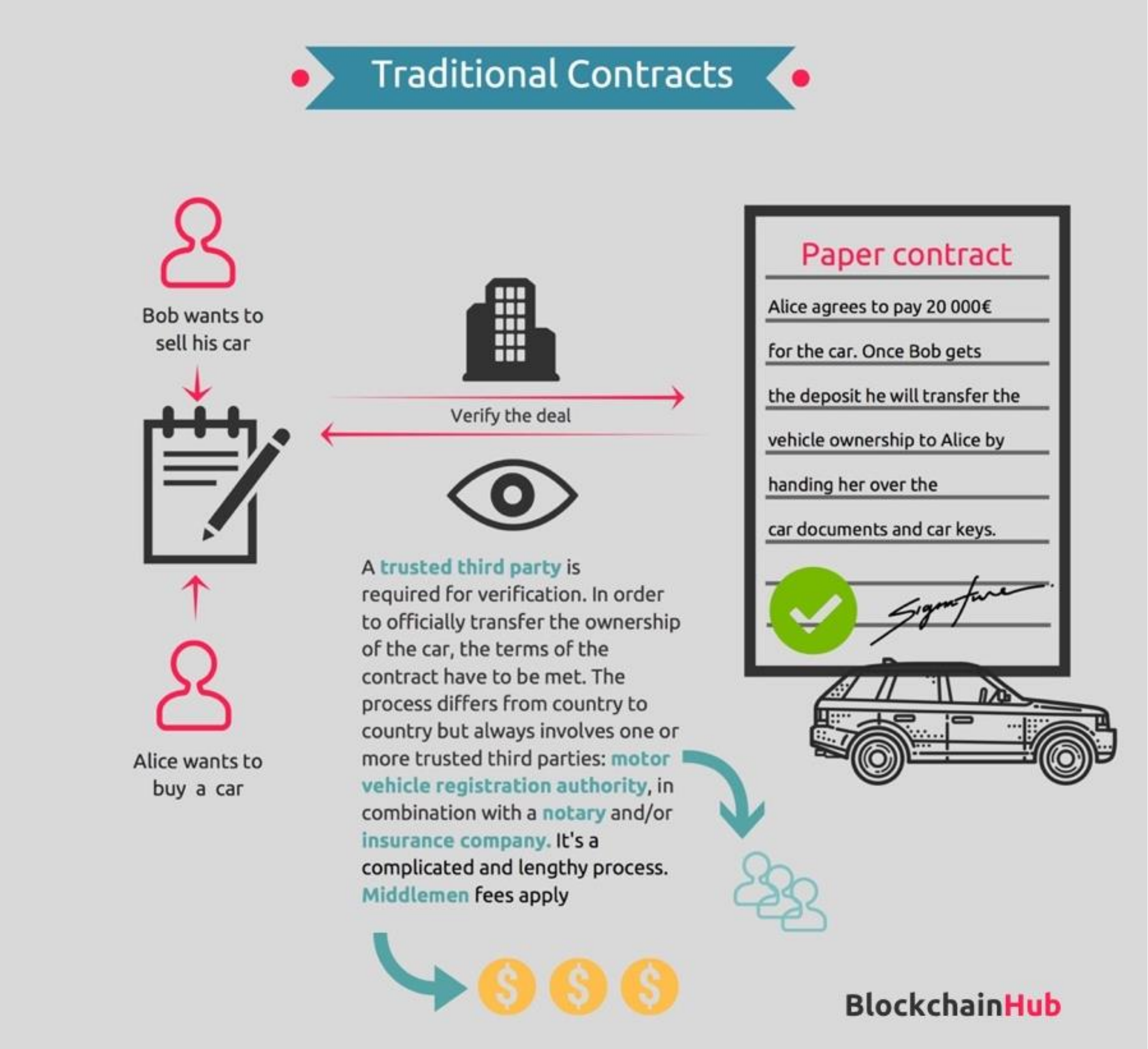
Traditional Contracts
Bob wants to sell his car
Verify the deal
Alice wants to buy a car
Paper contract
Alice agrees to pay 20 000€ for the car. Once Bob gets the deposit he will transfer the vehicle ownership to Alice by handing her over the car documents and car keys.
A trusted third party is required for verification. In order to officially transfer the ownership of the car, the terms of the contract have to be met. The process differs from country to country but always involves one or more trusted third parties: motor vehicle registration authority, in combination with a notary and/or insurance company. It's a complicated and lengthy process. Middlemen fees apply
$ $ $
BlockchainHub

Figure 6: Process of transactions with traditional contracts. Source: [74]

When two unknown and mistrusting parties want to initiate a transaction (e.g. buying/selling a car) the need of a TTP entity is necessary to inspect whether the two parties will honour the agreement of the contract. As a result transactions that require the presence of a TTP are not exceptionally advantageous because of the transaction fees both parties have to pay for the services of the TTP as well as the constraint of time which forces the involving parties to carry out the transaction during the working time schedule of the TTP.

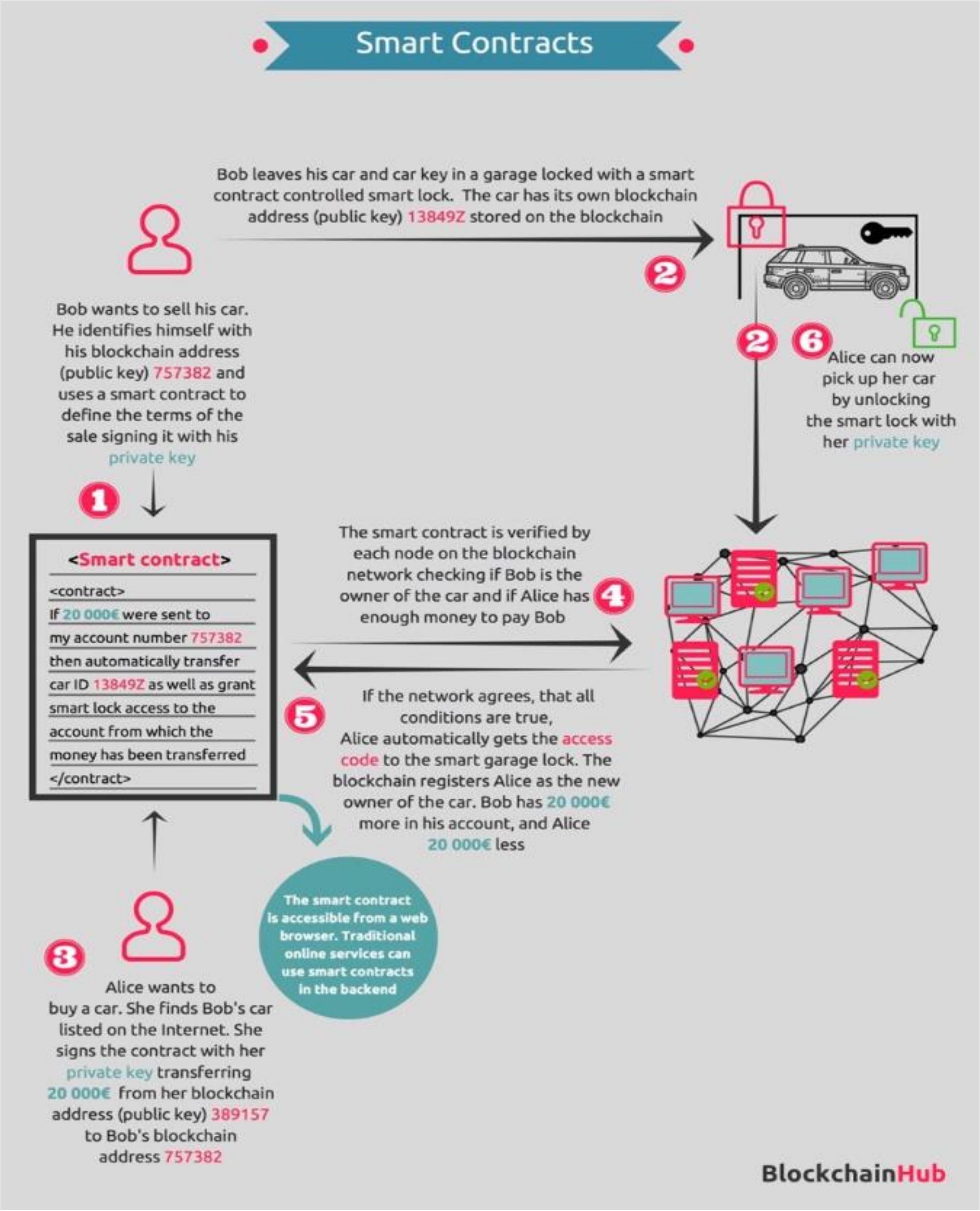
Smart Contracts
Bob leaves his car and car key in a garage locked with a smart contract controlled smart lock. The car has its own blockchain address (public key) 13849Z stored on the blockchain
2
Bob wants to sell his car. He identifies himself with his blockchain address (public key) 757382 and uses a smart contract to define the terms of the sale signing it with his private key
1
2
6
Alice can now pick up her car by unlocking the smart lock with her private key
<Smart contract>
<contract>
If 20 000€ were sent to
my account number 757382
then automatically transfer
car ID 13849Z as well as grant
smart lock access to the
account from which the
money has been transferred
</contract>
The smart contract is verified by each node on the blockchain network checking if Bob is the owner of the car and if Alice has enough money to pay Bob
4
5
If the network agrees, that all conditions are true, Alice automatically gets the access code to the smart garage lock. The blockchain registers Alice as the new owner of the car. Bob has 20 000€ more in his account, and Alice 20 000€ less
3
The smart contract is accessible from a web browser. Traditional online services can use smart contracts in the backend
Alice wants to buy a car. She finds Bob's car listed on the Internet. She signs the contract with her private key transferring 20 000€ from her blockchain address (public key) 389157 to Bob's blockchain address 757382
BlockchainHub

Figure 7: Process of transactions utilising smart contracts. Source: [74]

For a settlement of a transaction between two unknown parties using smart contracts stored in Blockchain, the necessity of a TTP is eliminated. Reason for this is, the network of Blockchain is the guarantor of the agreement instead of the TTP. Specifically, if the network agrees that the conditions of the contract are genuine, that Bob is the owner of the car and Alice has 20,000 euro in her eWallet then the transaction is automatically carried out and Alice is registered in the Blockchain as the new owner of the car while Bob has 20,000 euros more in his eWallet. This verification that is achieved by the participants of the network is possible due to the transparency of the Blockchain, since anyone can see who owns what if a transaction is stored in Blockchain thus they can easily verify who the legitimate owner is. Furthermore, the transaction can be settled anytime from anywhere in the world, offering the opportunity to people to acquire goods whenever they want without relying on a TTP.

3.2.1. Real life applications of Smart Contracts:

Smart contracts have a wide range of possible uses but its greatest potential is in the financial sector for the reason that they can resolve issues of distrust among businesses, people and their property. In particular, the rules that are declared in the contract specify the conditions the implicated parties assent. Nonetheless additional possible uses include: recording identification information (e.g. birth certificates, driver's license, passport), storing public records and land titles (e.g. storing ownership of property, vehicle registration, copyrights of music content), repository of physical assets (car rental, lending an apartment with a smart lock), private records (loans, inheritance) and enforcing insurance policies (e.g. if the house of a person who has a pre-defined contract with an insurance company is burnt down then the contract automatically is self-executed and the insurance money is released to the person without delay, a common issue with regular insurance policies that utilise tangible legal contracts which could take at least several days to activate due to paper work [76].

Additionally, certain companies that make use of smart contract in their business processes are:

Fizzy AXA: Is a French airline company that implements smart contracts in their business to improve their services [79]. Specifically, in September 2017 they started utilising smart contracts in order to compensate their customers in case there is a flight delay. Particularly, if the flight of their customers is postponed and their airlines details are stored in the Blockchain, then a remuneration is automatically deposited to the consumer's bank account. Currently this service is accessible for flights between U.S and Paris with plans to extend their service and cover flights all over the world.

Etherparty: Is a Canadian company that allows its users to create their own smart contracts [80]. Technical knowledge about smart contracts or programming skills are not necessary, in order to create a variety of contracts for the purposes of: real estate agreements, peer-to-peer transactions, escrow contracts and others. Companies, businesses as well as individuals can take advantage of this easily accessible service and as a consequence of the adoption and utilisation of the smart contracts technology, the performance and efficiency of the operations and transactions that are carried out among them will be greatly improved.

3.2.2. Characteristics of Smart Contracts:

Autonomy: Smart contracts are autonomous, which means if the conditions under which the contract is set up are satisfied and the contract executes itself, then the involving parties do not have to take any action [77]. Any agreement stated in the contract will be settled without additional activities from the participants.

Decentralisation: Blockchain is the most suitable technology to facilitate the creation, storage and execution of smart contracts. Because of its decentralised nature, contracts who are stored in the chain inherit certain properties of the Blockchain technology. Since they are distributed everyone in the network must validate the legitimacy of the contract, which means a fraudster is not capable of authenticating the contract by himself and consequently approve the self-execution of the contract. Furthermore, the decentralised nature of the Blockchain, allow anyone from around the world to be part of the network. As a result, this extends the number of people who can access and potentially initiate a transaction via a smart contract.

Immutability: Because smart contracts are stored in the blocks of Blockchain technology it is virtually impractical to alter their contents. As previously explained, the contents of every block in the chain are secured and tamper-proof by means of cryptography algorithms and complex mathematical equations. Moreover, even if altering the contents of a smart contract the network would quickly realise the tampering because the hash of the modified block would change entirely and the appropriate measures would be taken. Therefore, Blockchain technology reassures users that their smart contracts are radically secure and unalterable as long as they are stored in the Blockchain.

Removal of the Middleman: Smart contracts eradicate the need for a trusted third party to serve as a guarantor for transactions between unknown people who do not trust each other. This is because the distributed contracts that are stored in the Blockchain are accessible and auditable by anyone connected to the network. Therefore, because of the fact that anyone can have access to the Blockchain where they are stored along with the certainty about the legitimacy of a smart contract due to cryptography and consensus algorithms, people would choose to carry out a transaction via a smart contract rather than a trusted third party.

Low transaction costs: In essence, smart contract is self-executable computer code that depends on the satisfaction of the requirements stated in its code in order to carry out the transaction successfully. Therefore, as mentioned above, since there are no trusted third parties involved in the transactions, the fees that people would usually pay for the services of the lawyer or an insurance company are greatly reduced. However users still have to pay a negligible fee (also referred as ‘gas’) for the contract in Ethereum’s cryptocurrency (Ether) [78].

Secure: Unknown trust-less parties can carry out transactions through smart contracts from around the world while being assured about the legitimacy of the agreement. A transaction between two parties via a smart contract is only dependable to the specified circumstances stated in the contract. No entity can interfere or alter the conditions under which the contract is executed, therefore the involving parties are confident that there is no possibility of a fraudulent action. Further, because of the independence of smart contracts due to the automatic way they are self-enforced, the existence of a TTP is not necessary thus the concerning parties of a smart contract are supplementary assured that there is no possible risk of being defrauded by a TTP. As a result, it is safe to say that the biggest risk for a smart contract is the code programmed in it being flawed, rather than threats from exterior factors like fraud and breach of security.

Availability: Due to their automatic self-execution nature and the redundancy of a key 'actor' in the current financial system—the middleman, smart contracts offer accessibility and convenience without being dependable to the time schedule of financial or legal institutions, a representative characteristic of prevailing transactions that require the service of a TTP. When the associated parties consent to the ruleset of a smart contract that is appended in the Blockchain the agreement can be carried out any time, any day provided the conditions of the contract are fulfilled. This particular characteristic contributes to the growth in number and efficiency of transactions that are executed across the globe in consideration of the freedom and accessibility it grants to people.

Precision: One of the fundamental necessities of a smart contract, is to document the constraints and requirements in unambiguous detail. This is necessary because if a single obligation is not incorporated in the code of the contract then the transaction would be faulty and consequently unsuccessful. This proves that a smart contract is much more efficient and impeccable than traditional contracts that are more likely to be prone to misinterpretation because of human mistake.

Trust: Smart contracts effectuate definite assurance with respect to their execution. Because of their properties such as transparency and autonomy eliminate the possibility of any error and alteration occurring. Therefore, once a contract is determined, it is executed automatically by the decentralised network of Blockchain faultlessly.

Speed: As it was already stated, smart contracts are essentially pieces of code stored in the Blockchain, that produce certain output once the proclaimed conditions are satisfied. As a consequence the transactions are executed rapidly, an advantage not commonly found in legal contracts since the process of reviewing legal documents manually could take hours or even days.

3.3. Supply Chain Management (SCM):

In Supply Chain Management (SCM) in order for a product to be ready for purchase or consumption, it must pass through various stages and processes including: planning, manufacturing, acquiring required components from various manufacturers/suppliers, storage, delivery and more. Depending on the product the supply chain can expand over hundreds of stages, numerous international locations, several payments from one supplier to another, multiple intermediaries and extend over a lengthy time period (weeks to months). Additionally, the customers cannot be sure of the true value of a product due to the lack of transparency in the prevalent SCM. Despite the drawbacks of the current way the supply chain operates, by utilising Blockchain technology companies could streamline significantly the efficiency and identification of issues and obstacles during the process. Specifically, a Blockchain supply chain can assist the involving parties (manufacturers, suppliers, distributors, and retailers/customers) record the prices, locations, dates, quality and other important information that are necessary for the smooth operation and management of the chain. Moreover, if this information is available and accessible by the relevant parties through Blockchain, it can have considerable impact in the procedures that are carried out in the supply chain. For instance, the visibility (where things are) and traceability (where things have been) of the supplies and components would increase, the possibility of fraudulent actions and counterfeit could remarkably decrease and the organisations would be capable to estimate and predict with greater detail when and on what condition the items will be delivered. The modern supply chain depends to a great extent on paperwork which consists of crucial and sensitive information that due to concerns and fear of the information being leaked to a competitor, resulted in a mistrust between institutions and businesses. Consequently companies stopped sharing data and information between each other. However, Blockchains, the distributed ledgers that generate and store an immutable permanent record of every transaction carried out in every step of the supply chain, creates an unquestionable chain of trust. Every step that takes place in the SCM from the manufacturer to the consumer can be timestamped along with all the relevant information of the transaction between the related parties and subsequently appended in a tamper-proof block within the Blockchain. Moreover, they have the potential to reveal the whereabouts of an asset anytime, the identity of the owner and its status [87]. In addition, Blockchain technology can either be a public (permission-less) or permissioned ledger. In the case of SCM a permissioned Blockchain should be implemented and specifically a Consortium Blockchain which is a combination of public and private Blockchain. Since the SCM consists of many different parties, the data records stored on the Blockchain can be accessed and audited only by authorised parties, typically the ones (i.e. manufacturers, suppliers, distributors and retailers) involved in the supply chain while consumers would have the capability only to inspect the transactions without interfering in the editing and appendment of blocks. Further, because of the consensus mechanism in the Blockchain, there is no controversy with respect to transactions since all participants have the same copy of the ledger. Besides, by improving record keeping, then the settlements of disputes between companies can be improved which will result in faster payments. Also, because of the transparency, consumers can be assured that the products they buy, are of virtuous quality and environmental-friendly. Eventually, reliability and integrity, two key characteristics that are essential in a supply chain management can be found in Blockchain, hence why so many companies are interested in the technology with the purpose of improving the performance of their operations that are carried out in the SCM and tackling issues (e.g. paperwork errors, delay of delivery) commonly found in the current supply chain.

3.3.1. Examples of Blockchain utilised in Supply Chain Management:

As Blockchain gains publicity, large corporations and small-medium-enterprises (SME) started applying the technology in various sectors aside from finance. One of areas where companies experiment the potential of Blockhain is SCM. Below are several examples of Blockchain being utilised in the supply chain.

Walmart and IBM: Walmart was one of the first food giants that started employing the Blockchain technology in order to track the provenance and quality of pork meat that is shipped from China [92]. Specifically, the corporation partnered with IBM and used Hyperledger Fabric, a Blockchain developed by IBM and the Hyperledger Project, an open source project which allows the development of Blockchains and is supported by The Linux Foundation [88]. Particularly, it is a hybrid type of Blockchain which allows access and verification of transactions only to its few trusted and known participants. In this case the involved parties consisted of manufacturers, distributors, retailers and suppliers participating in the supply chain of pork from China to the Walmart stores. By using the innovative distributed technology, Walmart simplified its supply chain and was able to automatically track vital information, such as farm origins, factory data, expiration dates of meat, storage temperature and the quality of the pork, the shipping delivery dates as well as the safety regulations from every facility (e.g. warehouse, factory) where it passed from. The importance of Blockchain in a food supply chain can been seen noticeably because it offers transparency and integrity into the procedures where the food passes through, which reassures the stakeholders and consumers that the health guidelines, are conserved to the uttermost degree possible.

TrustChain and Everledger: TrustChain is a Blockchain-based project that consists of manufacturers and retailers of precious metals, specifically diamonds [89]. It uses IBM Blockchain tools to give the opportunity to the involving parties to validate the place of origin of the diamonds. Customers will be able to track the history of a diamond from the location where it was mined to the jewellery store from where they bought it. However TrustChain is not the first company utilising Blockchain technology in the diamonds supply chain. Another London based company called Everledger has digitally verified and appended information of over 1.6 million diamonds in their Blockchain [90]. For instance characteristics such as colour and carat of a diamond are stored in an immutable block in the Blockchain, where people can easily assess the quality a diamond as well as its provenance and be reassured the respective diamonds are genuine and not 'blood diamonds' (diamonds that are used by dictators and rebels to fund wars against legal governments) [91]. The technology offer the capability to the diamond suppliers and border security agents to substitute the time consuming and prone to human error process of documenting and storing paperwork with an immutable Blockchain ledger. As a result, the never before available to the general public origin of diamonds as well as legitimate significant information regarding the precious metals can be accessed by the potential buyer, improving the relationship of trust between large corporations, suppliers and customers.

BHP Billiton: the largest mining corporation in the world announced it will use Blockchain technology to improve the efficiency and performance of its procedures such as recording the state of the stones located in their drilled holes and secure the data with respect to the shipment and delivery of the precious metals from the mining to the warehouse [93]. The company relies profoundly on vendors nearly at each stage of the mining process, by contacting geologists to examine samples and shipping companies for the transport of their materials as BHP geophysicist R Tyler Smith stated. The technology of Blockchain can facilitate the sharing of data between the company and the involving parties in a secure, fast and efficient way. Moreover, with Blockchain the current paper system of record would be replaced by the reliable distributed ledger of Blockchain, the sharing of important information in real time among multiple parties would be possible and the permanence and inalterability of the records would be guaranteed by the inherit mechanisms of the technology.

3.3.2. Characteristics of SCM:

Decentralisation: By implementing Blockchain in the Supply Chain Management, the related parties involved in the process of the supply chain can have access in the distributed ledger of the technology where significant information is stored. The accessibility to that information would be immensely beneficial for the participants because they could check in real time on which specific stage the merchandise is. Therefore, the communication between them would improve and consequently if any issues occur during manufacturing or delivery, they would be tackled faster and more efficiently due to the fact the problem is visible to everyone involved in the supply chain. Further, due to the decentralised nature of the technology there is no central authority managing the supply chain therefore if something goes wrong (e.g. bad quality of products, delay in delivery) the problem would be identified quickly and the responsible party would face the consequences. As a result the company would not be accountable for that obstacle because all the relevant parties in the supply chain could review the chain of transactions and blame the responsible party. For instance, after auditing the Blockchain they would conclude that the products were delivered on time to the shipping company, thus the postponement is due to their fault. Moreover, because there is no central entity, every party would have a real time ledger stored in their system, where all the information and data of transactions is stored. As a result, many problems that occur because of loss of papers, verifications would not take place anymore, since all the required information and data required for the smooth operation of the SCM could be found online and safely stored by encryption in the Blockchain.

Transparency: An inherit characteristic of Blockchain is transparency. By utilising the technology in SCM all the participants in the supply chain could inspect and review every step that is completed and stored in the Blockchain as well as the timestamp of the event. Accordingly, the shipping company for example would be aware of the exact time the products are ready to be shipped which would result in a lot of time being saved. Further, in the current SCM if customers are not satisfied with a product they blame the retailer company from which they bought it however it is not always fair for the company to be held accountable for every issue. Blockchain could solve these issues by giving the ability to people to analyse the whole chain of transactions and in case a product was in a good condition when it left the warehouse, then the party responsible for the resulting condition (e.g. broken item) would be the distributor. Therefore, everyone in the Blockchain including the party at the end of the chain, the consumer, would be aware of the state and quality of the product at every step throughout the SCM. Consequently the consumers would trust more the companies and suppliers from which they buy the products due to the fact they are aware of every aspect of the product and are assured that the health and safety regulations are met. However the amount of information displayed to an observer can differ, since not everyone needs to have access to all the information (e.g. records regarding the price that companies pay the farmers for example might not be visible to consumers). Lastly, due to the transparency of the goods the involving parties would be aware if the corporate standards, safety and health regulations are met. One of the most well- known incident with regarding the negligence of health regulations is the Chinese 'Milk Scandal' in 2008 [94]. Specifically, The Sanlu Group one of the largest dairy manufacturers in China along with other dairy producers have altered milk powder with a toxic industrial liquid called 'melanine' which resulted in an approximate number of 300,000 children getting hospitalised and six of them eventually dying. With that said, disasters like these could be prevented by using Blockchain, which due to its characteristics of transparency and integrity of data, the company would not be able to degrade the milk as well as disregard the health regulations.

Security: Blockchain can contribute significantly in the increase of security in SCM. By attributing tags to each product and consequently record them in the Blockchain, all the necessary information regarding the items and transactions between parties are stored in the immutable and highly encrypted blocks within the Blockchain. Such information include: origin of product, warehouse location, quality, expiration dates, health and safety regulations and more. Furthermore, malicious parties cannot interfere with the product information because it is practically impossible to modify any record stored in the chain of blocks. These records are indestructible represent an unalterable evidence that guarantee the integrity of the information. Therefore, a fraudulent party cannot counterfeit or rob a certain number of the products, if they have been stored in the chain because any alteration in their quality, quantity or composition would be easily noticeable since the record in the chain would be dissimilar to the reality.

Speed: As already mentioned by implementing Blockchain in SCM, it’s distributed ledger stores all the essential information of the participants and the transactions that take place. Therefore, the technology would radically omit the current paperwork that is required in the prevalent SCM system. Additionally, delays of shipments due to loss of papers or mistakes in documents because of human error would be resolved since smart contracts could be implemented for transactions and due to their accuracy the agreements would be carried out flawlessly in a matter of minutes.

Visibility and Traceability: Resulting from the attribute of transparency, every asset in the supply chain can be tracked at every stage and transaction in real time throughout the chain. Specifically, the participants can follow the items from the manufacturer/producer up to the point of sale (i.e. retail shops) tracking them through every operation. Further, purchasers and companies can be confident for the quality of the items by understanding how the ingredients/components and merchandise are passing through the different subcontractors and consequently reducing or completely eliminate counterfeiting and frauds.

Efficiency: Blockchain can simplify the way administrative procedures are carried out and reduce their respective costs (e.g. lading) by presenting the mandatory data and information through its decentralised ledger. Particularly, processes that require manual inspection (e.g. custom clearance agents, port agencies) could delay the delivery of product significantly especially if the paperwork is wrong or important papers are lost. However, Blockchain can streamline substantially these operations, by storing the necessary papers and legal contracts digitally via its distributed nature technology.

Trust: In SCM system trust between transacting parties is vital and normally is developed over a lengthy period of time, after numerous transactions among the suppliers and companies. When the parties are confident about each other with regard to assurance and reliance, they share data and financial information however due to the great number of manufacturers and the complex market ecosystems trust is not always easy to be built between unknown companies. With that being said Blockchain offers a solution to the mentioned issue. The technology provides a shared immutable ledger which allows crucial information (e.g. payments details, quality of products, delivery requirements, place of origin) to be stored and accessed by the participants of the network. Because of the consensus mechanism, the immutability of the ledger and the encryption algorithms implemented in the technology, the participants are reassured about the legitimacy and the secure storage of the sensitive information. As a result, it is easier for new suppliers or companies to participate in this trustworthy platform and despite the fact that the parties are not necessary to be known with each other, the presence of trust is unquestionable by everyone.

Availability: Since all the information is recorded in the digital ledger of Blockchain, suppliers, manufacturers, companies and consumers can access the online information whenever they need or want to. They can audit the carried out transactions, inspect data regarding the assets, identify on what stage of the supply chain the items are and generally review from which processes the items have been passed through and subsequently will pass as they move through the supply chain. This characteristic of Blockchain technology is really advantageous for SCM, because of the fact that the involved parties need to have constant communication between them. In the current SCM system, the communication between companies and suppliers can be unpunctually due to the different time zones, miss of emails and sometimes expensive (e.g. foreign phone calls). Blockchain addresses this problem by offering a constant access to the ledger where all the transactions and records are kept which participants can access from anywhere at any time.

Automation: Blockchain technology allows the development and utilisation of smart contracts which are digital agreements that self-execute if the conditions specified in their code are met. Smart contracts can have a momentous impact in the operations of SCM. They can practically ensure the performance of unknown suppliers which gives an advantage to companies by providing them the capability to rely on distrusted parties. Furthermore, because of their speed, efficiency and ease of implementation corporations can employ them in their processes to save money and time. Specifically, numerous supply chain transactions can be carried out through the use of smart contracts including: delivery of materials, payments for services (e.g. shipping) and insurance compensations. For instance, a company can specify in a smart contract the specific time, date and location that a shipment must be delivered. If the specified conditions are met by the distributor then the contract self-executes and automatically transfer the declared amount of money set by the company to the distributor. In essence, smart contracts can automate processes in the SCM system that otherwise would require time and continual communication between the two parties in order for the transaction to be carried out with success.

4. Future uses of Blockchain technology:

Blockchain has the potential to become a source of disruptive innovations in numerous industries such as finance, healthcare, education and more. It is a tamper-proof, encrypted and decentralised ledger that is capable of converting centralised processes and organizations to independent and self-sufficient entities. Up to this point, only Blockchain applications related to finance and supply chain management industry have been described therefore in this section I will describe feasible and imminent uses of Blockchain in the healthcare, education and other sectors, to illustrate the humongous potential of the technology and its capability of influencing and transforming the way entire industries operate.

Real Estate: is a complex industry where changes can occur unexpectedly. Currently, the parties that are involved in this industry include: buyers, sellers and brokers. Moreover, the processes that are carried out in the mentioned industry in conjunction with the various parties that need to be involved for a transaction results in slow and unstable transactions. Blockchain can address this issue by utilizing smart contracts in order to carry out transactions between unrelated and distrusting parties. Due to the fact that people rely on trusted third party entities with regard to property purchase, they are forced to pay costly transaction fees to the TTP as well as dealing with a laborious and time consuming process of documentation. In addition, they have to reveal sensitive information such as identifying information and financial income to the TTP. Nonetheless, Blockchain technology can eliminate the need of a TTP and allow people to initiate transactions while being anonymous via the use of smart contracts. For instance, a Ukrainian developer that goes by the name Mark Ginsburg sold a property located in Kiev to the co-founder of TechCrunch for $60,000 through a transaction where smart contracts were used [95]. In essence, smart contracts are computer code that self-execute when the declared conditions in their code are satisfied. Therefore, people do not have to rely on a TTP since a smart contract does not need it to operate. Additionally, the disclosure of personal information is not necessary and all they have to do is to meet the requirements and once this happens the contract will self-enforce. Consequently, once the money (typically cryptocurrencies like Ether or bitcoins) transfer to the seller's wallet, the private key which represents the owner of the digital property (house) will be transferred to the buyer.

Digital Voting: Elections require verification of voter's identity, safe storage of records and a trustworthy register that calculates the votes. Blockchain technology can fulfil these requirements due to its immutable, decentralised and encrypted ledger. By casting votes as transactions, a Blockchain can be created that can monitors the number of votes being submitted. Digital voting could become reality in a few years by storing the votes on the Blockchain where they are safe from any attempt of tampering and modification as well as available for everyone to see the results. A start-up company by the name of Follow My Vote has released an alpha version of a digital voting platform that utilises Blockchain technology [96]. The benefits of a digital voting platform are numerous, including: decrease of costs, accessibility and convenience to voting and integrity of votes. In addition, another major benefit is accessibility, since through electronic people with disabilities can participate in the process of voting from their homes. Finally it reduces significantly the human error factor and provides transparency, auditability and accuracy of the results.

Forecasting: Blockchain is capable of disrupting even the forecasting industry. Augur is a decentralised prediction market platform, built on the Ethereum Blockchain which allows its users to forecast real life events and if they are correct then they are awarded in cryptocurrency. The concept of a decentralised platform for prediction market was coined in 2014 by the co-founders Jack Peterson and Joey Krug [97]. The platform operates on the basis of game theory and wisdom of the crowd ideas because prediction markets accomplish greater forecasting accuracy than an expert does. Due to the decentralised nature of the platform, participants from around the world can participate, either by asking the outcome of a forthcoming event or by buying/selling shares on the outcome of the forecasted market they wish to participate. Further, due to the large number of participants, users do not have to rely on the predictions of an individual with regard to a specific event. Additionally, all the money collected from the forecasting of an event are stored in a smart contract. Once the reporting of predictions is finished, the smart contract self-executes and allocates money based on the answer each user submitted. If he predicted correctly then he earns money otherwise he loses them. Finally, by rewarding reporters who predicted correctly the outcome money the Augur serves as a genuine prediction market platform.

Internet of Things (IoT): Another possible utilisation of Blockchain technology is in the IoT in conjunction with smart contracts. By using smart contracts, the creation of autonomous systems is feasible, which would spend money for the resources they deplete and earn money for the services they provide [56]. Particularly, specially designed sensors would gather data from the outside world and store it inside smart contracts within the Blockchain. However, if the values collected are not correct or have been modified the Blockchain cannot detect that and certainly is not accountable. Specifically, if an entity had control over the sensors or could alter the data it collects then important issues would emerge. If a way is found to ensure the legitimacy and immutability of the data the sensors collect then the coexistence of Blockchain and IoT along with the aid of smart contracts would offer a wide range of opportunities to the people.

Tourism: Nowadays people especially tourists, often seek recommendations for their purchases (e.g. souvenirs) from online review applications where they get informed about places to eat, historical sites, hotel reviews and more. It is very common especially for inexperienced tourists to have absolute faith on these reviews despite the fact they might not be accurate or modified by central entities like hotels and restaurants. Therefore, Blockchain technology could be implemented to ensure the legitimacy and integrity of the reviews [98]. Specifically, a review system could be created with the support of Blockchain, where each review can be traced back to an individual. However, the identity of the users does not have to be disclosed, instead each review could be signed with the private key of the user which guarantees that each review is distinct from the other since they have been signed with different private keys. That way, the duplication of reviews by the same entity would be impossible. In addition, since the reviews would be stored within the blocks on Blockchain, the information would be immutable.

5. Characteristics of tasks that would benefit from Blockchain technology:

In this section the characteristics of tasks that would improve to a great extent by the implementation of Blockchain will be described. As it was stated in the Initial Plan, the most frequent (mutual) characteristics of the successful applications that were explained in section 3 will be portrayed below.

Traceability/Transparency: By implementing Blockchain technology in a process the characteristic of traceability would improve to a great extent. As already stated, the distributed ledger technology allows any individual connected to its network to access information about any transaction that has been carried out throughout the history of the chain. Therefore, by adopting the Blockchain technology, as a result every operation, procedure and transaction that is carried out will be transparent. This is because of the decentralised nature of the DLT which gives the capability to every node to have a copy of the ledger, which is updated as soon as a block is appended to the chain. The attribute of traceability resulting from transparency would be very beneficial in a SCM company or in a financial system of transactions like Bitcoin.

Availability: Companies who want to ensure their services will always be online and available, could utilise Blockchain technology to achieve their goal. Specifically, a corporation that wants to provide constant accessibility to their users, should adopt the technology of Blockchain. The trait of availability results from the interconnection of the thousands of nodes in a DLS which means even if a node fails to operate normally the network of the Blockchain would still be online because of the fact that every node has a copy of the ledger and there is no single node that has the only copy of the ledger, like in centralised databases. The characteristic of availability would benefit companies in the SCM sector, consortium of financial institutions as well as Healthcare institutions where the accessibility of medical records at any time is exceptionally important since the survivability of human lives depends on the availability of the patient's medical record.

Speed: Corporations could implement Blockchain technology to improve the efficiency and speed of their processes. Because of the fact that every node is connected to the decentralised network as a result it would have access to the same ledger thus the communication between them would enhance. Furthermore, DLT facilitates the use of smart contracts, which are programmable code that is self-executed when its specified conditions are met. Therefore, operations that are supported by Blockchain technology could utilise smart contracts to speed-up the transactions between them, lower the transaction costs since a TTP is not necessary when smart contracts are being used and generally improve the performance of their operations.

Security and Integrity: DLT technology enchases substantially the immunity of any task due to it's inherit cryptography and encryption algorithms. In DLS every block that is appended in the chain of blocks contains the hash of the immediately preceding block, which means even if a fraudster managed to modify a block (a task virtually impossible) the hash of the modified block would change entirely and consequently the hash of the next block and so on. A transformation of the hashes within the blocks would be easily noticeable and the issue would be addressed relatively quickly. So, because of the security measures of a DLT any company that adopts the technology would have consequently higher security tolerance. This property can be useful for tasks where multiple mistrusting entities collaborate together and reliability and trust are not ensured, like in Bitcoin transactions or in SCM systems.

Decentralisation: Blockchain technology eradicates the necessity of a trusted third party thanks to its decentralised nature of the ledger. Due to the consensus mechanisms (PoW, PoS) the nodes of the network collaborate together to ensure the legitimacy of the transactions and operations that are carried out within the Blockchain. Thus, tasks and operations where there is no central authority can utilise the distributed ledger technology to improve their transparency, availability, reliability and decrease the burden of storage since the amount of information being stored would distribute equally over the network.

Anonymity: The identity of each node that is connected to the decentralised network of Blockchain is encrypted by means of cryptography. Specifically, the term anonymity is false, because in a DLS the nodes are anonymous as long as they don't initiate in a transaction. The moment they carry out a transaction, it is stored in a block within the chain, therefore anyone can audit and track the history of transactions of that individual and approximately be aware of the amount of bitcoins in his wallet. If he doesn't generate a new address he would be pseudonymous and not anonymous. However, Blockchain technology still offers the ability to its users to remain anonymous as long as they use a new address for each transaction. Eventually, DLT can increase and subsequently preserve the anonymity of its participants as long as they are consistent to changing addresses regularly. The trait of anonymity is remarkably useful in financial systems where the involving parties are unknown and there is no trust between them.

Trust: In processes where mistrusting parties are involved a measure in order to increase trust among the relevant parties is by utilising the Blockchain technology. As stated previously, in a DLS the nodes who typically do not trust each other work collaboratively in order to keep the copy of the ledger's state updated by communicating with each other. Moreover, through consensus mechanisms (PoW and PoS) they ensure that the transactions stored in the blocks are legitimate by competing in a race to solve complex mathematical puzzles. Because of that mechanism trust between unknown parties is ensured and cannot be questioned by anybody. In this way, corporations and businesses can make use of the Blockchain technology to guarantee that trust and reliability in their operations and settlements are present.

6. Conclusion

The purpose of this report was to investigate the practicability of Blockchain applications. In order to produce a comprehensive report I needed to carry out an extensive research on the Blockchain technology, its components and its most well-known applications in various industries such as finance, supply chain management and smart contracts. In the Background section i introduced the Bitcoin the first implementation of the emerging Blockchain technology, which provides decentralised management, an immutable track of records, availability of information as well as security and privacy. Then, I outlined all the necessary information with regard to the cryptocurrencies, a type of currency in digital form used primarily in financial systems that utilise DLT (e.g. Bitcoin, Ethereum). In addition, the renowned issue that goes by the name ‘Double Spending’, commonly found in digital currencies has been explained as well as how Blockchain technology prevents it from occurring. Further, the different types of Blockchains (public, private and hybrid) were described in detail along with their similarities and differences through a thoroughly inclusive table. In addition, an explanation regarding the distributed ledger technology (DLT) has been provided in conjunction with instances of DLT. Following, in section 3, I identified three of the most successful and well-known Blockchain applications, Bitcoin system, Smart Contracts and Supply Chain Management. I selected Bitcoin protocol and Smart Contracts because they are well-established applications of Blockchain technology because they are widely utilised by software developers among numerous industries. Moreover they have many uses in all kinds of applications which is evidence of their significance and rising potential. Furthermore, the industry of Supply Chain Management (SCM) has been chosen because the distributed ledger technology can have a considerable impact on the way operations are carried out in the respective industry. Because of the fact that Blockchain is a disruptive and innovative technology with a lot of potential in the industry world, many companies showed interest and started adopting the technology. As a result there are numerous Blockchain applications in existence, therefore after the initial phase of research I concluded that the most important and noteworthy, applications are the previously mentioned for the declared justifications. Moreover, apart from describing the applications, I identified and outlined their characteristics to provide a better overview of their potentiality and to emphasize on how Blockchain technology radically improves the efficiency and performance of their processes. Afterwards, in section 4, future uses of Blockchain were identified which included possible uses in a wide range of industry areas, from Tourism and Real Estate industry to Forecasting and Electronic Voting applications. The discussed future uses possess the potentiality to change significantly the prevailing system. For instance, if a successful application is created that can support Electronic Voting by using the Blockchain technology on a large scale then the societal impact will be tremendous. Additionally, in section 5, the characteristics of tasks that would benefit from the implementation of Blockchain technology in its processes defined. Blockchain technology can enhance tremendously certain tasks and procedures of various applications such as speed of transactions, provide constant availability of service, eliminate the need for a middleman during settlements and offer a distributed, immutable, highly encrypted public ledger that is accessible by everyone who is part of the network that serves as a storage of transaction’s records and information that are carried out on the Blockchain.

6.1. Learning Outcomes:

Through the research that I conducted for this project I learnt about the new evolving technology called Blockchain technology. The aims of the projects were too assess the feasibility of the Blockchain technology. In order to achieve this goal, an extensive research had to be carried out throughout the duration of the project (approximately four months). Moreover, during the research phase I acquired knowledge regarding the different types of distributed ledger technology, the components of the most famous Blockchain application, Bitcoin as well as information with regard to Cryptocurrencies and the Double Spending problem that can occur with digital currencies. Furthermore, I identified the advantages and disadvantages of Blockchain and provided instances of DLT applications like Ethereum and Hyperledger Fabric. In addition, by researching successful Blockchain applications I realised the potential of this emerging technology and how it can streamline the processes that are carried out within the society. With that being said, I also understood the way Smart Contracts work and how they can speed-up settlements while decreasing the transaction cost without the presence of a trusted third party. Further, by defining feasible future uses of the Blockchain technology it is safe to say that the distributed ledger technology can be applied ubiquitously while it is capable of being implemented for smaller, more specific tasks to improve their performance and efficiency. Finally, the section where the characteristics of task that could benefit from the implementation of a distributed ledger technology was proven to be exceptionally advantageous due to the fact that I acknowledged how the properties of Blockchain technology can streamline the performance of procedures and tasks. Eventually, in my opinion I think I provided compelling evidences that the Blockchain technology can be utilised in diverse applications and industries. It is a ground-breaking technology with the potential to disrupt radically financial and societal operations.

7. Reflection on Learning:

As it was mentioned in the Conclusion section, I consider the output of my research and work as adequate although section 5 could be improved considerably. This project was quite a challenge for me because I was not familiar at all with Blockchain technology and the research that had to be carried out included numerous technical aspects of the technology which made it even more difficult as my degree is Business oriented (Business Information Systems) and I had little to no prior knowledge regarding cryptography and how Blockchain works despite the fact the project was not technically focused. Moreover, because of the fact that Blockchain technology is still at an infancy stage, my research was based mainly on online articles and journals and several white papers. I believe the overall structure and presentation of information in the report is satisfactory with respect to the quality and justification of the presented evidence. However, in my opinion I did several mistakes during the period of three months during which we had to complete the dissertation. My first mistake is that I didn't discuss with my supervisor a more specific approach for the project. What I mean by that, the project as it is had a very broad scope and I was given a humongous task to carry out a research on such an extensive subject. I should have spoken with my supervisor and determine for example to focus only in the Finance industry compared to the current state of the project where I had to cover a wide variety of industries and applications. Because of that issue, the research phase of the project took more than I had estimated because of the fact that I had too much essential information to cover in the Background section regarding the components of Bitcoin system, applications of DLT, defining Cryptocurrency and the Double Spend problem that are not negligible. In addition, my second mistake was that I did not manage well my time during the last two weeks with respect to writing the report. I think it is obvious that the report is a lacking information in section 4, which is due to the fact that there was not enough time in the last week to include more information in the specified section of the report. Nevertheless, this project taught me a valuable life lesson, that I should manage my time more efficiently and plan more time for the writing of the report in future projects. Additionally, I should have been more consistent throughout the project. Ultimately, I learnt many precious lessons through this dissertation, particularly how to carry out efficiently projects of this size, and a valuable educational experience that has taught me what I have to do in order to perform better in future projects. Finally, having completed this dissertation I certainly have developed an interest in the Blockchain technology and will keep getting informed regularly through relevant online blogs where technological innovations and applications of this disruptive and innovative technology are constantly being published.

Abbreviations:

P2P – Peer-to-Peer

IoT – Internet of Things

SCM – Supply Chain Management

DDoS – Distributed Denial of Service

AI – Artificial Intelligence

DLT – Distributed Ledger Technology

PoW – Proof of Work

PoS – Proof of Stake

DLS – Distributed Ledger System

B2B – Business-to-Business

B2C – Business-to-Consumer

DApps – Decentralised Applications

BFT – Byzantine Fault Tolerance

SME – Small-Medium-Enterprises

TTP - Trusted Third Party

References:

[1] “Blockchain reaction: Tech plans for critical mass”, Ey, 2017. [Online]. Available: http://www.ey.com/gl/en/industries/technology/ey-blockchain-reaction-tech-plans-for-critical-mass [Cited 25th April, 2018]

[2] “Bank fees at a glance” [Online]. Available: https://www.moneyadviceservice.org.uk/en/articles/bank-fees-at-a-glance [Cited 25th April, 2018]

[3] Jay Stanley, “Blockchain Explained: How It Works, Who Cares and Its Future May Hold”. [Online] 5th February, 2018. Available:https://www.techspot.com/article/1567-blockchain-explained/ [Cited 25th April, 2018]

[4] “Banking Is Only The Beginning: 36 Big Industries Blockchain Could Transform”, Research Briefs, CBINSIGHTS, February 2018. [Online]. Available: https://www.cbinsights.com/research/industries-disrupted-blockchain/ [Cited 26th April, 2018]

[5] Hossein Kakavand and Nicolette Kost De Serves, “THE BLOCKCHAIN REVOLUTION: AN ANALYSIS OF REGULATION AND TECHNOLOGY RELATED TO DISTRIBUTED LEDGER TECHNOLOGIES”, Oct 2016. [Online]. Available:https://papers.ssrn.com/abstract=2849251 [Cited 29th April, 2018]

[6]”What are Transaction Costs”, Investopedia, 2018. [Online]. Available: https://www.investopedia.com/terms/t/transactioncosts.asp [Cited 29th April, 2018]

[7] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”. [Online]. Available:https://bitcoin.org/bitcoin.pdf [Cited 4th February, 2018]

[8]”THE MOST DEVASTATING CYBER ATTACKS ON BANKS”, SentinelOne, 10th August 2016. [Online]. Available: https://www.sentinelone.com/blog/the-most-devastating-cyber-attacks-on-banks/ [Cited 29th April, 2018]

[9] Rishi, “What is the difference between Wallet ID and Bitcoin wallet address”, August 2017. [Online]. Available: https://www.coindesk.com/information/what-is-bitcoin/ [Cited 30th April, 2018]

[10] Noelle Acheson, “How Bitcoin Mining Works”, 29th January, 2018. [Online]. Available: https://www.coindesk.com/information/how-bitcoin-mining-works/ [Cited 30th April, 2018]

[11] Steven Buchko, “How many bitcoins are left”, 3rd January, 2018. [Online]. Available: https://coincentral.com/how-many-bitcoins-are-left/ [Cited 30th April, 2018]

[12] “How do Bitcoin transactions work?”, 29th January, 2018. [Online]. Available: https://www.coindesk.com/information/how-do-bitcoin-transactions-work/ [Cited 30th April, 2018]

[13] Melvin Draupnir, “What is the Bitcoin mining block reward?”, 6th May, 2016. Available: https://www.bitcoinmining.com/what-is-the-bitcoin-block-reward/ [Cited 30th April, 2018]

[14] Noelle Acheson, "How does Proof of Work, um work?", 6th June, 2016. [Online]. Available: https://decentralize.today/how-does-proof-of-work-um-work-f44642b24215 [Cited 30th April, 2018]

[15] Dave Roos & Nathan Chandler, " HOW BITCOIN WORKS", [Online]. Available: https://money.howstuffworks.com/bitcoin2.htm [Cited 30th April, 2018]

[16] BitcoinWisdom, 2018. [Online]: Available: https://bitcoinwisdom.com/ [Cited 1th May, 2018]

[17] Sean Williams, 26th November, 2017, "The Only Cryptocurrency I'd Consider Buying", [Online]. Available: https://www.fool.com/investing/2018/03/16/how-many-cryptocurrencies-are-there.aspx [Cited 1st May, 2018]

[18] Pravin Palande, 19th May, 2017, "Here's why Bitcoin prices rose by 60% over a month", [Online]. Available: http://www.forbesindia.com/article/special/heres-why-bitcoin-prices-rose-by-60-over-a-month/47027/1 [Cited 1st May, 2018]

[19] Ebele Kemery and CN Chen, "Cryptocurrencies…the digital evolution of money", 8th December, 2017, J.P. Morgan Asset Management. [Online]. Available: https://www.fool.com/investing/2017/11/26/the-only-cryptocurrency-id-consider-buying.aspx [Cited 1st May, 2018]

[20] "Block", [Online]. Available: https://en.bitcoin.it/wiki/Block [Cited 1st May, 2018]

[21] "Mining", [Online]. Available: https://en.bitcoin.it/wiki/Mining [Cited 1st May, 2018]

[22] Melanie Swan, February 2015, "Blockchain: Blueprint for a New Economy". [Online]. Available: http://www.allitebooks.in/blockchain-blueprint-new-economy/ [Cited 1st May, 2018]

[23] Anish L J, "Bitcoin and other Cryptocurrencies-all you need to know", INSURANCE FUNDA, 2ndJune 2017. [Online]. Available: http://insurancefunda.in/bitcoin-cryptocurrency/ [Cited 1st May, 2018]

[24] "What is Fiat Money", Investopedia. [Online]. Available: https://www.investopedia.com/terms/f/fiatmoney.asp [Cited 1st May, 2018]

[25] "Cryptocurrency market cap analysis", Cryptolization, 2018. [Online]. Available: https://cryptolization.com/ [Cited 1st May, 2018]

[26] Josiah Wilmoth, "What is an Altcoin?", CCN, 12th September, 2014. [Online]. Available: https://www.ccn.com/altcoin/ [Cited 1st May, 2018]

[27] Samara Malkin, "NEO and Stellar (XLM): The Best Altcoins of 2018", 8th February, 2018. [Online]. Available: https://cryptocurrencynews.com/daily-news/altcoins/neo-and-stellar-xlm-best-altcoins-2018/ [Cited 1st May, 2018]

[28] SCHWAB NEWSROOM, "How Risky Is Bitcoin?", 16th April, 2018. [Online]. Available: https://www.schwab.com/resource-center/insights/content/how-risky-is-bitcoin [Cited 1st May, 2018]

[29] “2018’s Most Exciting New Cryptocurrency, XYO”, 2018. [Online]. Available: https://bitinfocharts.com/top-cryptocurrency-list.html [Cited 1st May, 2018]

[30] “What is Bitcoin Double Spending”, 23rd June, 2017. [Online]. Available: https://www.bitcoin.com/info/what-is-bitcoin-double-spending [Cited 1st May, 2018]

[31] Randy Clemens, “Decrypting Bitcoin-The Blockchain Technology Explained”, The Fifth Quill, 29th September, 2016. [Online]. Available: https://www.bitcoinmining.com/decrypting-bitcoin-documentary/ [Cited 2nd May, 2018]

[32] Salman Khan, “What is the difference between bitcoin and blockchain”, 21st June, 2016, Quora. [Online]. Available: https://www.quora.com/What-is-the-difference-between-bitcoin-and-blockchain [Cited 2nd May, 2018]

[33] David LEE Kuo Chuen, “Fintech Tsunami: Blockchain as the Driver of the Fourth Industrial Revolution”, Singapore University of Social Sciences. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2998093 [Cited 2nd May, 2018]

[34] ARMONK, NY “IBM Delivers Blockchain-As-A-Service for Developers; Commits to make Blockchain Ready for Business”, 16th February, 2016. [Online]. Available: https://www-03.ibm.com/press/us/en/pressrelease/49029.wss#release [Cited 2nd May, 2018]

[35] Daniel Roberts, “How big banks are paying lip service to the blockchain”, 17th February, 2017. [Online]. Available: https://finance.yahoo.com/news/big-banks-interest-in-blockchain-r3-052723646.html?soc_src=mediacontentstory&soc_trk=tw&guccounter=1 [Cited 2nd May, 2018]

[36] BLOOMBERG, “Blockchain Is Pumping New Life Into Old-School Companies Like IBM and Visa”, 26th December, 2017. [Online]. Available: http://fortune.com/2017/12/26/blockchain-tech-companies-ibm/ [Cited 2nd May, 2018]

[37] Phoebe Chua, “How many public blockchains currently exist (globally)? How are they doing?”, 8th September, 2017. [Online]. Available: https://www.quora.com/How-many-public-blockchains-currently-exist-globally-How-are-they-doing [Cited 2nd May, 2018]

[38] Noelle Acheson, “Smart property: what does that mean for blockchain?”, 9th December, 2015. [Online]. Available: http://www.fintechblue.com/2015/12/smart-property-what-does-that-mean-for-the-blockchain/ [Cited 2nd May, 2018]

[39] Dave Parrack, “ The First Bitcoin Was Mined 9 Years Ago Today”, 3rd January, 2018. [Online]. Available: https://www.makeuseof.com/tag/first-bitcoin-mined-today/ [Cited 3rd May, 2018]

[40] Max Thake, “What’s the difference between blockchain and DLT?”, 3rd February. [Online].Available:https://medium.com/nakamo-to/whats-the-difference-between-blockchain-and-dlt-e4b9312c75dd [Cited 3rd May, 2018]

[41] Jack Glowacki, “Blockchain: Public, Private or Hybrid?”, 19th February, Medium. [Online].Available: https://medium.com/@jackglowacki/blockchain-public-private-or-hybrid-664d4a413331 [Cited 3rd May, 2018]

[42] Warren Fauvel "Blockchain Advantages and Disadvantages", Medium, 11th August, 2017. [Online]. Available: https://medium.com/nudjed/blockchain-advantage-and-disadvantages-e76dfde3bbc0 [Cited 3rd May, 2018]

[43] Nolan Bauerle, "What are Blockchain's Issues and Limitations", coindesk. [Online]. Available:https://medium.com/nudjed/blockchain-advantage-and-disadvantages-e76dfde3bbc0 [Cited 3rd May, 2018]

[44] "Target Hash", Investopedia. [Online]. Available: https://www.investopedia.com/terms/t/target-hash.asp [Cited 4th May, 2018]

[45] "What is a Node?", 2018. [Online]. Available: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/nodes [Cited 4th May, 2018]

[46] "Genesis Block", Investopedia. [Online]. Available: https://www.investopedia.com/terms/g/genesis-block.asp [Cited 4th May, 2018]

[47] Sudhir Khatwani, "How Is Ethereum Blockchain Different From Bitcoin's Blockchain?", COINSUTRA, 24th December, 2017. [Online]. Available: https://coinsutra.com/ethereum-blockchain-vs-bitcoins-blockchain/ [Cited 4th May, 2018]

[48] Chase Smith, "Why scaling the Blockchain is about more than just Transaction Volume", Medium, 20th December, 2017. [Online]. Available: https://medium.com/@theOPENPlatform/why-scaling-the-blockchain-is-about-more-than-just-transaction-volume-54cbb93841a4 [Cited 4th May, 2018]

[49] Rosie Leizrowice , " A Begginer's Look at Ethereum: 7 Notable Facts", 7th March, 2018, Wirex. [Online]. Available: https://wirexapp.com/beginners-look-ethereum-7-notable-facts/ [Cited 5th May, 2018]

[50] "What is Ethereum. Guide for Begginers", COINTELEGRAPH. [Online]. Available: https://cointelegraph.com/ethereum-for-beginners/what-is-ethereum#who-created-ethereum [Cited 5th May, 2018]

[51] Ron Miller, "IBM unveils Blockchain as a Service based on open source Hyperledger Fabric technology", TechCrunch, 20th March, 2017. [Online]. Available: https://techcrunch.com/2017/03/19/ibm-unveils-blockchain-as-a-service-based-on-open-source-hyperledger-fabric-technology/ [Cited 5th May, 2018]

[52] Shashank, "Hyperledger Fabric- A Platform For Business Solutions", edureka!, 7th February, 2018. [Online]. Available: https://www.edureka.co/blog/hyperledger-fabric/ [Cited 5th May, 2018]

[53] Wolfie Zhao, "R3's DLT Software Corda Enters Public Beta", coindesk, 12th June, 2017. [Online]. Available: https://www.coindesk.com/r3s-distributed-ledger-software-corda-enters-public-beta/ [Cited 5th May, 2018]

[54] "The R3 Story", [Online]. Available: https://www.r3.com/about/ [Cited 5th May, 2018]

[55] "What is Corda", BLOCKCHAIN EXPERT, 4th December, 2017. [Online]. Available: http://www.blockchainexpert.uk/blog/what-is-corda [Cited 5th May, 2018]

[56] Karl Wust and Arthur Gervais, “Do you need a Blockchain?”, 27th April, 2017. [Online]. Available: https://eprint.iacr.org/2017/375 [Cited 5th May, 2018]

[57] “Blockchain and Distributed Ledger Technologies”, BlockchainHub. [Online]. Available: https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/ [Cited 5th May, 2018]

[58] Mike Myburgh, “Enterprise Blockchain: How is this Different from Bitcoin? Technology & Use Case Comparison”, TIBCO blog, 5th February, 2018. [Online]. Available: https://www.tibco.com/blog/2018/02/05/enterprise-blockchain-how-is-this-different-from-bitcoin-technology-use-case-comparison/ [Cited 5th May, 2018]

[59] Atul Khekade, “If you Thought Blockchain Was Amazing, Wait till You Read about Hybrid Blockchain”, 20th January, Entrepreneur India. [Online]. Available: https://www.entrepreneur.com/article/307794 [Cited 5th May, 2018]

[60] Saurabh Goyal, “Centralised vs Decentralised vs Distributed”, 1st July 2015, Medium. [Online. Available: https://medium.com/@bbc4468/centralized-vs-decentralized-vs-distributed-41d92d463868 [Cited 5th May, 2018]

[61] Diego Alberto Tamayo, “ibm blockchain explained”, SlideShare, 20th March 2017. [Online]. Available: https://www.slideshare.net/DiegoDiaz49/1-ibm-blockchain-explained [Cited 6th May, 2018]

[62] Harish Natarajan, Solvej Krause and Helen Gradstein, “Distributed Ledger Technology (DLT) and Blockchain, 2017. [Online]. Available: http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf [Cited 6th May, 2018]

[63] Jamie Redman, “Richard Branson: Blockchain Is an ‘Economic Revolution’, 3rd October 2016, Bitcoin.com. [Online]. Available: https://news.bitcoin.com/richard-branson-blockchain-revolution/ [Cited 6th May, 2018]

[64] Haseeb Rabbani, “What Is Hashing and Digital Signature in The Blockchain?”, October 2017. [Online]. Available: https://blockgeeks.com/what-is-hashing-digital-signature-in-the-blockchain/ [Cited 6th May, 2018]

[65] Aruna Gomathi, “Top 10+ Blockchain Development Companies & Developers-2018 Reviews”, 29th March, Medium. [Online]. Available: https://medium.com/@arunagomathi995/top-10-blockchain-development-companies-developers-2018-reviews-5271c5977696 [Cited 6th May, 2018]

[66] “What is Cryptocurrency”, Investopedia. [Online]. Available: https://www.investopedia.com/terms/c/cryptocurrency.asp [Cited 6th May, 2018]

[67] “What is Bitcoin, it’s Characteristics and Challenges?”, steemit$_{\text{beta}}$, March 2017. [Online]. Available: https://steemit.com/characteristics/@indrahang/what-is-bitcoin-it-s-characteristics-and-challenges [Cited 7th May, 2018]

[68] Kumar Ajay, “Five Characteristics of Bitcoin”, January 2018, unacademy. [Online]. Available: https://unacademy.com/lesson/lesson-3-five-characteristics-of-bitcoin/T7UZRMWA [Cited 7th May , 2018]

[69] Boris Dzhingarov, “The Main Characteristics Of Bitcoin”, 22nd December 2017, The Market Oracle. [Online]. Available: http://www.marketoracle.co.uk/Article61089.html [Cited 7th May, 2018]

[70] Shruti Duge, “What are the real-world applications of Blockchain technology?”, 7th December 2017, Nineleaps. [Online]. Available: https://medium.com/technology-nineleaps/blockchain-simplified-part-2-a42161e08762 [Cited 7th May, 2018]

[71] Martin Tillier, “Bitcoin: Why a Divisibility Model Makes Better Sense”, 10th March, 2017, Nasdaq. [Online]. Available: https://www.nasdaq.com/article/bitcoin-why-a-divisibility-model-makes-better-sense-cm453213 [Cited 7th May, 2018]

[72] “Benefits Of Well-Constructed Business Contracts”, THE MYERS GROUP LAW GROUP. [Online]. Available: https://www.themyerslg.com/Contract-Benefits.shtml [Cited 8th May, 2018]

[73] “Smart Contracts in Financial Services: Getting from Hype to Reality”, 11th October 2016, Capgemini Consulting. [Online]. Available: https://www.capgemini.com/consulting/resources/blockchain-smart-contracts/# [Cited 8th October, 2018]

[74] “Smart Contracts”, BlockchainHub. [Online]. Available: https://blockchainhub.net/smart-contracts/ [Cited 8th May, 2018]

[75] Alyssa Hertig, “How Do Ethereum Smart Contracts Work?”. [Online]. Available: https://www.coindesk.com/information/ethereum-smart-contracts-work/ [Cited 8th May, 2018]

[76] “Smart Contract Application Examples and Use Cases”, draglet. [Online]. Available: https://www.draglet.com/blockchain-services/smart-contracts/use-cases/ [Cited 8th May, 2018]

[77] Sergey Grybniak, “Advantages and Disadvantages of Smart Contracts in Financial Blockchain Systems”, 28th December 2017, HACKERNOON. [Online]. Available: https://hackernoon.com/advantages-and-disadvantages-of-smart-contracts-in-financial-blockchain-systems-3a443145ae1c [Cited 8th May, 2018]

[78] “WHAT ARE THE NETWORK TRANSACTION FEES RELATED TO ETHEREUM”, BITGO DEVELOPER PORTAL. [Online]. Available: https://platform.bitgo.com/ethereum-fees/ [Cited 8th May, 2018]

[79] “5 Companies Already Brilliantly Using Smart Contracts”, 8th March, Medium. [Online]. Available: https://medium.com/polyswarm/5-companies-already-brilliantly-using-smart-contracts-ac49f3d5c431 [Cited 9th May, 2018]

[80] “Etherparty Promises to Be LegalZoom of Smart Contracts”, 11th October 2017, ARTIFICIAL LAWYER. [Online]. Available: https://www.artificiallawyer.com/2017/10/11/etherparty-promises-to-be-legalzoom-of-smart-contracts/ [Cited 9th May, 2018]

[81] Ali Raza, “6 Bitcoins Apps That You Must Check Out”, 18th June, The Merkle. [Online]. Available: https://themerkle.com/6-bitcoin-apps-that-you-must-check-out/ [Cited 9th May, 2018]

[82] Kai Sedwick, “10 Bitcoin Apps That Everyone Should Have”, 14th December 2017, Bitcoin.com. [Online]. Available: https://news.bitcoin.com/10-bitcoin-apps-that-everyone-should-have/ [Cited 9th May, 2018]

[83] Marc Hochstein, “Meet Earn.com: 21 Rebrands Social Network In Shift Away from Bitcoin”, 30th October 2017. [Online]. Available: https://www.coindesk.com/meet-earn-com-21-rebrands-social-network-shift-away-bitcoin/ [Cited 9th May, 2018]

[84] “Gliph Basics”, Gliph. [Online]. Available: https://gli.ph/help.html#how-does-it-work [Cited 9th May, 2018]

[85] “Gliph”, crunchbase. [Online]. Available: https://www.crunchbase.com/organization/gliph [Cited 9th May, 2018]

[86] “Gliph”. [Online]. Available: https://gli.ph/bitcoin.html [Cited 9th May, 2018]

[87] IBM Institute, “Trust in trade”, September 2016. [Online]. Available: https://www.ibm.com/blockchain/supply-chain/ [Cited 10th May, 2018]

[88] Robert Hackett, “Walmart and IBM Are Partnering to Put Chinese Pork on Blockchain”, FORTUNE 500, 19th October 2016. [Online]. Available: http://fortune.com/2016/10/19/walmart-ibm-blockchain-china-pork/ [Cited 10th May, 2018]

[89] Jeff John Roberts, “IBM Blockchain Is Tracking Diamond Rings Across the Globe”, 26th April, 2018, Fortune 500. [Online]. Available: http://fortune.com/2018/04/26/ibm-blockchain-diamonds-helzberg/ [Cited 10th May, 2018]

[90] Jeff John Roberts, “The Diamond Industry Is Obsessed With the Blockchain”, 12th September 2017. [Online]. Available: http://fortune.com/2017/09/12/diamond-blockchain-everledger/ [Cited 10th May, 2018]

[91] Nick Collins, “What are blood diamonds”, 5th August 2010, The Telegraph. [Online]. Available: https://www.telegraph.co.uk/news/worldnews/7928039/What-are-blood-diamonds.html [Cited 10th May, 2018]

[92] Bernard Marr, “How Blockchain Will Transform The Supply Chain And Logistics Industry”, 23rd March 2018, Forbes. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2018/03/23/how-blockchain-will-transform-the-supply-chain-and-logistics-industry/2/#1d8e502416cc [Cited 10th May, 2018]

[93] Pete Rizzo, “World’s Largest Mining Company to Use Blockchain for Supply Chain Management”, 2nd October 2016, SupplyChain247. [Online]. Available: http://www.supplychain247.com/article/worlds_largest_mining_company_to_use_blockchain_for_supply_chain [Cited 10th May, 2018]

[94] Yanzhong Huang, “The 2008 Milk Scandal Revisited”, 16th July 2014, Forbes Asia. [Online]. Available: https://www.forbes.com/sites/yanzhonghuang/2014/07/16/the-2008-milk-scandal-revisited/#9263beb4105b [Cited 10th May, 2018]

[95] Anthony Cuthbertson, “BLOCKCHAIN USED TO SELL REAL ESTATE FOR THE FIRST TIME”, 10th December 2017, Newsweek. [Online]. Available:

http://www.newsweek.com/blockchain-sell-real-estate-first-time-ethereum-682982 [Cited 7th May, 2018]

[96] “FOLLOW MY VOTE”, followmyvote.com. [Online]. Available: https://followmyvote.com/ [Cited 7th May, 2018]

[97] Daniel Frumkin, “What is Augur”, 20th November 2017, Invest in Blockchain. [Online]. Available: https://www.investinblockchain.com/what-is-augur/ [Cited 4th May, 2018]

[98] Irem Onder and Horst Treiblmaier, “Annals of Tourism Research”, Science Direct, 26th March 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S016073831830029X [Cited 8th May, 2018]