***Blockchain-Etherium ledger application for Real Estate***

Dissertation presented to the Systems and Computation Engineering department

by

**Daniel Perilla Ocampo**

Consulting professors:

Sandra Julieta Rueda Rodríguez

Systems and Computation Engineering

Universidad de los Andes

Bogotá, Colombia

2021

Table of contents

[Image Table 4](#_Toc78290109)

[Summary 7](#_Toc78290110)

[Abstract 8](#_Toc78290111)

[Chapter I. Introduction 9](#_Toc78290112)

[Chapter II. General description 11](#_Toc78290113)

[2.1 Project objectives 11](#_Toc78290114)

[2.1.1 General objectives 11](#_Toc78290115)

[2.1.2 Specific Objectives 11](#_Toc78290116)

[2.2 Conceptual Framework 11](#_Toc78290117)

[2.3 Previous works 14](#_Toc78290118)

[References 58](#_Toc78290152)

# 

# Image table

[Figura 1 Detección de distancia (LiDAR) para una imagen [9] 12](file:///C:\Users\Vilma%20Tirado%20Gomez\Documents\Universidad\9no%20Semestre\Tesis%20ISIS\Documento%20Proyecto%20de%20grado.docx#_Toc78290153)

# 

# Summary

“The **World** **Economic** **Forum** (WEF) has identified **blockchain** technology as one of its six mega-trends in a new report broadly aimed at outlining the expected transition to a more digital and connected world”1. This Project has the intention of applying blockchain technology to the Real Estate field. To accomplish this objective, the first approach is to create an Etherium based blockchain application on horizontal property alone (land) and on a second moment, the addition of vertical properties (houses, apartments, etc.). The finished product will have the qualities of being persistent and allowing transactability between the participants of the blockchain. Such transactions are buy-sell transactions, registration of properties and deletion of properties. Also, the application will have the an auditing capability where consultation of a property’s transability and information verification.

# 

# Abstract

“The **World** **Economic** **Forum** (WEF) has identified **blockchain** technology as one of its six mega-trends in a new report broadly aimed at outlining the expected transition to a more digital and connected world”1. This Project has the intention of applying blockchain technology to the Real Estate field. To accomplish this objective, the first approach is to create an Etherium based blockchain application on horizontal property alone (land) and on a second moment, the addition of vertical properties (houses, apartments, etc.). The finished product will have the qualities of being persistent and allowing transactability between the participants of the blockchain. Such transactions are buy-sell transactions, registration of properties and deletion of properties. Also, the application will have the an auditing capability where consultation of a property’s transability and information verification.

# 

# Chapter I. Introduction

# Chapter II. General description

## 2.1 Project objectives

1. As of 2021 there is not a blockchain application system that has the information related to the ownership of Real Estate properties, as a result the system is inefficient and slow. Also, fake registers may appear, as in the case of the “Cartel de los escrituradores”.

2. For a future colonization of mars and extraplanetary entities, there needs to be a reliable source of information, transactionality and validity of ownership in relation to the ownership of extraplanetary land.

### 2.1.1 General objective

I want to make a blockchain application that not only has the information of who owns a certain piece of Real Estate in real life but also is also able to register the change of ownership of such properties in buy-sell transactions.

As a result, where it to be integrated in governmental agencies, there would be an increase in efficiency and a considerable security increase in respect to the safety and legitimacy of the registers in the ledger.

### 2.1.2 Specific objectives

* Research on Ethereum blockchain: Understand what the requirements are to create a viable blockchain on the Etherium platform.
* Creation of Etherium blockchain for horitzontal real estate (land, as if the earth was without buildings, use it to see implementation of mars and moon territories) this stage needs to include access control, transactability and security.
* Increase Etherium blockchain capability by adding horizontal properties. (Buildings)

## 2.2 Conceptual Framework

## 2.3 Previous works

# Capitulo III. Design and implementation

### 

Udemy: Introduction to Blockchain with Industry Applications

What is Blockchain?

“The blockchain is a digital, decentralised, distributed **ledger**.”[1]

“A ledger consists simply of data structured by rules. Any time we need a **consensus**about **facts**, we use a ledger.”

ledger - **a record in which commercial accounts are recorded;**

1. **Ledgers confirm ownership.**
2. **Ledgers confirm identity.**
3. **Ledgers confirm status.**
4. **Ledgers confirm authority.** Ledgers identify who can validly sit in parliament, who can access what bank account, who can work with children, who can enter restricted areas.

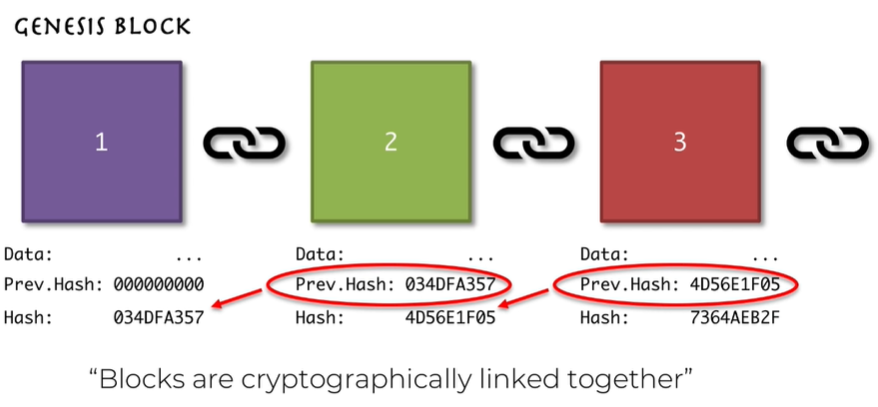
“A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography” – Wikipedia

Elements of the block:

1. Data: e.g. “Hello World!”
2. Previous Hash: 034DFA357
3. Current Hash: 4D56E1F05

“The current hash is a fingerprint of the data inside a block”, it works as an identifier of the information contained in the block.

“The first block in a blockchain is always called a genesis block because it will never change”, the previous hash of the genesis block is 000000000. If for example the first block has a current hash of 034DFA357 then the second block in the chain will have the hash 034DFA357 as its previous hash. For every new block, the previous hash will correspond to the current hash of the previous block. The relation between these blocks is described as them being “cryptographically linked” since every two sequential blocks will have the same hash code for a previous hash and for a current hash.



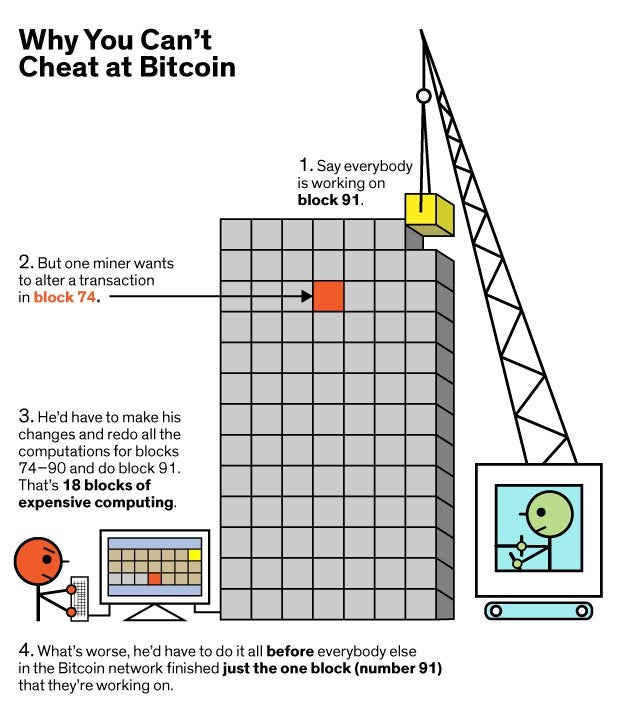
There are many ways to encrypt the information of a block, there is for example ECC, RSA and SHA256. In blockchain however it is most commonly used the SHA256 (WHY IS THIS ONE USED INSTEAD OF ECC)

Comparison of using a cryptographic code to a human fingerprint in its property of being unique.

SHA stands for (Secure Hash Algorithm 2) They are built using the [Merkle–Damgård construction](https://en.wikipedia.org/wiki/Merkle%E2%80%93Damg%C3%A5rd_construction), from a [one-way compression function](https://en.wikipedia.org/wiki/One-way_compression_function) itself built using the [Davies–Meyer structure](https://en.wikipedia.org/wiki/One-way_compression_function#Davies%E2%80%93Meyer) from a specialized [block cipher](https://en.wikipedia.org/wiki/Block_cipher).

In order to use a certain cryptographic function depends on if the function complies or not with the following:

1. One-way: There is no way to reconstruct the information of the block from the hash, just to create the hash from the block. (The hash is just used for identification)
2. Deterministic: Independent of how many times you apply the same operation over the same data the result must be the same.
3. Fast Computation: The calculation required to create the hash must occur in a fast manner.
4. The Avalanche Effect: Any change made on the block, regardless of the size of the change will completely change the resulting hash.
5. Must withstand collisions (Pidgeon hole principle): Given that the hash is limited in length (64 characters long) and there are more blocks that identifiers, there is a way for the algorithm to manage collisions.



Distributed P2P Network second mechanism of defense, even if there was someone who theoretically had the computational power and time to change the hashes of all blocks, there is still one characteristic of the blockchain that protects it form attack. Distributed P2P network, the blockchain resides in not only one computer but on many computers at the same time. This distribution allows the system to compare the different versions of the blockchain file that are in the different computer, if all are synchronous to one another then further transactions on the block are valid, if on the other hand there is one computer doesn’t have the same information as the others, the other computers in the network detect the different version of the blockchain an immediately restitute the different version to the version of the majority. (HOW DOES THE COMPARISON BETWEEN THE DIFFERENT VERSIONS OF THE BLOCKCHAIN OCCUR ) (HOW DO CHANGES IN THE BLOCKCHAIN HAPPEN AT THE SAME TIME?)

It is a decentralized way of managing the information, there is more than one (punto de falla)

The more computers that are on a network the safer it is, (EXPONENTIALLY PROPORTIONATE OR DIRECTLY PROPORTIONATE)

Characteristics of a blockchain:

1. Security: It is secure not only due to the cryptographic blockchain but also due to the P2P network implementation.
2. Access Control: The registers in a blockchain just contain the identification of the block. Without the corresponding private key to the already encrypted information with public key data in the blockchain, there is control in who is allowed to be given the private key to see the information in a block.
3. Transparency: Any one in the network can see the blockchain registers. There is no hiding things anyone can go and see the transactions that have taken place in the blockchain.
4. Traceability: There is a record of the history of an item, there is data of who bought, who sold, when was it sold and for how much.
5. Borderless: The blockchain can be based on computers in many different countries.
6. No intermediaries: It completely removes intermediaries, there is no bank or other entity that entangles with the transactions. There is no need for intermediaries as there is trust in the system since every actor in the system verifies the transactions, the trust is an inherent attribute of the technology.
7. Reduced Costs: No need for banking infrastructure, less costs in money transactions.
8. Speed: Transaction speeds can be increased since there are no intermediaries.
9. Efficiency: As there is only one system that serves the public the transactions in the blockchain are much more efficient since there is no passing of information.
10. Data ownership: No one organization can say that they own your data since it is your data that is distributed in a network and none but yourself have rights to it.

History:

“Ledgers appear at the dawn of written communication. **Ledgers and writing developed simultaneously** in the Ancient Near East to record production, trade, and debt. Clay tablets baked with cuneiform script detailed units of rations, taxes, workers and so forth. The first international ‘community’ was arranged through a [structured network of alliances that functioned a lot like a distributed ledger.](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3016649)”[1]

“The first major change to ledgers appeared in the fourteenth century with the invention of **double entry bookkeeping**. By recording both debits and credits, double entry bookkeeping conserved data across multiple (distributed) ledgers, and allowed for the reconciliation of information between ledgers.”[1]

“The nineteenth century saw the next advance in ledger technology with the rise of large corporate firms and large bureaucracies. These **centralised ledgers** enabled dramatic increases in organisational size and scope, but relied entirely on **trust**in the centralised institutions.[1]

“In the late twentieth century ledgers moved from analog to **digital ledgers**. For example, in the 1970s the Australian passport ledger was digitised and centralised. A database allows for more complex distribution, calculation, analysis and tracking. A database is computable and searchable.”[1]

“But a database still relies on trust; a digitised ledger is only as reliable as the organisation that maintains it (and the individuals they employ). It is this problem that the blockchain solves. The blockchain is a distributed ledgers that does not rely on a trusted central authority to maintain and validate the ledger.”[1]

Why is Blockchain secure?

The current hash of a block is generated with the data inside a block and the previous hash of the block.

As a result, if an intruder decided to change the data in a block, he would not only need to the current hash, but also the previous and current hash of all the blocks to the right, in ordered to make everything seem fine. This task is not only difficult, but considering that the blocks previous hash is unable to be modified after creation, the comparison between the previous hash a block and the current hash of the block being disrupted, will differ, which will immediately put in place a correction program.

Extraneous elements that need to be considered.

Identity shows who does a property belong to. Being that the “who” in this sentence refers to a person, and that a person is subjected to biological constraints. The death of a person and its status as alive or death needs to be reflected on the blockchain, and as a result there needs to be a move of properties that reflect that the property no longer belongs to a death person, but to a person/s that is/are alive. Properties are of no use to the dead.

“The register of Births Deaths and Marriages records the existence of individuals at key moments, and uses that information to confirm identities when those individuals are interacting with the world.”[1]

Industry Applications of Blockchain:

* Bitcoin

“But the relationship remains — the value of the bill is dependent on a social consensus about the stability of the currency and government that issued it. Banknotes are not wealth, as Zimbabweans and Yugoslavians and Weimar Republic Germans have unfortunately learned. A bill is a call on a relationship in a (now synthetic) ledger and if that relationship collapses, so does the value of the bill.”[1]

Benefits of bitcoin:

* Cross border transactions become easier
* Faster transactions
* No intermediaries
* Very low fees
* Anonymity.

Bitcoin monetary policy consists of two parts:

1. The Halving: Every four years since 2012 the number of bitcoins gained from mining a bitcoin block has decreased by half. There is a desire to limit the amount of bitcoins in circulation so as to not devaluate the currency. By approximation there will be 21 million Bitcoins by 2140.

Table

Description automatically generated

1. Block Frequency: Every 10 min a new block is created, and it is controlled by the bitcoin network through the complexity of the mining process (i.e. the challenge to process the block.)

*“[Bitcoin] won’t end well, it’s a fraud…worse than tulip bulbs…[but] if you were a drug dealer, a murderer, stuff like that, you are better off doing it in bitcoin than U.S. dollars,”*

*— Jamie Dimon: CEO, JP Morgan*

*“To me and many others, bitcoin is not a technical revolution as much as it is a triumph of political and economic incentives.”*

*— Two Bit Idiot*

*“Systems like Ethereum (and Bitcoin and NXT, and Bitshares, etc) are a fundamentally new class of cryptoeconomic organisms — decentralized, jurisdictionless entities that exist entirely in cyberspace, maintained by a combination of cryptography, economics and social consensus”*

*— Vitalik Buterin*

Table

Description automatically generated

Contrywise:

* Citizenship
* Passports
* Taxes
* Social security
* Property ownership
* licences
* Elections
* Fiscalia

Brazil may write new laws with data stored on the Ethereum blockchain

* Bioinformatics: patent the dna of people in a hash that is placed in a blockchain

“ **‘regtech’**— the application of technology to the traditional regulatory functions of auditing, compliance, and market surveillance.”[1]

Industry:

1. Healthcare:
2. Finance:
3. Energy:
4. Internet:
5. Supply Chain:
6. Real Estate:
7. Retail:
8. Education:
9. Data Storage:
10. Government:

Timeline

Description automatically generated

In this matrix, we can see the relationship between the different promises that blockchain brings and the different industries, when the square is filled with blue, then there is a big impact of that specific characteristic of blockchain to that industry.

Healthcare:

* Security: We want to be sure that our healthcare data is safe. Prevents data from being tampered, stolen or destroyed if a healthcare provider that stores your data is hacked.
* Access Control: We can specify which doctors has access to our data, this also enables us to have a better service since our medical data can be seen by any medical professional who we desire to see our medical data, despite the different businesses they may belong to.
* Borderless: To access your medical data despite where you are in the world, useful for example when traveling.
* Efficiency. Many different healthcare providers can have fast access to your data.
* Data ownership: You own your data. The healthcare providers are not the owners of your data.

Example of the use of blockchain in the medical field:

Medicalchain.

[Home (medicalchain.com)](https://medicalchain.com/en/)

Nebula genomics:

[Whole Genome Sequencing DNA Test | Nebula Genomics](https://nebula.org/whole-genome-sequencing-dna-test/)

“Nebula Genomics will leverage blockchain technology to eliminate the middleman and empower people to own their personal genomic data”

Doc.ai

“We believe that in the near future, human biological profile will be consumer-controlled, blockchain-based, AI-powered and omics-data-centric.”

[Top 12 Companies Bringing Blockchain To Healthcare | LinkedIn](https://www.linkedin.com/pulse/top-12-companies-bringing-blockchain-healthcare-mesk%C3%B3-md-phd/)

Finance:

* Security: Important to have money transactions and storage be safe.
* Borderless: Overseas transactions.
* No intermediaries: Reduced costs due to the absence of intermediaries.
* Reduced costs: No intermediaries
* Speed: No intermediaries

Bitcoin.

Ripple: app for bank, wants to improve international transactions, it’s a layer of communication for banks so that international transactions can happen almost instantaneously.

ripple.com

“The world’s only enterprise blockchain solution for global payments”

[5 blockchain use cases in financial services | Deloitte Blog](http://blog.deloitte.com.ng/5-blockchain-use-cases-in-financial-services/)

Energy:

* Traceability: There is a way to know where the energy they are using is coming from (e.g. coal, hydro, wind, etc.)
* No intermediaries: Exchange energy between one another without intermediaries (e.g. use of solar panels for self energy productions)
* Reduced costs: No intermediaries
* Efficiency: Single source of truth for energy exchange between people.

Powerledger.io

“Empowering individuals and communities”

“Power Ledger is the world leading peer-to-peer marketplace for renewable energy.”

Internet:

* Security: Guaranteed security of their data online.
* Access Control: Supervision of who can access your data.
* Borderless: Internet should never abide to any countries particular laws.
* Data Ownership: Your data is not controlled by any organization. (Facebook, instagra, youtube, etc.)

In this specific case, the notion is that for the web 3.0 the personal data of the users should be stored and a blockchain and applications may have access to this data with the approval of the users.

[Why the Web 3.0 Matters and you should know about it | by Essentia 1 | Medium](https://medium.com/@essentia1/why-the-web-3-0-matters-and-you-should-know-about-it-a5851d63c949)

Steemit.com

“Twitter on the blockchain”

D.tube

Supply chain:

* Transparency: Makes sure that throughout the process there is no alteration or corruption of the products.
* Traceability: Track the origin and the route of the products, and make sure that they came from responsible sources. (Burmese rubis (blood rubis), blood diamonds, coral, child labor, ethical labor, etc.)
* Borderless: Cross border accessibility
* Efficiency: Single source fountain of information.

Provenance.org/technology

[Blockchain for Supply Chain - IBM Blockchain | IBM](https://www.ibm.com/blockchain/industries/supply-chain)

(Tradelens)

Food trust ibm

Real Estate:

* Security: We want to make sure our data is tamper proof, nobody should be able to maliciously modify the data of your property.
* Transparency: Who sold, who bought, amount of money, date, etc. Track the data in case of disputes. Clear of mortgages, history of the assets.
* Reduced costs: No property transactions or real estate transactions associated costs absence of lawyers, accountants, governments.

[A Pioneer in Real Estate Blockchain Emerges in Europe - WSJ](https://www.wsj.com/articles/a-pioneer-in-real-estate-blockchain-emerges-in-europe-1520337601#:~:text=A%20Pioneer%20in%20Real%20Estate%20Blockchain%20Emerges%20in,in%20Stockholm%20in%20June.%20Photo%3A%20Mikael%20Sjoberg%2FBloomberg%20News)

[A Vermont City Tests Blockchain Technology for Property Deals - WSJ](https://www.wsj.com/articles/a-vermont-city-tests-blockchain-technology-for-property-deals-1517351207)

[Cook County Blockchain Report | CryptoCoins Info Club](https://cryptocoinsinfoclub.com/bitcoin/cook-county-blockchain-report)

Retail:

* Transparency: If there is a need for auditing, there information of sales stored in the audit may be seen easily in the blockchain when authorized.
* No Intermediaries: There is no need for entities between the sellers and the buyers.
* Reduced Costs: Absence of intermediaries reduces cost of products.
* Speed: Absence of intermediaries reduces speed of payment and shipment.

[deloitte-uk-blockchain-in-retail-and-cpg.pdf](https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/ConsumerIndustrialProducts/deloitte-uk-blockchain-in-retail-and-cpg.pdf)

Education:

* Access Control: Flexibility for content creators who wants to control who views their content.
* Traceability: For certifications, so that organizations can effectively trace that indeed a person has taken a certain course (assessments, videos views, tests, etc).
* Borderless: Access of education from anywhere.
* Data Ownership: Data of a student or content of a creator owned by a student or creator respectively.

Accredible.com

Blockcerts.org

[10 ways Blockchain could be used in education – OEB Insights](https://oeb.global/oeb-insights/10-ways-blockchain-could-be-used-in-education/)

Data Storage:

* Security: We want our data stored to be safe.
* Borderless: We want to access our data anywhere in the world.
* Data Ownership: We want to own our data, no central authority or company makes use or owns our data.

Sia.tech

Cloud storage using blockchain

Government:

* Security: Government data must be secure.
* Transparency: Audit of records in order to have certainty that there is no corruption in certain transactions.
* Reduced costs: Absence of many servers to maintain different ledgers
* Efficiency: Reduced the amount of systems used single digital ledger for different government organizations.

[Blockchain in Government: Making Operations More Efficient (coincentral.com)](https://coincentral.com/blockchain-in-government/)

* Employment
* **Cryptobank- “**n autonomous blockchain application that borrows short and lends long, perhaps matching borrowers with lenders directly. A cryptobank structured algorithmically by smart contracts would have the same transparency properties as the bank with a public blockchain ledger but with other features that might completely neglect the need for regulators. For example, **a cryptobank could be self-liquidating**. At the moment the cryptobank began trading while insolvent, the underlying assets would be automatically disbursed to shareholders and depositors.”[1]
* “Employment is a ledger, giving those employed a contractual claim on payment in return for work.”[1]
* Bioinformatics: patent the dna of types of plant like marihuana in a hash that is placed in a blockchain
* Patents
* Credito rotativo, BBVA, Repsol sign agreement to develop blockchain-based financial solution.

Systems:

* Capitalism

“Agreement about the facts and when they change — that is, a consensus about what is in the ledger, and a trust that the ledger is accurate — is one of the fundamental bases of market capitalism.”[1]

Consequences:

“Oliver Williamson, the 2009 Nobel laureate in economics, argued that people produce and exchange in markets, firms, or governments depending on the relative **transactions costs** of each institution. Williamson’s transactions cost approach provides a key to understanding what institutions manage ledgers and why.”[1]

Due to the fact that blockchain can reduce of costs and difficulty in relation to the amount of money a government has to use maintaining a series of institutions and in the intricacy of doing a transaction with one of the governments institutions. It can be said that blockchain not only has the capability of giving countries resources to grow, but also to accelerate transactions and decrease bureaucracy.

**“Firms and governments can use blockchains to make their work more efficient and reliable.** Multinational firms and networks of firms need to reconcile transactions on a global basis and blockchains can allow them to do so near-instantaneously. Governments can use the immutability of the blockchain to guarantee that property titles and identity records are accurate and untampered.”[1]

With the aim of prevent crime such as the one in the “El cartel de escrituradores: las estafas de compra y venta de predios – las dos orillas” “Alarma por red de estafadores inmobiliarios en el área metropolitana- vanguardia.com”

Or the creation of fake licenses . “Fiscalía denuncia construcción de edicios con licencias falsas en Santa marta- hoy diario del magdalena”

The solution is not as Jairo Mesa Supernotariodo said “Estamos luchando contra un cartel de las licencias de construcción” to require a security paper, this item can be falsified too, but instead to revamp the informational system with blockchain technology.

The solution is to have not only the licences, the terrenos and the properties in the same block.-

Problems with blockchain:

Energy: bitcoin is ineficient

References

1. CoinDesk. 2021. *World Economic Forum Survey Projects Blockchain 'Tipping Point' by 2023*. [online] Available at: <https://www.coindesk.com/world-economic-forum-governments-blockchain> [Accessed 9 August 2021].

[1]

Cryptoeconomics, “The Blockchain Economy: A beginner’s guide to institutional cryptoeconomics,” *Medium*, Sep. 27, 2017. https://medium.com/cryptoeconomics-australia/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2f2beec4.