International Journal of Advance Research, Ideas and Innovations in Technology

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 4)
Available online at: www.ijariit.com

PROJECT REPORT

on

"An Academic and Financial Overview of Blockchain: Applications in Educational Institutions"

Submitted in partial fulfilment of the requirements for the award of the Degree of Bachelor of Commerce (Honors) of CHRIST (Deemed to be University)

CHRIST
(DEEMED TO BE UNIVERSITY)
BENGALURU · INDIA

By

Sudarshan M

1511263

Under the guidance of
Dr. Karthigai Prakasam

DEPARTMENT OF COMMERCE

CHRIST (Deemed to be University), Bengaluru

2017-2018

ACKNOWLEDGEMENTS

I am indebted to many people who helped me accomplish this internship successfully.

First, I thank the Vice Chancellor Dr. Fr Thomas C Matthew of CHRIST (Deemed to be University) for giving me the opportunity to do my project.

Dr. Nithila Vincent, HOD, Commerce Department, Christ (Deemed to be University), for giving me this opportunity.

Dr. Karthigai Prakasam for his support and guidance during the course of my project. I remember him with much gratitude for his patience and motivation, but for which I could not have submitted this work.

I thank my parents for their blessings and constant support, and Ashwath Balakrishnan and Aayushman Agarwal, without whom this Research study would not have seen the light of day.

Sudarshan M

Register No: 1511263

Blockchain and Academia

A Financial and Academic Overview of Blockchain: Applications in Educational Institutions

Sudarshan M

Feb 2018

CONTACT DETAILS:

Sudarshan M

1511263

CHRIST (Deemed to be University)

Bengaluru

Phone: +918197947045

Email Id: sudarshan@supremepetrochemicals.com

Any contributions to the researcher can be done so to the following addresses:

Wallet IDs

BTC: 1JbinZVvtcAGA5hFUNhhYNbW95atsP2tjf

ETH: 0xb68b95c786638e0C77e0cbeeEDD115e79A0af5Fe

DOGE: DUHiBmJoi9J5b2Vt4tJMbQ232q6Gu41xaC

ZEC: t1XRgyS1NeLM9yC8aK5M4QmyromRNUqyW73

ABSTRACT

A tsunami of pressure, transparency, mess, job-cuts and efficiency; just some of the long standing disruptions that Bitcoin brought with it, since its inception 9 years ago in 2009. But, hand in hand with Bitcoin, came another revolution. A revolution touted to change the face of all centralized mediums. The underlying technology behind Bitcoin, that makes it a "Borderless Transparent Mutual Censorship Resistant and Immutable Currency", **Blockchain**, is the main aim of this study, along with finding possible solutions and implications in the field of Academics and Education. The fundamental and core concepts of Blockchain are explained with its potential influence in various sectors, mainly Education. Keeping in mind the current state of Academia, Christ University has been taken into consideration as a model for this study.

Table of Contents

Table of contents

Table of Figures:

I. Introduction

I. Introduction

Right after the 2008 Economic depression, a paper[1] surfaced on the Internet by an anonymous alias Satoshi Nakamoto, describing in detail, a new form of digital currency to eradicate or at least supplement Centralised mediums of exchange.

Is Blockchain supposed to be the next big thing? Is Blockchain repeating the innovation phase of the 90's Internet era all over again? Why is blockchain deemed to be the next big thing? Why has the world deemed to be shifting all its interests to this new technology? Is blockchain all what they say it is or is it just going to be the greatest job-cutter of all time?

2009 was the dusk of the Global Housing rescission. But virtually and economically, 2009 was the dawn of the Bitcoin era, that started off a wildfire of '*disruptive innovative'* use-case scenarios. With the addition of Ethereum[2] in 2013, the paradigm of Blockchain based thinking shifted to a new gear. New ideas and concepts started popping up in various fields and sectors. The time consuming and expensive process of long-distance remittance, for one, was eliminated with the advent of bitcoin. Thinking not just in monetary terms, but also in terms of centralised mediums, Blockchain, prospects itself as the disruptor of these mediums, and maybe the biggest disruptor since the Internet.

Figure 1.1 Introduction to Bitcoin

i. Brief history of Bitcoin

A 2008 whitepaper[3] written under the pseudonym Satoshi Nakamoto introduced the concept of Bitcoin as 'A Purely P2P version of electronic cash (that), would allow online payments to be sent directly from one party to another without going through a financial institution.'

[1] Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto

[2] Ethereum: A Secure decentralized generalised transaction Ledger; Vitalik Buterin, Gavin Wood (2013)

[3] Whitepaper - A **white paper** is an authoritative report or guide that informs readers concisely about a complex issue and presents the issuing body's philosophy on the matter. investopedia.com

With this statement, the whole class of 'Digital Assets' was put under question, as the concept of Bitcoin being a 'bearer asset[4]' was put forward. The value of the asset in question, Bitcoin (btc - ticker symbol), is derived and gained only by the importance it receives from the network or community that decided to value the asset, thus forming a new class of asset or instrument, backed by no underlying value, but of the mutual trust in the network. The traditional system of electronic cash involved uploading numbers that are stored on a centralised database of a financial authority, whose permission is needed for the use or transfer of those funds.

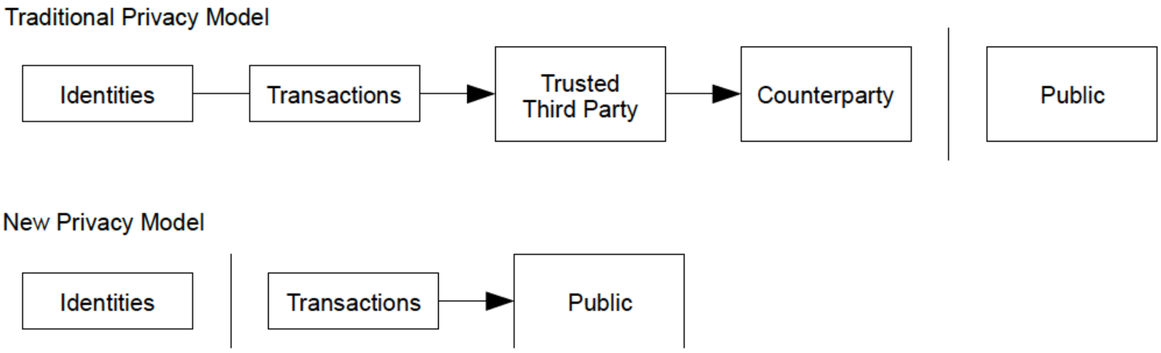


Figure 1.2: Traditional vs. New Model

Starting with Bitcoin, a decentralised remittance mechanism sprang into existence, that was backed by nothing but the mutual trust of the participants of the network, without the need for an issuing or centralised authority to govern the functioning of the network. The Bitcoin protocol was designed in a way to be free from any tampering of the original source code. No single participant, acting against the network, can deny use to the network in any way, making Bitcoin the first, in a series of 'Borderless transparent mutual censorship resistant immutable[5]' currency or medium of exchange.

'If the internet were an independent country, bitcoin was its first monetary value/medium of exchange'[6], said *Garrick Hileman*, Cambridge University Fellow and Blockchain enthusiast who has

[4] A Bearer instrument is one wherein the no ownership details are needed for ascertaining value of the asset as the value is derived from ownership alone.
bitcoinblocks.com

[5] Quote by Andreas M Antonopoulous, in MOOC 8 organised by the University of Nicosia

[6] Conversation with Garrick Hileman at Decentralized 2017, Cyprus

intensively studied the field of cryptocurrency and put forwards his research in the paper *Global Cryptocurrency Benchmarking Study (2017).*

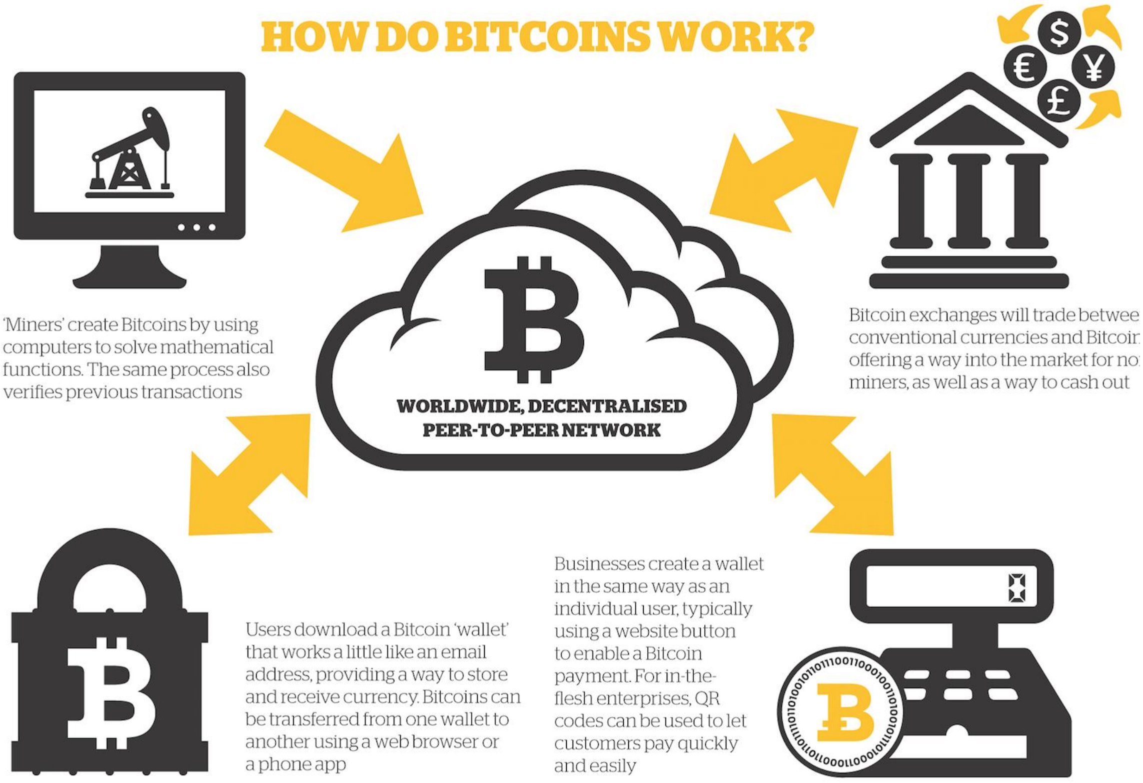
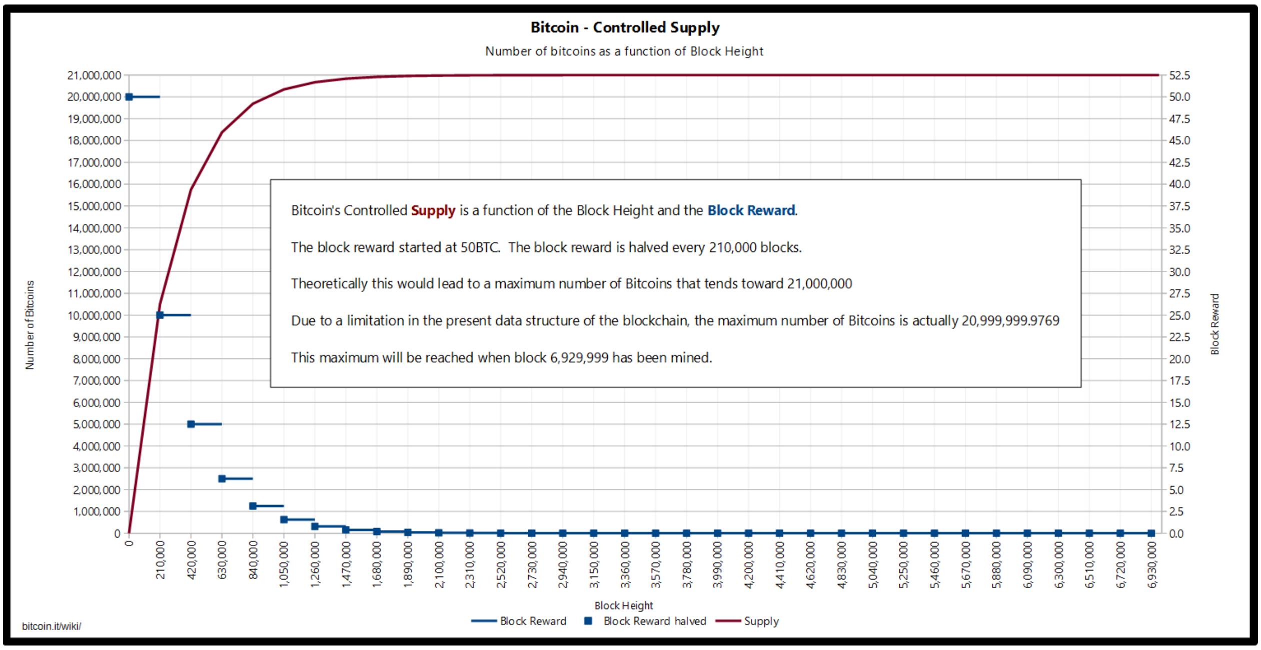

HOW DO BITCOINS WORK?
'Miners' create Bitcoins by using computers to solve mathematical functions. The same process also verifies previous transactions
WORLDWIDE, DECENTRALISED PEER-TO-PEER NETWORK
Bitcoin exchanges will trade betwee conventional currencies and Bitcoir offering a way into the market for no miners, as well as a way to cash out
Users download a Bitcoin 'wallet' that works a little like an email address, providing a way to store and receive currency. Bitcoins can be transferred from one wallet to another using a web browser or a phone app
Businesses create a wallet in the same way as an individual user, typically using a website button to enable a Bitcoin payment. For in-the-flesh enterprises, QR codes can be used to let customers pay quickly and easily

Figure 1.3: What is Bitcoin? What *Source:* goldeneagle.com

Bitcoin is the first peer-to-peer digital currency that works as a system without a central authority or administrator. The transactions on the bitcoin network are verified by network nodes[7] through the use of secure cryptography and then recorded on a distributed public open-source ledger, referred to as the *Blockchain.*

[7] nodes - a point in a network or diagram at which lines or pathways intersect or branch



Bitcoin's Controlled **Supply** is a function of the Block Height and the **Block Reward**.

The block reward started at 50BTC. The block reward is halved every 210,000 blocks.

Theoretically this would lead to a maximum number of Bitcoins that tends toward 21,000,000

Due to a limitation in the present data structure of the blockchain, the maximum number of Bitcoins is actually 20,999,999.9769

This maximum will be reached when block 6,929,999 has been mined.

Figure 1.4: Currency supply Creation of Bitcoin as per the protocol. Source: bitcoin.it/wiki

The Bitcoin network was created and administrated by the Bitcoin protocol that was applied by Satoshi Nakamoto in January 2009. The total money supply creation of bitcoin/btc, the currency of the Bitcoin network, was fixed at 21,000,000. This is affixed on a mathematical algorithm that keeps rewarding verifying participants of the network in the form of freshly created currency supply. This process of verification by network participants with a reward as their incentive is called cryptographic mining[8]. Bitcoin is encrypted using SHA-256[9] bit cryptographic hash function.

A simple solution that accomplishes decentralised verification without any trusted authority, the *Blockchain* forms the base of Bitcoin, which in turn happened to be one of the major disruptive innovations in the recent technological history.

ii. Underlying technology of Bitcoin

Blockchain, the underlying technology behind digital currencies like bitcoin, has been hailed as having world-changing potential for industries ranging from health care and banks to manufacturing.

[8] cryptographic mining - process by which transactions are verified and added to the public ledger, known as the blockchain, through a network of verifying nodes

[9] The SHA (Secure Hash Algorithm) is one of a number of cryptographic hash functions. A cryptographic hash is like a signature for a text or a data file. **SHA-256** algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one way function – it cannot be decrypted back. (xorbin.com)

Blockchain essentially functions as a decentralized ledger technology, used to record and verify transactions. While bitcoin and Ether[10], which run on their own distinct Blockchains, have the most visible usage at the moment, the technology has a myriad of applications beyond cryptocurrencies.

[10] Cryptocurrency of the Ethereum Blockchain Network

II. Review of Literature

II. Review of Literature

1. **Tapscott, D. & Tapscott. A. (2016). Blockchain revolution:** Considered the Bible of all blockchain related aspirations or motivation, the father-son duo in the form of Don and Alex Tapscott, both well-known economic thinkers, put forward their thinking of how the technology blockchain is going tho revolutionise all of business processes and possibly even more. Several ideas cited in the journal are inspired directly from their book.

2. **Antonopolous, A. (2014). Mastering Bitcoin:** Possibly the first printed form of clarity about the internal workings of the mysterious internet currency floating around, Mastering Bitcoin has helped in the understanding the core concepts of bitcoin and blockchain in general. Andereas has given all the information he could in every aspect so as to let the reader be absolutely aware of the inner workings of the network.

3. **Nakamoto, S. (2008). Bitcoin - A peer-to-peer electronic cash system:** In understanding the technology of blockchain, the first extract of a working ledger that was distributed and secures found here. The anonymous write Satoshi Nakamoto brought forward a new form of currency, solely dependent on the mutual co-operation of the participants of the currency. The whole concept of bitcoin and blockchain being its underlying technology was first seen on paper in this article.

4. **Buterin, V. & Wood, G. (2013). Ethereum - A secure dcentralized generalised transaction ledger:** The first revolutionary step into exposing the potential of Blockchain, Vitalik Buterin released the Ethereum whitepaper in 2013. In that paper, he discussed all the drawbacks that bitcoin brings along with it, along with being an open-source protocol that nobody can tamper with. Ethereum brought several changes and improvements to the blockchain sector, that are touted to be the next technological revolution. The ethereum paper changed the currency supply, the coding language, and also introduced an option to issue token based off of the Ethereal network. Essentially becoming a *'Blockchain of blockchains'.*

5. **Schwartz, D., Youngs, N. & Britto, A. (2014). The Ripple Protocol Consensus Algorithm:** While several algorithms were developed for solving the Byzantine General's Problem, many of those algorithms suffer from high latency and scalability problems that requires all network nodes to communicate synchronously. The contributions of Ripple Inc, the organisation behind Ripple cryptocurrency, to the blockchain study space has been extensively studied for this research.

6. **Popov, S. (2017). The Tangle (IOTA):** Keeping in mind the future of electronic communication, through the concept of Internet of Things, the Tangle technology was developed, to have devices that are connected through the internet, to each other, transact in a free-flow. Tangle, is the underlying technology behind the IOTA, that portrays itself as an upgrade to the concept of Blockchain and ensure a transaction fee-free transfer of information, both secure and distributed in nature. IOT implementation discussed in further chapters discusses this in detail.

7. **Duffield, E. & Diaz, D. (2013). Dash: A privacy-centric cryptocurrency:** An important revolution in the crypto space, Dash was formed as a cryptocurrency that is developed and pushed forward by active network participants, to be a privacy centric cryptocurrency that solely functions for the network. All the activities of Dash are governed by the Dash network participants, who ensure the development of the Dash protocol, making Dash the first organisation without an hierarchy, where each participant's contribution is rewarded with the network's monetary value.

8. **Snow, P. & Deery, B. (2014) Factom:** Realising the lack of trust in the global and digital sense, Factor was developed. The lack of trust requires the devotion of a tremendous amount of resources to audit and verify records, and ultimately reducing efficiency. Factom's 'ecosystem' showed the trust factor of blockchain as it removed the need for blind trust by providing the first precise, verifiable and immutable audit trail. Factom's importance for trust among network participants is taken as a reference in the research.

9. **Back, A. (2002). Hash Cash:** Satoshi's paper introduced bitcoin as an improvement to the HashCash internet currency mechanism proposed by Adam Back, way back in 2002. But the HashCAsh paper lacked the security and the distributed information protocol that made bitcoin what it is. HashCash can be seen as the telegram, in a world where bitcoin is the smartphone.

10. **Grech, A. & Camilleri, A. (2017). Blockchain in Education:** This study was designed and supported by the European Commission's Joint Research Centre (JRC). Its main view was to explain the possible application of this innovative field in the Education and academic sector. Blockchain and its disintermediation ideals make it apt for numerous areas and ideas to be explored. This research was extensively studied and referenced in the following paper.

11. **Surda, P. (2017). Economics of Bitcoin: Is Bitcoin an alternative to Fiat currency and Gold?:** In understanding the internal working of bitcoin and the internal economics that makes it a decentralised self-issuing currency, this paper gave a lot of insight. We can lookout the similarities of Bitcoin to Gold in terms of limited supply and an instrument of value. Can Bitcoin

be view as a main stream currency, where people transact in a currency with no central issuer. Is the situation viable at all?

12. **Anderson, N. Deloitte. (2017). Blockchain - A game changer in Accounting:** With the transparent nature of bitcoin, a new form of accounting can be seen, as all transactions on the bitcoin blockchain are open for all participants to audit and verify. With the use of cryptographic key infrastructure,

13. **Wong, L. (2015). New Economic Movement (NEM):** Another important Blockchain that is circulating around is the New Economic Movement and its cryptocurrency for the network XEM. NEM portrays itself as a blockchain that rewards it user of the network in terms of their participation of the network. The more a person transacts, the more the importance of that person increases in the network. This research paper or white paper gave the understanding of the deeper applications of the Blockchain that could involve including the Blockchain public ledger in real world applications.

14. **Dobilliauskas, J. (2017). Bankera - Bank for the Blockchain era:** Bankera was introduced in 2017 as an Ethereum based Blockchain token, that was backed by the functioning of the online-crowd sourced, self-proclaimed ‘Bank’ for cryptocurrencies, that involves Lend and borrowing with the introduction of Smart Contracts. Bankera, the organisation that was founded on the idea by Justas, has successfully managed to crowd source around $100 million in their ICO and pre-ICO sale, where they issued Bankera ownership tokens in exchange for contribution. Bankera’s whitepaper explained the further use of Blockchain, now in Banking where intermediaries and costs would be cut drastically.

15. **Zawistowski, J., Janiuk, P., Regulski, A. (2017). Golem Network:** The Golem Network was developed side by side the Story Network, where the idle computation power of a machine can be rented out in exchange for Golem Network Tokens (GNT). Any amount of machines can be linked to a particular account and any required participant could log in to the Network and use the Network’s computation in exchange for the Network’s currency. The concept of Blockchain, Smart contracts and Computation synergy was explained through the Golem whitepaper.

16. **Soldevilla Estrada, J.C., (2017). Volitity in Bitcoin:**When comparing different instruments, what would be the most important factor to cancel out to find absolute speculate return? Risk. Removal of risk from each instrument breaks down and shows you there core. This study published analyzed the volatility of Bitcoin. Obviously, the levels of volatility were extremely

high and way beyond that of any market we've seen yet. This helps us understand that to make a comparison of the instruments, risk or volatility must be adjusted so they're at the same level.

17. (**2017). Sirin Labs:** Sirin Labs was set up as a technology manufacturer, in the last decade as a gateway for interested personal to get their hands secured electronics, that are wary of any external tampering.

18. **Szabo, N. (1993). Smart Contracts:** Said to be one of the most relovutionary thinker of his time, all of the importance given to the Blockchain can be single-handedly traced back to this research paper where Nick Szabo suggested a mechanism called Smart Contracts that acted as virtual, non-reversible contracts and auctioned arbitrarily one relayed into action. With the introduction of Blockchain, and more importantly Ethereum in 2013, explored the concept of Smart Contracts and found it to be the most extensive kapplication possible for Blockchain based applications, that allows the use of irrefutable contracts binding two virtual parties.

19. European Central Bank. (2016). Distributed Ledger Technology: The introduction of Blockchain also introduced the concept of a Distributed Ledger where all participants are required to maintain a copy of the protocol, not as a compulsion, but as a part of the Blockchain protocol in itself. This technology allows for new ideas to be explore where the distribution of the ledger of transactions or information is limited. DLT is suggested to be revolutionary in this European study, where implications are discussed on a broader scale.

III. Methodology

III. Methodology

i. Statement

The main objective behind this study was to raise awareness about the upcoming and potentially, hugely influential, technology that could disrupt the traditional systems from their core and at the same time provide improved efficiency and reliability, in a way that precedes any revolutionary economic concept put forward. Blockchain deems itself to be the successor of the 90's Internet Revolution, where a large number of traditional practices were put to sleep because of the Global nature of the Internet. Many independent 'future thinkers' and 'innovators' had failed to recognize the true value of the Internet that has managed to grow exponentially since 1990.

The concept Blockchain falls on similar lines, is what this research paper tries to point out, by putting forwards already existing and new ideas in this field. Numerous use cases have been discussed, with a focus on the Education sector, as the need for Education and Academics in general, to have a major shift of momentum, could be seen. Blockchain, with its promise of transparency, disintermediation and immutability, can lead the way to a new technological revolution that looks to disrupt old means by replacing them with the automated nature of Blockchain.

ii. Objectives

- Discuss the innovative field of Blockchain technology, and sectors it could influence, rather than just being perceived as a remittance mechanism or investment vehicle, such as bitcoin
- Show the solutions achieved by Blockchain in the past and the upgrades that can be made to intermediate processes in the future
- Highlight the extended vision of Blockchain to hinder traditional and conventional means of management
- Blockchain, with an importance on the Education sector, is the main focus of this study. Means to use Blockchain in Academics by disrupting traditional practices are suggested in the study.

iii. Methodology used

- This study is purely Qualitative in nature. All reforms, changes or disruptions suggested or shown, are derived from the ideas and understanding of the researcher, based off of material put forward by thinkers and innovators in this field.
- Desk research, interviews, telephonic conversations and literature reviews were extracted to produce this study.

- Magnitudes of secondary data, for the purpose of understanding the core concepts and features of various applications of Blockchain, were referenced in the study.
- All analysis conducted is entirely descriptive in form, meaning that any suggestion put forward has its usage and mechanism explained in detail, occasionally accompanied with pictured representations.
- The technicalities of numerous concepts across the study are purposely simplified to allow for better perception and reach to a non-technical audience.
- For the purpose of eliminating any means of influence from financial aspect of the research, all financial details are reserved until the latter part of the study, so as to avoid any hindrance of flow of ideas.
- Christ (Deemed to be University) has been taken as a model for this study.

iv. Limitations of the Study

- All ideas and suggestions mentioned in the study has been extensively studied and referenced, but as the field of Blockchain in relatively new in nature, there is a possibility of the research being outdated in the very recent future. All interpretations required were done with the latest information available at hand.
- Limitations in terms of Quantitative suggestions can be seen in the study, as the researcher found it difficult to obtain or ascertain the exact figures that would be necessary to make a statement. Most of the data provided or implied is in Qualitative terms.
- By limiting the main aspect of the study towards the Education sector, various possible outcomes of Blockchain that could possibly emerge in other areas were excluded, thus limiting the possible outcomes the study.
- Blockchain technology is a growing trend, with on-going active global participation. Recent advancements have been taken for the study that could have been replaced with better ideas.
- It is possible for other case studies covering the same aspect of this study exist that are better are detailed. The researcher believes the study to be the best of his knowledge.
- The technicalities of numerous concepts across the study are purposely simplified to allow for better perception and reach to a non-technical audience.
- It is possible for the analysis and research to have not been conducted in a valid, relevant or rigorous enough way for the paper.

IV. What is Blockchain?

IV. What is Blockchain?

"The record book is the currency"

Blockchain is an emerging technology, paved way by bitcoin, with almost daily announcements of traditional practices being put to sleep by new innovations. Blockchain promises to cut through the clutches of centralisation. But why and how does blockchain promise to do so much and how does one plan the future with Blockchain technology reaching mass-adoption.

In simple words, *'Blockchain is a decentralised ledger, that provides a way for information to be recorded or time stamped.'*[11] This information is shared by the blockchain network. In a broad sense, think of a train of passengers. Each train has several bogeys (blocks) attached to it, and each boogey (block) contains a set of passengers (information) inside it. Just as the bogeys are connected for the passenger to transported to their destination, think if Blockchain as a connection of *blocks*, each block carries a certain amount of information, which forms a chain, the can be verified anytime. Each block is chronologically connected. Forming a chain of blocks. Thus, Blockhain!

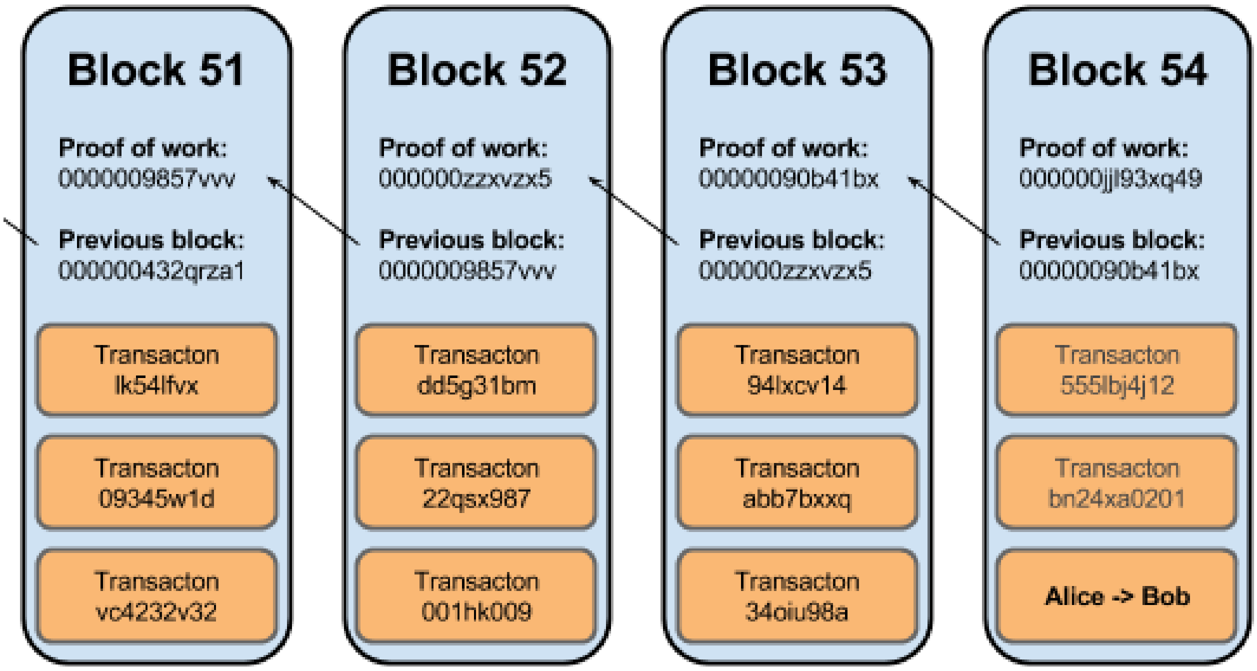


Figure 4.1: Flow of Blocks

The information stored on the blockchain, once approved by the community, is now permanent, transparent and easily verifiable, which makes it an 'open-source decentralised ledger'.

[11] Quote by Antonis Polemitis, MOOC 8 in University of Nicosia

'Blockchain technology and the potential it carries has the means to disrupt any field of activity that is founded on *centralised time-stamped record-keeping.'*[12]

The side by side invention of Blockchain with Bitcoin, set ablaze a fire of innovative ideas and use-case scenarios that blockchain can be a part of. The decentralized nature of blockchain makes it possible for better time keeping, improved audit processes, removal of intermediaries among a few.

The Byzantine's problem of distributed information systems was the key solution in Blockchain, solved by Satoshi Nakamoto, which found its way in the Bitcoin technical whitepaper.

i. The Byzantine Generals' Problem

a. Introduction

In 1982, three computer researchers, *Leslie Lamport*, *Robert Shortak* and *Marshall Pease* formulated an agreement problem deriving it roots from ancient Byzantine Army formations, called the Byzantine General's Problem. This problem talked about the drawbacks of centralised informations systems and the inability to reach an efficient distribution model. This problem formed the basis for countless speculation and possible 'solutions' to this problem were proposed that all failed in some way or the other. Until Bitcoin.

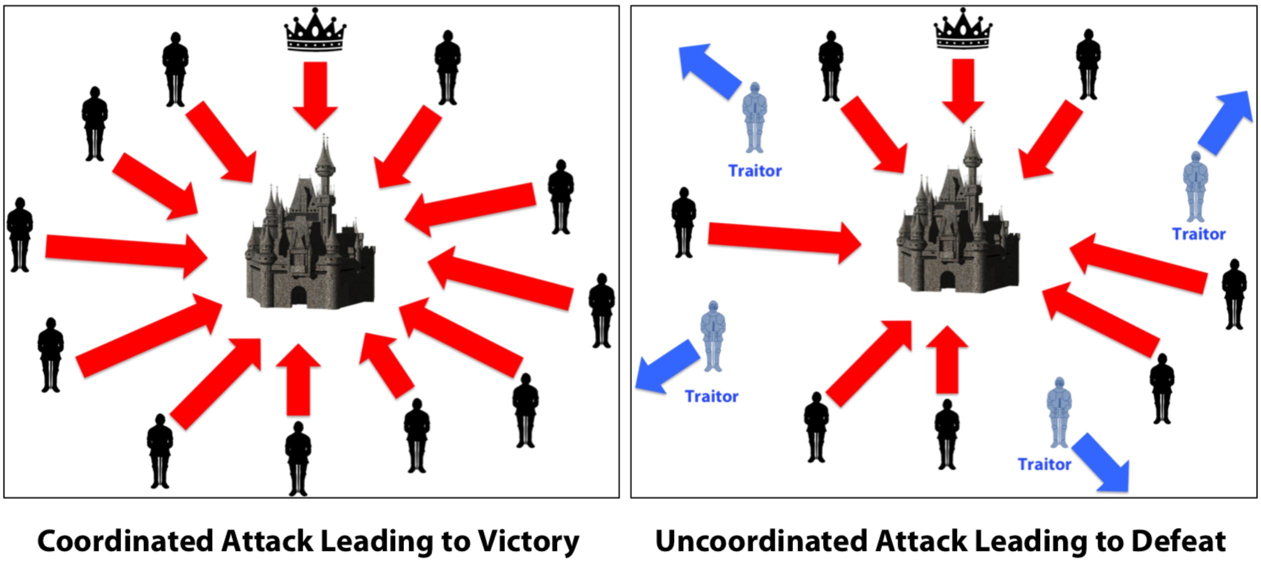
This problem in computing systems came to be known as Byzantine Fault Tolerance[13], that said information processing through 'Turing-complete systems[14]' always suffered from considerable amount of external interference. Byzantine Fault tolerance (BFT) is the resistance of a fault-tolerant[15] computing system, particularly distributed computing systems, towards component failure, i.e., BFT checks the computer's resistance in times of external computing attacks, not just by stopping or crashing, but also by processing requests incorrectly, corrupting their local state, and/or producing incorrect or inconsistent outputs. Due to this, a component server can inconsistently appear both failed and functioning to fail.

[12] Grech, A. & Camilleri, A. (2017). Blockchain in Education, JRC Study

[13] BFT - http://cryptography.wikia.com/wiki/Byzantine_fault_tolerance

[14] A Turing-complete system refers to a machine in which a program can be written that will find an answer, although with no guarantees regarding runtime or memory. In principle this means that it could be used to solve any computation problem. (Stackoverflow)

[15] Fault tolerance in computing systems Fault tolerance is the property that enables a system to continue operating properly in the event of the failure of some of its components. (Techopedia)



Coordinated Attack Leading to Victory **Uncoordinated Attack Leading to Defeat**

.Figure 4.2: How the Byzantine Generals' Sacked the Castle: A Look Into Blockchain Source: https://medium.com/@DebrajG/how-the-byzantine-general-sacked-the-castle-a-look-into-blockchain-370fe637502c

Correctly functioning components of a Byzantine fault tolerant system will be able to correctly provide the system's service assuming there are not too many Byzantine faulty components.

This problem manages to form a loop in itself. By checking itself of being Byzantine tolerant, the machine opens itself to internal and external failure. *The introduction of Blockchain allowed distributed computing systems, for the first time, to eliminate the factor of Fault tolerance, as Blockchain is fault tolerant by nature.*

b. The Age old Problem

The research paper put forward by Leslie Lamport, Robert Shortak and Marshall Pease talked about the problem by taking up the encircling of an enemy city by the Byzantine Army in the 6th century A.D.

This problem assumes a set of Generals, each controlling a portion of the Army, surround an enemy city castle and must now wait for the King's orders so that they coordinate an attack. This coordination would have been achieved only through physical transfer of messages between the King and his Generals. Because the Generals are all in hostile and unfamiliar territory, messages might fail to reach the destination or the message could be colluded or corrupted. An additional aspect of the problem is that some of the Generals may be traitorous, either individually or conspiring together and transfer messages intended to create false strategy that is doomed to fail for the Generals loyal to the King.

Assessing the problems of distributed information in the Ancient era gives us understanding of problems in the current sense. This similar problem can be imagined in a virtual sense where severals information systems might fail to execute information or external interference might tamper with the transfer. In a distributed ledger, any inputs (the messages) to the ledger (the agreed upon time of attack) must be trusted. Digital networks usually have millions of members (the generals) who are dispersed globally and there is no centralized command (no central governance), as it is impossible to know all the members.

c. Satoshi's Blockchain - The only known Solution

Since Bitcoin, the use of Blockchain was put forward. The decentralization and self-governance of Bitcoin is only possible because of blockchain.

The solution to the Byzantine Generals' Problem was developed by a man/group (identity unknown) who goes by the name Satoshi Nakamoto. Satoshi was the inventor of the increasingly popular and groundbreaking bitcoin blockchain. The blockchain is a general solution to the Byzantine Generals' Problem. Each army can be thought of as a node in the system. Messages can be thought of as transactions and the enemy city can be thought of as any man in the middle who seeks to alter the blockchain.

"The proof-of-work chain is a solution to the Byzantine Generals' Problem"[16]

Informal Explanation

A number of Byzantine Generals each have a computer and want to attack the King's wi-fi by brute forcing the password, which they've learned is a certain number of characters in length. Once they stimulate the network to generate a packet, they must crack the password within a limited time to break in and erase the logs, otherwise they will be discovered and get in trouble. They only have enough CPU power to crack it fast enough if a majority of them attack at the same time. They don't particularly care when the attack will be, just that they all agree. It has been decided that anyone who feels like it will announce a time, and whatever time is heard first will be the official attack time. The problem is that the network is not instantaneous, and if two generals announce different attack times at close to the same time, some may hear one first and others hear the other first.

[16] Satoshi Nakamoto in the original Bitcoin whitepaper

They use a proof-of-work chain to solve the problem. Once each general receives whatever attack time he hears first, he sets his computer to solve an extremely difficult proof-of-work problem that includes the attack time in its hash. The proof-of-work is so difficult, it's expected to take 10 minutes of them all working at once before one of them finds a solution. Once one of the generals finds a proof-of-work, he broadcasts it to the network, and everyone changes their current proof-of-work computation to include that proof-of-work in the hash they're working on. If anyone was working on a different attack time, they switch to this one, because its proof-of-work chain is now longer.

A blockchain doesn't use a master copy that is controlled or updated by a single authority. Instead, every node or computer connected to the system gets a copy of the blockchain. Each node, then, updates the record independently, but everyone still arrives at the same result. More importantly, if a node breaks down or disappears, the blockchain still lives via the other nodes that already downloaded it.

After two hours, one attack time should be hashed by a chain of 12 proofs-of-work. Every general, just by verifying the difficulty of the proof-of-work chain, can estimate how much parallel CPU power per hour was expended on it and see that it must have required the majority of the computers to produce that much proof-of-work in the allotted time. They had to all have seen it because the proof-of-work is proof that they worked on it. If the CPU power exhibited by the proof-of-work chain is sufficient to crack the password, they can safely attack at the agreed time.

The proof-of-work chain is how all the synchronisation, distributed database and global view problems you've asked about are solved.[17]

Blockchain technology has recently been touted as one of the greatest inventions since the internet. It is essentially a way to make consensus in a distributed system. It’s not just about money. It’s a very sophisticated and revolutionary way of building trust. Money is simply one of the applications. Blockchain technology has the potential to disrupt not only the finance industry but also healthcare, education, voting, and real estate among countless others. The idea of decentralized power, which blockchain technology is rooted in, has a lot of important implications many of which have yet to be imagined.

[17] Bitcoin P2P e-cash paper (https://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html)

ii. Basic principles

Blockchain is a decentralized ledger, open-source in nature, that removes the need for centralization by introducing better and improved version of *decentralized and distributed time-stamped record-keeping*. These basic principles that are applied on the blockchain making it incredibly efficient in a whole new range of use-case scenarios.

a. Distributed

One of the key features of the blockchain is that it is a *distributed* database; that is to say, the database exists in multiple copies across multiple computers. These computers form a peer-to-peer network, meaning that there is no single, centralized database or server, but rather the blockchain database exists across a decentralized network of machines, each acting as a node on that network.

The concept having multiple copies of the complete historical record of ledger entries that are verified by consensus is by nature attributed in the internal working of the core technology of Blockchain. With multiple copies that are periodically updated and stored, each verified by the consensus of the community, opens a whole paradigm of opportunities to be explored, in terms if improved efficiency and removal of centralization of record keeping.

Information held on a blockchain exists as a shared and continually reconciled database. This is a way of using the network that has obvious benefits. The blockchain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet.

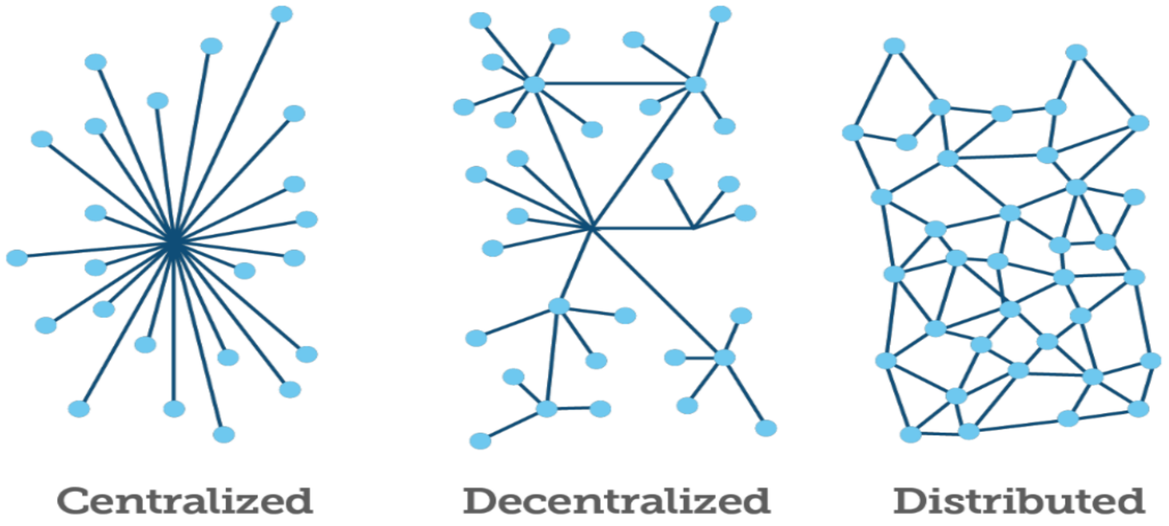


Figure 4.3: Centralized vs. Decentralised vs. Distributed visualised

b. Trustless

In a digital world, the basic concept of trust remains intact where all the parties involved must post forward their blind faith in a centralised authority. When referring to the non-blockchain world and using currency as an example, Banks and Governments provide things such as arbitration, conflict resolution and validation. All these things can happen on the Blockchain but without centralised control or authority.

The core and driving force that you are trusting when using Blockchain is the technology and its ability to not have to trust other participants from a protocol and ownership stance. Since every participant has the same rights as all others, majority consensus rules and the distributed consensus holds the only possible truth. The Byzantine Generals' Problem is often used to demonstrate this concept.

For the public and the enterprise, trust is a time game, the longer they work as expected the more domains they will be used in before Blockchain, also known as Distributed ledger technology, will become more and more mainstream. Below are other areas that contribute to the trust which can be placed in Blockchain technology:

- Trust that all other participants have to abide by the same rules as you do
- Trust that you control your identity on a blockchain
- Trust in the cryptography that secures data on the blockchain
- Trust in the privacy and anonymity a Blockchain may provide
- Trust in the security and safety of Smart Contracts
- Trust in underlying distributed consensus

c. Transparent

In principle, Blockchain is a technology obliged to be transparent in all processes and demonstrate provenance when required. The transparent nature of the Blockchain allows it to be continuously audited by magnitudes of participants of the network who look to avoid any form of discrepancy within the network.Every transaction on the decentralised, open-source, bitcoin ledger is recorded for all participants to see and updated periodically, that all ledgers are in sync, making duplication infeasible.Distributed ledgers can store digital representations of real world transactions that constitute or can be used to prove the current and historical ownership of the represented asset. By tracing eat ownership of the asset on the Blockchain from its inception, transparency of the ownership is demonstrated.

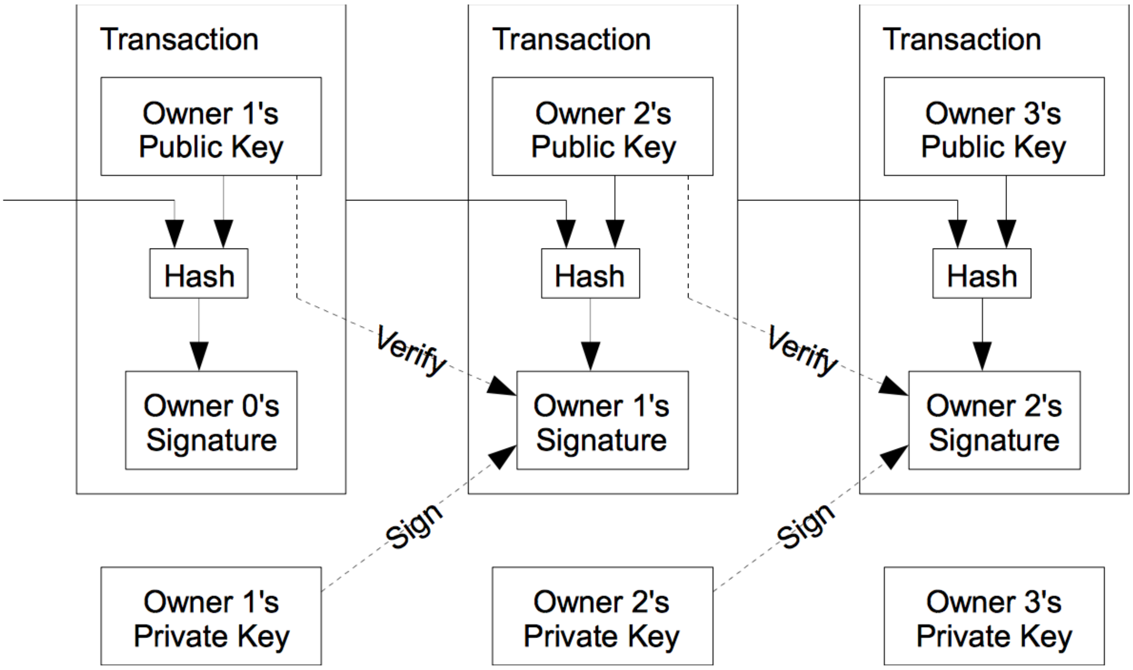


Figure 4.4: Verification of transactions of the Blockchain

On the Bitcoin Blockchain, each transaction is represented in the form of a hash code[18] that mathematically represents a link to the cryptographic keys of the owner of the asset. If the has of the asset matches has of the public key of the owner, that transaction can then be tracked both forwards and backwards making the blockchain truly transparent in all aspects.

d. Immutable

Immutability means an information transferred across some medium being secure, confidential and at the same time resilient and irreversible in nature. The Immutability of a transaction or an asset makes it prone to theft or even duplication. Not being able to duplicate a transaction or information or digital asset makes it easy to audit and track the ownership of that asset or information. The use of cryptographically assigned private and public keys are prominent in software purposes to pass information in a secure way. But it is still prone to outside virtual attacks as they still are stored on a centralized database.

[18] A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes. (GeeksForGeeks.com)

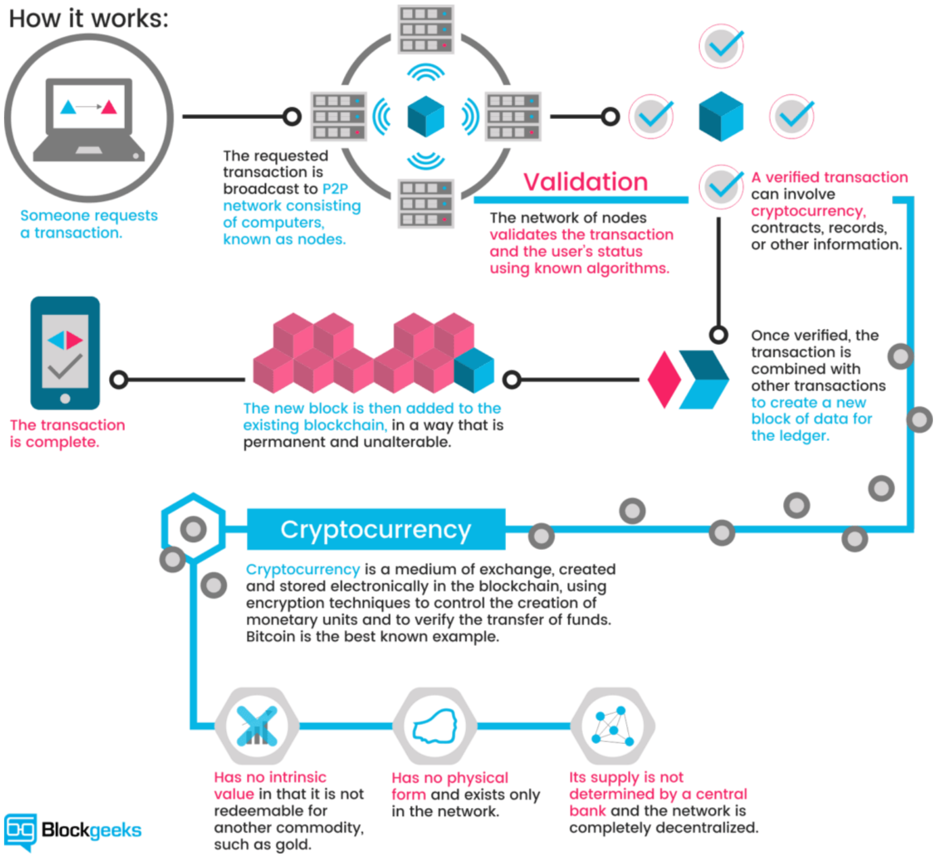

How it works:
Someone requests a transaction.
The requested transaction is broadcast to P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.
Cryptocurrency
Cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the best known example.
Has no intrinsic value in that it is not redeemable for another commodity, such as gold.
Has no physical form and exists only in the network.
Its supply is not determined by a central bank and the network is completely decentralized.
Blockgeeks

Figure 4.5:

Source: What is Cryptocurrency?

https://blockgeeks.com/guides/what-is-cryptocurrency

With the concept of cryptographic keys and distributed ledger consensus, blockchain proves itself to be the gateway for secure irreversible passage of information between parties. Blockchain transactions are computationally immutable, "meaning essentially it is impossible for changes to be made are established."[19]

For a transaction to be considered valid on the blockchain, all parties involved in the transaction must agree on its validity. These parties may/may not include the sender of the transaction, the receiver, the network validator on network node and the previous ledger containing the history of ownership. The validating method differs from network to network, but once a transaction has been verified and updated on the public ledger, it cannot be tampered. Blockchain proves an immutable and indisputable mechanism to verify that the data of the information or transaction or asset has existed over time.

[19] Grech, A. & Camilleri, A. (2017). Blockchain in Education, JRC Study pg.21

e. Disintermediation

When a person in India buys a product with Indian Rupee as the medium of exchange the buyer and the seller both trust the issuer of the Indian Rupee, in this case the Reserve Bank of India (RBI). This makes the RBI an intermediary that issues and controls the value and supply of the Indian Rupee. Over the years, the long term effect of centralisation has had an adverse effect on the economics of the world on numerous occasions such as the Great Depression, 2008 Sub-Prime Crisis, Greek Economic Crisis.

Satoshi Nakamoto, in his white paper, described in detail how the disintermediation of a currency would take place, the issuance mechanism and validation, such that no participant on the blockchain depends on a centralised authority, but rather entire network as a whole.

On a broader sense, thinking about disintermediation of facets other than currency issuance brings out interesting cases and scenarios as the need for centralised dependence is removed. With the peer-to-peer blockchain technology, consensus algorithm verify transactions eliminating the need for a third party. Overhead costs could drastically be reduced and the ascertainment of ownership would be instant.

"Every member in the community transacts with mutual trust within the community."[20]

iii. Distributed Ledger Technology (DLT)

A distributed ledger is essentially a record of information, or database that is shared across a network. It may be an open, publicly accessible database or access may be restricted to a specified group of users. From a technical perspective it can be used, for example, to record transactions across different locations. The technology that makes this possible is often referred to as "blockchain". The name comes from the fact that DLT solutions store all individual transactions in groups, or blocks, which are attached to each other in chronological order to create a long chain. This long chain is put together using a mathematical formula – complex cryptography – which ensures the security and integrity of the data. This chain then forms a register of transactions that its users consider to be the official record.

Record-keeping has always been a centralized process that requires trust in the record keeper. The most important innovation of DLT is that control over the ledger does not lie with any one entity but is with several or all network participants – depending on the type of DL. This sets it apart from other technological developments such as cloud computing or data replication, which are commonly used in existing shared ledgers.

[20] Quote by Andreas M Antonopoulous, MOOC 8 organised by the University of Nicosia

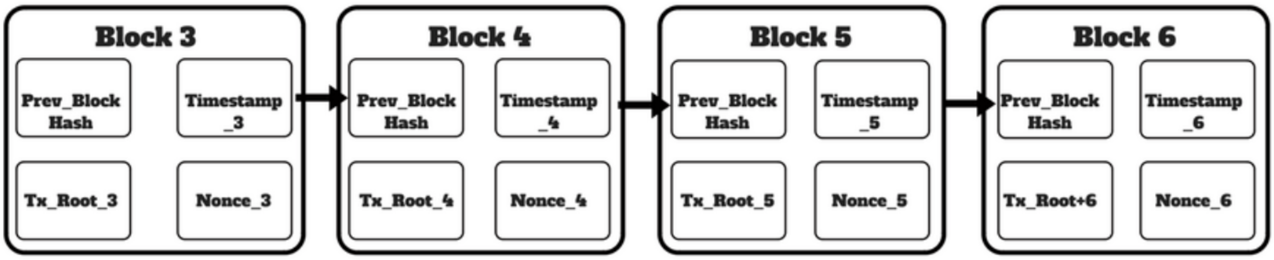


Figure 4.6: Components of a Block

De facto, this means that in a DL, no single entity in the network can amend past data entries in the ledgers and no single entity can approve new additions to the ledger. Instead, a pre-defined, decentralized consensus mechanism (see below) is used to validate new data entries that are added to the blockchain and thus form new entries in the ledger. There exists, at any point in time, only one version of the ledger and each network participant owns a full and up-to-date copy of the entire ledger. Every local addition to the ledger by a network participant is propagated to all nodes. After validation is accepted, the new transaction is added to all respective ledgers to ensure data consistency across the entire network.

V. Blockchain Use Cases

V. Blockchain Use Cases

Disruptive means of innovations are coming up every day. Blockchain with all its potential promises to be the job disruptor of all time, but at the same time, the efficiency and improvements it promises, and could bring in more and more ideas that are to be developed. A 2016 study by a group of researchers stated about 118 sectors or areas that Blockchain could provide assistance to. Any medium that requires data recording, but is limited by a centralized storage authority can easily be replaced using the Blockchain to reduce intermediation and threats of data tampering.

Following are some of the cases that have already been established by the Blockchain sector. Certain improvements are also suggested.

i. Non-intrinsic Monetary Value

"The Intrinsic Value of an asset or a currency is the actual value of that asset or currency based on the underlying perception of its true value in both tangible and intangible terms."[21]

If the Indian Rupee is traded on a global currency exchange, it derives its value from the Issuer of that currency, here being the RBI that honors the exchange of Indian Rupee as a monetary value. If a Gold Option derivative is being traded at the MCX, it derives its intrinsic or "true value" from physical gold that forms the underlying asset of the derivative. Same is the case with Stocks, Debentures, ETFs, Bonds, and SDRs etc. All of these instruments derive their intrinsic value from an underlying asset in the form of a business or commodity or even liquid cash.

With the first block being mined by Satoshi Nakamoto on January 21, 2009, Bitcoin became the first *exchange of value* in history to be backed by nothing other than the mutual trust between the users of the network. The value of Bitcoin gains only because the participants of the bitcoin network that think of it as undervalued. Thus, for the first time in economic history, an asset with no intrinsic value was brought into existence. A new asset class was formed, an asset that has no intrinsic value but also is a medium of exchange based on mutual trust.

[21] The intrinsic value is the actual value of a company or an asset based on an underlying perception of its true value including all aspects of the business, in terms of both tangible and intangible factors. This value may or may not be the same as the current market value. (Investopedia)

a. Remittance Mechanism

Because of Bitcoin being a non-intrinsic asset class, intermediaries involved in the transfer of the asset are also exponentially reduced, making it an ideal mechanism for remittance or transfer of value among the participants.

In the book "Blockchain Revolution" by Don & Alex Tapscott, they put down a real scenario over long distances. In the traditional system, a fund transfer for a Philippine immigrant would have taken 3 hours of her working time, loss of 5-7% in exchange and transaction cost, pass through 6-9 clearing banks and wait 2-5 working days for it to reach her family. But the same process on the Ripple[22] (XRP) cryptocurrency requires only both participant having a smart phone where the immigrant can transfer some money in a secure and fast way to her family within a second and the family could have it exchanged for the local currency. This entire process happened in an efficient way when compared to the traditional money transfer system and at the same time at the fraction of the cost.

ii. Digital Certification

Certification in a broad sense is the verification of a claim, presented by a person as a validation of their declared information issued by an authority recognised as an issuer of the claim. A Digital Certificate is the same validation of a claim done in a virtual sense. A Digital Signature involves the process of security identifying the claim with the use of Private Key Infrastructure.

In the pre-blockchain era, the issuance would reside within the hands of the issuer, deemed to be worthy of issuing a claim.

a. Components of Digital Certificate

A digital signature contains the following:

- A Hash Function
- A Private Key
- A Public Key
- Timestamp

[22] Ripple is a real-time gross settlement system (RTGS), currency exchange and remittance network created by the Ripple company. Also called the Ripple Transaction Protocol (RTXP) or Ripple protocol, it is built upon a distributed open source Internet protocol, consensus ledger and native cryptocurrency called XRP

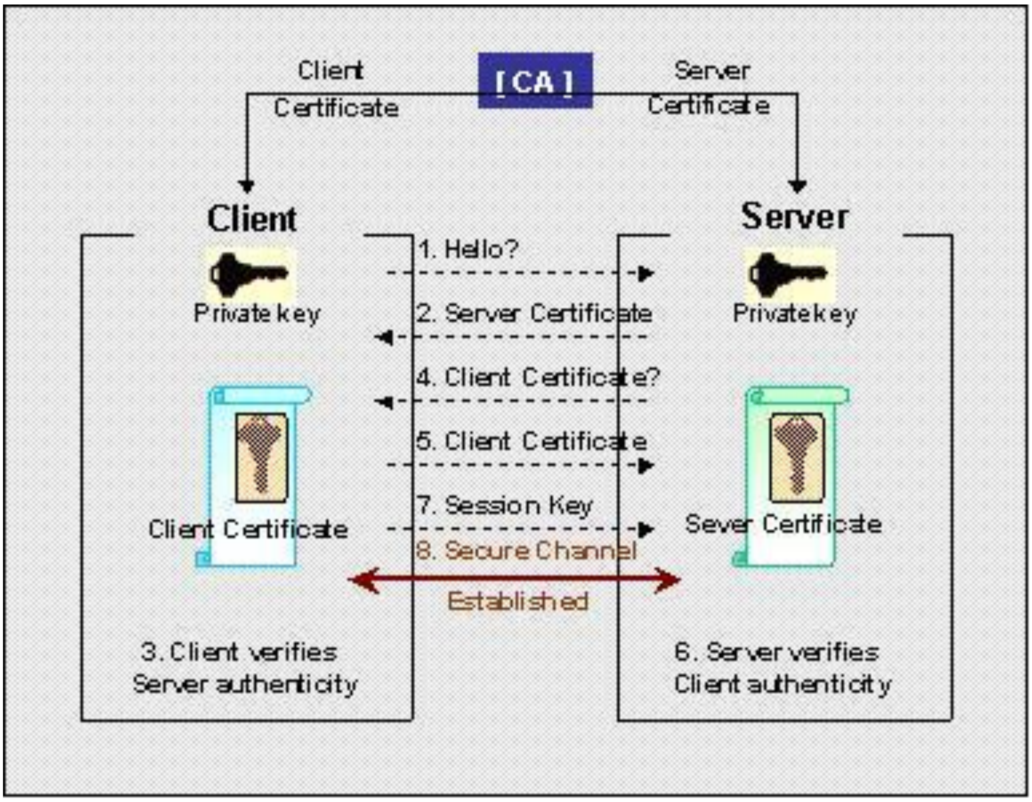


Figure 5.1: How are digital certificates issued?

Source: https://tender.eprocurement.gov.in/DigitalCertificate/faqs/gfaqs.htm

1. Hash Function

A hash function is a mathematical algorithm that maps data and is designed to be a one-way function. Hashing is a cryptographic technique that involves randomizing a string of data into a described set of random alphanumeric characters. A hash function is also called a one-way function, which means that a random string of data can be obtained by applying a hash function to the given data, but not the other way around. It is computationally infeasible to reverse a hash function in order to find the actual data.

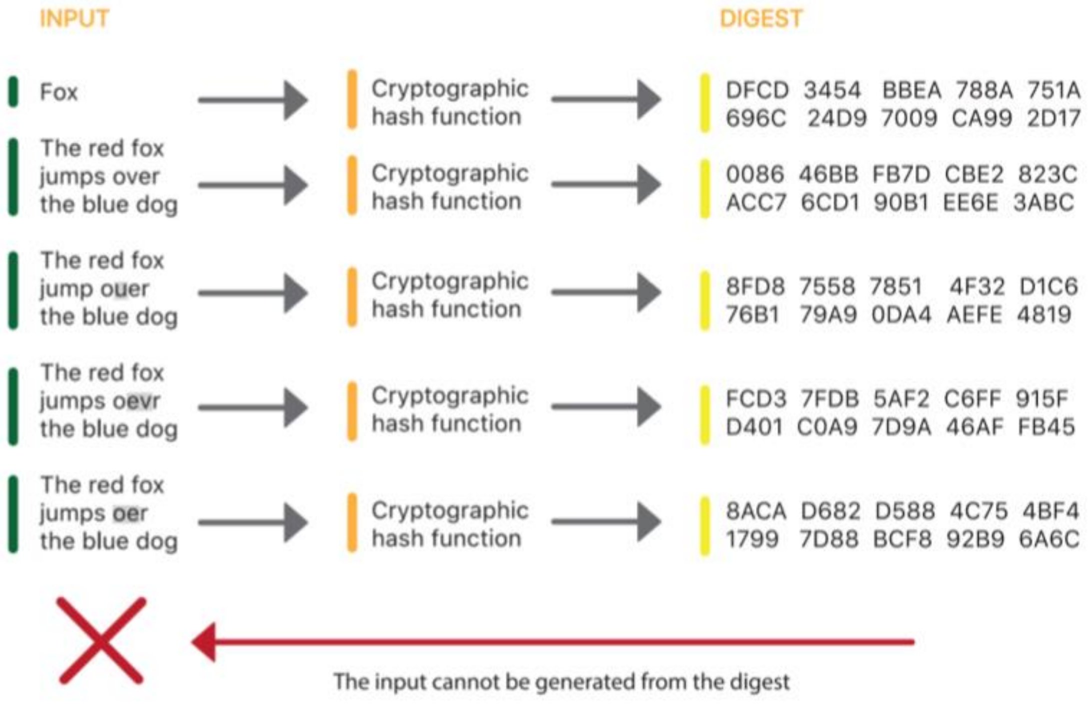

INPUT
DIGEST
Fox
The red fox jumps over the blue dog
The red fox jump ouer the blue dog
The red fox jumps oevr the blue dog
The red fox jumps oer the blue dog
Cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C
The input cannot be generated from the digest

Figure 5.2: Hash functions

Source: https:://commons.wikimedia.org/wiki/

If the hash of a data alone is distributed, then a verification process of the data just needs to give back the same hash code. This process is extensively used in password verification by websites, secure transfer of encrypted messages etc.

2. Private keys

In cryptography, a private key (secret key) is a variable that is used with an algorithm to encrypt and decrypt code. Quality encryption always follows a fundamental rule: the algorithm doesn't need to be kept secret, but the key does. Private keys play important roles in both symmetric and asymmetric cryptography.

A private key in the context of Bitcoin is a secret number that allows bitcoins to be spent. Every Bitcoin wallet contains one or more private keys, which are saved in the wallet file. The private keys are mathematically related to all Bitcoin addresses generated for the wallet.

Because the private key is the "ticket" that allows someone to spend bitcoins, it is important that these are kept secure. Private keys can be kept on computer files, but in some cases are also short enough that they can be printed on paper.

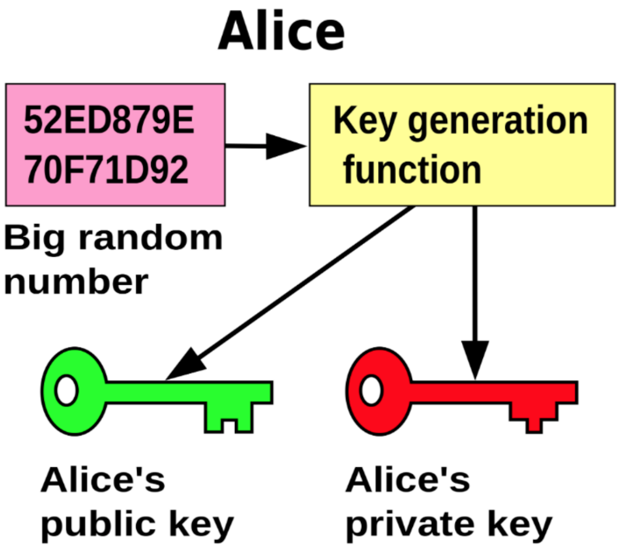


Figure 5.3: Alice's Keys

3. Public keys

The Public Key is what its name suggests - Public. It is made available to everyone via a publicly accessible repository or directory. On the other hand, the Private Key must remain confidential to its respective owner.

Because the key pair is mathematically related, whatever is encrypted with a Public Key may only be decrypted by its corresponding Private Key and vice versa.

For example, if Bob wants to send sensitive data to Alice, and wants to be sure that only Alice may be able to read it, he will encrypt the data with Alice's Public Key. Only Alice has access to her corresponding Private Key and as a result is the only person with the capability of decrypting the encrypted data back into its original form.

As only Alice has access to her Private Key, it is possible that only Alice can decrypt the encrypted data. Even if someone else gains access to the encrypted data, it will remain confidential as they should not have access to Alice's Private Key.

4. Time stamping

When the date and time of an event is recorded, we say that it is time stamped. A digital camera will record the time and date of a photo being taken, a computer will record the time and date of a document being saved and edited. A social media post may have date and time recorded. These are all examples of a timestamp.

Timestamps are important for keeping records of when information is being exchanged or created or deleted online. In many cases, these records are simply useful for us to know about. But in some cases, a timestamp is more valuable. Such as the transfer of monetary value, asset transfer or issuance, etc.

On the Bitcoin blockchain, When you timestamp a file, your computer creates a unique identifier, or *fingerprint*, for the file (a SHA Hash). The fingerprint is a unique number calculated from the file's contents.

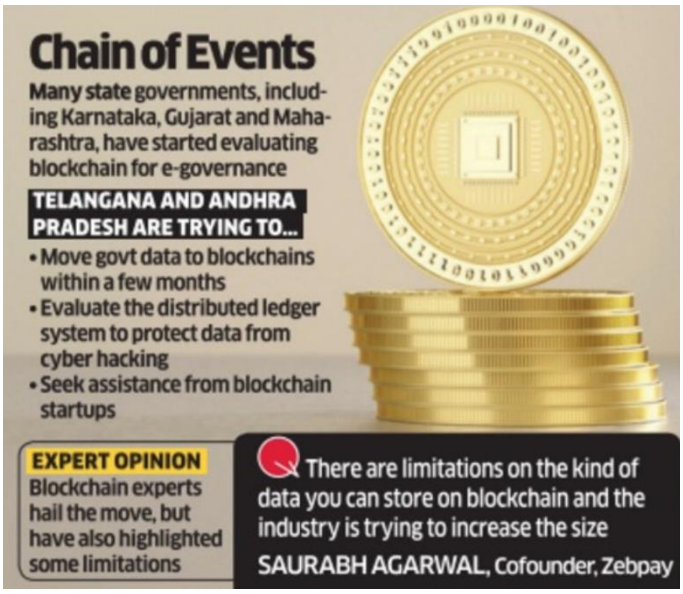
The issuance of Digital on the Blockchain removes the one drawback of Digital certificates since their inception, i.e., the removal of any hindrance that could be caused by the issuer or any party that could get their hands on the issuer. Blockchain along with Digital certifiedates proves to be virtually secure as the immutability of Blockchain becomes cryptographically linked to the Private-Public key mechanism of Digital Certificates. The Distributed Ledger Consensus Algorithm of Blockchain allow Digital certificated to be easily scalable, cost effective, immutable and instantly verifiable.

Digital certificates issued on the Blockchain could revolutionise the Academic sector as further evaluative thinking pushes toward linking all academic qualifications and ascertains, both formal and informal, by hashing them to the Blockchain to collectively form an individual Blockchain identity, as will be talked about in further chapters.

b. Uses of Blockchain based Digital Certificates

1. Property Transfer

Consider a scenario where XYZ is a citizen of a particular state that is governed by its own law, and has 2 land titles registered under his name. These titles, as the citizen recalls, were attained through huge red-taoism and corruption passage within the State authorities. A certain period later, am effort within the State led to the old Governance being overthrown by a new one that decided to scrap away the old ownership titles of Land and give away the Properties to its loyal subjects. Thus, all old owners were banished from their own land that they worked hard to attain.



Chain of Events

Many state governments, including Karnataka, Gujarat and Maharashtra, have started evaluating blockchain for e-governance

TELANGANA AND ANDHRA PRADESH ARE TRYING TO...

- Move govt data to blockchains within a few months
- Evaluate the distributed ledger system to protect data from cyber hacking
- Seek assistance from blockchain startups

EXPERT OPINION

Blockchain experts hail the move, but have also highlighted some limitations

There are limitations on the kind of data you can store on blockchain and the industry is trying to increase the size

SAURABH AGARWAL, Cofounder, Zebpay

Figure 5.4: Source: Blockchain tech is joining e-gov dots in AP, Telangana https://economictimes.indiatimes.com/small-biz/security-tech/technology/blockchain-tech-is-joining-e-gov-dots-in-ap-telangana/articleshow/59330625.cms

Once again, Blockchain comes to the rescue. The Indian State of Andhra Pradesh (AP), under the leadership of the Chief Minister Dr. Chandra Babu Naidu, realised the problem of scrabble ownership by change of Governance. Thus, the State decided to put their resources towards I'mmutable authentic ownership establishment, along with the abolishment of corruption and reduction in registration and transfer processes. The AP Government, under the guidance of Mr. JA Chowdary, Chief Security and IT advisor to the Chief Minister said, "The current system is rifle with corruption."[23] While referencing the traditional system of ownership or transfer in property.

The AP Government partnered with a Swedish start-up Chroma-way[24] to use '*Digital Ledger Technology to stores data in vast groupings allowing encrypted and tamper-proof data storage.'* This will make ownership ad transfer of Properties linked to the Blockchain to be immutable and free from any form of corruption.

2. Digital Assets

A Digital Asset in a virtual sense, is data existing in binary form and involves the right to use. Any data that does not involve this right does not constitute to be a Digital Assets. A Digital asset can be, but not exclusive to:

[23] CNBC interview with JA Chowdary in 2017, (https://www.cnbc.com/2017/10/10/this-indian-state-wants-to-use-blockchain-to-fight-land-ownership-fraud.html)
https://chromaway.com

- Digital Documents
    - Software Code
    - Patent
    - Spreadsheets
- Audible Content
- Motion Content
- Pictured Content

A Digital Asset is usually stored on applications such as:

- PCs
- Mobile devices
- Hardward wallets[25]
- Media Devices
- Detachable Storage Devices

A Digital Asset in the traditional management system would be issued by an issuing authority, responsible for maintaining the claim of the Asset. This technique suffers from various limitations relating to storage, security and transfer.

c. Limitations of traditional digital certificate

- Lack of Guidance Framework by Law
- Transferability of the Asset
- Inheritance of Digital Asset after death or other unforeseen circumstance
- Maintenance of Record under single authority
- No limitation on the ability of the issue to alter details or include fraudulent information

d. Digital Certificates on the Blockchain

Solutions achieved through Blockchain and Digital Asset integration

- Authentication and historical ownership tracking of the asset becomes easier and cost effective
- Duplication of certificates or Asset claims is not feasible as each certificate or claim carries its own unique identifying Hash

[25] A hardware wallet is a special type of digital asset wallet which stores the user's private keys in a secure hardware device. (bitcoin.wiki.com)

- Documentations of Assets for processes such as auditing, accounting and verification is readily available as all information is public and immutable
- Cross-verification and validation through physical means becomes unnecessary, unless in extreme cases, as all data pertaining to a particular hash is easily accessible through the Open nature of Blockchain
- Use of Smart contract based Digital Certification will allow for increased efficiency and operability within Institutions

iii. Tokenization

Tokenization is a relatively new concept that was paved way by advancements to Blockchain technology. *'Tokenization refers to the process of monetising the ownership or utility, or in some cases both, the work of a representative that drives value to that Blockchain based token.'* THe process of tokenisation is similar to the traditional Share certificate in the same way a Cat Is similar to a Lion. One paved way to the other through continuous evolution.

A Blockchain based *Token* is only similar to a traditional share in a way that the representative can issue Blockchain based tokens as ownership rights, in exchange for funds. But a token is not just limited to ownership. These tokens are secured and authenticated thought the Blockchain they are based on, and honoured periodically through the use of Smart Contracts (Discussed later in Contracts chapter), a term coined by futurist Nick Szabo and taken up extensively by Vitalik Buterin[26] and his foundation, Ethereum.

A token issuer can also choose not to issue the token as an ownership certificate, but as a token that represents a fuel to drive the network. *A utility token is a token extracting its derived value from a parent blockchain or blockchains, to create a community transacting with that token.*

(a) Storj - Decentralized Storage

Storj[27] is a Blockchain based startup developed by engineer *Shawn Wilkinson* who was introduced to the concept of decentralisation. They formulated a concept of decentraliseding the storage part of the Internet, thus eliminating the whole concept of centralised storage servers (The likes Google and Amazon cloud services) that are continuously prone to external attacks.

[26] Co-founder of Ethereum, http://fortune.com/40-under-40/vitalik-buterin-10/

[27] https://storj.io

Figure 5.5: Storj Logo

The concept of Storj revolves around securely storing, parts and pieces of provided data around all participants of the Storj network and rewarding the participants for storing data in the network's Storj token. Any participant that wishes to store data online and secure can do so on the Storj network by remunerating the participants for storing the data in the networks token.

The Storj token is based off of the Ethereum Blockchain that utilises the concept of smart contract for continuously enumerating and collecting the Storj token for the participants. The Storj token happens to fuel the network into decentralised storage by providing an incentive. Again, the value of that Storj token is derived from the importance it receives from its network.

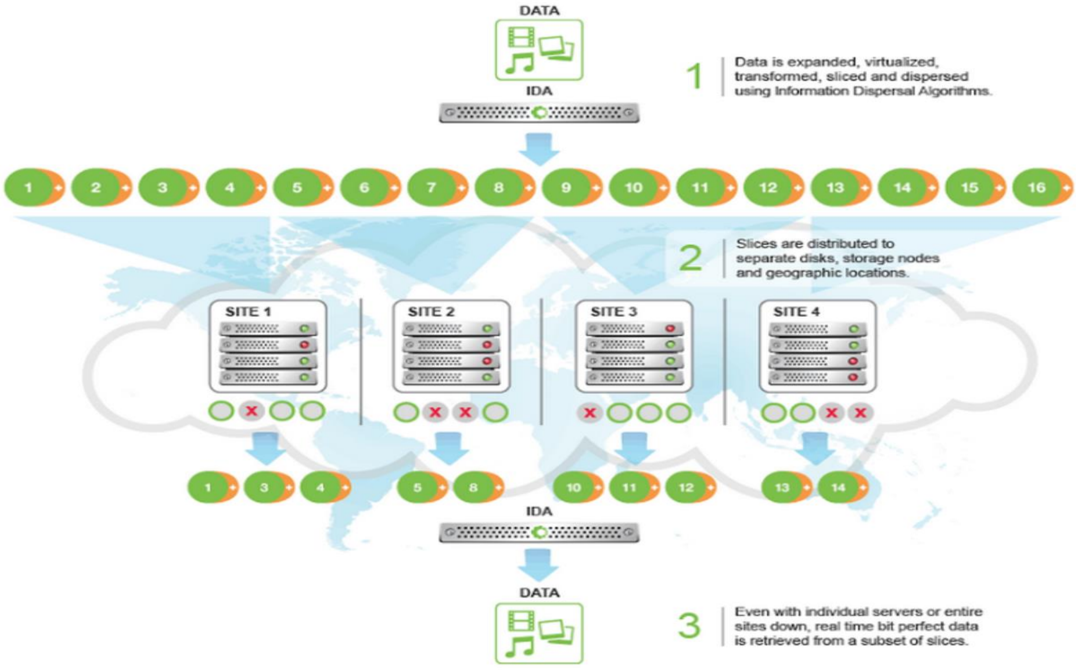

DATA
IDA
1
Data is expanded, virtualized, transformed, sliced and dispersed using Information Dispersal Algorithms.
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
2
Slices are distributed to separate disks, storage nodes and geographic locations.
SITE 1
SITE 2
SITE 3
SITE 4
1 3 4 5 8 10 11 12 13 14
IDA
DATA
3
Even with individual servers or entire sites down, real time bit perfect data is retrieved from a subset of slices.

Figure 5.6:Distribution of Data on a storage-based blockchain network

Source: http://blockchained.blogspot.in/2015/03/

iv. Accounting

The use of digital means for recording accounting entries is still in its infancy compared to other sectors adopting digitalization. Some sectors have even managed to be totally disrupted by digitalization. The accounting profession is broadly concerned with the measurement and communication of financial information, and the analysis of said information. Much of the profession is concerned with ascertaining or measuring rights and obligations over property, or planning how to best allocate financial resources.

Modern Financial is based on the Double-Entry Bookkeeping system that revolutionized the field of recording accounting transactions. The auditors and managers found a way to keep trust between books. However, public independent auditors have to be appointed as a necessity to verify the financial information and trust on a bigger scale.

The possibility provided by the use of blockchain may represent the next step for accounting practices as it could provide a “joint, distributed ledger that is cryptographically sealed”[28] instead of keeping separate records that are based on receipts and rely on physical verification. For accountants using blockchain, it could provide more clarity over ownership of assets and existence of obligations, and could dramatically improve efficiency.

The entire process of physical verification or periodical reconciliation is removed with the implementation of Blockchain into an organization. The operational efficiency and institutenal transparency (both internal and external) is highly increased with digitalising the accounting records. All transaction within an organisation can be easily audited and submitted to the regulatory authorities, with the highest level of transparency.

Blockchain based ledger transaction simply the trail process as it enables the recording of transactions in a way that leads to transparency and operational efficiency.

Blockchain is a replacement for bookkeeping and reconciliation work. This could threaten the work of accountants in those areas, while adding strength to those focused on providing value elsewhere. For example, in due diligence in mergers and acquisitions, distributed consensus over key figures allows more time to be spent on judgemental areas and advice, and an overall faster process.

[28] Delloite Accounting and Blockchain Study

a. Audit Trail

The physical verification of the accounting entries of large organisations takes up a lot of resources and man-hours as all or certain documents relating to all transactions have to be verified by the Auditors to ensure ethical practices have been maintained. With the introduction of a Blockchain based accounting system within an organisation, the mandatory physical verification of all or a set of transactions becomes redundant as all verification could be easily done with the open-ledger of the Blockchain, where all entries are cryptographically verified.

The reduction in the need for reconciliation and dispute management, combined with the increased certainty around rights and obligations, will allow greater focus on how to account for and consider the transactions, and enable an expansion in what areas can be accounted for. Many current-day accounting department processes can be optimised through blockchain and other modern technologies, such as data analytics or machine learning; this will increase the efficiency and value of the accounting function.[29]

v. IoTs

The Internet of Things (IOT) is a concept given by the Internet itself that expresses a harmony between a network of physical devices, vehicles, home appliances and other items embedded with electronics, softwares, sensors, and network connectivity which enables these objects to connect and exchange data.

Internet of Things
30

Figure 5.7: IoTs

Each IoT device is uniquely identifiable through its embedded computing system but is able to inter-operate with existing Internet structure. “Simply put, the IoT is a concept connecting any device with an on and off switch to the Internet.”[30] Everything from cellphones to lamps to wearable devices can talk to each other with their connection through the Internet.

[29] Blockchain and the future of accountancy (https://www.icaew.com/en/technical/information-technology/technology/blockchain/blockchain-and-the-accounting-perspective)

[30] https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#62193c8e1d09

The IoT devices that the Internet got together is building can install intelligence into existing infrastructure such as a power grid, a wired fence or dustbin, by adding smart devices that communicate with one another, can adjust the configuration, or even resist interruption. Don Tapscott said, "The Internet of Things needs a Ledger of Things"[31] IoTs could benefit enormously from a network able to complete high volumes of minute transaction. A smart device could probably "pay for its assembly, its maintenance, its energy and also for its liability insurance by giving its data, power, storage or service to other machines.

Turns out, Blockchain, the first open source ledger technology is critical to the future of IoTs. The element of Blockchain that makes it a vast, global distributed ledger or database running of millions of devices through mass collaboration and clever code. The IoT depends on LoT to track everything, ensure reliability, immutability and transparence, and pay for its contribution. The potential that IoT promises, through its integration with the Blockchain network surpass innovative disruptive bounds.

The cryptocurrency IOTA[32] developed by software engineer Serguei Popov[33] was formed for the main purpose of allowing seamless flow of data and transaction between micro devices that facilitates fee-less mechanism with a verification concept termed the Tangle[34]. As per Sergei himself, "Tangle is a form of Directed Acyclic Graphs[35] that naturally succeeds the Blockchain as its next evolutionary step, offers features that are required to establish a machine-to-machine micropayment system."

vi. Data mining

Data Mining is the process of discovering patterns in large data sets involving methods at the intersection of machine learning, statistics, and database systems. In computing systems, data mining is an important or essential process where intelligent methods and concepts are applied to extract data patterns. The long standing goal of data mining is to extract information from a data set and transform it into an understandable structure for further use. The analysis process in the "knowledge discovery in databases" (KDD Concept)

[31] Quote by Don & Alex Tapscott, in the book "Blockchain Revolution"

[32] IOTA Crypto currency (https://iota.org/IOTA_Whitepaper.pdf)

[33] https://blog.iota.org/@serguei.popov

[34] IOTA uses 'exclusively quantum resistant cryptographic algorithms' which are immune to this brute force attack (unlike current blockchain projects)called the Tangle that decreases impact of a Quantum consensus attack by 1 million times. Tangle is considered as an upgrade to the Blockchain.

35 A directed acyclic graph (DAG) is a directed graph that contains no cycles. A rooted tree is a special kind of DAG and a DAG is a special kind of directed graph. For example, a DAG may be used to represent common subexpressions in an optimising compiler.

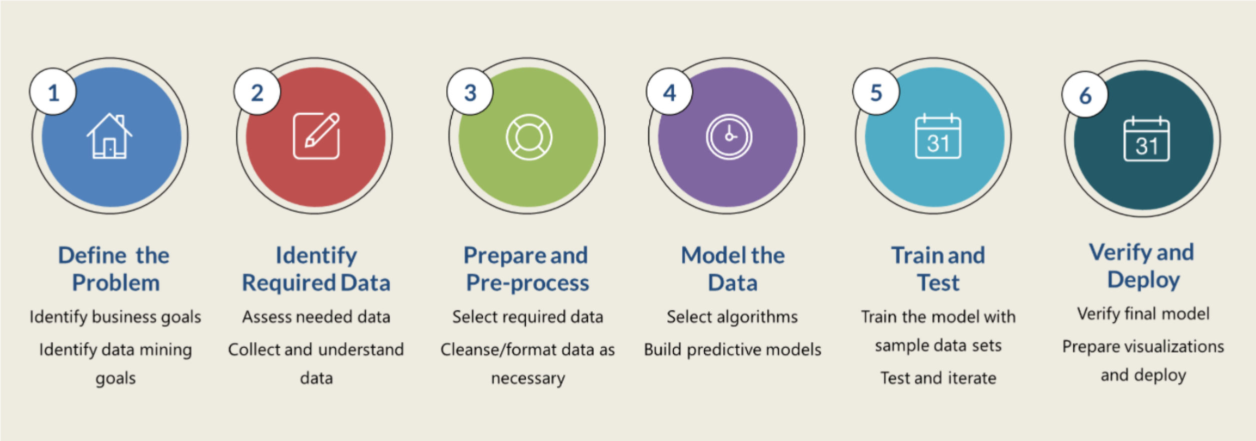


Figure 5.8: Source: Steps in Data Mining

https://digitaltransformationpro.com/data-mining-steps/

The importance of raw data; data about information relating to the end user was realized by organisations. This orang a whole new era of research and man-hours spent on data mining techniques and concepts so as to make interpretation of data in a clear and elaborate form.

a. KDD Process of Data Segregation

- Data Cleaning − the noise and inconsistent data is removed.
- Data Integration− multiple data sources are combined.
- Data Selection − data relevant to the analysis task are retrieved from the database.
- Data Transformation − data is transformed or consolidated into forms appropriate for mining by performing summary or aggregation operations.
- Data Mining − intelligent methods are applied in order to extract data patterns.
- Pattern Evaluation − data patterns are evaluated.
- Knowledge Presentation − knowledge is represented

b. Blockchain and Data Mining

"A blockchain is an open-source, distributed ledger that can record exchange of information between parties within a network." The recording of information along with the source property of Blockchains, allows it to be analysed in a paradigm of new ways. Blockchain use in data mining processes can promise greater confidence in the integrity of the data, Immutable ledger entries that are consensus-driven and time-stamped can give certainty of origin of data.

- The inherent immutability of Blockchain leads to more confidence in training and testing of data models produced.

- Cost of data storage could be a huge impact. The disinterredation and distribution of storage servers allows the cost of intermediation to be eliminated in its entirety.
- As Blockchain data analytics forwards, concepts of big data could be seen shifting from proprietary data silos to Blockchain-enabled data layers. The powers would finally end up with people who can collect data not with people who own the data.

Cloud computing is a $247 billion dollar market that is dominated by the likes of Amazon, Google, and Microsoft. The major players offer centralized computing for a variety of uses ranging from backing up your company's data to producing big data analytics remotely. However, there has been an interest in decentralized cloud computing as a cheaper option for businesses that cannot afford the prices set by incumbent providers.

vii. Voting

Through years of Governance, innovative and political thinking, and after witnessing magnitudes of regime changes, the concept of Voting was developed. "Voting is a method for a group, such as a meeting, elaborate decision making, usually following discussions, debates or campaigns."[36] The collective opinion expressed by a body or a specified group is indicted through voting.

Over the years, even though continuous innovation has been taken place to reduce the advent of corruption, a consistent track of manipulation in voting processes by oppressing the ideas or opinions of the mass by the few. Arguments have been raised about the drawbacks and limitations that traditional voting process carry that has kept the expression part hindered through mass manipulation by the few. Existing models for collaborative decision making once served our growing democracies well, yet today they are increasingly slow, expensive, and ineffectual. Public trust in their outcomes is eroding and results in voter apathy. All societies are hurtling into the future, but the democratic processes are stuck in the past, failing to advance at the same pace.

Figure 5.9: Logo of Horizon State

[36] dictionary.com

Voting methods such as tactical voting[37], Electoral Voting[38], paper-ballots[39] have been developed to reduce the hindrance of corruption, but large entities with sufficient resources, strategically manage to utilize the flaws of these methods. The existence of voting as a form of group expression has never represent itself in its true form. The execution and analyzing of voting has always managed to be centralized.

Having realised the need for a distributed information system, fast and secure enough to bring real-time results possible, without outside interference, Jaime Skella[40] decided to come up with an idea to integrate the core concepts of Blockchain in the Voting process, through his start-up Horizon State[41], that aims at "…. creating a more transparent, trustworthy, and democratic future….". Using a token-based Blockchain system, the HST (Horizon state) team have created a secure, anonymous, convenient and affordable voting Platform.[42]

viii. Health and medicine

The extended vision for blockchain to disrupt healthcare in the future would solve many issues that hinder and plague the industry today to create a common database of health information that doctors and providers of health information could access no matter what electronic medical system they are under; higher security and privacy and less administration time for doctors so there's more time to spend on patient care, rather than time spent on diagnosis. This will promote better sharing of research results.

Between 2015 and 2016, 140 million patient records were breached according to Protenus Breach Barometer report. With the growth of connected devices and the Internet of Medical Things (IoMT), existing health IT architecture is struggling to keep systems secure. Blockchain solutions have the

[37] In voting methods, tactical voting (or strategic voting or sophisticated voting or insincere voting) occurs, in elections with more than two candidates, when a voter supports another candidate more strongly than their sincere preference in order to prevent an undesirable outcome. (independent.co.uk)

[38] Electoral vote definition, the vote cast in the electoral college of the U.S. by the representatives of each state in a presidential election. (dictionary.com)

[39] A ballot is a device used to cast votes in an election, and may be a piece of **paper** or a small ball used in secret voting. (dictionary.com)

[40] Jaime Skella, Co-founder of Horizon State. (https://medium.com/@jamieskella)

[41] Horizon State has built a token-based blockchain voting and decision-making platform that delivers unprecedented trust through the integrity and post-unforgeable attributes of blockchain technology. Horizon State delivers a secure digital ballot box that cannot be hacked, wherein results can never be altered, and voter identities are protected. (https://horizonstate.com)

[42] Talk by Jaime Skella at Decentralized'17 conference, Cyprus

potential to be the infrastructure that is needed to keep health data private and secure while reaping the benefits of connected medical devices.

“Although blockchain technology is currently changing the healthcare industry, keep in mind this is a marathon, not a sprint.”[43]

a. Conversation with Bryant Joseph Gilot[44]

Bryant Joseph (MD CM DPhil MSc) is a medical practitioner. While practicing in Philadelphia, he developed a passion for the innovative field of blockchain technology. In 2014, he enrolled into the online, long-distance MSc in Digital Currency programme at the University of Nicosia. Bryant, among a handful of participants, became one of the first graduates in the world with a degree in blockchain technology, he combined his medical career with his passion to chase a new dream. Presently, Bryant works as the Chief Medical Officer at Blockchain Health Co.[45], headquartered in San Francisco. Bryant now lives in Tübingen, Germany where he is pursuing his research at the University of Tübingen. Bryant managed to attend the first Decentralized ’17 conference[46], hosted by the University of Nicosia, who Bryant is closely associated with, in Limassol, Cyprus.

Figure 5.10: Logo of BlockchainHealth

At the Decentralised - 2017 Conference held at Limassol, Cyprus a discussion with Bryan Joseph Gilot about his startup Blockchain Health was possible. Bryant extensively explained how his startup was trying to revolutionise the Health industry through his and his team’s knowledge in Blockchain and keeping in mind their medical background.

His startup, Blockchain Health, mainly aims to provide a detailed history of each person’s medical record wherein every person is extensively diagnosed and all their records are securely updated on a

[43] This Is Why Blockchains Will Transform Healthcare (https://www.forbes.com/sites/bernardmarr/2017/11/29/this-is-why-blockchains-will-transform-healthcare/2/#3fc846ef229d)

[44] Conversation with Bryant Joseph Gilot at Decentralized ’17, Cyprus where Bryant answered questions relating to his contribution to the Health industry with extensive Blockchain knowledge.

[45] Blockchain Health (https://www.blockchainhealth.co)

[46] https://www.unic.ac.cy/events/decentralized-2017

distributed database system (Blockchain) so that the next time a new patient has similar diagnosis, he could be provided with the detailed historical records of series of patients and the best treatment could be made swiftly available.

This could also be used in the research field wherein new doctors could get access to information needed with the help of the distributed database and patients can be remunerated for their contributed of their data through the use of medical smart contracts.

ix. Identity management

Identity management (ID management) is the organizational process for identifying, authenticating and authorizing individuals or groups of people to have access to applications, systems or networks by associating user rights and restrictions with established identities. The managed identities can also refer to software processes that need access to organizational systems. Organisations have realised the importance of segregation of data, thus maintain separate records of data for each Identity, helping them to manage their outcome in a strategic way.

An identity and access management (IAM) system can provide a framework that includes the policies and technology needed to support the management of electronic or digital identities.

Many of today's IAM systems use federated identity, which allows a single digital identity to be authenticated and stored across multiple disparate systems.

The problem with Identity Management on a digital scale lies with the centralisation of data storage as organisations with data on identity of individuals, for example UIDAI, can be manipulated or stolen by third parties with enough resources.

Numerous scams and identity thefts have occurred through digital data history. Blockchain. Here aims to provide a solution with its core concept such as distributed data, disintermediation and transparency.

a. Example of Identity Management Mechanism

Just as the digital certificate management was explained in the previous chapter the same concept, on a broader scale, can be applied on an individual’s identity. Each individual can have his identity hashed on the blockchain where all his data is stored securely on the distributed ledger and his identity could be managed so that any party wanting to access his data would have to seek individual’s permission; or the individual can customise his data in a way different organisations or parties would view the data only relating to their interests.

x. Irrefutable Digital Contracts

The concept of Irrefutable Contracts was brought forward by **Nick Szabo** in his technical paper in 1994. Szabo went on to explain how the concept of irrefutable contracts, or in his words smart contracts, can be applied on a digital sense wherein two or more interested parties could get into a contract that is obligated by a software. This concept wasn't given much importance back then as no application could be designed that could successfully perform what Szabo envisioned.

"Like regular contracts where after reaching an agreement parties must execute the contract, for it to take place, a smart contract is self-executing. With the introduction of Smart Contracts, a whole new ecosystem of technical automation is introduced with a new social fabric that enables civil efficiencies, personal mobility and institutional information."[47]

If such a platform is centralized – like Kickstarter[48], for instance – then it acts as a third party between product teams and supporters who donate their money. This means both sides need to trust Kickstarter and, in fact, pay an additional fee to Kickstarter to serve as an intermediary.

Jumping forward 20 years, with the introduction of Ethereum, Vitalik Buterin reignited the concept of **Smart Contracts** by integrating it with the blockchain. Adding the core concepts to the blockchain, with the vision of Nick Szabo Ethereum made possible a contract wherein two parties when mutually obligated to honor their side of the agreement.

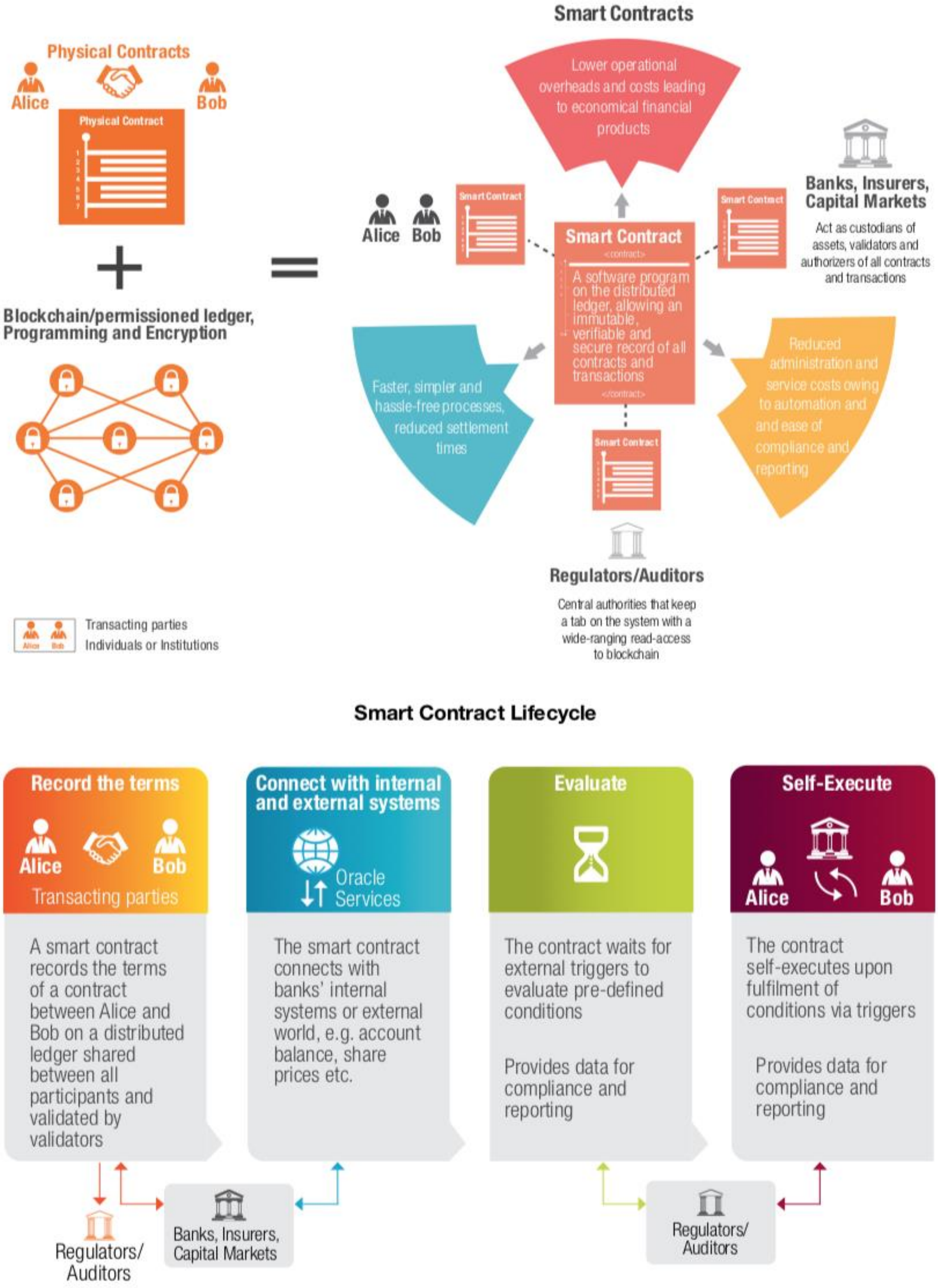
Smart contracts have been designed to automate transactions and allow parties to agree with the outcome of an event without the need for a central authority. Key features of smart contracts are:

- A smart contract automatically executes based on programmed logic.
- Multi-sig allows two or more parties to the contract to approve the execution of a transaction.
- Independently – a key requirement for multi-party contracts.
- Programmability, multisig authentication escrow capability and oracle inputs[49]
- External inputs such as prices, performance, or other real-world data may be required to process a transaction, and oracle services help smart contracts with inputs such as these:

[47] European Commission, Joint Research Commission Study (2017), Smart Contracts, pg 22.

[48] Kickstarter is an American public-benefit corporation based in Brooklyn, New York, that maintains a global crowdfunding platform focused on creativity.

[49] An oracle, in the context of blockchains and smart contracts, is an agent that finds and verifies real-world occurrences and submits this information to a **blockchain** to be used by smart contracts. Smart contracts contain value and only unlock that value if certain pre-defined conditions are met. (https://blockchainhub.net/blockchain-oracles/)



Lower operational overheads and costs leading to economical financial products

A software program on the distributed ledger, allowing an immutable, verifiable and secure record of all contracts and transactions

Act as custodians of assets, validators and authorizers of all contracts and transactions

Faster, simpler and hassle-free processes, reduced settlement times

Reduced administration and service costs owing to automation and and ease of compliance and reporting

Central authorities that keep a tab on the system with a wide-ranging read-access to blockchain

A smart contract records the terms of a contract between Alice and Bob on a distributed ledger shared between all participants and validated by validators

The smart contract connects with banks' internal systems or external world, e.g. account balance, share prices etc.

The contract waits for external triggers to evaluate pre-defined conditions

Provides data for compliance and reporting

The contract self-executes upon fulfilment of conditions via triggers

Provides data for compliance and reporting

Figure 5.11: How Smart Contracts Work in a Permissioned Blockchain

https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/smart_contracts_paper_long_0.pdf

a. Example of a Smart Contract in a broader sense

The use of Smart Contracts on a small scale can be imagined wherein two parties can get into a contract, such that only if the resources by one party reaches the other party their remuneration is provided. For example, buying a software code through the Ethereum Blockchain, as soon as Party A transfers the amount needed to purchase the code, the smart contract obligates Party B to transfer the code without Party B's knowledge. The transfer is coded in a way that Party B does not need to authenticate every transaction. In a broader sense, think of a Smart Contract being applied on a Stock Exchange.

On a traditional Stock Exchange if Mr.XYZ wanted to purchase a share of a company he would have to go through his broker who then has to pass through the intermediary such as the Clearing House and the Exchange. Mr.XYZ has to wait 2 days and has to bear the commission fees of 3 or more intermediaries to get his share certificate.

But, if this process is shifted on the Ethereum, or other similar blockchains, as soon as Mr.XYZ expresses his will to purchase a share of a company, transferring a certain amount would result the company's share being credited to his account, the company's ledger would be updated and the company would receive the required amount. All of these processes would happen immediately and all of the intermediaries in the traditional system would get eliminated.

xi. Academia

The interest on blockchain disrupting the traditional means of education has been insignificant as yet. With the exceptions of a few major institutions such as European Commission, University of Nicosia, Massachusetts Institute of Technology, Open University (UK) (all of whom have been extensively studied for this research), no major contribution has been seen.

Keeping in mind the core concepts of Blockchain, innovative use cases can be developed if only resources are put to use. This research aims to provide such new ideas in this field so that further studies can be incorporated.

VI. Blockchain and Academia

VI. Blockchain and Academia

i. Known use cases

With the spark of Blockchain starting in 2011, many institutions have been known to take up research on this new technology. Some institutions such as UNIC and MIT has gone as far as setting up Blockchain Research Institutes within their premises for interested individuals to study.

"Blockchain is a technology that clearly has applications in the world of learning at the individual, institutional, group, national and international levels. Rather than the old hierarchical structures, the technology becomes the focus, with trust migrating towards the technology, not the institutions. It really is a disintermediation technology."[50]

a. University Of Nicosia - Blockchain Initiative

The University of Nicosia (UNIC) is the largest university in Cyprus, with its main campus located in Nicosia, the capital of Cyprus. It also runs study centres in Athens, Bucharest and New York City. The University of Nicosia has 12,000+ enrolled students from 70+ countries studying on its Bachelor, Master and Doctoral degree programmes that are delivered by its 6 schools.

Figure 6.1 Logo of the University of Nicosia

The University of Nicosia (UNIC) broke new ground in University adoption of Blockchain technology by being the first university in the world to publish all diplomas of all graduating students (Bachelor's, Master's, PhD) on the Bitcoin Blockchain, as of the graduating class of Spring 2017.

The University of Nicosia was previously the first university in the world to publish academic certificates on the Blockchain (Spring 2014) and, subsequently, to publish diplomas on the Blockchain on a trial basis (Spring 2015). It is now the first university in the world to move from

[50] Quote by Donald Clark

trials to full implementation of this pioneering new technology, for all graduating students, on an ongoing basis.[51]

This service was announced by UNIC's CEO, Mr. Antonis Polemitis[52], during his opening remarks at the Decentralized '17 conference, a business and academic summit relating to the technical and societal implications of decentralization, cryptocurrency and Blockchain technology, organized by UNIC in Limassol, Cyprus on 2-3 November 2017.

The University, a fore runner in innovation, is also the first University in the world to offer a Masters course in Blockchain education in the form of M.Sc in Digital Currency. This course was laid by Antonis Polemitis and Andreas M Antonopoulos[53].

b. MIT

MIT states that blockchain-issued academic certification gives student unprecedented "autonomy over their own records."

"*The technology has the potential of dramatically changing how we conduct transactions on a global scale, as it offers secure payments without the necessity of a costly and often slow intermediary. This could disproportionately help segments of the population that are currently underserved by financial intermediaries as well as countries with weak financial institutions.*"[54]

In 2017, MIT began began issuing digital diplomas to select groups of students graduating within Undergraduate, Masters, and PhD degree programs. These tamper-proof records are registered on the Bitcoin blockchain, so they can be shared peer-to-peer and independently verified. The bitcoin blockchain, combined with strong cryptography, provides a new security infrastructure that guarantees the authenticity of these records and enables convenient verification.

[51] University of Nicosia Issues Block-Chain Verified Certificates (https://www.coindesk.com/university-nicosia-issues-block-chain-verified-certificates/)

[52] Antonis Polemitis is the CEO of the University of Nicosia and also serves as a Director on the co-ordinating Board of the University. He is an adjunct faculty member and leads the industry advisory committee for the University on digital currency. He is co-teaching the introductory MOOC on the introduction to blockchain program.

[53] Andreas M. Antonopoulos is a technologist and serial entrepreneur who has become one of the most well-known and well-respected figures in bitcoin. He is the author of the book: "Mastering Bitcoin," considered the best technical guide to bitcoin.

[54] MIT Blockchain Institute (http://blockchain.mit.edu)

Figure 6.2: Logo of Massachusetts Institute of Technology

1. Process of Certification Issuance

The process starts with an invite email requesting that students download the open-source mobile app (Blockcerts[55]) for iOS or Android, and then add MIT as an issuer. The mobile app provides the most convenient way to generate keys, which are used to demonstrate ownership, and send their public key to MIT The app makes this as simple as adding a friend.

In addition to the standard security measures, the Institute wanted to add an additional layer of security to ensure the identity of students by asking them to login to the MIT identity system as part of this on-boarding process. Once diplomas were issued, they arrived to students by email as an attachment that can be stored anywhere. And importing that file into the mobile app provides a convenient way to view and share these records. MIT also decided to host these files, which makes them easy to share with just a link.

While any I.T. system can include a blockchain lookup service for verification, MIT provides an additional convenience by hosting a verification site at *https://credentials.mit.edu*, where any verifier can paste a link or upload a file to independently verify a diploma. This process works by using an open source blockchain lookup service (Blockcerts) to compare a compare the uploaded diploma to the hash stored on the blockchain. The power of decentralized verification is that both organizations could disappear and graduates would still be able to have their records verified.

[55] Blockcerts is an open standard for building apps that issue and verify blockchain-based official records. These may include certificates for cvic records, academic credentials, professional licenses, workforce development, and more. (https://www.blockcerts.org/guide/)

VII. Christ (Deemed to be University) and Blockchain scenario

VII. Christ (Deemed to be University) and Blockchain scenario

Figure 7.1: Logo of Christ (Deemed to be University)

i. About the University

Founded in 1969, Christ University declared as an institution 'deemed to be university' under section 3 of UGC Act, 1956. The University is under the management of the priests of the Catholic religious order, Carmelites of Mary Immaculate (CMI). The University has over 18,000 students and more than 800 faculty members. It has a foreign student community of about 700 from 58 nationalities.

The campus is often proclaimed as a living example for harmonious multiculturalism with students from all the states of the country and from around 72 foreign countries. CHRIST (Deemed to be University) publishes six peer-reviewed journals and has published more than 300 books in Kannada, English and Malayalam.

In 2016, the University was accredited by National Assessment and Accreditation Council with **A Grade**. The university offers nationally and internationally recognised undergraduate, postgraduate and research programmes in academic disciplines in Humanities, Social Sciences, Sciences, Law, Engineering, Business Administration, Commerce, and Management. It offers professional courses in fields including Business Management, Computer Application, Hotel Management, Mass Communication, Social Work, Engineering and Tourism.

ii. Existing methodologies

Christ (Deemed to be University) has a campus that includes 7 study-blocks and 2 libraries and other amenities include a recycling plant, 2 playing fields; that serves a population of approximately 18000 students and 800 faculties hailing from different geographical backgrounds. The amenities of the college are considered a step ahead when compared to other institutions at the same stature. The University provides a wide array of study programmes. Christ follows a learning pattern which is holistic in nature. The mission of the University has always remained to adopt changes efficiently.

- Christ (Deemed to be University) library follows a digital method where all recording of issuing of books is integrated to the main Christ server. University library stacks contains 2,20,589 books as of May 2015. The library database is completely digitized and is managed through Koha software.

- The University is a member of the Association of Indian Universities.

- The campus is a zero waste campus and recycles its wet waste and used paper.

- The campus is cashless with students being provided with smart cards which also serve as the identity cards and debit cards of the institution, through tie-up with the South Indian Bank.

iii. Suggested advancements

All changes suggested are while keeping in mind the existing methodology of the university. Any change suggested is made with the researcher's knowledge in this particular field and should not be taken in exact terms.

a. Blockchain based identity

Blockchain based can be used to facilitate the self-sovereignty of individuals or participants by giving each participant the ability to be the ultimate owner of all the data and personal information, accessible only by the participant. Individual and group learners could finally own, manage and share the details of all their credentials and also be able to self-authenticate the information periodically.

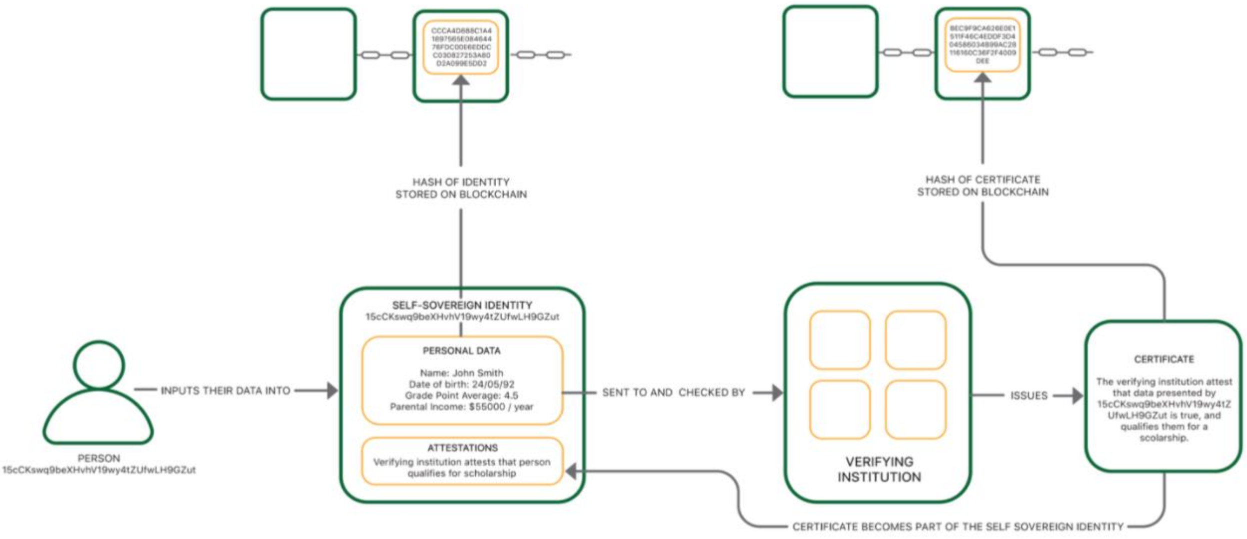

CCCA4D888C1A4 1897565E084644 76FDC00E6EDDC C030827253A80 D2A099E5DD2
HASH OF IDENTITY STORED ON BLOCKCHAIN
BEC9F9CA626E0E1 511F46C4EDDF3D4 04586034899AC28 116160C36F2F4009 DEE
HASH OF CERTIFICATE STORED ON BLOCKCHAIN
PERSON
15cCKswq9beXHvhV19wy4tZUfwLH9GZut
INPUTS THEIR DATA INTO
SELF-SOVEREIGN IDENTITY
15cCKswq9beXHvhV19wy4tZUfwLH9GZut
PERSONAL DATA
Name: John Smith
Date of birth: 24/05/92
Grade Point Average: 4.5
Parental Income: $55000 / year
ATTESTATIONS
Verifying institution attests that person qualifies for scholarship
SENT TO AND CHECKED BY
VERIFYING INSTITUTION
ISSUES
CERTIFICATE
The verifying institution attest that data presented by 15cCKswq9beXHvhV19wy4tZUfwLH9GZut is true, and qualifies them for a scolarship.
CERTIFICATE BECOMES PART OF THE SELF SOVEREIGN IDENTITY

Figure 7.2: Architecture of a Verified Blockchain - Secured Self - Sovereign Identity. Camilleri, Anthony; Grech, Alex (22017): Source: https://doi.org/10.6084/m9.figshare.5371516.v1

b. Smart Contracts

Smart contracts, enabled by blockchain or distributed ledgers, have been held up as a cure for many of the problems associated with traditional financial contracts, which are simply not geared up for the digital age. Reliance on physical documents leads to delays, inefficiencies and increases exposure to errors and fraud. Financial intermediaries, while providing interoperability for the finance system and reducing risk, create overhead costs for and increase compliance requirements.

Use of Smart Contracts could be implemented in a proper way within the institution in numerous forms. Being just a backend code, any agreement between two or more participants within the institution or between institutions can be issued using a Smart Contract. With the use of blockchain, Smart Contracts are given an extra fire, making them irrefutable and secure. Smart Contracts can be imagined as a well-structured, digital escrow account that promises to provide the required end-result, in exchange for the stated renumeration.

Smart contracts may be used to mitigate the increased complexity resulting from eliminating intermediaries through blockchain use. Smart contracts represent programmatic means to efficiently apply these structures for value exchange. this ability to evaluate, commonly interpret, and maintain transparency of different parties' smart contracts is enhanced if the contracts implement formal models—whether they are mathematical, logical, or simulation-based.

A Smart Contract contains the following characteristics:

- Both parts of the agreement are Digital in nature or can be converted to a digital code
- Involves or requires intermediation for continuous, periodical authorization and execution
- Transfer requires verification and authentication
- Trust factor is missing between parties
- Enforcing of certain rights with prior permission

Further use of Smart contracts and their applications within the Institution is explained in the following chapters.

c. Revocable Digital Certificates

As certificates are stored on the blockchain, even if an organisation closes down or the system collapses; certificates can still be authenticated and verified against the Blockchain as all entries are immutable by nature. This will allow for countless people in backward areas or people who travel a lot, to easily verify or provide for verification, all their records. Institutuons, on the other hand, need not spend any resources on the verification process of certificates as they are self-verifiable, cutting down on hundreds of man-hours and internal costs. The verification of the authenticity of a certificate only requires comparison between with the hash of the certificate and the hash stored on the Blockchain by the issuer.

But, in a future scenario, a certain individual might want his/her details on the certificate to be changed. This causes a problem as all data stored on a blockchain is immutable and cannot be tampered with. This introduces the concept of Revocable Digital Certification on the Blockchain. Concepts like sidechains and shortened database storage can be used to solve this problem.

The objective of notarising certificates on the Blockchain is to transform or convert a traditional certificate that a student usually receives from an institution, into a self-verified

This is where the blockchain can help as a trust-less intermediary to act as

- A wallet for all different certifications so one can have them in one place and showcase them easily, in-case of need
- An easy way to validate all certifications of a person as all information stored on the Blockchain is verified by the Network and can be considered authentic

1. Contents of a Digital Certificate issued by an Institution

- **Qualification:** All details regarding the course taken up and functions of the course
- **Time-stamp:** the time-stamp of the certificate being recorded
- **Result:** Grades and contents of the grades through the course of programme
- **Certification of Result:** certification or guarantee of the results achieved by the issuer of the certificate
- **Additional relevant information:** All additional information relevant to the student such as grants, category, quota etc.

These information's that are to be included in a digital document pertaining to a certificate of a participant has to be mentioned, to authenticate the document and could sometimes run for several pages.

In the traditional system, it could have been stored on a central database: but with the Integration of Blockchain, it might prove to be unfeasible to store large amounts of data on a distributed network.

Therefore, to supplement this process of large data distribution, the contents of a certificate issued on the blockchain can be reduced, and include a link to an external storage database or another blockchain itself, containing all other relevant information relating to a data. Side chains[56] can be introduced to help this process of accumulating and authenticating information on the Blockchain.

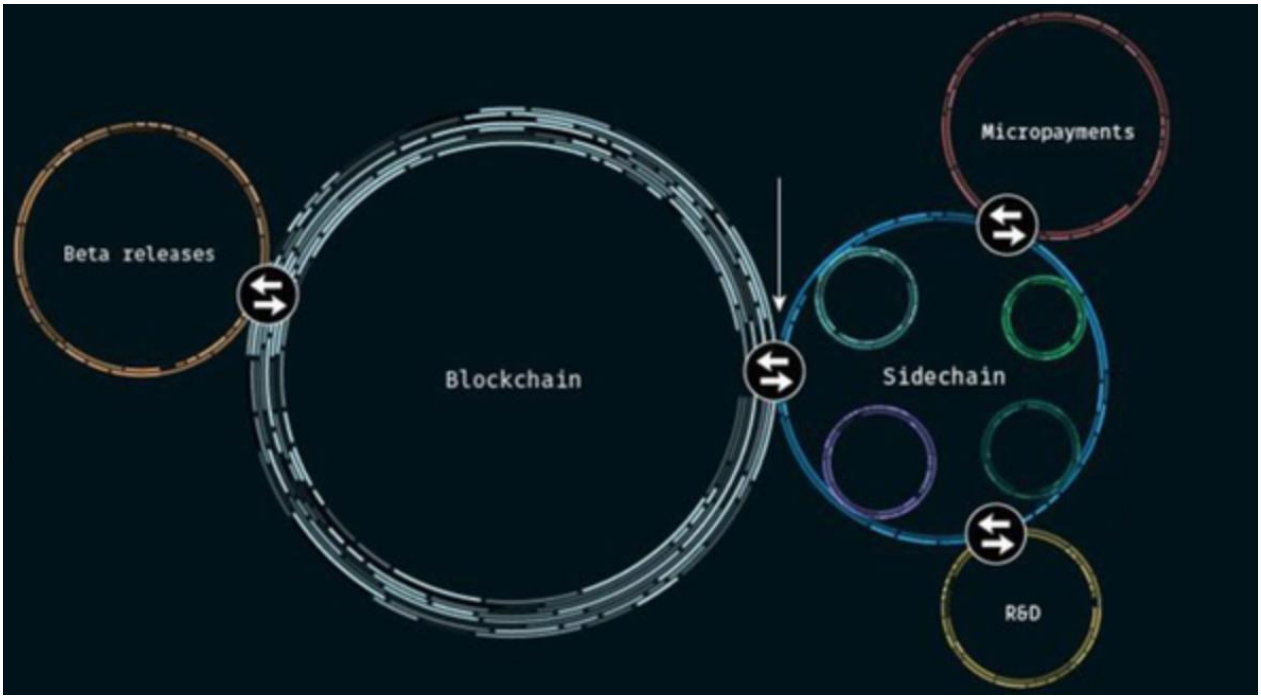


Figure 7.3: Blockchain and Sidechains

2. Issuing Certificates on the blockchain

In the case of Christ University, all certificates can be issued on the Blockchain, making all refining and validating of documents easier and intermediary-less. Internal costs can also be cut with in the Institution as issuing of in-house certificates such as, leave of absence, on-duty leave, can be done with the Personal Unique Identity provided to each student.

A. Mechanism

First, the certificate issuer, in this case, Christ needs to publish their public key to identify themselves and proof that the certificates they issue are in fact from that institute. Then, when a nominee earned a certificate she might request the certificate to be issued on the blockchain and provides her/his own

[56] Sidechains are a separate blockchain, attached to the parent through the use of a two-way peg, which allows for assets to be interchangeable and moved across the chain at a fixed deterministic rate. This two-way peg works by utilizing simple payment verification to show and prove ownership of the assets on the parent chain.

public key so the issuer can sign a transaction with the certificate and the public key of the nominee which then can be recorded on a smart contract. The second part is a front-end for the dAPP[57] (for eg: the one used by MIT called Blockcerts[58]) that displays all certificates for a person which is easy to share (put up a link on your CV or linkedin) and fairly easy to validate as you just have to compare it with the public key of the issuer.

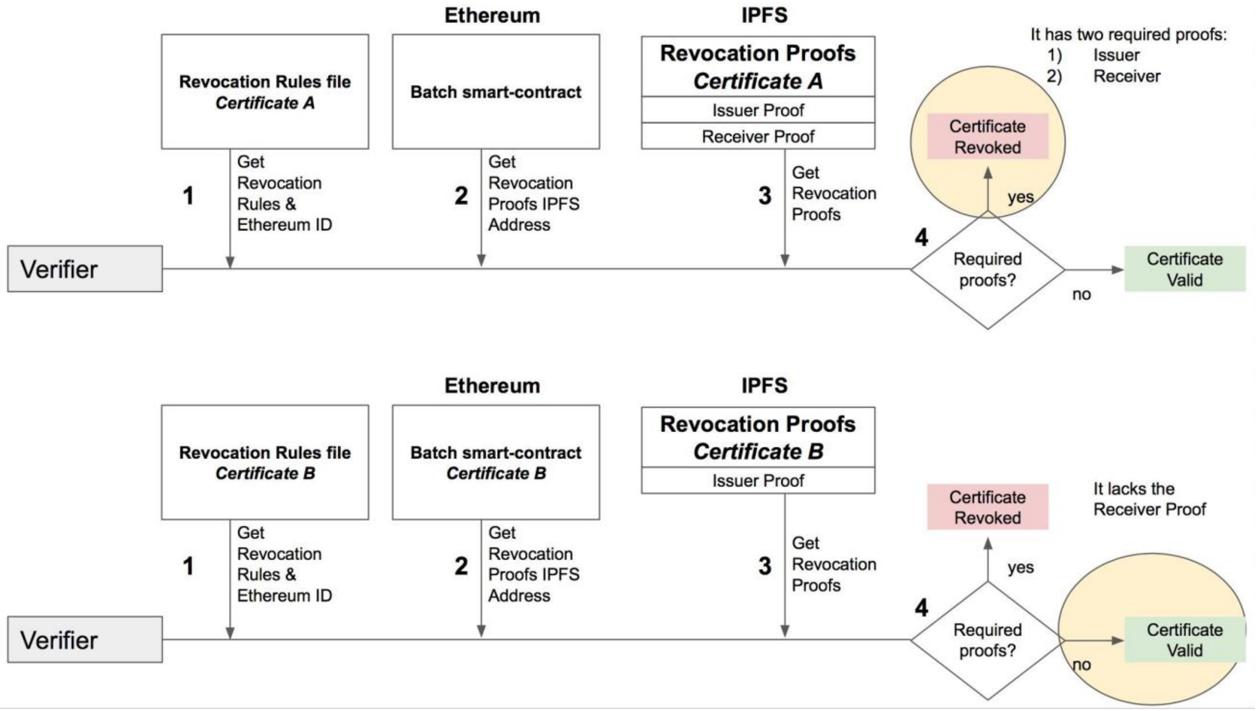


Figure 7.4: Revocable Digital Certification on the Ethereum Blockchain. Source: https://github.com/blockchain-certificates/revocation

d. Accounting practices

In a scenario which is open-source in nature, i.e., Blockchain, all transaction within the University can be audited both internally and externally in a simpler way. Internal authorities that need to keep a check on the functioning of the University can easily do so with the help of personal identity

[57] DApp is an abbreviated form for decentralized application. A DApp has its backend code running on a decentralized peer-to-peer network, contrast this with an app where the backend code is running on centralized servers.

[58] Blockcerts is an open standard for creating, issuing, viewing, and verifying blockchain-based certificates. These digital records are registered on a blockchain, cryptographically signed, tamper-proof, and shareable. The goal is to enable a wave of innovation that gives individuals the capacity to possess and share their own official records. They invite feedback, contributions, and general discussion. The initial design and development was led by MIT's Media Lab and Learning Machine. For ongoing development, this open-source project actively encourages other collaborators to get involved. The goal of this community is to create technical resources that other developers can utilize in their own projects. Rather than independently developing custom implementations, let's work together to build an interoperable future. (https://www.blockcerts.org/about.html)

management. External authorities in order to audit the institution can be provided with exact details of all transactions within the University but in a private and secure way which does not require to reveal the personal identity of each individual.

1. Micro-payments

The emergence of the blockchain protocol and cryptocurrency will solved the problem of micro transactions or micropayments model that can be utilized within the University, in which access to the services or content provided, as well as low-cost purchases, is possible. Small amounts of transactions are unprofitable for electronic payment systems due to large inter- organisation transaction costs or waste or ordeal, whereas in cryptocurrencies it is very low and do not depend on the size of the transaction.

- Micro-payments within the university such as penalties, internal reimbursements can be done in a quicker way by integrating Smart Contracts

- Transactions within the University can be carried out digitally, extending the University’s vision to transform into a digital campus, removing the need for cash based transactions. This will also help in the audit of transactions as all entries are open-source.

- Student funding and scholarship drives be easily conducted. All students considered worth by the University, can be added to list that includes all Public keys of the students, allowing for in-house funding and allocation of resources.

e. Intellectual Property Management

Intellectual property/capital are terms used to describe intangible assets: the results of human endeavour that have value and are original, such as designs, publications, inventions, computer software and music. These assets increasingly making up a large proportion of company net worth. The protection and management of these assets has become a commercial imperative, requiring the development of a set of practices that are encompassed within field of Intellectual Property Management (IPM)[59] Integration of Blockchain allows for increases operability and tracking for the Digital Assets. These assets can also be used to monetise, by the use of Smart Contracts.

[59] Paasi et al., 2010; Rivette and Kline, 2000

1. Research papers

In the traditional system, the journal companies and organisations would be responsible for the citation of Articles and papers, the data is made available to them. Any participant would have to take the help of these entities to ensure the collection of data and not feasible to do this process individually or independently. These intermediaries also put up limits on the use of their services and increase the costs for better services.

By shifting the referencing process on the blockchain, the backing of citations becomes much easier. Using a Blockchain instead of intermediaries will allow for more open-source material to be available, wherein each individual will be able to keep accurate track of the use of material cited.

The mechanism would involve a blockchain that would distribute the details of the released publication to all network nodes, making an entry on the public ledger. This entry would contain all details relating to the paper, and also links or connections to other previous publications. Thus, any usage of the publication linked to the blockchain would be available to view on the Blockchain.

2. Copyrights

Copyrights management within the university, such as Patents developed, digital assets of the university, digital content such music and video, can all be hashed to the blockchain by the University hash and be used to extensively track and generate revenue out of the copyrights issued using customised Smart Contracts.

f. Data mining

With the use of Data mining procedures, as explained in previous chapters, the institution could achieve greater heights, as the collection, mining and interpretation of all data available on the private blockchain of the institution could lead to various analysis and interpretations helping institutional growth.

The data collected by the University through all the practices within the Institution can be put to better use. Because of the open-source nature of the Blockchain, all participants of the Blockchain network can make use of the data available and use it as per their own understanding. Third-party institutions that specialize data interpretation practices can be allowed to make use of the data and also remunerate the data owners as and when their data is being used, through the use of optimized Smart Contracts that are tailored by the Institution as per its needs.

Blockchain can be used to help Data mining practices in ways like:

- Securing the data collected and transferred through the distributed feature of the blockchain
- Making use of the open-source nature to collect, interpret and analyse information collected within the institution or let participants or third-parties to make use of the data in exchange for remuneration through the use of Smart Contracts
- The data collected by the University through all the practices within the Institution can be put to better use. Because of the open-source nature of the Blockchain, all participants of the Blockchain network can make use of the data available and use it as per their own understanding.
- Third-party institutions that specialise data interpretation practices can be allowed to make use of the data and also remunerate the data owners as and when their data is being used, through the use of optimised Smart Contracts that are tailored by the Institution as per its needs.

1. Exchange of data

Data available on the Blockchain can be used to transfer or exchange information in a secure way. Because of the disturbed nature of the Blockchain, being prone to outside hindrance of data is embedded by default.

2. Inter-department/inter-institutional data transfer

Data transfer within the institution becomes much more simple and easy. Customizing a blockchain as per the Institution's needs, will help the Institution to optimise its resources through faster day transfer, allowing for greater innovation to be achieved.

g. Supply Chain Management

According to Morgan Stanley, blockchain *"has the potential to join autonomous trucks, drones, and the 'uberization' of freight as a key disruptive technology that can bring operating and cost efficiency to supply chains—while also being a threat to existing asset-light business models."* The concept of Supply Chain Management can be improved with the integration of IoT devices around the campus. Recycling bins, libraries, canteen amenities, and other inventories within the campus can be smartly organised through the use of Blockchain.

1. Library

- The already existing Digital Library Records of the University can be improved by integrating Blockchain, students wishing to get a hold of a particular book can make use of the open-source nature of Christ Blockchain. They can personally contact the previous holder of the book or the library by looking at the internal public ledger of the university.

- Smart Contracts can be issued within the Library wherein a particular set of books that carry higher importance can be issued on a contract basis. Issuers can be penalised for their late submission with the reserves they hold against library

2. Campus Amenities

- Recycling bins, trolleys, can be integrated with IoT devices that transfer real-time information and notification to the internal authority, for example if a recycling bin integrated with an IoT device (that keeps a check on the time, weight, temperature, etc. of the recycling bin) finds it to be full it can relay a message to the concerned department calling for a change.
- Thinking ahead, if a lamp post (also integrated with an IoT device) finds itself out of service, it can contact the provider for a change and pay them with the allocated reserves it has been provided. The intermediaries within the college are cut down drastically.

VIII. Conclusion

VIII. Conclusion

The blockchain is a technological innovation that reduces uncertainty of value exchange but it may very well also lead to increased complexity resulting from having to subsume work that displaced intermediary institutions had performed.

With the introduction of bitcoin, a new era of innovation sparked, with interesting ideas and use-cases being developed for the underlying technology of bitcoin. Blockchain has promised to disrupt magnitudes of traditional practices. Any practice involving the use of an intermediary, that can use the Basic Principles such as Transparency, Immutability, Distribution and Trust-less (all of which have been extensively covered in this research), can be replaced in the future by the use of an open-source software and ledger-protocol that can securely store and transfer data on its distributed network.

The research aims to show the use of Blockchain management in Educational Institutions. Any institution, organisation or practice, looking forward to optimize their resources with the sole view of dedicating those resources to better practices, can use this process. Schools, Colleges and Universities can use this study to get familiar with the core concepts of Blockchain and how its role in the recent future could be major depending upon the interest shown. The implementation of Blockchain within an Institution and the changes it would bring, and the innovation it brings along, will allow for greater interest among parties looking to break down their practices.

IX. Key terms overview

– Blocks

Transaction data is permanently recorded in files called blocks. They can be thought of as the individual pages of a city recorder's recordbook (where changes to title to real estate are recorded) or a stock transaction ledger. Blocks are organized into a linear sequence over time, also known as the blockchain. New transactions are constantly being processes by miners into new blocks which are added to the end of the chain and can never be changed or removed once accepted by the network.

– P2P

Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes.

– Decentralized

Decentralization is the process of distributing or dispersing functions, powers, people or things away from a central location or authority. While centralization, especially in the governmental sphere, is widely studied and practiced, there is no common definition or understanding of decentralization.

– Cryptography

Cryptography, or cryptology, is the practice and study of hiding information. It is sometimes called code, but this is not really a correct name. It is the science used to try to keep information secret and safe. Modern cryptography is a mix of mathematics, computer science, and electrical engineering.

– Hashing Algorithm

A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes. Hash functions accelerate table or database lookup by detecting duplicated records in a large file.

– Cryptocurrency

A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

– Cryptographic mining

Mining is the process of adding transaction records to a blockchain’s public ledger of past transactions (and a "mining rig" is a colloquial metaphor for a single computer system that performs the necessary computations cryptographic for "mining"). This ledger of past transactions is called the block chain as it is a chain of blocks.

– Time-stamp

A timestamp is the current time of an event that is recorded by a computer. Through mechanisms such as the Network Time Protocol (NTP), a computer maintains accurate current time, calibrated to minute fractions of a second.

– ICO

An Initial Coin Offering or ICO typically involves selling a new digital currency at a discount — or a “token” — as part of a way for a company to raise money. If that cryptocurrency succeeds and appreciates in value — often based on speculation, just as stocks do in the public market

– Whitepaper

A white paper is an authoritative report or guide that informs readers concisely about a complex issue and presents the issuing body's philosophy on the matter. It is meant to help readers understand an issue, solve a problem, or make a decision.

– Nodes

A network node is a connection point for data transmissions on a communications network that can function as a redistribution point or an endpoint.

– Digital Signature

A digital certificate, an electronic document that contains the digital signature of the certificate-issuing authority, binds together a public key with an identity and can be used to verify a public key belongs to a particular person or entity.

– Multi-Signature

Multi-signature (often called multi-sig) is a form of technology used to add additional security for cryptocurrency transactions. Multi-signature addresses require another user or users sign a transaction before it can be broadcast onto the block chain.

– Bitcoin

Bitcoin is a digital currency created in 2009. It follows the ideas set out in a white paper by the mysterious Satoshi Nakamoto, whose true identity has yet to be verified. Bitcoin offers the promise of lower transaction fees than traditional online payment mechanisms and is operated by a decentralized authority, unlike government-issued currencies.

– Ethereum

Launched in 2015, Ethereum is a decentralized software platform that enables SmartContracts and Distributed Applications (ĐApps) to be built and run without any downtime, fraud, control or interference from a third party. Ethereum is not just a platform but also a programming language (Turing complete) running on a blockchain, helping developers to build and publish distributed applications.

– ERC20 Tokens

The ERC-20 defines a common list of rules for all Ethereum tokens to follow, meaning that this particular token empowers developers of all types to accurately predict how new tokens will function within the larger Ethereum system. The impact that ERC-20 therefore has on developers is massive, as projects do not need to be redone each time a new token is released. Rather, they are designed to be compatible with new tokens, provided those tokens adhere to the rules.

– dAPP

DApp is an abbreviated form for decentralized application. A DApp has its backend code running on a decentralized peer-to-peer network. Contrast this with an app where the backend code is running on centralized servers.

– Smart Contracts

A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible.