GRENOBLE ECOLE DE MANAGEMENT, FRANCE.

Why Business Schools need to teach about the Blockchain.

An overview of Cryptocurrency and Blockchain technology based business initiatives and models.

Kariappa BHEEMAIAH

3/2/2015

Table of Contents

Abstract

As technology increasingly gains a place in every aspect of our lives, the economic footprint left in its wake is beginning to take a new form. Primarily technological improvements were looked at from a cost benefit perspective with advances being historically linked to increased scope and scale, coupled with a reduction in cost and price. Other features such as augmented safety and automaticity were the next steps in this evolutionary route.

However as the mega-trend of autonomous action becomes a reality, a new restructuring is starting to take form in the financial sector which forces us to rethink the modus operandi of financial institutions and the basis of our economic policies. Traditional in nature but revolutionary in its outlook, cryptocurrencies have often been mistrusted and discredited by critics due to their price volatility and fixed supply[1].

In spite of these limitations, cryptocurrencies offer the possibility of rewiring the financial system based on the Blockchain, the underlying technology of all cryptocurrencies, which is heralded for its mathematical exactitude. In recent times, an increasing number of developers, mathematicians, entrepreneurs and academics have begun to leverage this technology, thus creating new business models and innovative ways in which value can be transferred without the use of traditional channels.

As financial institutions, central banks and sovereign states begin to acknowledge these changes, formal research conducted by business schools is found lacking in this space. Thus, this report aims to explain the concept of the Blockchain and presents the reader with an explanation of the technical jargon in a non-technical manner, without which it is difficult to comprehend these new business models. Having grasped these concepts, the report then delves into the new innovative companies using this technology and gauges the potential of these Blockchain-based businesses to change the economic structures and the rarified services offered to its proponents in today's digital age.

[1] Does not apply to all cryptocurrencies

Introduction

Despite its obscure origins, negative press reviews and volatile price fluctuations, cryptocurrencies such as bitcoin[2] have continued to gain traction in recent years. At the end of 2013, venture capitalists had invested a total of $30 million in Bitcoin ventures. At the end of 2014, that number had risen to over $440 million (Bitcoin Venture Capital, 2015) . Now in early 2015, Coinbase, a company that provides online wallet services, has already received $75 million in venture-capital fundraising, while 21 Inc., another bitcoin startup, raised $116 million in its latest funding round (Casey, 2015). At this rate, investment in cryptocurrency ventures looks poised to cross the billion dollar mark before the end of 2015.

The end of 2014 also saw companies Microsoft accepting bitcoins as a form of payment (Chansanchai, 2014), joining other billion dollar companies such as DELL, PayPal and Expedia. Simultaneously countries like the Philippines (Romero, 2014) have announced their intention to put its Peso on the Blockchain, the underlying technology that underpins all crypto currencies. At the same time the Bank of England is actively researching the emergence of cryptocurrencies, as they prepare to adapt to these fundamental technological and institutional changes (Bank of England, 2015). As tech entrepreneurs, commercial banks and even sovereign states begin to seriously analyze cryptocurrencies, the question lies in what is the reason for this change in outlook?

While most critics argue that the deflationary aspect of bitcoin (which stems from the fixed supply of certain cryptocurrencies), will ultimately lead to its down fall (Bheemaiah, 2015), a growing mass of proponents and entrepreneurs are now heralding the Blockchain as the true genius of this invention. By finding a solution to a cryptographic problem called the time-stamp problem, or more commonly referred to as the Byzantine general's problem (Nakamoto, 2009), not only was Satoshi Nakamoto, the anonymous inventor of Bitcoin able to resolve the double spending conundrum, but he was able to do so without comprising the decentralized and distributed nature of the network. In doing so, he indirectly proved that the Bitcoin program was both a protocol and a currency. But more importantly, it was also a way of using the nodes or computers in a distributed network to arrive at a consensus about a transaction without depending on a trust-based system or a central counter-party.

It is this fundamental aspect of the technology that is leading to a disruption in various industries today. By eliminating the necessity of a third party to verify the validity of a transaction, the Blockchain is in effect forcing us to reexamine not just the operating methodologies and the structure of the current financial system, but also the way the economy works as a whole. However, to completely understand these new business models, it is essential to understand the underlying mode of operation and the jargon being used by the practitioners of this technology. Understanding cryptocurrencies requires a certain comprehension of monetary economics, cryptography, game theory, psychology and computer science. Although it goes beyond the scope of this paper to cover all these subjects, a foundational understanding of these topics and the associated vocabulary is pivotal to comprehend and leverage this technology.

[2] There are currently over 1000 cryptocurrencies in use. For the sake of simplicity, we refer to Bitcoin as an example since it is the oldest and most commonly used cryptocurrency. Satoshi Nakamoto is the elusive inventor of Bitcoin. The Bitcoin network is written with a capital 'B', while the bitcoin currency is written with a small 'b'. The sign for bitcoin is BTC.

Transitioning Technology

In December 1974, Vint Cerf and Robert Kahn designed something revolutionary- the TCP/IP Internet network protocol. TCP/IP was first developed as a way for any computer to connect and communicate with the ARPANET (Crocker, 2000). Since then, the project mutated exponentially to allow any computer to communicate with any other computer, finally metamorphosing today into the Internet of Everything.

But the base technologies have remained unchanged. The IP address still acts like a unique address that enables any internet enabled device to identify itself on the internet, while the TCP technology guarantees delivery of the data packets by dividing them into segments, which is referred to as packet switching (V.G. Cerf *et all*, 2003). TCP and IP are used in conjunction to increase the probability of the data packet to get from origin to destination.

Leveraging on this mode of functioning, Tim Berners-Lee created the Hyper Text Transfer Protocol or HTTP, which became a way for Web browsers to communicate with Web Servers. Today, along with HTTP, a whole suite of protocols like DNS and ARP, work together to provide us with the network experience we are accustomed to. Email, Search Engines, Web pages, API's and other Internet Services (SaaS, PaaS, IaaS) are all products that have evolved on this framework giving us today's digital economy.

As emails changed the way the information was exchanged, it brought with it previously unforseen inconveniences such as spam email and denial-of-service (*DoS*) attacks. These attacks flood servers with bogus requests for its services. When the number of requests exceeds the number of requests the server can handle, legimitate users begin to expereince delays or receive files containing malware. As DoS attacks frequently occur with the aid of a botnet[3], it becomes hard to determine the origin of these attacks.

Spam and malware distributiuon is predicated on economies of scale. If the cost of sending an email or the individual effort to be used to send an email involves a big investmetnt of time and money, then the cost of sending a spam becomes uneconomic. On this basis, a programmer named Adam Back divised a concept which later came to be know as Proof of Work (Back, Hashcah, 2003).

His idea was to ensure that each email should contain evidence or proof that a certain amount of computational effort had gone into their composition. To achieve this goal, Back developed a system called Hashcash (Back, Hashcah, 2003), in which a textual stamp was attached to the header of the email acting as a proof of the senders effort. Another form of this proof of work is seen as CAPTCHA's which help differenciate between humans and machines.

As the hashcash represented a unit of work, another programmer named Hal Finney, suggested that it be used as a store of value (Antonopoulos, 2014). At the same time this proof should be reusable so as to ensure integrity of function but without unnecessary repetition. Although the idea made sense at the time, it did not have any tangible economic use until the emergence of Bitcoin.

[3] A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. They are frequently used to send spam email or participate in distributed denial-of-service attacks.

Understanding the Blockchain

Today, the Blockchain protocol is following a similar path of evolution with one major difference. Just as TCP/IP and HTTP are protocols of *communication*, the Blockchain is a protocol of *value exchange.* As the Bitcoin network is a decentralized network, it lacks a central authority to serve as a verifier of transactions. Hence , every transaction that occurs between the members of this network, requires to be verified and validated so as to ensure that every transaction occurring within the network is between two individual accounts and that there is no risk of double spending.

This issue is commonly referred to as the Byzantine general's problem and was resolved by Satoshi Nakamoto in his foundational paper[4]. He proposed to take a queue of transactions over a finite time period (approx. 10 minutes) and to add a mathematical problem to this queue that took roughly 10 minutes to solve.

Here it should be understood that it is the transactions that form the backbone of cryptocurrencies and the Blockchain. Every structural element of a cryptocurrency is constructed in order to create, broadcast and validate these transactions.

Keys, Wallets and Cash: Don't leave your node without it

When a member of the network downloads the Bitcoin software[5] to their computer, the software generates unique public and private keys which are stored in a wallet, which is akin to a bank account. Users also have the option to not download the software and to use an online wallet service instead, such as the services provided by companies such as Coinbase.

Online Wallets or Web Clients have gained increasing usage recently and the service provided is quite similar to email. The user's wallet is stored on a 3rd party's server who provides the service much like Gmail holds a users correspondence (Antonopoulos, 2014). However, if the service provider gets hacked, then the hacker could get access to the wallet.

It should be mentioned that while wallet users stil enjoy anonymity (Reid, 2013) the companies providing web wallet services still require the user to provide authentification of identity, in order to respect regulatory requirements. The user thus needs to provide a scan of their passport or a photograph of their National identity card in order to register as a user.

There are a number of different kinds of wallets a user could choose from (How to Store Your Bitcoins, 2014) including; Desktop Wallets, Mobile Wallets, Hardware wallets Ledger USB wallets and Paper wallets to name a few. Each kind of wallet offers different levels of security and anonymity by offering varying encryption and digital-signature options. But irrespective of the type of wallet used, the primary function of a wallet is not to store bitcoins, but to safegaurd the public and private keys (Swanson, 2014).

---

[4] In 2008, Satoshi Nakamoto published a paper on The Cryptography Mailing list describing the bitcoin digital currency (https://bitcoin.org/bitcoin.pdf). The paper is now a seminal reference for developers of cryptocurrencies.
[5]There are two variations of the bitcoin program: one with a graphical user interface (usually referred to as "Bitcoin"), and another version (called bitcoind). They are both compatible with each other.

This is because bitcoins exist exclusively on the network and only change ownership (Nakamoto, 2009). When transactions are made on the network, the users are essentially changing the address of ownerhip for a block of bitcoins from themselves to another. The wallet thus holds no actual bitcoins, but is rather a storage space for the key-pair which are used to affirm transactions or the change of ownership of the bitcoins. In other words, Bitcoin transactions are nothing more than chains of digital signatures which represent a change in the ownership of bitcoins.

The private and public keys are generated as a key-pair using a branch of cryptography known as Elliptical Curve Cryptography (Bos, 2014) and is based on Kerchoff's principle[6]. The private key is used to digitally sign a transaction, much like signing a check, which can then be verified by anyone in the network. The public key thus acts like an email address where a member can receive funds, while the private key acts like a password with which the member can access or send funds.

When a user wishes to send some bitcoins, they use the private key to sign a message that states to whom they wish to send the funds to and the amount they wish to send. All transactions that occur on the network are published on the network, making the Bitcoin network an open and publicly verifable ledger of accounts, where each and every transaction is verified, published and irreversible. As the digital signatures are unique to the key-pair, the verifying party can ascertain the ownership of the bitcoins being transferred by analysing the public key and ascertaining if that key has the necessary bitcoins attached to it to perform a transfer of a specified amount.

Although this method provides a decentralized way to validate transactions, it raises the question as to why the other members of the network would use their time and the computational capability of their computers to check the legitimacy of someone else's transaction? To respond to this question, Nakamoto needed to provide an incentive to the members of the network. He did so by using aspects of game theory and by attaching a mathematical problem to the transactions occuring in the network. Apart from verifying the transactions, team members willing to earn some points or *tokens* would need to solve a mathematical problem to gain these tokens, or in this case, bitcoins.

The first node in the network to resolve the problem, then receives an award of tokens/bitcoins. In this way not only is the transaction validated, but it also provides a monetary incentive to the users of the network to ensure the correctness of the transactions. Apart from being a brilliant method of introducting trust, with regards to the transactions occuring within a decentralized network, it also functios as the manner in which a supply of the currency could be introduced into the network.

This entire process of verifying transactions and solving a mathematical problem is referred to as **mining** (Kroll, 2013), as the number of bitcoins that can ever be 'mined' is limited to 21 million. At the time of writing this report, the total number of bitcoins mined and in circulation is approximately 13.7 million and approximately 90% of the money supply will be in circulation by 2022 (Controlled supply, 2014). But although the current supply of bitcoins is inflating, the long-term money supply is deflationary, as will be

[6] In cryptography Kerchhoff's principle states that when communicating in the presence of adversaries the cryptographic algorithm should be made public, but its encryption keys must be held private.

explained later. Since Bitcoin follows a deflationary monetary policy, it not only functions as an alternative means of exchnage but also as an experiment in monetary economics.

It can thus be seen that the mathematical problem attached to the transactions actually performs a role quite similar to proof of work in the hashcash system, first devised by Adam Back. It is this proof of work and the list of transactions that the members need to verify that is called a 'Block' (Antonopoulos, 2014). This process of verification is carried out by certain members of the network called *miners*, who use specialized & easily available software along with the processing power of their computers to verify the transactions and solve the mathematical problem. The Blockchain is thus nothing more than a chain of blocks of transactions.

Just as proof of work served as a manner to verify that the email sent was not a spam email, the proof of work in the bitcoin network serves as a way to ensure the integrity of the transactions. At the same time, this mode of functionning also ensures that the rate at which bitcoins are mined can be regulated without any outside intervention.

The mathematical problem in mining is boot-strapped, time-stamped and difficult

While the hashcah involved adding a textual stamp to the header of an email as a means of providing Proof of Work, in the Bitcoin network the text stamp is replaced with a mathematical problem. Apart from confirming the transactions within a block and ensuring that no double spending occurs, the miners apply a mathematical formula called a *hash function* to the block.

A hash function is an algorithm that takes any arbitary length of data as an input and always provides a fixed length string of data as an output. When a hash function is applied to a block, it converts the information within the block into a random sequence of letters and numbers called a hash (Gilbert, 2004). The hash function used as evidence of the miner's proof of work is the SHA-256 hash function, which produces a hash of 256 bits or 32 bytes, and which was first divised by the NSA (Cryptography, 2010).

Depending on the hash function that is used (eg: SHA-1, SHA-256, etc.), the length of the output always remains the same irrespective of the size of the input data (Eyal, 2014). A hash function can also be used on any kind of data, be it text, numbers or even an image. Every unique peice of input data will always be transformed into the same output when run through the same hash function. In this way hashing provides the input data with a unique digital fingerprint, making it easier to classify and work with data.

Trying to determine the input data just by observing the output hash is a futile endeavour. Secondly, each hash is unique, such that, changing even a single character within a block completely transforms the hash. Finally, as each hash is created at a certain time, the newly created hash is attached to the block of transactions, whilst simultaneosuly taking into account the hash attached to of the prevoius block of transactions. By digitally time-stamping a block at a certain time, the hash introduces another layer of security to the Blockchain. The linking of the blocks via the hashes hence further secures the older transactions in the previous blocks, as an attacker who wishes to comprimise the transactions would have to change the data not just in the most newly formed block but in the block before it and thus every block

before it as well. Hence attaching new hashes to the chain of blocks exponentially increases the security of the older transactions.

At this point it would be prudent to provide a caveat. Althought this process is computationally laborius, hashing is a relatively rapid process for computers. Hence to further bolster the integrity of the Blockchain, the protocol demands that the resulting hash obtained after the SHA-256 hash function has been applied to a transaction block, has to have a very particular format and has to start with a certain number of zeros. This format changes over time and is discussed in more detail later in this section.

To obtain the required format, the miners add a random piece of data know as a 'nonce' to the block of transactions. If the resulting time-stamped hash produced after the introduction of the nonce to the transaction block does not conform to the required format, the miner needs to repeat the process with another nonce until the required format is produced. It is this iteratative process of finding the appropriate nonce that is the actual mathematical problem that miners attempt to solve.On achieving the required format, the miner announces to the network that they have managed to do so and publish the block to the public ledger. This process repeats itself with the fresh block of transactions thus ensuring the continuity of the Blockchain. For their efforts, miners are currently awarded 25 Bitcoins. The reward given to miners is set to reduce by half every 210,000 blocks ≈ every 4 years (Controlled supply, 2014).

Apart from mining the bitcoin tokens, miners also receive a stream of revenue from transaction fees. When a user wishes to make a transaction they have the option of adding a small tip (eg: 0.0001 BTC = a few cents) in order to increase the speed at which their transaction is added to the Blockchain. Currently miners make 99% of their revenue from mining and approximatley 1% of their revenue from transaction fees (Antonopoulos, 2014). Mining is not the only way to obtain bitcoins; non-mining members of the network wishing to obtain bitcoins may purchase them at an exchange or directly via their wallet service providers.

At the time of writing this article, the Blockchain is approximately 350,000 blocks long (Bitcoin Network Data, 2015). A block is currently being mined approxiamtely every 10 mintutes. To maintain the integrity of the Blockchain and this rate of bitcoin production, the network automatically adjusts the level of the difficulty of finding the hash with the appropriate format for each block. The network has to ensure a certain amount of *block difficulty*, or else the miners would hash the blocks of transactions at a rate that would ensure the totality of the currency will be mined in minutes. Hence, the bitcoin protocol deliberately makes it more difficult and this condition is coded into every bitcoin node.

The block difficulty is adjusted every 2016 blocks or approxiamtley every two weeks (Controlled supply, 2014). By comparing the time stamps of two blocks 2016 blocks apart, the program is capable of estimating the change in computational power of the entire network since the last adjustement. As the reward reduces over time, this may provide an incentive for some miners to leave the network. As this happens, the number of miners who are veryfing the transactions will reduce and so will the diffuclty of the Proof of Work and hence the problem gets easier for the remaining miners. So even though the compensation reduces, the amount of work reduces as well. As a result the least efficient miners leave and the network self-balances.

The difficulty and the time-stamped hashes attached to each block not only allows us to trace every transaction back to the genesis block[7], but also makes it computationally impractical to modify a transaction, as mentioned before. When an attacker attempts to change a transaction in a block, time does not stand still and the other miners continue to mine the transactions. As a result, this complicates the situation for the attacker, as even if they change a transaction in a block, they would now need to modify the transactions in the blocks formed after the compromised block as well, in order to provide a new proof of work that can be consensually accpeted by the network. The attacker would thus have to maintain a pace of block hashing that surpasses the hashing power of the network. The only way an attacker could perform such a feat is to command a hash rate, that provides the attacker with a hashing power that is stronger than the hashing power of 50% of the network. As a result this kind of an attempt to compromise the integrity of the Blockchain is called a **51% attack** (Eyal, 2014).

But apart from the technological know-how, the computational power required to stage such an attack is formidable. The current computational power of the Bitcoin network today outperforms the top 500 supercomputers combined. In fact, it is 8 times more powerful than the computational power of 500 advanced supercomputers combined (Cowley, 2013). Even if an attacker is able to obtain a hashing rate that is greater than 51% of the network, they still will not be able to destroy the currency. They maybe abe to reject future transactions but the working mechanism of the Blockchain ensures that they cannot change previous transactions; which reduces the profitablity incentive of the attack. It is this resilience that is also one of the reasons that bitcoin has gained so many adopters.

The best pharse that highlights the security of the Blockchain is this statement from Nick Szabo, a legal scholar and cryptographer known for his research in digital contracts and digital currency : *"The core protocol of Bitcoin is sound…and has an unprecidented reliability and security.." It is more reliable and secure than any other digital technology that has ever been fielded"* (Szabo, 2011).

Hence, within the Bitcoin network, the Blockchain acts as a distributed datbase, that functions as a public ledger showing all the transactions ever completed in the network since the creation of the genesis block on January 3rd, 2009. It is for this reason that the true innovation of cryptocurrencies is not bitcoin, but rather the Bitcoin protocol and the Blockchain technology, which ensures a decentralized consensus in a distributed system based on Proof of Work.

[7] The genesis block is the first block of the Blockchain.

Businesses leveraging on the Blockchain

As we continue to transition from IPv4 to IPv6, the Internet of Everything is increasingly becoming part of business reality. Today businesses and societies are noticing that the line between physical and virtual existence is beginning to blur at an increasing rate. In this transitionary ambience, the centralized approach to building an IoT business model is expensive, lacks privacy and is not designed for endurance, as it fails to address the issues related to scale and complexity.

A secondary effect of the internet of everything is that it will also create an economy of everything (Panikkar, 2015), as every device capable of connecting to the internet becomes a point of transaction and economic value generation for consumers and prosumers[8] in a sharing economy. In this form of a colloborative digital economy, a decentralized model is a sounder model to adapt, as it removes the fallacy of having a single failure point that is inherent of todays client-server based business models. On the contarary, in a decentralized structure, the addition of more nodes to the system actually decreases the risk of system failure as if one node fails to function, the whole network is not compromised.

As an increasing number of businesses, both large and small, begin to understand the advantage of having a decentralized system, the possibilites that are offered by the Blockchain technology begin to make economic sense. Most importantly is the issue of user-privacy, which is fast becoming an increasingly debated topic as an increasing number of consumer-data led companies make large profits with limited or no consent feedback loops to the providers of the information (Lanier, 2013).

In addition, decentralized architectures offer better cost benefits to companies as the peer-to-peer sharing of resources in a distributed network removes dependency on a cental server, optimizes resource use and reduces costs. In other words, it is the network that does the heavy lifting of gaurding privacy, maintaining a homogenous level of service and developing reputation based brand equity (Doctorow, 2012).

As distributed networks begin to act as a channel of value-based transactions and in light of the afore mentioned advantages, a new breed of Blockchain based businesses are now beginning to show signs of disprution in various domains of the market. This section analyses the new companies that are taking pionnering steps in advancing the advent of bitcoin and Blockchain based businesees. Based on the manner in which these businesses are leveraging the technology, we notice the immergence of two salient groups:

I) Businesses that provide services and products built on the Blockchain.
II) Businesses that emulate the Blockchain to offer decentralised products and services.

[8] A prosumer is a producing consumer- a phrase originally coined by the economist Jeremy Rifkin.

I) Businesses built on the Blockchain.

Sector: Finance

The fisrt companies to enter the bitcoin space were those which provided web wallet services, as it was this part of the Bitcoin ecosytem that was first required to grow in order to increase the number of users. Today, some of these companies now provide other services such as currency exchange, forex hedging services,data analytics, etc. Based on VC funding received until the end of 2014, the most popular web wallet providers are today are[9]- *XAPO ($60M), Coinbase ($31.7M), Blochchain ($30M), Circle ($26M) and Bitgo ($12M).*

Contrary to popular belief, traditional banking and finanical services do not extend to the majority of the world's popuation. According to the World Bank, out of the 7 billion people on the planet, only 2 billion have bank accounts and participate in e-commerce (World Bank, 2013). This statistic even holds true in developed countries, such as the USA, where almost 17 million adults – or 7% of the adult population is unbanked (Klapper, 2012). In India the numbers are even more startling where almost half of the population does not have a bank account. Currently two-thirds of the 'unbanked' population do not have enough money to use a bank (World Bank, 2013). However since 3.07 billion people of the total 7 billion people on the planet have access to the internet (World Internet Users Population Stats, 2014), the concept of transacting directly via the internet immediately churns interest with merchants who realise they can increase their client base by several factors by accepting bitcoin.

The finance sector is thus seeing an unprecidented period of innovation with the advent of cryptocurrencies. As the Blockchain allows for the removal of 3rd party transaction validation bodies and allows for the creation of trust without government or institutional intervention whilst performing a transaction, the purpose of cryptocurrencies precipitates to assuring monetary reciprocity and to the exchange of value directly between the transacting parties. These features along with the very low transaction costs have allowed companies to pionner new business models that allow participants in the cryptocurrency network to exchange value irrespective of the size of the transaction.

Microfinance and Remittances: Traditional transaction companies such as Mastercard and Visa, have large asset investments, dispute resolution costs and payment procedures that necessitate high transaction fees (World Bank, 2014). This centralized structure makes it impractical to transact small sums and conduct micropayments or ad hoc payments. However, today companies such as ChangeCoin, now offer products like ChangeTip which allow users to make micropayments via their social media channels. Micropayments are an evolutionary step in digital media payment schemes, as now users can pay small sums to access selected content published by magazines, bloggers, artists and publishing houses. Rather than paying for a monthly subscription, a user can now pay on a use-as-they-go basis which could increase readership and subscriptions, whilst providing a monetary incentive for the publisher to regularly provide quality content.

[9] Data accessible at coinmarketcap.com

With regards to remittances, the current average transaction fees for remittances is approximately 10% for worldwide transfers. On the other hand, intra-Africa transaction fees can rise up to 30% (World Bank, 2014). These fees include the agents commission, access to the service, forex, etc.. However sending a remittance payment using bitcoin and via a serivce like Bitpay or Coinbase, has a transaction fee between 0.01 to 0.05% of the transfer, which includes the 1% of the transaction fee paid to the service provider (Coinbase Support, 2014). Users wanting to send money to African countries can now use BitPesa, a remittances provider focused in East Africa, which allows the sender to send a payment in bitcoins. The company charges a 3% transfer fee, converts the bitcoins into the local currency and delivers the payment irrespective of the size of the payment (BitPesa, 2015). Not only does this allow the receiver to obtain every KES shilling, but it also allows the sender to save up to 97% in fees.

In 2013; the total revenue earned via transaction fees amounted to $ 550 billion dollars of which remittances accounted for $49 billion. Using a bitcoin service ensures a 90% reduction in transaction costs thus providing users with $43billion in savings (Milken Institute, 2014). In terms of retail transaction fees, consumers will be able to save $260 billion by using bitcoin.

Sector: IoT and FinTech

IoT: The distributed architecture of cryptocurrencies also provides the opportunity to develop innovative financial services on the protocol in conjuction with the Internet of Things (Ericsson, 2014). As the transition from IPv4 to IPv6 continues, it provides each person on the planet with an IP address for all their devices and sensors. But now since a device with an IP address can connect to the Blockchain, it can thus act as an economic point of transfer.

For instance; a refrigerator with a built in compter can now be programmed to perform actions in context to a household's food budget. Based on the owner's eating habits, the regrigerator can communicate with the website of the local super market and conduct a transaction on behalf of the owners based on their pre-programmed instructions, monetary constraints and preferences. Once the transaction is made, the owners could receive a notification via email asking their permission to validate the transaction. Final approval is still made by the owners, but by connecting the user's digital wallet to interoprable household devices, the time spent on perfoming mundane tasks is reduced dramatically in the process. This mode of operation can then be extended to other devices in a habitation in order to regulate power supply, water consumption, bandwith useage, parking charges, etc. In essence, it provides the user with the capacity to program their money.

Another sector that could capitalize on this kind of innovation is the manufacting industry and the Industrial Internet (Industrial Internet Insights Report, 2015). As an increasing amount of manaufacturing jobs get automated and roboticized, processes that currently need human intervention can now be controlled by a machine. A production unit which functions with an AI, can be fed input data specifying the future volume to be produced and the time delays related to transportation and inventory. Based on these parameters, the AI could then estimate the raw materials required to respect this rate of production and calulate if the raw materials it has in its possesion will be sufficient to address this demand. As the AI is connected to the Blockchain, it can directly communicate with the supplier, send a requisition order and

pay for the transaction. Multi-sig technology (discussed in the next section) can also be used to ensure a certain amount of managerial control. But by automating these processes and using the Blockchain to directly ensure stocks purchases and production rates, the manufacturing unit will be able to reduce the required manpower, inventory costs and transportation time lags, thus increasing efficency.

One company currently working on this form of monetary automation is Kinetics which provides hardware payment systems, like BitSwitch, which are capable of using the Blockchain to automize products and services and exchages. An interpretation of automating processes in the corporate environment is also currently leading to the formation of Autonomous agrents and DACS (Decentralized Autonomous companies), discussed in the later part of this report. With the Internet of things sector already estimated to reach $14.4 Trillion in Value at Stake (Cisco, 2013) by 2020, the implications of this form of automation and capablility allowing machines to use programmable money could be quite consequential.

FinTech: The Finanical Technology industry has also seen strong linear growth over the past five years (Accenture, 2014). However the growth has not been multi-dimensional. Although the banking system does have APIs[10], only those developers with an approved relationship with the bank are allowed to build applications for these services. This produces a stifling environment of encirclement in terms of bolstering innovation. Since Bitcoin is open sourced, the companies that provide Bitcoin services also follow the same ideal and in doing so, have managed to shift the model of Application development from one that excludes developers to one that includes. The result is that these companies now offer APIs for financial processes which are available to everyone and which are faster to upgrade as there is a larger number of developers and users who provide real time feed-back. These Bitcoin API providers are focused on software development services and offer free tools to outside developers to build 3rd party products, tools and services that use Blockchain data, notifications and wallets. Chain.com is one of these companies that currently offers developers an ecosytem to share and develop APIs, products and complex transaction tools in colobaration with other volonteers.

As a result, today companies like BitPay and Coinbase now provide APIs that act as 3rd party merchant support payment systems, allowing merchants to accept bitcoins at fixed fiat conversion rates thus protecting them from currency fluctuations. This allows merchants to receive the cost and security benefits of bitcoin payments, without the exchange rate volatility risk. Merchants who find themselves in economies with turbulent fiat currencies (like Argentina) can also hedge their risk by using the services provided by companies like BitLagos which allow merchants to accumulate bitcoins. By the end of 2014, BitPay and Coinbase had signed up over 80,000 merchants incuding DELL, Expedia, Microsoft and PayPal. The rate of bitcoin adopters is currently doubling every 8 months. The number of bitcoin merchants now accepting bitcoin payments is currently outpacing this user adoption rate. As a result of these innovations, today companies such as IBM are now rethinking the architecture of the Internet of Things and are finding inspiration from the decentralized and distributed architecture of the Blockchain (Panikkar, 2015).

[10] Application Programming Interface

Sector: Legal/Escrow Services and Insurance

In the last section, we briefly touched on the subject of programming money. However, the applications of this concept are futher amplified when the core strucutre of bitcoin is considered. Bitcoin has a basic programming language that is build into each transaction which is know as '*script*' (Antonopoulos, 2014). It is the transaction script that specifies rules that must be obeyed in order for the currency to change ownership. Most rules are quite simple in this context; eg: the next owner must prove the ownership of their private key to the bitcoin address where the funds are stored. However other rules can also be added such as multi-signature conditions and time lock requirements. These aspects and the associated business models will be discussed in this section.

Smart Contracts and Smart Properties: Escrow services are 3rd party services used to facilitae transactions and resolve contract disputes between two transacting parties. As a bitcoin token is written in script, these kinds of services can now be encoded into the token, which has led to the creation of smart contracts and smart properties. A smart contract is essentially a program that is encoded with certain conditions and outcomes (Buterin, 2014). The code is agreed upon by the contracting parties in advance and takes into consideration their interests. The encoded instructions function as a set of rules and can take the form of be business logic, laws, or even a mission statement. As the rules are written in a programming language, the contracts can now interact with any service that accepts cryptographically signed commands, such as a bitcoin token that has been encoded to accept these commands and perfom certain simple actions on receiving these instructions (Buterin, 2014).

In a future scenario, if a buyer wishes to purchase a used autonomous car they could use a smart contract that registers the change in the ownership of the car as the transaction is made. Once the transaction is verified and published on the BlockChain, the conditions of the contract have been met. Since the transaction is timestamped on the Blockchain, the process is irreversible and the whole network can verify its validity. The state of ownership can now be verified by any device that is connected to the internet and the Blockchain, which in this case, is the car. The car receives this information, geo-localizes it's new owner via the cellphone number attached to the mobile wallet, and proceeds to make its way to the new owner. This example introduces the concept of Smart Property and the same idea can be extended to a host of other transactions such a real estate purchases , asset selling, etc.

One of the many functions carried out by lawyers is to provide proof for the existence of a document—a will, a deed to a house, power of attorney, etc. As this involves signing a document at a particular date and time, the Blockchain can now be used to perform similar time stamped operations. Today, cypto-law companies convert the contents of a document into a hash and store it on the Blockchain. As the hash cannot be changed, the validity of the documents within a block on the Blockchain can now be proved ubiquitously in any court of law at a later date .

The legal services provided using this kind of technology would thus be:

- Translating the contract into code which can be complicated when you consider the possible outcomes, the breach of penalty etc.
- Agreeing which code to use.

Today, companies are providing these kinds of serives to make to your own contracts in the form of modules. Some of companies who are pioneering this form of Blockchain notarization are Empowered Law, Bitrated.com, CryptoCorp, Colored Coins and Codius.

In case there are more than 2 parties involved, or if the transaction parties wish have added layers of security to a transaction, users also have the possibility of making a transaction using *multi-sig,* which is short for Multiple Signatures. Instead of one Private Key, two or even three private keys are attached to the same public key. To complete the transaction, the digital signatures from each private keys needs to be received. Only then is the transaction validated.
Hence an escrow service oversseing a contract, can provide the parties with a bitcoin address whilst controlling one of the private keys. To complete a transaction the smart contract needs to have 2 of 3 signatures of a multi-sig address which include that the client, the supplier and the escrow service. This is called 2-factor authentication (S.Goldfeder, 2014) and is used by a number of bitcoin services, including online wallets. Multi-sig can also be used for automating production lines as mentioned in the previous section.

CryptoCorp is one of the companies that is using 2 factor authentication for insurance (Buterin, 2014). When their server receives a transaction to co-sign, the transaction is run through a machine learning software based fraud detection model, which analyses:

1. The amount of the transaction,
2. The frequency of trade with the attached address (which can already be verified by anyone)
3. The amounts of the previous transactions
4. The address of the recipient.

Based on these paprameters, it calculates a risk score for the transaction. If the score is low, the transaction is carried out. If it represents a level of medium risk, it can ask for 2 factor confirmation by sending a text message to the user or via email. If the score is high, then it asks for a manual review. Since machine learning is used, the algorithm uses the input data to learn and provide a desired output, thus adapting its level of security, based on the transactions of the network. This technology is already used by banks for establishing withdrawal limits. But using the Blockchain now allows etrepreneurs and data scientists to identify fraud and malpractise in sectors like insurance.

Some of the other uses of smart contracts are for auctions. The contract can be programmed to automatically sell an item at a certain price. The bidders makes their bid and sends their payments; but the contract only takes the highest bid and returns the rest of the money to the wallets it came from thus providing real-time hedging. Augur, another company that uses Blockchain technology, is using a version of this technology in analysing the derivates market.

II) Businesses that emulate the Blockchain technology.

One of the limitations with bitcoin transactions is the transaction speed. Currently, the Bitcoin network can treat 7 transactions/sec. PayPal on the other hand, processes 150 transactions/sec and VISA can processes between 2000 to 42,000 transactions/sec, based on the seasonality effect (Biggs, 2014).

Transaction speeds are directly related to the number of blocks that are 'orphaned' by the network. As miners race to compile transactions and include them into the block that they are creating, they prefer to select transactions that are smaller in size; i.e: transactions containg small amounts of data describing where they come from and where they go to (input and ouput meta data). If a transaction has a number of inputs and/or outputs, then the amount of this data increases. As a result, it occupies a bigger amount of space in a block and increases the difficulty for a miner to relay the block on the network. This leads to the creation of an orphaned block. It is for this reason that complex transaction with multiple levels of input and output data are transmitted with a higher transaction fee, as this provides an incentive for the miner to inculcate this transaction into a block.

Bitcoins 10 minute block-time was selected to provide a low number of orphaned blocks (0-5 on average per day), as the creation of orphaned blocks poses a risk of affecting the block creation time and the security provided by confirmations. At the same time, block-time and transaction confirmation have a symbiotic relationship. Faster block-times could reduce the integrity of the transaction confirmations on the Blockchain, especially in the presence of orphaned blocks.

In an attempt to experiment with this trade-off between block time and confirmation reliability, a number of developers have created alternative forms of cyryptocurrecnies that try to reduce transaction time whilst safeguarding the robustness of the confirmations. This has led to a proliferation in the number of cryptocurrencies that now exist on the market which are variants of bitcoin and are referred to as Alt-coins.

As the protocol is open sourced, developers interested in making new currencies can create customized variations of the protocol by adopting a method known as *forking*, where developers copy the source code of a software and independently develop on it or make modifications to it, creating a distinct or even a separate piece of software in the process. Forking has gained momentum as developers find the proof of work based consensus algorithm of Bitcoin too slow. At the same time the development of alt-coins offers the possibility of experimenting with different configurations for a cryptocurrency. This has led to the creation of over a 1000 alt-coins, some with minor variations to the bitcoin code, and others with innovative technological changes. Nine of these new alt-coins have a market cap of over $10M and two alt-coins (Ripple and Litecoin) have a market cap greater than 1% of Bitcoin's market cap[11].

Although creation of an alt-coin is quite feasible, the true challenge to these cryptocurrencies is to develop a network of users.

[11] Data available at coinmarketcap.com

Bitcoin 2.0- From Bitcoin to Alt-Coins

Some alt-coin developers have built extensions on the Blockchain which are forward and backward compatible with the existing Blockchain, but can also address issues such as scalability, pace of invention, transaction throughput, multi-asset issuance, and extensions to the smart contract scripting language.

Since all cryptocurrencies exist on the network and in the form of code, pieces of code an be added to the *script* that change the nature of the transaction being done with the token. This process involves using a small amount of bitcoin tokens to reresent something else, eg: a stock, a bond, property, etc. In doing so, the Blockchain no longer remains just a decentralized channel of bitcoin transactions, but also a decentralized asset exchange channel, capable of tracking the flow of an assets exchanged from one address to another and updating this change in ownership on the public ledger.

One of the first companies to implement this process was Coloured Coins, who use a method of tagging an asset or any commodity to a token of bitcoin. This process is know as *colouring* a coin (Bradbury, 2013). As each bitcoin is now tagged to represent, say one gram of gold, a transfer of 10 bitcoins would be effectively transferring the ownership of 10 frams of gold from one party to another. The value of the token remains the same, but the new owner can now redeem the 10 grams of gold as transfer of the bitcoins has resulted in a change of ownership of the bitcoins, making him/her the new owner of the tagged bitcoins and the gold associated with them. Some other companies who are doing this are MasterCoin and Counterparty.

While Coloured Coins use bitcoins and do not create an alt-coin, Mastercoin uses its own currency (Omni) instead of the bitcoin, but which still rests upon the Blockchain and uses bitcoin to clear the underlying transactions. The founders of Mastercoin also created Counterparty, which offers numerous features such as the creation of custom assets, dividends and derivatives . Counterparty also uses its own currency (XCP) but uses the blockchain to assure transactions.

Leveraging on the programming capability of cryptocurrencies has led to the creation of Autonomous Agents and Decentralized Autonomous Companies, or DACs, that can operate without any human involvement and operate autonomously on a blockchain. DACs function under the control of a programmed mission statement which is implemented as publicly-available business rules in the form of auditable open-source software, distributed across the computers of the stakeholders (Johnston, 2015). These unmanned companies could own capital, hire people, issue shares, produce profits and distribute those profits to the shareholders who host the DAC on their computer, buy stock in the company or receive *crypto-equity*[12] payments for providing services for the company.

One company developing this technology is Bitshares, which provides an open source software that can be used to launch DACs. The most notable DAC using this technology is Dacsunlimited which uses a version of the Bitshares technology (BitsharesX), to create an unmanned decentralized exchange where users can perform collateralized long and short trade options on crypto assets. These financial assets, called *bitAssets,* are similar to derivaties and are pegged to a currency or commodity. The assets are called

[12] Crypto-equities are dividends that are paid to shareholders from the profits generated by transaction fees.

Polymorphic Digital Assets (Johnston, 2015) as they track the value of a commodity, a stock or a currency while paying dividends to holders and avoiding all counterparty risk (Larimer, 2013).Examples of bitassets include- BitUSD, BitCNY, BitGLD and BitBTC. Currently, BitSharesX has the 4th largest market capitalization preceeded by Bitcoin, Ripple and Litecoin.

Blockchain 2.0

As an increasing number of Alt-coins began to proliferate the market, a solution was needed to trade and exchange these currencies in a harmonious manner along withh fiat currencies. The first company to implement a payment and trust network that was asset independent and allowed individuals to make transactions in any currency or assets was Ripple.

Ripple uses it own cryptocurrency known as Ripple XRP. As in Bitcoin, the transactions are shared and replicated across a distributed network. But the difference with Ripple is that the enteries on the ledger can be in XRP, USD, Euros, or even Gold. In fact, the XRP is used to facilitate transactions between other currencies. As different assets can be exchanged using the Ripple network, they do not use mining and Proof of Work as a means of arriving at a consensus on the network. Instead they use a consensus mechanism based on trusted sets of servers, which hosts the network (Schwartz, 2014).

In the Ripple network, a server is any entity in the network that runs the Ripple Server software. Members have the choice of running the Ripple Client software (which only allows a client make transactions) or the Server software, which allows them to participate in the consensus process. Any client hosting the Server software can introduce a transaction on the network, and participate in verifying its validity. However, the advantage of hosting it on servers also allows Ripple transactions to be confirmed within a few seconds rather than Bitcoins' 10-minute time lag.

As a result of these advantages and primarily because Ripple is also a privately owned company which is subject to laws and regulations, banks and financial companies are now paying greater interest in searching for ways to plug-in this mechanism for international funds transfers (Bank of England, 2015). Hence, although the server centric structure of Ripple goes against the principal infrastructure of Bitcoin, Ripple pursuses the same goal of decentrlaized consesus in a different way. The success of Ripple can be measured by it market cap, which currently stands at over $400M, second only to bitcoin, in spite of its recent introduction[13] into the cryptocurrency sphere.

While Ripple continues to revolutionize financial transactions, another company that shares certain elements of commonality with the philosophy of Bitcoin but which aims to have a larger scope than Ripple is Ethereum. Initally founded as a platform project in Jan 2014, Etheruem aims to be a podium for Smart Contracts and not just financial transactions. Ethereum aims to do so by improving the scripting langauge of its currency, Ether. Bitcoin's script language was kept deliberately simple in order to protect itself from attackers who wished to change the scripting langauge for their own means. By keeping the code simple, there is less room for attackers to make changes. Ethereum aims to use a far more robust programming

[13] Ripple was created in Early 2013.

language built into the transaction processing system itself, thus making the language Turing complete[14]. By using a more versatile script, Ethereum intends to provide developers with a platform where they can share and create complex financial operations, smart contracts and products. The argument for this endeavour is that although Smart contracts exist in bitcoin, they have a limited capacity. Ethereum aims to resolves these issues by using Ether and its own independent Blockchain.

From Blockchains to Side Chains

Apart from creating new currencies with faster processing times, companies such as Tendermint and Bitshare are now implementing versions of another block verification algorithm called *Proof of Stake* (Back, 2014). With these algorithms, a miner earns the currency based on the amount they already own; i.e: someone holding 1% of the currency can mine 1% of the blocks and thus earn more tokens. Earnings are based upon the number of coins, or the 'stake' held by the miner. The more they hold, the more they can mine.

The advantages that cited by developers include, faster transaction times, increased security, compatibility with other Blockchains and a sizeable reduction of electricity consumption. It is these innovations that are currently branching the innovation in this space in 2 directions-

1. Adding new features to the Bitcoin Blockchain.
2. Creating new blockchains with new currencies , which provides additional features, but whose value is pegged to to that of Bitcoin. Adam Back of the hashcash fame, came up with this concept and calls it Side Chains. Along with some other very notable names in the cryptocurrency space, they have created a company using this technology called Blockstream.

Side chains allow a user to lock coins on one Blockchain and unlock a corresponding number of coins on another blockchain. By switching between Blockchains the user could enjoy the benfits of using a particular alt-coin/token, but they ultimately still operate using bitcoin. is using alt-tokens/coins. This offers the possbility of eliminating the risk of volatile price fluctuations witnesed by most alt-coins, whilst still allowing developers to create new kinds of cryptocurrencies that have additional features and strengths. By using bitcoin as a representative cryptocurrency, users can still benefit from the advanced features of a particular alt-coin, without needing to choose or switch between currencies with volatile price fluctuations.

Blockstream enables this feat by using the concept of pegging, in which one-way and two-way pegs exist between the Bitcoin network and a Side Chain network. In this way pegging addresses the issues of digital scarcity offering a chance to introduce alternative and competitive tokens that povide additional services, whilst staying true to bitcoin at its core. Apart from introducing an element of competition it also fosters a nuturing ambience for innovation in the Bitcoin space. Hence, in summary, we find that depending on the type of technology and the philosophy of the founders, cryptocurrency companies are divided into 4 distinct branches:

[14] A language is considered Turing complete when its scripting capabilities allow for any computation behavior can be programmed using the language.

1. Those that use the Bitcoin currency, techonogy and the protocol.
2. Those that use an independent network but are still is pegged to bitcoin;ie: Side-Chains (Blockstream)
3. Those that use the Blockchain but not bitcoin; eg: Cloured Coins
4. Those that use an independent currency and an independent blockchain; eg: Etherum, Ripple.

Alternative uses of mining

As the computational prowess of the Bitcoin network increases, an increasing number of questions have arisen as to whether this computational power can be used for purposes other than mining. It is imperative to note that although the mining operation might appear to be some form of mathermatical puzzle, the resulting outcome is one of pertinent importance. By verifying and hashing the blocks, the miners are collectively performing the actions of a central bank within the network. However, a few ideas that have recently arisen include using the mining computational power to perform other tasks, such as protein folding. One project working on this concept is CureCoin.

Launched in 2013, the CureCoin project aims to combine the mining operation with medical research. Members of the CureCoin project are not required to use any particular mining software and use the computational power of their computers to perform 'SHA-256 Mining and Folding@Home Protein Folding' (Smith, 2013). Contributors also have the chance to earn CureCoins which are paid in proportion to the amount of computational power provided for the scientific/medicinal research. The value of each CureCoin token from the network grows as the amount of folding done for the network increases. The greater the the amount of research done, the greater the value of the coin.

New Ideas and business models

As the Blockchain is open and irrefutable, allowing for authenticity of transactions, it allows for the creation of new possibilities in different dimensions of society and business. This has led to the development of companies who either use some of the business ideas discussed in the previous sections, or who create a mélange of various new ideas and technologies to deliver innovative products or services. This section enumerates a few of the recent developments according to the sector of their involvement:

Supply Chain

Currently, bar codes are used as a way of identifying and tracking a product. However, SKU CHAIN, a San Francisco based start-up is experimenting with the idea of using hashes instead of barcodes as identifiers. Based on this concept, SKU Chain intends to use multi-sig technology in order to provide users with an indisputable verification system. A manufacturer can verify the items he has received from his supplier, by signing the transaction with a private key, while his client is the owner of another private key that is linked to the same public key. By using this method of 2-factor authentication, not only does this allow the supplier to track the orders individually, but the cryptographic security of the keys also curbs the risk of fraud and counterfeit. Considering the fact that counterfeit drugs cost pharmaceutical companies like Pfizer $200 billion a year (Poison Pills, 2010), makes this experiment a worthwhile effort to follow.

Transportation

Blockchain innovation is also giving a new perspective to services that are made to function in a shared economy. A primary example is La'Zooz which is now being considered as a decentralized UBER. Uber has already disrupted multiple taxi and transportation businesses and is currently valued at $41 billion (WSJ, 2014). However like most data companies, Uber's worth is not determined by its assets but because of the data they possess regarding how people move about in cities. It is this data that is transmitted to drivers, providing them with the shortest available routes and which allows them to be efficient.

La'Zooz on the other hand is a transportation service that is owned by its users and aims to fuse ride sharing with Blockchain technology. Instead of bitcoins, users make transactions using *ZOOZ* tokens. Rather than using Bitcoin's Proof of work method of generating new tokens, La'Zooz generates new tokens with *'Proof of movement*. (Sander Duivestien, 2014). Essentially, the driver turns on the La'Zooz app as they drive, earning Zooz tokens as they move.

When they wish to pay for a ride from someone else within the La'Zooz community, they can pay for this service using Zooz. On the other hand, passengers can also earn Zooz tokens by providing data about which are the best routes to be taken by drivers. By revamping the data led business model of Uber, La'Zooz allows users to earn tokens for providing this data. The riders and passengers get paid in Zooz tokens and passengers pay only for the distance covered. This is different from other online ride sharing services, which are more like taxi services where the driver earns a profit. Thus La'Zooz offers to provide a ride sharing service that is based on the principles of a sharing economy, rather than monetary incentive.

Crowdfunding

The crowdfunding sphere is now leveraging on alt-coins, alternative Blockchain's and the concept of Proof of Stake to provide a completely new way of getting funds from investors. Instead of just investing a sum

of money, investors can now release certain sums or invest more as the project achieves certain milestones. This idea works in tandem with a recently elaborated concept by AngelList a well-known crowd and startup funding platform that has been titled as 'The Patron Saint of Equity Crowdfunding' (Crowdfund Insider, 2014), and has helped create over 127,000 startups.

Since cryptocurrencies have a built in scripting language that allows for the creation of new currencies, these new Alt-currencies or tokens can then be programmed to perform certain financial actions, essentially replacing what is done by a large part of the financial sector with code. An entrepreneur looking for funds can now host software that uses this technology on a distributed network and investors interested in investing in this venture, can make monetary investments in exchange for a token or coin specific to this project. Thus in this way, the tokens essentially act as equity (Ravikant, 2014).

The revenues received by the entrepreneur can then be used to scale up the project, operational costs, R&D, etc. As the project achieves certain milestones, the investors have the option of pre-programing their tokens to release additional funds to the venture. As the project receives attention, the network grows and so does the value of the tokens. Tokens can also be exchanged with ease in case investors wish to radiate their risk.

One of the first moves to implement this idea has been already begun in the form of the Medici Project. The online retail company Overstock, an early adopter of Bitcoin, has teamed up with Counterparty and aims to list Overstock securities on a Blockchain based exchange. The Medici project lists 'being able to run a legal peer-to-peer exchange, that would incur just 20% of the costs carried by the current, centralized system' (Metz, 2014) as one of its aims.

Prior to the advent of cryptocurrenies, these activities were and still are, carried out by bankers, salesmen and angel investors which created higher costs to the fledgling company. But today, these services can be done in code. AngelList itself is an example of this statement. The company which has over half a billion USD worth of funds both online and offline is run by a grand total of 22 people. Almost all operations are done in code eliminating the need of extra personnel.

Transitioning Technology, again

While some developers have built extensions on the Blockchain which are compatible with the existing Bitcoin Blockchain, others have come up with a way to replicate the Bitcoin model, but not just create another currency or an alternative payment network. Instead they have created a different set of technologies that are built on top of the Blockchain and offer services which were previously centralized:

Decentralized Data Storage

MaidSafe is a company that is creating a way to decentralize the way we store Data. It provides users with its own tokens called SAFECOINS and anyone that wishes to store any kind of information can buy these tokens and use it to store this information on this network. The difference with this system and say DropBox, is that there is no central server. Instead the data is stored on the nodes that are part of the network and they each store small amounts of the information of a file in a fully encrypted way.
Hence instead of paying for data storage on Amazon or Dropbox, MAidsafe provides a cheaper and more secure alternative that has no single point of failure as it is decentralized. Another company doing this is STORJ which works as a decentralized Storage App.

Decentralized Data Computation

Ethereum is pionnering this new form of technology by providing users with the ability to host Smart Contracts on the network. Each Ethereum contract has its own scripting code which is activated when the contract recieves a transaction. Upon receiving a transaction, the contract can activate itself, perform certain actions (finanical or non-financial) and then goes back into hibernation. By storing such a contract on a distributed network, Ethereum is essentially decentralizing computation for its users. Apart from Ethereum, Codius is also providing users with the similar services and options.

Decentralized Bandwidth

Open Garden is a mobile app that allows users to share their bandwidth with others users via their phone or router. Although this technology has existed for a while, the question arises as to why would users want to share their bandwidth? In order to provide users with an incentive, open garden released a protocol that allows users to share their bandwidth from any device in exchange for tokens Just as more nodes joining a network, increase the computational power of the network , the more users there are on the Open Garden Network, the more bandwidth they have available. It thus acts an alternative to current mobile data subscription offers.

Decentralized Identity

Just as financial and asset transactions can be decetralized, so can records. Currently identity records (eg: birth certificates) are stored in government run centralized networks making them suspectible to attacks, (*for example*: like the recent attack on SONY servers)[15]. However this information can be stored on the Blockchain. Factom is currently providing a service that attaches a hash to a block of records instead of

[15] On November 24, 2014, Sony Pictures Entertainment was hacked by group called themselves the "Guardians of Peace" who released confidential data belonging to the company, including; personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of (previously) unreleased Sony films, and other information.

transactions. Thus every 10 minutes, millions of records can be hashed, encrypted and stored on the Blockchain. The user now possesses a reference number of a block in which their records are permanently stored and which can be accessed and audited form anywhere in the world.

Risks and Challenges

Although cryptocurrenices and the Blockchain technology provide users with multiple new innovative uses and threatens to ramify a number of sectors and institutions, the deployment of this technology on a large scale is faced with a number of challenges. Some of these include:

Regulation

Risk: High. From an accounting standpoint, cryptocurrencies face a number of regulatory hurdles today. Apart from the lack of taxation guidelines regarding cryptocurrencies, users, merchants and service providers trading in cryptocurrencies need specific rules pertaining to the accountability of funds, the amounts stored in offline wallets and the market value of those funds in fiat currency. The programmability of transactions and the possibility to exchange assets without any 3rd Party regulatory body overseeing the change in ownership of assets, further adds to the complexity of the regulatory challenges.

However the biggest challenge to cryptocurrencies might come from a monetary policy perspective. Central banks today derive a portion of their revenue from monetary seigniorage, which is the difference between the value of money and the cost to produce and distribute it[16]. Secondly, if the currency issued by a country's central bank is used as a global reserve currency, it allows the bank to print a larger amount of the currency without significantly raising inflation in its home country. As cryptocurrencies act as a direct competitor to a nation's currency, there is a strong possibility that central banks will offer resistance to their official introduction.

Price Volatility

Risk: High. In spite of exhibiting the 6 characteristics of good money (Scarcity, Durability, Divisibility, Fungibility, Portability and Recognisability) and also exhibits Programmability. Yet, cryptocurrencies continue to be plagued by high price volatility. A number of economists, including the current Greek minister of Finance, Yanis Varoufakis[17], and economists such as Paul Krugman have attacked bitcoin on this issue, when reflecting upon the danger of using a deflationary currency. However, no comments have been made on the underlying integrity of the Blockchain technology.

There are various reasons associated with the fluctuating price of bitcoins and other cryptocurrencies. *Firstly*, the quantity of bitcoins is fixed at 21 million and increases at a predictable rate. The reason Satoshi Nakamoto decided to limit the total supply to 21 million units is directly related to the divisibility of bitcoins. Each bitcoin can be divided into a 100,000,000 satoshi's which equates to 21 quadrillion currency units. This number was selected as 21 quadrillion is greater than the entire M1 supply of the world in pennies, which was estimated to be enough to run the world economy. However the price of a bitcoin

[16] http://en.wikipedia.org/wiki/Seigniorage

[17] http://cointelegraph.com/news/113520/greeces-varoufakis-bitcoin-can-be-used-in-eurozone-as-weapon-against-deflation

token is set by the demand for the currency which is effectively related to its supply. Since the rate of production is known, the rate of demand needs to follow this rate of production to keep the price stable. As the market cap of bitcoins and other cryptocurrencies is small today, small changes in this paradigm create amplified swings in their price.

Secondly, issues regarding 3rd party security failures (eg: the crash of Mt. Gox) have always resulted in a dramatic price drops. These kinds of occurrences will continue to affect adopter's confidence levels which will result in price drops; much like stock prices.

Thirdly, 50% of the bitcoins in current circulation is in the hands of approximately 50 early adopters. As a result this creates the early adopter effect which is seen in tech stocks.

In the near future the only solution to stabilizing the price of bitcoins and other currencies will be the increased adoption of users till the network effect establishes a sense of fluctuating uniformity as is seen in todays Forex markets. But this will only be confirmed with the passage of time.

3rd Party Failure

Risk: High/Medium. Currently a large number of cryptocurrency adopters use 3rd Party transaction platforms, exchanges and web wallets in order to connect to a cryptocurrency network. Although this provides ample advantages to the users, it does not negate the risk of institutional failures. If the servers of these service providers become susceptible to an outside attack, it gives the attacker access to the information contained within them. Furthermore, wallets are not insured as commercial bank accounts are in most countries, as the definition of whether cryptocurrencies are a commodity, asset or a monetary substitute is an ongoing debate that chances from one geographical zone to another. Examples of these kinds of scenarios where server have been compromised leading to the loss of large sums of capital have already occurred, notably with the collapse of Mt. Gox in February 2014. Institutional attacks are a constant reminder to users, merchants and service providers to be wary of the security of their systems.

Mining Pools

Risk: Medium/High. Mining pools, are groups of miners who work together in order to collectively mine bitcoins. When miners join a mining pool, they combine their computational resources to mine bitcoins and share the rewards between them. As mining pools exist on a decentralized network, miners have the option to rapidly switch from one pool to another in a few seconds if they wish to do so. However as some mining pools increase in size, the issue of industrialized mining creates the risk of having fewer unique mining members and threatens the decentralized structure of the Bitcoin network and also increases the risk of a malicious mining pool attempting a 51% attack.

51% attack

Risk: Medium/Low. Although there is always the possibility of a 51% attack, this is a low risk scenario as it will not compromise the public and private keys and thus keep the currency safe from the hands of the attacker. The 'honest' nodes can also make changes to upgrade the underlying code in order to respond against the attack. Lastly, even in the possibility of this scenario becoming a reality, the attacker can only stop future transactions and will still not be able to make changes to the previous transactions. However it would reduce the confidence of the network, which would lead to a price fall and maybe even the collapse of the network as a whole in an extreme scenario.

Future 51% attack scenario

Risk: Medium/High. One of the main hurdles to launching a 51% attack is the associated cost. However as companies begin to trade their shares using the Blockchain (as mentioned in the example with Overstock.com), the associated cost could be offset by the gains. If a high value company tags bitcoins to represent the price of a share, as with BitsharesX (Roy, 2015), then irrespective of whether they use side chains or the Blockchain, the profit that can be attained by hackers will increase in terms of the price of the share. This gives further incentives to launch such attacks and also questions if crypto-equity issuance can function with a currency that has a fixed quantity.

Cryptographic Failure

Risk: Low. One of the most profound technical risks that could be faced in the future is the failure of the underlying cryptography that secures all cryptocurrencies. In this scenario, an attacker might be able to compromise the public-private key generation algorithm used to generate a key pair enabling them to be able to compute the private key via the public key address. This would comprise the network and eliminate the value of all the tokens within the system. The fact that hashing functions used a few decades have already been deemed unsuitable for today's uses is a sign of this risk coming to fruition in the future. Although this scenario is not yet likely to occur with SHA-256, the rapid advances being made in computing, notably quantum computing, could result in a reduction of the robustness and usability of the cryptographic algorithms currently used. The only solution to this limitation would be the constant upgrade of the currencies' core cryptography in order to counteract such a threat.

Apart from the afore mentioned issues, other problems which have been previously discussed in the report such as scalability, transactions speeds, storage limitations and harmonized consensus are some of the current challenges that the developers and free lancers are actively working to resolve.

Closing thoughts

Cryptocurrencies have resulted in an advent of innovation and entrprenerial captainship since the publication of Satoshi Nakamoto's seminal whitepaper. The business models and pionnering initiatives that have been illsutrated in this report represent a small fraction of the work that is currently being carried out in this field.

However inspite of this stellar display of ingenuity and brilliance, there has been a dearth of research piloted by business schools on this subject. This seems to indicate that the biggest challenge to the adoption of cryptocurrencies and the Blockchain is not the risks listed above but rather the mindset in the business academia, which is currently suffering lagging behind in comparision to other fields exploring this subject.

A primary reason for this dichotomy is because the subject of cryptocurrencies is both complex and complicated. It is complicated as it involves technical subjects such as cryptography, game theory, monetary theory and computer science. But it is complex because its comprehension requires a basic understanding of all these subjects, to visualise how they work in unision. As this goes beyond the territory of the cirriculum, their discussion has been overlooked by most educators and institutions.

However, as seen in this report, the technology behind crypocurrencies has the potential to disrupt numerous industries in the near future. This poses some uncomfortable potential when the current economic environment is taken into perspective. An increasing amount of research from scholars such as Erik Brynjolfsson, Andrew McAfee, Thomas Picketty and Robert Reich, all indicate that income inequaltiy and job employability is currently being adversely effected by automisation and advances in technology. At the same time advances in technology are now also limiting data and information processing jobs (Autor, 2014), which were primarily the employment opportunities for young business school graduates.

In light of these transitions, it becomes increasingly important for students and the business leaders of tomorrow to become more technically literate and be capable of understanding the working concepts of some of these new technologies in order to thrive in today's digital economy. This understanding does not restrict itself to digital currencies but also extends to other technologies such as quantum computing, advances in the life sciences, alternative energy technologies, synthetic biology, nanotechnology, 3D printing and a host of others technologies. Without this kind of a peripheral vision, business students might find it increasingly difficult to adapt to the economy of tomorrow and risk falling behind others graduates with specializations in STEM subjects.

Hence, what this technology offers us is not just a chance to witness a reformation of economic and monetary theory as a whole, but also a chance for the academic community to partake in some disciplined introspection and questioning. Current monetary theory is based on a centralized system and depends on consumption and credit in order to assure progress. However the Bitcoin experiment challenges this equation and forces us to rethink the current socio-economic model.

As we are bear witness to this fundamental change in economic and the societal infrastructure, it puts educators and students at the very threshold of learning, while also offering us the possibility of creating a sharing economy that is decentralized, distributed and democratic. While this raises some questions that are quite pregnant with purpose for both parties, the question for business schools is not how are they to go about teaching these subjects, but how fast can they inculcate these subjects into their curricula.

Bibliography and Cited Works

(n.d.). Retrieved from http://www.crowdfundinsider.com/2014/06/41007-angellist-patron-saint-equity-crowdfunding/

Sander Duivestien. (2014, 12 11). *La'zooz, the decentralized version of Uber*. Retrieved 01 27, 2015, from Sogeti Labs: http://labs.sogeti.com/lazooz-decentralized-version-uber/

AngelList – The Patron Saint of Equity Crowdfunding. (2014, 06 04). Retrieved 11 09, 2014, from Crowdfund Insider: http://www.crowdfundinsider.com/2014/06/41007-angellist-patron-saint-equity-crowdfunding/

Antonopoulos, A. (2014). *Mastering Bitcoin.* California: O'Reilly Media.

Autor, D. H. (2014). *Polanyi's Paradox and the Shape of Employment Growth.* Massachusetts: MIT.

Back, A. (2003, 03). *Hashcah.* Retrieved 11 13, 2014, from Hashcash.org: http://www.hashcash.org/

Back, A. (2014, 10 22). *Enabling Blockchain Innovations with Pegged Sidechains .* Retrieved 01 16, 2015, from Blockstream: http://www.blockstream.com/sidechains.pdf

Bank of England. (2015). *One Bank Research Agenda.* London: Bank of England.

Bheemaiah, K. (2015, 01 06). *Blockchain2.0: The Renaissance of Money*. Retrieved 01 31, 2015, from Wired: http://www.wired.com/2015/01/block-chain-2-0/

Bitcoin Network Data. (2015, 02 23). Retrieved 02 27, 2015, from Coindesk: http://www.coindesk.com/data/bitcoin/

Bitcoin Venture Capital. (2015, Feb 19). Retrieved Feb 20, 2015, from Coindesk: http://www.coindesk.com/bitcoin-venture-capital/

BitPesa. (2015, 01). Retrieved 02 03, 2015, from https://www.bitpesa.co/

Bos, J. W. (2014). Elliptic Curve Cryptography in Practice. In J. A. Joppe W. Bos, *Financial Cryptography and Data Security* (pp. 157-175). Redmond: Microsoft Research.

Buterin, V. (2014, 01 23). *Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform.* Retrieved 07 29, 2014, from Bitcoin Magazine: https://bitcoinmagazine.com/9671/ethereum-next-generation-cryptocurrency-decentralized-application-platform/

Buterin, V. (2014, 01 05). *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.* Retrieved 06 24, 2014, from GitHub: https://github.com/ethereum/wiki/wiki/White-Paper

Buterin, V. (2014, 03 12). *Multisig: The Future of Bitcoin*. Retrieved 09 18, 2014, from Bitcoin Magazine: https://bitcoinmagazine.com/11108/multisig-future-bitcoin/

Casey, M. (2015, 03 10). *WSJ.D*. Retrieved from Wall Street Journal: http://blogs.wsj.com/digits/2015/03/10/secretive-bitcoin-startup-21-reveals-record-funds-hints-at-mass-consumer-play/

Chansanchai, A. (2014, Dec 11). *The Fire Hose*. Retrieved Jan 03, 2015, from Microsoft : http://blogs.microsoft.com/firehose/2014/12/11/now-you-can-exchange-bitcoins-to-buy-apps-games-and-more-for-windows-windows-phone-and-xbox/

Coinbase Support. (2014). Retrieved 11 14, 2014, from Coinbase: https://support.coinbase.com/

Controlled supply. (2014, 08 11). Retrieved 12 24, 2014, from Bitcoin Wiki: https://blockchain.info/charts/total-bitcoins

Cowley, S. (2013, May 23). *Bitcoin more powerful than fastest supercomputers*. Retrieved Nov 12, 2014, from CNN Money: http://money.cnn.com/2013/05/23/technology/enterprise/bitcoin-supercomputers/

Crocker, S. D. (2000, Jan 07). *ARPANET -- The First Internet.* Retrieved 12 19, 2014, from Living Internet: http://www.livinginternet.com/i/ii_arpanet.htm

Crypto-Currency Market Capitalizations. (2015). Retrieved 2015, from Coin Market Cap: http://coinmarketcap.com/

Danny Bradbury. (2013, 06 14). *Colored coins paint sophisticated future for Bitcoin*. Retrieved 06 24, 2014, from CoinDesk: http://www.coindesk.com/colored-coins-paint-sophisticated-future-for-bitcoin/

Doctorow, C. (2012, 06 06). *The Curious Case of Internet Privacy.* Retrieved 03 2014, from MIT Technology Review: http://www.technologyreview.com/news/428045/the-curious-case-of-internet-privacy/

Fergal Reid, M. H. (2013). An Analysis of Anonymity in the Bitcoin System. *Security and Privacy in Social Networks*, 197-223.

Henri Gilbert, H. H. (2004). *Security Analysis of SHA-256 and Sisters.* New York : Springer.

How to Store Your Bitcoins. (2014, 12 22). Retrieved 12 23, 2014, from Coindesk: http://www.coindesk.com/information/how-to-store-your-bitcoins/

ICT and the Future of Financial Services. (2014, 11 5). Retrieved 11 15, 2014, from Ericsson: http://www.ericsson.com/industry-transformation/wp-content/uploads/sites/6/2014/11/ict-and-the-future-of-financial-services.pdf

(2015). *Industrial Internet Insights Report.* GE.

Institute, M. (2014). Money Goes Virtual: The Bitcoin Bourse. *Milken Institute.* Washington.

Ittay Eyal, E. G. (2014). Majority Is Not Enough: Bitcoin Mining Is Vulnerable. In *Financial Cryptography and Data Security* (pp. 436-454). Springer.

John Biggs. (2014, 09 8). *CoinSafe May Have Solved The Bitcoin Transaction Speed Problem*. Retrieved 09 30, 2014, from Techcrunch.com/: http://techcrunch.com/2014/09/08/coinsafe-may-have-solved-the-bitcoin-transaction-speed-problem/

Johnston, D. (2015, 02 02). *The General Theory of Decentralized Applications, Dapps.* Retrieved 02 23, 2015, from GitHub: https://github.com/DavidJohnstonCEO/DecentralizedApplications

Joshua A. Kroll, I. C. (2013). *The Economics of Bitcoin Mining.* New Jersey: Princeton University.

Joshua Smith. (2013, 11 11). *CureCoin development continues*. Retrieved 11 19, 2014, from bitcointalk: https://bitcointalk.org/index.php?topic=330685.0

Klapper, L. (2012, 09 13). *Why are so many Americans unbanked?* Retrieved 09 29, 2014, from World Bank: http://blogs.worldbank.org/allaboutfinance/why-are-so-many-americans-unbanked

Lanier, J. (2013). *Who Owns the Future?* New York: Simon & Schuster.

Larimer, D. (2013, 10 03). *BitShares A Peer-to-Peer Polymorphic Digital Asset Exchange (P2P-PDAE).* Retrieved 12 29, 2014, from SCRIBD: https://www.scribd.com/doc/173481633/BitShares-White-Paper

Learn Cryptography. (2014). Retrieved 01 30, 2015, from http://learncryptography.com/51-attack/

Metz, C. (2014, 06 01). *Overstock.com Assembles Coders to Create a Bitcoin-Like Stock Market*. Retrieved 12 07, 2014, from Wired: http://www.wired.com/2014/10/overstock-com-assembles-coders-build-bitcoin-like-stock-market/

Nakamoto, S. (2009, Jan). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved 12 09, 2014, from bitcoin.org: https://bitcoin.org/bitcoin.pdf

Naval Ravikant. (2014, 03 19). *The Bitcoin Model for Crowdfunding*. Retrieved 09 08, 2014, from Startupboy: http://startupboy.com/2014/03/09/the-bitcoin-model-for-crowdfunding/

Nick Szabo. (2011). Retrieved 11 19, 2014, from Wikipedia: http://en.wikipedia.org/wiki/Nick_Szabo

Orphaned Blocks. (n.d.). Retrieved 01 25, 2015, from Blockchain.info: https://blockchain.info/orphaned-blocks

P. Vigna, M.J. Casey. (2015, Jan 20). *Coinbase Raises $75 Million in Funding Round*. Retrieved Jan 30, 2015, from Wall Street Journal: http://www.wsj.com/articles/coinbase-raises-75-million-in-funding-round-1421762403

Paolo S. Romero. (2014, Oct 05). *Solon pushes E-Peso Act*. Retrieved Dec 13, 2014, from Philstar: http://www.philstar.com/business/2014/10/05/1376516/solon-pushes-e-peso-act

Poison pills. (2010, September 02). Retrieved from The Economist: http://www.economist.com/node/16943895?story_id=16943895

Poison Pills. (2010, September 02). Retrieved from The Economist: http://www.economist.com/node/16943895?story_id=16943895

Roy, M. (2015, 01 12). *Is 'the blockchain application stack' a probable or improbable future?* Retrieved 02 15, 2015, from Hyperledger: http://hyperledger.com/posts/2015-01-12-block-chain-application-stack.html

S.Goldfeder, J. B. (2014). *Securing Bitcoin wallets via threshold signatures.* Retrieved 12 28, 2014, from Princeton.edu: http://www.cs.princeton.edu/~stevenag/bitcoin_threshold_signatures.pdf

Sanjay Panikkar, S. N. (2015). *IBM ADEPT Practictioner Perspective .* Retrieved from SCRIBD: https://www.scribd.com/doc/252917347/IBM-ADEPT-Practictioner-Perspective-Pre-Publication-Draft-7-Jan-2015

Schwartz, D. (2014). *The Ripple Protocol Consensus Algorithm.* Retrieved 11 17, 2014, from Ripple: https://ripple.com/files/ripple_consensus_whitepaper.pdf

Suite B Cryptography. (2010, Feburary). Retrieved from National Security Agency: https://www.nsa.gov/ia/programs/suiteb_cryptography/

Swanson, T. (2014). *The Anatomy of a Money-like Informational Commodity: A Study of Bitcoin.* Seattle, Washington: Amazon.

The Boom in Global Fintech Investment. (2014, 03 26). Retrieved 02 23, 2015, from accenture.com: http://www.accenture.com/Microsites/fsinsights/capital-markets-uk/Documents/Accenture-Global-Boom-in-Fintech-Investment.pdf

The Internet of Everything Economy. (2013, 02 12). Retrieved 01 5, 2015, from Cisco: http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf

Uber Snags $41 Billion Valuation. (2014, December 05). Retrieved from The Wall Street Journal: http://www.wsj.com/articles/ubers-new-funding-values-it-at-over-41-billion-1417715938

Vinton G. Cerf, D. D. (2003). *A Brief History of the Internet.* Chicago: ACM SIGCOMM Computer Communication Review.

World Bank. (2013). *Who are the Unbanked*. Retrieved 11 2014, from World Bank: http://siteresources.worldbank.org/EXTGLOBALFIN/Resources/8519638-1332259343991/world_bank3_Poster.pdf

World Bank. (2014, 06). *Remittance Prices Worldwide.* Retrieved 12 13, 2014, from World Bank : https://remittanceprices.worldbank.org/sites/default/files/rpw_report_june_2014.pdf

World Bank. (2014). Social Protection and Labor. *Payments and Transactions.* World Bank. Retrieved from The World Bank: http://www.worldbank.org/content/dam/Worldbank/Event/social-protection/Payments_and_Transactions_Session_Packet.pdf

World Internet Users and 2014 Population Stats. (2014). Retrieved Jan 2014, from Internet Usage Statistics: http://www.internetworldstats.com/stats.htm