

Addis Ababa university

FACULTY OF NATURAL AND COMPUTATIONAL SCIENCES

DEPARTMENT OF COMPUTER SCIENCE

**Blockchain**

technical report writing

by

ADDISMIRAPH ABEBE NSR/2009/08

BIRUK TAMIRU NSR/9151/08

AMANUEL SHIMELES NSR/6860/08

Advisor: Berhanu Abebe

January 2019

DECLARATION

This is to declare that this project work which is done under the supervision of Berhanu Abebe and having the title AAU Push is the sole contribution of:

ADDISMIRAPH ABEBE NSR/2009/08

BIRUK TAMIRU NSR/9151/08

AMANUEL SHIMELES NSR/6860/08

No part of the project work has been reproduced illegally (copy and paste) which can be considered as Plagiarism. All referenced parts have been used to argue the idea and have been cited properly. We will be responsible and liable for any consequence if violation of this declaration is proven.

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Group Members:

Full Name Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CERTIFICATE

I certify that this BSc final project report entitled

AAU Push by:

ADDISMIRAPH ABEBE NSR/2009/08

BIRUK TAMIRU NSR/9151/08

AMANUEL SHIMELES NSR/6860/08

is approved by me for submission. I certify further that, to the best of my knowledge, the report represents work carried out by the students.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date Name and Signature of Supervisor

**Table of Contents**

DECLARATION i

CERTIFICATE ii

List of Figures 3

List of Tables 4

Definition, Acronyms and Abbreviations 5

References 5

1. Introduction 6
   1. Background 6
   2. Bitcoin - First Application of Blockchain 7
   3. A Brief History of Blockchain 7
2. Literature review 9
   1. Introduction 9
   2. Working Model 10
      1. What is a Block? 10
      2. Core Concepts 12
   3. Classification of Blockchain System 13
   4. Consensus Algorithms 13
   5. Uses of Blockchain 13
      * 1. Technical analysis 14
3. Related works 17
   1. Introduction 17
   2. Crypto-currency 17
   3. Something else 17
4. Applications of blockchain 17
   1. Importance of Blockchain in Healthcare Data Management 19
   2. Blockchain & Healthcare 19
   3. Pharmaceuticals And Fraud Detection 20
   4. Drug And Food Supply Chain 20
   5. Blockchain And Government 21
      1. Land Registry 21
      2. Elections 22
5. Future work 22
   1. Introduction 22
   2. Crypto-currency 23
6. Conclusion 23

List of Figures

List of Tables

Definition, Acronyms and Abbreviations

| Abbreviations | Definitions |
| --- | --- |
|  |  |
|  |  |

References

<https://www.blockchain-council.org/>

[1] <https://www.vanityfair.com/news/2018/07/the-man-who-created-the-world-wide-web-has-some-regrets>, January 28, 2019

[2] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[3] Haber, S. & Stornetta, W.S. J. Cryptology (1991) 3: 99. <https://doi.org/10.1007/BF00196791>

[4] BlockChain Technology Beyond Bitcoin, Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, October 16, 2015

[5] BEYOND BITCOIN: A LITERATURE REVIEW OF BLOCKCHAIN TECHNOLOGY, SARAH PROWSE, August, 2017

[10] https://www.smartdubai.ae/initiatives/blockchain, January 28, 2019

1. Introduction
   1. Background

Since the invention of the Internet and the World Wide Web, we have seen an unprecedented change in the way we live. Today, everything is a click away. Do you need a pack of pens? Click and Amazon will send it to you. Do you need a ride to a friends house? Click and an Uber or a RIDE will show up. In this whole process, the use physical cash is slowly disappearing. Electronic cards and online bank account transactions have simplified our payment systems. Social media applications made by companies like Google and Facebook have made connecting with distant friends and relatives easier than ever. Using instant-messaging applications, we are able to chat in realtime with people across the world. After seeing all the advantages we get from the Web, are there any disadvantages?

The inventor of the World Wide Web, Tim Berners-Lee, has seen this evolution of his brain child through the decades. He saw the utility it brought to humanity. However, he is now confronted with an alarming future and is devastated by it.1 This concern arises from the way in which the Web has developed. We live in a centralized world. From social media apps to financial activities, we give our personal information to be stored in that service’s server, wherever it might be in the world. This has put users, who have lost control of their data, at the mercy of service vendors.

“Centralization, or control by a single authority or entity, is a common and pervasive form of governance. Governance refers to principles of organization and power. We must trust central authorities, like banks, governments, and other institutions to maintain order and structure within the space they operate. This trust is broken when the central authorities can not maintain that order and structure. For example, if your credit card information is stolen from the database of a bank you transact with, the centralization of your information in this bank has been used against you. Centralized technology and data allows for both the monopolization of power and creates a security risk.” (ConsenSys Academy, 2017)

This poses a single point of failure for the whole system. The Blockchain technology saw it debut in the financial sector in 2009, when it was used to host a cryptocurrency known as Bitcoin. Blockchain combines a number of known technologies to create a distributed public ledger (database for transactions) that is cryptographically secure against modification, ensuring identity and integrity. After its success, the blockchain platform has been in development to be applied to many other areas.

* 1. Bitcoin - First Application of Blockchain

“The one thing that’s missing is a reliable e-cash, whereby on the internet you can transfer funds from A to B without A knowing B or B knowing A” - Nobel Prize Winning economist Milton Friedman, 1999

Almost 10 years later, on October 31, 2008, in the midst of the financial crisis, Satoshi Nakamoto (an alias for a still unidentified individual or group of individuals) published the Bitcoin Whitepaper, titled Bitcoin: A Peer-to-Peer Electronic Cash System.2 This paper described a way of exchanging a currency, Bitcoin, that combines cryptography, computer science, and game theory in its design and implementation. Satoshi’s creation enabled a participant to digitally transact directly with another participant without relying on a single, centralized intermediary, such as a bank, to validate the payments. Bitcoin was able to do this by using and running on what it called a blockchain. **Blockchain** is distributed, decentralized, public ledger. It is made up of blocks that hold data and each block is cryptographically connected to ensure integrity. In the case of Bitcoin, each block holds the transaction information.

This decentralized nature of blockchain has made it:

* Less likely to fail because they rely on many separate components.
* Harder to attack because the networks are spread across many computers.
* Harder for users with malicious intent to take advantage of users who are using the platform for its intended purpose.

If one node stops working, or even 100 nodes, the blockchain survives assuming there is at least one node up and running. This makes the blockchain very resistant to attacks. The blockchain does not stop working even if the power is lost in an entire country. This makes the blockchain very resilient, which cannot be said of many of the existing systems we use on the Internet.

* 1. A Brief History of Blockchain

The technique used in blockchain to ensure integrity of data was first described in 1991 by Stuart Haber and W. Scott Stornetta in their article title “How To Time-Stamp a Digital Document” in the Journal of Cryptography. They raised “the issue of how to certify when a document was created or last changed.”[3] Since it was easy to modify the date of creations or edit of a document using different tools. They saw the need to time-stamp the data itself and “propose[d] computationally practical procedures for digital time-stamping of such documents so that it is infeasible for a user either to back-date or to forward-date his document, even with the collusion of a time-stamping service.”[3] They created with technique to make sure that the privacy of the documents were maintained and required no record-keeping by time-stamping services.

The first blockchain was conceptualized by a person or group known as, Satoshi Nakamoto, in 2008. The design was implemented the following year by Nakamoto as the core component of the implementation for the Bitcoin digital currency.

In the following chapters of this paper, we will look at how this technology works, its applications and the exciting future it holds.

1. Literature review
   1. Introduction

So what exactly is a Blockchain? The term blockchain is still yet to be defined with clarity and agreement. Currently it can refer to a data structure, algorithm, a group of technologies, and/or as a definition used for distributed peer-to-peer systems with a common application system.

A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. [4]

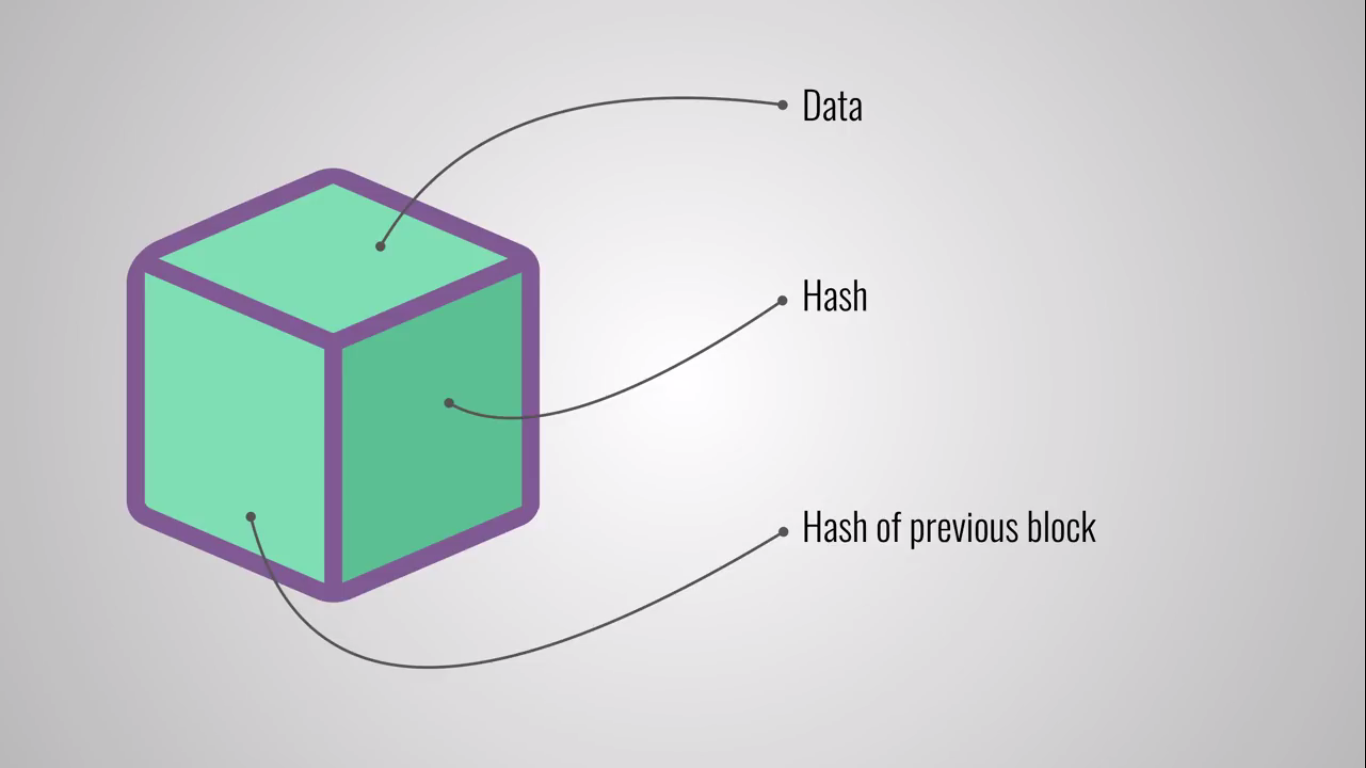
Blockchain is a vast, global, distributed database. That doesn’t run on one computer rather runs on all computers and is not accessible to a few but accessible to all. And not just to information but potentially anything of value, money, financial asset, intellectual property, energy, even votes and elections can be moved, stored and managed securely and privately and where trust is not established by a third party but rather through mass collaboration, Cryptography and cleaver code.[5]

Block chain is a distributed ledger that is completely open to anyone. It has many properties that make it appealing — one of which is that when something it written to the blockchain, it is very hard to reverse it.

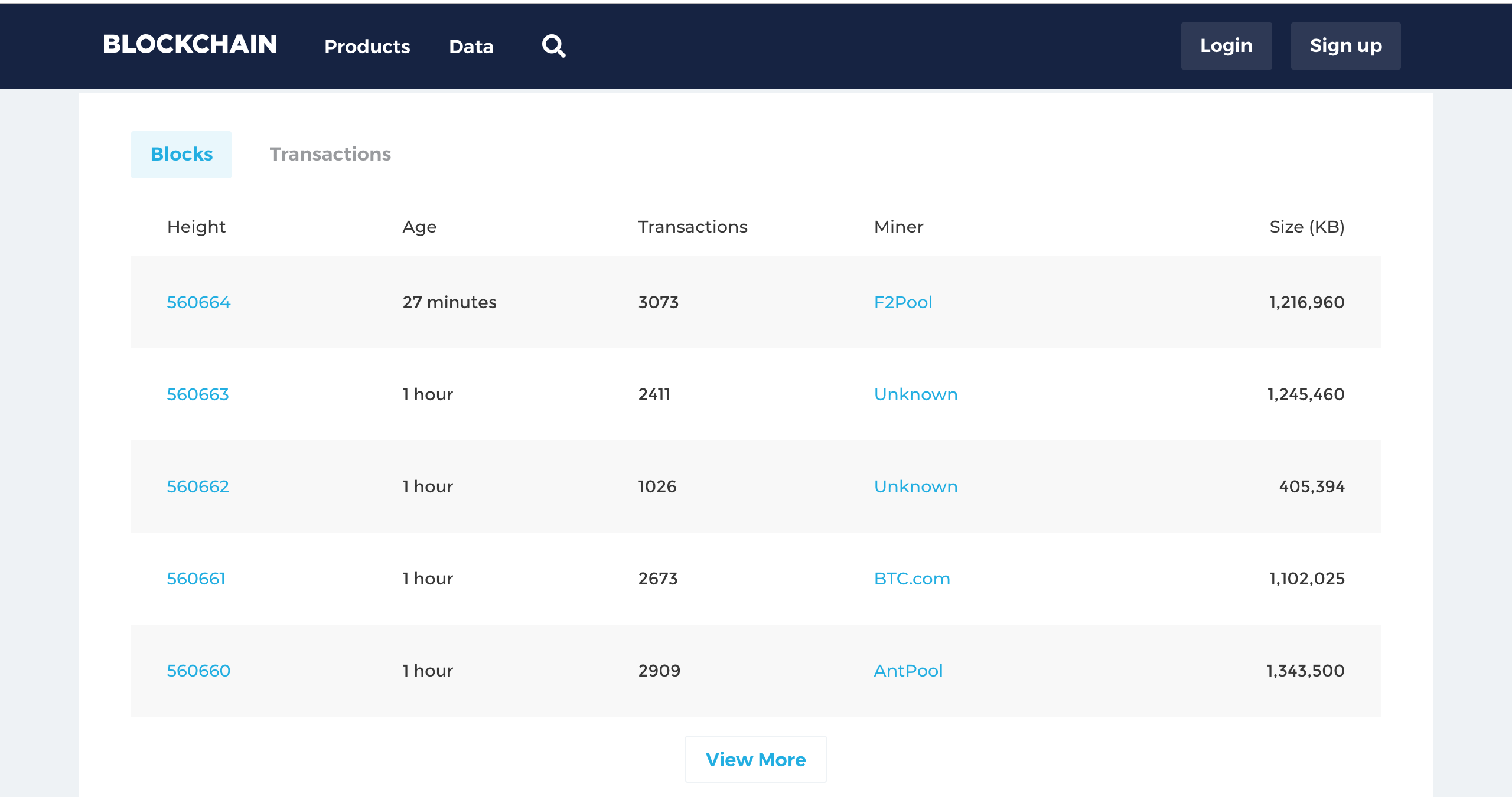
Key Features Of Blockchain:

* Decentralization – Blockchain works on the principle of decentralization, it means that the information is not stored on a central server, rather, its distributed.
* Provenance – This is yet another important feature of Blockchain wherein it becomes easy to track the origin of the product. This feature is very useful in supply chain management.
* Immutability – This feature of Blockchain makes it difficult for anyone to change or alter the data. Once the information is fed in the ledger, it gets time-stamped and changing this information becomes nearly impossible.

Blockchain is a smart combination of known techniques. It is a shared, replicated ledger with consensus, provenance, immutability and finality. In the following sections, we will look at each component of a blockchain and how it works.

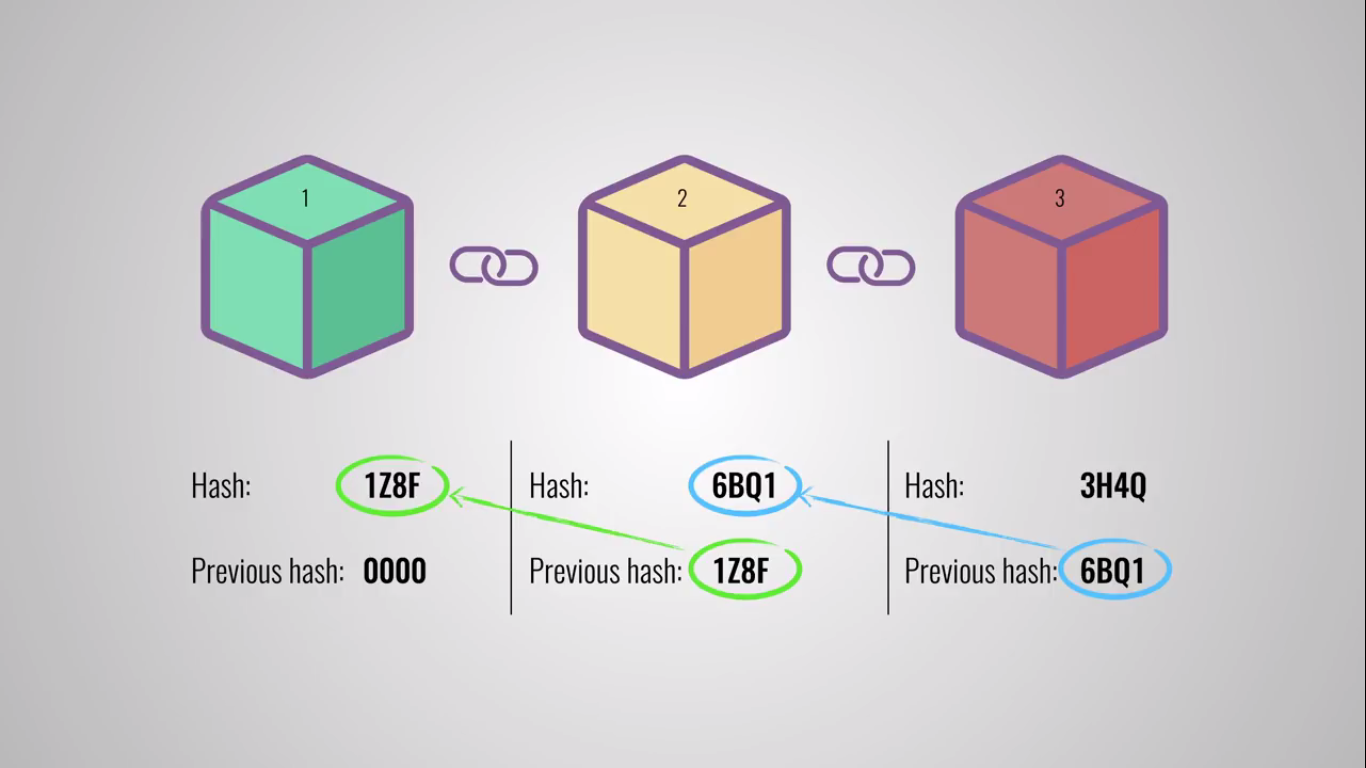
* 1. Working Model
     1. What is a Block?

**Block:** A block is simply a file that hold three main components: data (main content of the block), hash of the previous block, hash of the block. Let’s look at each part closely.

**Data:** the contents of the data stored within a block can differ from one blockchain to another depending on the purpose of the blockchain. For Bitcoin, a number of transactions are stored within the block. Figure below shows the blockchain of Bitcoin.

Each row is a block and the ‘Transactions’ column shows the number of transactions recorded or stored in that block. The file column titled ‘Size’ shows the space that block file takes.

For other blockchain, the data stored might be completely different. For example, the blockchain is used for food supply chain management, the data for one block could contain ‘Batch Number,' ‘Date of Production,' ‘ID of Transport Truck,' ‘Temperature Level in Truck,' ‘Humidity,’ and ‘Date of Delivery.’

**Hash:** To give each block a unique identification, a hashing algorithm is used on the contents of the block — reducing it to a string or number of a given length. The data of the block is hashed together with the hash output of the previous block on the chain. This creates the chain and associates each block to the one before it. Hashing makes it easy to check if the contents of the block is edited or not.

**Hash of Previous Block:** The third important component of a block is including the hash of the previous block. The figure above illustrates how the blocks are connected with hashes.

The first block of a chain is called the Genesis block. It is the only block that does not contain a hash of a previous block.

Let’s say an attacker tampers with the contents of one block. That would change the hash for that block. Because the next block contains the hash of the edited block, the hash for the next block would also change. And this would go on to the end of the blockchain. That means the whole chain is different because of one small adjustment. This is what makes blockchain hard to tamper with.

* + 1. Core Concepts

**Decentralization:** to remove the risk that comes with storing all data centrally, in blockchain, data is stored and replicated across all nodes across its peer-to-peer network.

Node - a computer connected to the blockchain network that performs the task of validating and relaying transactions — which gets a copy of the blockchain, which gets downloaded automatically upon joining the blockchain network.

Every node on the blockchain has a copy of the block chain. Because there is no central authority, there is no ‘official copy.’ Each node has the data. When a new block is added to the chain, it is broadcasted to all on the network. Each node will then update its local copy to reflect the latest chain available.

Any node can create a new block to add to the chain. But since there is no central authority of regulate and check it is a valid block, there needs to be a protocol on the network that ensures each block added is valid. The process of a block being accepted as valid by nodes is called consensus.

**Consensus:** is an agreement across all nodes that a block is valid and should be added to the chain.

There are several ways used to achieve consensus. The one used the most currently is consensus through proof-of-work. This process requires the node adding the block to do a costly computation to prove that the block is valid. This technique will be discussed in better detail in section 2.4.

**Asymmetric Key Cryptography:** The blockchain network utilizes the capabilities of public key cryptography for secure operation of the blockchain. The private key of a user is used to generate digital signatures and show ownership. The public key is used as a pseudonym user address.

* 1. Classification of Blockchain System
  2. Consensus Algorithms
  3. Uses of Blockchain

There are various areas in academics where Blockchain and its key features can be used. Let us analyze them.

* Data Management – Every year there are thousands of students that enroll in college and universities. Though we have a digital system nowadays still most of the work remains in the paper. Thus, finding particular data from the pool of so many data not only becomes time-consuming but also a tedious task. But having all the information fed on the ledger will make it easy for people associated with it, easily extract any piece of information without any delay.
* Digital identity — with the changing times, there is a huge demand for digital identity. With the help of Blockchain technology, we can give complete control of one’s personal data to individuals and this would lower the cost of the data management system and personnel. Basically, Blockchain will bring a huge transformation from a paper-based system to a paperless system.
* Data Verification – This is another area where Blockchain can prove to be extremely beneficial in this sector. With the help of Blockchain, we can easily verify data. Once the data or information of student is entered in the ledger it gets time-stamped and then altering the data is not possible. Since every information or block is associated with another, changing one data would require the hacker to change 6 other blocks which are a nearly impossible task. Thus, the Blockchain based system in higher education can be used for data verification. This becomes even more important in times like today when we need system from where we can easily track the data and also ensure that the information is authentic.
* New Job Prospect – Another key area where Blockchain can prove beneficial is introducing it as a part of our curriculum. We know that the world is slowly realizing the importance of Blockchain and with companies like Facebook creating a spate division for Blockchain based development, the future holds a lot of opportunities for students. Many institutes have introduced Blockchain as a part of regular education.
* Smart Contracts – Well, whenever we talk about Blockchain, then often smart contracts are associated with payments but, its application is huge. Institutes can use this technology to hand over certificates and degrees once the student successfully clears the exams on the parameter set by the institute.

Blockchain technology has come a long way from its origin as a financial instrument that was free from the control of any world government or corporation. But as the blockchain mania of the last two years has shown us, blockchain’s use case goes far beyond what was initially thought possible. The new use case for blockchain is largely attributed to the second generation of blockchain platforms like Ethereum which enabled smart contract functionality.

* + - 1. Technical analysis

Block chain

Bitcoin keeps a public ledger of all transactions, called the block chain. This is, in essence, a peer-to-peer distributed timestamp server. Its role is to prevent double spending and modification of previous transaction records.

Each full node in the Bitcoin network keeps a complete copy of the block chain, containing all blocks validated by that particular node. Consistency across the network is guaranteed by following a series of consensus rules. When several nodes in the Bitcoin network independently arrive at identical block chains, they are considered to be in consensus.

The terms ‘cryptocurrency’ and ‘altcoins’ or ‘altcurrency’ can be used interchangeably to “describe platforms that rely on the blockchain and on double-key cryptography and employ a peer-to-peer structure, to ‘issue digital cash’, usually called ‘coin’, with the aim of transmitting economic value across the Internet.

Bitcoins are generated by using an open-source computer program to solve complex math problems in a process known as mining each Bitcoin is defined by a public address and a private key, which are long strings of numbers and letters that give each a specific identity. This means that Bitcoin is not only a token of value but also a method for transferring that value.

Let’s take a closer look at a Block:

**Data** - Depends on the type of the block chain. The bitcoin block chain for example stores the details about the transaction in there.

**Hash** - you can compare a hash to a fingerprint. It identifies a block in all of its contents and its always unique. It is very useful to detect changes through block. If the hash of a block changes, it is then no longer is the same block.

**Hash of previous block** - This effectively makes a chain of blocks and it is this technique that makes it secure.

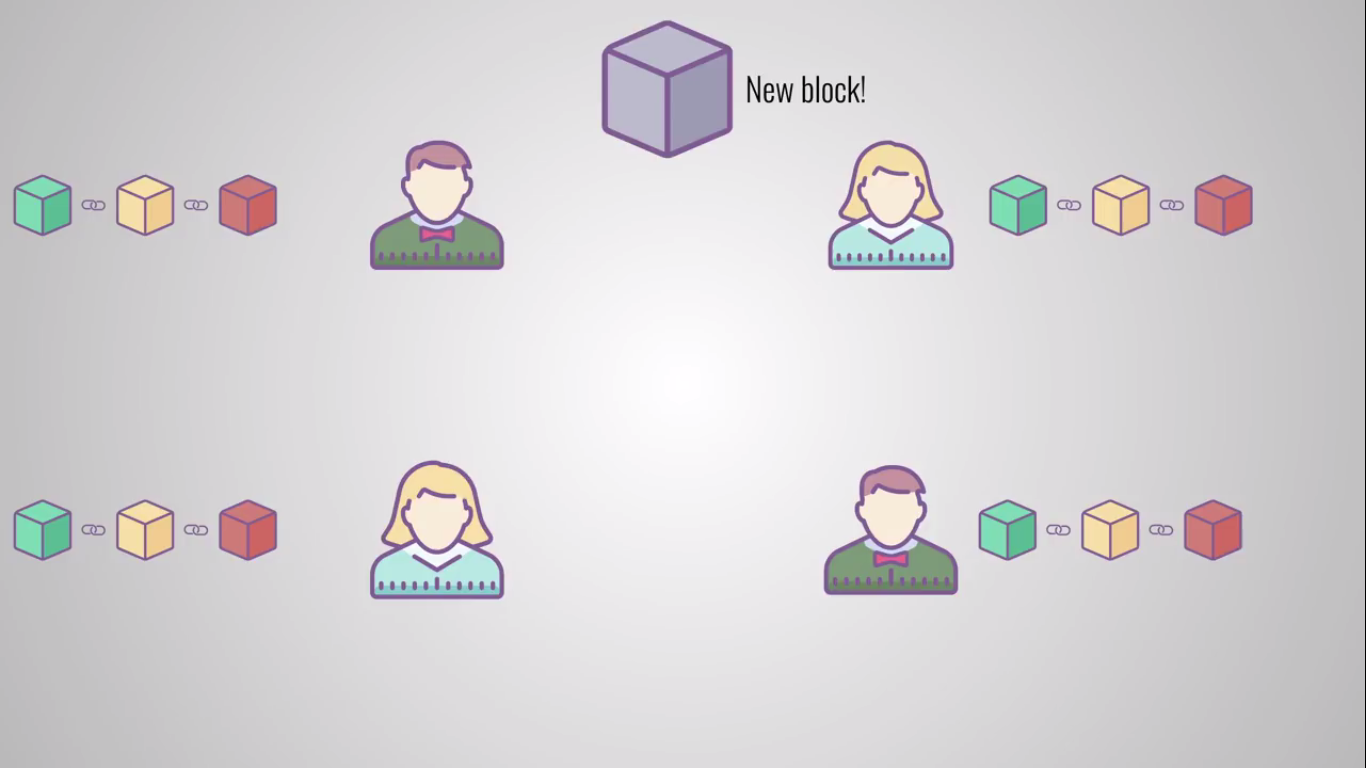
We call the first block the Genesis block, which has no previous hash and it cannot point to a previous block because it’s the first one.

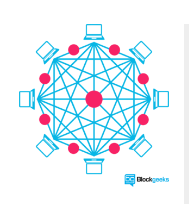
Let’s say we tamper with the second block, this causes the hash of the block to change as well. Therefore it would make block three and all the following blocks invalid because they no longer store a valid hash of the previous block. So changing a previous block will make following blocks invalid.

**Proof of work** validates transactions submitted to the blockchain through a collective process known as ‘mining’ in which miners must solve a mathematical puzzle derived from the transaction’s header before a new block can be added to the chain. As transactional blocks are created miners take the information in the block, and apply a mathematical formula to it creating a far shorter, seemingly random sequence of letters and numbers known as a hash. This unique hash is stored with each block, and also incorporates the hash of the preceding block in the chain, creating a definitive time-stamping process. The most widely used secure hash algorithm (or SHA) is SHA-256, which produces a unique fixed-size 256-bit hash.

But using hash is not enough to prevent tampering. There is another way block chain secures itself and that is by being distributed. Instead of using a central entity to manage the chain, block chains use a P2P(peer-to-peer) network where everyone is allowed to join. When someone joins he/she gets a full copy of the blockchain .

When someone creates a new block that block is sent to everyone on the network. Each node verifies the block to make sure it hasn’t been tampered with and each node adds the new block to their own blockchain. All the nodes create consensus, they agree upon what blocks are valid and which are not. Those that are tampered with will be blocked by nodes.





A network of so-called computing “nodes” makes up the blockchain.

Node - a computer connected to the blockchain network using client that performs the task of validating and relaying transactions — which gets a copy of the blockchain, which gets downloaded automatically upon joining the blockchain network.

Cryptographic keys aim to protect data from unauthorized entities; these digital keys utilize encrypted data known as cypher text, which appears as a random assortment of letters and numbers. This data can only be unencrypted with a corresponding key. A public key is typically distributed or made readily available, while only authorized users keep a private key confidential. Known as asymmetric cryptography, data can flow in either direction when using public and private keys and is utilized within blockchain to identify accounts and authorize transactions.

The main purpose of this component of blockchain technology is to create a secure digital identity reference. Identity is based on possession of a combination of private and public cryptographic keys. The combination of these keys can be seen as a dexterous form of consent, creating an extremely useful digital signature. In turn, this digital signature provides strong control of ownership .

Public to private transactions can be likened to a mailbox; anyone can submit a letter (public key) but only the owner can open the box (private key). Private to public transactions are similar to a noticeboard where everyone who has a copy of the public key can read the messages, but only the owner of the private key can create and post.

1. Related works
   1. Introduction
   2. Crypto-currency
   3. Something else
2. Applications of blockchain

Blockchain technology has the potential to upend the way every industry manages its information and data, not only financial services.

Imagine being able to track shipments through your supply chain with ease, down to the individual package or even component level. Or, executing a contract with a vendor without the need for an intermediary auditor. Blockchain can even help verify materials and food sourcing to ensure health and ethical standards are maintained.

The potential industry disruptions included are-

Legal: “Smart contracts” stored on the blockchain track contract parties, terms, transfer of ownership, and delivery of goods or services without the need for legal intervention.

Supply Chain: By utilizing a distributed ledger, companies within a supply chain gain transparency into shipment tracking, deliveries, and progress among other suppliers where no inherent trust exists.

Government: Blockchain offers promise as a technology to store personal identity information, criminal backgrounds, and “e-citizenship,” authorized by biometrics.

Energy: Decentralized energy transfer and distribution are possible via micro-transactions of data sent to blockchain, validated, and re-dispersed to the grid while securing payment to the submitter.

Food: Using blockchain to store food supply chain data offers enhanced traceability of product origin, batching, processing, expiration, storage temperatures, and shipping.

Retail: Secure P2P marketplaces can track P2P retail transactions, with product information, shipment, and bills of lading input on the blockchain, and payments made via Bitcoin.

Healthcare: Electronic medical records stored in a blockchain, accessed and updated via biometrics, allow for the democratization of patient data and alleviate the burden of transferring records among providers.

Insurance: When autonomous vehicles and other smart devices communicate status updates with insurance providers via the blockchain, premium costs decrease as the need for auditing and authenticating data vanishes.

Travel and Hospitality: Passengers store their authenticated “single travel ID” on the blockchain for use in lieu of travel documents, identification cards, loyalty program IDs, and payment data.

Education: Educational institutions could utilize the blockchain to store credentialing data around assessments, degrees, and transcripts.

* 1. Importance of Blockchain in Healthcare Data Management

**Healthcare Industry Rife With Data Breaches**

The last few years have seen several high profile cyber attacks in healthcare systems across the world. Perhaps none was more shocking and enormous than the hacking of United Kingdom’s National Health Service (NHS) on 12 May 2017. The UK spends over £125 billion every year on the NHS which has over 100,000 doctors and close to 400,000 support staff. The NHS treats more than 64 million patients every year in the UK and 54 million patients in England alone. The hack which was part of the larger wave of cyber attacks called “WannaCry” ransomware affected over 300,000 computers worldwide and brought the NHS to its knees. The  WannaCry exploit was reportedly distributed via email attachments and could propagate itself throughout the network from one infected machine. Once the exploit had been replicated to a large number of machines, the payload was delivered in the form of locking up all of the files on the computers by encrypting them to prevent access. Then the hackers demanded payments in untraceable cryptocurrencies in order to give back access. Affected areas were severely hit in their ability to treat patients and estimates put the number of deaths due to the hack at close to 900.

* 1. Blockchain & Healthcare

Due to their decentralized nature, blockchain has a very large amount of computational power backing them up which makes it virtually impossible for them to get hacked. Blockchain also allows for users on the internet to be securely identified using their cryptographic private keys. These two properties of blockchain can be combined to create data management systems that are completely resilient to hacks because they don’t suffer from a single point of failure.

In fact, ID management companies are using blockchain for this very purpose – they upload a digitally verified copy of a user’s ID documents like passports or driving licenses to their blockchain. Later, when an entity requests access to that document, the user gets a prompt on their phone from which they can choose to allow or deny the request. The same model can be applied to healthcare records as well so that people are not left in the dark about their sensitive information being exposed like in the case of a hack. This also has the added advantage of simplifying data provenance – users can opt-in to share the medical data with researchers anonymously so that their results can be used to develop better treatments in the future. Also since there are no middlemen in this transaction, healthcare researchers can be sure that data integrity has not been compromised.

The current literature surrounding blockchain and the healthcare industry indicates promise in simplifying an array of healthcare data transactions on both the business and clinical sides of healthcare--from claims adjudication to precision medicine.Centered at the core of such discussions is the concept of interoperability across a range of stakeholders. Capitalizing on this technology has the potential to connect fragmented systems to generate insights and to better assess the value of care.

* 1. Pharmaceuticals And Fraud Detection

Not unlike cryptocurrency transactions, blockchain technology can be used in a similar fashion to monitor the production and distribution of pharmaceutical drugs. Mettler (2016) notes that in 2010 the World Health Organization estimated “[10%] of drugs are counterfeit worldwide” with increases as high as 30% in developing countries. Pharmaceutical products include lifestyle supplements and “also drugs for the treatment of cardiovascular disorders and cancer, antibiotics, painkillers, contraceptives and other[s]”. The World Health Organization notes that counterfeit pharmaceuticals often include the correct active ingredient in a higher or lower than stated dose, causing adverse or undesired reactions (WHO, 2010).

* 1. Drug And Food Supply Chain

Medical supply chain may benefit from blockchain technology to help protect public health. Such systems can trace the origins of drugs by logging time series drug transaction data generated by IoT sensors to a blockchain to prevent counterfeits. The record of drug transactions among manufacturers, wholesalers, retailers, pharmacies, hospitals, and consumers, can turn the drug supply chain from regulating (government audits) to surveillance (by every participants collaboratively) .

* 1. Blockchain And Government

Douglas (2017) observed that blockchain technologies offer innovative solutions for two of the most persistent problems currently faced by governments – the establishment of identity records, and the creation of trust in digital environments. Such elements are crucial to the success of nation-states, as:

* + “untrustworthy civil registration entries may mean that citizens are unable to prove their identities as a necessary precondition of accessing social protection benefits, or that opportunities for identity fraud emerge that undermine a country’s immigration policies and national security”

Three emerging areas within the literature surrounding blockchain implementation include identity records and the case of e-Estonia(country that first implemented E-identification for residents), land registry systems in both the Western and developing world, and emerging theories on the potential use for democratic elections and other third-party voting systems.

* + 1. Land Registry

A land registry typically refers to the means by which a government agency records matters of ownership and rights to land; this may include evidence of title, and the facilitation of possession transactions, with the intent to prevent unlawful or fraudulent activities.

The advantages of blockchain in this instance are twofold.

* First, creating an accessible land registry utilizing blockchain technology allows citizens a new means of participation — in both registering assets, and in verifying legitimacy of current land titles. With transactions placed on a private blockchain, the subsequent cryptographic hash is:
  + made public on the Bitcoin blockchain to verify the authenticity of certificates. The hash serves as a digital fingerprint allowing anyone to verify that the data matches what is on the blockchain without actually seeing the data itself.
* Second, a land registration transaction in the Republic of Georgia historically requires at least 24 hours processing time with a fee, paid in-person by a buyer or seller to a registry house; under the blockchain system, fees to buyers and sellers are “in the range of $.05-$.10[USD]” with subsequently reduced processing timeframes .
  + 1. Elections

In lieu of current paper-based systems of voting, blockchain offers a solution in conjunction with the use of i-voting (where votes can be cast using a web browser) and/or e-voting (electronic votes tallied at a polling station). The aims of digital voting systems utilizing blockchain are twofold: first, to provide an unprecedented level of voter privacy, and second, to ensure each voter is unique and able to ensure their vote is tallied as cast. In considering the efficacy of such suggested digital systems, several social assumptions are made: that a country or jurisdiction utilizes a system of constituency based voting, that all voters have been assigned a unique identifier or other form of reference, and in the case of e-voting, a reliable network connection must be present at all polling stations (Barnes, Brake and Perry, 2016).

* RETAIL INDUSTRY: THE EXCHANGE OF GOODS & SERVICES

Much of the current blockchain literature focuses on establishing systems of trading for non-physical assets, be they digital or financial. However, emerging trends also exhibit a natural evolutional interest in a decentralized marketplace for both goods and services.

* MEDIA, CULTURE AND ENTERTAINMENT

Intellectual property protection for digital media is also a common blockchain application. The system in proposes to register self-embedding watermarking processed images on the blockchain in order to preserve transaction trails and content modification histories, and provide tamper detection for digital image management and distribution.

Blockchain technology application transforms the roles of third party intermediaries in the media industry, making artists' careers more sustainable by improved overall transparency of the value chain.

1. Future work
   1. Introduction

Dubai will be the first blockchain powered government, driving the future economy.

"Adopting Blockchain technology Dubai stands to unlock 5.5 billion dirham in savings annually in document processing alone — equal to the one Burj Khalifa’s worth of value every year." The Dubai Blockchain Strategy establishes a roadmap for the introduction of Blockchain technology for Dubai and the creation of an open platform to share the technology with cities across the globe. The Dubai Blockchain strategy is built on three pillars of government efficiency, industry creation and international leadership. [10]

* 1. Crypto-currency

1. Conclusion

With blockchain, we can imagine a world in which contracts are embedded in digital code and stored in transparent, shared databases, where they are protected from deletion, tampering, and revision. In this world every agreement, every process, every task, and every payment would have a digital record and signature that could be identified, validated, stored, and shared. Intermediaries like lawyers, brokers, and bankers might no longer be necessary. Individuals, organizations, machines, and algorithms would freely transact and interact with one another with little friction.