ISTITUTO UNIVERSITARIO SOPHIA

LAUREA MAGISTRALE IN SCIENZE ECONOMICHE E POLITICHE

POSTGRADUATE MASTER'S DEGREE IN ECONOMIC AND POLITICAL SCIENCES

PROGRAMME IN ECONOMICS AND MANAGEMENT

SPECIALIZATION IN HUMANISTIC MANAGEMENT

TRUSTING A TRUSTLESS NETWORK

The Paradoxes of Trust in Blockchain Technology

JENA MARIE ESPELITA N°18LOEF0489

Supervisor:

Prof. ANNETTE PELKMANS-BALAOING

Co-supervisors:

Prof. IVAN VITALI

Prof. BENEDETTO GUI

ANNO ACCADEMICO 2019-2020

TABLE OF CONTENTS

ACKNOWLEDGEMENTS 6

INTRODUCTION 7

TRUST 10

1. Defining trust 10

1.1. Types of trust 11

1.2. Vulnerability and trustworthiness 13

2. The rise of distributed trust 14

2.1. How trust is broken 15

2.2. A crisis of trust 15

2.3. The trust shift 16

3. The Trust Stack 17

3.1. Trusting the idea 18

3.2. Trusting the platform 19

3.3. Trusting the other person 19

4. Trust Architectures 21

4.1. Peer-to-peer trust 21

4.2. Leviathan 22

4.3. Intermediary 22

5. “Trustless” Trust Architecture 23

BLOCKCHAIN 25

1. Defining a blockchain 25

1.1. Immutability 26

1.2. Distributed Ledger 28

1.3. Consensus 31

1.4. Tokenization 34
1.5. Smart Contracts 35
2. The Blockchain Trilemma: Decentralized, Scalable and Secure 38
2.1. Decentralization 38
2.2. Security 39
2.3. Scalability 39
3. Blockchain Ecosystems Landscape 41
TRUST AND BLOCKCHAIN 43
1. The paradoxes of trust in blockchain technology 43
1.1. Decentralized yet centralized 44
1.2. Immutable yet changeable 49
1.3. Transparent yet highly encrypted 53
1.4. Algorithmic yet human 58
1.5. Other considerations 61
2. Blockchain for Social Impact 62
2.1. Health 62
2.2. Agriculture 64
2.3. Land Rights 65
2.4. Energy 66
2.5. Digital Identity 67
2.6. Financial Inclusion 68
2.7. Governance and Democracy 69
SUMMARY, RECOMMENDATIONS AND CONCLUSIONS 71
BIBLIOGRAPHY 78

TABLE OF FIGURES

FIGURE 1. DEPICTION OF TRUST 13
FIGURE 2. TRUST LEAPS 17
FIGURE 3. SYMBOLIC REPRESENTATIONS OF THE THREE ESTABLISHED TRUST ARCHITECTURES 21
FIGURE 4. THE BLOCKCHAIN'S "TRUSTLESS" TRUST ARCHITECTURE 24
FIGURE 5. THE ARCHITECTURE OF MERKLE TREE IN THE BLOCKCHAIN 26
FIGURE 6. (A) CENTRALIZED. (B) DECENTRALIZED. (C) DISTRIBUTED NETWORKS 29
FIGURE 7. HOW A BLOCKCHAIN WORKS 35
FIGURE 8. HOW BLOCKCHAIN CRYPTOGRAPHY WORKS 36
FIGURE 9. THE BLOCKCHAIN TRILEMMA 40
FIGURE 10. CURRENT SECTORS USING BLOCKCHAIN IN EUROPE 41
FIGURE 11. REPRESENTATION OF A HARD FORK 52

ACKNOWLEDGEMENTS

This work is the culmination of all my adventures in these last two years, which are ironically unrelated to academics, but are of friendship, self-love, and perseverance even in the midst of a world that literally seemed to be falling apart – 2020, you are a wonder.

And with a heart full of gratitude, I would like to say “thank you” to:

My dad, who was the first one to read anything I’ve ever written, and has been the hardest and best critic. To my mom, who has supported me throughout everything: you and dad have been pliant bows to this living arrow. To my weird sisters: I have never come across such odd rocks; I hope you know how much you mean to me. To my on-call brother, who always picks up my calls at the strangest hours: here’s to adulting, eh? To my big brother, who I will always look up to: looky! I made a thingy! You all are the reason I’m still here, in every sense.

To my companions throughout these years in Sophia: non sarei soppravvissuta senza di voi, sarete sempre le mie sorelle. To Loppiano, the Filipino community, and all those who have given me light even through the briefest of encounters: each of you will forever be etched on my soul. To Sophia, and the exemplary professors who have given us so much more than just lessons in the classroom: you have inspired me and influenced me deeply as a person, and as a citizen of the world. To my supervisor and co-supervisors, thank you for the guidance and the freedom you have allowed me, with which I was able to write a thesis that I can be proud of. And finally, to my stripy friend and constant pep talker: it was a crazy ride, wasn’t it?

Thank you all, for every piece that each of you has added into this strange masterpiece that I’ve found myself in. To God be the glory.

INTRODUCTION

The Edelman Trust Barometer is a global survey that measures the people's trust in relationship with the four core institutions – companies or brands, governments, NGOs and media. For the year 2018, it revealed that trust has changed profoundly, and noted that although there is a divergence of trust in other aspects, the world is united on one front – all share an urgent desire for change. Only one in five feels that the system is working for them, with nearly half of the mass population believing that the system is failing them (Edelman, 2019). Studies attribute this loss of trust to the Global Financial Crisis of 2008, as its aftermath exposed systemic flaws that brought the world economic order to the brink of collapse (Edelman, 2017; Nandwani, 2019). The study further reveals that for the year 2019, despite it being in an era of strong global economy and near full employment within the surveyed countries, none of the four societal institutions that the study measures are trusted (Edelman, 2020).

Concurrently, technology continues to alter human behaviors and instincts, pushing institutions to keep up with changing customer expectations while simultaneously developing the technologies of the future (Marshall, 2018). According to Rachel Botsman (2017), these changes are indicative of a new phase in the evolution of trust. The dwindling of trust in institutional power is accompanied by an emergence of a new kind of trust that moves power away from a single source and shares that responsibility across a wide range of sources.

With the Global Financial Crisis as foreground, a white paper introducing Bitcoin was published in 2008 by a person (or a group) called Satoshi Nakamoto. It described the concept of a cryptocurrency implemented on top of a *blockchain*, which could provide an alternative way to build trust, record truth, secure transactions and create a decentralized network spanning the globe outside the purview of any authority (Nandwani, 2019). Riding the wave of *distributed trust*, the blockchain has been cause for much excitement since its very nature allows the empowering of communities over central authorities.

The potential impact of the underlying technology, much more than that of the cryptocurrency, is often compared to the impact of the Internet, which now pervades our

everyday life (Arun et al., 2019), and is considered a potential *disruptive technology*, i.e., an innovation that significantly alters the way that consumers, industries, or businesses operate because of the way it "generates" trust where there is none (Werbach, 2018).

The scope of this study derives from the literature gap in the definition of "blockchain trust". Andreas Anotonopoulos (2015), author of *Mastering Bitcoin*, calls the blockchain "trust-by-computation", while Reid Hoffman (2015), venture capitalist and LinkedIn founder, labels it "trustless trust". Academic Kevin Werbach (2018) contends that it is a new kind of trust altogether, while security technologist Bruce Schneier (2019) argues that there is no good reason to trust blockchain at all. The question, therefore, that the research poses is this: "How can 'blockchain trust' be defined, and can blockchain be trusted?".

This research is an exploratory one, given that blockchain is a relatively new technology and that most case studies are still in their infancy, save the earlier blockchains such as Bitcoin and Ethereum. The study employs a secondary research method, consisting largely of online and literature research. Case study research on the 2016 DAO hack has also proved useful in determining the limitations and areas for improvement of the technology. Primarily, the objective of the study is to examine the hypothesis that blockchain is indeed a technology that can pervade the world of finance, economics and other sectors as a new architecture of trust.

To understand the correlation between trust and blockchain, a deconstruction of some of our existing social and philosophical constructs is required, such as how we trust each other and how we arrive at the truth and then record it (Nandwani, 2019). Thusly, the first chapter discusses the general definition of trust, how trust is built, how trust is broken, the rise of distributed trust, and the various architectures of trust that have developed over history. Theoretically, this chapter aims to describe the societal foundations on which the blockchain is set.

In chapter 2, a technical overview of blockchain is presented, along with an outline of the so-called "Blockchain Trilemma". This section discusses the core concepts of blockchain, such as hashing, consensus algorithms, distributed ledger technology, and smart contracts. The Blockchain Trilemma, on the other hand, describes the ongoing attempt of developers to solve the equilibrium between decentralization, security and scalability. The chapter is capped off with a brief overview of the blockchain ecosystem and the technology's diffusion on a global scale.

Chapter 3 presents the findings about blockchain trust, structured into four paradoxes: decentralized yet centralized, immutable yet changeable, transparent yet highly encrypted, algorithmic yet human. It aims to adequately describe the various benefits, implications and limitations of each element that are inherent in a blockchain – the very features that make blockchain unique. The chapter then ends with some notable applications of blockchain in the social sector, demonstrating the possibilities that blockchain has in store for us.

Chapter 1

TRUST

Trust is an elusive concept. Despite its pervasiveness in the decisions we make on a daily basis, its definition has been a subject of discussion among philosophers for centuries. As Larue Tone Hosmer (1995) states, "There appears to be widespread agreement on the importance of trust in human conduct, but […] an equally widespread lack of agreement on a suitable definition of the construct."

Without trust, we would need to verify and secure the reliability of everyone we encountered, which is practically impossible. Trust is fundamental to almost every action, relationship and transaction (Werbach, 2018). Communities would definitely not exist without it, and so it makes human society itself possible (Luhman, 1979). It enables small and large acts of cooperation that all add up to increased economic efficiency (Botsman, 2017). Virtually every commercial transaction has within itself an element of trust, certainly any transaction conducted over a period of time (Arrow, 1972). In this sense, it is the oil that lubricates social and business transactions, and the factor that renders the boundless complexity of the modern world tractable (Werbach, 2018).

1. Defining trust

How do we define trust? Trust is not binary – one need not be categorized as either perfectly trusting or purely untrusting (Cross, 2005). Putnam (2000) distinguishes "thick" trust, arising from close-knit social relationships, from "thin" trust, among a society in general. Fukuyama (1996) differentiates high-trust and low-trust societies. Fernando Flores and Robert Solomon (2001) differentiate "naïve" trust, based on pure faith, from "authentic" trust, grounded in relationships. Botsman (2017) distinguishes "local" trust

from “institutional” trust, and later on “distributed” trust. For many, trust is about confidently relying on another person. The more we interact with a person over time, the more confident we become about how they will behave. This kind of trust is known as “personalized” trust, while “generalized” trust is the trust we attach to an identifiable but unidentified group or thing (Sapienza and Zingales, 2011). Trust can therefore be viewed on a spectrum along multiple dimensions.

1.1. Types of trust

Among the various taxonomies of trust, it can be broken down into two basic theoretical types: *cognitive trust* and *affective trust*. Although these two concepts are not perfectly discrete, they can serve as tools in analyzing and understanding the concept of trust.

1.1.1. Cognitive trust

A simplistic definition of trust is cognitive risk assessment: is it reasonable to rely on this person or organization? In its strictest form, it is based upon a cost-benefit analysis of the benefits of trust versus the associated risks (Cross, 2005). Economist Oliver Williamson (1993) describes this as “calculativeness” because it is subject to rational calculation. In a business context, it is necessary for any large entity to trust upon agents to perform transactions in order for the entity to gain the benefit of new business. On a more personal level, a mother gains free time from trusting a babysitter to watch her child. There is, of course, a running risk in both cases. An agent in the company might usurp a business opportunity, while the babysitter could harm the mother’s child. Cognitive trust requires an assessment of the probability and the magnitude of that risk of harm (Cross, 2005).

The cognitive assessment of trust is also affected by the facility and effectiveness of monitoring the party to be trusted. With the possibility of monitoring, one can find out if one’s trust is misplaced and thus withdraw from trusting. In assessing the relative risk of trusting, the *ex-ante* risks are often part of the equation as well, such as the reputation or past experiences or recommendations. *Post facto* remedies are also incorporated in the assessment of this risk. For example, laws against embezzlement provides a form of hedging against the risk that a company’s trust was misplaced (Luhman, 1979). Another example can be found in e-marketing, wherein the customer is asked to give the number

of his credit card to the marketer on a platform such as Amazon or other online retailers. While it would seem unlikely that such private information should be entrusted to a stranger, people do indeed give up their credit card numbers because of legal protections against credit card fraud, plus the effects and potential legal penalties on the marketer's firm should discourage misuse of the number. Taking everything into account, a cognitive assessment of the user would arrive at the conclusion that the credit card number would not likely be abused (Cross, 2005).

1.1.2. Affective trust

While the cognitive dimension is important, it cannot represent the entirety of trust. Otherwise, trust would be nothing more than rational reliance. Affective trust, on the other hand, is considered to be "true" or "real" or "moralistic", and has no obvious strategic component (Rose, 1995). It is the optimistic disposition toward others that operates outside strategic motivation – an expectation of goodwill on the part of an agent (Baier, 1986). In this category, "to trust someone is to have an attitude of optimism about her goodwill and to have the confident expectation that, when the need arises, the one trusted will be directly and favorably moved by the thought that you are counting on her". In affective trust, "we impute honorable motives to those we trust" and "typically do not even stop to consider the harms they might cause if they have dishonorable motives" (Jones, 1996). In a business context, we can think of the bank that gives a failing but sympathetic borrower another chance, rather than foreclosing when it has the right to do so.

Moreover, there are moral aspects to affective trust (Wicks et al., 1999). Trust is an expression of our goodness, not simply of our self-interest. Fukuyama (1996) describes trust as "a set of ethical habits and reciprocal moral obligations internalized by members of a community." Such moral trust is a statement about how people *should* behave and how "they ought to trust each other" (Cross, 2005). If so, trust is commanded as a general rule, and is not a strategic calculation. Trust, therefore is a more complex psychological state that incorporates social and emotional factors, and is concerned with motives, not just actions or interests (Blair et al., 2018).

1.1.3. Combining cognitive and affective trust

Although there is a practical distinction between affective and cognitive trust, affective trust may itself be fundamentally cognitive and strategic if our nature is hardwired

by evolution into our brains or is the product of experience (Cross, 2005). Cognitive trust, while retaining its conscious assessment of risk, likewise contains an affective component. The most cognitive analysis of trust must still require some affective optimism about the party to be trusted. As a matter of human nature, behavior is rarely either entirely instrumental or purely emotion. Optimal trust, hence, is the combination of affective and cognitive trust (Wicks et al., 1999).

1.2. Vulnerability and trustworthiness

Trust, as we all know, is not an ironclad guarantee of performance, since trust can be exploited by the untrustworthy. As portrayed in Figure 1, trust is shown alongside the presence of danger. Do I trust in his strength or capacity to hold on to the arrow? Does he have any hidden intentions of hurting me? A gap exists, a grey area where something unknown could happen. A gap constantly exists in every transaction – in the encrypted algorithms upon entering your credit card details to buy something online; the first time you eat at a restaurant; or in our mere getting on a plane or train. To trust is to be vulnerable to the one trusted (Rousseau et al., 1998).

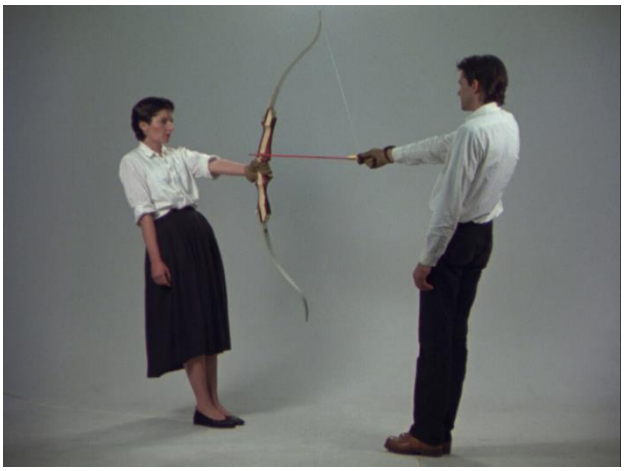


Figure 1. Depiction of Trust
(Marina Abramović and ULAY, 1980)

Vulnerability entails an interdependence between the actors in a relationship of trust, and calls to attention a second aspect: trustworthiness. According to Onora O'Neill (2002), the four traits of trustworthiness are the following: competency, reliability, integrity, and benevolence. Furthermore, Vittorio Pelligra (2013) cites various explanations in terms of game theory as to why a rational agent may decide to be trustworthy. The *Folk Theorem* suggests that in the long run, or more precisely in an infinitely repeated "trust game", it shows that trusting and being trustworthy are the most

rational courses of action. This is due to the fact that the choice of being or not being trustworthy could have repercussions on the future interactions with the partner. Other theories, such as enlightened self-interest, altruism, inequality-aversion, reciprocity, guilt-aversion, collective rationality and trust responsiveness are also cited, considering both exogenous and endogenous elements of influence on one's choices. Social approval, reputation, as well as the player's self-esteem, are all drivers of trustworthiness. In this regard, trust and trustworthiness can be considered as relational concepts, emerging and developing within a trust relationship (Pelligra, 2013).

Roger Mayer (1995) and his coauthors write: "Trust is the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other part." Trust, therefore, is a two-sided coin. On one side is a belief rooted in some combination of rational and emotional factors; on the other is acceptance of uncontrolled risk (Hurwitz, 2013). It is exactly this vulnerability alongside trust, however, that Satoshi Nakamoto, creator of blockchain technology, hopes to eliminate by proposing "a system of electronic transactions without relying on trust" (Nakamoto, 2009). The costs incurred along with the need for trust in intermediaries or third-parties are thus eliminated through a system based on cryptographic proof. This gave Reid Hoffman (2015) reason to label blockchain trust as "trustless trust". The questions that come to mind are: How can this kind of trust be defined? Or, does blockchain truly eliminate the need for trust?

2. The rise of distributed trust

In 2017, The Edelman Trust Barometer released a report entitled *An Implosion of Trust* and reveals that trust is in crisis around the world (Edelman, 2017). It finds that two-thirds of the surveyed countries are now "distrusters", i.e., less than half of the population trust the mainstream institutions of business, government, media and NGOs to do what is right. Around the world, high-trust societies outperform low-trust ones (Fukuyama, 1996). Business scholars similarly find empirically that companies where trust is high perform better (Davis et al., 1995). Societal trust has the capacity to shape interactions, potentially in very significant ways. It shapes both the macrostructures of national economic performance and the microstructures of individual and firm interactions (Werbach, 2018).

Those who are trusted are powerful, and systems that alter the scope of trust are therefore capable of changing societies. What then is causing the fraying of societal trust today?

2.1. How trust is broken

Trust can fail in three ways: direct violations, opportunistic behavior, and systemic collapse (Werbach, 2018). Violations of trust are the clearest examples – a restaurant that serves you substandard food; a friend who borrows money without any intention of paying you back; a politician stealing state funds – each takes advantage of the trustor's vulnerability to cause harm.

Trust is especially difficult to restore when the untrustworthy behavior involves deception, which is the foundation for the second category of trust breakdown: opportunism (Werbach, 2018). «Opportunism means violating the spirit, but not necessarily the letter, of an agreement by taking advantage of asymmetric information» (Muris, 1981). Gaming the reputational system, i.e., using fake accounts to post high-rated reviews on their own products, breaks the whole idea of trustworthiness within e-commerce.

Finally, trust sometimes fails not because the parties to an arrangement are necessarily untrustworthy, but because the environment is inimical to trust. Despite the capacity, competency and willingness of the actors to be trustworthy, there is a systemic failure that makes it unwise for anyone to trust (Werbach, 2018). An example would be how an unfair administration of the criminal justice system undermines trust, and therefore law-abidingness (Tyler, 2001).

2.2. A crisis of trust

The profound crisis cited in the Edelman Trust Barometer Report has its origins in the Great Recession of 2008, and is the culmination of events and patterns that have been developing for many years (Edelman, 2017). The systemic breakdown of trust comes down to an application of different rules for different folks. It is another type of inequality that is rising – that of the fundamental inequality of accountability (Hayes, 2013). Furthermore, Hayes states that we cannot have a just society that applies the principles of accountability to the powerless and the principle of forgiveness to the powerful. Yet, in the past decades, there have been blatant displays of this inequality. Just one of the many reasons why

institutional trust is eroding on a global scale is the release of the Panama Papers that revealed proof of tax evasion by billionaire business moguls and superstar athletes alike (Edelman, 2017).

2.3. The trust shift

A trust shift is happening. According to the Edelman Trust Barometer of 2016, a friend or an acquaintance on Facebook is viewed as twice more credible than a government leader. The mass population is relying less on newspapers and magazines and more on self-affirming online communities (Edelman, 2016). As institutional trust collapses, a space for new systems of trust emerges. Technology is enabling trust across huge networks of people, organizations and intelligent machines in ways that are unbundling traditional trust hierarchies. The stories of multi-billion-dollar companies such as Airbnb and Uber, whose success depends on trust between strangers, independent of one's credentials or affiliation with a trusted institution, is characteristic of this novelty. This is the rise of *distributed trust* (Botsman, 2017).

We are at the start of the third, biggest trust revolution in the history of humankind. A trust shift does not mean that the previous forms will completely be superseded, only that the new form will become more dominant. The first phase was local trust, where it was based on one-to-one interactions and personal reputation. Next came institutional trust – to cope with mass urbanization and international trade, institutions and institutional mechanisms were invented, from brands and the idea of middlemen to things like insurance and contracts. Distributed trust, on the other hand, takes the power away from a single source and shares the responsibility across a wide range of sources (Botsman, 2017).

While still in its beginnings, certain characteristics are already apparent. Trust that used to flow upwards to authorities and experts is now flowing horizontally, in some instances to our fellow human beings and, in other cases, to programs and bots. Distributed trust helps us understand why digital cryptocurrencies such as bitcoin could potentially be the future of money, and why the blockchain is being invested in for everything - from provenance tracking of food and blood diamonds, to independently copyrighting digital and intellectual assets, to selling our homes without the need for estate agents. The real disruption that is happening is not technology itself, but the massive trust shift it creates (Botsman, 2017).

3. The Trust Stack

To understand how we can even begin to trust blockchain technology, a breakdown of the process of building trust in a new technology is studied. A lot of the things we normally do in the digital space now were not always automatically trusted. For example, the use of peer-to-peer technology systems to transfer money instead of using a bank, post office or brands such as Western Union, is a method that is quickly getting traction. A *trust leap*, or that which occurs when we take a risk and do something new or in a fundamentally different way, is needed (Botsman, 2017). The era we live in requires us to take trust leaps at a surprisingly high rate – we have jumped from using credit cards to dabbling with cryptocurrencies; from making reservations at trusted hotel brands to booking rooms from complete strangers; from public transportation to using Uber or Blablacar; from libraries and encyclopedias, to open information-sharing hubs such as Stack Overflow and Wikipedia; and just recently, we've started to take a giant trust leap on self-driving cars and Artificial Intelligence.

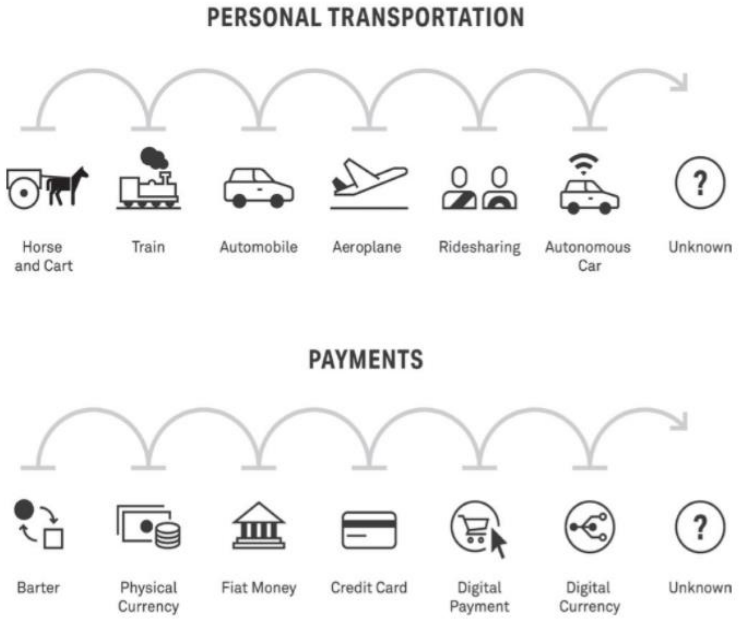


Figure 2. Trust Leaps (Botsman, 2017)

For a trust leap to occur towards new or disruptive technologies, certain conditions need to be fulfilled, just as deciding to trust another person calls for certain prerequisites. Amid the fascinating nuances in how trust works, there is an observed common behavioral pattern that people follow in forming trust in new technologies and businesses. This pattern is described in the Trust Stack model and comprises the following: trust in the *idea,* trust

in the *company or platform*, and trust in the *other person* (in other instances a machine or robot) (Botsman, 2017).

3.1. Trusting the idea

On the first level, we have to trust that the *idea* is safe and worth trying. There has to be enough understanding and certainty, or reduced uncertainty, to make us willing to try the idea. To fill the gap of uncertainty, we need to grasp what it can do and what it can give us. Until that chasm is crossed, we will not abandon what we already have (Moore, 2006).

Take the idea of self-driving cars for example. Initially, the idea of being driven by an invisible driver was met with much hesitation[1]. On the other hand, it was predicted that by 2040, autonomous vehicles will account up to 75% of vehicles on the road (Newcomb, 2012). Also, statistics dictate that human error and inconsistent driving cause more than 90% of crashes, ergo, driverless cars could reduce traffic fatalities by up to 90% (GRGB Law, 2016). Lastly, a typical American commuter spends on average more than fifty-two minutes per day in traffic, which adds to more than 4 billion hours of wasted time a year in the United States alone - time that could have been used in better ways (Thrun, 2017).

For first-time passengers of an autonomous car, the ride is met with awe and amazement, and sometimes even fear. However, Dr. Brian Lathrop, expert in cognitive psychology and human interface design, recounts in an interview that after an average of 20 minutes, a shift happens – the experience begins to feel normal, even boring. As it turns out, being driven by an intelligent machine is just not that exciting. This is because we are, in fact, very much used to being in the passenger seat with someone else driving (Lathrop, 2016). The trust leap, in this case, is not of taking on a new experience, but that of trusting a machine versus a human to drive. Once that happens, trust occurs almost too easily - to the point of being comfortable enough to nod off in an autonomous car. The point of global adoption of self-driving cars does not depend on engineering success, nor on the users'

[1] In a survey done by the American Automobile Association (AAA) on how much trust its members had in self-driving cars, three out of four participants said they would feel "afraid" to ride in them. Only one in five said they would trust a driverless vehicle to drive itself with them inside. The reasons people gave included: "trusting their own driving skills more than the technology" (84%); "feeling the technology is too new and unproven" (60%), and "not knowing enough about the technology" (50%) (Edmonds, 2016)

understanding of the technology. It depends on the principle of getting people to trust an idea[2] (Botsman, 2017).

3.2. Trusting the platform

The next stage is about knowing whether or not our trust is intelligently placed in the hands of an unfamiliar entity. Do I trust in the brand? Or in the case of digital platforms: do I have confidence in the platform itself, the app, payments, rating system, or in the algorithm? In the late 1800's, branding used to be the primary way of deciding on this stage of the trust stack. As cities expanded and goods became mass-produced, person-to-person trust was no longer viable (Botsman, 2017). Since then, a whole field of psychology for marketing has developed - one that taps into consumer's emotions as a way of gaining one's trust and influencing one's purchasing decisions (Gillette, 2015).

With the onset of social media in the 21st century, the person formerly known as a "passive consumer" suddenly participates as a social ambassador through photo posts and "likes". A shift in the companies' interest took place as they then prioritized delivering authentic experiences, as opposed to exaggerated or false claims, and focusing on customer support and interfacing in real time. Now, customers have become communities, and the communities have themselves become the platforms that shape the ups and downs of a brand (Botsman, 2017). In a recent survey by Nielsen (2015), it was revealed that the most credible advertising comes straight from the people we know and trust.

3.3. Trusting the other person

The third and final stage is the use of the different bits of information to decide whether the other person (or machine) is trustworthy or not. Personal encounters and social cues assist in evaluating these traits, but what happens on the digital platform, where all we have to go on is the pseudo-identity of a vendor? Today, we can make decisions on

[2] The experience of something familiar such as that of being a passenger in a friend's car is something that facilitates the trust leap, since it hinges on to the combination of something new with something familiar to make it "strangely familiar". This is a phenomenon called the "mere-exposure effect" or the Law of Familiarity (Goldstein, 2011). The law of familiarity states that things that form patterns that are familiar or meaningful are likely to be grouped together. To trust a new idea, bridges that are easy to find and to cross are needed. In this way, the unknown is reduced such that it lets our mind feel as if these mental processes are familiar (Botsman, 2017).

trust based on *collective experience* - the experiences other people have shared through reviews and social networks. The fact that everything is rated on both sides – from houses and drivers vs. occupants and passengers, on to products and services vs. buyers or clients, etc. – is our way of distinguishing the trustworthiness of both the vendor and the consumer (Botsman, 2017).

Technology, however, is creating trust between the unlikeliest of characters, even in the nefarious world of the "Darknet" - an encrypted network of secret websites that allows the exchange of illegal assets such as drugs, stolen financial data, and firearms (Reiff, 2020). The great oxymoron is that it is populated by hundreds of thousands of vendors who would commonly be stereotyped as untrustworthy, yet here they are creating highly efficient markets[3] (Botsman, 2017). As it turns out, user ratings create a social pressure or economic incentive that can make even drug dealers care about their online brand and customer satisfaction.

Reputation is trust's closest sibling, and is an essential asset, yet it is not the only thing that fuels trust. Benevolence comes down to empathy and goodwill, but where does that fit in with regards to the Darknet? Political scientist Russel Hardin (2002) argues that trust is really about *encapsulated interest,* i.e., a kind of closed loop of each party's self-interests. Like the real estate agent who sells a house at a reasonable price not because she cares about the client but because her commission is directly tied to the sale price, the drug dealer also earns more by being honest rather than by colluding.

Sections 1, 2 and 3 cite various ways by which trust is defined, broken and built, but it should be acknowledged that there is a vast area of studies elsewhere, in the socio-philosophical field and in the field of economics and game theory, that expounds on the definition and the processes within trust.

[3] Despite the absence of legal regulations governing the exchanges, drugs on the Darknet tend to be of higher purity than those available on the streets (Mounteney et al., 2016).

4. Trust Architectures

To understand further the predisposition of people to trust in different ways, the main institutional structures for manifesting trust are presented. Additionally, this distinction collocates the emergence of blockchain on the trust map, i.e., where blockchain fits into this whole story of trust. Just as the physical architecture of neighborhoods determines the character of communities, or the digital architecture of communications networks shapes opportunities for innovation, creativity, and free expression online, the architectures of trust embody the multiple ways trust is formed. The following are the three main architectures are **Peer-to-peer, Leviathan** and **Intermediary** (Werbach, 2018)**.**

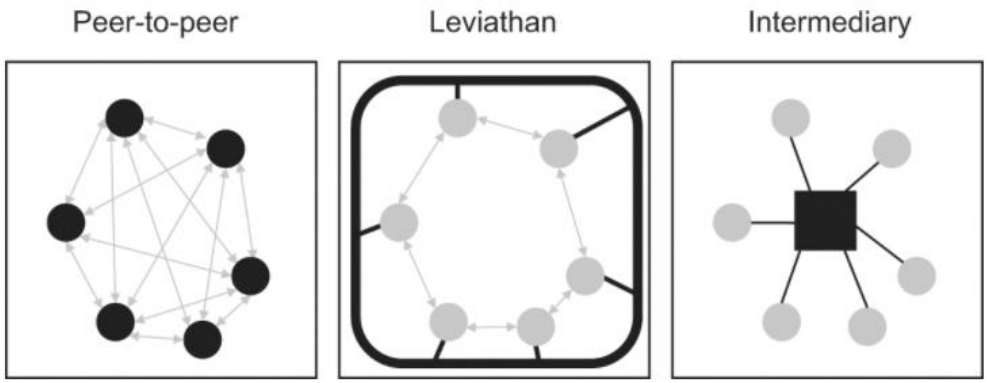


Figure 3. Symbolic representations of the three established trust architectures. The black elements of each are the trusted components (Werbach, 2018).

4.1. Peer-to-peer trust

P2P trust is based on relationships and shared ethical norms, and is the earliest human trust structure to develop, often manifesting in the interpersonal trust among families and clans. This trust falls under "local" trust, or trust that rests in someone specific, particularly in one we are familiar with. P2P trust architectures are prevalent even to this day, and exhibit three main characteristics: they are in communities with shared social norms; they have effective governance mechanisms among themselves; and there is an adherence to a set of principles for self-governance, coupled with the flexibility of individuals and communities to adjust in order to solve problems (Ostrom, 1990).

Since it rests on mutual commitments and personal relationships, it can be considered as a "thick" kind of trust, rather than a "thin" trust that relies on momentary convenience (Putnam, 2000). Traditional P2P trust, however, has a relatively small radius.

Trust in a member of the same community might not go beyond unimportant transactions where the stakes are relatively low. For this, the design requires clear group boundaries and the opportunity for those affected by the rules to participate in modifying them (Werbach, 2018).

In this digital age, a new kind of P2P trust has emerged. The same structure can be seen in systems such as Wikipedia, open-source software communities, and user-moderated content sites such as Reddit. These models expand the scope of peer-to-peer trust into a form of distributed trust, while maintaining its dependence on a combination of formal rules and communal standards that are rarely present in complex impersonal marketplaces (Frischmann, 2013).

4.2. Leviathan

Based on the vision of seventeenth-century philosopher Thomas Hobbes, the Leviathan architecture grants a governing body monopoly on the legitimate use of violence. Trust is nevertheless, according to Hobbes, the foundational force in the establishment (Hobbes, 1651). With Leviathan trust, a powerful central authority not afflicted with greed or tendencies toward self-interest operates largely in the background to prevent others from imposing their will through force or trickery. Leviathan trust is therefore a strong form of institutional trust. Knowing that there are penalties for breach, the individuals and organizations that take part in the architecture feel comfortable taking the risks inherent in trusting relationships (Werbach, 2018).

Leviathan trust relies highly on bureaucratic rules for participation, as well as dispute resolution. It is essentially through law enforcement or military activities that the central authority maintains a baseline level of trust in social stability. The legal system, with its thicket of doctrine, defines constraints on arbitrary state power. Therefore, when the legal system fails, so does trust (Tyler, 2001).

4.3. Intermediary

In an Intermediary architecture, a third party intervenes to provide valuable services that induce individuals to hand over power or control, and hence falls under institutional trust as well. The local rules and the reputation of the intermediaries take the place of social norms and government-issued laws to structure transactions (North, 1990).

Like commercial banks that facilitate the transaction flow between depositors and borrowers, activity is possible through the intermediaries' ability to aggregate activity on both sides. Financial services relationships are a good example of intermediary trust – commercial banks mediate the transaction flow between depositors and borrowers, generating and paying interest along the way (Werbach, 2018).

Intermediary trust is particularly significant online (Hurwitz, 2013). Advertisers trust platforms such as Google because of its transparency in its pricing and performance metrics for their ads. On the other hand, users trust it because it returns high-quality search results surrounded by ads that are tailored and therefore relevant to the user. While Amazon and eBay are among the top trusted intermediaries for online transactions, in general, the reputational system used for even the smallest online shop can be effective in inciting trust among buyers. Although these platforms are often described as peer-to-peer, they are more appropriately considered to be intermediary, because users are actually trusting the platform, not the personal relationships or community-defined rules of governance (Werbach, 2018).

5. "Trustless" Trust Architecture

In retrospect, all three architectures defined above involve a trust trade-off wherein users give up some freedom to gain the benefits of trust. In P2P, the participants must conform to the norms of the community in order to partake in it, and in turn be trusted by other members of the community. Leviathan trust reduces the member to subservience to the state, with the knowledge that other members who are potential perpetrators are equally subservient as well. In the case of intermediary trust, members cede control over personal data, trusting the third party not to exploit its power despite the asymmetry of information (Werbach, 2018).

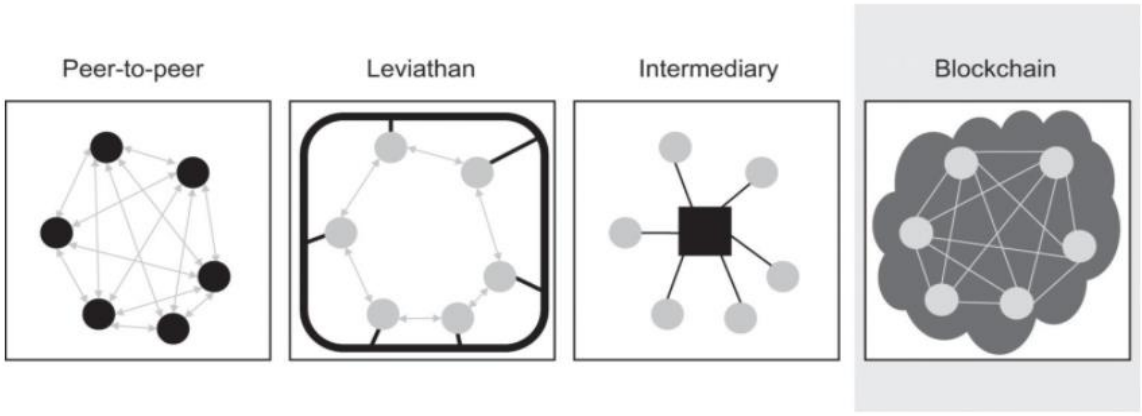


Figure 4. The blockchain's "Trustless" Trust Architecture
Promoting trust in the network without trusting any individual actor, compared to alternatives (Werbach, 2018).

The blockchain creates a new kind of architecture that none of the established models encompass. On a blockchain network, nothing is assumed to be trustworthy except the output of the network itself (Werbach, 2018). On any transaction, there are three elements that may be trusted: the counterparty, the intermediary, and the dispute resolution mechanism (Botsman, 2017). Simply put, blockchain tries to replace all three elements with software code. People are represented through arbitrary digital keys, thus eliminating contextual factors that humans use to evaluate trustworthiness. The intermediary is replaced with a transaction platform that is distributed and machine-operated. Finally, the dispute resolution occurs through "smart contracts" that execute predefined algorithms (Werbach, 2018).

In doing so, blockchain trust severs the connection between institutional actors and the system. Compared to its alternatives, the blockchain's "trustless" architecture promotes trust in the network without trusting any individual actor (Fairfield, 2005). The consensus of distributed collection of independent computers confirms the true state of the ledger – this is the trust architecture of the blockchain and distributed ledger technology (Werbach, 2018).

Chapter 2

BLOCKCHAIN

The three traditional architectures mentioned above thrive in existence because they have fundamentally evolved based on people's understanding of trust while shaping how users see the world in turn (Werbach, 2018). If this is true, we should then ask: what kind of reality does a trustless architecture shape for us? Furthermore, in order for us to make a trust leap, we move onto the first level of the trust stack: trusting the idea. What is blockchain, how does it function, and what can it give us?

1. Defining a blockchain

Blockchain and other distributed ledger technologies (DLTs) are technologies enabling parties with no particular trust in each other to exchange any type of digital data on a peer-to-peer basis with fewer or no third parties or intermediaries. Data could represent, for instance, money, insurance policies, contracts, land titles, medical records, birth and marriage certificates, buying and selling goods and services, or any other type of transaction or asset that can be translated into a digital form (Coding Tech, 2018).

Originally proposed in a white paper entitled *Bitcoin: A Peer-to-Peer Electronic Cash System* in 2008 by Satoshi Nakamoto, a pseudonymous person or group of persons, the basic blockchain concept can be defined quite simply as a shared, decentralized, cryptographically secured, and immutable digital ledger (De Ponteves, 2020). Another quick definition: it is a continuously growing list of records called *blocks* which are linked

and secured using cryptography to form a *chain*, hence the name blockchain (Narayanan et al., 2016).

1.1. Immutability

A *block* contains batches of valid transactions that are *hashed* and encoded into a *Merkle Tree*. In very simple terms, a Merkle Tree is a way of structuring data that allows a large body of information to be verified for accuracy both extremely efficiently and quickly[4]. The Merkle Tree is crucial to a blockchain's security, since it makes it possible to use as little data as possible when processing and verifying transactions. The block is then time-stamped, and is secured by a hashing process. It links together and incorporates the hash of the previous block (Srivastav, 2019).

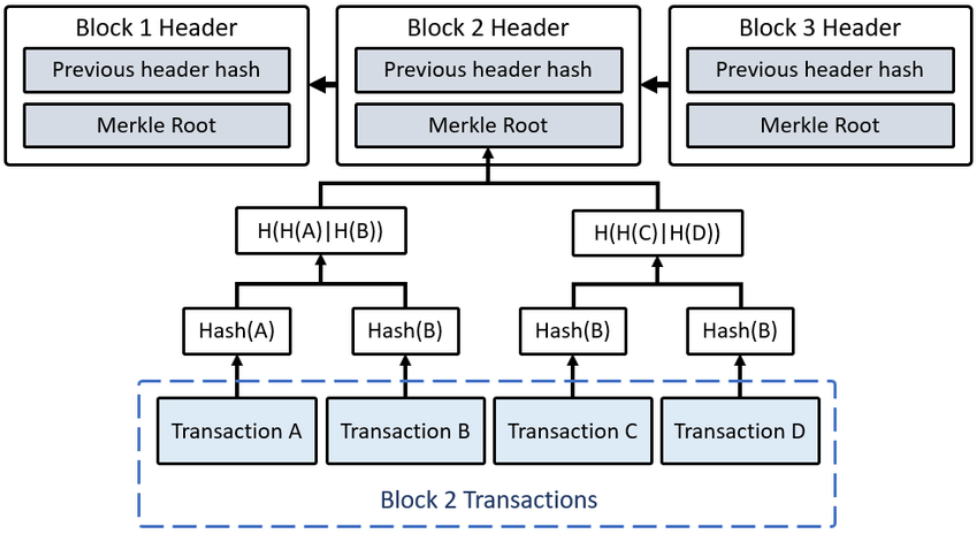


Figure 5. The architecture of Merkle tree in the blockchain (Chen et al., 2019).

A hash, on the other hand, can be defined as a digital fingerprint to serve as an identifier for anything digital - in this case, a block. Some of the most common hashing functions are MD5, SHA-3 and SHA-256. Developed by the National Security Agency (NSA), SHA-256 consists of 256 bits; 64 characters in hexadecimal. SHA-256 generates

[4] A single block can contain up to several thousand transactions, therefore it becomes clear that memory space and computing power could become two big problems. To solve this, the Merkle Tree algorithm performs a loop, grouping all of the data inputs into pairs again and again, each time cutting the number of codes in half, until it results in one 64-character code – the Merkle Root. The Merkle Root is vital because it authorizes any computer to quickly verify that a specific transaction took place on a certain block as accurately as possible (SelfKey, 2019).

an almost-unique signature for a text. For a hash algorithm to be secure, it needs to conform to these 5 requirements [5] (Tel, 2008):

One-way: The content of the item should not be identifiable by that hash

Deterministic: The same item should always generate the same hash

Fast computation

Avalanche Effect: The hash should change with the most minimal alteration of the content or of other determining entries.

Must withstand collisions: That hash combination should be so unlikely and so rare that it shouldn't be probable for the algorithm to generate collisions. It must also withstand artificial conditions such as hashes generated by hackers.

The previous block's hash links the blocks together and prevents any block from being altered, or being inserted between two existing blocks. Since it includes the meta-data of the previous block, a link is established between the block and the chain, rendering it unbreakable (Srivastav, 2019). In this way, each subsequent block strengthens the verification of the previous block and hence the entire blockchain. This iterative process confirms the integrity of the previous block, all the way back to the initial block known as the *genesis block*. Since the blocks are linked in a proper, linear and chronological order, it follows that if one is tampered with, all the subsequent blocks would also be altered (Coding Tech, 2018). This method renders the blockchain tamper-evident, lending to the key attribute of immutability (de Ponteves et al., 2020).

Immutability means that no participant can tamper with a transaction after it has been recorded to the ledger. If a transaction is an error, a new transaction must be used to reverse the error, and both transactions will then be visible. Changing anything prior to the

[5] For example, the hash generated for the sentence «Hello, my name is jena.» would look like this:
6f345edb9b2e0ebde75cefd3ae5d9b07a393bdd8d1b14a87a01a31cf00a6824e.
For «Hello, my name is Jena.», it would generate the following hash:
413f42335898a42e99b005784447182389efc0c910423959ad7bdee06843078f
Notice that only by merely changing the case of the letter "J" drastically changes the entire hash - this is the avalanche effect. Furthermore, each phrase will always generate the same combination of characters, which accounts for its deterministic effect. It is one-way because from the generated hash, it is impossible to reproduce the original phrase. And finally, each hash was computed in an average 0.170 milliseconds, which is extremely fast.

current block means forking the entire chain back to that point. Because every block is linked in a specific sequence, such an action will be rejected without a majority of consensus (de Ponteves et al., 2020). The characteristics of non-repudiation and non-forgeability guarantee that there is a unique and historical version of the records which can be agreed and shared among all participants in a particular network[6] (Nascimento et al., 2019).

1.2. Distributed Ledger

To be clear on the terminology, blockchain is part of the broader family of Distributed Ledger Technology (DLT). DLTs are particular types of databases in which data is recorded, shared and synchronized across a distributed network of computers or participants (Nascimento, 2019). A distributed ledger can be described as a ledger of any transaction or contract supported by a decentralized network from across different locations and people, eliminating the need for a central authority. Although a ledger consists simply of data structured by rules, it matters profoundly to all sorts of transactions because it provides a consensus about facts. Ledgers record the facts underpinning the modern economy. The traditional implementation of a ledger, however, relies entirely on trust in the centralized institutions. Even in the shift from analog to digital ledgers or databases, a database still remains centralized and relies on trust, ergo a digitized ledger is only as reliable as the organization that maintains it. The blockchain is a distributed ledger that does not rely on a trusted central authority to maintain and validate the ledger[7] (Cryptoeconomics, 2017).

"Decentralization" is one of the words that is used in the cryptoeconomics space most frequently, but it is also one of the words that is perhaps defined most poorly. "Distributed" means not all the processing of the transactions is done in the same place, whereas "decentralized" means that not one single entity has control over all the

[6] A hacker should therefore manipulate the target block, and then compute the valid hashes of all the subsequent blocks in the chain within a few minutes for it to be considered as a successful hack on one node.

[7] While the blockchain contains transaction data, it is not a replacement for databases, messaging technology, transaction processing or business process. Instead, the blockchain contains verified proof of transactions. Although blockchain essentially serves as a database for recording transactions, its benefits extend far beyond those of a traditional database. Most notably, it removes the possibility of tampering by a malicious actor (Laurence, 2019).

processing. In this sense, blockchain is both decentralized, and also distributed (Buterin, 2017).

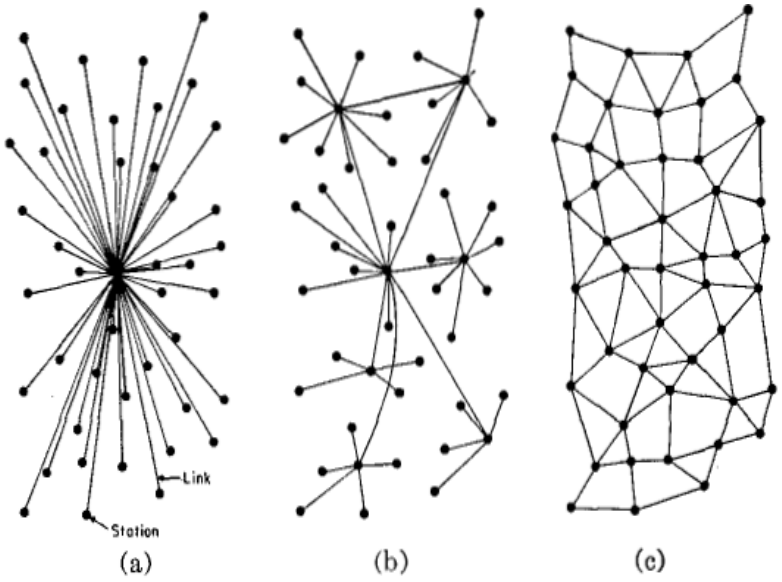


Figure 6. (a) Centralized. (b) Decentralized. (c) Distributed networks (Buterin, 2017).

Why is decentralization useful in the first place? There are generally several arguments raised. Decentralized systems are less likely to fail accidentally because they rely on many separate components, and are therefore fault-tolerant. They are more expensive to attack and destroy or manipulate because they lack sensitive central points that can be attacked at much lower cost than the economic size of the surrounding system. Finally, it is much harder for participants in decentralized systems to collude to act in ways that benefit them at the expense of other participants, whereas the leaderships of corporations and governments collude in ways that benefit themselves but to the disadvantage of less well-coordinated citizens, customers, employees and the general public all the time (Buterin, 2017). There are many different types of blockchains with distinct functionalities and architectures. They can be distinguished according to three functions: *who can read, who can execute,* and *who can validate transactions* (Nascimento et al., 2019).

Public or open: When anyone can access a whole blockchain and read its contents.

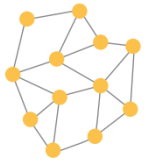
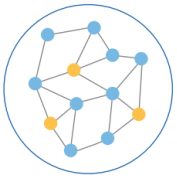
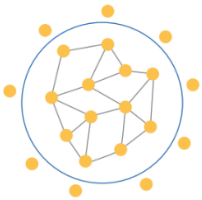
Close or private: When only authorized entities have access.

Permissionless: If anyone can send and validate transactions.

Permissioned: If entities need to be authorized to execute or validate transactions, or both.

As needed, hybrid blockchains combining different aspects along a continuum can be utilized. In general, four major blockchain types can be distinguished: public permissionless, public permissioned, private permissioned and private permissionless blockchains, as shown in Table 1.

Table 1. Examples of blockchain types[8] (Nascimento et al., 2019)

Blockchain type	Explanation	Example	Visualization
Public permissionless blockchains	In these blockchain systems, everyone can participate in the blockchain's consensus mechanism. Also, everyone worldwide with an Internet connection can transact and see the full transaction log	Bitcoin, Litecoin, Ethereum	
Public permissioned blockchains	These blockchain systems allow everyone with an Internet connection to transact and see the blockchain's transaction log although only a restricted number of nodes can participate in the consensus mechanism	Ripple, private versions of Ethereum	
Private permissioned blockchains	These blockchain systems restrict both the ability to transact and view the transaction log to only the participating nodes in the system, and the architect or owner of the blockchain system is able to determine who can participate in the blockchain system and which nodes can participate in the consensus mechanism.	Rubix, Hyperledger	
Private permissionless blockchains	These blockchain systems are restricted in who can transact and see the transaction log, although the consensus mechanism is open to anyone.	(Partially) Exonum	

[8] In Table 1, the yellow dots represent the validating nodes, which means they are able to validate the transactions in the system and participate in the consensus mechanism. The light-blue dots are participants in the network, in the sense that they can transact, but are not able to participate in the validation mechanism. The light-blue dots do not participate in the consensus mechanism. A blue circle means that only nodes within the circle can see the transaction history. Illustrations without a circle mean that everyone with an Internet connection can see the blockchain's transaction history (Nascimento et al., 2019).

1.3. Consensus

In a distributed peer-to-peer network, the blockchain is copied across all computers in the network, and all subsequent changes are broadcast across the network to be constantly checked to match up with the other nodes. A blockchain protocol is set, defining the rules that dictate how the computers or *nodes* in the network should verify new transactions and add them to the blockchain. The protocol employs cryptography, game theory, and economics to create incentives for the nodes to work toward securing the network instead of attacking it for personal gain. If set up correctly, this system can make it extremely difficult and expensive to add false transactions but relatively easy to verify valid ones (Orcutt, 2019).

In a blockchain, everyone can have his or her own copy of a ledger and trust that all those copies remain the same, even without a central administrator or master version (Werbach, 2018). Trust between participants is based on the set of rules that everyone follows to verify, validate and add transactions to the blockchain – the *consensus mechanism*. We can define a consensus algorithm as the mechanism through which a blockchain network reaches consensus. It ensures that all agents in the system can agree on a single source of truth, even if some agents fail. In other words, a consensus algorithm renders a system *fault-tolerant* [9] (Arun et al., 2019). The most common implementations of blockchain consensus algorithms are Proof-of-Work (PoW) and Proof-of-Stake (PoS) (Binance Academy, 2020). Satoshi Nakamoto (2008), the creator of Bitcoin, proposed the Proof-of-Work system to coordinate its participants.

1.3.1. Proof-of-Work

In a Proof-of-Work (PoW) system[10], the validators (referred to as *miners*) have to verify the transactions grouped in a memory pool called *mempool*. This transaction

[9] In the unlikely event that a hacker succeeds in manipulating a blockchain on a single node, the system uses a consensus algorithm to distinguish which is the true blockchain on the network, and then re-copies and restores the blockchain on the compromised node. The attacker, therefore, would have to gain control of more than half of the network's computing power and use it to rewrite the transaction history – an impressive feat for larger blockchain networks consisting of thousands of nodes (de Ponteves et al., 2020). This is called a 51% attack, which will be discussed later on.

[10] Although first implemented in Bitcoin, the actual concept of Proof-of-Work was invented by Cynthia Dwork and Moni Naor in 1993 as a way to deter denial-of-service attacks and other service abuses

verification process is called *mining*. To include the transaction in the next block, the miner needs to know the cryptographic hash value of the last recorded block, which is hidden from everyone. This hash value must be reference for creating a new block (edChain, 2018). The protocol then sets out conditions for what makes the hash of the new block valid in a cryptographic puzzle that requires immense computing power to solve[11]. After finding a hash that fits the conditions of the puzzle, the miner announces it to the network for the other nodes to verify, and proceeds to add the new block to the chain (edChain, 2018).

The stake, or that which the validator must put forward in order to discourage them from acting dishonestly, is the cost of these machines and the electricity required to run them. In major blockchains, to compete with other miners, high levels of computing power and special hashing hardware is necessary to be in with a chance of producing a valid block. The incentive for using up so much of one's resources usually consists of the protocol's native cryptocurrency. Mining yields a significant reward if you successfully add a new block to the blockchain (Werbach, 2018).

Through PoW, Satoshi Nakamoto solved the problem of decentralized time-stamping and double spending. To trust that a coin was not spent twice, there must be a reliable way to track exactly when each transaction happened. On a decentralized network, there is no master clock to which every machine can synchronize. The PoW system therefore imposes consensus on the precise order of transactions. Nodes are agreeing not just on what happened, but in what sequence it happened. The same consensus algorithms that allow each node to have an identical copy of the ledger allow it to perform identical computations, in the same order. That provides what computer scientists call "shared state", i.e., a picture of the status of the system at any moment (Werbach, 2018).

---

such as spam on a network by requiring some work from a service requester, usually meaning processing time by a computer (Cook, 2018).

[11] An example of a condition would be: only a block whose hash begins with 0000 will be valid. The only way for the miner to create a hash combination that matches the requirements is to brute-force inputs or tweak parameters to produce a different outcome for every guess until they get the right hash (de Ponteves et al., 2020).

Each cryptocurrency functions differently according to the design of its creators[12]. Generally, the value of digital money is based on the volume and velocity the digital currency's payments are running through the ledger, and on the speculative future use of the digital currency.

1.3.2. Proof-of-Stake

In a Proof-of-Stake (PoS) system, there is no concept of miners, specialized hardware, or massive energy consumption. Instead of putting forward an external resource such as electricity or hardware as the stake, the stake is an internal resource – cryptocurrency, a.k.a. *crypto tokens*. All cryptocurrencies in this network are already created, which means that their number doesn't change, and that there is no mining required. This eliminates the need to solve a complex cryptographic puzzle, along with the need for a continuous upgrade of hardware and soaring energy costs (Werbach, 2018). Tokens are then acquired by investing in the company running the cryptocurrency in exchange for their native cryptocurrency in a fundraiser called Initial Coin Offering (ICO). ICO is the cryptocurrency industry's equivalent to an initial public offering (IPO), which is a way by which a company looking to create a new coin, app, or service could raise capital (Frankenfield, 2020).

Rules differ with every protocol, but there is generally a minimum amount of funds to be eligible for staking – they must own and maintain a certain number of native tokens in a specified location to qualify as a validator (Werbach, 2018). The larger the amount of stake and the longer the duration of the stake, the better are the chances of the *staker* to get transaction validation responsibility. Once tokens have been staked, a selection algorithm chooses one validator to propose a new block for validation. The selection process could have multiple variations, either according to the staking size, the staking age, or through

[12] Specific to Bitcoin, a finite ceiling of 21 million bitcoins was set such that the supply of the digital currency would be limited and finite. On average, these bitcoins are introduced to the bitcoin supply at a fixed rate of one block every ten minutes (Hayes, 2020). The amount of bitcoin released in each of these aforementioned blocks is then reduced by 50% every four years to slow down the coin circulation (Botsman, 2017). Furthermore, the system is set to adjust the difficulty of the mathematical problems depending on how fast they are being solved, the goal being to further slow down the miners and slow the release of bitcoins. Over time, the miners find the cryptographic puzzle easier, and the block generation time reduces from 10 minutes. Hence, the puzzle is revised every 14 days to make it more complex. Effectively, this means that more computing power will be needed henceforth (edChain, 2018).

randomization. Selecting a validator is one of the most crucial aspects of a PoS algorithm, and is thus essential to align the selection process with the network's incentives. As a result, different blockchains employ different methods, which may correspond to the mentioned techniques, or represent a combination of several techniques suitable for the desired purpose (The Bridge, 2020).

Once the validator has been selected, the consensus mechanism adds the new block, which is either according to a pre-defined frequency (Chain-based proof-of-stake), or through a process where other validators vote on the validity of the proposed block (Byzantine-fault-tolerant proof-of-stake). A digital wallet is used to lock up the validator's funds, and if his block is verified as a valid block by the majority, a proportion of the transaction fees will be received as reward. The more funds the miner has, the more there is to gain. However, in an attempt to cheat by proposing invalid transactions, a portion, or possibly all of the stake could be confiscated or "slashed" for misbehavior. Therefore, similar to PoW, acting honestly is more profitable than acting dishonestly (Binance Academy, 2020).

Proof-of-Work and Proof-of-Stake are the most discussed consensus algorithms, but there are a wide variety of others, each with their own advantages and disadvantages. Other notable consensus mechanisms could be the use of multi-signatures wherein a majority of validators must agree that a transaction is valid, or through the Practical Byzantine Fault Tolerance (PBFT), an algorithm designed to settle disputes among computing nodes when one node in a set of nodes generates different output from the others in the set (Arun et al., 2019).

1.4. Tokenization

It is also important to mention that not all blockchains have a cryptocurrency. Blockchains such as R3's Corda and IBM's Fabric are examples of blockchains that do not use tokens, but instead utilizes the main features of blockchain to ensure transaction validity and uniqueness (Sandner, 2017). Furthermore, token types may vary significantly depending on the type of blockchain or distributed ledger. A token, in its simplest terms, is a unit of value – a specific amount of digital resources which a participant can control and reassign control of to someone else. Quite different from its incentive use in Bitcoin, a token can also function as a claim to an asset that is fungible and tradable, such as cash, bonds, securities, stocks, and even cars and houses. The provenance of that asset can be

easily tracked on a blockchain by assigning a "token" to it. Tokens can hence serve as proof of the ownership history of the asset, and the ability to divide assets into smaller fractions of ownership enables greater liquidity for that asset (Perez, 2017).

To outline the process of the blockchain, we refer to Figure 7. As transactions are made, they are broadcast to the network to be validated by its nodes or peers. Once there is a consensus on the legitimacy of the contents, the group of transactions is converted to a Merkle Root, and clustered into a block to be hashed and time-stamped along with the hash of the previous block, and then added to the blockchain. The new block is then distributed to all nodes, thus concluding a transaction cycle.

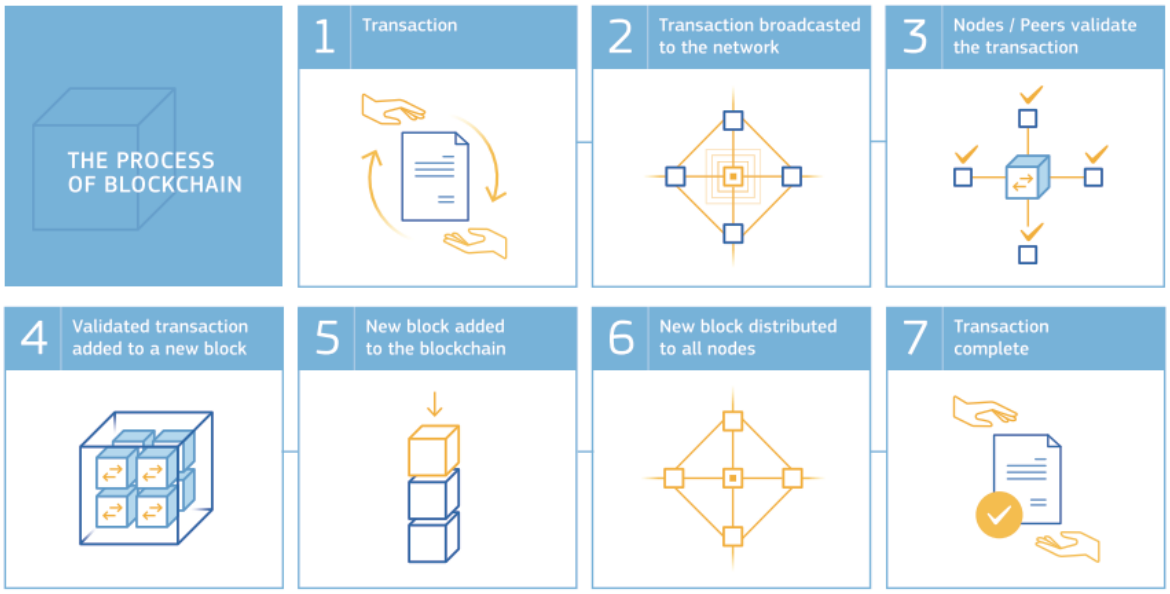


Figure 7. How a blockchain works (Nascimento et al., 2019)

1.5. Smart Contracts

In a traditional information system, contracts are managed by centralized authorities such as insurance companies, agencies and banks. The task of maintaining and enforcing agreements depends heavily on third party organizations, and is often a cause for delay and inefficiency, and effectively creates bottlenecks. The term "smart contract" was first coined by Nick Szabo (1994), where he defined it as a computerized transaction protocol that executes the terms of a contract. In its recent implementation in the release of the Ethereum Project, smart contracts, or "decentralized applications" (Dapps) turned into a notable term in cryptoeconomics as it allowed individuals to create their own contractual agreements that can automatically be executed by the computer code, removing

the possibility of downtime, censorship, fraud or third-party interference[13] (McGrath, 2018).

A smart contract, in essence, is a binding agreement between two parties to do or not do something. It is a program that runs within a blockchain that contains a set of rules that constitute an agreement made between two or more parties. When these rules are met, the digital contract executes the transaction. It is similar to a regular application that implements some business rules, only it uses a blockchain as a database (Bekemysheva, 2018). A smart contract can therefore be used to store a business's terms of agreement (Werbach, 2018). Anyone can examine the source code to understand what exactly the program does, and can know that this code cannot be modified by hackers or viruses because smart contracts rely on blockchain cryptography (Bekemysheva, 2018). Blockchain makes extensive use of Public Key Cryptography (PKC), with the goal of trivially transitioning from one state to another while making reversing the process nearly impossible[14].

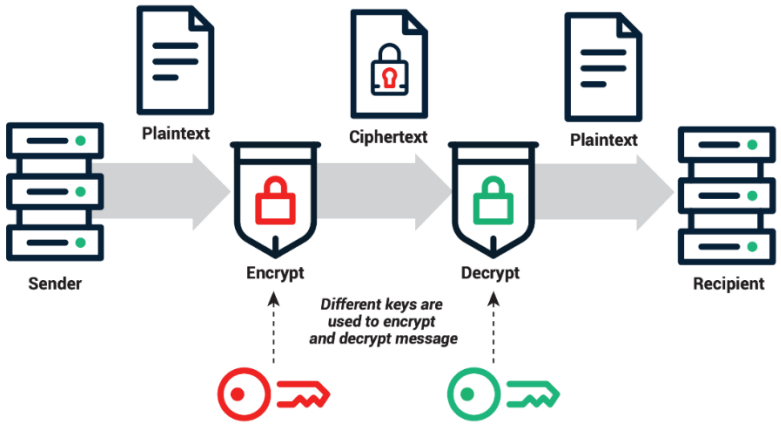


Figure 8. How blockchain cryptography works (Sectigo, 2020)

[13] Ethereum does this by building what is essentially the ultimate abstract foundational layer: a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions (Buterin, 2013).

[14] The product of PKC is subsequently a one-way mathematical function (Ledger Academy, 2019). PKC uses a pair of a public key and a private key to perform transactions. Public keys are widely distributed, while private keys are kept secret. The analogy is very much like the public key as a username and the private key as the password. Using a person's public key, it is possible to encrypt a message or the contents of a transaction so that only the person with the private key can decrypt and read it. Using a private key, a digital signature can be created so that anyone with the corresponding public key can verify that the content was created by the owner of the private key and was not modified since (Massessi, 2018).

The first smart contract was built on the Ethereum platform in 2014, and although it experienced some issues of security, scalability and the slow transaction speed, many platforms have since then evolved from its original design. Well into its third generation, smart contract development is now focusing on solving the main critical problems faced by the previous generations such as scalability, interoperability, governance and sustainability (Henten and Windekilde, 2020).

Smart contracts are self-verifying due to its automated nature, are self-enforcing when the rules are met at all stages, and are tamper-proof. Because the contract does not subsist on a central server but on a network of nodes, the execution and output of a contract is validated by each participant to the system, and the distributed ledger guarantees the correct execution of the contract (Destefanis et al., 2018). This enables autonomy between members, not having to be in further contact after a transaction. Being implemented on a blockchain renders the smart contracts immutable, thus assuring that all participants automatically have their fair share (Werbach, 2018).

Blockchain and smart contracts reduce time and cost associated with management and rule enforcement. In place of the time spent, there is instead a much greater amount of exchange that can take place and thus enables a true services economy. It reduces corruption, due to its incorruptible nature, and reduces dependence on centralized organizations. It can deliver certainty, since all possible outcomes are predetermined, and in turn enable parties to know exactly what will happen[15] (Coding Tech, 2018).

[15] Nick Szabo (1994) suggested that the main objectives of smart contract design are «to satisfy common contractual conditions (such as payment terms, licenses, confidentiality, and enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs».

2. The Blockchain Trilemma: Decentralized, Scalable and Secure

Before diving into the dynamics of the Trilemma, we broadly define what scalability, security, decentralization mean:

Decentralization: refers to the degree of diversification in ownership, influence and value in the blockchain

Scalability: is the ability of the blockchain to accommodate a higher volume of transactions

Security: is the ability to protect the data held on the blockchain from different attacks or blockchain's defense against double-spending

Without these three qualities, blockchain projects that aim at a global adoption, will not work. The interplay among the three elements, however, make it a challenge to achieve (ricc, 2020). The trade-off of pure decentralization, for example, is speed. Given similar security parameters, we see that scalability is inversely proportional to decentralization. On the other hand, at constant decentralization, scalability and security are proportional (The Bridge, 2020). The Blockchain Trilemma, its name originally coined by Ethereum founder Vitalik Buterin, states that you will always achieve one of the three main attributes at the expense of others, and that it is impossible to maximize all three properties at the same time. The perfect blockchain, therefore, would be capable of maximizing all three factors, resolving the Trilemma (Prasanna, 2019).

2.1. Decentralization

As mentioned, this is a concept regarding the *degree* of decentralization, meaning that it is not a binary attribute. Ethereum, for example, is very decentralized, Eos is partially decentralized; while Twitter is not at all decentralized. Decentralization is desirable because it increases the robustness of the system. It makes the network resistant to censorship and thus allows anyone to use the network uplifting the property rights. However, it does come at a cost. If a transaction requires multiple confirmations before reaching consensus, then inherently, it would take longer than if a transaction can be confirmed by a single entity (The Bridge, 2020). Therefore, certain protocols like Bitcoin or Ethereum that use PoW mining to produce new blocks require vast amounts of energy, but also compromises on performance on speed. This can be problematic for use-cases that

require high throughput. On the other hand, there are more gridlocks in blockchains with many nodes, so nodes with fewer resources or poor Internet connection paralyzes the network additionally (NeonVest et al., 2018).

2.2. Security

Security is the ability of a blockchain to maintain irrevocability of transactions. It does so by forcing network participants to expend resources to earn rewards. The more resources network participants spend, the more secure the blockchain. It also refers to the level of defensibility a blockchain has against attacks from external resources. Internally, or within the blockchain itself, it is a measure of how resistant the system is to change. Decentralization and security go hand in hand. In many cases, the more nodes there are, the less reliant the network is on a centralized party, and therefore the less risk of having a central point of failure (NeonVest, 2018).

The primary benefit of robust security is that the blockchain is less vulnerable to attack. This is ideal for applications that require sovereign grade security with confidential data, such as financial services. A security-focused blockchain also enables transfers which are quicker and cheaper than traditional value transfers. Since the security of public blockchains comes from network participants, higher security implies higher network effects which are not easy to replicate. Scalability and security are proportional because if the hash rate is higher, the confirmation time is lower, thus increasing scalability (The Bridge, 2020).

2.3. Scalability

Scalability is important for mass adoption. It is the question of how much a blockchain system can sustain (users, use cases, transactions), and whether the system can operate smoothly as demand increases (CertiK, 2019). It essentially boils down to reducing the settlement time to increase the number of transactions per second (TPS) or the throughput of the system. The blockchain's scalability increases in two ways: the reduction of the number of entities vetting the transactions, which is a compromise on decentralization; or the reduction of block time, which demands reducing difficulty of the network, compromising instead the security of the system. Scalability-focused networks are advantageous in the sense that it allows the network to support a high volume of

transaction, and is particularly useful in applications where security is not a prime focus, such is the case in a social messaging application (The Bridge, 2020).

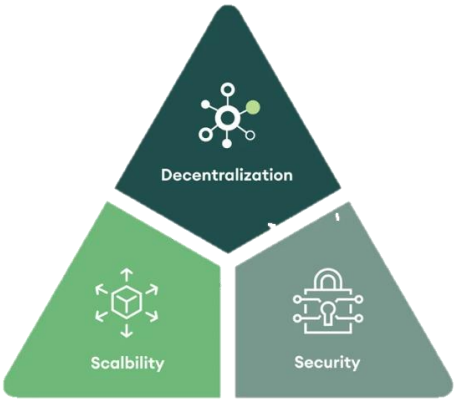


Figure 9. The blockchain trilemma (The Bridge, 2020).

Although there is no actual law stating that the three aspects should be satisfied, development teams are working on different approaches in attempts to solve the Trilemma. It is important to note as well that the Trilemma is simply a model to conceptualize the various challenges facing blockchain technology. As depicted in Figure 8, the Trilemma could be conceptualized as a pyramid[16]. Regardless of the different implementations, it is agreed that it is difficult for any blockchain to effectively achieve decentralization, scalability, and security (CertiK, 2019). The Blockchain Trilemma is most likely unsolvable (Prasanna, 2019), but it does open up an endless number of possibilities as to the approaches in finding the right balance, each tailor-made to the objective that one hopes to achieve.

[16] The CertiK Foundation, for example, considers security as the base layer that is fundamental in upholding all others. In their approach, security creates the groundwork for both decentralization and scalability to flourish, while decentralization is a process that takes time, and scalability is an aspect that should always be improving (CertiK, 2019).

3. Blockchain Ecosystems Landscape

Blockchain start-ups started to emerge in 2009, though the attention of worldwide investors shifted to blockchain companies only a few years later. Blockchain has gone beyond just financial applications and has gained traction in many other sectors. A new set of players, from industry to academia, governments and supranational organizations, began reflecting on how blockchain could transform significant parts of industry, the economy, and society in the future (Davidson et al., 2016, UK Government Chief Scientific Adviser, 2016). As of 2018, the largest number of blockchain firms was established in the USA, followed by China. Within the EU, the United Kingdom hosts almost half of the blockchain start-ups, followed by Germany, France and Estonia.

Currently, the sectors using blockchain in Europe are the following:

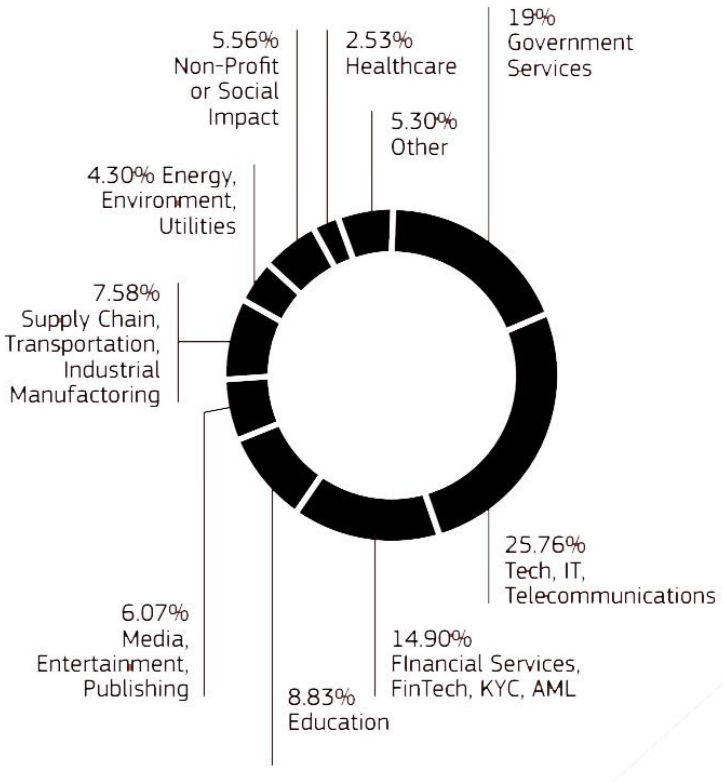


Figure 10. Current sectors using blockchain in Europe (Next Generation Internet, 2019).

The rise of blockchain is characterized by both the sharp growth in startups and by the growing volume of funding going in. Massive funding started in 2014 and rapidly increased to EUR 3.9 billion in 2017 and over EUR 7.4 billion in 2018 (Nascimento, et al., 2019). Blockchain and Distributed Ledger Technologies are now considered one of the

technologies to have a profound impact over the next 10 to 15 years (OECD, 2016). Then again, as regards its economic impact, recent analyses give mixed signals. A large majority (77%) of chief information officers acknowledged that their organization had no interest or plans to investigate or develop blockchain systems, and only 1% identified any form of blockchain adoption within their organizations (Furlonger and Kandaswamy, 2018). Also, a high rate of projects is either abandoned or do not achieve a meaningful scale (Deloitte, 2017). When it comes to ICOs, over half of the projects become inactive in four months (Benedetti and Kostovetsky, 2018), while over 80% were identified as scams in 2017 (Satis Group, 2018; Nascimento et al., 2019). Based on these statistics, it shows that blockchain adoption is not a simple affair, and early flocking to the new technology may have attracted funding, but does not necessarily turn out to be transformative. Nevertheless, alongside misgivings concerning the impact of blockchain, its added value, or concrete paths for its widespread deployment, signs of compelling possibilities for its application, and potential growth are becoming worthy of attention (Nascimento et al., 2019).

In this chapter, we've understood how blockchain works, what it can do, a bit of what is already being done, and what drives the various approaches to its applications. To conclude, we ask the simple question: why is blockchain so significant when it comes to trust? For one thing, it is the first time in the history of humanity where there is the potential to create a permanent public record of virtually anything, of which no single person or third party has control over, and where we can all reliably agree on the correctness of what is written (Botsman, 2017). Its potential is quite up to our imagination. It is, however, important to state that blockchain does not follow a "one-size-fits-all" model, nor is it a panacea, i.e., a technology that will solve all economic frictions, but is a General-Purpose Technology (GPT), capable of influencing many sectors of the economy simultaneously (Nascimento et al., 2019; Werbach, 2018).

Chapter 3

TRUST AND BLOCKCHAIN

1. The paradoxes of trust in blockchain technology

At this point, the answer to the initial question, "how can 'blockchain trust' be defined?" has begun to take shape. To summarize, blockchain trust is a form of *distributed* trust that banks on the processes of cognitive risk assessment, since it deals with the incentivization of good behavior and the punishment of misbehavior. Monitoring is made possible through the system's inherent traceability, and *ex-ante* risk is reduced through a certain degree of predictability offered by its algorithms. The question that remains is if a degree of affective trust still lingers, since the participants on the network, although anonymous, are nevertheless known to be fellow human beings. Calculative trust is typically generalized to trust relationships involving non-volitional trustees (such as a product, electronic agent, or a technology) (Wang and Emurian, 2005; Jones, 2002; Marcella, 1999). However, trust in the non-volitional trustee and its underlying operator is inseparable, i.e., the operators or participants acting on the system do have their own volitions and thus could involve an affective dimension of trust (Li et al., 2008). We will delve deeper into this aspect within this chapter.

Blockchain trust is found to depend on on its four main characteristics: decentralized, immutable, encrypted and algorithmic. The next step is to determine the various implications of each characteristic on trust, and if this kind of trust is indeed relevant to these times – a step closer to answering the question, "can blockchain be trusted?". A historical analysis of the first blockchains, Bitcoin and Ethereum, was performed along with a literature review focusing on these previously defined

characteristics. Encapsulated into four paradoxes, each is presented with its benefits and limitations in the aspect of trust. This section aims to provide the reader a space to slow down the *accelerated trust*[17] process, also in the attempt to surmount the second level of the trust stack, i.e., trusting the *platform*.

1.1. Decentralized yet centralized

Centralized trust creates negative externalities even when those at the center remain trustworthy. As the market expands, a purely person-to-person approach breaks down and would necessitate the presence of intermediaries. Intermediation, on the other hand, serves many roles, but also imposes costs, especially when the intermediary is a private company that expects to generate revenue in return for the value it provides. The reconciliation costs create lock-in and value-extraction opportunities for the intermediaries[18] (Werbach, 2018). In this context, Nakamoto saw the dependence on trust as a liability, and thus aimed to eliminate the necessity of involving intermediaries through mathematics (Nakamoto, 2008). A distributed ledger does away with costs from reconciling information between parties that don't trust each other by replacing those redundant processes with a single record that everyone trusts (Werbach, 2018).

The Internet itself was designed to support trustworthy communication on a distributed network of networks (Werbach, 1997). Users can rely on the network to deliver data even though the system is extremely heterogenous, and no one manages the end-to-end flow of traffic. This was made possible through the use of the Internet Protocol (IP) – a "spanning layer" that provides the definitions that permit *translation* to occur between a

[17] «One of the enemies of trust, as it turns out, is efficiency. Trust needs friction, time, investment, and effort, yet technologies now are rendering systems to be so seamless that we may not always be fully conscious of the risks that we are taking. […] Quite ironically, one of the issues we face today is not the lack of trust, but the speed and ease at which we are trusting». As seen in the phenomenon of dating apps, where we practically go against our mothers' advice of not meeting up with strangers; or of fake news, a rampant sharing without actually reading articles, and terrible dependencies on summaries rather than delving deeper; or of ticking the checkbox on the Terms and Conditions of Facebook, not actually knowing that we are giving away certain rights to privacy and being covertly used in social experiments - «this is called *accelerated trust*. And when we are in an accelerated mode of trust, we can be impulsive. It requires a conscious gear change to slow down and think twice about our decisions». (Botsman, 2017)

[18] For example, immigrants and temporary workers in developed countries send nearly $554 billion annually back to relatives in the developing world, generating roughly $39 billion in transaction fees (World Bank, 2020).

range of services or technologies (Clark, 2005). As long as everyone agrees to support IP, what people do at higher and lower layers is up to them.

While the Internet architecture has garnered much success due to its promotion of tremendous innovation and creative freedom, a problem arose – it allowed for proprietary solutions and the concentration of power at higher levels. In 2017, Facebook[19] generated more than $30 billion in revenue from online activity on their platform, yet the users who actually provided the data that feeds this profit machine received little or none of the financial benefits. While Facebook and other online intermediaries are phenomenally innovative companies that have helped to connect the world and, in many ways, changed life for the better, the power that they have acquired is inherently corrupting. Intermediaries necessarily shape markets to serve their own interests[20] (Werbach, 2018).

Distributed ledger networks operate differently. A cryptocurrency token can be used to monetize ownership value, distributing profit to whom it is due. For example, the Inter Planetary File System (IPFS) offers a blockchain-based distributed cloud-storage technology. Instead of storing files in a particular location, accessible through a uniform resource locator (URL) address, IPFS stores multiple copies of files, in pieces, across many hard drives through the network. It is designed to use its native currency Filecoin to incentivize users to contribute storage space. The token provides the intermediation by establishing incentives on both sides. Those who upload files contribute tokens, and those who store them earn tokens. IPFS, the company, provides the technology, but has no control over the content stored on the network, and the value of the tokens depends on supply and demand (Werbach, 2018).

Removing unnecessary intermediaries can be a significant benefit, but it does not always occur. This is commonly caused by the "Oracle" problem – the conundrum of how to link the digital world with the physical world. For example, if a blockchain records title records of houses, and a ledger entry is to be recorded in the blockchain when the title of a particular house is transferred from A to B, how does the blockchain know if the house

[19] Facebook is distributed in the sense that the content on the platform is not being controlled (as long as it fits within content policies) or owned by one specific entity, but is centralized in the sense that the platform where the users' activity and data is being stored is owned by one entity.

[20] In 2017, for example, the European Union imposed a $2.7 billion fine on Google for manipulating online-shopping search results to benefit its affiliates (Scott, 2017).

has been physically transferred from A to B in the real world? A trusted authority in the physical world is needed to certify that the transaction being recorded on the blockchain has also been executed in reality (Nandwani, 2019).

On the other hand, centralization also has its benefits. In 2013, an update to the Bitcoin Core software accidentally triggered a potentially catastrophic discrepancy within the blockchain (Bitcoin, 2013). The Bitcoin community quickly recognized that the best course of action was to downgrade to the earlier version, destroying the unwanted deviation in the blockchain. The core developers were able to reach consensus in less than an hour through online chat room conversations. A more decentralized community might not have been able to respond in time to stave off a crisis. Therefore, to some degree, trusting a blockchain system means trusting its developer's judgement[21] (Werbach, 2018).

1.1.4. Consensus Attacks

One of the vulnerabilities already foreseen by Nakamoto is the so-called 51% attack – a phenomenon wherein the majority of the computing power on the network is controlled by an attacker or group of attackers. In such a scenario, the attacker would have enough mining power to intentionally exclude or modify the ordering of transactions, allowing them to halt payments between some or all users (Binance Academy, 2020). They would also be able to reverse transactions that were completed while they were in control of the network, meaning that they could double-spend[22] coins, which is the key incentive to conduct such an attack (Frankenfield, 2019). Upon preventing some or all of the other miners from mining, a *mining monopoly* would occur, blocking the distribution of the mining power and retaining the hash rate in the hands of a single entity (Binance Academy, 2020).

In technical terms, all the cryptocurrencies that use Proof-of-Work (PoW) are vulnerable to a 51% attack because the network is open for anyone to mine, including attackers (The Bridge, 2020). Practically speaking, the computing power needed to do this

[21] Other software updates termed as hard forks were also performed by Bitcoin, but were generally for technical fixes due to double-spending bugs that mar the integrity of the distributed ledger (Werbach, 2018).

[22] Double spending takes place when a malicious actor creates a copy of a transaction and adds it to a blockchain, erasing earlier transactions on the network as if they never took place (The Bridge, 2020).

is astronomical, and is accordingly extremely expensive[23]. Although it is quite difficult to attack a network with the magnitude of Bitcoin, it is not so challenging to achieve on smaller cryptocurrencies because of the lower hash rate[24]. Ironically though, doing so would crash the value of the currency, thus diminishing the incentive to attack new cryptocurrencies especially if the scale of the blockchain is miniscule. As a fix, shifting towards the Proof-of-Stake approach could mitigate attacks by allowing the possibility of rejecting the funds that an attacker is attempting to steal (Fintech Futures, 2019).

Nevertheless, in a podcast with Levine, Antonopoulos, Murphy and Mohan (2020), they state that the 51% attack nightmare scenario[25] is not actually that bad. Due to the preexisting rules on the blockchain, the possibilities of illicit activity that can be done in such an attack are in fact quite narrow and could quickly be mitigated[26]. In theory, a 51% attack would probably not destroy a blockchain-based currency outright, even if it would prove highly damaging, both on the integrity of the blockchain and on the trust of its constituents (Binance Academy, 2020). Furthermore, it does not put the whole cryptoeconomics space in a state of emergency, since the conditions that led to the successful attacks are case-specific, and highly dependent on the scale of the blockchain[27].

[23] It is thought that it would require more than $700,000 an hour to launch an attack on the Bitcoin network (Crypto51, n.d.).

[24] It could be economically feasible for an attacker to rent enough mining power to take over a network's hash rate. With the rising popularity of platforms such as NiceHash, a hash power broker that allows people to rent mining power, attackers have a larger possibility of conducting 51% attacks (Werbach, 2018).

[25] As of August of 2020, the once presumed to be purely theoretical and near impossible 51% attack caught the members of Ethereum's Classic (ETC) off guard. They suffered not one, but three 51% attacks from the same attacker, resulting in a massive reorganization of 4,236 blocks and the successful double-spending of $1.68 million worth of cryptocurrency. The attack caused the leading organization to execute a strategy of defensive mining, intended to stabilize the network's plummeting hash rate and resist future 51% attacks (Studnev, 2020).

[26] The most an attacker can do is to make use of the rules to work for his benefit, such as creating valid transactions of money transfers to their own wallets, or denying service to other actors to maintain a mining monopoly, or to diminish the general confidence in the system. Succeeding would still not enable them to create new coins, nor alter blocks that were created before the attack (Frankenfield, 2019). Also, even if the attacker does manage to disrupt the network, the software and protocol could be quickly modified and adapted as a response to that attack, resulting in a *hard fork* (explained further in the next section) that would require the other network nodes to reach consensus and agree on these changes (Levine et al., 2020).

[27] ETC has 20 times less hash rate than that of Ethereum and is 18th in rank in terms of the scale of the cryptocurrency. To attack Bitcoin, for example, the attackers would need about 4,500 times the amount of hash than what was needed for ETC, which is highly unlikely to happen any time soon (Clarke, 2019).

1.1.5. Mining pools

Another pressing issue around the PoW approach is the power it requires to keep the blockchain running. Theoretically, the mining power was envisioned to be distributed over different nodes across the world (Binance Academy, 2020). Reality begs to differ, as bitcoin miners in China are dominating the network, accounting for 65% of the bitcoin network's computer power, with the U.S. as the second-largest bitcoin mining country, contributing 7% (Bambrough, 2020). Bitcoin mining is heavily driven by energy and infrastructure costs, and is therefore lucrative to situate bitcoin mining pools in countries such as China where the electricity is cheap and renewable[28].

The carbon footprint, i.e., the emissions associated with the electricity, is therefore a point of argument[29]. In order to keep global warming below 2°C — as internationally agreed in Paris COP21 — net-zero carbon emissions during the second half of the century are crucial (United Nations, 2015). Put into context, cryptocurrencies cause a relatively small fraction of global emissions. Still, to take the right measures, policy-makers need to understand the carbon footprint of cryptocurrencies. In the long run, bitcoin miners are envisioned to increasingly establish their operations near large sources of renewable energy, which also triggers further development of renewable generation resources at the respective sites (Stoll et al., 2019).

1.1.6. Remarks

While threats such as 51% attacks exist, solutions such as switching to a PoS consensus mechanism are already in place. Even so, PoW still retains adequate robustness for larger cryptocurrencies such as Bitcoin and Ethereum, and although mining pools suggest a degree of residual centralization, it also serves its purpose as a barrier of entry, making it difficult for malicious actors to acquire resources needed to hack the system. More to the point, the limit of decentralization is the fact that questions of governance and regulation cannot be dismissed. This is the paradox of blockchain technology as stated by Vili Lehdonvirta: «If they truly have no means of collectively resolving disputes other than

[28] As of July 2019, Bitcoin's total energy consumption equaled that of Switzerland, estimated at around seven gigawatts of electricity or 0.21% of the world's supply (Baraniuk, 2019).

[29] The electricity used by Bitcoin produces about 22 megatons of CO2 annually, which is as much as Kansas in the U.S. produces (Stoll et al., 2019).

voluntary agreement, they will most likely fail. On the other hand, when these networks adopt formal or informal governance structures, they are no longer truly decentralized». The very mechanisms that could make decentralized systems effective seemingly make them no longer decentralized (Kaminska, 2017).

1.2. Immutable yet changeable

Immutability, as explained in the second chapter, represents the time dimension of blockchain trust. Blockchain eliminates the need for an intermediary that typically validates the content of a transaction. To trust that the information currently displayed in a database is the information originally recorded, one must trust the goodwill and procedures of each intermediary. This is what the blockchain addresses by decentralizing trust. In such a system, however, information is reliable only if it is highly resistant to tampering. The blockchain addresses this problem by making transactions immutable, and is therefore an important factor in making ledgers trustworthy in a decentralized way. It serves as a proxy for trust in the actors that maintain the information in traditional trust architectures. If the ledger is immutable, the risk of manipulation of the records is highly unlikely, which makes it remarkably reliable (Werbach, 2018).

1.2.1. Cryptoassets

Blockchain's immutability is a significant reason why tokenization holds so much promise. Indeed, the real potential gamechanger in the economics of financial services is the fundamental change in industry structure brought about by blockchain's tokenization model. The traditional way of making something valuable is to make it scarce, such as in the case of gold and diamonds versus copper and granite. The Internet economy, by contrast, is governed by the economics of abundance. A physical bookshop has scarce shelf space, whereas Amazon virtually has no limit in listing yet another item. While it is virtually costless to make a perfect digital copy of content and distribute it around the world, the creative industries resorted to a series of copyright law battles to keep their business going (Werbach, 2018).

Blockchain technology, instead, is a technology of *artificial scarcity*. It combines the benefits of digital transactions with assurance that digital resources cannot be copied. Content owners can thus use cryptography in the form of digital rights management to prevent unauthorized copying of audio and video files. Once a token represents scarce

value, it can be used more than money; it becomes a cryptographically secured digital asset, or *cryptoasset* (Burniske and Tatar, 2018). Cryptoassets can represent physical goods, scarce digital identities, as well as the utility of the network itself[30]. Alternatively, tokens can be created through the previously mentioned initial coin offering (ICO) or through a security token offering (STO), producing different tokens such as equity, shares in a company, ownership in a piece of real estate, or participation in an investment fund (Laurent et al., 2018).

By tokenizing typically illiquid assets such as fine art or real estate, these tokens can be then traded on a secondary market of the issuer's choice. This access to a broader base of traders increases the liquidity, thereby capturing greater value from the underlying asset. Transactions are made faster and cheaper, since they are facilitated by smart contracts, and are more transparent since the token is inherently embedded with the token-holder's rights and legal responsibilities. Through these benefits, the possibility of unlocking trillions of euros in currently illiquid assets and vastly increasing volumes of trades is foreseen (Jerry, 2020).

As always, the big problem revolves around regulatory alignment, and thus far the realization of mass adoption has still a long way to go. Certain assets cannot exist only in the digital realm, as they are a part of the physical world. Therefore, any attempt to asset tokenization would have to take government regulations into account, at least to some extent. In terms of current regulations, most countries would agree that tokens are nothing more than codes without any value. That means users would have no legal ground to associate them with pieces of property. There is also a degree of uncertainty in code of conduct and common standards for the development and management of tokenized assets, and thus needs the adoption of formal frameworks to ensure trust among all market participants (Jerry, 2020).

In summary, the following factors should be considered before making a trust leap into cryptoassets: the business model, or the definition of the roles of financial institutions

[30] For Ethereum, the value of its utility is based on its ability to create decentralized applications (Dapps), using "ether" to pay for the necessary "gas" to execute computations. The term "gas" is used to describe a special Ethereum unit designed to measure the amount of work necessary to perform a certain action or a set of actions. Gas exists inside the Ethereum Virtual Machine in a form of a count. Its role is to calculate how much work is being performed. And while paying for the gas, a certain number of ether is charged as a transaction fee (Magento, 2017).

within the value chain; cybersecurity and its capacity to mitigate the risks of weak points regarding the management of private keys and wallets; platform integration, or an infrastructure that can provide both economic and technical solutions to the business models without having to change much of the legacy systems; jurisdiction reconciliation, or the regulatory and legislative frameworks that are compliant to both the investor's and issuer's jurisdictions; and compliance to the regulations that are already existing within the digital space, such as Know Your Customer (KYC) utilities and other similar entities (Philip, 2020).

1.2.2. Probabilistic and flexible immutability

Immutability, as it turns out, is not always well defined. In the case of blockchain, it does not mean that the records can never be changed or rolled back. Blockchain trust is immutable not in a binary sense, but in a probabilistic sense. Distinguishing untrustworthy chains from the consensus is not an all-or-nothing decision. The more subsequent blocks are added following one block in question, the more processing power is required to fork the chain back to that point (Werbach, 2018). The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power (Nakamoto, 2008). Over time, therefore, trust in prior transactions increases. To accept the longest chain is to trust in the probability that it is the reigning version of truth (Werbach, 2018).

The immutability of blockchain is also not absolute, as is already noted in the previous section. There are at least two groups of actors in a distributed ledger network with the power to unwind recorded transactions: *developers* and *verification nodes*. In 2016, the Ethereum network, particularly the Decentralized Autonomous Organization (DAO), was struck by an ill-famed hack[31] wherein an unknown attacker managed to siphon off more than a third of the network's cryptocurrency – the equivalent of $70 million at the time (Werbach, 2018).

[31] The hack was executed through a series of smart contracts that were formally valid within the system's rules. There was no legal or technical way to recover the funds without undermining the entire system in the sense that even if a court ordered the funds to be returned, there was no one to carry out that order (Werbach, 2018).

In an attempt to rewrite history, Vitalik Buterin, the co-founder of Ethereum, and others, convinced a majority of nodes to split the entire Ethereum blockchain. Such a system-wide move is called a *hard fork* that creates two incompatible chains, and is implemented through a software update. Each blockchain treats the other as invalid, as though someone maliciously added illegitimate transactions. If everyone agrees to go down one fork, it becomes the real chain. For those running the new software, the DAO hack never happened, and their blockchains do not recognize the currency transfers related to that hack (Werbach, 2018).

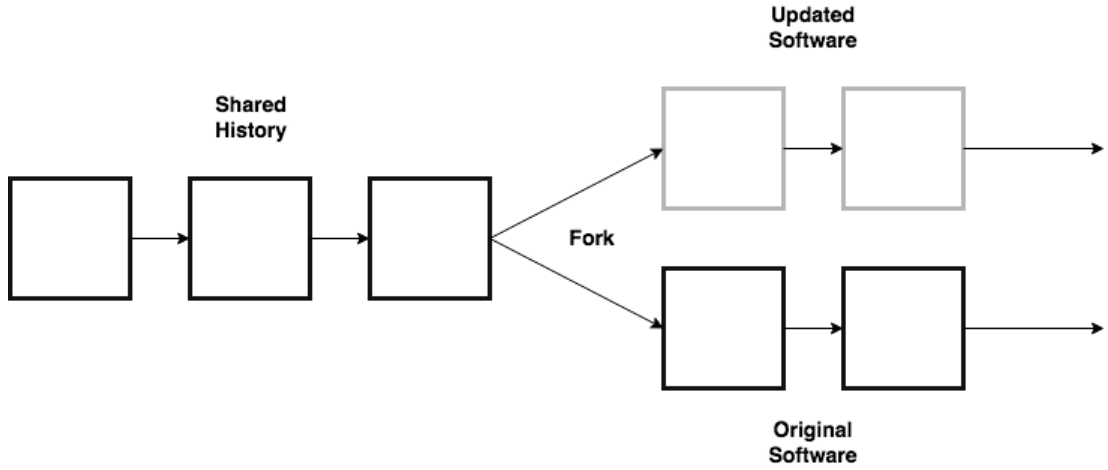


Figure 11. Representation of a hard fork (Maddrey, 2018)

This catastrophe has had several repercussions as it practically destroyed the DAO and weakened the confidence in the Ethereum platform. More importantly, it signified that blockchains were not truly immune from centralized interference, and raised questions about what might happen if governments or central authorities would become concerned about records stored on distributed ledgers (Werbach, 2018).

In any case, a hard fork is a rare and difficult occurrence, as it requires more than half of the nodes in the network to shift to the new chain. That being said, the network software developers are not the only ones who can initiate a hard fork. The operators of the verification nodes could independently choose to update their software to fork the chain. If most of the nodes are running software code that specifies a prior transaction is invalid, it will no longer be included in the blockchains they recognize. If one side of a hard fork disregards a previously verified transaction, it directly breaks the immutability of the ledger (Werbach, 2018).

1.2.3. Remarks

Even though blockchain's immutability is not absolute, it does not undermine the trust value of these systems. Furthermore, the fact that miners and core developers can exert influence over the direction of a blockchain does not invalidate the basic claim of decentralization either. Immutability holds up as long as the network is collectively more powerful than the attacker. Furthermore, governance mechanisms – under which transactions may be reversed or rules of the network changed – could also be implemented to address this conundrum (Werbach, 2018). More importantly, rather than claiming that a blockchain is immutable, a more suitable term would be "tamper-resistant". Tamper-resistant is not the same as "immutable" or "unchangeable", but rather means "extremely difficult to change" (Nascimento, et al., 2019).

1.3. Transparent yet highly encrypted

In a public blockchain, every transaction is broadcast across the network. In the Bitcoin network for example, anyone can view[32] and download the entire blockchain back to the genesis block mined by Satoshi in early 2009. As mentioned in the second chapter, blockchain employs public-key cryptography, wherein the parties involved are identified only by cryptographic keys which are associated with transactions rather than accounts. Due to its pseudo-anonymous nature, a blockchain is capable of keeping a wide range of identities while maintaining their privacy (Berg et al., 2018). The pseudonymity within the public blockchain is not enough to guarantee full anonymity, since it is possible to de-anonymize a user by analyzing network traffic or the blockchain itself. Furthermore, transparency in a blockchain may not necessarily conflict with privacy but is beneficial to data integrity (Zetzsche et al., 2017). It adds to the level of security as it allows third parties to provide analytics services that examine transaction patterns across the network, removing the possibility of malicious content in the blocks (Werbach, 2018).

[32] See https://www.blockchain.com/explorer

1.3.1. Quantum Computing

In the past couple of years, developing new quantum algorithms[33] has become an active field of research that has seen increasing growth (Barmes et al., 2019). Since Google announced that it achieved quantum supremacy, there has been a growing number of articles predicting the demise of currently used cryptography in general, and Bitcoin in particular (Barmes and Bosch, 2019). The Shor's algorithm has the potential to break most of the currently used public-key cryptography, hence breaking the assumption of asymmetric cryptography (Barmes et al., 2019). This means that anyone with a sufficiently large quantum computer could use this algorithm to derive a private key from its corresponding public key, and thus, falsify any digital signature (Barmes and Bosch, 2019).

There are two types of addresses from which Shor's algorithm could decrypt the public and private key from[34]. Currently, there are over 4 million BTC (about 25% of all Bitcoins) that are potentially vulnerable to a quantum attack – at current price[35] amounting to almost 142 billion USD. To mitigate the risk of Bitcoin being stolen from these addresses through quantum computing, transferring Bitcoins to a "pay to public key hash"[36] address that has never been used to spend Bitcoins should safeguard the wallet since their public keys have never been revealed. In this sense, the prerequisite of being "quantum safe" is that the public key associated with the address is not public. As soon as

[33] Quantum computing is a branch of computer science that is based on the principles of the superposition of matter and quantum entanglement and uses a different computation method from the traditional. In theory, it would be able to store many more states per unit of information and operate with much more efficient algorithms (Iberdrola, 2020). By entering into this quantum area of computing where the traditional laws of physics no longer apply, we open up the prospect of creating processors that are significantly faster, possibly a million or more times faster than the ones we use today (Marr, 2017).

[34] In the early days of Bitcoin, the dominant address type was called "pay to public key" (p2pk), wherein the public key serves as the Bitcoin address of the recipient. Quantum computing is a direct threat to these, because the public key is directly obtainable from the address. Since all transactions in Bitcoin are public, anyone can obtain the public key from any p2pk address. A quantum computer running Shor's algorithm could then be used to derive the private key from this address. This would allow an adversary who has a quantum computer to spend the coins that the address had (Barmes and Bosch, 2019).

[35] As of the 2nd of February, 2021, the price of bitcoin is at $35,477.00

[36] In the second type of transaction, the address of the recipient is composed of a hash of the public key. A hash is a one-way cryptographic function, and as such, the public key is not directly revealed by the address. The first and most popular implementation of this is called "pay to public key hash" (p2pkh) and was designed to solve the issues on the long checksum and address length of p2pk. However, as soon as a user initiates a transaction from a specific p2pkh address, the public key is revealed. As a precaution, many wallets are programmed to avoid address reuse. It is only ideal not to use the same address again, but not all users take this advice to heart (Barmes and Bosch, 2019).

a transaction is made from that address, however, the public key is revealed, making the address vulnerable (Barmes and Bosch, 2019).

In the Bitcoin blockchain, it currently takes about 10 minutes for transactions to be mined. As long as it takes a quantum computer longer than that to derive the private key of a specific public key, then the network should be safe. Current scientific estimations predict that a quantum computer will take about 8 hours to derive a typical Bitcoin private key from a public key. However, as the field of quantum computers is still in its early stages, it is unclear how fast such a computer will become in the future. If a quantum computer achieves derivation of a private key within the 10-minute mark, then the Bitcoin blockchain will inherently be broken. The most resilient solution in this case is to transition to a new type of cryptography called "post-quantum" cryptography, which is considered to be inherently resistant to quantum attacks. These types of algorithms present other challenges to the usability of blockchains and are still in the process of being investigated by cryptographers (Barmes and Bosch, 2019).

1.3.2. The Darknet

Aside from the threat of quantum computers, one of the more disreputable issues of blockchain's pseudo-anonymous privacy is that of Bitcoin's history with the previously mentioned "Darknet" – a place where people could buy anything they want without being identified (Kethineni, 2017). In addition to offering extreme privacy and protection from the surveillance of authoritarian governments, the dark web facilitates a growing underground marketplace that sophisticated criminals use to traffic drugs, stolen identities, child pornography, and other illicit products and services (Kumar and Rosenbach, 2019). Unfortunately, the anonymity that blockchain provides may act as a powerful motivation for people to use it in facilitating criminal activity (Mihm, 2018).

Bitcoin emerged in 2011 as the currency of choice for drug dealers conducting transactions on a Darknet site known as the Silk Road. The combination of an encrypted network hidden from most of the world and a transactional currency that is nearly

untraceable by law enforcement officials resulted in a small but significant marketplace[37] of illicit vendors selling illegal wares (Kumar and Rosenbach, 2019). Although the serious nature and rapid growth of illicit transactions on the dark web should concern governments and global financial institutions, the overall portion[38] of worldwide commerce transacted on the dark web is miniscule compared with global illicit commerce (Kumar and Rosenbach, 2019).

Be that as it may, many of the most corrosive threats to society today operate in the encryption of the Tor network, and thus merit the attention of international regulators, financial institutions and law enforcement agencies. The challenge for these in question is for them to devise approaches that are within the fine line of protecting liberal principles in an age of information control, while identifying and eradicating these insidious activities on the dark web. Through improving information sharing, sharpening law enforcement's technical capabilities, the international community has already made significant progress in addressing these challenges. Nevertheless, close cooperation between law enforcement, financial institutions and regulators around the world is required to mitigate the density of nefarious activity (Kumar and Rosenbach, 2019).

1.3.3. Security through structured transparency

There exists a second level of blockchain transparency. The algorithms of blockchain are not hidden, like that of Google or Facebook; the software is, in fact, *open source*. Most of the critical software programs underpinning the Internet, including the Linux operating system and Apache web server, are open source (Werbach, 2018). Since the codes are available for inspection by all participants in the ecosystem, anyone can review or suggest improvements to the code. Trusting the efficacy of the consensus mechanism on these networks, therefore, is not just a matter of reputation or legal enforcements; it can be backed by direct inspection and analysis of algorithms (Maurer, et al., 2013).

---

[37] Up to 75% of 200 domains catalogued as illegal appear to be marketplaces, mostly fueled by Bitcoin and other cryptocurrencies (Kharif, 2019).

[38] A report from Chainalysis, a leading crypto-payment analytic firm, shows that the proportion of Bitcoin transactions tied to illicit deals has declined by 6% since 2012, and now accounts for less than 1% of all Bitcoin activity (Kharif, 2019).

In traditional trust architectures, there is an assumption that something transparent is inherently untrustworthy. Trust is generally reinforced through secrecy in traditional architectures[39]. Open-source blockchain software, by contrast, is freely available to copy and modify. The essence of the cryptoeconomic trust model is in fact the overcoming of strategic behavior through game theory, not through obfuscation[40]. This is one of the great insights of modern cryptography and software development: the traditional solution of "security through obscurity" is often misguided and can be replaced with security through structured transparency (Werbach, 2018).

Trust emerging from transparency is not new. Public companies are required to report detailed information about their financial performance every quarter, corporations are required to submit to regular audits. This is to ensure that the information that firms report is accurate and that the conclusions they draw about their performance match the underlying reality. Still, auditing is an imperfect process. Auditing can fail, especially when the auditors' incentives are misaligned with that of the investors. In cryptoeconomic systems, distributed ledger platforms are structured to align incentives with trustworthiness (Werbach, 2018).

Finally, in some cases, there may be good reasons not to make all transactions transparent. In a supply chain environment, for example, transaction flows may have significant competitive value. Participants may not want their competitors to know their exact transaction patterns, or secrecy may be particularly important to the user or the application. As a result, most permissioned blockchains do away with Bitcoin's transparent ledger. This is also beneficial as removing the *flooding* requirement to broadcast every transaction throughout the network significantly improves the system's performance (Werbach, 2018).

---

[39] However, the reason a bank will not show you its full transaction ledger is not because it would make you question the accuracy of its records, but because it would reveal the action of other customers. In this sense, it is often a confusion of trust with reputation or privacy (Werbach, 2018).

[40] More developers having access to the source code means that more people can identify bugs. Members of the community engage in white hat (friendly hacking) operations to identify, isolate, and mitigate possible vulnerabilities in the algorithms. Security flaws are easier to spot when the code is out in the open (Werbach, 2018).

1.3.4. Remarks

Although threats such as quantum computing exist and could very well break the foundations of blockchain, new quantum-safe cryptographies are already being explored. Moreover, while open-source software may have its advantages, it will always be exposed to malicious users. Thus, stringent quality control processes must be put in place to ensure that no grave vulnerability is left unmitigated. Also, the fact that anyone can take apart, evaluate operations, create extensions to the code, or even create a modified version of it can lead to fragmentation, but it also promotes innovation.

Lastly, the appropriate level of transparency of blockchain systems must be considered on a case-to-case basis, since it is also possible to have multiple levels of transparency on the same network. In the different contexts described above, one can conclude that various encryption approaches, transparency structures and enforcement of regulations should be carefully studied in existing as well as future applications in moving towards achieving global adoption. While blockchain's encrypted transparency remains a challenging trust leap to take, one has to admit that there is some sort of poetic justice in the fact that the blockchain itself was created by someone anonymous.

1.4. Algorithmic yet human

Defined in simple terms, an algorithm is a set of instructions designed to perform a specific task, or more specifically, it is a process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer. In a blockchain system, what is being trusted is not the people, but the software and underlying math of the consensus process. As in any form of algorithm, the trustworthiness of the code depends very much on the technical skill, as well as the intent of the developer. As explained in the previous section, the reliability of the code is increased when the source code is freely accessible, since anyone can examine the code and preview the mechanisms used to generate trustworthy results (Werbach, 2018).

The benefits of smart contracts are obvious, but they must be used with caution. Many businesses, for example, have found the use of smart contracts to be too dependent on formal rules and on well-specified inputs. It leaves little room for multiplicity of eventualities where rules may need to be slightly altered because of unforeseen circumstances. For example, a car used on demand may simply shut itself down if unpaid, but will be unavailable to use in case of a life or death situation. Smart contracts are good

for simple transactions, but for complex situations, a governing body with human involvement is still needed to provide assessments (Coding Tech, 2018). For this, it is arguable that smart contracts are neither *smart* (capable of translating complex legal agreements into software) nor *contracts* (they have no underlying legal or contractual provisions) (Orcutt, 2018).

Vitalik Buterin, co-founder of Ethereum, distinguishes two kinds of cryptoeconomic systems: *objective* and *subjective*. In an objective system, the protocol's operation and consensus can be maintained at all times using solely nodes, knowing nothing but the rules of the protocol itself. Subjective systems, on the other hand, require more additional knowledge that has to come from a source, typically a central authority.

Objective systems seem desirable, relying entirely on machines and not fallible and opportunistic humans. There is, however, a catch – machines may be running the code, but humans are acting on it. A subjective system might be able to differentiate between legitimate and illegitimate transactions in a way that an objective one could not. Concepts like manipulation, takeovers and deceit are undetectable, or in some cases indefinable in pure cryptography, thus the need for a human community surrounding the protocol[41] (Buterin, 2015). Intent, for example, is something that computers cannot determine under the terms of a smart contract (Werbach, 2018).

The ever-infamous DAO hack is notable in this regard, as its raison d'être was to be a radical social experiment that explored the possibilities of a self-running company – an enterprise without executives, managers, or any type of chief[42]. The idea was to create

[41] Blockchains can incorporate human decision-makers explicitly, as can be seen in Multisig or multi signatures. In a basic bitcoin transaction, the recipient of the currency must provide his or her private key to receive funds. The sender specifies that some fraction of a larger number of keys is required and triggers a simple arbitration process. If all parties agree, their keys are sufficient to consummate the transaction. If a tie exists between the parties, an additional key-holder would be required to break the tie. This allows the blockchain to connect with human-based trust because an arbitrator can break the tie between adversarial parties (Werbach, 2018).

[42] In traditional companies, all agents of a company have employment contracts that regulate their relationship with the organization and with each other. Their rights and obligations are regulated by legal contracts and enforced by a legal system which is subject to the underlying governing law of the country they reside in. DAOs, on the other hand, involve a set of people interacting with each other according to a self-enforcing open-source protocol. Keeping the network safe and performing other network tasks is rewarded with the native network tokens. Blockchains and smart contracts hereby reduce transaction costs of management at higher levels of transparency, aligning the interests of all stakeholders by the consensus rules tied to the native token. Individual behavior is incentivized with a token to collectively contribute to a common goal. Members of a DAO are not bound together by a legal entity, nor have they entered into any

smart computer code that could make decisions and autonomously run the organization in place of individuals, with blockchain as its core – hence the name Decentralized Autonomous Organizations (DAO). Benevolently, the DAO's main purpose was to redistribute power away from the rent seekers and incumbent middlemen and back into the hands of the people actually creating value (Botsman, 2017). From an idealist's perspective, smart contracts are meant to be stand-alone agreements and therefore are not subject to interpretation by outside entities or jurisdictions. The code itself is meant to be the ultimate arbiter of "the deal" it represents (Siegel, 2016). However, as the DAO theft demonstrated, humans are quite hard to remove from the equation[43].

Similarly, the blockchain can use algorithmic decision-making to take humans out of the loop more thoroughly through systems that incorporate machine learning or artificial intelligence. Advances in machine learning are behind the rapid improvements in everything from the Siri and Alexa intelligent agents to autonomous or driverless cars (Botsman, 2017). Since the system evolves in response to the data, the results of the system may become increasingly complex. The problem is that the algorithm's machine learning comes from abstract statistical correlations that are more and more difficult for humans to interpret and audit. Trusting an AI-trained system, therefore, adds another degree of risk over trusting a system based on a hard-coded algorithm (Werbach, 2018).

In this regard, Coye Cheshire distinguishes *interpersonal trust* (human to human) and *system trust* (human to system). System trust was thought to be more simplistic since there was no need to consider that systems are capable of betrayal. It has become far more intricate, as Cheshire states: «We are working with these systems that are using complex algorithms to manage information to make decisions on our behalf, but they are getting too

formal legal contracts. Instead, they are steered by incentives tied to the network tokens, and fully transparent rules that are written into the piece of software, which is enforced by machine consensus (Voshmgir, 2020).

[43] In 2016, the DAO fund (daohub.org) was launched in a crowdsale or an initial coin offering (ICO) – an initial funding period in which people add funds to the DAO by purchasing tokens that represent ownership, so as to give it the resources it needs. In this process, people can then make proposals to the DAO on how to spend the money, and the members who have bought in can vote to approve these proposals. The ICO earned an equivalent of 150 million USD within a 28-day funding window – the biggest token sale at its time. In the process of development and debugging the initial projects, an unknown attacker began draining the DAO of ether (ETH) collected from the sale of its tokens, exploiting a loophole in the DAO fund smart contract. Essentially, a programming mistake in the code allowed a DAO shareholder to create an identical clone fund as a "child DAO" and then move money freely. The attacker managed to drain more than 3.6M ether into a child DAO, consequently dropping the price of ether from $20 to under $13 (Siegel, 2016).

complex for our brains to understand». Today, systems embody everything from online platforms that are blurring the line in terms of our awareness around what the machine is doing. In some ways, we have offloaded some of our cognitive power, and interpersonal trust and system trust are becoming more and more comparable (Cheshire, 2011).

> «Indeed, software engineers have become so much more than just creators of digital systems that process complex forms of information. […] In the past, engineers would typically work on physical infrastructure projects such as roads, rail lines, gas pipelines and bridges. Today, however, they are designing new kinds of social infrastructure: online bridges that bring friends, families and strangers together. They are trust engineers» (Botsman, 2017).

1.5. Other considerations

I have contemplated on dedicating a greater space to the legal grey areas within blockchain, but I have found it to be a field too broad and unfamiliar, and with high risk of presenting a study that lacks foundation without further research. Nevertheless, I shall briefly present my findings specific to the following sub-paradox, which could effectively be a recommendation for future studies as well.

> Auditable yet unaccountable: Turning back to the DAO Hack where the hacker exploited a loophole in a smart contract, the interesting point lies in the fact that the theft was done through a legitimate action. In terms of law, the action of the actor was fully compliant with United States criminal and tort law. Clearly, the power of smart contracts was abused, and the lack of human intervention removes the situation from the domain of judicial oversight. Due to the transparent nature of blockchain, manipulation attempts are easily auditable and traceable, yet actors behind these attacks are nevertheless protected by their pseudo anonymous identities. Furthermore, there exists no traditional recourse for the tokens stolen, as these are basically uncharted legal waters. With smart contracts, there are no judges – the parties specify the terms at the outset, and the blockchain network automatically enforces them once the contract is activated. This can produce scenarios where a contract is executed in a way that none of the parties intended, or it can give one party extraordinary power over the other without judicial restraints (Werbach, 2018).

2. Blockchain for Social Impact

At this point of the study, we understand that blockchain technology is not a perfect solution to the problem of trust. The fact is, neither are the systems that are being currently employed in our traditional infrastructures. Blockchain is inherently more secure than centralized systems, and opens up opportunities that go beyond concerns of security and recordkeeping. There are limitless possibilities for blockchain, and by now there are hundreds of initiatives already well on their way. The question we have to ask ourselves now is: "For what purpose should we use blockchain?"

Inevitably so, and as was presented in the previous sections, this novelty of a technology has already been used for motives that are less than benevolent. Distributed trust is far from foolproof, and the questions that really matter are ethical and moral, not technical. With the technology's inherently borderless nature, the risk of straying is equally high. The dawn of the fourth greatest industrial revolution is upon us (Botsman, 2017), and we must contemplate a great deal on what we want to do with it. Otherwise, the head, heart and soul of blockchain will be one that is not social and civil.

We are on our third and final step in the Trust Stack: trusting the *other person.* In this particular case, identifying the person can be quite complicated due to the nature of blockchain and its participants. However, the motive behind the creation of the blockchain could very well serve as an element by which we can determine the benevolence, and thus in part, the trustworthiness of the person or persons involved. The "sky is the limit" with blockchain, so in the choice to use it to change one's harsh reality into that which is desirable also for others, it becomes a step towards having a social impact (Good Finance, 2018). In this next section, we take a look into the concrete reality of things – what has already been done, and where lies the potential of blockchain within the social sector.

2.1. Health

The largest number of blockchain for good initiatives resides in the Health Sector, according to the Stanford Research, *Blockchain for Social Impact: Moving Beyond the Hype.* Its applications can be found in digital health records maintenance and pharmaceutical supply chain management. The siloed nature of electronic health records is one of the biggest challenges in this sector, with limited interoperability between each information management system. Furthermore, the safe transport of medicine and vaccines

from manufacturer to end user is a concern worldwide (Galen et al., 2018). Provenance and environmental condition tracking are vital to keeping certain medicines from being discarded, and from keeping counterfeit drugs out of the market. The WHO estimates that 700,000 deaths each year are connected to counterfeit malaria and tuberculosis drugs alone (Farmer, 2020).

Currently, we are tackling a pandemic that has affected many social, economic and environmental determinants of health. As of now, numerous companies have announced COVID-19 vaccines with efficacy rates of more than 90%. The global distribution of these vaccines poses a grand challenge, due to the conditions in which they must be stored. According to Netta Korin (2020), tackling COVID-19 will require the first-ever deployment of blockchain in the global distribution of a vaccine. Modum.io, with the use of hardware sensors placed in each package, tracks temperature conditions of a medicinal product while in transit. Smart contracts on the blockchain automate notifications to the supplier and the receiver upon meeting the requirements of shipment. Founded in 2016, Modum.io has already completed three pilot projects, and its first-generation sensors are well into mass production (Galen et al., 2018).

Another blockchain-based app launched during the coronavirus outbreak is Coalition, which aids in contact tracing and prevents the spread of the virus through proactively identifying and advising individuals. Similar to the Immuni app of Italy, it can be used to monitor movements of people who are positive with the virus, and notifies others of potential interactions with an infected person. It also uses Bluetooth-enabled cryptography technology to track meetings and generate anonymous random IDs to protect the identity of the user, with all data locally saved on a user's phone (The Local, 2020).

As was witnessed in Italy, however, systems like these are unable to reach their full potential if they lack adoption by the majority of the population. The more people download the contact-tracing app, the better it will become at notifying users of whether they may have been in contact with an infected person (The Local, 2020). Part of the problem, therefore, is not a technical one, but one of trust, as reservations regarding privacy have been brought up despite the valid claim that the system functions on totally anonymous grounds.

2.2. Agriculture

Traditional agricultural supply chains rely on paper-based or database systems to store compliance data, such as data on the safety, sustainability, and certificate status of food products (Ge, 2017). This structure results in costly operational management and high potential for fraud and corruption, or human and technology-based error. Furthermore, the WHO estimates that one in 10 people fall ill every year from eating contaminated foods (World Health Organization, 2015)

Investments in blockchain for Agriculture are still at an early age, with 93% percent of initiatives at either the concept stage or small pilot stage. For blockchain to be fully implemented in any supply chain, the engagement of each stakeholder – farmer, distributor, packager, trucker, retailers, etc. – would be required. It also requires a level of digital literacy and viable Internet connections, which would prove a challenge within rural areas of developing countries (Galen et al., 2018).

Despite these challenges, Bext360 has succeeded in reaching hundreds of farmers through small projects in Ethiopia, Nicaragua, Colombia, Uganda and California as of 2017, and has anticipated reaching thousands by the end of 2018. Founded in 2015, Bext360 has developed a device that combines machine learning and artificial intelligence with blockchain to create a more efficient and transparent coffee supply chain (Galen et al., 2018). Typically, farmers tend to be paid on the basis of quantity, rather than quality, and often do not receive payment right away. For those making less than $2 a day, this presents a myriad of challenges (World Bank, 2016). The machine thus ensures that farmers are paid fairly and immediately, while simultaneously helping consumers better understand where and how their coffee was produced. The machine weighs, analyzes and prices coffee directly at the source, offering a price to farmers immediately and impartially, and utilizes smart contracts to enable digital/mobile payments instantly (Galen et al., 2018).

Although blockchains may be immutable ledgers, the accuracy of data inserted by the sensors or by persons cannot always be guaranteed. The inclusion of a certifying authority, which is for all intents and purposes an intermediary, could still be needed to ensure the validity of the data. Another technical issue is the integration of blockchain with legacy traceability systems, while preserving the blockchain's distributed and decentralized nature. Furthermore, the financial and environmental cost and benefits have yet to be evaluated, since its usage comes with an enormous amount of energy and financial

cost. Nevertheless, investment in these fast-developing technologies, along with artificial intelligence, in combination with blockchain technology could lead to the establishment of the smart agriculture paradigm where all the different services, components and stakeholders could be interconnected. This envisions benefits towards more efficient production, by leveraging big data and machine learning algorithms (Demestichas, 2020).

2.3. Land Rights

Keeping an up-to-date and accurate registry is one of the biggest challenges for land governance in developing countries. Many countries do not even have a ledger, and for those who do, property records are typically vulnerable to inconsistencies, as well as issues such as tampering, damage, and loss (Kriticos, 2019). Today, having secure land tenure is considered a form of economic empowerment, a safeguard against displacement or exploitation, and even a foundation of cultural identity, especially for communities and indigenous people (Galen et al., 2018). In many parts of the world, however, land rights are a rare luxury, with only 30% of the world's population having a legally registered title to their land (World Bank, 2017).

Blockchain as a solution promotes various benefits. The transparency blockchain brings to land registries could be publicly beneficial, as the visibility of prices, areas, ownership, and overarching trends could be gleaned from land registries. Smart contracts could foster efficiencies in official processes related to registering land, like purchase, sale, subdivision, or inheritance. Also, the technology's "double-spending" solution could prove useful, making it difficult to register one plot of land to multiple owners or over-leverage financing from different sources on the same plot, and could potentially prevent illicit sale of already-owned land to new parties (Galen et al., 2018).

Some of the major drawbacks of using blockchain technology to manage land transactions are infrastructural. Implementing blockchain for land registries requires digitized records and widespread Internet connectivity (Galen et al., 2018). Most developing countries still operate with paper-based cadasters that are largely incomplete, leaving the significant challenge of digitizing and updating records to accurately reflect property and ownership characteristics (Kriticos, 2019). Another question for blockchain in the Land Rights sector is the quality of the data. Proving legitimacy of land claims and occupancy is usually a task for courts. Judicial processes are only as functional as their outcomes, and in many places in the world, these outcomes can be a result of willingness

or capacity to pay for legal help. Blockchain implementations for land must then consider how to avoid further concentrating power in the hands of the already powerful (Galen et al., 2018). Bureaucratically, blockchain is poorly understood by many government stakeholders, making it difficult for a land registry to identify issues that the technology can help to solve. Blockchain is also inherently political, as the technology offers to decentralize and/or democratize both governance and socioeconomic structures. Sufficient political will or public support may not always exist to allow for innovation (Panfil et al., 2019).

Chromaway, a Swedish-based startup is currently working with governments in Sweden and the Indian state of Andhra Pradesh to maintain land titles and legal records of property transactions on a blockchain-based system. In Sweden, new technology simply brings greater efficiencies to already functioning systems. In India, however, storing land titles on a publicly verifiable and immutable blockchain could greatly reduce fraud and corruption because land titles could be traced over time. Ultimately, the goal is to empower citizens to interact directly with the government systems that facilitate societal interactions. This empowerment could be measured in terms of increased economic activity, decreased numbers of court disputes over land, or increased trust between citizens and land authorities (Galen et al., 2018).

2.4. Energy

Globally, only 85% of the world's population has access to electricity, and not necessarily from an affordable, reliable, or clean source (World Bank, 2016). Moreover, the energy sector operates in a highly regulated market, often with significant overhead and energy losses during transmission (Chediak and Wells, 2013). Blockchain is foreseen as an efficient tool of allocating generation assets to a specific point of consumption, and can even be used to establish a hierarchy of priorities when it comes to sources of origin. This allows renewable energy certification processes to be sped up and automated, attributing to the traceability of the technology. The agreements in the certification could ensure that the energy is from 100% green sources, and could encourage large corporations to purchase this type of energy (Galen et al., 2018).

With the pilot project Grid Singularity, the creators have come up with a system wherein energy could be sourced and distributed in a decentralized and efficient way. The platform will be invisible for end-users, but will allow other companies to develop

applications on top of this infrastructure to support, for example, micropayment channels, data analysis, and benchmarking green certificates, smart grid management, and energy trade validation (Galen et al., 2018). The vision is that each household will be able to buy and sell energy through this network. In order for this transition to take place, all stakeholders must first agree on market standards and how the technology will grow (Grid Singularity, 2020).

2.5. Digital Identity

In 2019, the World Bank estimated that over 1 billion people around the world are without any officially recognized ID, of whom half live in Africa (ID4D, 2019). Many of these people come from remote, underserved regions. Using blockchain technology for digital identity solutions holds promise because it can reduce fraud, increase transparency, and increase efficiency. There are still quite a few challenges to adoption, such as conforming the right-to-be-forgotten law, stating the right for people to delete their data, which is simply not possible on a blockchain. One potential solution to this problem is to improve the anonymization of the data so that sensitive data is not publicly viewable (General, 2017).

One of the major threats to human dignity poses itself underneath the new waves of worldwide migration from unstable states and economies. Along with this, the weakening and at times even the loss of personal identity arising from the fading bonds of citizenship is often the result of the circumstances of migration. Blockchain technology has the potential to create new solutions for refugee and identification systems, providing a digital verification mechanism for people unable to prove their identity, and allowing them to share their identity and transact with other actors (Morrow, 2018). In contrast to existing centralized identity databases, blockchain-based solutions allow for user-centric databases that give users complete control over who access their data. With several key advantages such as increased efficiency and transparency, and reduction in cost, blockchain technology surpasses current solutions to delivering a digital identity.

Among the promising pilot projects, there is BanQu – a U.S. based tech company that seeks to solve the problem of the inability of unbanked citizens to interact with the global economy. Through their platform that can run on any cell phone, they are able to record their economic and financial transactions, purchase goods, and prove their existence in global supply chains. This creates an economic passport that enables them to engage

with family members, global corporations, development agencies, government organizations, and global financial institutions. Already being used in six countries by farmers, workers, and micro-businesses in some of the world's poorest regions, their model paves the way to a sustainable form of digital identity (Galen et al., 2018).

The overall assessment of Stanford's 2017 research is that most projects are still in the pilot phase, but several blockchain identities should be gaining strong traction by the end of 2018. Blockchain-based digital identity is a high-impact global scale application, as half of projects documented are expected to impact over one million users (Galen et al., 2018).

2.6. Financial Inclusion

Deeply linked with digital identity is the problem of financial inclusion, with over two billion unbanked people around the world. Financial inclusion refers to the delivery of affordable and usable financial access for unbanked and underbanked people. There are approximately 2 billion individuals who lack financial access, and an additional 1.5 billion individuals who are underserved by the financial service industry. These groups of people have to pay significantly higher opportunity, travel or monetary costs in order to use financial services (Digital Currency Group, 2017).

Blockchain is a viable solution due to its capacity to lessen the settlement time and transaction costs usually incurred with a trusted third-party intermediary. However, a trust leap has yet to be made, since the complexity of the technology makes regulators and incumbents hesitant, along with its lack of formal regulation frameworks. Another issue to its adoption is the fact that its implementation would reduce profit for certain third-party authorities and incumbents, thus rendering it an unprofitable transition with little incentive for those in question (Galen et al., 2018).

An innovative pilot project can be found in the Philippines, called KUSINGph. It is a digital currency platform that focuses on farmers, fisherfolk, out-of-school youth, and Filipinos who do not have access to owning a bank account. Interconnectivity is a challenge in the Philippines, as data shows that almost 45% or 46 million of its citizens do not have access to the Internet. KUSINGph, is a system that uses standardized communication protocols that can enable transactions through a simple exchange of short text messages or SMS, consequently widening its scope of possible users. With the use of

a mobile phone or the Facebook messenger app, anyone is able to set up an account with which they can then transfer and receive funds even across countries.

Despite the many benefits of blockchain, its usage in Financial Inclusion is still in early development. While blockchain transaction speed is superior to available options in the developing world, its current speed is still limited compared to settlements in developed countries. Scalability is thus a challenge, if global implementation is the ultimate goal (Galen et al., 2018).

2.7. Governance and Democracy

When it comes to administrative and bureaucratic processes, one of the banes is the repetitive requesting of an individual's information between agencies or functions. Furthermore, a system relying on a centralized architecture denotes a single point of vulnerability, which is an easy target for hackers or even hostile nation-state actors. Distributed ledger technologies can address many security and even logistical practices of government data exchange, allowing systems to cross-verify if they contain the same information or correspond to the same individual without having to transmit or view the underlying information itself. So-called zero-knowledge proofs offer positive implications for privacy since sensitive data can be verified without being transmitted by agencies, or even without being accessed by a government employee (Galen et al., 2018).

There are certain reservations being held by citizens, particularly on sensitive issues like voting. In addition, many citizens may lack an understanding of digital applications, much more on blockchain systems, or may have difficulty accessing the Internet. The lack of regulations and the large legal ambiguity around blockchain also contributes to the hesitation of governments (Galen et al., 2018). In 2018, the European Union General Data Protection Regulation (GDPR) was created to strengthen privacy and personal data protection in the EU, giving persons more control over their personal data. The mandate on the "Right to be Forgotten", for example, is in direct opposition to blockchain's nature of immutability, thus opening up a crack in the case of compliance that has yet to be filled (De Meijer, 2018).

In making the transition to a blockchain-based e-services ecosystem, some governments are more aptly poised than others. Estonia, for example, has been seeking to provide government services electronically and over the Internet since 2001, issuing e-ID cards and making digital signatures possible for every citizen. By 2012, a fully secured

blockchain system called e-Estonia came online, allowing citizens to track all government-related transactions that use their personal information in an audit log that is accessible through the state portal. Citizen data itself is not stored in the chain, rather, the aggregated ledger of registrations shows that the data exists and was certified by the proper entity. There are now more than 1,000 services available through e-Estonia, relying on the platform Guardtime for ensuring the integrity of the digital registries and repositories. This allows for a constant, true, situational awareness of government and citizen data, and timely detection of any attempts to attack, modify, or otherwise compromise the system (Galen et al., 2018).

An outstanding boost in efficiency has been noted, as e-Estonia cites on its website, saving 844 years of working time every year and a contribution of two percent of the country's GDP. It is rarely necessary now for citizens to go personally to government offices, and as claimed by Guardtime, 99% of citizens do not even need to be familiar with its technology to interact with the system. The success of e-Estonia should not, however, render it a possible solution that can be indiscriminately applied in any environment. Trust in the government, and the citizens' willingness to share data among government agencies, along with the gradual and transparent implementation of new processes have been crucial to the success of the system (Galen et al., 2018).

Chapter 4

SUMMARY, RECOMMENDATIONS AND CONCLUSIONS

The objective of this study is to elucidate the concept of "blockchain trust", and to build the theoretical framework needed to scrutinize the hypothesis that blockchain is indeed a technology that can pervade the world of finance, economics and other sectors as a new architecture of trust. This involved a research of the literature concerning the relationship between trust and blockchain, their definitions, and the implications – both positive and negative – of blockchain trust.

The paper begins with the definition of the types of trust, trustworthiness, and the aspect of vulnerability in a relationship of trust. The Trust Stack model is then discussed, showing the observed pattern in building trust in a new technology or business, comprising three levels: trust in the *idea*, trust in the company or *platform*, and trust in the *other person*. The model is later used throughout the paper as a guide in the process of analyzing blockchain's trustworthiness.

If trust can be built, then it can also be broken. A systemic collapse of trust is presented as a contemporary issue – the economic collapses and betrayals of the past decades seem to have corroded the population's trust in the mainstream institutions of business, government, media and NGOs. Consistent with the phenomenon of trust in strangers, a rise in trust in self-affirmed communities has begun to overshadow that of trust in experts and authorities. Trust is beginning to flow horizontally rather than vertically, and is indicative of a revolutionary trust shift. This is the rise of distributed trust – the foundation on which technologies such as blockchain and distributed ledgers are set.

An overview of the traditional trust architectures is then presented, namely: Peer-to-Peer, Leviathan and Intermediary. Blockchain trust is determined not to fall under any

of these traditional constructs, and instead represents a new kind of architecture wherein nothing is assumed to be trustworthy except the output of the network itself. Then, through an overview of the components of blockchain, the *idea* of blockchain is explained, thus kicking off a theoretical simulation of the Trust Stack process.

Through the four paradoxes described in the third chapter, a deepened understanding of blockchain as a platform and catalyst of trust is attained. Blockchain is found to be a promising technology that is still in its nonage, and that needs balance between its extremes in terms of decentralization, immutability, transparency, and algorithm dependency. The chapter then ends with the already existing applications of blockchain, specifically in the social sector. Here, the potential scope of blockchain technology is expounded, and is found to have use in an impressively wide range of sectors such as agriculture, land rights, energy, digital identity, financial inclusion, and governance, to mention a few.

The eminent limitation of this study is the youth of the blockchain technology itself, with the majority of projects still in their pilot stage. A wide field of study has yet to be explored on the societal impacts of “trustless” trust, on whether or not it is beneficial to social capital – a study that would probably have to employ empirical methods of research on existing and, at the same time, successful case studies. An area of interest in this regard could be that of Decentralized Autonomous Organizations (DAOs), wherein every action and contribution of its participants is rewarded in a purely incentivized system. The effects of such an environment on intrinsic motivation is yet to be discovered under the lens of the self-determination theory, which talks about human development towards a coherent sense of self. Studies have shown that extrinsic motivation with a controlling functional significance, such as a tangible reward, tends to diminish the intrinsic motivation of a person (Ryan & Deci, 2004). A point for future study, therefore, could be on the integration of these external regulations into self-regulation, possibly allowing nevertheless a basis for self-determined behavior even in a company managed by incentives and pure algorithm.

Moreover, in the vision of equal opportunities for all participants, a study on the distribution of wealth in a cryptocurrency network is a topic that could further be explored. Bitcoin and Ethereum holdings, for example, are found to be quite concentrated, yet to what degree is still unclear. Hence, the points of residual centralization in a blockchain could be a subject for future research. Finally, the sub-paradox "auditable yet

unaccountable" discussed in the third chapter could also open up a study of substantial value.

Truthfully, the research question was brought about by the perplexing term, "trustless trust", and the lack of discussion around the term. It should be said that in the itinerary that I have done to study how blockchain works, the first few months consisted mainly of an idealized concept of blockchain, and not much was questioned regarding its infallibility. Delving into the countless articles, papers and courses on its decentralized, highly-efficient, positively disruptive nature was indeed enchanting, yet it required a great deal of research to finally arrive at the point wherein the criticisms of blockchain naysayers started to set in. This study is thus the fruit of confronting both sides of the coin, in the endeavor of treating the analysis with impartiality, in the spirit of curiosity, and in the hopes of contributing to the field of knowledge regarding this nascent technology.

The starting point from which Satoshi Nakamoto created Bitcoin, and consequently blockchain, was the premise that trust is a liability in transactions, and so the need for it should be reduced or eliminated. In his effort of doing so through practically transforming every element in a transaction into algorithm, one important aspect is forgotten. Nakamoto forgets the muddled, chaotic and exceedingly unpredictable element of human behavior present in each transaction, which thus reintroduces the need for trust. No matter the transaction, trust is nevertheless its fuel. It is determined, then, that blockchain is not without trust. It may promote justified confidence, but does not by any means replace the need for trust in the participants of the system, nor in the system itself. Rather than claiming that blockchain eliminates the need for trust, I would say that trust is the emergent property of the network as a whole. In saying so, I agree with Kevin Werbach's (2018) position in saying that it represents a reinvention of trust – one that addresses the needs that arose from the fraying of conventional trust structures.

The term "trustless trust" is thus revealed to be misleading. "Trustless trust", as an expression, conveys a trait of blockchain being inimical to trust, when in fact it is the contrary. Not only does blockchain thrive on trust, it is able to "generate" trust in circumstances where there is none, such as impersonal cases brought about by the scale of a network typically found in collaborative transactions done in a globalized setting. In this digital era, we cannot anymore rely on personalized trust; and institutionalized trust, as we have found, is prone to be conducive to corruption and the abuse of power. The shift

towards distributed trust, therefore, was born out of a dire need for change, and for which blockchain is a viable tool.

Through the course of analysis of the various definitions of trust, it has been determined that "blockchain trust" can be defined as *generalized* trust, since it does not deal with personal relationships; it is a form of *distributed* trust, because the truth is ensured not by a centralized body but through a consensus of all the participants; it has both *affective* and *cognitive* aspects of trust, due to the fact that although human elements were aimed to be replaced by algorithm and mathematics so as to satisfy the risk assessment needs of the cognitive aspect, an affective optimism towards the programmers, miners, entrepreneurs and the experts who establish and maintain cryptographic protocols still remains.

The four main characteristics of blockchain trust – decentralized, immutable, transparent and algorithmic – have been amply discussed and scrutinized. In the course of the research, it struck me as crucial to discover that each characteristic should not be taken as absolute, but that each has degrees as to how it is implemented. The degree of decentralization, for example, seems to weigh heavily on the technology's success, since purists consider this feature to be blockchain's identity – to betray it would be to defeat blockchain's purpose of removing power from the hands of a privileged few. As was expressed in Vili's paradox, the lack of formal governance structures would very much likely be the cause of demise for blockchains, yet in the adoption of these structures, blockchain would no longer become truly decentralized. I, however, would argue that there could be governance structures that could nevertheless promote decentralization – a direct democratic form of governance without the need of a central authority.

Although the tamper-resistance of the blockchain adds to the fortitude of the system, in my opinion it should be open to the right amount of "leniency", for lack of a better term. We have well established the fact the humans cannot be taken out of the equation, hence the systems we build should cater to humans' unpredictability, creativity and volatility. In a sense, there is a need to create a space for forgiveness even in a blockchain because we cannot expect humans not to err. Excessive severity based on unrealistic expectations is much more rampant in a blockchain system than the risk of fraudulent manipulation. Much of the distrust in blockchain comes from the promise of absolute immutability, yet this would call for perfection even from the part of the participants – an unrealistic expectation. It stands to reason that the strength of blockchain

trust lies within its maturity since the length of the chain increases trust in a probabilistic sense. This is therefore beneficial in the aspect of forgiveness because the system continues to retains a version of truth that everyone agrees upon even in the presence of faults and historical gaffes here and there.

Just as legal structures exist to promote trust within a Leviathan trust architecture, the same is true for a Trustless one. The grey area in legal regulations in the digital space is a crucial point to improve on, since the missing link towards widespread use involves security on a regulatory and governance basis. In taking away the veil that protects illicit activities fueled through cryptocurrencies and allowing justice to prevail, the dissipation of governments' reluctance towards the technology could finally take place. The good news is that the policy framework foundation has already been set in motion. To address the challenges raised by Distributed Ledger Technologies and their applications, certain bodies of experts have been created, such as the Global Blockchain Policy Centre. Among the countless blockchain-related events held across the world, the OECD Global Blockchain Policy Forum is the leading international event that provides a unique platform for stakeholders to focus on the policy implications of blockchain and other distributed technologies, compelling governments to consider their policy response, and in some cases, embracing blockchain within their own institutions (OECD, 2019).

In conclusion, the primary hypothesis of this research is answered in a positive sense, yet not in absolute. Yes, blockchain technology could very well launch us into a new architecture of trust, but in a gradual manner. The elements mentioned above can be condensed into a concept similar to that of the People, Process, and Technology (PPT) framework, with each element having equal weight, such as the pegs of a three-legged stool. If one leg is out of balance, the entire stool wobbles. It is thus in the harmony between these elements that blockchain can be pushed into global adoption. Indeed, blockchain technology is young and imperfect. It is possible as well that cryptocurrency, due to its volatile nature, will not become a global revolution. Nevertheless, the trust leap towards blockchain technology is a very important one, because it could either be THE groundbreaking technology that changes the world, or is a step closer towards it.

Blockchain is beyond just a cryptocurrency, and although it will not be our salvation, it will nevertheless be fundamental in reducing frictions. The need for a trustworthy record will always be vital for all kinds of transactions, and blockchain is a huge innovation leap in terms of security, traceability and in recording truth. Indubitably,

the advent of blockchain has accelerated the progress of digital records, and its processes are far more transparent than ever before. The possibility of conducting complex transactions without ceding power to either government authorities or intermediaries, and with little or no transaction cost is within itself a gamechanger. Prudence must be practiced nonetheless, with the knowledge that blockchain is not the solution to all problems and that blockchain may fit better in some domains than in others. An innovation is a novel match between a need and a solution, thus an in-depth deliberation of any case study's requirements should be performed to see if blockchain is the best approach, or if other existing technologies could address the problem just as well.

It is pertinent to mention that although some of the applications of blockchain for social good presented above could be achieved by other technologies, it is difficult to say the same for the case of blockchain as a gateway to a real and self-sovereign digital identity. The relevance of blockchain technology finds a secure place in its irreplaceability, and in this regard, it holds a prime spot. Aside from the billions of individuals who fall under the unbanked and unregistered category, digital identity could benefit any individual taking part of any society. For example, the neutral essence of algorithm, and blockchain's distinctive traceability could prove particularly useful in situations wherein pursued biases could very much alter history, such as in the case of government elections. Contestations of the results of a blockchain-based election would be groundless, if not illogical, in terms of the accuracy of the vote count.

Data is the most powerful asset in this digital age as it is involved in practically every transaction we do on a daily basis, in what we purchase, what we do online, and in interactions with society in general. However, any regular user of the internet today is limited in terms of control over one's information being stored online, since platforms such as Google or Facebook have monopolized this task. The best most of us can do at the moment is to strive to be aware of which personal data is being used. Awareness, however is, not ownership. This still entails having to agree to terms and conditions that we do not fully understand, and handing over information that intermediaries can then use for their own interests. Blockchain is by far the most applicable solution towards owning our digital identities, promoting privacy, and having complete knowledge and control over which personal data is exposed in each transaction.

Finally, after much deliberation, I have come to believe that blockchain's immaturity should not be taken against it. Just like in the analogy made by Rachel Botsman (2017) on the early days of the automobile: it took decades to create norms like traffic lights, stop signs and pedestrian lanes. Similarly, the balance between People, Process and Technology within blockchain will have to be tried and tested through years and maybe even decades of collective experience and interdisciplinary research. This does not mean that we can begin to trust blockchain only when this balance is reached. Thankfully, trust does not have to hinge on a promise of perfection. Rather, a confident relationship with blockchain's unknowns is possible even today, knowing that trust and vulnerability are in continuous interplay – two sides of the same coin.

BIBLIOGRAPHY

Antonopoulos, A. M. (2015). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies.* Sebastopol, CA: O'Reilly

Arrow, K. (1972). *Gifts and exchanges.* Philosophy and Public Affairs

Arun, J. S., Cuomo, G., Gaur, N. (2019). *Blockchain for Business.* Addison Wesley Professional. Retrieved July 17, 2020, from https://www.slideshare.net/EdelmanInsights/2016-edelman-trust-barometer-global-results.

Baier, A. (1986). Trust and Antitrust. *Ethics*, *96*(2), 231-260. Retrieved January 2, 2021, from http://www.jstor.org/stable/2381376

Bambrough, B., (2020, August 28). *China Is 'No Threat To Bitcoin,' Promises Foundry CEO After $100 Million Bitcoin Mining Bet.* Forbes. Retrieved July 31, 2020 fromhttps://www.forbes.com/sites/billybambrough/2020/08/28/china-is-no-threat-to-bitcoin-promises-foundry-ceo-after-100-million-bitcoin-mining-bet/?sh=3b65a61d6066

Baraniuk, C. (2019, July 3). *Bitcoin's energy consumption 'equals that of Switzerland'.* BBC News. Retrieved August 13, 2020, from https://www.bbc.com/news/technology-48853230#:~:text=Currently%2C%20the%20tool%20estimates%20that,same%20power%20consumption%20as%20Switzerland.

Barmes, I., Bosch, B. (2019, December 12). *Quantum computers and the Bitcoin blockchain: An analysis of the impact quantum computers might have on the Bitcoin blockchain.* Deloitte Nederland. Retrieved October 10, 2020, from https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html

Barmes, I., Czaszyński, B., Schellekens, R. (2019). *Quantum computers and their impact on Cyber Security: Threats and opportunities in the new realm of computation.* Deloitte Nederland. https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-their-impact-on-cyber-security.html

Bekemysheva, A., (2018, May 7). *Making Effective Use of Smart Contracts*. Steel Kiwi. Retrieved March 23, 2020, from https://steelkiwi.com/blog/making-effective-use-of-smart-contracts/

Berg, A., Berg, C., Davidson, S., Potts, J. (2018). *The Institutional Economics of Identity.* http://dx.doi.org/10.2139/ssrn.3072823

Binance Academy (2020). *Byzantine Fault Tolerance Explained.* Binance Academy. Retrieved May 12, 2020, from https://academy.binance.com/en/articles/byzantine-fault-tolerance-explained

Binance Academy (2020). *What is a 51% Attack?* Binance Academy. Retrieved July 1, 2020, from https://academy.binance.com/en/articles/what-is-a-51-percent-attack

Binance Academy. (2020). *What is a Blockchain Consensus Algorithm?* Binance Academy. https://academy.binance.com/en/articles/what-is-a-blockchain-consensus-algorithm

Bitcoin (2013, March 11). *11/12 March 2013 Chain Fork Information.* Bitcoin. Retrieved July 14, 2020, from https://bitcoin.org/en/alert/2013-03-11-chain-fork

Blair, M., Stout, L., Library, C. (2018). *Trust, Trustworthiness, and the Behavioral Foundations of Corporate Law.* Center for Open Science. Retrieved December 28, 2020, from https://ideas.repec.org/p/osf/lawarx/swx6r.html

Botsman, R. (2017). Who Can You Trust? How Technology is Rewriting the Rules of Human Relationships. PublicAffairs.

Burniske, C., Tatar, J. (2018). Cryptoassets: The innovative investor's guide to bitcoin and beyond. New York, McGrawHill.

Buterin, V. (2013). *Ethereum Whitepaper.* Ethereum. Retrieved March 12, 2020, from https://ethereum.org/en/whitepaper/

Buterin, V. (2015). *The Subjectivity/Exploitability Tradeoff.* Ethereum Blog. https://blog.ethereum.org/2015/02/14/subjectivity-exploitability-tradeoff/

Buterin, V. (2017). *The Meaning of Decentralization.* Medium. Retrieved June 20, 2020, from https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

CertiK (2019, October 4). *The Blockchain Trilemma: Decentralized, Scalable, and Secure?* Medium. Retrieved June 29, 2020, from https://medium.com/certik/the-blockchain-trilemma-decentralized-scalable-and-secure-e9d8c41a87b3

Chediak, M., Wells, K., (2013, August 13). *Why the U.S. Power Grid's Days Are Numbered*. Retrieved September 4, 2020, from https://www.bloomberg.com/news/articles/2013-08-22/why-the-u-dot-s-dot-power-grids-days-are-numbered

Cheshire, C. (2011). *Online Trust, Trustworthiness, or Assurance.* American Academy of Arts & Sciences. DOI: 10.1162/DAED_a_00114

Clark, D. (2005, April 15). *Interoperation, Open Interfaces, and Protocol Architecture.* Massachusetts Institute of Technology. Retrieved December 9, 2020, from http://web.archive.org/web/20050415042854/http:/www.csd.uch.gr/~hy490-05/lectures/Clark_interoperation.htm

Clarke, G. (2019, January 9). *After Ethereum Classic Suffers 51% Hack, Experts Consider - Will Bitcoin Be Next?* Forbes. Retrieved April 7, 2020, from https://www.forbes.com/sites/ginaclarke/2019/01/09/after-ethereum-classic-suffers-51-hack-experts-consider-will-bitcoin-be-next/?sh=34ab7ea3a56b

Coding Tech. (2018, February 7). *Blockchain Technology Explained.* [Video]. YouTube. Retrieved July 2, 2020, from https://youtu.be/qOVAbKKSH10

Cook, J. (2018, November 11). *What is proof-of-work?* John D. Cook Consulting. Retrieved February 4, 2021, from https://www.johndcook.com/blog/2018/11/11/proof-of-work/

Cross, F. (2005). *Law and Trust*. McCombs School of Business. Retrieved August 6, 2020, from http://ssrn.com/abstract=813028

Crypto51 (n.d.). *PoW 51% Attack Cost*. Crypto51. Retrieved November 13, 2020, from https://www.crypto51.app/

Cryptoeconomics. (2017, September 27). *The Blockchain Economy: A Beginner's Guide to Institutional Cryptoeconomics.* Medium. Retrieved November 24, 2020, from https://medium.com/cryptoeconomics-australia/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2f2beec4

De Meijer, C. (2018, October 9). *Blockchain versus GDPR and who should adjust most.* Finextra. Retrieved April 3, 2020, from https://www.finextra.com/blogposting/16102/blockchain-versus-gdpr-and-who-should-adjust-most#:~:text=For%20blockchain%20the%20most%20controversial,are%20designed%20to%20last%20forever.

De Ponteves, H., Eremenko, K., SuperDataScience Team. (2020). *Blockchain A-Z: Learn How to Build Your First Blockchain.* [Video]. Udemy.

Deloitte (2017). *Evolution of blockchain technology: Insights from the GitHub platform.* Deloitte. Retrieved April 5, 2020, from https://www2.deloitte.com/content/dam/insights/us/articles/3255_3D-opportunity_blockchain/DUP_3D-opportunity_blockchain.pdf

Demestichas, K., Peppes, N., Alexakis, T., Adamopoulou, E. (2020). *Blockchain in Agriculture Traceability Systems: A Review.* Applied Sciences. DOI: 10.3390/app10124113

Destefanis, G., Bracciali, A., Ma, M. (2018*). Smart Contracts Vulnerabilities: A Call for Blockchain Software Engineering?* Campobasso, Italy: IEEE 19 IWBOSE 2018.

Deutsch, M. (1973). *The Resolution of Conflict.* Yale University.

Digital Currency Group, Chamber of Digital Commerce (2017, March). *Blockchain and Financial Inclusion: The role blockchain technology can play in accelerating financial inclusion.* Georgetown University, McDonough School of Business. Retrieved May 25, 2020, from https://digitalchamber.org/assets/blockchain-and-financial-inclusion.pdf

edChain (2018, June 12). *POW vs. PoS: a comparison of two blockchain consensus algorithms.* Medium. Retrieved July 31, 2020, from https://medium.com/@EdChain/pow-vs-pos-a-comparison-of-two-blockchain-consensus-algorithms-f3effdae55f5

Edelman (2016). *2016 Edelman Trust Barometer - Global Results.* Edelman. Retrieved December 14, 2020, from https://www.slideshare.net/EdelmanInsights/2016-edelman-trust-barometer-global-results

Edelman (2016). *Beyond the Grand Illusion.* Edelman. Retrieved March 12, 2020, from http://www.edelman.com/p/6-a-m/beyond-grand-illusion/

Edelman (2019, January 20). *2019 Edelman Trust Barometer.* Edelman. Retrieved March 21, 2020, from https://www.edelman.com/trust/2019-trust-barometer

Edelman (2020, January 19). *2020 Edelman Trust Barometer.* Edelman. https://www.edelman.com/trust/2020-trust-barometer

Edelman, R. (2017). *2017 Edelman Trust Barometer: Executive Summary.* Edelman. Retrieved April 29, 2020, from https://www.edelman.com/post/an-implosion-of-trust

Edmonds, E. (2016, March 1). Three-Quarters of Americans “Afraid” to Ride in a Self-Driving Vehicle. AAA Newsroom.

Farmer, B. (2020, April 21). *'We must not turn back the clock': WHO warns malaria deaths might reach 769,000 due to coronavirus.* The Telegraph. Retrieved August 13, 2020, from https://www.telegraph.co.uk/global-health/science-and-disease/must-not-turn-back-clock-warns-malaria-deaths-might-reach-700000/

Fintech Futures (29 October 2019). *Cryptocurrencies and the critical vulnerability of a 51% attack. Fintech Futures.* Retrieved November 8, 2020, from https://www.fintechfutures.com/2019/10/cryptocurrencies-and-the-critical-vulnerability-of-a-51-attack/#:~:text=In%20January%20this%20year%2C%20one,time%2C%20likely%20only%20get%20worse.

Frankenfield, J. (2019, May 6). *51% Attack.* Investopedia. Retrieved April 4, 2020, from https://www.investopedia.com/terms/1/51-attack.asp

Frankenfield, J. (2020, November 3). *Initial Coin Offering.* Investopedia. https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp

Frischmann, B. (2013). *Infrastructure: The Social Value of Shared Resources.* Oxford: Oxford University Press.

Fukuyama, F. (1996). Trust: Human Nature and the Reconstitution of Social Order. Free Press.

Furlonger, D., Kandaswamy, R., (2018, March 7). *Blockchain Status 2018: Market Adoption Reality*. Gartner Research. Retrieved May 17, 2020, from https://www.gartner.com/en/documents/3869693

Galen, D., Brand, N., Boucherie, L., Davis, R., Do, N., El-Baz, B., Kimura, I., Wharton, K., Lee, J. (2018). *Blockchain for Social Impact: Moving Beyond the Hype.* Graduate School of Stanford Business, Center for Social Innovation.

General (2017, October 29). *Reconciling Blockchain and Data Protection.* Camilleri Preziosi Advocates.

Gillette, C. (2015, September 1). *The Psychology of Trust in Marketing: How to Earn It and How to Keep It.* Salesforce. Retrieved June 6, 2020, from https://www.salesforce.com/ca/blog/2015/08/psychology-of-trust-in-marketing.html

Goldstein, E. (2011). Cognitive psychology: Connecting mind, research, and everyday experience (3rd ed.). Wadsworth Cengage Learning.

Good Finance (2018). *Social impact. What is it? How do I measure it?* Good Finance. Retrieved July 30, 2020, from https://www.goodfinance.org.uk/latest/post/blog/social-impact-what-it-how-do-i-measure-it

GRGB Law (2016). "More than 90 Percent of Automobile Accidents Caused by Human Error". GRGB Law.

Grid Singularity (2020). Energy Singularity Challenge 2020: Testing Novel Grid Fee Models and Intelligent Peer-to-Peer Trading Strategies. Medium. Retrieved May 2, 2020, from https://gridsingularity.medium.com/

Hardin, R. (2002). *Trust and Trustworthiness*. Russell Sage Foundation.

Hayes, A. (2020, August 24). *What Happens to Bitcoin After All 21 Million Are Mined?* Investopedia. Retrieved October 7, 2020, from https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/#:~:text=Bitcoin%20also%20has%20a%20stipulation,one%20block%20every%20ten%20minutes.

Hayes, C. (2013). Twilight of the Elites: America after Meritocracy. Broadway Books.

Henten, A., Windekilde, I. (2020). *Blockchains and Transaction Costs.* CMI, Department of Electronic Systems, Aalborg University.

Hobbes, T. (1651). Leviathan or the Matter, Forme, & Power of a Common-wealth Ecclesiastical and Civill. Cambridge: Cambridge University Press.

Hoffman, R. (2015, May 15). *Reid Hoffman: Why the blockchain matters.* Wired. Retrieved October 20, 2020, from https://www.wired.co.uk/article/bitcoin-reid-hoffman

Hosmer, L. T. (1995). *Trust: The Connecting Link Between Organizational Theory and Philosophical Ethics.* In Academy of Management Review (Vol. 20, Issue 2, pp. 379–403). https://doi.org/10.5465/amr.1995.9507312923

Hurwitz, J. (2013). *Trust and Online Interaction, 161 U. PA. L. Rev. 1579.* Penn Law, University of Pennsylvania Carey Law School, Legal Scholarship Repository.

Iberdrola (2020, April 13). *Quantum computing and supercomputers will revolutionise technology.* Iberdrola. Retrieved October 28, 2020, from https://www.iberdrola.com/innovation/what-is-quantum-computing

ID4D Identification for Development (2019). *2019 Annual Report.* World Bank Group.

Jerry (2020, November 25). *Real Estate Tokenization – How Blockchain Technology Could Revamp and Streamline an Entire Industry*. The Blockbox. Retrieved December 22, 2020, from https://theblockbox.io/blog/real-estate-tokenization-how-blockchain-technology-could-revamp-and-streamline-an-entire-industry/

Jones, J. (2002). On the concept of trust. *Decision Support Systems 33*(3), 225-232, https://doi.org/10.1016/S0167-9236(02)00013-1

Jones, K. (1996). *Trust as an Affective Attitude.* Ethics, 107(1), 4-25. Retrieved January 2, 2021, from http://www.jstor.org/stable/2382241

Kethineni, S., Cao, Y. & Dodge, C. (2018). Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. *Am J Crim Just 43,* 141–157. https://doi.org/10.1007/s12103-017-9394-6

Kharif, O. (2017). *1000 People Own 40% of the Bitcoin Market.* Bloomberg Businessweek. Retrieved April 17, 2020, from https://www.bloomberg.com/news/articles/2017-12-08/the-bitcoin-whales-1-000-people-who-own-40-percent-of-the-market

Kharif, O. (2019, July 1). *Bitcoin Criminals Set to Spend $1 Billion on Dark Web This Year.* Bloomberg. https://www.bloomberg.com/news/articles/2019-07-01/bitcoin-criminals-set-to-spend-1-billion-on-dark-web-this-year

Korin, N. (2020, November 20). *Using blockchain to monitor the COVID-19 vaccine supply chain.* World Economic Forum. Retrieved July 30, 2020, from https://www.weforum.org/agenda/2020/11/using-blockchain-to-monitor-covid-19-vaccine-supply-chain/

Kriticos, S., (2019, March 29). *Keeping it clean: Can blockchain change the nature of land registry in developing countries?* World Bank Blogs. Retrieved August 3, 2020, from https://blogs.worldbank.org/developmenttalk/keeping-it-clean-can-blockchain-change-nature-land-registry-developing-countries

Kumar, A., & Rosenbach, E. (2019, September). The Truth about the Dark Web. International Monetary Fund. *Finance & Development, 56*(3), 22-25. https://www.imf.org/external/pubs/ft/fandd/2019/09/the-truth-about-the-dark-web-kumar.htm

Lathrop, B., "After an average of 20 minutes" and subsequent quotes from Brian Lathrop, Interview by Rachel Botsman, 2016, August 16. *Who Can You Trust? How Technology is Rewriting the Rules of Human Relationships.* PublicAffairs.

Laurence, T. (2019). *Blockchain For Dummies.* John Wiley & Sons.

Laurent, P., Chollet, T., Burke, M., Seers, T. (2018, November 19). *The tokenization of assets is disrupting the financial industry. Are you ready?* Inside Magazine, 1(19), Part 02. Retrieved October 14, 2020, from https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/lu-tokenization-of-assets-disrupting-financial-industry.pdf

Ledger Academy (2019, October 23). *What Are Public Keys and Private Keys?* Ledger Academy. Retrieved December 19, 2020, from https://www.ledger.com/academy/blockchain/what-are-public-keys-and-private-keys

Levine, A. (Host), Antonopoulos, A., Murphy, S., Mohan, J. (2020, September 27). The 51% Attack Nightmare Scenario (Isn't That Bad). [Audio podcast episode]. *Speaking of Bitcoin.* Coindesk. Retrieved May 5, 2020, from https://www.coindesk.com/51-percent-attack-explained-podcast

Li, X., Hess, T.J., Valacich, J.S. (2006) Using attitude and social influence to develop an extended trust model for information systems. *Database for Advances in Information Systems 37*(2-3), 108-124. https://doi.org/10.1145/1161345.1161359

Luhman, N. (1979). *Trust and power: Two works.* Chichester: Wiley.

Magento (2017, June 14). *What is Ethereum Gas?* Firebear Studio. Retrieved June 8, 2020, from https://firebearstudio.com/blog/ethereum-gas.html

Marcella, A.J. (1999). *Establishing Trust in Vertical Markets.* The Institute of Internal Auditors, Altamonte Springs, FL.

Marr, B. (2017, July 4). *What Is Quantum Computing? A Super-Easy Explanation for Anyone.* Forbes. Retrieved August 2, 2020, from https://www.forbes.com/sites/bernardmarr/2017/07/04/what-is-quantum-computing-a-super-easy-explanation-for-anyone/?sh=54009e6c1d3b

Marshall, M. (2018, October). *The rise of distributed trust.* Global Intelligence for Digital Leaders. Retrieved September 8, 2020, from https://www.i-cio.com/big-thinkers/rachel-botsman/item/the-rise-of-distributed-trust#:~:text=As%20its%20name%20suggests%2C%20distributed,and%20platforms%2C%E2%80%9D%20Botsman%20says.

Massessi, D. (2018, December 12). *Public Vs Private Blockchain In A Nutshell.* Medium. Retrieved September 14, 2020, from https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f#:~:text=Public%20blockchains%20are%20decentralised%2C%20no,Blockchain%20is%20a%20permissioned%20blockchain.&text=The%20open%20versus%20closed%20brings,able%20to%20read%20that%20data.

Maurer, B., Taylor., Nelms, T., Swarts, L. (2013, April 1). *"When perhaps the real problem is money itself!": the practical materiality of Bitcoin*. Social Semiotics, 23(2), 261-277, DOI: 10.1080/10350330.2013.777594

Mayer, R., Davis, J., Schoorman, D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review, 20*(3), 709-734. http://www.jstor.org/stable/258792

McGrath, J. (2018, December 7). *What could smart contracts do for business?* Raconteur. Retrieved May 27, 2020, from https://www.raconteur.net/technology/blockchain/smart-contracts-blockchain/

Mihm, S. (2013, November 18). *Are bitcoins the criminal's best friend?* Bloomberg view. Retrieved June 19, 2020, from https://www.bloomberg.com/opinion/articles/2013-11-18/are-bitcoins-the-criminal-s-best-friend-

Moore, G. (2006). Crossing the Chasm: Marketing and Selling High-Tech Products to Mainstream Customers. HarperCollins.

Morrow, M. (2018). The Promise of Blockchain and Safe Identity Storage for Refugees. UNHCR The UN Refugee Agency.

Mounteney, J., Oteo, A. and Griffiths, P. (2016). 'The internet and drug markets: shining a light on these complex and dynamic systems': The internet and drug markets (European Monitoring Centre for Drugs and Drug Addiction: Insights 21). Publications Office of the European Union, Luxembourg.

Muris, T. (1981). *Opportunistic Behavior and the Law of Contracts.* Minnesota Law Review. Retrieved June 20, 2020, from https://scholarship.law.umn.edu/mlr/2443/

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin. Available at: Retrieved August 19, 2020, from https://bitcoin.org/bitcoin.pdf

Nandwani, K. (2019). *Squaring the Blockchain Circle.* The Browser, India. ISBN: 978-93-88150-01-9

Narayanan, A., Bonneau, J., Felten, E., Miller, A., Golfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.* Princeton University Press.

Nascimento, S., Polvora, A., Anderberg, A., Andonova E., Bellia M., Calès, L., Inamorato dos Santos, A., Kounelis, I., Nai Fovino, I., Petracco Giudici, M., Papanagiotou, E., Sobolewski, M., Rossetti, F., Spirito, L. (2019). *Blockchain Now and Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies.* Publications Office of the European Union.

NeonVest, Viswanathan, S., Shah, A. (2018, October 20). *The Scalability Trilemma in Blockchain.* Medium. Retrieved May 11, 2020, from https://medium.com/@aakash_13214/the-scalability-trilemma-in-blockchain-75fb57f646df

Newcomb, D. (2012). *You won't need a driver's license by 2040.* WIRED. Retrieved June 1, 2020, from https://www.wired.com/2012/09/ieee-autonomous-2040/

Nielsen (2015). *Global trust in advertising.* Nielsen. https://www.nielsen.com/wp-content/uploads/sites/3/2019/04/global-trust-in-advertising-report-sept-2015-1.pdf

North, D. (1990). Institutions, Institutional Change, and Economic Performance. Cambridge: Cambridge University Press.

O'Neill, O. (2002). *A Question of Trust.* Reith Lectures. BBC Radio 4. Retrieved June 18, 2020, from http://www.bbc.co.uk/radio4/reith2002/

OECD (2019). The Policy Environment for Blockchain Innovation and Adoption: 2019 OECD Global Blockchain Policy Forum Summary Report. OECD Blockchain Policy Series.

OECD (2016). *OECD Science, Technology and Innovation.* Paris, OECD Publishing. http://dx.doi.org/10.1787/sti_in_outlook-2016-6-en

Orcutt, M. (2018). *States that are passing laws to govern 'smart contracts' have no idea what they're doing.* MIT Technology Review. Retrieved August 2, 2020, from https://www.technologyreview.com/s/610718/states-that-are-passing-laws-to-govern-smartcontracts-have-no-idea-what-theyre-doing/

Orcutt, M. (2019, February 19). *Once hailed as unhackable, blockchains are now getting hacked.* MIT Technology Review. Retrieved October 2, 2020, from https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

Ostrom, E. (1990). *Governing the Commons: The Evolution of Institutions for Collective Action.* Cambridge: Cambridge University Press.

Panfil, Y., Mellon, C., Robustelli, Fella, T. (2019, June 12). *PropRightsTech Primers: How New and Emerging Technologies Can be Harnessed for Property Rights.* New America. Retrieved August 29, 2020, from https://d1y8sb8igg2f8e.cloudfront.net/documents/Primer-Blockchain_and_Property_Rights.pdf

Pelligra, V., (2013), Trust, in Bruni, L., Zamagni, S. (Eds.), *Handbook on the Economics of Philanthropy, Reciprocity and Social Enterprise*, Cheltenham, Edward Elgar, pp. 415-420

Perez, S. (2017, December 8). *Does a Blockchain Need a Token?* Medium. Retrieved September 5, 2020, from https://medium.com/swlh/does-a-blockchain-need-a-token-66c894d566fb#:~:text=Yes%2C%20a%20bitcoin%20is%20indeed,of%20blockchain%20or%20distributed%20ledger.

Philip (2020, November 25). *How Blockchain is Disrupting Major Industries Across the Globe.* The Blockbox. Retrieved September 30, 2020, from https://theblockbox.io/blog/blockchain-disrupting-major-industries/

Prasanna (2019, July 17). *Blockchain Trilemma: Explained*. CryptoTicker. Retrieved October 18, 2020, from https://cryptoticker.io/en/blockchain-trilemma-explained/

Putnam, R. (2000). Bowling Alone: The Collapse and Revival of American Community. Simon & Schuster.

Reiff, N. (2020). *What is the DarkNet?* Investopedia. Retrieved December 21, 2020, from https://www.investopedia.com/insights/what-dark-net/

ricc (2020, February 28). *Examining the Blockchain Trilemma*. Hackernoon. Retrieved June 2, 2020, from https://hackernoon.com/examining-the-blockchain-trilemma-from-algorands-prism-2kcb32qd

Rose, C. (1995). *Trust in the Mirror of Betrayal*. Yale Law School. Retrieved February 4, 2021 from https://digitalcommons.law.yale.edu/fss_papers/1811/

Rousseau, D., Sitkin, S., Burt, R., Camerer, C. (1998). *Not so Different after All: A Cross-Discipline View of Trust.* Academy of Management Review 23, no.3: 393-404

Ryan, R.M., & Deci, E.L. (2004). *Handbook of Self-determination Research.* University Rochester Press.

Sandner, P. (2017, June 25). *Comparison of Ethereum, Hyperledger, Fabric and Corda*. Medium. Retrieved June 20, 2020, from https://philippsandner.medium.com/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6

Sapienza, P., Zingales, L. (2011). *Trust and Finance.* NBER Reporter Online, National Bureau of Economic Research. Available at: Retrieved September 14, 2020, from http://www.nber.org/reporter/2011number2/paola@luigi.html

Schneier, B. (2019, February 6). *There's No Good Reason to Trust Blockchain Technology*. Wired. Retrieved November 11, 2020, from https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/

Scott, M. (2017, June 27). *Google Fined Record $2.7 Billion in E.U. Antitrust Ruling.* The New York Times. Retrieved November 17, 2020, from https://www.nytimes.com/2017/06/27/technology/eu-google-fine.html

SelfKey (2019, November 15). *What is a Merkle Tree and How Does it Affect Blockchain Technology?* SelfKey Blog. https://selfkey.org/what-is-a-merkle-tree-and-how-does-it-affect-blockchain-technology/

Siegel, D. (2016, June 25). *Understanding The DAO Attack.* Coindesk. Retrieved May 4, 2020, from https://www.coindesk.com/understanding-dao-hack-journalists

Solomon, R. C., & Flores, F. (2001). *Building trust in business, politics, relationships, and life.* New York: Oxford University Press.

Srivastav, K., (2019, March 29). *A Guide to Blockchain Immutability and Challenges.* DZone. https://dzone.com/articles/a-guide-to-blockchain-immutability-and-chief-chall#:~:text=Immutability%20can%20be%20defined%20as,principle%20or%20a%20hash%20value.

Stoll, C., Klaaßen, L., Gallersdorfer, U. (2019). *The Carbon Footprint of Bitcoin.* Joule. Retrieved July 5, 2020, from https://www.cell.com/action/showPdf?pii=S2542-4351%2819%2930255-7

Studnev, A. (2020, August 8*). Ethereum Classic Attack, 8 August: Catch me if you can.* Bitquery. https://bitquery.io/blog/ethereum-classic-attack-8-august-catch-me-if-you-can

Szabo, N. (1994). *Smart Contracts.* Retrieved April 17, 2020, from https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

Tel, G. (2008). *Cryptographic in Context.* Retrieved from Retrieved July 28, 2020, from https://webspace.science.uu.nl/~tel00101/liter/Books/CrypCont.pdf

The Bridge (2020, January 23). *Proof-of-Stake: Have skin in the game.* SEBA Bank. Retrieved August 2, 2020, from https://www.seba.swiss/research/Proof-of-Stake-have-skin-in-the-game

The Bridge (2020, October 29). *The Blockchain Trilemma.* SEBA Bank. Retrieved November 12, 2020, from https://www.seba.swiss/research/the-blockchain-trilemma

The Bridge (2020, September 24). *Are blockchains that safe? How to attack and prevent attacks.* SEBA Bank. Retrieved December 9, 2020, from https://www.seba.swiss/research/are-blockchains-safe-how-to-attack-them-and-prevent-attacks

The Local (2020, October 6). *Immuni: Here's what you need to know about using Italy's contact-tracing app*. The Local. Retrieved August 31, 2020, from https://www.thelocal.it/20201006/immuni-heres-what-you-need-to-know-about-using-italys-contact-tracing-app

Thrun, S., (2017, March 4). *Google's driverless car.* [Video file]. Retrieved September 12, 2020, from https://www.ted.com/talks/sebastian_thrun_google_s_driverless_car/up-next

Tyler, T. (2001). Trust and Law Abidingness: A Proactive Model of Social Regulation. Yale University.

United Nations (2015). *Paris Agreement.* United Nations. Retrieved September 26, 2020, from https://unfccc.int/files/essential_background/convention/application/pdf/english_paris_agreement.pdf

Voshmgir, S. (2020). *Tokenized Networks: What is a DAO?* Blockchainhub Berlin Retrieved October 29, 2020, from https://blockchainhub.net/dao-decentralized-autonomous-organization/

Wang, Y., & Emurian, H. (2005). An overview of online trust: concepts, elements and implications. *Computers in Human Behavior 21,* 105-125. doi:10.1016/j.chb.2003.11.008

Werbach, K. (1997, March). *Digital Tornado: The Internet and Telecommunications Policy. OPP Working Paper Series 29.* Office of Plans and Policy Federal Communications Commission. Retrieved December 12, 2020, from https://transition.fcc.gov/Bureaus/OPP/working_papers/oppwp29.pdf

Werbach, K. (2018). *The Blockchain and the New Architecture of Trust.* The MIT Press. https://doi.org/10.7551/mitpress/11449.001.0001

Wicks, A., Berman, S., & Jones, T. (1999). The Structure of Optimal Trust: Moral and Strategic Implications. *The Academy of Management Review, 24*(1), 99-116. Retrieved February 8, 2021, from http://www.jstor.org/stable/259039

Williamson, O. (1993). *Trust, and Economic Organization.* The University of Chicago Press. Retrieved July 12, 2020, from http://www.jstor.org/stable/725485?origin=JSTOR-pdf

World Bank (2016). *Access to electricity (% of population)*. The World Bank. https://data.worldbank.org/indicator/EG.ELC.ACCS.ZS

World Bank (2016, February 25). *A Year in the Lives of Smallholder Farmers.* The World Bank. Retrieved August 19, 2020, from https://www.worldbank.org/en/news/feature/2016/02/25/a-year-in-the-lives-of-smallholder-farming-families

World Bank (2017, March 24). *Why Secure Land Rights Matter*. The World Bank. Retrieved September 4, 2020, from https://www.worldbank.org/en/news/feature/2017/03/24/why-secure-land-rights-matter

World Bank (2020, April 22). *World Bank Predicts Sharpest Decline of Remittances in Recent History.* The $39 billion figure is based on the World Bank's statistic that fees average around 7 percent. The World Bank. Retrieved September 13, 2020, from https://www.worldbank.org/en/news/press-release/2020/04/22/world-bank-predicts-sharpest-decline-of-remittances-in-recent-history

World Health Organization (2015). *Estimating the burden of foodborne diseases.* Word Health Organization. Retrieved November 20, 2020, from https://www.who.int/activities/estimating-the-burden-of-foodborne-diseases#:~:text=Each%20year%20worldwide%2C%20unsafe%20food,number%20is%20likely%20an%20underestimation.

Zetzsche, D., Buckley, R., Arner, D. (2017). *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*. SRRN Electronic Journal. 10.2139/ssrn.3018214.

LIST OF FIGURE REFERENCES

Figure 1: Marina Abramović and ULAY (1980). *Rest Energy*. [Photograph]. Marina Abramović: The Artist Is Present. https://www.moma.org/audio/playlist/243/3120

Figure 2: Botsman, R. (2017). *Trust Leaps*. [Graph]. Who Can You Trust? How Technology is Rewriting the Rules of Human Relationships. PublicAffairs.

Figure 3: Werbach, K. (2018). *Established Trust Architectures*. [Graph]. The Blockchain and the New Architecture of Trust. The MIT Press. https://doi.org/10.7551/mitpress/11449.001.0001

Figure 4: Werbach, K. (2018). *Trustless Trust Architecture.* [Graph]. The Blockchain and the New Architecture of Trust. The MIT Press. https://doi.org/10.7551/mitpress/11449.001.0001

Figure 5: Chen, Y., Chou, Y., Chou, Y., (2019*). The architecture of Merkle tree in the blockchain*. [Graph]. An Image Authentication Scheme Using Merkle Tree Mechanisms. Future Internet. DOI: 10.3390/fi11070149

Figure 6: Buterin, V. (2017). *Types of networks*. The Meaning of Decentralization. Medium. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

Figure 7: Nascimento, S., Polvora, A., Anderberg, A., Andonova E., Bellia M., Calès, L., Inamorato dos Santos, A., Kounelis, I., Nai Fovino, I., Petracco Giudici, M., Papanagiotou, E., Sobolewski, M., Rossetti, F., Spirito, L. (2019). *How a blockchain works*. [Graph]. Blockchain Now and Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies. Publications Office of the European Union.

Figure 8. Sectigo (2020, June 9). *How Blockchain Cryptography Works*. [Graph]. Public Keys and Private Keys in Public Key Cryptography. Sectigo. https://sectigo.com/resource-library/public-key-vs-private-key

Figure 9. The Bridge (2020, October 29). *The Blockchain Trilemma*. [Graph]. The Blockchain Trilemma. SEBA Bank. https://www.seba.swiss/research/the-blockchain-trilemma

Figure 10. Next Generation Internet (2019, September 12). *Current sectors using blockchain in Europe*. [Graph]. Next Generation Internet: The Internet of Humans. European Union. https://www.ngi.eu/wp-content/uploads/sites/48/2019/09/NGI-Brochure_A5_HR_FinalPrinted.pdf?fbclid=IwAR29_j4tvFC3ePHcVl_miqFsOFUzi8soGkHguwnL-aMeFtxLZRCxUV24di8

Figure 11. Maddrey, N. (2018, September 18). *Blockchain forks*. [Graph]. Blockchain Forks Explained. Digital Asset Research.