An Analysis of Blockchain Technology and its Commercial Exploitation

Author: Timothy Fisher
Student ID: c1309127

Supervisor: David W Walker
Moderator: Yukun Lai

Degree: BSc Business Information Systems
Module Title: One Semester Individual Project
Module Code: CM3203
Credits: 40

Abstract

The revolutionary distributed ledger technology known as Blockchain is possibly the most exciting technological invention since the internet. Although there is often a misconception that Blockchain technology is only associated with Bitcoin, it actually has the potential to be much more. Blockchains can solve complex problems, and are already changing the way organisations work.

This report is aimed at venture capitalists, as well as individuals interested in the technology and its commercial exploitation. Although substantial research is being undertaken in Blockchain-related areas, with the technology still in its infancy, there are often questions over how profitable Blockchain solutions can be. This report looks at a problem venture capitalists currently have: is the technology worth investing in, and if so, what particular area or application should be invested in?

The report covers how the technology works from a technical viewpoint, with emphasis on how it ensures a secure and trustable record of transactions. Furthermore, the report aims to provide a detailed explanation on how Blockchain technology achieves distributed consensus. The report continues by covering the difference between private and public Blockchains, before exploring current and potential uses.

By grouping Blockchain applications into 8 distinct categories and analysing each of these via a SWOT analysis, the report singles out the ‘verifiable data’ category as particularly promising. The report concludes by briefly analysing 3 potential industries that can (and should) be invested in: the pharmaceutical industry, the land registry industry, and the healthcare industry.

Table of Contents

Table of Figures

Introduction

Aims

The overall purpose of this project report is to inform a hypothetical group of venture capitalists (the report's beneficiaries) on the commercial exploitation of Blockchain technology. The report aims to categorise Blockchain technology into distinct application groups, and further investigate the most profitable area. To achieve this end-goal, 3 specific aims have been chosen:

1) Gain an understanding of how Blockchain technology works from a technical viewpoint

2) Highlight current Blockchain uses, as well as promising areas of interest for Blockchain

3) Produce a summary for a group of venture capitalists, highlighting potential Blockchain related areas that they can invest their money into (e.g. propose a 'solution' to their 'problem')

Scope

In March 2016, PwC's Global Blockchain Team identified over 700 companies entering the *FinTech* industry[1]. This figure does not include companies that have already entered other industries such as: real estate, automotive, healthcare and even the diamond industry[2]. Therefore, it would be unfeasible to cover every possible Blockchain application, in every industry. As a result, this report focuses particularly on applications that I deem 'potentially profitable' following the initial research phase.

Similarly, due to the large number of applications, there are also inevitably hundreds of variations of protocols and mechanisms which underlie Blockchain applications. When covering the sections 'How Blockchain Technology Works' and 'Consensus Mechanisms (and Types)', the report focuses on widely used protocols such as proof-of-work and proof-of-stake.

Outcome

The project report's main outcome will be a set of SWOT analyses, and a summary of Blockchain-related investment options. The SWOTs will be used to identify the category deemed the most profitable. The final summary will include a single recommendation, as well as 2 backup options (all from different industries). As alluded to in the 'Aims' section, the key aim of this report is to benefit venture capitalists by suggesting areas that they should invest their money into.

Background/Related Work

In a world filled with emerging technologies, 'Blockchain technology' (often colloquially referred to as 'Blockchain') is arguably one of the most exciting, being labelled as 'disruptive' and 'innovative' by many[3]. Despite often being associated only with Bitcoin and other *cryptocurrencies*, the underlying technology – the digitally distributed public ledger – 'Blockchain' has been receiving attention from a variety of industries. The concept of recording transactions in a secure, stable, chronological and scalable way, has led to possible applications in many areas.

Traditionally, when transacting money or assets (or general things of value), people have relied on middlemen (intermediaries). Examples of these intermediaries include banks and governments. Intermediaries are used to ensure trust and certainty with regards to carrying out transactions and record keeping.

When it comes to digital transactions, third parties are normally necessary, with digital assets known to be very easy to reproduce. Therefore, it's possible to spend the same unit of value more than once, also known as the '*double-spending'* problem[4]. However, conducting digital transactions without an intermediary is now possible via Blockchain technology.

Blockchain technology was first detailed in a white paper released in 2008 by an individual (or group of individuals) using the pseudonym 'Satoshi Nakamoto'[5]. The white paper 'Bitcoin: A Peer-to-Peer Electronic Cash System' detailed an innovative digital currency system which would allow payments to be transferred directly, without an intermediary (peer-to-peer). In 2009, using Blockchain technology, Bitcoin was released. In 2017 (8 years later), Blockchain.info, a bitcoin wallet and block explorer service, claim to have already "powered over 100M transactions and empowered users in 130 countries across the globe"[6].

Although Bitcoin is currently the largest application of Blockchain, influential individuals such as Richard Branson (Founder, Virgin Group), as well as world renowned companies (including IBM, Deloitte and Microsoft) are backing the technology and its possible uses in other industries[7].

One application which is also arguably revolutionary, is the development of Ethereum – another public Blockchain. Ethereum provides a way to execute peer-to-peer contracts (known as 'Smart Contracts'). The contracts are essentially programs written that can verify if a product or service has been sent by a supplier. Once verified, money will be transmitted to the recipient.

The future may not be clear for Blockchain, however it is likely that the technology will have a significant impact in the next few years. PwC's executive claimed in the first 9 months of 2016, $1.4 billion was invested globally in Blockchain start-ups[8]. It is believed banks and other financial institutions can save money (potentially billions) through Blockchains transparency, security and accuracy.

Although there is no official or agreed upon way of categorising Blockchain applications, this report classifies Blockchain applications into 8 areas. The 8 areas which will be briefly assessed in the report are:

- Currency
- Payment Infrastructure
- Smart Contracts
- Digital Assets
- Identify
- Verifiable Data
- File Storage
- Voting

In recent years there has been a lot of research undertaken related to Blockchain, however, it is still unclear whether the technology can be profitable. Since the technology is still in its infancy, there are not many examples of individuals reaping the benefits from previous investments. This is why the report intends to focus on profitability – a previously neglected area of research.

Most (relevant) high-profile white papers, journals and articles focus on how Blockchain can be used (or adapted) to create new opportunities and improve processes. Other non-application research predominantly focuses on the technical and legal issues. This report builds upon the commercial exploitation element of Blockchain technology, assessing the available (or soon-to-be available) investment options for venture capitalists (the report's main audience).

With a 12 – 15 week timescale for undertaking the project, there will not be a sufficient amount of time to analyse whether the investors do in fact profit from the report's suggestions in the long term. The report also does not have a budget to undertake excessive research. However, some of the key white papers related to Blockchain technology, which the report will refer to (and build upon) throughout the report are:

- 'Bitcoin: A Peer-to-Peer Electronic Cash System' by Satoshi Nakamoto
- 'The Ripple Protocol Consensus Algorithm' by Ripple Labs Inc
- 'Practical Byzantine Fault Tolerance' by Miguel Castro and Barbara Liskov (MIT)
- 'MultiChain Private Blockchain' by Dr Gideon Greenspan, Founder and CEO, Coin Sciences Ltd

The above white papers introduce protocols, concepts and possible applications related to Blockchain. This report will use these papers (and other sources) to help explain how Blockchain works, and how it can be applied. The report extends on this related work by providing a solution to the previously unanswered problem; is Blockchain technology worth investing in, and if so, what particular area or application should be invested in?

Approach

To understand whether Blockchain technology is worth investing in (and if so, what particular area/application), the report first focuses on what Blockchain technology is, and how it works.

The justification behind this approach, is that by developing an understanding of how Blockchain works, the report's beneficiaries can gain an initial insight into the technology's potential (and realistic) applications. The purpose of the 'Current (Mainstream) Blockchain Uses and Companies' section is to reinforce the introductory sections, whilst leading into the 'Blockchain Application Profitability: SWOT Analysis' section. By combining all of the previous research, as well as demonstrating further research conducted on: investment strategies, application profitability, and the role of venture capitalists, the 'Venture Capitalist Summary' section answers the problem that the report attempts to solve.

The 'Venture Capitalist Summary' Section is the main output of the report – an 11 page summary which assesses the suitability of investing in 3 different Blockchain related applications (each in a distinct industry). For the output to be successful, applications were initially grouped into 8 main areas, before 1 area was selected based on how investable it appeared to be (negative aspects and risks were taken into account). This approach was taken as it would be unfeasible to give an in-depth analysis of the profitability and risks associated with every Blockchain application ever mentioned. From the main category selected, 3 possible investment options were then chosen.

The SWOT (Strengths, Weaknesses, Opportunities, and Threats) method was used as an initial method of evaluating each application area. The benefits of this methodology are that it:

- Is cost-effective
- Offers insight, whilst being simple to undertake
- Allows the use of quantitative and qualitative information
- Provides a visual overview
- Highlights clear areas of strengths, weaknesses, opportunities and threats without showing too much bias to any particular area

For the majority of the report, the following types of sources were used to conduct Blockchain research: online journals, articles, white papers, and eBooks. Discussions with experts in the field were also attempted via email, social media, online article comment sections, and public forums. Qualitative research helped gain an understanding of underlying reasons, opinions and motives behind the use of the technology.

To help with the 'Venture Capitalist Summary' section, quantitative research was used where possible to enhance the validity of the profitability angle the report intends to focus on. Although public surveys and questionnaires are often seen as useful ways to gather data and opinions, these were avoided for one main reason. Blockchain is an up-and-coming technology, and the majority of the world's population either have not heard of the technology, or they do not have a complete understanding yet.

As mentioned in the ‘scope’ section of the report, the potential scope of the project is large, with too many potential Blockchain applications to cover in detail. With approximately 12 – 15 weeks to undertake research and report writing, as well as having no budget, the report was approached in a way which meant only a selection of Blockchain applications were assessed in terms of profitability. Similarly, only consensus mechanisms considered mainstream and secure were covered in the ‘Consensus Mechanisms (and Types)’ section.

To see the benefits of this project in the long term, there would need to be more time and commitment invested in this project. Many investments take several years before a return is seen. Furthermore, when investing in companies that are experimenting with new technologies, there is normally an initial period which will involve switching technologies, early operating costs, and on-going maintenance.

As a whole, this report aims to contribute to society by giving investors and individuals interested in technology the opportunity to understand the future of Blockchain technology from both a technical and business perspective.

How Blockchain Technology Works

Introduction to Blockchain Technology

Blockchain technology (also referred to as Blockchain, the blockchain, or even Block Chain) is often perceived to be a complicated subject. In a single sentence, it can be described simply as a digitally distributed ledger for transactions. The ledger can store information on assets, inventory, money, and anything that can be transacted.

The ledger (essentially a decentralised database) is stored and maintained on a distributed set of computers that are able to communicate with one another. The replicated ledger is synchronised via the internet, and made visible to anyone on the network. If the Blockchain is public (and permissionless) then anybody in the world can access the network as long as they have a device and an internet connection.

Data about the transactions that take place is electronically arranged and stored in cryptographically protected fixed structures or 'batches' known as blocks. These blocks use cryptographic validation techniques, linking the blocks together and forming a linear, chronological chain (hence the name 'Blockchain'). The blocks identify each other by using a *hashing function* to draw upon the previous block in the chain.

Every transaction in the history of time is on the Blockchain (and all blocks are linked together). The blocks are timestamped, and the chain is updated continuously on every ledger on every node. Hacking the decentralised Blockchain is thought to be near-impossible since every block, on every machine, would need to be changed. This is why transactions are seen as reliable and secure.

Blocks have a header and content. The header includes a block reference number (unique), the timestamp, and a link back to the previous block. The content is a validated list of the assets (e.g. bitcoins). The 'blocksize', the amount of the transaction, and the addresses of those involved in the transaction are also included[9].

To reach consensus across the network, participants/nodes on the network usually need to use their computing power to authenticate and verify each created block (although this isn't the only method for reaching consensus). These participants are often referred to as 'miners'. Miners are normally incentivised to use their computing power, for example, Bitcoin miners are rewarded with the network's currency – bitcoins (spelt with a lower 'b'). Different Blockchains use different consensus mechanisms.

Despite public Blockchain networks (such as Bitcoin) often dominating the news, Blockchains can be private with restricted membership. There's also arguably another type of Blockchain, although it is sometimes coupled with 'private Blockchains'. This Blockchain type is known as a consortium, which can be described as a "hybrid between the 'low-trust' provided by public Blockchains and the 'single highly-trusted entity' model of private Blockchains"[10].

What’s Common to all Blockchains?

In Satoshi Nakamoto’s original paper, there was never actually a mention of the word ‘Blockchain’, although there were clear references to blocks being chained[5]. It is unknown who originally coined the term ‘Blockchain technology’.

Many industry experts and individuals have debated the difference between Blockchains and distributed ledger technology. For example, can a Blockchain be private, or is ‘being public’ a key characteristic? Are private blockchains simply glorified databases? Bitcoin maximalists, those who look down upon alternative uses cases outside of Bitcoin, may argue that the Bitcoin Blockchain is the only Blockchain[11]. This subject will be looked at in detail later on in the report. However, assuming Blockchains can be private, below is a list of the elements common to all Blockchains:

- The ledger is decentralised – it is distributed across more than one computer in real-time

- The entire ledger of records is available to all users on the network (if the Blockchain is public and ‘permissionless’ then this will be everyone)

- Multiple participants in the network are needed to reach consensus (using their computers to verify each block)

- Blockchains are persistent due to consensus, they can’t easily be misplaced or taken offline by one computer on the network

- There are mechanisms which make the Blockchain theoretically immutable. Historic data cannot be altered unless rules have been put in place

- Cryptography and digital signatures are used to prove identity; cryptography also helps ensure the integrity of the ledger

- Transactions are timestamped, allowing them to be tracked (useful for verifying information at a later date)

How do Transactions Work? (Using Bitcoin as an Example)

As mentioned, when a transaction takes place within a Blockchain ecosystem (and the nodes reach agreement), there is a change to all of the distributed ledgers on the network. In the context of Bitcoin, a transaction is handled within a program known as a ‘wallet’. The transaction is sent from one wallet to another, with the transaction being digitally signed to enhance security. In Satoshi Nakamoto’s paper, a bitcoin (an electronic coin) was defined as ‘a chain of digital signatures’[5]. Cryptography is used to validate the transactions, and this is why bitcoins and other digital currencies (e.g. Litecoin) are known as ‘cryptocurrencies’[12].

The current bitcoin owner (the sender and ‘signer’) transfers the ‘money’ to the receiver by signing a hash of the previous transaction (as seen in Figure 1 below). The public ECDSA (*Elliptical Curve Digital Signature Algorithm*) key of the receiver is used by the signer, along with the signer’s private key. When the transaction is broadcast, the network’s participants know the new owner of the bitcoins is the owner of the new associated key[13]. The signature verifies the message is authentic.

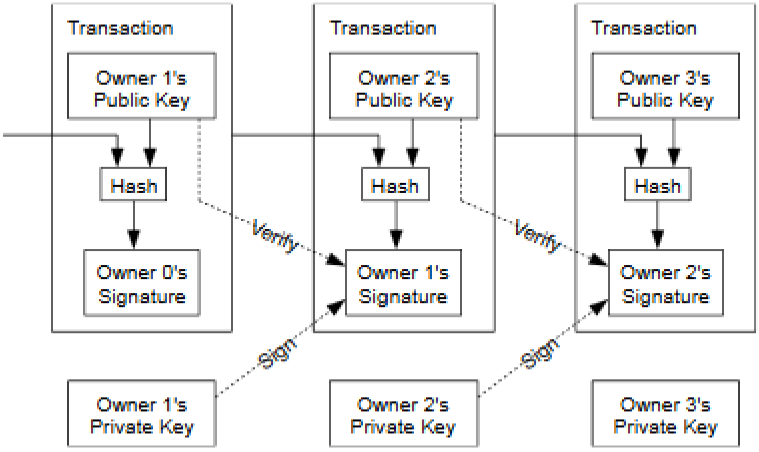


Figure 1: Hashing of Blockchain transactions on the Bitcoin network[5]

To simplify the above diagram, and further clarify how public cryptography works, imagine Alice wanted to send a bitcoin to Bob (a transaction) over the network. Using a wallet, a message would be broadcast to all network nodes (including Bob), and the amount (e.g. 1 bitcoin) would also be known.

When Alice broadcasts a message using her wallet, she is in fact requesting Bob's public key – which is known to all network participants. The public key is used to 'jumble' (encrypt) the broadcast message. Bob, who has the paired (private) key, can decrypt and read the message[14]. The private key should be kept secret so only Bob can 'unjumble' the message.

Alice's transaction request is encrypted with her own wallet's private key. Alice actually generates a digital signature which is used to verify and validate the legitimacy of the transaction. Although anyone can verify the digital signature using public keys (available to everyone), making the digital signature requires a private key. In essence, the digital signature links the request, Alice's identity, and Alice's private key together. A digital signature must be:

- Unique to the message
- Unique to the sender (preventing forgery and denial)
- Computationally infeasible to forge
- Relatively easy to recognise and verify
- Small enough to store

Since digital signatures are a string of characters, it is easy to tell if a transaction has been tampered with. If a single character in the transaction is changed, the signature changes, and all nodes will be notified. This is just one of the reasons Blockchain technology is seen as secure.

Once a transaction takes place, each network node applies the requested transaction to their ledger. Alice and Bob's wallets update to reflect their new bitcoin value. Although the Blockchain network does not 'store' account balances, it stores the transactions which are then used to calculate balances. Technically, bitcoins don't actually exist anywhere, there are no bitcoins, only records of transactions[15]. All transactions are visible in the Blockchain, and using a Blockchain browser (also known as Blockchain explorer), every transaction can be viewed in a human-readable format. The website 'https://blockchain.info/' is an example of a popular browser[16].

Transactions are typically made up of 3 components; the input, the content and the output (sometimes content and output are combined as 1 component):

Input – A reference to an output from a previous transaction. Often, multiple inputs are listed in a transaction. All of the inputs included on the transaction are added up. This is to allow value to be split and combined. The total of the input (minus any transaction fee) is used by the outputs.

Content – The actual transaction, in the case of Bitcoin it will be the amount of bitcoins to be sent.

Output – Contains instructions for sending bitcoins; the recipient's wallet address.

A transaction will normally include either a single input (larger than the output), or several inputs with smaller values combined. There will be at most two outputs, one for the actual payment and one for returning the change back to the individual making the payment[17]. This can be seen in Figure 2.

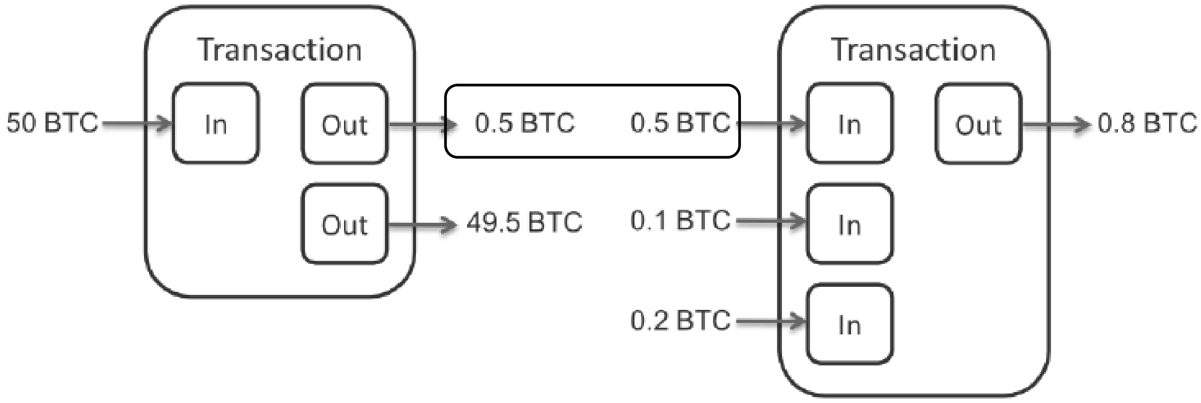


Figure 2: Example diagram of Bitcoin transactions and their inputs and outputs[18]

If bitcoins are 'misplaced' or broadcast to a wrong address, it is likely that they will be lost forever. Due to the decentralised and distributed nature of Blockchain (particularly in the Bitcoin example, and other public Blockchains), there is no 'customer support'.

However, having a single (public) ledger which states in what order transactions were received, means the network can avoid having to use a central authority to check whether a bitcoin was double-spent. All previous transactions can be seen, and the receiver can see the sender did not sign any earlier transactions.

<u>What are Blocks?</u>

After a transaction in the Bitcoin network, you have to typically wait an average of 10 minutes for the transaction to be confirmed and authenticated by all nodes (miners). This is because miners need to finish the process of grouping transactions into files called blocks[9]. The time it takes for transactions to be verified depends on the consensus mechanisms/algorithms used – for example, Ethereum blocks take 12 seconds to be confirmed on average[19]. Consensus mechanisms will be covered in-depth later on in the report.

Transactions are only placed in the same block if they have taken place within a similar timeframe. Transactions that are not yet in a block are considered 'unconfirmed'. On Februrary 18th 2017 at 12:23 GMT, there were 453,617 blocks on the Bitcoin Blockchain[20].

The (Bitcoin) block structure contains:

- A 'magic' number (always the same number – used to identify the type of file/data structure)
- The block size
- A transaction counter
- The transactions
- The Block header (which is made up of: the block version number, the timestamp, hash information, and the answer to a mathematical puzzle)

The key bits of information are that the block is a record of transactions at a point in time, and that the block contains an answer to a difficult to solve mathematical puzzle. This puzzle is unique to each block[21].

Introduction to (Bitcoin) Consensus

Although Blockchains can use different consensus algorithms and protocols, this report initially discusses Bitcoin's proof-of-work protocol. Since every chain of blocks on all ledgers has to be the same, there needs to be a mechanism which allows consensus amongst network nodes. For a block to be submitted to the network, an answer to a puzzle needs to be given – this is the process of 'mining'. Essentially, nodes compete to find the answer that 'solves' the block. Once a correct (valid) answer is found, the rest of the network confirm the solution and add the block to their version of the chain[9].

To 'solve' the block, miners use significant computing power. Miners repeatedly guess random numbers on their computer in an attempt to establish a correct answer (there are actually multiple solutions). A nonce, an arbitrary number used once, is a big part of the proof-of-work system.

Another key part of the proof-of-work system is a hash, a sequence of characters converted into a string of 64 letters or numbers. If any of the text is changed, an entirely new hash is formed. If a hash on the Blockchain is changed, everyone will know – this is why transactions should be secure and tamper-proof.

The hash of the previous block of transactions is known to everyone (since records are public). The hash forms the start of the miners 'solution'. Miners add the current block of transactions that they're working on to the previous hash, and then add a nonce (the random number). Then the miners hash the block to give a string of characters. The correct answer must have a certain number of zeros in front of it (determined by the network). Although it may sound relatively easy for a computer, it is thought that the computer performs 10^{21} computations (a lot of computational effort)[22]. The mathematical problem is extremely difficult to solve, but a valid solution is very easy for the rest of the network to confirm.

Since computing power improves over time, the mathematical problem's difficulty is appropriately adjusted by the network. This happens approximately every 2 weeks, with the network coming to consensus and making the change automatically. The system attempts to make it so 6 blocks are solved per hour. This is why transactions take an average of 10 minutes before they are confirmed[9].

Although it may not seem clear why individuals are willing to spend considerable amounts of money on computers and electricity to solve the blocks, there is in fact an incentive. Different Blockchains have difference incentives, Bitcoin's being bitcoins (the currency).

Another incentive for nodes to 'mine' is transaction fees. If the output of a transaction is less than the input, the difference is the transaction fee which is added to the incentive value of the block. This is why nodes stay honest. As Satoshi Nakamoto alluded to, users find it more profitable to 'play by the rules'[5]. As a result, this helps Bitcoin's Blockchain ensure distributed consensus.

In June 2016, The New York Times ran an article detailing how cheap electricity in China meant the country were the leaders in terms of supercomputers performing 'mining' activities. At the time the article was published, one individual who described himself as "an expert in finding cheap energy" estimated his Bitcoin mining machines in his (28) facilities used approximately 38 megawatts of electricity, enough to power a small city[23].

The proof-of-work protocol works in a way whereby 51% of the Bitcoin networks hash power needs to be controlled by malicious nodes for the Blockchain to be 'destroyed'. This is known as a '51% attack'. Although it is extremely unlikely a single node will have the power to do this, it is thought that mining pools may be a risk. Due to the high difficulty in securing blocks, 'pools' of miners often form, where multiple clients contribute to the generation of a block. The reward is then split[24]. Mining pools may have the potential to control 51% of the network, allowing them to generate fraudulent transactions or cause serious disruption.

Although this may seem like a big potential risk to the Blockchain, so far there has never been a successful 51% attack in the history of Bitcoin. The website 'Bitcoin wiki' ensures there are steps taken to prevent 'cheating' with regards to pooled mining[25]. This helps ensure transactions are secure and trustworthy.

Another reason why transactions are considered trustworthy, is because of the low probability of two blocks being solved at the same time. Although it is considered near-impossible, it can occasionally happen, forming temporarily splits of the chain (also known as forks in the chain). However, the splits are solved within a short period of time, with the longest chain surviving. The longest chain is defined as the chain with the most combined difficulty (the one with the most work gone into it), hence the name 'Proof-of-work'[9].

It is worth noting, that to save disk space, Merkle Trees are used. Merkle Trees allow efficient and secure verification of transactions without breaking the block's hash. Since all of the transaction hashes are hashed themselves, the result is a Merkle root. Only the root is stored in the block (more specifically, the block header). This means only the root needs to be checked to verify a transaction has been accepted by the network. This can be seen in the below diagram (Figure 3) taken from the original Bitcoin white paper.

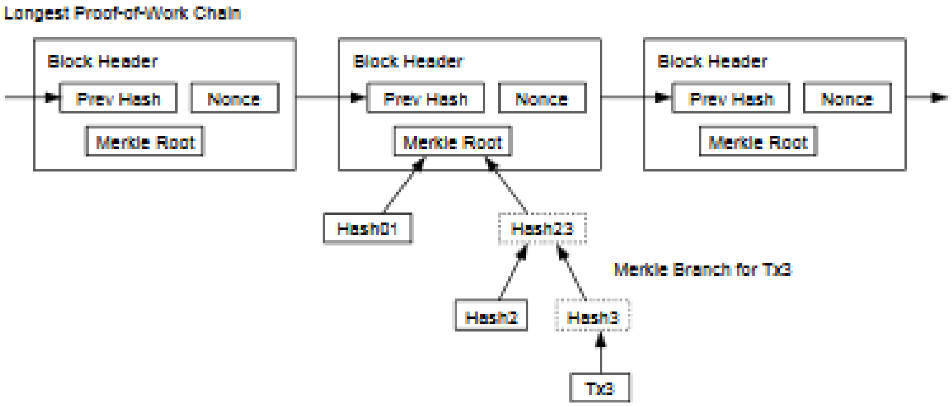


Figure 3: Verifying a network transaction (abbreviated to 'Tx') via a Merkle Tree[5]

Consensus Mechanisms (and Types)

A common misunderstanding about Blockchain technology is that companies ‘build’ Blockchain technology. A former Blockchain blogging website ‘Truthcoin’ use an interesting analogy to clear this up. People work on using the Blockchain. Like Uber does not build cell phone technology, companies do not build Blockchain technology[26]. However, different consensus mechanisms can be used to make the technology successful.

Consensus (a general agreement) is not a new idea or concept, it has existed long before computers were created. However, when it comes to Blockchains and distributed ledgers, a consensus mechanism is essentially a way in which the majority of nodes on the network agree on transactions and the ‘correct’ ledger. Consensus mechanisms can be considered the backbone of Blockchain technology. This section will look at what defines a consensus mechanism, as well as some popular mechanisms currently used.

Parameters That Define a Consensus Mechanism

Although there are variations between each consensus mechanism, below are parameters (listed in a KPMG white paper) that must be fulfilled before consensus mechanisms can be applied:

- Decentralised Governance. No single node on the network (or a single centre of authority) can determine the finality of a transaction.

- *Quorum* Structure. Nodes must be structured in a way which allows transacting in predefined ways.

- Authentication, Integrity and Non-Repudiation. All nodes must be able to verify the identity of each other, and transactions should be valid. There must also be a way to verify the initiator/sender of the transaction. This is achieved via cryptography.

- Privacy. Only the intended recipient of a message should be able to read it, maintaining confidentiality. Similarly to authentication, integrity and non-repudiation, this is also achieved using cryptography.

- Fault Tolerance. Even if several nodes fail (or become slow), the network should operate efficiently and in a normal manner. Essentially, nodes should always work together as a single unit.

- Performance. The performance of the Blockchain should be to a high standard. The performance includes throughput (transaction per unit of time), scalability (how many nodes can be added without affecting performance), and liveness (the transmission of concurrent data)[27].

Popular Consensus Mechanisms

Although proof-of-work is often the mechanism of choice when it comes to Blockchain technology, there are many consensus mechanisms that are already in use or being trialled. Below is a list (featuring brief explanations, advantages and disadvantages) of some of the most common mechanisms. These mechanisms can often be combined or adjusted depending on the associated Blockchains purpose:

Proof-of-Work

As explained in the report previously, miners build blocks filled with transactions, and then calculate the hash of their block header to see if it fits the current target. The difficulty of the ‘challenge’ requires miners to try quadrillions of times before they find a solution[28].

One advantage of this method is that miners are provided with financial incentives to process as many transactions as they can in a short period of time. Another advantage is that this consensus mechanism has been researched the most, and it has proved it can work (e.g. the Bitcoin network).

On the other hand, one disadvantage is that it is resource exhaustive. A white paper from the National University of Ireland Maynooth estimates that the power currently used for Bitcoin mining is comparable to Ireland’s electricity consumption[29]. There is also the potential for somebody extremely rich to invest millions in computing hardware, making it easier for them to successfully mine. Off the back of this, the difficulty of adding blocks will increase, and other miners will start to exit as the likelihood of a reward is reduced. Another downside is that secure transaction settlement means there can be a delayed wait (potentially tens of minutes).

Proof-of-Stake

The second most common mechanism used in Blockchains is proof-of-stake (PoS). Similarly to proof-of-work, this mechanism attempts to prevent double-spending. Miners (referred to as voters or validators) do not solve computational problems. The probability of mining a block depends on the resource that the miner holds – essentially the higher the ‘value’ of the validator, the more chance of submitting a block (although the block creator is selected in a pseudorandom way). For example, if proof-of-stake was used in Bitcoin, someone holding 1% of bitcoins available can mine 1% of the proof-of-stake blocks[30].

With regards to cryptocurrencies, there is no coin creation using this mechanism, as all coins exist from day one – validators are rewarded via transaction fees. Validators invest in the coins of the system, rather than computer hardware. Once a block has been created there still needs to be a method for adding this to the Blockchain. Methods can include randomly chosen groups of signers, or every node needing to sign the block until the majority of nodes across the network agree[31]. The actual generation of blocks can be considered similar to proof-of-work, however the hashing operation is done through a limited search space (proof-of-work is unlimited)[32].

The method for determining the initial distribution of stake can vary. Nxt (an open source cryptocurrency) asked for small donations of bitcoins (using a forum ‘bitcointalk’) to decide who would receive what amount of coins when the genesis (first) block was created. A total of 1,000,000,000 coins were distributed to 73 stakeholders[33].

One advantage of proof-of-stake is speed; blocks can be added within seconds. Secondly, it is harder for malicious miners to attack the Blockchain as it is expensive to carry out attacks, and there are reduced incentives for doing so. This makes the mechanism potentially more sustainable and scalable. It is also considered ‘greener’ since it does not require an excessive energy bill[34]. Proof-of-stake is best used by companies that are constrained by computing power.

Despite this, there are several concerns. Firstly, the ‘richest’ node/participant will always be the most likely to create a block. This creates a problem of the rich getting richer. Another (technical) concern is that the proof-of-stake principle can create an issue known as the ‘nothing at stake’ problem where validators can be incentivised to build multiple branches/forks of the Blockchain. A validator can create two blocks in an attempt to claim two sets of transactions fees. If there is nothing to lose, then there is no reason to not do it. Furthermore, block generators have nothing to lose by voting for multiple Blockchain histories, which can cause consensus issues (consensus is never resolved)[35]. There have since been attempts to solve this problem.

One interesting example, is that Ethereum (a popular public Blockchain platform) plan on transitioning ‘mid-flight’ from proof-of-work to the proof-of-stake protocol in late 2017 or early 2018. They plan to use a protocol called Casper which punishes users trying to take advantage of the ‘nothing at stake’ problem. CoinDesk (the world leader in Blockchain news), published an article featuring an extreme analogy by Vitalik Buterin (the co-founder of Ethereum). The analogy explained that you make $1 each time you sign the transaction history that others sign, and if you want to be malicious and repeatedly sign something different then “your house burns down"[36].

Delegated Proof-of-Stake

A variant system of proof-of-stake is delegated-proof-of-stake (DPOS) – a democratised Blockchain model. In regular PoS systems, every wallet with coins is able to participate in the process of validating transactions, being rewarded with transaction fees in return. In DPOS, every wallet which contains coins is able to vote for delegates (sometimes referred to as representatives). It is these delegates who take part in the actual consensus, validating the transactions[37].

An advantage of this method, is that small and medium wallet holders can profit from this mechanism. BitShares (a decentralised exchange) were the first to implement this model. They claim that by deterministically selecting the block producers, this allows transactions to be “confirmed in an average of just 1 second”. In addition, the protocol is “designed to protect all participants against unwanted regulatory interference”[38].

Despite BitShares claiming the protocol is the most decentralised model available, the delegate method means only a smaller number of people are involved. This is arguably less decentralised and resilient as a result. Voter apathy is also problem, if regular users fail to vote, the network could potentially be controlled by powerful/large individuals who have the ability to vote for themselves.

Round Robin

The round robin approach is best suited to a ‘private’ Blockchain (explained in detail later). In a private Blockchain the miners (or ‘block-adders’) are known, so there is no need for a mining puzzle. MultiChain (a reputable build-your-own Blockchain service) offer solutions whereby users can configure how their Blockchains behave. Depending on the settings/rules chosen, it can be possible for any miner to add a block at any time (strictness of 0). It is also possible to have a Blockchain that has a strictness of 1, meaning once a block has been added the miner can’t add any more until every other node has added one[39].

The round-robin method utilises a random approach, with each block needing to be digitally signed by the miners before it is added to the ledger. The percentage of users that must sign the block for it to be valid is usually tailorable on private Blockchains. Although this can be a simple, tailorable, and a beneficial method for a private blockchain, it is unlikely to be used for public Blockchains.

Practical Byzantine Fault Tolerant

The Practical Byzantine Fault Tolerant (PBFT) mechanism was first mentioned in 1999, when two individuals from MIT published an academic paper describing how PBFT can be used to allow systems to continue to work correctly even when there are software errors[40].

PBFT is based on the Byzantine general's problem. This problem is the idea of a group of generals, each commanding part of the Byzantine army. Each part of the army surrounds a city, and the generals can only communicate by messenger. Each group can choose to attack or retreat. If one (or more) of the generals involved is a traitor distorting messages (in an attempt to ruin the plan), then how many traitors would be needed to 'overthrow' the unified force[27]? This is translatable in terms of computers and digital assets. In a Blockchain system, nodes can be compared to generals. How many malicious nodes (traitors) can be present before the system's reliability is damaged?

The Hyperledger project, an open-source Blockchain platform hosted by The Linux Foundation, utilises the PBFT mechanism. The purpose of the Hyperledger project is to allow developers to create their own digital assets with a distributed ledger. In the Hyperledger PBFT system, each node publishes a public key. Messages coming through each node are signed by that node to verify its format. After enough identical responses the transaction is deemed valid[41].

PBFT is a good mechanism for a digital asset transaction system requiring low latency (high transaction volume but not a large throughput). Consensus can be reached fast and efficiently using this mechanism, and the system does not require hashing power as part of its process[28].

However, PBFT has three disadvantages. Firstly, PBFT comes at the cost of anonymity; all parties need to agree on the exact list of network participants. Off the back of this, membership in this system is set by a central authority[28]. Thirdly, with no mining incentives, there may be no reason for nodes to behave.

Federated Byzantine Agreement (FBA)

Federated Byzantine Agreement (FBA) is also based on the Byzantine general's problem. This mechanism assumes network participants know all of the other participants. Each node can also distinguish other nodes which it considers important. Essentially, FBA relies on small sets of parties who trust each other's information. A node in question waits for other nodes to agree on a transaction before considering the transaction settled. If enough sets of trusted parties form (the majority of the network), then consensus is achieved.

Ripple (a software company specialising in financial settlement) created a protocol based on maintaining robustness in the face of Byzantine failures. Using an iterative consensus process, it is energy efficient, and it can take only a few seconds to finalise transactions[42]. The mechanism uses a native currency called XRP (ripples), and as of early 2017, Ripple was the third-largest cryptocurrency by market capitalisation[43].

Stellar, an open-source protocol for value exchange, is also based on FBA. The founder, Jed McCaleb (who originally worked for Ripple), ensures they have "tested to 100 million accounts and a few hundred transactions per second", and that the system currently holds up under those loads[44]. This shows the scalability of the mechanism. However, it is not suitable for systems where decentralised control is an imperative.

Leader-Based Consensus

In leader-based (or leader-elected) systems, a leader is elected by the network, who then validates transactions and sends data to the other nodes. This node stays in control until a vote decides on a new leader.

One example of this consensus model is PAXOS, an academic protocol that is deemed complicated and difficult to implement in real-world conditions[45]. An alternative (but similar) protocol to PAXOS was developed and published in 2014. The mechanism was named RAFT, and was supposed to be easier to understand and utilise. More alternative leader-elected mechanisms have been developed since, including Tangatoa and Juno12[27]. None of these mechanisms have truly became mainstream, showing that there are probably better consensus mechanisms that are available.

Proprietary Distributed Ledger

A Proprietary Distributed Ledger (PDL) is a ledger that is unique in nature. It may or may not be based off existing consensus mechanisms[27]. However, PDLs relate to an owner; a central entity or a consortium (several companies). Potential scenarios that PDLs could be suitable for include: supply chains, trading groups, or companies that want to work together but are competitors.

As an example, the technology and chipmaker company 'Intel' came up with their own consensus mechanism called Proof of Elapsed Time (PoET). The protocol is similar to proof-of-work but is advantageous as it uses less electricity. Other benefits include scalability, as well as a pre-existing trust between participants that allows for agreed upon security measures[31]. An obvious disadvantage is that PDLs require trust in the central authority (e.g. Intel). Some may argue that the whole reason for Blockchains in the first place was to remove third parties and intermediaries.

Node to Node (N2N)

A Node to Node (N2N) system encrypts transactions between nodes, but only the nodes involved have access to the data. These systems are suitable for the regulated financial industry as third parties (e.g. regulators) may have opt-in privileges[45]. Therefore, a benefit of this method is a high degree of transaction confidentiality.

An example of a N2N system is R3 CEV's ledger 'Corda', aimed at banking consortiums. Using a set of rules that participants have agreed upon, an environment is created where everyone has access to the same data. Despite initially being dubbed a Blockchain platform (and receiving financial backing from more than 70 of the world's biggest financial institutions)[46], there has been disputes whether Corda is in fact a 'shared ledger' platform which does not officially use Blockchain technology[47].

Types of Blockchain (Public vs Private)

Public vs Private – Definitions

Although the report has so far focused on public Blockchains (specifically Bitcoin's Blockchain), Blockchains can be public or private. There is also arguably a 'meet-in-the-middle' Blockchain – a consortium (or hybrid), however some people prefer to classify this as a private Blockchain. This section of the report will look at what defines the Blockchain type, as well as advantages and disadvantages. Below are brief summaries of the 3 types:

Public – A Blockchain that anyone in the world can (theoretically) be part of – sometimes referred to as a 'permissionless' Blockchain. Participants can read the ledger, send transactions, and be part of the consensus process. There is usually little (or no pre-existing) trust between participants. However, using cryptography, consensus mechanisms, and possibly incentives, the Blockchain can be seen as secure and trustworthy. As a result, central authorities are not needed.

Hybrid/Consortium – A Blockchain where the consensus process is controlled by pre-selected nodes. Pre-existing trust normally exists to some extent. In a blog by Ethereum co-founder Vitalik Buterin, a consortium Blockchain is described as "partially decentralised". The blog extends the definition with an example; imagine 15 financial institutions, each operating a node. For a block to be valid, at least 10 of these 15 institutions must sign the block. The Blockchain ledger may be partially public (everyone can read it, but not write to it) or restricted to the participants[10].

Fully Private – A Blockchain where write permissions are kept centralised to one organisation – similar to a database (but with cryptographic auditability). Read permissions can be public or restricted. Use cases could include auditing purposes, or simply a more secure database management system.

Again, it is worth noting that 'consortium' and 'fully private' Blockchains can simply be referred to as 'private' Blockchains. From this point onwards, the report will refer to only public and private Blockchains.

Advantages and Disadvantages of Blockchain Types

There are many different views on whether there is room for both public and private Blockchains to prevail. Some experts believe a blend of the two types could even be foreseeable[48]. Although there is some overlap, below is a summary of the advantages and disadvantages of both types:

Advantages of Public Blockchains:

- Resistance to censorship. Public blockchains can't simply be taken 'offline', and developers have a way of saying 'I have no power to do this, even if I tried'. Eric Larchevêque, CEO of Ledger (a Blockchain solution provider) believes "public Blockchains with censorship resistance have the potential to disrupt society" whereas "private Blockchains are merely a cost-efficiency tool for banking back offices" [49].

- Decentralisation. Trust does not arise from a centralised authority, since the Blockchain is maintained by the underlying mathematics (and the users themselves). Having no centralised point of failure ensures reliability and longevity. If one node fails, the Blockchain can still process transactions.

- Openness. Any users can broadcast transactions (that conform to the protocols used). Being permissionless and public means greater amounts of people will willingly 'take part'. Having more entities using the system means it is more likely to be sustainable over time. Bitcoin has incentivised people to mine for example, so more nodes join the network to compete for the block reward.

- Immutability. Over time, the Blockchains history will not change (only grow). Transactions and related information cannot be deleted since public Blockchains are designed to be append-only. This makes the ledger more trustworthy.

- Disintermediation. Although private Blockchains are still be peer-to-peer, public Blockchains allow both producers and consumers to avoid the use of intermediaries. This should theoretically mean no bank charges of levied charges when transacting goods/services.

Disadvantages of Public Blockchains:

- Often secured by hashing power. Most cryptocurrencies use the proof-of-work system. If this system is used, it is possible for fraudulent activity to take place on a network if someone 'rich' comes into play. Even worse, the network could be taken down. For example, a '51% attack' was potentially possible on the Bitcoin network when a pool from China (GHash.IO) held 54% of the hashrate for a day – before the situation was swiftly responded to[24].

- Computational resource needed. Although different algorithms can mean less need for computational power, it is still likely that a public Blockchain will have more users in comparison to a private Blockchain. Nodes normally need to meet a basic hardware requirement, costing money in terms of hardware and electricity. This means scalability problems are also a potential disadvantage.

- Privacy concerns. Although identities are normally hidden, this doesn't mean it is impossible to trace users. In one example, when signing up to Blockchain services, emails are often used. These emails are potentially linked to a real user. This brings up a whole new question, whether this is a disadvantage of Blockchain technology, or a fault from the service providers.

- Security concerns. Despite cryptography being used, there's often security concerns associated with public Blockchains. One example is a potential eclipse attack, which is described as "crippling one of the nodes in such a way that it fails to interact with other nodes"[50]. Bitcoin's Blockchain may be seen as secure, but there are many other public Blockchains in the world.

- Irreversibility. Although the immutable and irreversible characteristics are often seen as a positive, if a legitimate user loses (or accidentally reveals) their private key on a public network then this can mean a loss of assets.

Advantages of Private Blockchains:

- Flexibility. Companies/consortiums running a private Blockchain can potentially change the rules of the system. This means transactions can be edited if needed. For example, an Ethereum blog brings up a valid point that this functionality would be a necessity in a land registry (transaction) system[10]. The ability to give chosen individuals different read/edit/write permissions is also possible.

- Validators are known. Having designated mining nodes and known identities can reduce the risk of an attack (since nodes are considered trusted). Traceability also becomes a factor, as any 'frowned upon' activities can be linked to individuals.

- Smaller amount of nodes. Less users on the network can mean cheaper transactions (thousands of high processing power machines are unnecessary). A smaller network also means faults can be fixed quicker.

- Shorter block creation times. Mass consensus amongst nodes may not be needed. Trusted nodes mean mechanisms can be used which lead to (almost) instant confirmation of blocks.

- Greater level of privacy. Permissioned Blockchains mean read and write permissions can be restricted. If an organisation only wants a small number of people to be authorised to have access to the Blockchain data, then this is possible.

- No cryptocurrency needed. Public Blockchains like Bitcoin and Ethereum often use their own cryptocurrencies. In the case of Ethereum, 'Ether' (a '*crypto-fuel*') is a necessary element for operating the distributed application platform. A private Blockchain would not need this.

- Enhances collaboration. A consortium model is a good way of working with competitor firms – for example, using a private Blockchain as a way to have a cryptographically secure balance sheet with another organisation. Private Blockchains also have the potential to make supply chains more efficient.

- Cryptographic auditing. Private Blockchains can be used in a similar way to a decentralised database, but the cryptography behind it ensures trustworthiness. Max Kordek, CEO of Lisk (a public Blockchain platform) believes "a private Blockchain is a great first step towards a more cryptographic future"[49].

Disadvantages of Private Blockchains

- The technology is still in its infancy. There are still misunderstandings about the technology, and whether or not it can truly have an impact in everyday organisations. One example, is that companies such as Santander and Goldman Sachs previously invested in R3 CEV's Blockchain and then later pulled out[51].

- Regulatory status. Although Blockchain-as-a-Service was approved for use by the UK government, there are still other regulatory and legislation concerns. Public Blockchains also have this problem, but this is particularly an issue with private Blockchains since one of the main reasons they were introduced was to be used by financial companies. In a PwC article, the CEO of Coin Sciences Ltd (who offer a private Blockchain solution) stated: “Blockchains only really work legally if they’re also controlled and permissioned. Otherwise the entity issuing an asset is exposing itself to the wrong side of the law”[48].

- Potentially an unnecessary expense. Some people will argue that although a private Blockchain adds some layers of encryption, it still doesn’t justify the cost. For example, Brian Hoffman, founder of OpenBazaar (a decentralised network for peer-to-peer commerce) said “I personally don’t believe that private Blockchains provide much added value above a privileged database and have yet to really see a necessary use case for them”[49]. Having a private Blockchain may not be too different from a regular database system either – especially from a security standpoint. If access is gained to the ‘controlling’ keys, the network can still be corrupted. So why spend excessive amounts of money on something which practically already exists in organisations?

Summary of Public vs Private Blockchains

Ultimately, the choice of Blockchain comes down to what is required by the company deploying the technology. Both public and private Blockchain companies have received backing in the form of generous investments.

Due to renowned companies offering ‘complete’ Blockchain solutions ready for immediate use, there are already too many private Blockchains deployed to keep track of. These companies include Deloitte (offering Rubix), AlphaPoint (offering StreamCore), and Monax (creators of Eris Industries). Microsoft also offer “Blockchain-as-a-Service” (BaaS), which allow users to deploy nodes within Microsoft Azure (the cloud service). Finally, another popular option is MultiChain, a ready-to-use platform for launching private Blockchains. These Blockchains can be deployed rapidly on a desktop computer[52].

Popular companies that have public Blockchain offerings include Ethereum, Ripple and Hyperledger. The next section covers more of these companies, actual Blockchain applications, and their profitability.

Current (Mainstream) Blockchain Uses and Companies

So far, the report has predominantly covered the theory behind Blockchain applications, without necessarily covering actual uses for the technology. This report categorises Blockchain applications into 8 main categories:

- Currency
- Payment Infrastructure
- Smart Contracts
- Digital Assets
- Identify
- Verifiable Data
- File Storage
- Voting

Each of these Blockchain areas will be analysed in the next section in the form of a SWOT analysis, however the report will first cover some of the mainstream uses and companies related to each of the Blockchain areas.

Currency

As already discussed, the original use of Blockchain technology was to allow peer-to-peer transactions of ‘money’. As of March 2017, there were over 740 cryptocurrencies that had a circulating supply[43]. Some popular cryptocurrencies that can be invested in include: Dash, Monero (XMR), Ripple (XRP), and Litecoin (LTC).

Bitcoin – Although this report has already covered the technical aspects of Bitcoin in detail, there are still doubts whether Bitcoin (the most popular cryptocurrency) is profitable to invest in, in 2017. Some people may wonder what makes bitcoins valuable in the first place; however they’re scarce and useful. The shift to people using digital currencies has made the value of bitcoins rise from approximately £25 in March 2013, to £1050 in March 2017[53].Being the first mover in the cryptocurrency industry has also led Bitcoin to hold the largest market capitalisation by far (almost 10 times the market capitalisation of its nearest competitor)[43]. However, it is worth noting there is no official bitcoin price. Bitcoin’s price is set by what people are willing to pay (supply and demand). CoinDesk is an example of a site specialising in Bitcoin prices.

There is undoubtedly interest in the currency, for example, Forbes ran an article detailing that there was significant movement on Wall Street (in 2015). The New York Stock Exchange launched a Bitcoin index (NYXBT), and the Bitcoin Investment Trust (GBTC) began trading[54].

Despite Bitcoin clearly taking off, the question is not just whether you should invest in Bitcoin, but also how to invest. There a 5 main ways of investing: buy and hold, daily trading, Bitcoin mining, selling mining equipment, and investing in Bitcoin-related companies.

Although it is a finite resource, the price of a bitcoin is extremely volatile. Investing more than you are willing to lose may be risky, with any negativity towards the currency (particularly in the media) likely to have an impact on the overall worth of bitcoins. A piece of advice would be to have a solid plan: be knowledgeable on how to store bitcoins (to avoid losing the currency), understand the market, and have a set goal to know when to 'cash out'.

From a venture capitalist point-of-view, investing in companies that have acknowledged Bitcoin as a reliable and tradeable currency is a high risk, high reward strategy. In one example, EVR (a small New York City Bar) gained a lot of attention for being the first NYC bar to accept Bitcoins back in 2013[55]. Bigger and more reputable companies that also accept bitcoins as payment (albeit through Bitcoin processing partners) include: Microsoft, Subway, Reddit, Tesla Motors and Virgin Galactic[56].

Payment Infrastructure

Although it is linked to the currency category, payment infrastructure is another Blockchain application. Cryptocurrencies such as Bitcoin can be bought, sold or traded.

BitPay – Founded in 2011, BitPay offers payment processing services for Bitcoin. As of 2017, it is one of the largest processing services for merchants, allowing small and large businesses to accept Bitcoin payments from customers anywhere on earth. Their partners including Microsoft, PayPal and Warner Bros Records. The total equity funding for the company reached $32.51 million in 3 rounds (from 17 investors, including Richard Branson)[57].

Abra – Although Abra has not reached the UK at the time of this report (early 2017), there is a lot of media coverage for the peer-to-peer digital cash start-up. The Silicon Valley-based company are beginning their global rollout, with its wallets supporting buying, selling and storing bitcoins as well as over 50 traditional currencies. According to the popular Bitcoin and Blockchain news site CoinDesk, $14 million has been raised so far in venture capital funding[58].

Other notable mentions include Santander, Bitbond, Coinbase and Circle. Santander were the first bank in the UK to use Blockchain technology for international payments[59]; Bitbond is a German peer-to-peer bitcoin loaning platform; Coinbase claim to be "the world's most popular way to buy and sell bitcoin and Ethereum"[60]; and finally, Circle are a payment app "on a mission to change the global economy"[61]. Circle allows peer-to-peer payments utilising traditional *fiat currencies*, and is backed by $136 million from investors including Goldman Sachs[62].

Smart Contracts

Smart contracts are programmable digitised contracts (entered on the Blockchain) that execute themselves automatically under the right circumstances. For example, bitcoins, property, shares (or anything of value) can be released by the contract under certain conditions, rather than having to trust a single central authority. Smart contracts are essentially computer programs that work on an 'If-Then' premise. Real examples include:

- Imogen Heap, a Grammy-award winning British musician, released her single "Tiny Human" using Blockchain-based technology. Buyers pay for her single on the website Ujomusic.com, using Ethereum's currency Ether, before the audio file is 'released' to the user[63].

- IBM believe Blockchain-supported IoT (*Internet of Things*) networks of energy grids will enable peer-to-peer transactions of energy. In one example, excess rooftop solar energy can be sold to other users who need the energy[64].

- Slock.it allow apartments to be rented via a smart contract; once the funds for the apartment have been received, then the apartment access code and digital receipt are released. If the access code is not given within the encoded time limit, the funds are reimbursed[65].

Ethereum – Ethereum is an open-source, non-profit, crowd-funded project. It is a decentralised platform that allows a network of peers to run smart contracts (that run exactly as programmed). The goal is to have smart contracts to run without any downtime, censorship, fraud, or middleman interference. These apps run on a custom built Blockchain allowing 'value' to be moved about[66]. It is thought these decentralised apps (coined 'DApps') will likely soon become 'consumer apps', with many currently in development. Decentralised applications (particularly ones that are also distributed) are promising due to their fault tolerance[67].

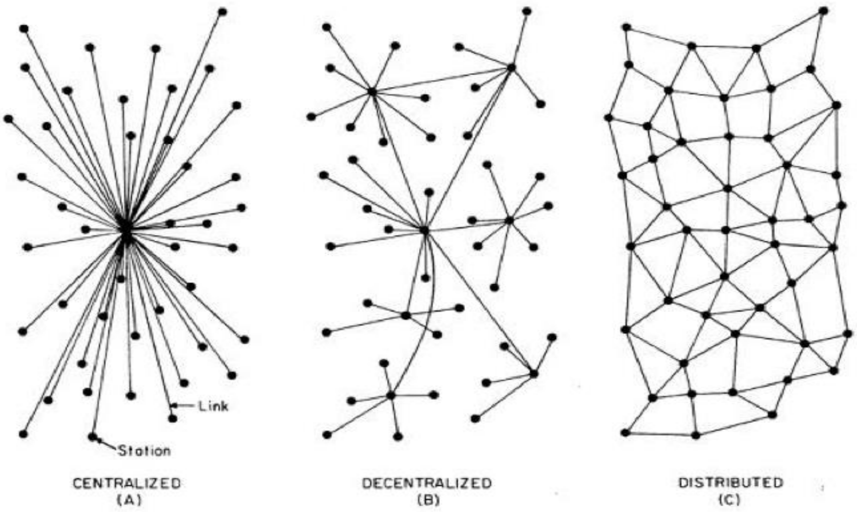


Figure 4: The three types of software applications[68]

Ether (ETH), technically a cryptocurrency, helps operate the distributed platform. It is the incentive that ensures developers create quality applications. It is needed to build, access and interact with smart contracts on the Blockchain. However, Ethereum's website prefers to refer to Ether as a 'fuel' or 'crypto-fuel'. The website states that Ether is intended to be treated as a token whose "purpose is to pay for computation" rather than to be used as a rival for bitcoins or other cryptocurrencies and assets. Ether is currently mined via the proof-of-work consensus (blocks are created every 12 seconds)[69].

Using an Ethereum wallet as a gateway to decentralised applications on the Ethereum Blockchain, users can hold Ether or other assets built on the platform. Ethereum wallets also allow contracts to be written and deployed. Smart contracts are normally wrote in the language Solidity (similar to JavaScript), but Serpent (a Python-like language) and LLL (based on Lisp) can be used[70].

Ethereum's co-founder Vitalik Buterin hopes the project will allow the formation of "decentralised autonomous organisations"— virtual companies that are essentially sets of rules running on Ethereum's Blockchain[2].

The DAO – Despite the global hype of Ethereum, Communications of the ACM cites the rise and fall of The DAO – a decentralised autonomous organisation based on Ethereum technology[71]. The DAO was an investor-directed venture capital fund that had an objective to provide a new decentralised business model for enterprises[72]. A series of smart contracts would raise funds for Ethereum-based projects, and these funds (ETH) would be distributed depending on the votes of the community[73]. The system was built with the purpose of being stateless, and not tied to any nation state[74].

Funding for The DAO project ended on May 28th 2016, with the project becoming the highest funded crowdfunding project in history. The total amount raised was ETH 11.5 million, equivalent to over $150 million (from 11,000 investors)[75]. According to the The New York Times, on May 27th 2016 (one day before funding closed), a paper was released by a group of computer scientists describing a number of security vulnerabilities with The DAO[76].

On June 17th 2016, The DAO was subject to a hack which removed approximately 3.6 million Ethers (equivalent to more than $50 million at the time)[75]. After much debate from the community, a controversial *hard fork* (see Figure 5) was implemented on July 20th 2016. This returned the Ether from an account owned by an unknown hacker to a new smart contract designed to let original token owners withdraw funds[77].

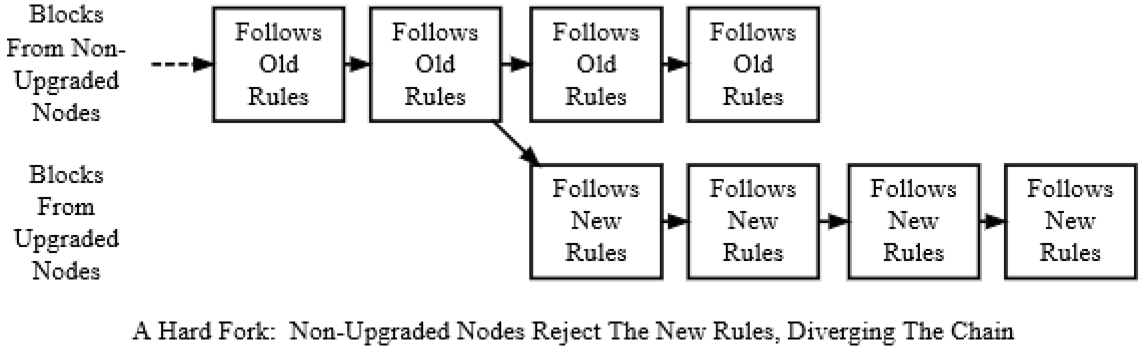


Figure 5: An illustration of a hard fork, in an attempt to reverse transactions [78]

Digital Assets

Blockchain technology can help with creating, issuing, transferring, trading and controlling digital assets (such as stocks and bonds). A lot of these assets are created using protocols on top of the Bitcoin Blockchain. Although there are too many companies to name in this space, some recent and notable examples include:

Chain Core – Technology company 'Chain' offer Chain Core, an infrastructure software that enables financial assets to be issued and traded on permissioned Blockchain networks. A federate consensus mechanism is used ensure the immediate confirmation of transactions. Chain Core is built specifically for financial services companies, with the company meeting security and governance demands by working with the likes of: Visa, Citigroup, NASDAQ and Fidelity[79].

Chain do not offer help with hosting, however Microsoft's Blockchain-as-a-Service allows users to run Chain Core on Azure (a cloud platform)[80]. After being founded in 2014, Chain went on to raise

$43.7 million over 3 rounds of funding. The last round of funding reached $30 million in the summer of 2015[81].

Hyperledger, IBM and Northern Trust – Northern Trust (NT) partnered with IBM in February 2017 to launch the first commercial deployment of Blockchain in the *private equity* market. Using a solution based on Hyperledger Fabric (an innovative Blockchain for managing assets, agreements and transactions[82]), NT are managing a private equity fund managed by Unigestion – a Swiss-based asset manager with over $20 billion worth of assets[83].

In a blog by IBM, the company describe how the Blockchain technology can help NT by eliminating much uncertainty, opacity and worry via Hyperledger Fabric's trust, transparency and security. Fund information is shared and accessed using cryptography (digital keys) and permissioning. Participants involved with the private equity ecosystem each have a unique ledger and node; thus creating "a single version of the truth". One particularly interesting aspect is that the Guernsey Financial Services Commission, the regulator, can access the ledger[84].

EquiChain – Described as a Blockchain for Capital Markets, EquiChain is a London-based FinTech start-up that wants to drive market efficiency. Furthermore, the company want to improve global investor access in *frontier markets*. Although the solution is still patent-pending (as of March 2017), EquiChain hope to enable "direct interaction and exchange of value between incumbent participants" but without needing multiple (inefficient) touchpoints. EquiChain have had one initial funding round in 2017, however details of the deal have yet to be shared[85].

Identify

Blockchain technology can offer a solution to many identity issues, by managing and tracking digital identities in an irrefutable, immutable, secure, and efficient manner. For example, in an attempt to avoid the use of password-based systems, Blockchain identity authentication means you only need to know the transaction was signed by the correct private key; and whoever has access to the private key is the owner. Blockchain start-up Onename is an example of this, creating a 'Passcard', a "digital key to your identity"[86].

Many other companies in this space want to work towards the idea of a self-sovereign identity. This means from birth you will a get a Blockchain digital identity – similar to an electronic passport but with a lot more data. As you progress through life, key information such as qualifications and credit scores will irreversibly be added to your identity. This identity could be used for many things: maybe to apply for universities, establish social media accounts, or to open a bank account.

ShoCard – ShoCard, founded in February 2015, have one vision: "Everyone will know, with certainty, who they are interacting with at any time, but with only the information they need for their purpose". The company aim to provide a scalable solution that allows individuals, businesses and the government to verify/exchange identity information in a private and secure manner[87].

Identity information that can be stored and exchanged includes biometrics such as fingerprints, voice, and facial recognition. The 'identity' is carried via the user's mobile phone, and they can determine which details are shared. A cryptographic hash image of the individual's ID or personal file is taken, and a digital signature of the hash is created and put on the Blockchain. The Blockchain is used as a public and immutable ledger that allows third parties (e.g. banks) to validate data[88].

ShoCard use cases include:

- Financial Institutions. For example, storing a user's credit score tied to their identity. By hashing the individual's score on the user's mobile phone, and having the bank digitally sign it with their private key, information can be placed on the Blockchain so associated institutions can see it.

- Airlines. Partnering with SITA, ShoCard have created an app that generates a travel token which will show all of the user's associated travel documents as well as biometrics. As users board flights, staff can retrieve the passport, visas, and biometrics without the necessary paperwork.

- Alternative to Passwords. Users can log into ShoCard enabled platforms without passwords. By linking their ShoCard ID with the website, any log-in attempts in the future will be without the need for remembering usernames and passwords. [89]

The company held 4 rounds of funding in 2015, raising $1.5 million in *seed* money[90].

<u>Verifiable Data</u>

Verifiable records of data, files, or business processes can be created via Blockchain technology. One example is in the land registry industry, using Blockchain to digitise real estate processes. Countries such as Georgia, Honduras and Sweden have all tested systems for registering and recording *land titles*[91].

The diamond industry has also seen implementations of Blockchain technology to track diamonds "from mine to market"; this includes tracking features such as diamond cut and quality. In a Communications of the ACM article, it is stated that Everledger, a company involved with diamond tracking, have also considered applying Blockchain to fine art, vintage cars, and wine[71]. Other projects/companies related to verifiable data include:

Tierion – A self-proclaimed pioneer of the verifiable data category, Tierion envisage a future where Blockchains can verify everything from patient records (in the health industry), to purchasing approvals of goods and services. Tierion claim to be the first system that could record millions of records in the Bitcoin Blockchain, generating a Blockchain receipt for each record. Tierion state that one use case of their service is insurance claims, with both parties involved given a verifiable record of the time and content of the initial claim[92].

In January 2017, Microsoft announced a partnership with Tierion, leveraging their technology to link data to a Blockchain, generating proof of data integrity[93]. Tierion raised $1 million in seed funding in April 2016[94].

Hyperledger, IBM and Maersk Line – Using Hyperledger Fabric, IBM and Maersk Line (the world's largest container shipping company) have ran a Blockchain pilot test. The purpose of the project is to create a verifiable supply chain that includes a network of freight forwarders, ocean carriers and ports. By the end of the year (2017), the goal is to get 10 million containers on the Blockchain (out of a total 70 million).

In an article posted by the International Business Times, it states IBM estimate $38 billion per year can be saved via Blockchain technology in the maritime industry. In a test case scenario, tracking avocados from Mombasa to Rotterdam, IBM estimated the cost of paperwork associated with the shipping container movement was $300 (15-20% of the entire operation costs). A vice-president at IBM (Ramesh Gopinath) said that later in the year there will be more clarity on exactly who would be running the permissioned network nodes[95].

In an IBM press release, the company stated the Blockchains immutable, secure and transparent network would allow end-to-end visibility across the supply chain. Network participants should be able view the real-time progress of goods, as well as the status of key documents. As a result, fraud and errors should be reduced, products should spend less time in transit, inventory management will improve, and waste costs should be minimised[96].

File Storage

Decentralised file sharing networks may allow users to avoid having to place trust in cloud storage providers such as Dropbox, Google Drive and Microsoft OneDrive. The main Blockchain-based projects competing in this area so far are: Storj, Siacoin and Filecoin.

Storj – Pronounced 'Storage', Storj is a cloud storage platform that aims to avoid being monitored/censored. It also aims to never have downtime. Storj encrypts user data, shreds the files into 'shards', before sending them out to a decentralised network of computers with easy to track basic metadata. Aspects of Blockchain technology such as: a transaction ledger, public/private keys, and cryptographic hash functions are a vital part of the system.

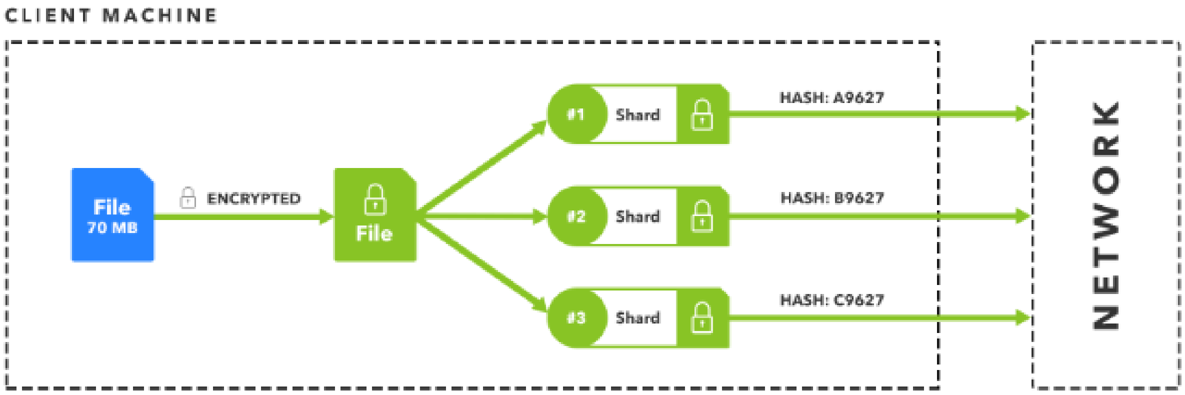


Figure 6: Visualising the Shard Process[97]

Storj uses a cryptocurrency: Storjcoin (SJCX). The network is comprised of nodes run by users of the service (across the globe), who rent out their unused computer hard drive space in return for the cryptocurrency. The term the company use to describe renting out extra hard drive space is "Drive Farming". No 'farmer' (similar to the concept of a miner) holds the entire user uploaded file – the files are also encrypted as extra safety. Any files that have been edited by the farmers will result in the node being identified as malicious (and therefore dropped). The network does not pay malicious/cheating nodes. Farmers compete to win files (the business of users), with users agreeing on competitive rates. Farmer's computers must be left on at all times, however the system works in a way whereby node failures do not mean access to a file is lost[98].

SJCX (the cryptocurrency) is a *counterparty asset* that uses the Bitcoin Blockchain for its transactions. The FAQ section of Storj's website says that although Bitcoin compatibility is likely in the future, reasons for using a new cryptocurrency are that bitcoins are too expensive and fluctuate too much (they don't want the profitability of nodes to be affected). Furthermore, payments can be locked in micropayment channels, and Storj do not want to 'hold up' bitcoins while still testing the protocol[98].

The company state on their website that they have investment opportunities available. Currently, Storj have raised $4.3 million, including $3 million seed funding in late February 2017 [99].

Voting

Currently, Estonia are the only country in the world that heavily rely on internet voting when it comes to legally-binding national elections. Approximately 25% of votes are cast online[100]. Security concerns are likely one of the reasons that almost no countries currently use online voting – something Blockchain could potentially solve.

Follow My Vote – By casting votes as transactions, the Blockchain can keep track of the total number of votes on a network. Transactions/Votes are public, meaning everyone can agree on the final outcome as they can count the votes themselves. Furthermore, due to the audit trail, everyone can verify that no votes were changed or removed, and that no illegitimate votes were added[101].

In an example scenario, wallets could be issued along with a single coin (one vote). Each voter will then cast their vote online using a unique user ID and their private key, along with a webcam and government issued ID (as a means to authenticate themselves)[102].

Follow My Vote's CEO notes that his concept is gaining interest in countries such as Norway, Iceland and Germany. Similar Blockchain voting technology was used by Denmark's Liberal Alliance (a political party) to vote for its internal elections[103]. According to CrunchBase, Follow My Vote raised $71.4 thousand in funding in 2016[104].

Other

Although this report has covered 8 main areas, there are possibilities of combining parts from each application group. For example, one Blockchain area worth briefly mentioning are Blockchain-based marketplaces (a mix between currency, smart contracts and payment infrastructure).

OpenBazaar – Taking home three of five awards during the 2016 Blockchain Awards (including 'Best New Start-up'), OpenBazaar is one of the most talked about Blockchain projects[105]. OpenBazaar intend to create a decentralised network for peer-to-peer commerce with no fees or restrictions. Instead of having a website, users download a program onto their computers to connect with others, allowing them to buy/sell goods using bitcoins. Once users agree to a price, the client creates a contract with both user's digital signatures and sends it to a third party user who moderates the transactions. Two out of three of the people involved must sign the contract for bitcoins to be released[106].

OpenBazaar raised an initial $1 million in seed capital, followed by $3 million of venture capital in late 2016[107].

Blockchain Application Profitability: SWOT Analysis

Below are the 8 SWOT analyses which look at how investable each Blockchain application area appears to be. After each SWOT analysis, a short summary contains a decision on whether it should be taken as a serious investment opportunity. The section concludes with a justification of the single area which will be looked at in-depth in the report's 'Venture Capitalist Summary' section.

Currency

Strengths
- Cryptocurrencies have a combined market capitalisation of over $24,000,000,000 as of late March 2017; Bitcoin makes up over $16,000,000,000 of this value[43]. - 34 cryptocurrencies have a market capitalisation of over $10 million[43]. - There have been over 200,000,000 Bitcoin transactions, and over 12,000,000 wallets created[108]. - The Bitcoin Volatility Index shows significant progress over the last 6 years, with the Index depicting a downwards trend (See Figure 8). - More than $270 million has been raised in *Initial Coin Offerings* (ICOs) since 2013, with over half of the top 20 crowdfunded projects being cryptocurrency related[109].
Weaknesses
- Most ICOs do not offer equity in start-ups, but instead offer cryptocurrency discount prior to the currency becoming available from exchanges. This means ICOs sit outside of legal frameworks according to a Harvard Business Review article[110]. - An Australian mining group, Bitcoin Group, have faced many problems with Australian regulators after announcing they wanted to conduct the first bitcoin-focused *Initial Public Offering* (IPO). After several blocked attempts the firm raised $5.9 million (2016) from investors out of a target of $20 million. The Australian Securities Exchange said more capital needed to be raised, and a new application would have to be submitted[111]. - Cryptocurrencies often have a lot of negativity surrounding them, particularly with Bitcoin often being associated with *the dark web*. - The irreversibility of transactions can currently cause problems, 'chargebacks' or disputed transactions are possible via banks and card providers in the regulated world. There are also no Anti-Money Laundering laws or Know Your Customer frameworks. - According to a white paper by MultiChain, the Bitcoin Blockchain has limitations when it comes to capacity. The Bitcoin Blockchain currently supports 300,000 transactions per day (determined by the maximum blocksize), whereas Visa's network in the US handles 150 million daily transactions[112]. With Bitcoin becoming too popular, network delays can happen and additional fees need to be paid to prioritise transactions.

Opportunities

- Initial Coin Offerings (ICOs) or ‘Token Sales’ are becoming more popular; a spin on the traditional venture capital business model. Price dynamics determined by supply and demand mean a value of the currency can be decided on by participants. Two cryptocurrencies (Monero and NEM) saw 2000% increases after ICOs in 2016[113]. ICO review companies also exist to provide independent and analytical research on Blockchain companies raising funds.

- The liquidity of cryptocurrencies can offer big returns for investors. Investors do not necessarily have to wait long periods of time, having the ability to pull profits quickly and easily by converting cryptocurrencies to fiat currency.

- The world is inevitably becoming more digital, with big name companies accepting Bitcoin and other cryptocurrencies as payment[56].

Threats

- Cryptocurrencies can have varying political and government opinions associated with them. For example, Bitcoin is deemed illegal in 4 countries[114]. Governments may not be able to officially take down cryptocurrencies, but interactions between cryptocurrencies and fiat currencies could become throttled to the extent where they’re regarded as useless.

- There’s arguably a lack of need for cryptocurrencies. Off the back of this, volatility of cryptocurrencies may render them worthless, there are no guarantees when it comes to return on investments.

- Scalability issues, particularly with Bitcoin, could affect the profitability of investing in cryptocurrencies (see weaknesses section). As of March 2017 there is a strong debate whether Bitcoin should hard fork to deal with more transactions; this debate saw a temporary fall (24%) in the cryptocurrency[115].

- There is always the possibility of mining attacks, and hacks. For example, the 51% attack has caused concerns for proof-of-work systems. The Mt Gox exchange is also an example, whereby a Bitcoin exchange (note, it wasn’t specifically the Blockchains fault) was allegedly hacked with almost half a billion dollars stolen/lost[116]. Similarly, once cryptocurrencies have been bought, they need to be securely stored. Trust needs to be put into wallet providers. Although ‘cold storage’ (for example paper-based QR codes) is possible, this can be risky to store significant amounts of value.

Figure 7: Currency SWOT Analysis

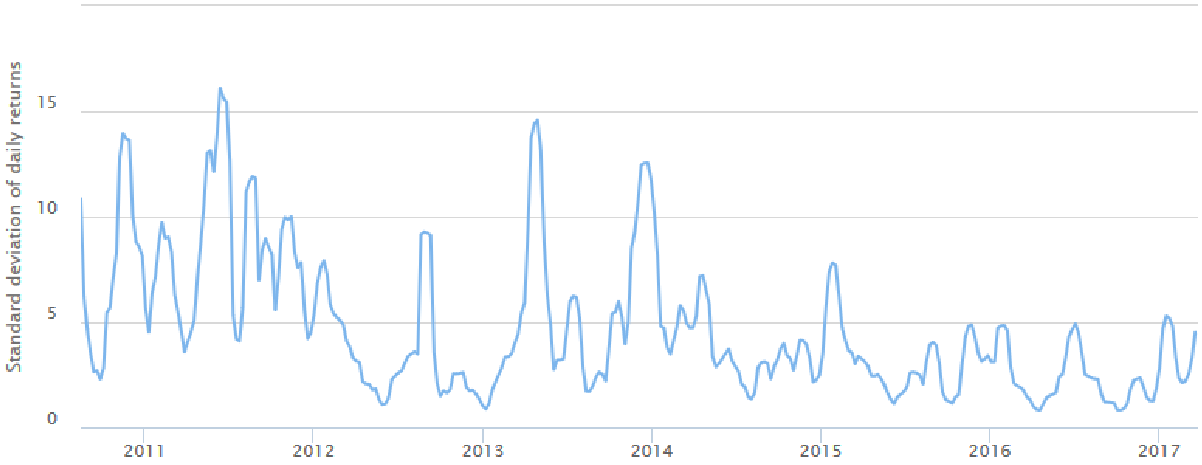


Figure 8: The Bitcoin Volatility Index from 2011 to early 2017[117]

Summary

In terms of venture capital, cryptocurrencies aren't the easiest thing to invest in; however ICOs and trading cryptocurrencies can certainly be a good way to make money. Despite the volatility and scalability issues associated with cryptocurrencies, the liquidity makes them attractive to buy and sell. Although cryptocurrencies won't replace traditional currencies any time soon, and it is unlikely that majority of our generation will have electronic wallets, cryptocurrencies are here to stay. That being said, a serious venture capitalist that wants to make big returns (and actually invest in a specific company) may want to look elsewhere.

<u>Payment Infrastructure</u>

Strengths
- Payment applications in the remittance space (especially cross-border) will likely take off due to the amount of money they can save. Taking Lloyds Bank as an example, their website suggests a payment of £9.50 is required to send funds internationally, and a minimum of £5 (or 0.25%) is charged for payments received[118]. Blockchain payment applications can potentially bring these figures to almost 0. - With cryptocurrencies on the rise, there needs to be exchanges to buy/sell value. Payment infrastructure applications are a necessity. - If managed correctly, bigger companies in the market should be able to prevail over competitors, whether it's by exchanging currencies at lower rates, or partnering with renowned businesses (e.g. BitPay and Microsoft). In a slightly different example, BitBond (a Bitcoin lender), make interest on loans. Even if the bitcoin value changes, interest on initial payments mean they won't lose money.
Weaknesses
- Business models for payment infrastructure companies are not always clear. Venture capital funded companies often use the initial funding to build their customer base before they figure out

how to actually monetise the market. This can lead to no return on investment, or a very long-term investment project. Circle, a peer-to-peer payment company, admitted in a blog that although they “fully intend to be revenue-generating” they must first have a basic product that will be free[119]. To speculate on approaches to earning revenue: advertising, partnering with large technology companies (for a fee), or adding transaction fees may be possible approaches. - Many Blockchain-related payment infrastructure companies that exist are heavily dependent on cryptocurrencies. Fiat currencies can mostly be considered stable, however if cryptocurrencies become worthless then the majority of the Blockchain payment infrastructure market will collapse. - Payment infrastructure applications are not easy or cheap to create. It will be a hard industry for new companies to get into the space, requiring vast amounts of funding in the first place. Applications also likely need to be ‘the first of a kind’ to gain traction. - The industry has low switching costs for individuals if they do not like a payment service. People can easily opt out and buy, sell, trade, or transfer funds elsewhere.
Opportunities
- Investors in this space may profit significantly if there’s an increase in cryptocurrency uptake. In 2016, 10 different cryptocurrencies had an increase in value of over 120%[113].
Threats
- Legal and regulatory aspects can threaten this industry. BitLendingClub (a bitcoin lending platform) shut down after citing regulatory hurdles as the reason behind its decision[120]. - As mentioned in the ‘Weaknesses’ section of this SWOT analysis, cryptocurrency volatility is a problem. For example, some applications want to let people trade fiat currencies and cryptocurrencies. Imagine you did not want to take part in foreign exchange or trade deals, but instead wanted to send a friend or family member a bitcoin. You wouldn’t be happy to see that the £900 bitcoin that you had in your account has now turned to £750 overnight. Combined with low exit costs, the payment application market may not last long. - As with most long-term investments, a return is not always guaranteed. BitPay may have raised upwards of $30 million[57], yet one article analysing the company’s financial figures suggests the salaries they pay are greater than the revenue they generate[121]. Eventually, investors are going to want to make money.

Figure 9: Payment Infrastructure SWOT Analysis

Summary

Although Blockchain-related payment infrastructure companies will exist as long as cryptocurrencies are relevant, it is hard to see many profitable business models in this industry. It appears too many companies are surviving on venture capital without necessarily giving their investors the returns they want to see. In other words, many start-ups favour the Get Big Fast (GBF) approach, but lack long-term sustainability. Any companies which do become profitable likely already exist, and do not require further funding. Regulatory hurdles is another reason to avoid investing in this area.

Smart Contracts

Strengths

- After cryptocurrencies, smart contracts are arguably the most talked about Blockchain application. Whether they're used as legal contracts or not, they have many advantages which include: autonomy (self-executing, no middlemen), trust and safety (encrypted on a distributed ledger), speed and cost-reduction (less paperwork and manual hours), and accuracy (less forms to be filled out, with the terms encoded). Smart contracts also integrate well with IoT, AI and machine learning – see the opportunities section.

- The Depository Trust & Clearing Corporation (DTCC) are partnering with IBM and venture capital funded start-up Axoni to move a significant part of their $1.5 quadrillion worth of *securities* to a distributed ledger. IBM's vice president of Blockchain solutions stated that when the project is fully implemented, "the entire life-cycle of a credit derivative will be captured as a smart contract or a suite of smart contracts"[122]. This shows significant progress in the smart contract industry. If computers control contracts, every day business will become more efficient.

Weaknesses

- Governments will need to make a judgement on how to regulate contracts, something which has yet to be done. For example, how can governments tax these smart contracts? How will courts intervene if contracts violate laws? If contracts exist on the Blockchain, who will have jurisdiction? If a party involved with the contract did not have the legal capacity to enter the smart contract (e.g. underage), what will happen? Will there need to be industry standards and protocols produced for this concept to work?

- Since smart contracts are made up of code, if the contract does not reflect what the parties understood their agreement to be (or if the outcome/effect of the code was represented to be different to what it actually was), then problems could occur.

- Profit-making methods for companies utilising smart contracts aren't always clear. Taking the music industry as an example, Ujo (which rides on Ethereum) is a platform for artists to use. The platform aims to let artists keep all revenue generated when songs are bought (and do not charge revenue-share fees). If sign-up fees aren't applicable, and the website does not become large enough for advertising money to be made, why would investors want to give their money to a company? Users may also be inclined to use existing services such as Spotify, YouTube, iTunes or illegal downloads instead.

- Using the music industry example again, smart contracts may be a huge amount of effort for every day consumers. To buy music on Ujo, it's an exhaustive 7 step process (including downloading a wallet, buying currency, and verifying personal information on the music platform). This will certainly be off-putting for non-technical users.

- For smart contracts to work, there needs to be someone with sufficient skills to code them in the first place.

- It will inevitably take time for smart contracts to become mainstream. The lack of education and experience in IT departments will be an initial concern. Furthermore, there will need to be education for regulators and legal teams.

Opportunities
- Smart contracts can help exchange anything of value including: money, property, jewellery, and shares. This makes them applicable in a number of industries, particularly the: healthcare, real estate, automobile, music, finance, and legal industries. This allows investors to invest in specific companies, industries, or smart contract providers. - Smart contracts have the potential to become commercially prominent. In an IBM/Samsung collaboration, a Samsung washing machine was configured to use smart contracts to "issue commands to a detergent retailer in order to receive new supplies". Funds can be released by the device with the retailer shipping the detergent[123]. - The future of legal contracts may involve a hybrid mode, involving a Blockchain that contracts are verified on, but with paper documents also filed. If this is the case, smart contracts can slowly be bought in with the hope of the smart contract concept taking over the industry in the future.
Threats
- Although the Blockchain may be secure, there's always the threat of bugs getting into the smart contract's code. With an immutable ledger, this may threaten the way smart contracts work. Similarly, hacking is also an issue. The notorious DAO attack is just one extreme example of this. - The idea of smart contracts may come across as very alien to every day individuals, especially those that are not computer literate. - A professor from Cornell University mentions that not all distributed applications featuring smart contracts may be beneficial. Cryptocurrency gambling applications are just one example[71]. - Going back to a previous example of a smart contract use case, the report mentioned the possibility of an apartment being rented out to an individual after receiving funds via a smart contract. A lawyer, Bill Marino, points out possible issues with this. For example, what happens if an incorrect apartment code is sent, or maybe the right code is sent yet the apartment is condemned before the rental date arrives[124]? The contract will perform no matter what, and there may be no legal team which can help the victim.

Figure 10: Smart Contract SWOT Analysis

Summary

There's no denying that smart contracts are an incredibly clever invention – they're also applicable to many scenarios. Despite this, a lack of clarity around the legality of smart contracts will hinder the applications success in the near future. The DAO hacking is also concerning, particularly the amount of money that was stolen, and how quickly and easily it took place. There's likely to be areas in which they do take off, especially in IoT use cases, but with Ethereum being both popular and open-source, it'll be hard for venture capitalists to make a profit on smart contract companies.

Digital Assets

Strengths
- The Digital Assets category has likely received the most amount of funding from investors. One example is the company Digital Asset Holdings, who received more than $60 million from the likes of IBM and Goldman Sachs[125]. - With many recent financial technology innovations happening on the front-end, Blockchain can help improve the back-end in post-trade processing. Many reputable companies are willing to trial the technology, such as NASDAQ. Their product, Linq, changes what is normally a paper-based system and makes the process “more efficient, more electronic and less prone to errors”[126]. - Blockchain technology can help financial companies to work with their regulators. In the NASDAQ example, a “special” node in the ledger network could be given to allow regulators to see what is happening with better transparency than we have today[126].
Weaknesses
- From an investor’s point of view, there is a lot of top-competition in the industry. R3 CEV, a Blockchain group featuring more than 70 financial firms, was supposedly the next big thing – focusing on using R3’s Corda ledger. In late 2016, it was reported several companies had begun to pull-out including Santander and Goldman Sachs, both who invest in rival company Digital Asset Holdings[51]. In February 2017 it was also announced that 30 companies (including J.P. Morgan, Microsoft, and Intel) have come together to form ‘Enterprise Ethereum Alliance’, a group that will focus on foreign exchange markets and settlements[127]. - As with a lot of Blockchain-based innovations, IT departments need training. The technology is still in its infancy, and most people are yet to fully understand what it is, or how it well help. - Most institutions are still making profit with centralised systems, and therefore it may be hard to see a viable reason to switch. The Australian Securities Exchange posted a paper in March 2017 after investing $17.4 million in Digital Asset Holdings. After months of consultation, the paper states that the implementation costs of transitioning to the new system make the “economics of change unattractive”, with brokers also wanting the Blockchain to do more[128]. Essentially, high stakes can make it hard to justify shifting and investing in Blockchain.
Opportunities
- From a financial market survey, global management consulting firm Bain & Company found approximately 80% of executives believe distributed ledger technology will transform their industry. A similar percentage expect their companies to adopt the technology by 2020[129]. IBM also found 30 banks out of 200 surveyed believe they will already have live platforms in 2017[130]. - Various studies estimate that Blockchains will save enormous amounts of money in the financial industry. According to Santander bank, by 2022 the technology could cut the industry’s bills by $20 billion a year[2].

- Global management consulting firm Oliver Wyman suggests expenditure in capital markets total $100-150 billion per year, with an extra $100 billion on top with servicing fees. They believe Blockchain technology can reduce the cost of providing securities services by 30 percent (or more)[131]. - Similarly, Accenture (consulting) published a report (January 2017) suggesting the technology could save banks $12 billion per year, cutting costs by more than 30% across the middle and back office[132]. Tackling settlement latency and avoiding the delays of days and weeks is just one example of how Blockchains can greatly reduce costs.
Threats
- The Blockchains unknown regulatory status will inevitability continue to cause concerns. In a Financial Times article (October 2016), a former CIO of UBS believes it will take a lot longer than expected for the technology to go mainstream. He notes that although regulators are embracing the technology’s potential, sandboxes are safe for playing around, but not in the real-world. Therefore, regulators will need to be sure large-scale platforms are 100 percent “bullet proof before they are released”[130]. There is no guarantee that Blockchains will withstand regulation pressures at all. - Innovative companies may relish the Blockchain, however investors could be put off by the resistance to change from organisations using bureaucratic systems. Not only does the idea have to be sold to the majority of important stakeholders, companies often aren’t set up in a way which allows them to deal with such a disruptive change to their organisation (leading to integration concerns). - As with any digital technology, cyber-attacks are a possibility. Even with the Blockchain touted as fully secure, the development of quantum computers may pose a threat in the future.

Figure 11: Digital Assets SWOT Analysis

Summary

Although it may take time for financial institutions to adopt Blockchain solutions in place of centralised systems, this will be an investable area. Companies that work with banks and regulators before releasing solutions will prosper, avoiding legal issues as a result. The amount of money Blockchain technology will save the industry will lead to institutions paying large amounts for complete solutions. The three biggest worries with digital assets are: regulatory complications, resistance to change, and extremely large companies like Goldman Sachs and JP Morgan investing in their own Blockchain solutions (rather than a start-up).

Identify

Strengths
- The self-proclaimed number 1 website for Global FinTech insights, Let’s Talk Payments, released an article in February 2017 listing 21 pioneering companies that are working in the digital identity space. These companies offer a range of services such as: anti-counterfeit solutions, document verification (with smart contracts), and biometric security suites[133]. With so many companies working in this space, it’s likely several will be profitable to invest in. - There is currently a demand in the market for Blockchain-based digital identities, with Blockstack Labs being just one successful example. By offering personal identities backed by a Blockchain, the company already has a user base of 50,000 identities[134].
Weaknesses
- In a 2016 GOV.UK blog, the author (a technical architect) urges caution about the technology as it stands, citing the European Identity & Cloud Conference 2016 which highlighted issues with Blockchain in the identity industry. The article also states that expectations are high, but little evidence points towards success, with red flags including security issues (such as lack of key management), and scalability problems. According to the consensus of ‘identity experts’, there is a resounding agreement that Blockchain won’t revolutionise digital identity[135]. Identity processes can be improved, but if there is nothing majorly broken with the current system, then it appears expensive and complicated Blockchain systems are not necessarily required. - Using an earlier example from the report – ShoCard hope to use digital identities in the travel industry. For example, boarding a flight using travel tokens associated with your identity. This would all take place through a mobile phone application. The weakness with this idea is that bringing mobile phones into the equation immediately puts the older generation, and poorer individuals at a disadvantage. There also needs to be a clear plan in place, for example, what if a mobile phone breaks on the way to the airport? How can individuals access their ‘travel tokens’, especially if they’re the only one with the associated keys? - In reality it seems unlikely the idea of a self-sovereign identity will take off anytime soon. There is no logical plan of how to put every individual’s identity (including tribes or the homeless) on a Blockchain. Although the concept may work (if agreed upon by governments) from birth, it would still need to take worldwide adoption to be truly effective.
Opportunities
- Although the GOV.UK digital identity blog believes Blockchain won’t revolutionise digital identity, there are opportunities to use the technology in the future. One example is building a chain of evidence surrounding refugee camps where there is a need to prove identity[135]. Having multiple applicable areas gives a broad range of investment options. - ID2020 is a partnership that wants to capture attributes and credentials that can uniquely identify a person. It is working towards a U.N. Sustainable Development Goal, “legal identity for all”. The goal is to help all people become part of society, with a system in place by 2020. The system aims to be technically and legally compliant for all ages, genders and nationalities[136]. If mainstream projects like this take off, it will be more likely that the idea of Blockchain digital

identities will become a reality.
Threats
- Governments need to buy into the majority of these systems to make them successful. With no government uptake, many digital identity projects will fail. There is also the question whether governments would pay money for these systems, and if not, then the Blockchain identity category is unattractive from an investor's point of view. - One big concern is what happens if a digital identity is compromised and fraudulent activity takes place. Not only is someone's whole life on this identity, but the irreversibility of the system could cause big problems. On a similar note to the irreversibility point, one article brings up the issue of events such as changing gender, or changing nationalities for security reasons. It is unlikely that these individuals will want to keep a record of their past that they intend to escape from[137]. - The lack of established standards may prevent widespread adoption. Similarly, aspects of the proposed ideas may not work. Biometrics (for example fingerprints) will likely not work well on an infant. Currently, the risk and challenges of implementation probably outweigh benefits. - Public keys are arguably not convenient for user IDs, and private keys aren't equivalents of passwords since they can't be easily remembered. The GSM Association (a trade body representing mobile operators) notes that storing associated identities is a real challenge[138]. Although mobile wallets may help, there will always be security worries. - Jeremy Grant of Chertoff Group (an advisory firm) believes there is a "wave of ignorance" surrounding Blockchain in the digital identity area. He believes people often don't know enough about the industry to speak intelligently on the subject. It's possible this can lead to investors putting their money into ideas which are actually flawed[139].

Figure 12: Identity SWOT Analysis

Summary

Self-sovereign identities are a fascinating concept, but without significant backing from governments around the world, the idea will never become a reality. Aspects of digital identity can be improved with Blockchain technology, however many experts are sceptical of the industry being completely reshaped. Therefore, Blockchain identity is an area to avoid investing in, at least until fundamental security issues have been solved.

Verifiable Data

Strengths
- There is a genuine need for problems to be solved in the verifiable data category, and Blockchain can most definitely be a part of the solution. This is applicable to: land ownership, healthcare, supply chain management, and high-value item tracking. The opportunities section outlines some recent industries which are likely to significantly (and positively) change in the near future.

- Although people may argue Blockchain technology will be slow to make an impact, it is already being implemented (particularly in this category). The International Business Times reported that in 2016, Estonia secured 1 million electronic health records by integrating Guardtime's Blockchain technology into Oracle's database engine, combating insider threat as a result[140]. Guardtime also had revenues of $25 million in 2015, showing that they can make positive changes to the world as well as being an investable company[141].

Weaknesses

- Investors may struggle to find a successful company to provide venture capital to that hasn't already been bought out or partnered with a well-known technology company. Companies like IBM (with their Hyperledger partnership) and SAP Ariba (with their Everledger partnership) have cornered a lot of the market off using their experience and expertise[142]. Although there will always be start-ups that can be invested in, the competition from the large technology company partnerships will be hard to compete against.

- Although Blockchain can solve many problems in this category, companies can be non-profit, and therefore are not viable investment opportunities. Bitland are an example of this, they help to record land ownership in Ghana, acting as a liaison to the government when disputes occur. However, they do not intend to make profit[143].

- Blockchain technology is not necessarily the perfect solution to solve verifiable data-related issues. For example, Google's AI-powered health subsidiary DeepMind Health will use Blockchain-like features for data auditing (e.g. an append-only ledger), but there will be differences in the technology. According to a DeepMind blog entry, the 'chain' aspect won't be used, and the system will be more centralised than a traditional Blockchain[144].

- There are questions about who will control nodes in certain industries. Although it is easy to say paperwork aspects can be replaced (saving money), there needs to be an understanding and appreciation of the technology. If someone forgets to record information on the Blockchain (e.g. in the maritime/shipping industry), there could be some serious implications.

Opportunities

- Although mentioned on the strengths section, verifiable data Blockchain solutions are applicable to almost any large industry which has a need for supply chain management or verifying ownership. There are a wide variety of companies, solutions and industries that can be invested in.

- In March 2017, Computer Weekly posted an article listing some Blockchain applications which are up-and-coming. Electron are building a system for recording UK energy metres, IBM and the US Food and Drug Administration are tracking personal health (with the help of IBM Watson), and Everledger are developing *RFID* tags for bottles of wine to track them on a Blockchain whilst ensuring they're tamper-free[145].

- There are great amounts of money that can be saved using Blockchain solutions. For example, trading in the oil industry has "high processing costs", and IBM, Trafigura (a commodities trading house) and Natixis (an investment bank) are currently building a Blockchain solution to solve this problem[146].

- Over in the e-commerce industry, it is thought half a trillion dollars of counterfeit/pirated goods are imported each year, with criminal organisations in Italy running a $16 billion business selling fake food and wine products. As a result, Alibaba have partnered with PwC (March 2017) to develop a “food trust framework” to improve its global supply chain[147]. - In one more money-saving example, medical fraud is estimated to have cost around $30 billion in the past 20 years. PA consulting believe the technology to revolutionise the healthcare industry is here, it is the business process integration that needs to be looked at[148]. Therefore, an early investment in the technology could be lucrative for venture capitalists.
Threats
- Although DeepMind aren’t specifically using a Blockchain solution, they acknowledge a technical challenge surrounding complex design questions that need resolving. Different users of the system will have different needs[144]. In the medical industry, doctors, surgeons, nurses, pharmacists, and patients will all require different data for different purposes. These design issues may halt the progress of a ‘complete’ medical chain. Design and access issues are relevant to other industries too. - Legacy systems present challenges in many industries. New Blockchain systems need to be integrated and any old systems need to be interoperable until the switch is fully made. Initial costs (as well as operating costs) may further deter organisations from making the switch. - As with most Blockchain applications (not just in the verifiable data category), resistance to change, political issues, and training are three of the major problems. Using Blockchain technology normally requires a major overhaul to any sizable organisation that already has other systems in place.

Figure 13: Verifiable Data SWOT Analysis

Summary

Since verifiable data can be applicable to a wide variety of industries including the: oil, energy, maritime, and healthcare industries, this makes the category particularly important when it comes to the future of Blockchain. Not only is there a broad range of problems to be solved in supply chain management, there are areas to save money/cut costs. There are also many start-ups which can be invested in, making this a good category to focus on. The main threats and weaknesses in this category are applicable to all Blockchain categories (e.g. training and resistance to change), and therefore this shouldn’t be highlighted as a significant problem.

File Storage

Strengths
- The idea that no one has a complete copy of your file (not even in an encrypted form) is strongly appealing to users. Investors have also already seen the potential in the idea, with the likes of Google Ventures contributing to $3 million in seed funding (for the company Storj)[149]. Storj are also open to more investments, potentially a great opportunity for venture capitalists looking to invest in the near future.

- Storj claim their decentralised peer-to-peer model can be faster (by 10 times), cheaper (50% less expensive) and more secure than traditional storage solutions. They also believe there will be a 99.99999% chance of no downtime[150]. If these statistics are true then users will start finding reasons to swap to this type of file storage.

- The Storj community currently has over 8,200 farmers (renting out hard drive space) and more than 15,000 API users[151]. The numbers clearly show that there is legitimate interest in Blockchain file storage.

Weaknesses

- It appears it'll be hard for Storj to start making profit in the short term. The company offer 1GB (per month) for $0.015, which is cheaper than the likes of Amazon S3 and Microsoft Azure ($0.023 and $0.030)[98]. With Storj being a new company with a new concept, this will not be a sensible investment for venture capitalists looking for short term investments.

- Using the Storj system to save files is not as easy as signing up and dragging files onto the web browser to save them. Users also cannot simply save a file on their device and hope for a backup. A terminal or command prompt must be used to upload files or download them from the system. See Figure 15. This will inevitably deter non-technical users

- Although users simply wanting storage can pay in fiat currency, a cryptocurrency (SJCX) is involved in other aspects (such as farming). To convert this into real money, users will have to go through exchanges, lengthening the process. The volatility of cryptocurrencies can possibly be a weakness too.

- The drive farming idea may sound like an attractive concept (renting out unused drives), however it may be more hassle than it's worth. Storj's FAQ section state that it would likely "require an upfront investment of a couple hundred dollars" to purchase equipment that can make a real profit[98]. For a user that has a spare 2 GB on their laptop, they'll likely bring in pennies over a year (based on renting at $0.015). User's also have to compete for the right to rent out their drives in the first place.

Opportunities

- Gartner believe that by 2020, the 'cloud shift' will affect more than $1 trillion in IT spending[152]. People are clearly interested in cloud technology, so an early investment in Blockchain cloud storage could give a big return on investment.

- Storj care about minimising costs, in late March the company suggested moving from counterparty assets to the Ethereum Blockchain, which will further help the community to grow. [153].

Threats

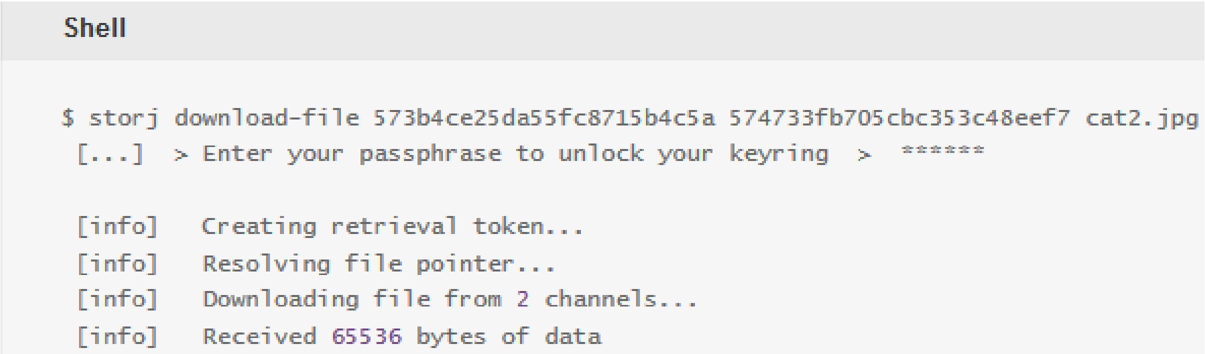
- Legal issues could possibly arise when it comes to storing illegal and indecent content using the system. Due to the encrypted nature of the system there is no way of checking exactly what is stored. If files stored turn into criminal activity, or if *data exfiltration* takes place then who is liable? Other legal issues could involve data becoming lost or unavailable; who will be liable in this situation?

- As always, there could be a slow uptake from widespread users. There are currently no significant studies which suggest users are not happy with using large corporations to back up their data (e.g. Microsoft, Google and Amazon). For example, Morgan Stanley predict that Microsoft cloud products will make up 30% of the industry's revenue by 2018[154]. Individual's that do not trust these companies may simply use physical storage instead of putting their trust in a start-up like Storj.

Figure 14: File Storage SWOT Analysis

Summary

Despite having speed and cost advantages, Blockchain file storage (as it currently is) does not appear to be an attractive investment. Interfaces for these companies are hard to use (see Figure 15), and the cryptocurrency (and wallet) aspects will deter non-technical users. Users attempting to make substantial amounts of money from spare storage will find it hard. Legal implications may also affect the industry at some stage. Finally, large technology companies such as Google, Amazon and Microsoft understand this market, and will likely continue to dominate. Google Ventures investing $3 million into Storj is likely a clever back-up plan just in case the idea does become a success. Venture capitalists should invest elsewhere.



Shell

```
$ storj download-file 573b4ce25da55fc8715b4c5a 574733fb705cbc353c48eef7 cat2.jpg
 [...]  > Enter your passphrase to unlock your keyring  >  ******

 [info]  Creating retrieval token...
 [info]  Resolving file pointer...
 [info]  Downloading file from 2 channels...
 [info]  Received 65536 bytes of data
```

Figure 15: Downloading files stored in a Storj 'bucket'[155]

Voting

Strengths
- Blockchains secure nature means once a transaction (vote) has taken place and is stored across thousands (potentially millions) of nodes, modifying it would theoretically require computational power that no single malicious user could bring together. In essence, no centralised system means tampering on a large-scale basis is not possible. - In paper-based voting systems, there is no easy way to detect a breach of security. For example, you can't see if extra votes have been cast, or if votes have been removed or tampered with. Blockchain technology's cryptographic and transparent nature is a huge advantage when it comes to voting.

- Follow My Vote, the most recognised Blockchain-related company in the voting industry, ensure elliptic curve cryptography technology is used. This helps keep the voting process secure, while protecting each voter's right to privacy. This should stop individuals being personally identified with individual votes [156].

- In Follow My Vote's current system, votes can be changed right up until the deadline – this stops the possibility of harassment and safeguards against pressured voting. Voting can take place from the comfort of your own home (unless stated otherwise by a government or authority controlling the vote system)[156].

Weaknesses

- Although electronic voting may help ensure whatever vote is entered is correctly recorded, this does not solve general problems with voting such as dictatorship or corruption. Countries can have corrupt/incompetent political systems which count votes in different ways to sway outcomes – even if votes are not tampered with once cast.

- Follow My Vote have only raised $71.4 thousand in funding. This figure is considerably low when you compare it to other Blockchain start-ups which have raised upwards of $100 million[104].

- Follow My Vote have open sourced their code, they simply wish to "reduce costs of our elections and free up taxpayer money"[101]. This makes the industry hard to invest in.

Opportunities

- Currently only Estonia heavily rely on internet voting in legally-binding national elections. Although this may be seen as a weakness, there is the potential for countries and parties to trial the technology. The Government-owned Australian Post, Russia's central securities depository (NSD), Abu Dhabi's Stock Exchange, Denmark's Liberal Alliance party, and Estonia's e-residency program have all trialled Blockchain voting systems[157].

- There are multiple white papers on the benefit of Blockchain electronic voting, and the idea is gaining traction[158][159].

- There are hybrid options available for *e-voting*, a full electronic process does not have to come into effect straight away. Dr Jeremy Clark, who specialises in cryptographic voting (Concordia University), suggests "an end-to-end verifiable voting system that uses a Blockchain as a public ledger but requires voters to show up and vote in" as an excellent first step[160].

- In a 2015 digital democracy report published by the House of Commons, it was stated "In the 2020 general election, secure online voting should be an option for all voters"[161]

Threats

- The biggest concern is probably the ease of convenience when it comes to voting. Voting needs to be accessible to everyone, not just technology literate individuals. The concept of public/private keys and wallets can be seen as complicated.

- Although the Blockchain is thought to be secure, we can assume there is still a possibility of a serious hack one day. Estonia's current system may not use Blockchain technology, but an independent report states that there are “staggering gaps” in operational security and the architecture of the system. The report also believes cyberattacks from the likes of Russia are possible[162].

- If there was a way for malicious users to link the wallet/transaction to an identity (affecting anonymity), this could cause huge concerns. There has yet to be concrete evidence that this Blockchain-style of voting will indeed work on a large-scale.

- Follow My Vote admit that although they have hired malware analysts, and can minimise threats by avoiding web-based platforms, there are no real safeguards against malware on a voter’s device. In addition, wallets can be lost or fall into malicious hands if the user is not careful[156].

Figure 16: Voting SWOT Analysis

Summary

Internet voting will inevitably be an option in the near future, and Blockchain technology can be a great aid in helping voting become secure. Even if a Blockchain is only used to verify results, and voters still need to turn up to a physical location (a hybrid model), the technology will have an impact. However, with Follow My Vote’s code being open-source, it will be hard for this area to be profitable. If governments or groups do wish to use Blockchain-based voting, it is likely they’ll partner with an already established technology company (e.g. IBM or Microsoft) to implement the system, rather than a start-up.

Final Decision

From the SWOTs undertaken, it is clear that there are vast amounts of uses for the technology, and many will have a significant and positive contribution to our future (such as internet voting). Despite this, it doesn’t make Blockchain solutions necessarily profitable. Companies often fail to offer convincing business models, such as start-ups that fall in the payment infrastructure category.

Overall, there are several ways to make profits off the technology. Offering consultancy services, or project/product managers are examples of utilising human services to make profits, however this is no use to venture capitalists looking to invest in specific Blockchain applications. Investors need to find companies which can offer bespoke or complete solutions (for a fee) which will help customers cut costs and save money. By charging on-going maintenance and support fees (potentially Blockchain-as-a-Service), these start-ups can have viable business models.

Although there will be many Blockchain applications (across all 8 categories) that will be profitable, the positives and negatives of each category need to be taken into account. Therefore, this report believes the 3 most profitable areas are:

1. Verifiable Data
2. Digital Assets
3. Smart Contracts

For a smart contract platform to be profitable, they need to offer solutions that can work in a commercial manner. As already stated, smart contracts work well with the development of IoT (for example the Samsung/IBM washing machine collaboration), and this could be an area where start-ups can prosper. A clever way for smart contract companies to make money, would be to dual-license their software. This would mean they offer a restricted free version, as well as an enterprise edition. On top of this, they could offer other professional services such as paid support to customers. With the help of investor-backed capital, the company could grow until it reaches a big enough customer-base where they can survive on advertising and their enterprise software income.

Digital asset companies will likely make their money by offering solutions to significant financial institutions, helping them advance the middle and back office processes (such as post-trade processing). In doing so, the Blockchain solution providers will save the financial organisations substantial amounts of money, allowing them to charge hefty amounts upfront.

Although digital assets and smart contracts are likely to be a significant part of our future, as the UK-based law firm Blake Morgan points out, Blockchain technology is being developed and implemented quicker than existing legal frameworks can be adapted[163]. Politicians may not want to restrict innovation by overregulating the technology, however eventually adaptations will need to be made to guarantee acts, regulations and laws are complied with. For now, venture capitalists should look elsewhere for investments to avoid legal obstructions. As a result the report will continue to look at Blockchain technology related to verifiable data.

Verifiable data-related Blockchain applications will of course come up against regulatory problems at some point, nonetheless, live systems are already being put into place in a variety of industries. Not only this, there are various business models that can be used, and a broad range of problems that can be solved in this category.

Admittedly companies like IBM are becoming dominant in this area, with Ginni Rometty (CEO) stating the company is currently working with over 400 clients on Blockchain initiatives (taken from the IBM annual letter, 2016)[164]. Therefore, now would be a good time for investors to put their money into businesses and technology (particularly start-ups) to reap maximum financial gains from investments before big companies buy out these profitable start-ups.

The next section further analyses 3 industries within the verifiable data category that venture capitalists should seriously consider investing in. These 3 industries were singled out as good investment opportunities after conducting further research.

Venture Capitalist Summary

With investor interest shifting from speculative to strategic, now is the time for venture capitalists to start picking out the next big companies and products. The verifiable data category should be particularly appealing in terms of financial gains. Below are 3 of the most prominent industries and applications that should be taken into account. The summary starts with 2 back-up investment areas (investment opportunities number 3 and 2) and finishes with the report's suggested area of investment (opportunity number 1):

Investment Opportunity #3 – Pharmaceutical Supply Chain Management

The Industry: Background

The global pharmaceutical industry is projected to be worth over $1 trillion in 5 years' time[165]. However, it is estimated that $75 to $200 billion of the global market is made up of counterfeit drugs. In low income countries, half of all the drugs distributed can be counterfeit, and often dangerous. INTERPOL seized more than $53 million medicines in 2016, and suspended around 5,000 websites selling these drugs[166].

How Blockchain Technology Will Help

Deloitte's Rubix Blockchain team identified 3 areas where the pharmaceutical supply chain will benefit from the technology: drug safety, drug channels, and public safety[167]. Below is an expanded explanation of each:

- Drug safety. Blockchain solutions can track how drugs are manufactured via the traceability of the technology. Faulty drugs can be detected if they do not contain correct ingredients, and if a supply chain breaks down (anywhere between manufacturer and consumer), the point of failure can be identified.

- Drug channels. Incompatible legacy systems can be a thing of the past, and the way drugs move through the supply chain can be tracked. Pharmacy retailers, third parties, and other members of the supply chain can use the single ledger of truth for their own benefit/research.

- Publics safety. End-consumer issues can be addressed, with the Blockchain possibly being able to identify prescription abuse. Recall management can also be dealt with more easily.

Research and Applications

A Deloitte study of 308 senior executives highlighted that the life science industries (which includes pharmaceutical science) have the most aggressive deployment plans out of other industries. Over a third of respondents said their company will have Blockchain solutions within 2017[168].

Several companies (including many start-ups) have working prototypes or solutions already in this space. Blockverify, iSolve and Chronicled are all working in the drug counterfeit area, engaging in pharmaceutical supply chain solutions.

In a blog post by the Principal of one of the above companies, iSolve, 4 main opportunities were highlighted. These opportunities include: inventory management, regulatory submission, data management for 3rd parties, and clinical trial management[169].

Risks and Challenges

The use of Blockchain in the pharmaceutical industry looks very promising, however it is only at the beginning of its journey. Oris Valiente, co-founder of Deloitte's Rubix, believes supply chain problems need to "be tackled in a number of steps"[167]. Not every problem in the supply chain industry can be solved straight away, so focusing on following drug products from their ingredients down to the patient's pillbox as a first step doesn't make sense.

Secondly, getting every manufacturer, and every 'member' of the supply chain to get on board with this new concept (in a widespread manner) will be a challenge. Several small pilots will need to be implemented to show the benefits to all participants, resulting in a gradual culture change. There's also no guarantee that all legacy systems are easily replaceable, so compatibility issues with other systems could be a problem early on.

Any US pharmaceutical company will also need to satisfy and adhere to the Drug Supply Chain Security Act (made by President Obama in 2013). This act relates to electronic systems tracing prescription drugs as they are distributed in the US[170]. There will inevitably be other protocols/acts which will also need to be complied with.

Case Study – IBM and Hejia

IBM have developed a partnership with Chinese supply chain management company Hejia. Using Hyperledger Fabric, the aim of the project is to focus on the financial aspects of the pharmaceutical supply chain.

In China, it can take 60 – 90 days for small and medium sized pharmaceutical companies to receive money after delivering drugs and medicines to hospitals. To make matters worse, these companies often find it hard to get traditional loans. With a Blockchain solution that eliminates inefficiencies and speeds up transactions, it may be possible for banks to fund these retailers within 48 hours.

As soon as July 2017, Hejia aim to expand the system to involve several pharmaceutical retailers, hospitals and banks. Although there hasn't been many details released about how exactly nodes will be managed, the company believe the transparent, encrypted and innovative nature of the Blockchain will help build a "business model that will contribute to China's economic development"[171].

Example Investments, Profitability and Justifications

In one investment example, Chronicled appear to be a very investable company. In the last 12 months the company have had an estimated revenue of $3.9 million[172]. They have also received $4.83 million in funding, with the latest round as recent as March 2017[173].

Chronicled offer a CryptoSeal solution, which involves Blockchain registered, tamper-evident adhesive strips that have a *Near Field Communication* (NFC) chip embedded. This chip is customisable and can be placed in all shipments of pharmaceuticals, sealing individual cartons/containers. The serial number data can then be tracked creating an unbroken chain[174].

Industry giants such as GlaxoKlineSmith, Pfizer, and Johnson & Johnson have all reportedly attempted to use RFID tags to trace drugs, however the cost in trialling these technologies outweighs benefits. Still having centralised computer systems can also cause problems[166]. With big companies needing solutions, a company like Chronicled can charge reasonable fees for their technology, infrastructures and APIs (making profit as a result).

Chronicled announced they are opting for a phased development, and will prove that at least one pharmaceutical manufacture can comply with regulations, meeting 2017 and 2023 requirements. The upcoming phases will likely involve participants from all aspects of the chain including hospitals, and manufacturers[170].

In the distant future, supply chain Blockchains may be able to automate the flow of goods, money, and documents, all whilst using smart contract technology. Investing at the start of the company's journey will likely see an extremely good return on investment for a venture capitalist.

Investment Opportunity #2 – Land Titling (Registering Property)

The Industry: Background

In many countries across the globe, land registries are badly kept, mismanaged or corrupt. Africa is an example of this, with the continent having a big social issue on their hands. With 54 countries, and 1.1 billion inhabitants speaking 3,000 languages, it's often hard to link property rights and land ownership to individuals. The land registry problem is prevalent in Ghana, with the African Business Review explaining how Ghanaians often having to paint "This land is NOT for sale" on the side of their homes. With The Ghana Land Commission having all property information on paper, this can lead to long delays in land registering processes, or even worse – corruption. It is possible for fraudsters to sell land they do not own, causing 'new owners' to have mortgage obligations on something they do not own[175].

The Economist also looked at an example of a land registry issue, this time in Honduras. Ms Izaguirre was evicted from her home after living inside it for 30 years. Ms Izaguirre even held documentation for the land. Despite this, Honduran police evicted the resident after claiming the country's Property Institute showed a different owner registered to the property. Before the situation was sorted, the house was demolished[2].

How Blockchain Technology Will Help

The implications of a Blockchain-based approach for registering properties, is that fraud can be prevented, and process efficiency can be increased. Although the system would still be centralised in terms of a governing body, costs and timings can greatly be reduced, and the system becomes fairer and more secure (disputes can easily be sorted out). This will be particularly helpful in developing countries.

Property transactions can be handled in a similar way to digital currency payments. The only difference, is that each 'coin' in a transaction has the same value, but with associated information added to it (the house or land). If all houses are on a ledger, it is easy to see the history of ownership, as well as the current owner. The actual deeds/documents can be hashed so that they do not have to be stored on the Blockchain. Property transactions could even incorporate smart contracts, which release money when a transaction goes through.

Blockchain technology won't just help in less developed countries though, with countries such as Sweden also trialling the technology (with the help of start-up ChromaWay). The CEO of ChromaWay believes using the technology in a country with high trust in public authorities will be "a great benefit" for the economy, and can influence other countries to follow in Sweden's footsteps[176].

Research and Applications

The World Bank estimates 70% of the global population lack access to land titling – making it difficult for the world's population to agree on property ownership[177]. Furthermore, Peruvian economist Hernando DeSoto, believes that globally there is "dead capital" (assets informally held and not legally recognised) totalling $20 trillion[178].

There are many small and large-scale projects which are attempting to solve these problems. For example, 2 of the 5,570 Brazilian *municipalities* are trialling Blockchain technology. The company behind the trial, Ubiquity, hope to embed land ownership information into the Bitcoin Blockchain. Information such as: property address, owner, and zone classification will be hashed using the *coloured coin protocol*[179].

In the Sweden/ChromaWay collaboration, consultancy firm Kairos Future estimate the Swedish taxpayer will save over €100 million. Land authorities and banks can see copies of records, with the system acting as a storage service for property transactions. However, a consultant from Kairos Future makes it clear there is no chance to lose land like you can bitcoins. The end goal is to have a fully digital system in place by 2019, with other public bodies (e.g. tax authorities) integrated[180].

Blockchain solutions for the UK land registry have also been researched. In a public sector research paper, Deloitte highlight that there were over 1.2 million residential property transactions completed in the 2014-15 financial year. With this amount of transactions comes a considerable amount of fraud. Current fraud prevention methods are thought to cost over £74 million, however, property fraud is notoriously difficult to identify[181]. A Blockchain solution may become a reality in the future as a way to reduce fraud prevention costs.

Risks and Challenges

Investing in land registry Blockchain solution providers also has its risks. Getting governments on board in the first place can be challenging. Even after this happens and a trial is in place, solid communication between companies and the government is needed.

A proof-of-concept test in Honduras failed in 2015, with the government and supporting-company Factom allegedly having a breakdown in communication. There were also rumours that the Honduras/Factom project failed due to political issues[182]. Other legal aspects may disrupt progress. For instance, ChromaWay can't currently fully digitise the land titling process in Sweden, as the law requires physical signatures on papers[176].

Venture capitalists also need to ensure they're investing in profitable Blockchain start-ups, not companies which are non-profit (such as Bitland, who are helping with land titling in Africa).

Case Study – Georgia and BitFury

BitFury believe a secure Blockchain property registry has the potential to make a "significant social and economic impact globally". By partnering with the Georgian government, the collaboration is currently the biggest (and most successful) land registry pilot so far.

The Republic of Georgia already have a good software infrastructure in place, and according to the World Bank they are in the top three countries for ease of property registration via their National Agency of Public Registry (NAPR) service. This may seem like a country that doesn't need the Blockchain for land titling, however having minimum obstacles to implement makes it the perfect pilot.

The NAPR can verify/sign documents containing essential citizen property information, with the timestamping service allowing these citizens to ensure their documents are legitimate without exposing confidential information (made possible by providing citizens with a hash).

The diagram below (Figure 17) shows the end-to-end process. Services and operations will still work in a similar way as before, with staff providing help through public service halls. The only difference is that software is used to help with the existing processes, and the Blockchain acts as a validator as well providing immutability and transparency[183].

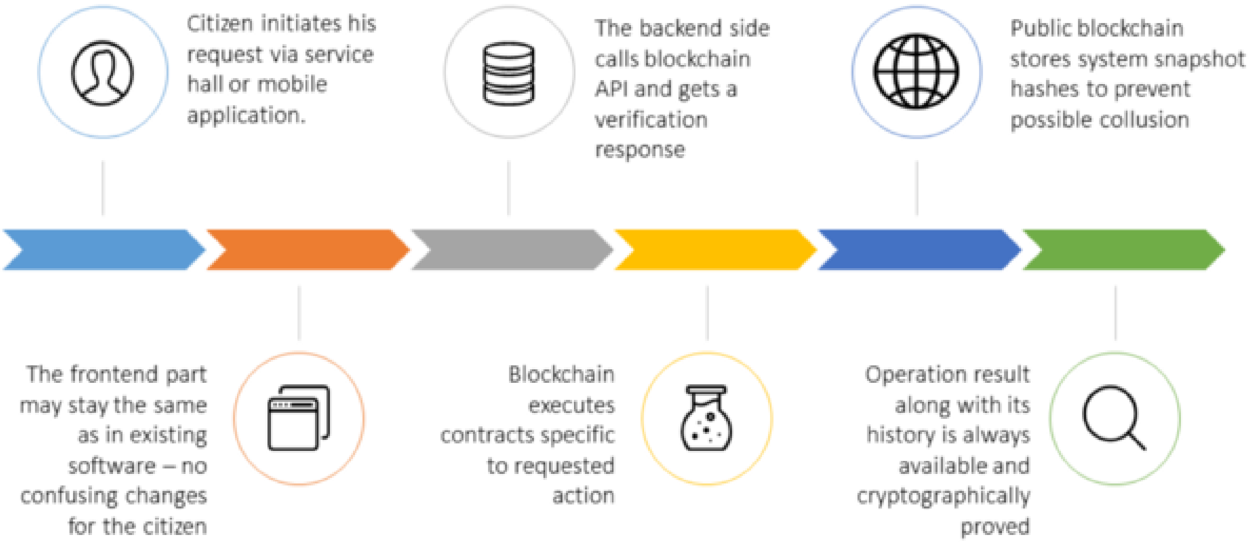

Citizen initiates his request via service hall or mobile application.
The frontend part may stay the same as in existing software – no confusing changes for the citizen
The backend side calls blockchain API and gets a verification response
Blockchain executes contracts specific to requested action
Public blockchain stores system snapshot hashes to prevent possible collusion
Operation result along with its history is always available and cryptographically proved

Figure 17: Blockchain Registry: How does it work?[183]

Example Investments, Profitability and Justifications

Although at first it may not be clear how this will be profitable for investors, Governments are willing to pay these start-ups substantial sums of money for their services. In a 2017 blog post, ChromaWay spoke about how their product, as well as their participation in conferences and associations (with renowned companies) makes them a very "profitable start-up"[184].

Using BitFury as an example, the company first became profitable through making Bitcoin mining equipment, before branching out as a full-service company. They have also partnered with EY[185]. The company received $30 million in venture capital as recent as January 2017 ($90 million in total) showing their potential. Furthermore, it is estimated that BitFury had a revenue of around $6 - 15 million in 2016[186].

According to Reuters, BitFury have since partnered with the Ukrainian government in what has been described as "by far the biggest government Blockchain deal ever", however the costs have yet to be revealed. The partnership will involve moving all of Ukraine's government's electronic data onto the Blockchain, initially focusing on real estate. It is very possible that this project will branch out further, using the Blockchain for state registers, public services, energy tracking, social security and more[187].

Therefore, not only can a land registry partnership with a government make money from the offset, it has the potential to create more business further down the line. Essentially, capturing the attention of a government can make an investor even richer.

With a variety of land registry projects taking off around the globe, now would be a good time for investors to get involved. There are many start-ups offering these services, and as BitFury demonstrated with the Ukraine deal, land registry projects may lead to even bigger opportunities.

Investment Opportunity #1 – Medical and Health Industry (Information Sharing)

The Industry: Background

Although every country will have a different method for storing patient medical data, the process will be vital nonetheless. In the US, Electronic Health Records (EHRs) are used to collect patient data, which can then be used by doctors (with the data being transferrable). However, the EHR system has a significant overhead with healthcare providers using complicated systems to ensure they stay compliant with the Health Insurance Portability and Accountability Act of 1996. Data formats are often not compatible with other providers, which can lead to duplicated results. Premier Healthcare Alliance believe a lack of *interoperability* can cost 150,000 lives, as well as $18.6 billion per year[188].

The current US Secretary of Health (Tom Price) is aware of this, and believes physicians and other important medical staff have been turned into "data entry clerks", which "detracts greatly from their ability to provide quality care"[189].

How Blockchain Technology Will Help

It is estimated that in the US, within one year (2015), over 112 million healthcare records were breached[190]. Another significant statistic is that medical fraud is thought to have cost around $30 billion in the last 20 years[148]. This gives the health industry a problem, not only are healthcare record systems often made up of disconnected databases, there's no guarantee they're accurate, or have not been tampered with.

Staying with the US EHR system as an example, Premier Healthcare Alliance believe that when they have successfully shared data over the last 4.5 years, 92,000 lives have been saved, as well as $9.1 billion[191].

Blockchain technology can continue to help with sharing data, as well as storing it securely and reducing unnecessary industry costs. Having one ledger of truth and hashing data onto the Blockchain means each healthcare provider (who will likely operate a node) can store a local copy of patient records, in a tamper-proof way. Each node will have an associated pair of keys, with patient's also holding keys. A patient's private key would be used to access relevant information (allowing patients to maintain control). If a patient's key is compromised, only this record will be affected, with all other patient records remaining secure.

Standardising data should solve incompatibility issues between software and records (across different healthcare providers), saving the industry money in the long-term. A sizable time-stamped chain also makes the system easy to audit.

This technology isn't only relevant to the US healthcare industry. In a NASDAQ article, Dr Stewart Southey (an NHS consultant) says the NHS "is a perfect example" of an area that Blockchain technology can help, and that many start-ups will get involved soon. Dr Southey believes within a year and half, UK health records will be a major area of change, with healthcare soon to be provided in an "efficient, cost-effective way". In the same interview, Dr Southey mentions fraud can be reduced, and administration can become primarily automated to reduce unnecessary expenditures[192].

Research and Applications

There have been many research papers, surveys, and reports surrounding medical Blockchains, as well as proof-of–concepts and trial runs. In one example, the US Department of Health and Human Services ran a sponsored challenge to encourage white papers to be created on Blockchain applications in the healthcare industry. There were 15 winning papers, with ideas ranging from medical insurance claims processing, to health information exchange[148].

IBM also created a report "Healthcare Rallies for Blockchains" which surveyed 200 healthcare executives. The survey identified the following positive statistics:

- 16% of executives say trial phases have been completed and that they will have a scaled commercial solution in 2017
- 90% of respondents will invest in Blockchain pilots by 2018
- 70% expect the healthcare areas which will benefit most are: clinical trial records, regulatory compliance, and medical health records[193]

Tierion, a pioneer in the verifiable data category, also undertook research. Although they believe the technology is in it's infancy, Blockchain has the potential to support new approaches to "health data interoperability, claims processing, medical records, physician-patient data sharing, and data security"[194]. Similar themes can be seen across the industry research conducted.

In terms of recording patient data in an interoperable manner, MedRec (developed by graduate research students) are using the Ethereum Blockchain to act as an interface for healthcare institutions. IBM have also partnered with the US Food and Drug Administration (FDA) to identify methods for accessing electronic medical records. The partnership will also look at clinical trials and health data taken from wearable devices (using IBM Watson in the process)[145].

Risks and Challenges

The IBM healthcare survey identified that executives believe the biggest barriers to adoption are the immature technology and insufficient skills in the industry (See Figure 18). In a survey by Deloitte, similar responses were gathered, with obstacles to adoption including a lack of technical standards for a still-immature technology, as well as regulatory uncertainties[148].

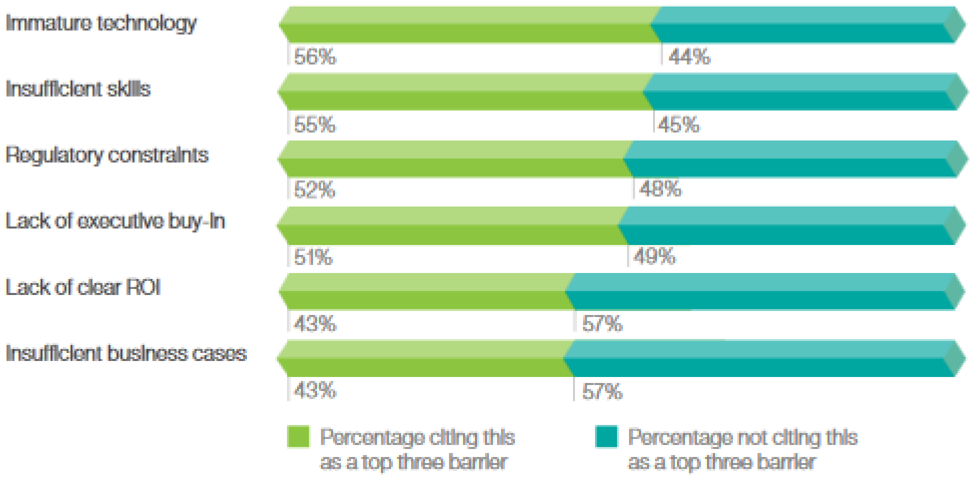


Figure 18: IBM Survey results to the question: "name the 3 biggest barriers to Blockchain adoption"[193]

Making significant changes to healthcare systems will also inevitably present challenges in terms of costs (both implementation and staff training), timings, and interoperability. However, any time a system is replaced in a business (Blockchain-related or not), these problems always need to be considered. Therefore, healthcare institutions will likely make these changes in the future, regardless of concerns.

Issues of scalability also need to be considered (something companies will have already thought about). For example, a consensus mechanism which does not require large amounts of power will need to be used. Dataconomy (a technology and business news site) note that although Blockchain is good for storing data fields (such as age and gender), it may not be good for storing expansive medical notes (such as MRI scans). This may lead to the data requiring alternative storage, with integration layers being built to interoperate with the Blockchain system[188].

Case Study – Gem Helth

Start-up Gem are in a partnership with Philips to build a patient-focused approach to medical record sharing. In a white paper collaboration between Gem and Ark Invest, an example scenario where their Blockchain infrastructure can be used has been identified. The 13-page paper has been summarised below:

Alice knocks her head while on a hiking trip away from home, and is taken to a local emergency doctor. The doctor believes it is only mild concussion but needs to see a full medical history before he can discharge her. Alice can add the doctor as a permissioned user (using Gem's infrastructure), and he can temporarily view Alice's EHR and append information (he can't delete any history).

Alice does this by looking up the doctor and adding him as a temporary viewer on a friendly user interface. If Alice was unconscious, a connected database could find a currently active provider that already has access to Alice's information – allowing them to send over information to the doctor.

The Blockchain used won't store massive amounts of data, but instead it will act as a baseline protocol that connects data sources. Alice can also give access to her wearable device if this is necessary/useful. The doctor's access would end at a predetermined window, and Alice's primary doctor and insurance payer gets a complete verifiable record of the event.

Data can be recorded and verified only through consensus of all parties (potentially similar to a round-robin approach). This means patients can also monitor the data entered into the EHR, approving, denying or sharing changes. This allows better privacy control and engagement, with the white paper referring to this as a "platform of trust".

All timestamped events that are added to the Blockchain are assigned a hash as a unique record identifier. If data inherent to the document changes, a different hash is produced by the algorithm. The contents of files are irreversible, although others can see the hash without the underlying information.

Blocks will still be used for consensus (appended to the Blockchain at a predictable rate), and the block will also receive its own hash. Each node on the network will be managed by a healthcare institution and if one goes down, as with all Blockchain systems, this won't affect the rest of the network. This guarantees integrity of records as well as ensuring that they're tamper-proof.

A key part of Gem's Blockchain system is a Blockchain operating system 'GemOS'. The Blockchain acts as a shared registry of events/information (in a chronological sequence), with GemOS providing layers of logic and privacy that leverage this information. It is the GemOS which allows information exchange amongst different parties, forming a network that connects all users (e.g. patients, healthcare providers, and insurance companies)[195]. Figure 19 shows how Gem's system works.

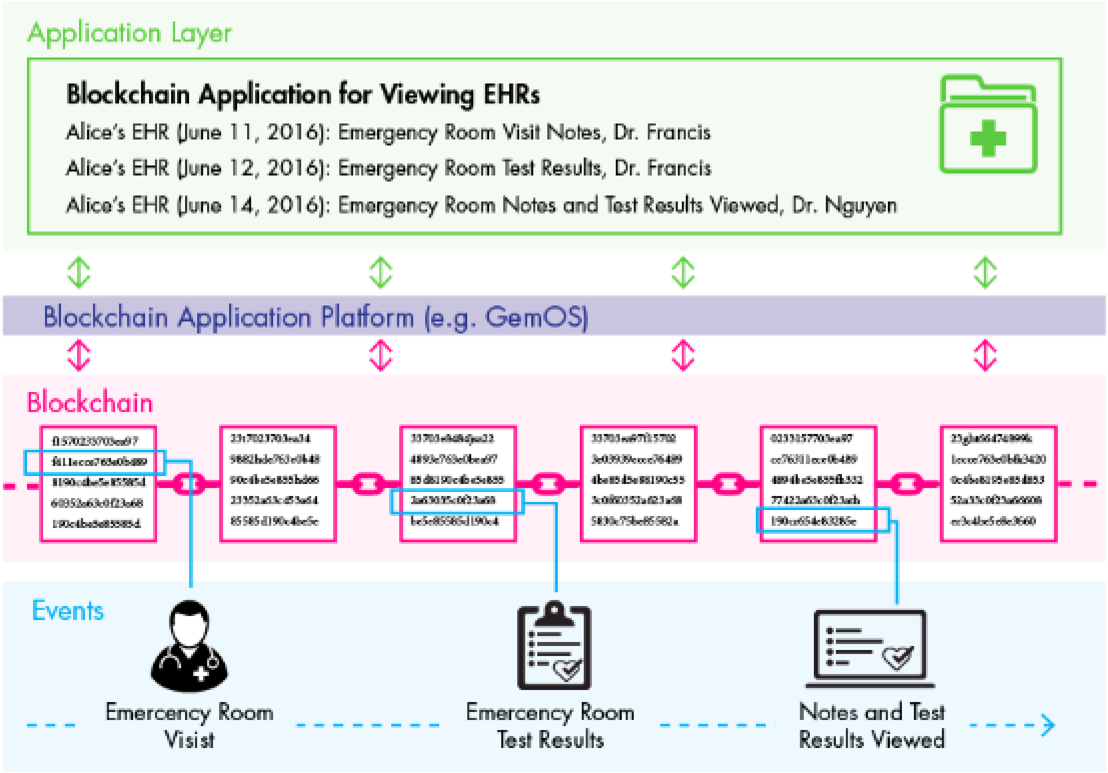

Application Layer
Blockchain Application for Viewing EHRs
Alice's EHR (June 11, 2016): Emergency Room Visit Notes, Dr. Francis
Alice's EHR (June 12, 2016): Emergency Room Test Results, Dr. Francis
Alice's EHR (June 14, 2016): Emergency Room Notes and Test Results Viewed, Dr. Nguyen
Blockchain Application Platform (e.g. GemOS)
Blockchain
Events
Emercency Room Visist
Emercency Room Test Results
Notes and Test Results Viewed

Figure 19: Gem's Blockchain and GemOS system, enabling healthcare interoperability[195]

Example Investments, Profitability and Justifications

Following on from the case study, Gem are a company that can make a large profit on their products. For the company to make revenue, they can either offer a pre-built complete solution (Software-as-a-Service), or build custom Blockchains for enterprise clients (either with a one off fee, or with added maintenance costs). Gem have already had 24 investors (totalling $12.5 million of funding), which shows they're open to investment opportunities[196].

With national healthcare expenditure in the US expected to rise 5.8% annually through to 2025, clients are likely to spend a lot of money for cutting-edge solutions (that can reduce costs)[197]. As identified earlier in the report, healthcare executives are already keen to make changes, with Deloitte highlighting 35% of healthcare representatives saying that their company will likely put Blockchains into production during 2017[168]. From a UK point-of-view, interest in Blockchain technology is also rising, with a government initiative (Connected Health Cities) putting forward £20 million to improve data flows across the North of England[198].

In a final example, one of the more advanced start-ups in this industry, Patientory, have a clever approach to becoming profitable. The company have a similar mission to others in this space – connect digital medical records without compromising privacy. The company allow healthcare providers to rent storage space (for health information), and offer smart contract functionality.

However, the new business model involves offering a token sale (ICO) for their token known as PTY. The start-up believe moving away from the fee-for-service model to the "current value-based model" will allow organisations to "link quality, value and effectiveness of medical interventions through a reputable compensation model"[199]. Company developers believe coordinating patient care through a Blockchain-based system will reduce costs "by a factor of a million"[200].

Whether the company end up being big-players in the market or not, having the first-of-a-kind idea, combining a cryptocurrency with a medical system, will likely see them make a huge amount of initial revenue from their May (2017) token sale. Investors should think about investing in companies that have these unique ideas early on, or failing that, they could even buy the cryptocurrency and make a profit following methods outlined in the report's 'Currency' section.

Future Work

The constantly evolving technology makes it challenging to pinpoint a guaranteed area of profitability for investors. Therefore, continual research would be required to further develop this project. Carrying out a research project of this size (as the project currently stands) is likely not a one-off task, and would require substantial dedication if it were to be continued.

The time constraints meant the project cold only focus on a few areas of research, yet the project deliverables still needed to change slightly: only 1 'category' was assessed rather than the intended 3. Within this one category, only the top 3 promising areas were also covered, which was a change from the original plan of 6.

The generic nature of the project, generally assessing the technology and its applications, often made the report become 'an ultimate guide to Blockchain' instead of an investment guide. To develop the project further, and to stay on the topic of analysing the commercial exploitation, the following steps could take place:

- Collect more quantitative figures, focusing on return on investments, revenues, profits, and company growth figures. The infancy of the technology made it hard to gather reliable and significant figures as of early 2017. The report currently often lacks solid figures to back up justifications.

- If time allows, reassess the other 7 Blockchain 'categories'. Whilst writing the report, daily news caused the report to change direction. For example, at one point cryptocurrencies looked like a clever investment opportunity with the volatility stabilising, but almost out of nowhere, the Bitcoin price temporarily crashed with debates over a possible fork in the chain.

- Time constraints meant only 3 applications from 1 category (verifiable data) were researched in detail. In the future, it would be sensible to continue research on verifiable data, looking at other supply chain uses (for example oil supply chains). The digital asset and smart contract categories should also be looked into. Although they weren't prioritised in this report due to the legal/regulatory uncertainties, they are still definitely promising areas.

- Conduct more interviews with industry experts and respected Blockchain advocates. Although these interviews may lead to opinionated responses, it can give insights which were previously unattainable from online articles. By the time the report was in a good enough position to conduct several interviews, the project was coming to a close. At this point it was hard to find individuals willing to answer questions.

- Keep an eye on promising research institutes that have recently been announced. One of these is the International Blockchain Research Institute, a partnership between the Canadian government, other government bodies, and private sector companies. Founding members include: IBM, Accenture, PepsiCo, NASDAQ, SAP and Digital Asset. Affiliate organisations also feature Hyperledger and the Enterprise Ethereum Alliance[201].

Alternatively, and probably the preferred approach, would be to tailor the project making it more problem-specific. The current format of the project attempts to generically assess every Blockchain opportunity. An approach that would be sensible, would be to narrow down the research to one specific industry.

From this report, I would suggest researching Blockchains in the medical and healthcare industries (an area which genuinely looks profitable). Resources and time spent on the project could then go into relevant studies, rather than carrying out generic research. Local healthcare establishments (such as doctor surgeries) could also be worked with to understand if there is a need for the technology.

Moreover, venture capitalists could be interviewed, gathering their current opinions and knowledge of the healthcare industry. This would allow research to be directed in a specific direction, with the outcome truly benefiting the investors as a result.

Conclusion

To conclude, it is important to review the 3 primary aims that this report set out to cover (as stated in the initial plan). These were:

1) Gain an understanding of how Blockchain technology works from a technical viewpoint

2) Highlight current Blockchain uses, as well as promising areas of interest for Blockchain

3) Produce a summary for a group of venture capitalists, highlighting potential Blockchain related areas that they can invest their money into (e.g. propose a 'solution' to their 'problem')

To understand the fundamentals of how the technology works, the Bitcoin Blockchain was analysed. This showed how distributed nodes and cryptographic techniques ensure transactions are secure. Furthermore, consensus mechanisms (such as proof-of-work and proof-of-stake) were briefly explored. The challenge with this, is that consensus mechanisms and Blockchain permissions vary depending on the Blockchain in question's purpose. However, I'm confident by achieving the deliverable "Complete the section 'How Blockchain Technology Works'", the reader can understand the basics of the technology from a technical viewpoint.

To cover aim 2, highlighting current uses, the report split Blockchain uses into 8 categories: currency, payment infrastructure, smart contracts, digital assets, identify, verifiable data, file storage, and voting. Examples of current/promising companies and uses were then covered in a subsection for each of the categories. From this part of the report, the audience learnt that there are many possible Blockchain applications. It was difficult to narrow down the most successful and exciting companies/applications in each category, and present them in an easy-to-read and insightful manner. However, the report clearly demonstrates that there are a wide range of opportunities out there.

Each of these 8 categories were then assessed via a SWOT analysis, which uncovered the top 3 promising areas of investment: verifiable data, digital assets, and smart contracts. The verifiable data category was chosen to be further assessed as it is applicable to a wide variety of industries, it can reduce costs by solving plenty of problems, and it can greatly improve process efficiency (e.g. in supply chains). From the SWOT analysis, the threats and weaknesses identified weren't unique to verifiable data and need to be considered regardless of the industry/application (such as training costs, resistance to change, and political pressures).

To achieve the final aim, and to gain an understanding of promising investment options, further research was conducted and laid out in the report using clear headings. The report believes that 3 of the best areas of investments are within the: pharmaceutical industry, the land registry industry, and the healthcare industry.

Although there has been major research undertaken regarding Blockchains, there are little resources that assist venture capitalists. This report admittedly does not give a definitive list of options out there, but it has achieved its intended goals/aims by suggesting investing in companies that are working in the 3 spaces identified above.

The healthcare industry appears to be the most profitable as there’s a demand for the technology from healthcare executives, live systems are already being put in place, healthcare record interoperability problems can be solved, lives can be saved, and costs can be reduced. Therefore, organisations and institutions are already willing to spend considerable amounts of money for a solution – and a Blockchain system can be the answer.

Additional work is still needed, particularly with regards to financial figures. This lacked from the report mainly because of time constraints, the difficulty in obtaining these figures, and the infancy of the technology. Having a limited network of Blockchain advocates at my disposal also meant the report largely focused on online articles, journals and white papers. Towards the end of the project, Blockchain authors, experts, and industry professionals were contacted via email, social media, online article comment sections, and public forums. Disappointingly, response rates were very low.

Nonetheless, all 7 of the original deliverables from the initial plan were delivered. The healthcare industry looks very promising, and it will most certainly use aspects of Blockchain technology in the near future. As one Blockchain website points out, investing in Blockchain technology today is like investing in the internet in 1994[202].

Reflection on Learning

Reflection on Methods Undertaken and Outcomes

As stated in the conclusion, I believe the intended outcomes for the report were achieved. Despite this, there are aspects which could have been improved. Admittedly, although I was learning about Blockchain myself for the first time, when completing the 'How Blockchain Technology Works' section, the research was often regurgitated from other sources.

The immaturity of the technology meant I was limited by a lack of sources other than online material. Having said that, e-books were available, and I should have reached out to interview experts in the field as soon as the project was underway. Alternatively, although surveys and questionnaires weren't an obvious choice (due to the widespread lack of understanding surrounding the topic), this may have added some more originality to the report. Unfortunately, I was slow to realise that interviews could really benefit me, something I would like to do if the project were to continue.

Looking back, the consensus section was also often blocks of text. Despite still completing the deliverable, it was a challenge to keep the report focused and concise when there are many consensus mechanisms used today. I probably spent too long trying to research and explain every type of consensus, rather than keeping it short, something venture capitalists would prefer to read. In the future, I will prioritise quality rather than quantity.

The project description given to me by my supervisor stated that I should highlight "any promising prospects for commercial exploitation". I believe the SWOT analysis was a good method for doing this, a method I learnt during the University module 'Managing The Modern Organisation'. The SWOT analysis approach allowed me to identify potential applications, but gave me the opportunity to realistically assess the threats and weaknesses associated. Looking back, the SWOT analysis taught me how to appreciate different viewpoints.

When completing one of the final deliverables, writing the venture capitalist summary, it was hard to give a solid justification as to why the healthcare industry was the best to invest in. Despite having information on how many healthcare executives want Blockchain solutions, and how much spending is increasing by in the industry, having no real investment figures made the justification extremely speculative. I often relied on crowdsourced websites such as Owler; the world's largest community-based business insights platform. It's arguable that this site, along with Crunchbase (which I also used for investment figures), may not be the perfect sources of information. The objective was completed nonetheless, and I believe I completed the work to the best of my ability.

Reflection on Module Learning Outcomes

The following section assesses my performance against the University learning outcomes for the module "CM3203 - One Semester Individual Project", as found on Cardiff University's 'Module Handbooks' page[203].

The module description mentions individuals should be able to practice “communication” and “management” skills, whilst executing the project “independently”. Reflecting on the project as a whole, I believe I demonstrated good communication by attending all of my fortnightly supervisor meetings. At certain point, the meetings were also weekly. If there were any questions I needed answering, I would leverage the University email system to contact my supervisor. I also believe my written communication skills within the report were of a high standard.

With regards to the management skills, I believe this project taught me the importance of breaking down work into smaller chunks even when facing a daunting task. Originally, the 15 week project looked like a challenge, but by carefully planning, organising, and completing the tasks within the time constraints, I delivered a completed report within the deadline.

Finally, on completion of the project the report’s author should be able to “exhibit a sound knowledge in the subject area related to the project”. Coming from a Business-oriented degree (Business Information Systems), it was a rewarding challenge to understand the technical aspects of an unfamiliar technology. Although I may not be an expert in the subject area, I believe the piece is well written, and I have certainly gained an interest in Blockchain technology.

Reflection on the Project as a Whole

From the beginning of the project I was aware of the amount of work required. I definitely put a great amount of effort into the project, almost treating it as a full-time job. Although I didn’t work with a traditional client or team, I still stuck to deadlines, and as a whole I managed my time well.

I stayed open-minded throughout the project, coping well with the extensive research periods. I never went into the project with a ‘solution’ (the best area to invest in) already in mind, and this allowed me to be fair throughout.

Unfortunately, after choosing the ‘profitability’ angle and focusing on this, I eventually realised it was a misconception that there is a lot of investment data available (as already mentioned). I was potentially naïve in thinking I could come up with a report which would become a vital guide to assist venture capitalists. On reflection, the reason that there is not ‘Investor Guides’ for Blockchain technologies, is because the required quantitative information just isn’t available. I still believe I produced a good summary, despite the justifications being rather speculative.

One aspect which was briefly touched on in the future work section, was the generic nature of the project. Rather than having a problem in a specific industry, I had a wide scope which I narrowed down by categorising applications and then carrying out the SWOTs. The timescale was still sufficient for me to produce a report, but at times it potentially lacked clear direction. This was also mentioned in the initial plan feedback which was received at Week 6 of the project. At this point in the project it was too late to start fresh, and I continued to work long hours to produce the best report that I could.

Overall, the last 3 – 4 months gave me a valuable experience of how to execute projects of this magnitude. As a result I believe I have become more independent. If I were to complete the project again, I believe I would narrow the scope – focusing on just one category, or one industry. Furthermore, although it would have been hard to arrange, it may have been beneficial to work alongside a real venture capitalist from the offset to give me guidance, and to act as a mentor.

Abbreviations

AI – Artificial Intelligence

API – Application Programming Interface

ECDSA – Elliptical Curve Digital Signature Algorithm

IBM – International Business Machines (Corporation)

ICO – Initial Coin Offering

IoT – Internet Of Things

IPO – Initial Public Offering

NFC – Near Field Communication

RFID – Radio Frequency Identification

SWOT – Strengths, Weaknesses, Opportunities and Threats

Glossary

Artificial Intelligence – The development of computers being able to perform tasks that normally require human intelligence

Application Programming Interface – An API is a set of commands, functions, tools, and protocols that specify how software components should interact

Coloured Coin Protocol – A way of adding metadata to bitcoins. Coins are ‘coloured’ because they represent a specific asset

Counterparty asset – A currency that has been created within the Bitcoin Blockchain. The currency is separate from the bitcoins themselves, however they exist inside bitcoin transactions

Cryptocurrency – A digital currency that uses cryptography for security.

Crypto-fuel – A token which is used to pay for computation. Although widely regarded as a cryptocurrency, it is not intended to be considered as a currency or asset

Data Exfiltration – A malicious activity which entails unauthorised copying, transfer or retrieval of data from a computer/server

Double-spending – Spending a coin in multiple transactions (often done by attempting more than one transaction at the same time)

Elliptical Curve Digital Signature Algorithm – A cryptographic algorithm that attempts to stop users spending coins that don’t belong to them

E-voting – A voting system that allows users to record votes electronically

Fiat Currencies – Currencies that are declared a legal tender by order of the government

FinTech – A portmanteau of financial technology – often used to describe companies that aim to make financial services more efficient via technology

Frontier markets – Countries that have less established stock markets, often at an early stage of economic/political development

Hard fork – A permanent and radical change to a protocol, requiring all users to upgrade to the latest version of the software. A hard fork often makes previously valid blocks invalid

Hashing Function – A function that is used to transform a value into a (usually) shorter fixed-length random string of characters that represents the original value. Hashing if frequently used to index/retrieve items in a database; it has speed advantages.

Initial Coin Offering – An unregulated method of raising funds for a new cryptocurrency. Early backers/investors often receive the new cryptocurrency as a result

Interoperability – The ability of computer systems and software to exchange information with one another. The term is often used in the healthcare industry to describe the communication and use of information from a different system

Internet Of Things – The development of everyday objects becoming interconnected via the internet, allowing these devices to send/receive data

Initial Public Offering – Offering a company stock on a public stock exchange for the first time. Often offered by smaller companies looking to expand via capital

Land titling – The act of individuals/families being given the formal property rights for land or housing they have informally owned

Municipalities – Districts with local governments

Near Field Communication – A set of communication protocols that allows objects/devices to establish communication wirelessly

Private equity – Capital that has not been noted on a public exchange. Often funds that have been invested directly into private companies.

Quorum – A minimum number of members that must be present for something to take place (and be valid)

Radio Frequency Identification – A technology that uses electromagnetic fields to identify and track tags attached to objects

Securities (in finance) – A tradeable financial asset, can be categorised into debt securities (e.g. banknotes, bonds), equity securities (e.g. stocks), or derivatives

Seed – Seed funding or seed capital is a form of investment in return for an equity stake in the company. Usually an early-stage type of funding used to cover initial operating expenses

The Dark Web – A part of the World Wide Web that can’t be accessed without a special browser, theoretically allowing users to operate anonymously. The Dark Web is often associated with illegal activities (e.g. drug buying)

References

[1] "Blurred lines: How FinTech is shaping Financial Services", *PwC*, 2016. [Online]. Available: https://www.pwc.ru/en/banking/publications/fintech-global-report-eng.pdf. [Accessed: 10- Feb- 2017]

[2] "The great chain of being sure about things", *Economist.com*, 2017. [Online]. Available: http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable. [Accessed: 12- Apr- 2017]

[3] "Blockchain reaction: Tech companies plan for critical mass", *EY*, 2016. [Online]. Available: http://www.ey.com/Publication/vwLUAssets/ey-blockchain-reaction-tech-companies-plan-for-critical-mass/$FILE/ey-blockchain-reaction.pdf. [Accessed: 21- Feb- 2017]

[4] C. Thompson, "How does the Blockchain Work (for Dummies) explained simply", *Medium*, 2016. [Online]. Available: https://medium.com/the-intrepid-review/how-does-the-blockchain-work-for-dummies-explained-simply-9f94d386e093#.90bob5c5u. [Accessed: 17- Feb- 2017]

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", *bitcoin.org*, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: 10- Feb- 2017]

[6] P. Smith, "Our legacy and a new logo", *Blockchain Blog*, 2017. [Online]. Available: https://blog.blockchain.com/2017/01/13/our-legacy-and-a-new-logo/. [Accessed: 13- Feb- 2017]

[7] J. Redman, "Richard Branson: Blockchain Is an 'Economic Revolution'", *Bitcoin News*, 2016. [Online]. Available: https://news.bitcoin.com/richard-branson-blockchain-revolution/. [Accessed: 13- Feb- 2017]

[8] J. Kennedy, "$1.4bn investment in blockchain start-ups in last 9 months", *Silicon Republic*, 2016. [Online]. Available: http://linkis.com/Ayjzj. [Accessed: 13- Feb- 2017]

[9] "Block”, *Bitcoin Wiki*, 2016. [Online]. Available: https://en.bitcoin.it/wiki/Block. [Accessed: 20- Feb- 2017]

[10] V. Buterin, "On Public and Private Blockchains", *Ethereum Blog*, 2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. [Accessed: 13- Feb- 2017]

[11] V. Buterin, "On Bitcoin Maximalism, and Currency and Platform Network Effects ", *Ethereum Blog*, 2014. [Online]. Available: https://blog.ethereum.org/2014/11/20/bitcoin-maximalism-currency-platform-network-effects/. [Accessed: 17- Feb- 2017]

[12] "What is a blockchain?", *Deloitte*, 2016. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-deloitte-what-is-blockchain-2016.pdf. [Accessed: 17- Feb- 2017]

[13] "How bitcoin works", *Bitcoin Wiki*, 2016. [Online]. Available: https://en.bitcoin.it/wiki/How_bitcoin_works. [Accessed: 17- Feb- 2017]

[14] M. D'Aliessi, "How Does the Blockchain Work?", *Medium*, 2016. [Online]. Available: https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae#.ejzkzkksr. [Accessed: 17- Feb- 2017]

[15] "How do bitcoin transactions work?", *CoinDesk*, 2015. [Online]. Available: http://www.coindesk.com/information/how-do-bitcoin-transactions-work/. [Accessed: 18- Feb- 2017]

[16] "Bitcoin Block Explorer", *Blockchain.info*, 2017. [Online]. Available: https://blockchain.info/. [Accessed: 18- Feb- 2017]

[17] "Transaction", *Bitcoin Wiki*, 2016. [Online]. Available: https://en.bitcoin.it/wiki/Transaction. [Accessed: 17- Feb- 2017]

[18] J. Monaco, *Two Bitcoin transactions with multiple outputs and multiple inputs. The total values of the inputs must be distributed to the outputs*. 2015 [Online]. Available: https://www.researchgate.net/figure/277248471_fig3_Figure-5-Two-Bitcoin-transactions-with-multiple-outputs-and-multiple-inputs-The-total. [Accessed: 17- Feb- 2017]

[19] V. Buterin, "Toward a 12-second Block Time", *Ethereum Blog*, 2014. [Online]. Available: https://blog.ethereum.org/2014/07/11/toward-a-12-second-block-time/. [Accessed: 18- Feb- 2017]

[20] "Blockcount", *Blockexplorer.com*, 2017. [Online]. Available: https://blockexplorer.com/api/status?q=getBlockCount. [Accessed: 18- Feb- 2017]

[21] "Block hashing algorithm", *Bitcoin Wiki*, 2015. [Online]. Available: https://en.bitcoin.it/wiki/Block_hashing_algorithm. [Accessed: 20- Feb- 2017]

[22] N. Acheson, "How does Proof of Work, um, work?", *Decentralize Today*, 2016. [Online]. Available: https://decentralize.today/how-does-proof-of-work-um-work-f44642b24215#.lnkdmjio1. [Accessed: 20- Feb- 2017]

[23] N. Popper, "How China Took Center Stage in Bitcoin’s Civil War", *The New York Times*, 2016. [Online]. Available: https://www.nytimes.com/2016/07/03/business/dealbook/bitcoin-china.html?_r=0. [Accessed: 20- Feb- 2017]

[24] M. Bastiaan, "Preventing the 51%-Attack: a Stochastic Analysis of Two Phase Proof of Work in Bitcoin". [Online]. Available: http://referaat.cs.utwente.nl/conference/22/paper/7473/preventing-the-51-attack-a-stochastic-analysis-of-two-phase-proof-of-work-in-bitcoin.pdf. [Accessed: 21- Feb- 2017]

[25] "Pooled mining", *Bitcoin Wiki*, 2017. [Online]. Available: https://en.bitcoin.it/wiki/Pooled_mining. [Accessed: 20- Feb- 2017]

[26] "Private Blockchains, Demystified", *Truthcoin.info*, 2016. [Online]. Available: http://www.truthcoin.info/blog/private-blockchains/. [Accessed: 23- Feb- 2017]

[27] S. Seibold and G. Samman, "Consensus - Immutable agreement for the Internet of value", *KPMG*, 2016. [Online]. Available: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf. [Accessed: 08- Mar- 2017]

[28] R. Chan, "Consensus Mechanisms used in Blockchain", *LinkedIn*, 2016. [Online]. Available: https://www.linkedin.com/pulse/consensus-mechanisms-used-blockchain-ronald-chan. [Accessed: 08- Mar- 2017]

[29] K. O'Dwyer and D. Malone, "Bitcoin Mining and its Energy Footprint", *National University of Ireland Maynooth*, 2014. [Online]. Available: https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf. [Accessed: 08- Mar- 2017]

[30] "Proof of Stake - Bitcoin Wiki", *Bitcoin Wiki*, 2015. [Online]. Available: https://en.bitcoin.it/wiki/Proof_of_Stake. [Accessed: 08- Mar- 2017]

[31] A. Castor, "A (Short) Guide to Blockchain Consensus Protocols", *CoinDesk*, 2017. [Online]. Available: http://www.coindesk.com/short-guide-blockchain-consensus-protocols/. [Accessed: 08- Mar- 2017]

[32] S. King and S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake", *Archive.org*, 2012. [Online]. Available: https://archive.org/stream/PPCoinPaper/ppcoin-paper_djvu.txt. [Accessed: 08- Mar- 2017]

[33] "[ANN] Nxt :: descendant of Bitcoin", *Bitcointalk.org*, 2013. [Online]. Available: http://bitcointalk.org/index.php?topic=303898 [Accessed: 08- Mar- 2017]

[34] T. van der Loop, "Introduction to Proof of Work or Stake in the Blockchain | Blog post", *Capgemini*, 2016. [Online]. Available: https://www.capgemini.com/blog/capping-it-off/2016/04/introduction-to-proof-of-work-or-stake-in-the-blockchain. [Accessed: 08- Mar- 2017]

[35] A. Poelstra, "Distributed Consensus from Proof of Stake is Impossible", 2014. [Online]. Available: https://download.wpsoftware.net/bitcoin/old-pos.pdf. [Accessed: 08- Mar- 2017]

[36] A. Hertig, "Where's Casper? Inside Ethereum's Race to Reinvent its Blockchain", *CoinDesk*, 2017. [Online]. Available: http://www.coindesk.com/ethereum-casper-proof-stake-rewrite-rules-blockchain/. [Accessed: 08- Mar- 2017]

[37] "Delegated Proof of Stake (DPoS) for Beginner's", *Cryptorials*, 2015. [Online]. Available: http://cryptorials.io/glossary/delegated-proof-of-stake/. [Accessed: 09- Mar- 2017]

[38] "Delegated Proof-of-Stake Consensus", *Bitshares.org*. [Online]. Available: https://bitshares.org/technology/delegated-proof-of-stake-consensus/. [Accessed: 09- Apr- 2017]

[39] A. Lewis, "In a nutshell: MultiChain", *Bits on blocks*, 2016. [Online]. Available: https://bitsonblocks.net/2016/03/07/in-a-nutshell-multichain-epicenter-bitcoin-interview-nov-2015/. [Accessed: 09- Mar- 2017]

[40] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance", *Massachusetts Institute of Technology*, 1999. [Online]. Available: http://www.pmg.lcs.mit.edu/papers/osdi99.pdf. [Accessed: 09- Mar- 2017]

[41] D. Cawrey, "How Consensus Algorithms Solve Issues with Bitcoin's Proof of Work", *CoinDesk*, 2014. [Online]. Available: http://www.coindesk.com/stellar-ripple-hyperledger-rivals-bitcoin-proof-work/. [Accessed: 10- Mar- 2017]

[42] D. Schwartz, N. Youngs and A. Britto, "The Ripple Protocol Consensus Algorithm", *Ripple Labs*, 2014. [Online]. Available: https://ripple.com/files/ripple_consensus_whitepaper.pdf. [Accessed: 14- Mar- 2017]

[43] "CryptoCurrency Market Capitalizations", *Coinmarketcap.com*, 2017. [Online]. Available: https://coinmarketcap.com/. [Accessed: 27- Mar- 2017]

[44] S. Higgins, "Jed McCaleb Talks Stellar's New Protocol for Consensus", *CoinDesk*, 2015. [Online]. Available: http://www.coindesk.com/stellar-founder-jed-mccaleb-new-protocol/. [Accessed: 10- Mar- 2017]

[45] C. Thompson, "How to know which Blockchain you should use", *Medium*, 2016. [Online]. Available: https://medium.com/the-intrepid-review/what-blockchain-should-we-use-6ba9cca8df22#.uhxdye5n7. [Accessed: 10- Mar- 2017]

[46] J. Kelly, "Exclusive: Blockchain platform developed by banks to be open-source", *Reuters UK*, 2016. [Online]. Available: http://uk.reuters.com/article/us-banks-blockchain-r3-exclusive-idUKKCN12K17E. [Accessed: 10- Mar- 2017]

[47] A. Begum, "R3’s Corda uncovered: It’s not blockchain", *Global Trade Review (GTR)*, 2017. [Online]. Available: http://www.gtreview.com/magazine/volume-15issue-3/r3s-corda-uncovered-not-blockchain/. [Accessed: 10- Mar- 2017]

[48] A. Morrison, "The argument for private blockchains", *PwC*, 2016. [Online]. Available: http://www.pwc.com/us/en/technology-forecast/blockchain/gideon-greenspan-interview.html. [Accessed: 21- Feb- 2017]

[49] J. O'Connell, "What Are the Use Cases for Private Blockchains? The Experts Weigh In", *Bitcoin Magazine*, 2016. [Online]. Available: https://bitcoinmagazine.com/articles/what-are-the-use-cases-for-private-blockchains-the-experts-weigh-in-1466440884/. [Accessed: 23- Feb- 2017]

[50] H. Malviya, "Can Blockchain be Hacked?", *Its Blockchain*, 2017. [Online]. Available: http://itsblockchain.com/2017/01/09/can-blockchain-be-hacked/. [Accessed: 24- Feb- 2017]

[51] G. Noto, "Santander Follows Goldman’s Lead, Drops Out of R3 Blockchain Group", *Bank Innovation*, 2016. [Online]. Available: http://bankinnovation.net/2016/11/update-santander-follows-goldmans-lead-drops-from-r3-blockchain-group/. [Accessed: 27- Feb- 2017]

[52] L. Parker, "Private versus Public Blockchains: Is there room for both to prevail?", *Magnr*, 2016. [Online]. Available: https://magnr.com/blog/technology/private-vs-public-blockchains-bitcoin/. [Accessed: 14- Mar- 2017]

[53] "Bitcoin Price Index - Real-time Bitcoin Price Charts", *CoinDesk*, 2017. [Online]. Available: http://www.coindesk.com/price/. [Accessed: 15- Mar- 2017]

[54] L. Shin, "Should You Invest In Bitcoin? 10 Arguments In Favor As Of December 2015", *Forbes*, 2015. [Online]. Available: https://www.forbes.com/sites/laurashin/2015/12/11/should-you-invest-in-bitcoin-10-arguments-in-favor-as-of-december-2015/#cefd9e62df28. [Accessed: 15- Mar- 2017]

[55] E. Fox, "The New York bar that takes Bitcoins", *CNNMoney*, 2013. [Online]. Available: http://money.cnn.com/2013/04/08/investing/bitcoin-bar-new-york-city/. [Accessed: 15- Mar- 2017]

[56] J. Chokun, "Who Accepts Bitcoins As Payment? List of Companies", *99bitcoins.com*, 2016. [Online]. Available: https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/. [Accessed: 27- Mar- 2017]

[57] "BitPay | crunchbase", *Crunchbase*, 2017. [Online]. Available: https://www.crunchbase.com/organization/bitpay#/entity. [Accessed: 16- Mar- 2017]

[58] J. Keane, "Is Bitcoin App Abra Finally Ready for Its Big Debut?", *CoinDesk*, 2017. [Online]. Available: http://www.coindesk.com/is-bitcoin-app-abra-finally-ready-for-its-big-debut/. [Accessed: 16- Mar- 2017]

[59] G. Prisco, "Santander Becomes First U.K. Bank to Introduce Blockchain Technology for International Payments", *Bitcoin Magazine*, 2016. [Online]. Available: https://bitcoinmagazine.com/articles/santander-becomes-first-u-k-bank-to-introduce-blockchain-technology-for-international-payments-1464795902/. [Accessed: 16- Mar- 2017]

[60] "Bitcoin & Ethereum Wallet", *Coinbase*, 2017. [Online]. Available: https://www.coinbase.com/?locale=en. [Accessed: 16- Mar- 2017]

[61] "Circle Pay App | About", *Circle*, 2017. [Online]. Available: https://www.circle.com/en-gb/about. [Accessed: 16- Mar- 2017]

[62] "Circle | crunchbase", *Crunchbase*, 2017. [Online]. Available: https://www.crunchbase.com/organization/circle-2#/entity. [Accessed: 16- Mar- 2017]

[63] J. Witt, "Live stream: Imogen Heap releases Tiny Human using blockchain technology", *The Guardian*, 2015. [Online]. Available: https://www.theguardian.com/membership/2015/oct/02/live-stream-imogen-heap-releases-tiny-human-using-blockchain-technology. [Accessed: 20- Mar- 2017]

[64] A. Gantait, J. Patra and A. Mukherjee, "Implementing blockchain for cognitive IoT applications, Part 1", *IBM*, 2017. [Online]. Available: https://www.ibm.com/developerworks/cloud/library/cl-blockchain-for-cognitive-iot-apps-trs/index.html. [Accessed: 20- Mar- 2017]

[65] "What Are Smart Contracts? A Beginner's Guide to Smart Contracts", *Blockgeeks*, 2016. [Online]. Available: https://blockgeeks.com/guides/smart-contracts/. [Accessed: 20- Mar- 2017]

[66] "Build unstoppable applications", *Ethereum*, 2016. [Online]. Available: https://www.ethereum.org/ [Accessed: 21- Mar- 2017]

[67] M. Gord, "How Decentralized Applications Could Bring the Blockchain to New Industries", *Bitcoin Magazine*, 2016. [Online]. Available: https://bitcoinmagazine.com/articles/how-decentralized-applications-could-bring-the-blockchain-to-new-industries-1455324259/. [Accessed: 21- Mar- 2017]

[68] S. Raval, *The three different types of software applications*. 2016 [Online]. Available: https://www.safaribooksonline.com/library/view/decentralized-applications/9781491924532/ch01.html. [Accessed: 21- Mar- 2017]

[69] "Ether – The Crypto-fuel For The Ethereum Network", *Ethereum*, 2016. [Online]. Available: https://www.ethereum.org/ether [Accessed: 21- Mar- 2017]

[70] "A 101 Noob Intro to Programming Smart Contracts on Ethereum", *ConsenSys*, 2015. [Online]. Available: http://consensys.github.io/developers/articles/101-noob-intro/. [Accessed: 21- Mar- 2017]

[71] S. Underwood, "Blockchain Beyond Bitcoin", *Communications Of The ACM*, 2016. [Online]. Available: https://cacm.acm.org/magazines/2016/11/209132-blockchain-beyond-bitcoin/fulltext. [Accessed: 21- Mar- 2017]

[72] A. Williams, "The DAO: a radical experiment that could be the future of decentralised governance", *Swinburne.edu.au*, 2016. [Online]. Available: http://www.swinburne.edu.au/news/latest-news/2016/05/the-radical-dao-experiment.php. [Accessed: 21- Mar- 2017]

[73] M. Castillo, "The Hard Fork: What's About to Happen to Ethereum and The DAO", *CoinDesk*, 2016. [Online]. Available: http://www.coindesk.com/hard-fork-ethereum-dao/. [Accessed: 21- Mar- 2017]

[74] "Crypto-investing: The DAO of accrue", *The Economist*, 2016. [Online]. Available: http://www.economist.com/news/finance-and-economics/21699159-new-automated-investment-fund-has-attracted-stacks-digital-money-dao. [Accessed: 21- Mar- 2017]

[75] N. Popper, "A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency", *The New York Times*, 2016. [Online]. Available: https://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html?_r=0. [Accessed: 21- Mar- 2017]

[76] N. Popper, "Paper Points Up Flaws in Venture Fund Based on Virtual Money", *The New York Times*, 2016. [Online]. Available: https://www.nytimes.com/2016/05/28/business/dealbook/paper-points-up-flaws-in-venture-fund-based-on-virtual-money.html. [Accessed: 21- Mar- 2017]

[77] M. Castillo, "Ethereum Executes Blockchain Hard Fork to Return DAO Funds", *CoinDesk*, 2016. [Online]. Available: http://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds/. [Accessed: 21- Mar- 2017]

[78] "Hard Fork", *Investopedia*. [Online]. Available: http://www.investopedia.com/terms/h/hard-fork.asp. [Accessed: 21- Mar- 2017]

[79] "An Introduction to Chain Core", *Chain*. [Online]. Available: https://chain.com/assets/brochure.pdf. [Accessed: 22- Mar- 2017]

[80] P. Rizzo, "In Milestone Release, Chain Open-Sources its Blockchain Tech", *CoinDesk*, 2017. [Online]. Available: http://www.coindesk.com/milestone-release-chain-protocol-developer-platform/. [Accessed: 22- Mar- 2017]

[81] "Chain | crunchbase", *Crunchbase*, 2017. [Online]. Available: https://www.crunchbase.com/organization/chain-2#/entity. [Accessed: 23- Mar- 2017]

[82] "Welcome to Fabric — hyperledger-fabricdocs master documentation", *Hyperledger*, 2017. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/. [Accessed: 23- Mar- 2017]

[83] "Northern Trust + IBM Use Blockchain for Private Equity Admin", *IBM*, 2017. [Online]. Available: http://www-03.ibm.com/press/us/en/pressrelease/51655.wss. [Accessed: 23- Mar- 2017]

[84] K. Pleiter, "Northern Trust Trusts Blockchain for Private Equity - THINK Blog", *IBM*, 2017. [Online]. Available: https://www.ibm.com/blogs/think/2017/02/39850/. [Accessed: 23- Mar- 2017]

[85] D. Ngo, "Blockchain for Capital Markets: EquiChain Unveils Working Prototype", *NASDAQ*, 2017. [Online]. Available: http://www.nasdaq.com/article/blockchain-for-capital-markets-equichain-unveils-working-prototype-cm747303. [Accessed: 23- Mar- 2017]

[86] J. Maxim, "Onename Launches Blockchain Identity Product Passcard", *Bitcoin Magazine*, 2015. [Online]. Available: https://bitcoinmagazine.com/articles/onename-launches-blockchain-identity-product-passcard-1431548450/. [Accessed: 27- Mar- 2017]

[87] "About ShoCard – ShoCard | Identity for a Mobile World", *Shocard*, 2017. [Online]. Available: https://shocard.com/about/. [Accessed: 25- Mar- 2017]

[88] "Identity Management on the Blockchain – ShoCard", *Shocard*, 2017. [Online]. Available: https://shocard.com/cpt_news/identity-management-on-the-blockchain/. [Accessed: 27- Mar- 2017]

[89] "ShoCard Solutions + Use Cases", *Shocard*, 2017. [Online]. Available: https://shocard.com/. [Accessed: 27- Mar- 2017]

[90] "ShoCard | crunchbase", *Crunchbase*, 2017. [Online]. Available: https://www.crunchbase.com/organization/shocard-inc#/entity. [Accessed: 27- Mar- 2017]

[91] P. Rizzo, "Sweden Tests Blockchain Smart Contracts for Land Registry", *CoinDesk*, 2016. [Online]. Available: http://www.coindesk.com/sweden-blockchain-smart-contracts-land-registry/. [Accessed: 23- Mar- 2017]

[92] "Tierion: Blockchain Proof Engine", *Tierion*, 2017. [Online]. Available: https://tierion.com/features#blockchain-receipt. [Accessed: 24- Mar- 2017]

[93] P. Rizzo, "Microsoft Details Collaboration With Blockchain Startup Tierion", *CoinDesk*, 2017. [Online]. Available: http://www.coindesk.com/microsoft-details-collaboration-blockchain-startup-tierion/. [Accessed: 23- Mar- 2017]

[94] "Tierion | crunchbase", *Crunchbase*, 2017. [Online]. Available: https://www.crunchbase.com/organization/tierion#/entity. [Accessed: 23- Mar- 2017]

[95] "Maersk and IBM want 10 million shipping containers on the global supply blockchain by year-end", *International Business Times UK*, 2017. [Online]. Available: http://www.ibtimes.co.uk/maersk-ibm-aim-get-10-million-shipping-containers-onto-global-supply-blockchain-by-year-end-1609778. [Accessed: 25- Mar- 2017]

[96] "Maersk and IBM Unveil Supply Chain Solution on Blockchain", *IBM*, 2017. [Online]. Available: https://www-03.ibm.com/press/us/en/pressrelease/51712.wss. [Accessed: 25- Mar- 2017]

[97] S. Wilkinson et al., "Storj A Peer-to-Peer Cloud Storage Network", *Storj*, 2016. [Online]. Available: https://storj.io/storj.pdf. [Accessed: 19- Mar- 2017]]

[98] "Storj - Decentralized Cloud Storage", *Storj*, 2017. [Online]. Available: https://storj.io/faq.html. [Accessed: 29- Mar- 2017]

[99] "Storj | crunchbase", *Crunchbase*, 2017. [Online]. Available: https://www.crunchbase.com/organization/storj#/entity. [Accessed: 19- Mar- 2017

[100] "Independent Report on E-voting in Estonia", *Estoniaevoting.org*, 2014. [Online]. Available: https://estoniaevoting.org/. [Accessed: 16- Mar- 2017]

[101] "Blockchain Technology in Online Voting", *Follow My Vote*. [Online]. Available: https://followmyvote.com/online-voting-technology/blockchain-technology/. [Accessed: 28- Mar- 2017]

[102] B. Dickson, "Blockchain tech could fight voter fraud — and these countries are testing it", *VentureBeat*, 2016. [Online]. Available: http://venturebeat.com/2016/10/22/blockchain-tech-could-fight-voter-fraud-and-these-countries-are-testing-it/. [Accessed: 16- Mar- 2017]

[103] M. Daniel, "Blockchain Technology: The Key to Secure Online Voting", *Bitcoin Magazine*, 2015. [Online]. Available: https://bitcoinmagazine.com/articles/blockchain-technology-key-secure-online-voting-1435443899/. [Accessed: 16- Mar- 2017]

[104] "Follow My Vote | crunchbase", *Crunchbase*, 2017. [Online]. Available: https://www.crunchbase.com/organization/follow-my-vote-inc#/entity. [Accessed: 28- Mar- 2017]

[105] R. Kastelein, "Decentralized Marketplace OpenBazaar Integrates ShapeShift, Allowing Payment with Any Digital Asset", *Blockchain News*, 2016. [Online]. Available: http://www.the-blockchain.com/2016/12/20/decentralized-marketplace-openbazaar-integrates-shapeshift-allowing-payment-with-any-digital-asset/. [Accessed: 29- Mar- 2017]

[106] S. Patterson, "What is OpenBazaar?", *OpenBazaar*, 2017. [Online]. Available: https://openbazaar.zendesk.com/hc/en-us/articles/208020193-What-is-OpenBazaar-. [Accessed: 29- Mar- 2017]

[107] "OpenBazaar | crunchbase", *Crunchbase*, 2017. [Online]. Available: https://www.crunchbase.com/organization/openbazaar#/entity. [Accessed: 29- Mar- 2017]

[108] "Blockchain – Total Number of Transactions", *Blockchain*, 2017. [Online]. Available: https://blockchain.info/charts/n-transactions-total 27. [Accessed: 27- Apr- 2017]

[109] M. Chwierut, "ICOs and crowdsales: Over $270 million raised and counting", *Smith + Crown*, 2016. [Online]. Available: https://www.smithandcrown.com/icos-crowdsale-history/. [Accessed: 27- Mar- 2017]

[110] R. Kastelein, "What Initial Coin Offerings Are, and Why VC Firms Care", *Harvard Business Review*, 2017. [Online]. Available: https://hbr.org/2017/03/what-initial-coin-offerings-are-and-why-vc-firms-care. [Accessed: 27- Mar- 2017]

[111] S. Higgins, "Australian Bitcoin Miner Withdraws Bid for Public IPO", *CoinDesk*, 2016. [Online]. Available: http://www.coindesk.com/australian-bitcoin-miner-withdraws-bid-for-public-ipo/. [Accessed: 27- Mar- 2017]

[112] G. Greenspan, "MultiChain Private Blockchain — White Paper", *MultiChain*, 2015. [Online]. Available: http://www.multichain.com/download/MultiChain-White-Paper.pdf. [Accessed: 27- Mar- 2017]

[113] D. Muszyński, "2016's top cryptocurrencies", *BitHub*, 2017. [Online]. Available: http://bithub.pl/2016s-top-cryptocurrencies/. [Accessed: 31- Mar- 2017]

[114] "Global Bitcoin Political Support & Public Opinion", *Coin Dance*, 2017. [Online]. Available: https://coin.dance/poli. [Accessed: 27- Mar- 2017]

[115] J. Wong, "Bitcoin's civil war threatens to blow up the cryptocurrency itself", *Quartz*, 2017. [Online]. Available: https://qz.com/937312/bitcoin-btc-is-tearing-itself-apart-again-and-its-price-is-yo-yoing/. [Accessed: 27- Mar- 2017]

[116] "After Mt Gox - Bitconned", *The Economist*, 2014. [Online]. Available: http://www.economist.com/blogs/schumpeter/2014/03/after-mt-gox. [Accessed: 27- Mar- 2017]

[117] E. Dourado, "The Bitcoin Volatility Index", *Btcvol.info*, 2017. [Online]. Available: https://btcvol.info/. [Accessed: 27- Mar- 2017]

[118] "Lloyds Bank - Online International Payments & Overseas Money Transfers", *Lloyds Bank*, 2017. [Online]. Available: https://www.lloydsbank.com/online-banking/benefits-online-banking/international-payments.asp. [Accessed: 31- Mar- 2017]

[119] P. Neville, "Circle Debut Questions", *The Circle Blog*, 2014. [Online]. Available: https://blog.circle.com/2014/05/21/circle-debut-questions/. [Accessed: 31- Mar- 2017]

[120] S. Higgins, "Bitcoin Loan Platform BitLendingClub to Shut Down", *CoinDesk*, 2016. [Online]. Available: http://www.coindesk.com/bitcoin-loan-bitlendingclub-shutdown/. [Accessed: 31- Mar- 2017]

[121] T. Swanson, "A gift card economy: breaking down BitPay's numbers", *Great Wall of Numbers*, 2015. [Online]. Available: http://www.ofnumbers.com/2015/04/17/a-gift-card-economy-breaking-down-bitpays-numbers/. [Accessed: 31- Mar- 2017]

[122] M. Castillo, "$11 Trillion Bet: DTCC to Process Derivatives With Blockchain Tech", *CoinDesk*, 2017. [Online]. Available: http://www.coindesk.com/11-trillion-bet-dtcc-clear-derivatives-blockchain-tech/. [Accessed: 01- Apr- 2017]

[123] S. Higgins, "IBM Reveals Proof of Concept for Blockchain-Powered Internet of Things", *CoinDesk*, 2015. [Online]. Available: http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things/. [Accessed: 01- Apr- 2017]

[124] B. Marino, "Smart Contracts: The Next Big Blockchain Application", *Cornell Tech*, 2015. [Online]. Available: https://tech.cornell.edu/news/smart-contracts-the-next-big-blockchain-application. [Accessed: 01- Apr- 2017]

[125] "Goldman Sachs And IBM Join 13 Investors In Digital Asset, Bringing Funding Round To More Than $60 Million", *Digital Asset*, 2016. [Online]. Available: https://digitalasset.com/press/goldman-sachs-and-ibm-invest-in-digital-asset.html. [Accessed: 02- Apr- 2017]

[126] L. Shin, "Why Nasdaq Is Even More Optimistic About Blockchain Than It Was 3 Years Ago", *Forbes*, 2017. [Online]. Available: https://www.forbes.com/sites/laurashin/2017/02/21/why-nasdaq-is-even-more-optimistic-about-blockchain-than-it-was-3-years-ago/#1a583bc31a26. [Accessed: 04- Apr- 2017]

[127] R. Hackett, "Big Business Giants From Microsoft to J.P. Morgan Are Getting Behind Ethereum", *Fortune*, 2017. [Online]. Available: http://fortune.com/2017/02/28/ethereum-jpmorgan-microsoft-alliance/. [Accessed: 02- Apr- 2017]

[128] J. Eyers, "Brokers want ASX blockchain to do more", *Australian Financial Review*, 2017. [Online]. Available: http://www.afr.com/technology/brokers-want-asx-blockchain-to-do-more-20170305-gurbg7. [Accessed: 02- Apr- 2017]

[129] T. Olsen, "Blockchain in Financial Markets: How to Gain an Edge", *Bain & Company*, 2017. [Online]. Available: http://www.bain.com/publications/articles/blockchain-in-financial-markets-how-to-gain-an-edge.aspx. [Accessed: 02- Apr- 2017]

[130] O. Bussmann, "Banks will not adopt blockchain fast", *Financial Times*, 2016. [Online]. Available: https://www.ft.com/content/8fc96cbc-8ed9-11e6-a72e-b428cb934b78. [Accessed: 02- Apr- 2017]

[131] J. Van de Velde et al., "Blockchain in Capital Markets - The Prize and the Jour ney", *Oliver Wyman*, 2016. [Online]. Available: http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2016/feb/BlockChain-In-Capital-Markets.pdf. [Accessed: 23- Mar- 2017]

[132] "Blockchain Value Analysis for Investment Banks | BANKING ON BLOCKCHAIN", *Accenture*, 2017. [Online]. Available: https://www.accenture.com/us-en/insight-banking-on-blockchain. [Accessed: 02- Apr- 2017]

[133] E. Mesropyan, "21 Companies Leveraging Blockchain for Identity Management and Authentication", *Lets Talk Payments*, 2017. [Online]. Available: https://letstalkpayments.com/22-companies-leveraging-blockchain-for-identity-management-and-authentication/. [Accessed: 03- Apr- 2017]

[134] "Blockchain Identity", *Blockstack*. [Online]. Available: https://blockstack.org/posts/blockchain-identity. [Accessed: 03- Apr- 2017]

[135] A. Cooper, "Does digital identity need blockchain technology? | GOV.UK Verify", *Gov.UK*, 2016. [Online]. Available: https://identityassurance.blog.gov.uk/2016/08/15/does-digital-identity-need-blockchain-technology/. [Accessed: 03- Apr- 2017]

[136] “ID2020 - CONCEPT FOR PUBLIC/PRIVATE PARTNERSHIP", *ID2020*, 2017. [Online]. Available: https://static1.squarespace.com/static/578015396a4963f7d4413498/t/589334bc5016e124bb583809/1486042340845/ID2020+White+Paper+-+Jan+2017. [Accessed: 03- Apr- 2017]

[137] A. Noble, "Identity, verification and blockchains", *Finextra*, 2016. [Online]. Available: https://www.finextra.com/blogposting/13345/identity-verification-and-blockchains. [Accessed: 04- Apr- 2017]

[138] G. Hazari, "The Relationship Between Blockchain and Digital Identity", *GSMA*, 2017. [Online]. Available: http://www.gsma.com/personaldata/the-relationship-between-blockchain-and-digital-identity. [Accessed: 03- Apr- 2017]

[139] Z. Martin, "Blockchain and identity", *SecureIDNews*, 2016. [Online]. Available: https://www.secureidnews.com/news-item/blockchain-and-identity/. [Accessed: 04- Apr- 2017]

[140] I. Allison, "Guardtime secures over a million Estonian healthcare records on the blockchain", *International Business Times UK*, 2016. [Online]. Available: http://www.ibtimes.co.uk/guardtime-secures-over-million-estonian-healthcare-records-blockchain-1547367. [Accessed: 07- Apr- 2017]

[141] O. Williams-Grut, "Estonia is using the technology behind bitcoin to secure 1 million health records", *Business Insider*, 2016. [Online]. Available: http://uk.businessinsider.com/guardtime-estonian-health-records-industrial-blockchain-bitcoin-2016-3. [Accessed: 07- Apr- 2017]

[142] G. Keirns, "SAP Ariba Inks Blockchain Supply Chain Partnership With Everledger", *CoinDesk*, 2017. [Online]. Available: http://www.coindesk.com/sap-ariba-blockchain-supply-chain-everledger/. [Accessed: 07- Apr- 2017]

[143] "Overview – Bitland", *Bitland*, 2017. [Online]. Available: http://www.bitland.world/overview/. [Accessed: 07- Apr- 2017]

[144] "Trust, confidence and Verifiable Data Audit", *DeepMind*, 2017. [Online]. Available: https://deepmind.com/blog/trust-confidence-verifiable-data-audit/. [Accessed: 04- Apr- 2017]

[145] S. Mathieson, "Blockchain starts to prove its value outside of finance", *ComputerWeekly*, 2017. [Online]. Available: http://www.computerweekly.com/feature/Blockchain-starts-to-prove-its-value-outside-of-finance. [Accessed: 07- Apr- 2017]

[146] L. Parker, "Hyperledger used to track US oil on a blockchain", *Brave New Coin*, 2017. [Online]. Available: https://bravenewcoin.com/news/hyperledger-used-to-track-us-oil-on-a-blockchain/. [Accessed: 07- Apr- 2017]

[147] D. Ngo, "Blockchain in Global Supply Chains to Prevent Counterfeits and Fake Goods", *Coinjournal*, 2017. [Online]. Available: https://coinjournal.net/blockchain-supply-chains-counterfeits-fake-goods/. [Accessed: 07- Apr- 2017]

[148] C. De Meijer, "Blockchain in Healthcare: make the Industry better", *Finextra*, 2017. [Online]. Available: https://www.finextra.com/blogposting/13801/blockchain-in-healthcare-make-the-industry-better. [Accessed: 09- Apr- 2017]

[149] "Storj Labs Raises $3 Million in Seed Funding", *Storj*, 2017. [Online]. Available: http://blog.storj.io/post/157615681743/storj-labs-raises-3-million-in-seed-funding. [Accessed: 29- Mar- 2017]

[150] S. Vaughan-Nichols, "Storj introduces a distributed blockchain-protected cloud storage service", *ZDNet*, 2017. [Online]. Available: http://www.zdnet.com/article/storj-introduces-a-distributed-blockchain-protected-cloud-storage-service/. [Accessed: 29- Mar- 2017]

[151] C. Mellor, "Become a blockchain-secured space farmer with your hard drive", *The Register*, 2017. [Online]. Available: https://www.theregister.co.uk/2017/02/23/storj_labs_open_source_cloud_storage/. [Accessed: 29- Mar- 2017]

[152] R. van der Meulen, "Gartner Says by 2020 "Cloud Shift" Will Affect More Than $1 Trillion in IT Spending", *Gartner*, 2016. [Online]. Available: http://www.gartner.com/newsroom/id/3384720. [Accessed: 29- Mar- 2017]

[153] S. Wilkinson, "Migration from Counterparty to Ethereum", *Storj*, 2017. [Online]. Available: http://blog.storj.io/post/158740607128/migration-from-counterparty-to-ethereum. [Accessed: 29- Mar- 2017]

[154] L. Columbus, "Roundup Of Cloud Computing Forecasts And Market Estimates, 2016", *Forbes*, 2017. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2016/03/13/roundup-of-cloud-computing-forecasts-and-market-estimates-2016/#5244f3292187. [Accessed: 29- Mar- 2017]

[155] "Upload/Download - Documentation", *Storj*. [Online]. Available: https://storj.readme.io/docs/uploading-and-downloading-cats. [Accessed: 29- Mar- 2017]

[156] "Online Voting Platform FAQ's", *Follow My Vote*. [Online]. Available: https://followmyvote.com/online-voting-platform-faqs/. [Accessed: 29- Mar- 2017]

[157] B. Dickson, "Blockchain tech could fight voter fraud — and these countries are testing it", *VentureBeat*, 2016. [Online]. Available: https://venturebeat.com/2016/10/22/blockchain-tech-could-fight-voter-fraud-and-these-countries-are-testing-it/. [Accessed: 29- Mar- 2017]

[158] A. Barnes, T. Perry and C. Brake, "Digital Voting with the use of Blockchain Technology", *The Economist*. [Online]. Available: https://www.economist.com/sites/default/files/plymouth.pdf. [Accessed: 29- Mar- 2017]

[159] P. Noizat, "Blockchain Electronic Vote", *WeUseCoins*. [Online]. Available: https://www.weusecoins.com/assets/pdf/library/blockchain-electronic-vote.pdf. [Accessed: 29- Mar- 2017]

[160] J. Koven, "Block The Vote: Could Blockchain Technology Cybersecure Elections?", *Forbes*, 2016. [Online]. Available: https://www.forbes.com/sites/realspin/2016/08/30/block-the-vote-could-blockchain-technology-cybersecure-elections/2/#539b8f867fe7. [Accessed: 29- Mar- 2017]

[161] "Report of the Speaker's Commission on Digital Democracy", *Digital Democracy - Parliament UK*, 2015. [Online]. Available: http://www.digitaldemocracy.parliament.uk/documents/Open-Up-Digital-Democracy-Report.pdf. [Accessed: 29- Mar- 2017]

[162] "Independent Report on E-voting in Estonia | A security analysis of Estonia's Internet voting system by international e-voting experts.", *Estoniaevoting.org*, 2014. [Online]. Available: https://estoniaevoting.org/. [Accessed: 29- Mar- 2017]

[163] L. Russell, "Blockchains: The legal landscape", *Blake Morgan*, 2016. [Online]. Available: https://www.blakemorgan.co.uk/training-knowledge/features-and-articles/blockchains-legal-landscape/. [Accessed: 09- Apr- 2017]

[164] "IBM 2016 Annual Report", *IBM*, 2016. [Online]. Available: https://www.ibm.com/annualreport/2016/images/downloads/IBM-Annual-Report-Chairmans-Letter-2016.pdf. [Accessed: 09- Apr- 2017]

[165]C. Hebblethwaite, "Tracking prescription drugs with Chronicled", *Blockchain Expo*, 2017. [Online]. Available: https://blockchain-expo.com/2017/04/blockchain/tracking-prescription-drugs-chronicled/. [Accessed: 11- Apr- 2017]

[166] P. Bajpai, "Blockchain Technology Can Help Reduce Flow Of Counterfeit Drugs", *NASDAQ*, 2016. [Online]. Available: http://www.nasdaq.com/article/blockchain-technology-can-help-reduce-flow-of-counterfeit-drugs-cm721230. [Accessed: 11- Apr- 2017]

[167] "Rubix by Deloitte on Blockchain Use Cases for the Pharmaceutical Supply Chain", *Red Chalk Group*, 2017. [Online]. Available: http://www.redchalk.com/feature/rubix-by-deloitte-on-blockchain-use-cases-for-the-pharmaceutical-supply-chain/. [Accessed: 18- Apr- 2017]

[168] "Blockchain reaches beyond financial services with some industries moving faster – Press release", *Deloitte*, 2016. [Online]. Available: https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-survey-blockchain-reaches-beyond-financial-services-with-some-industries-moving-faster.html. [Accessed: 11- Apr- 2017]

[169] K. Piskorska, "4 Key Use Cases Where Pharma is Leveraging the Blockchain with BlockRx Pilot Program", *LinkedIn*, 2017. [Online]. Available: https://www.linkedin.com/pulse/4-key-use-cases-where-pharma-leveraging-blockchain-pilot-piskorska. [Accessed: 19- Apr- 2017]

[170] S. Das, "US Pharma Looks at Blockchain Tech to Track Prescription Drugs", *CryptoCoinsNews*, 2017. [Online]. Available: https://www.cryptocoinsnews.com/us-pharma-taps-blockchain-tech-to-track-prescription-drugs/. [Accessed: 18- Apr- 2017]

[171] "IBM + Hejia Launch Blockchain Platform for Pharmaceuticals", *Www-03.ibm.com*, 2017. [Online]. Available: https://www-03.ibm.com/press/us/en/pressrelease/52055.wss. [Accessed: 19- Apr- 2017]

[172] "Chronicled Company Profile | Owler", *Owler*, 2017. [Online]. Available: https://www.owler.com/iaApp/12053190/chronicled-company-profile. [Accessed: 11- Apr- 2017]

[173] "Chronicled | crunchbase", *Crunchbase*, 2017. [Online]. Available: https://www.crunchbase.com/organization/chronicled#/entity. [Accessed: 11- Apr- 2017]

[174] "CryptoSeal (CSS100) PRODUCT BROCHURE", *Chronicled*. [Online]. Available: http://www.chronicled.com/download/CryptoSeal-Datasheet.pdf. [Accessed: 12- Apr- 2017]

[175] W. Chibelushi, "Harnessing the blockchain to rejuvenate Africa's developing markets", *African Business Review*, 2017. [Online]. Available: http://www.africanbusinessreview.co.za/leadership/2767/Harnessing-the-blockchain-to-rejuvenate-Africas-developing-markets. [Accessed: 12- Apr- 2017]

[176] J. Keane, "Sweden Moves to Next Stage With Blockchain Land Registry", *CoinDesk*, 2017. [Online]. Available: http://www.coindesk.com/sweden-moves-next-stage-blockchain-land-registry/. [Accessed: 12- Apr- 2017]

[177] C. Heider and A. Connelly, "Why Land Administration Matters for Development", *World Bank Group*, 2016. [Online]. Available: http://ieg.worldbankgroup.org/blog/why-land-administration-matters-development. [Accessed: 13- Apr- 2017]

[178] L. Shin, "The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project", *Forbes*, 2017. [Online]. Available: https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#171e7dff4dcd. [Accessed: 13- Apr- 2017]

[179] G. Keirns, "Blockchain Land Registry Tech Gets Test in Brazil", *CoinDesk*, 2017. [Online]. Available: http://www.coindesk.com/blockchain-land-registry-tech-gets-test-brazil/. [Accessed: 13- Apr- 2017]

[180] J. Wong, "Sweden's blockchain-powered land registry is inching towards reality", *Quartz*, 2017. [Online]. Available: https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-a-reality/. [Accessed: 13- Apr- 2017]

[181] A. Shelkovnikov, "Blockchain applications in the public sector", *Deloitte*, 2016. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-app-in-public-sector.pdf. [Accessed: 12- Apr- 2017]

[182] P. Rizzo, "Blockchain Land Title Project 'Stalls' in Honduras", *CoinDesk*, 2015. [Online]. Available: http://www.coindesk.com/debate-factom-land-title-honduras/. [Accessed: 13- Apr- 2017]

[183] R. Pipan, "The Bitfury Group and Government of Republic of Georgia Expand Historic Blockchain Land - Titling Project", *BitFury*, 2016. [Online]. Available: http://bitfury.com/content/4-press/the_bitfury_group_republic_of_georgia_expand_blockchain_pilot_2_7_16.pdf. [Accessed: 17- Apr- 2017]

[184] I. Ferre, "A Great 2016", *ChromaWay*, 2017. [Online]. Available: https://chromaway.com/post/2017/01/09/a-great-2016/. [Accessed: 17- Apr- 2017]

[185] L. Parker, "Ukraine and BitFury launching first 'full-scale' blockchain eGovernment pilot", *Brave New Coin*, 2017. [Online]. Available: https://bravenewcoin.com/news/ukraine-and-bitfury-launching-first-full-scale-blockchain-egovernment-pilot/. [Accessed: 17- Apr- 2017]

[186] "Bitfury Company Profile | Owler", *Owler*, 2017. [Online]. Available: https://www.owler.com/iaApp/1179486/bitfury-company-profile. [Accessed: 17- Apr- 2017]

[187] G. Chavez-Dreyfuss, "Ukraine to launch big blockhain deal with tech firm Bitfury", *WHTC (Holland's News Leader)*, 2017. [Online]. Available: http://whtc.com/news/articles/2017/apr/13/ukraine-to-launch-big-blockhain-deal-with-tech-firm-bitfury/. [Accessed: 17- Apr- 2017]

[188] A. Rana, "Is Blockchain The Solution for Healthcare?", *Dataconomy*, 2017. [Online]. Available: http://dataconomy.com/2017/03/blockchain-solution-healthcare/. [Accessed: 09- Apr- 2017]

[189] G. Shaw, "Tom Price weighs pros, cons of electronic health records at Senate HELP Committee hearing", *FierceHealtchare*, 2017. [Online]. Available: http://www.fiercehealthcare.com/ehr/tom-price-weighs-pros-cons-electronic-health-records-at-senate-finance-committee-meeting. [Accessed: 09- Apr- 2017]

[190] D. Munro, "Data Breaches In Healthcare Totaled Over 112 Million Records In 2015", *Forbes*, 2015. [Online]. Available: https://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#1b810f3d7b07. [Accessed: 09- Apr- 2017]

[191] B. Monegain, "Data-sharing initiative reduces deaths", *Healthcare IT News*, 2013. [Online]. Available: http://www.healthcareitnews.com/news/data-sharing-initiative-reduces-deaths. [Accessed: 09- Apr- 2017]

[192] M. Scott, "Reshaping U.K.'s National Health Service With the Blockchain", *NASDA*, 2017. [Online]. Available: http://www.nasdaq.com/article/reshaping-uks-national-health-service-with-the-blockchain-cm765582#ixzz4dlOqA4ue. [Accessed: 09- Apr- 2017]

[193] "Healthcare rallies for blockchains: Keeping patients at the center", *IBM*, 2016. [Online]. Available: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03790USEN. [Accessed: 09- Apr- 2017]

[194] A. Zieger, "Deloitte | EMR and HIPAA", *Emrandhipaa.com*, 2017. [Online]. Available: http://www.emrandhipaa.com/tag/deloitte/. [Accessed: 09- Apr- 2017]

[195] C. Burniske et al., "HOW BLOCKCHAIN TECHNOLOGY CAN ENHANCE EHR OPERABILITY", *Gem*, 2016. [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2016/10/ARKInvest_and_GEM_Blockchain_EHR_Final.pdf. [Accessed: 11- Apr- 2017]

[196] "Gem | crunchbase", *Crunchbase*, 2017. [Online]. Available: https://www.crunchbase.com/organization/bitvault#/entity. [Accessed: 11- Apr- 2017]

[197] "National Health Expenditure Projections 2015 - 2025", *CMA.gov*, 2015. [Online]. Available: https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/Downloads/proj2015.pdf. [Accessed: 11- Apr- 2017]

[198] L. Stevens, "Connected Health Cities creates a prototype blockchain patient consent model", *Digital Health*, 2017. [Online]. Available: https://www.digitalhealth.net/2017/04/chc-creates-a-protoype-bitcoin-patient-consent-model/. [Accessed: 27- Apr- 2017]

[199] "Patientory Leads Tokenization of Healthcare To Deliver Blockchain-Based Patient Care Model", *Patientory.com*, 2017. [Online]. Available: http://patientory.com/2017/04/25/patientory-leads-tokenization-of-healthcare-to-deliver-blockchain-based-patient-care-model/. [Accessed: 28- Apr- 2017]

[200] M. Scott, "Delivering a New Blockchain-Based Patient Care Model", *Patientory.com*, 2017. [Online]. Available: http://patientory.com/2017/03/03/delivering-a-new-blockchain-based-patient-care-model/. [Accessed: 28- Apr- 2017]

[201] J. Willms, "Tapscott Announces International Blockchain Research Institute", *Bitcoin Magazine*, 2017. [Online]. Available: https://bitcoinmagazine.com/articles/don-tapscott-announces-international-blockchain-research-institute/. [Accessed: 19- Apr- 2017]

[202] "Blockchain Investments - Distributed Ledgers and Blockchain Technology", *Blockchain Technologies*, 2016. [Online]. Available: http://www.blockchaintechnologies.com/blockchain-investments. [Accessed: 19- Apr- 2017]

[203] "One Semester Individual Project - 40", *Cardiff University*, 2017. [Online]. Available: http://handbooks.data.cardiff.ac.uk/module/CM3203.html. [Accessed: 21- Apr- 2017]