KONRAD ADENAUER STIFTUNG

Blockchain Contributions for the Climate Finance

Introducing a Debate

FGV | INTERNATIONAL INTELLIGENCE UNIT

Imprint

Authors

Leonardo Paz Neves

Gabriel Aleixo Prata

Publisher

Dr. Christian Hübner

Konrad-Adenauer-Stiftung e.V

Regional Programme Energy Security and Climate Change in Latin America (EKLA)

Design

Presto Design

FGV | INTERNATIONAL INTELLIGENCE UNIT

Director of FGV IIU

Renato Galvão Flôres Junior

International Intelligence Analyst of FGV IIU

Leonardo Paz Neves

FUNDAÇÃO GETULIO VARGAS

International Intelligence Unit

210 Praia de Botafogo – 12th floor
Rio de Janeiro
Brazil

KONRAD ADENAUER STIFTUNG

Head of EKLA - KAS

Dr. Christian Hübner

Project Manager of EKLA - KAS

Karina Marzano Franco

KONRAD-ADENAUER-STIFTUNG

Regional Programme Energy Security and Climate Change in Latin America (EKLA)

Calle Cantuarias 160 Of. 202
Miraflores, Lima 18 - Perú
Phone +51 13 20 28 70
Energie-Klima-La@kas.de

Report

Blockchain Contributions for the Climate Finance

Introducing a Debate

September, 2018

Realized by:

FGV | INTERNATIONAL INTELLIGENCE UNIT

Supported by:

KONRAD ADENAUER STIFTUNG

Bibliography Chart designed by Mario Henrique Simonsen/FGV Library

Neves, Leonardo Paz e Prata, Gabriel Aleixo
Blockchain contributions for the climate finance [recurso eletrônico] : introducing a debate / Leonardo Paz Neves, Gabriel Aleixo Prata. – Rio de Janeiro : FGV, International Intelligence Unit, 2018.
1 recurso online (74 p.) : PDF, il.

Dados eletrônicos.
Em parceria com Konrad-Adenauer-Stiftung.
Inclui bibliografia.

1.Blockchains (Base de dados). 2. Instituições financeiras - Inovações tecnológicas. 3. Transferência eletrônica de fundos. 4. Mudanças climáticas - Aspectos econômicos. I. Fundação Getulio Vargas. Núcleo de Prospecção de Inteligência Internacional. II. Título.
1. Blockchain. 2. Emerging Technologies 3. Climate Finance. 4. Climate Change. 5. Public Policy

CDD – 332.178

Contents

Foreword

Dear Readers,

The Climate Issue continues to be a main concern for the global society. Many American countries, south of the Rio Grande, are owners of invaluable natural assets while still struggling to find a stable development path. A path which, combined with credible and adequate political institutions, would lead them to more prosperity and less unequal, fairer communities; with a wise use of their resources, endowments and environment.

The Konrad Adenauer Stiftung, always aware of the major public governance problems facing societies constructing a better future for their generations, within a true spirit of liberty and social dialogue, has established in Lima, Peru, a Latin American Centre, KAS EKLA, for discussing and fostering modern, constructive debate and solutions to the Climate Issue.

It is with enormous pleasure that the International Intelligence Unit, FGV IIU, a think tank directly linked to the FGV Presidency, in Rio, Brazil, has started a partnership with KAS EKLA on the extremely challenging topic of the uses of Blockchain technology in climate finance,

The Report, an outcome of workshops, discussions with experts and needed research work on this new field, opens a window on the problem. Blockchain itself is promising though full of uncertainties, not least on its privacy and data protection -from a global citizen's viewpoint- aspects; the climate narrative needs no words to describe how emotional and complex it continues to be today.

I'm sure that KAS EKLA and FGV IIU are aware of the Pandora box they have opened with this pilot Project. But it lies entirely within their objectives: my congratulations for the initial work here completed.

I wish both institutions lots of good luck in further exploring such a challenging theme, always for the benefit of our planet, and, particularly, our South and Central American, Mexican and Caribbean societies.

Renato G. Flôres Jr
Director of FGV IIU

Dear Readers

In recent years, the politics on climate finance have gained a lot of attention from very different perspectives. It became a crucial measure to incentivize finance flows to fight climate change as a whole. Meanwhile, a global climate finance architecture has been created, facilitated by major events like the Paris Agreement. Currently, institutions like The Green Climate Fund are working on the implementation of concrete projects to adapt to the impacts of climate change, or to reduce CO2 emissions.

As the global activities and the amounts on climate finances are increasing, questions regarding transparency and efficiency are being raised and new technologies are coming to the focus of major stakeholders. Blockchain Technology seems to be a very promising new approach to overcome centralized structures and remain reliable. Especially for climate finances, it can help to earn the donors' trust by offering a maximum of transparency. In addition, it increases the efficiency of climate finance flows as a whole. May be the most important issue is that it can bring a lot of new stakeholders into the climate finance circle by reducing complexity. Startups are developing smart phone apps that allow everybody to work on climate finance. To fight against climate change it could be the next level for being much more effective, as climate finance becomes a very decentralized issue, concerning more and more people.

The enclosed study is part of the starting debate on crossing climate finances with Blockchain-technology. It gives the context and shows the connection. And more importantly, it gives certain recommendations on how it can be used to improve climate finances. The study was born from the first Workshop on this topic, which was held in Rio de Janeiro, together with our partner the FGV International Intelligence Unit. This Workshop was a starting point for our Regional Programme to find out how Blockchain can be used in environmental governance. I wish you all an interesting read.

Dr. Christian Hübner
Head of EKLA - KAS

Executive Summary

The consequences of climate change have rapidly become one of the most important issues of the global agenda. Along with the consequences of global warming, the current course of climate change is directly related to a series of environmental impacts such as: the rising of sea levels, increased frequency of extreme weather events, the shifting patterns of rainfall, increased risks for the wildlife, economic instability (especially in the agricultural sector), to name a few. The dimension of the expected impacts, combined with the speed of the climatic events, poses a significant challenge not only to countries, but to the international community as a whole, in designing a set of actions to adapt to and to mitigate those consequences.

In order to address these challenges, a significant amount of resources is needed. For instance, under the logic of the concept 'Common but Differentiated Responsibilities' the developed countries have pledged, under the UNFCC, to mobilize 100 billion US dollars yearly until 2020 to fund adaptation and mitigation efforts, especially in the developing world.

The international flows of capital aimed to fund climate initiatives have gained a lot of attention recently and has been at the center of the climate change debate. The massive volume of resources and its multiples financing channels have posed an enormous challenge in managing and guaranteeing the efficiency of the funding. Amidst the main challenges in the Climate Finance sector, we would highlight: difficulties to establish **Standards and Definitions**, lack of **Transparency and Accountability**; low frequency of **Monitoring/Tracking and Evaluation** processes; and **Overlapping and Double Counting**.

The Urgency in spending to curb the environmental impact in time; the Fragmentation, of the players involved in funding and operating the climate funds; and the Volume of resources, which is necessary to promote change in a global scale are fundamental characteristics of the Climate Finance process. Nonetheless, those are unchangeable features. Combined with the issues aforementioned, they provide a serious combination that allows delays, inefficiency and corruption to thrive in the way Climate Finance is managed. In that sense, tackling those issues seems paramount to the success of the international efforts to deal with climate change.

Encouraged by the UNFCC and the Paris Agreement recognition of the importance that technology has on mitigation and adaptation, and their call for the critical role that innovation has to foster and enable those technological solutions – a variety of actors has searched for alternatives.

The Distributed Ledger Technologies (among which Blockchain has gained world-wide recognition) is undoubtedly one of the forerunners in this process. The recent successes of one of its applications, the Bitcoin and other cryptocurrencies, have propelled the Blockchain technology to be considered one of the Top 10 Emerging Technologies by the World Economic Forum, besides Nanotechnology, Artificial Intelligence and others cutting-edge innovations.

The process in which the Blockchain technology operates relies on a number of characteristics that offers us a compelling case by the impressive complementarity between what Blockchain has to offer and what the Climate Finance needs. Blockchain applications generally provide gains in several areas that seems to be critical for dealing with the challenges experimented by Climate Finance. From those, worth mentioning the following: **Transparency**; **Time Stamp and Traceability**; **Trust-Minimizing; Identity Management**; **Privacy**; **Immutability**; **Decentralization**; and **Reliable Data Storage & Compliance**.

It is true, however, that the adoption of Blockchain solutions might bring with it several challenges, some even seems to go in the opposite direction of "saving the climate", such as the issue of the energy consumption. Nonetheless, rather than barriers, those challenges, if carefully addressed, could even strengthen the adoption of the technology. Therefore, further research are required to help in identifying the strengths and weakness of the Blockchain technology and assess to which extend it could provide a valuable contribution to the climate sector.

This report is one of the frontrunners in this regard. It hopes to foster an informed debate in order to demystify some general ideas regarding the technology and to deepen the level of the debate. This report takes a policy oriented approach, that goes further than providing a context, it also offers several recommendations in critical areas, such as: the importance in **Bridging the Institutional Gap** focus on countries and Civil Society Organizations; how to **Enhance Civil Society Role**; **Foster New Solutions**; and **Strengthen the Political Debate**.

Above all, we hope with this report to shed light to the issue at hand. By focusing the debate in a positive agenda, we expect that adoption may thrive in an environment where regulation would take an enabling approach, rather than a prohibitive one. If so, we believe that soon Blockchain-based solutions would greatly improve the Climate Finance processes and thus our effort in coping with the Climate Change.

1

Climate Change and Finance

The consequences of climate change have rapidly become one of the most important issues of the global agenda. Along with the consequences of global warming, the current course of climate change is directed related to a series of environmental impacts such as: the rising of sea levels, increased frequency of extreme weather events, the shifting patterns of rainfall, increased risks for the wildlife, economic instability (especially in the agricultural sector), among others.

The dimension of the expected impacts, combined with the speed of the climatic events, poses a significant challenge to the international community in designing a set of actions to adapt to and to mitigate those consequences. Under the international efforts to cope with the climate change, the United Nations Framework Convention on Climate Change (UNFCCC) was adopted in the 1992 Earth Summit in Rio de Janeiro, aiming to limit the man-made interference in the climate. It sought to manage the greenhouse gas emissions in order to limit its interference on climate. Since then, the Conference of Parties (COP) has been organizing the Convention on Climate, yearly, to determine the international strategies, approaches and solutions to the matter.

Among the main achievements of the COP meetings, it is important to highlight:

Kyoto Protocol (1997)

It determined legally binding emission targets for developed countries on major greenhouse gases. It also established mechanisms to aid countries in achieving those targets;

Marrakesh Accords (2001)

It created The Special Climate Change Fund (SCCF) and The Least Developed Countries Fund. The former aimed to finance projects related to adaptation initiatives in various sectors, such as: agriculture, waste management, technological transfers, among others. The latter expected to support the least developed countries in their effort to develop their national adaptation programs.

Copenhagen Accord (2009)

Despite the fact that the Copenhagen COP failed to reach an agreement on the Kyoto Protocol matter, it succeed in recognizing the 2°C rising limit to the global temperature, which, according to most of the scientific community, has been consistently rising to dangerous levels. It also managed to get commitments from the develop countries for a US$ 100 billion voluntary collaboration to finance projects that aimed to reduce the emission of greenhouse gases.

Paris Climate Agreement (2015)

Among its chief achievements, the Paris Agreement distinguishes itself by reaffirming the concept of the 'Different Starting Points and the Common but Differentiated Responsibilities'. In that sense, it acknowledges that developed countries should still take the lead in the international effort to mitigate the climate change and support developing countries in their initiatives. For that, the Agreement established the need of a US$ 100 billion yearly contribution by developed countries, to fund mitigation and adaptation efforts in developing countries, to be extended until 2025. Moreover, in a shift to a "bottom-up approach", it also established the 'Nationally Determined Contributions' (NDCs), in which each country would determine their own targets and actions on how to reduce their emissions and fight climate change.

The clarity of how advanced the global warming process is and the consciousness of the amount of resources needed to be invested to address the adaptation and mitigation efforts required have been an essential part of the debate, especially in the COP meetings. The debate regarding the need for a financial instrument to foster the sustainable development, especially in developing countries is a constant presence in the COP meetings. It also brings up an important question of who would make available the resources for this these instruments. The challenge of the funding matter also derives

from the additionality concerns and the wide variety of actors, both private and public, operating in this context – which, in many cases, lacks coordination, transparency, generates overlaps and are oriented by vested interests.

The logic of financial additionality determines that the funding commitments directed to climate change initiatives could not occur at the expense of ODA commitments; additional resources would be necessary for the climate change action. The diversity of the funding sources and initiatives operators has been a particular point of concern, both for the aforementioned issues and for the multiplicity of standards and divergence in the governance used by the funding sources. That matter has become a major issue for many local project operators, and even some governments, since the complexity of this context has generated a demand for many 'third' parties and/or intermediaries, which has reduced the transparency and accountability of the resource flows.

Players

The climate finance ecosystem has been growing rapidly and one of the main indicators for this expansion is the number of players, which greatly varies in functions and nature.

Regarding financing players, it is important to mention the multilateral players, which control the bulk of the climate finance resources, to wit: Multilateral Development Banks, Development Finance Institutions, Climate Bonds, Multilateral and Bilateral Funds, National Funds, among others.

The major players in this field are the Multilateral Trust Funds. Created through intergovernmental processes, those funds amass an important amount of resources dedicated to climate change. Beyond financing projects and programs, those funds also distinguish themselves by, occasionally, providing innovative standards in governance and accountability, which could bolster a positive spillover on other institutions in their effort to develop transparency and compliance mechanisms. Among the major climate related Multilateral Funds, we may highlight the following:

Global Environmental Facility (GEF)

One of the oldest initiatives regarding multilateral trust funds, it was created in 1991 as a pilot project from the World Bank. Soon after, in 1994, it was restructured as a result of a joint venture of the World Bank with the United Nations Development Program and the United Nations Environmental Program. The GEF initiative is a byproduct of the 1992 Rio Summit context, which defined the role of the GEF as a major supporter of the developing countries in meeting the goals established by the major international environmental treaties.

The Climate Investment Funds (CIFs)

Created in 2008 by multilateral development banks, such as the World Bank, the CIFs stands for two funds: the Clean Technology Fund and the Strategy Climate Fund. The Clean Technology Fund aims to support emerging countries in financing projects related to low carbon technologies in order to aid in their transition. The resources of this particular fund usually support projects in clean transport, renewable energy and energy efficiency. The Strategic Fund, also concerned in supporting developing countries, comprises three different funding areas: Climate Resilience, Scaling up Renewable Energy and Forestry Management.

The Adaptation Fund

Created in the context of the Kyoto Protocol, the Adaptation Fund is a financial instrument under the UNFCCC that aims to finance adaptation projects, especially in developing countries that are considerably exposed to climate change consequences. The Adaptation Fund became notorious by facilitating the access to their funding schemes, simplifying and accelerating the process and reducing the number of intermediaries.

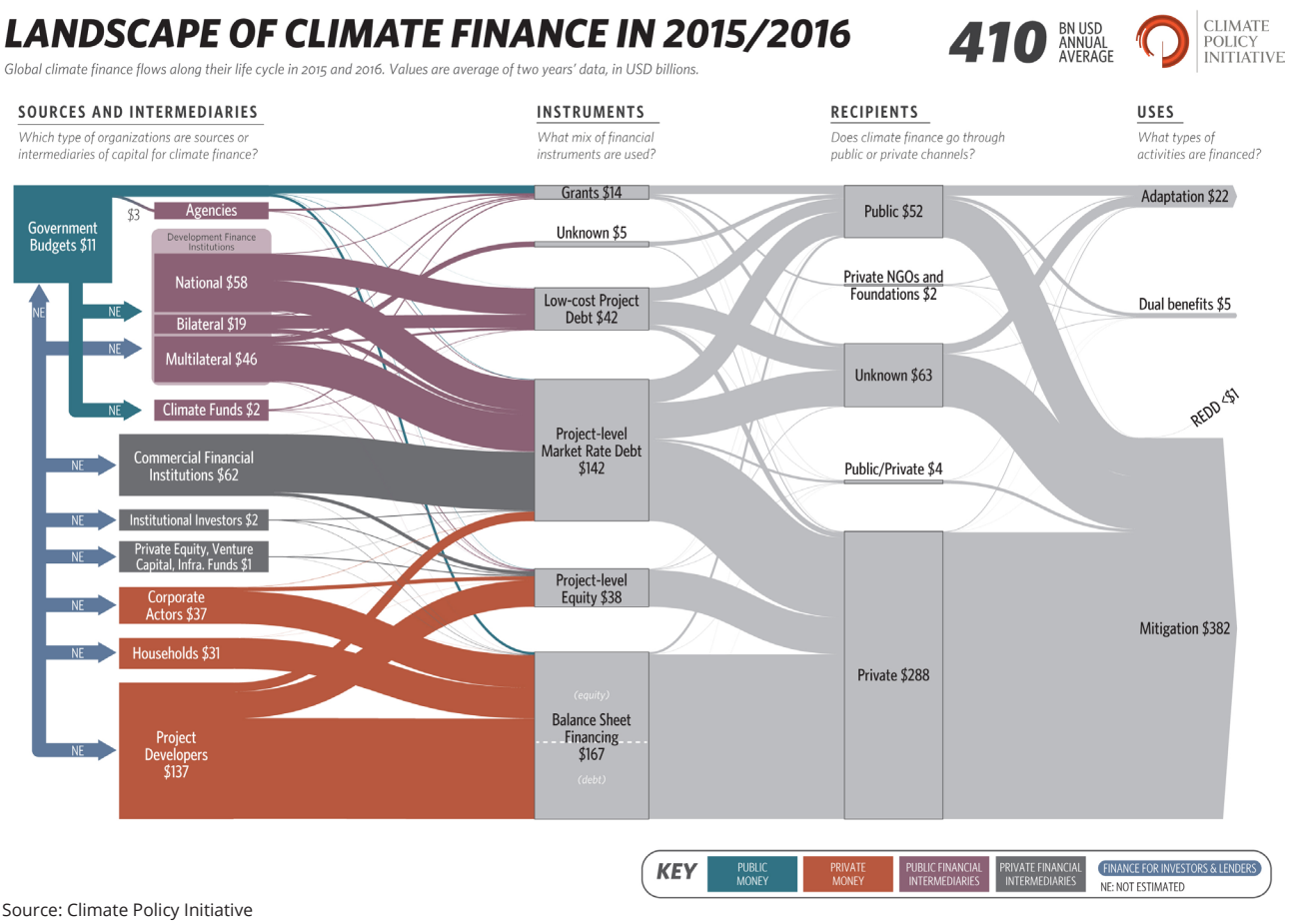
Green Climate Fund (GCF)

The GCF is also a financial instrument under the UNFCCC, but it was created in the context of the Paris Agreement, aiming to aid developing countries in developing projects to mitigate and adapt to the effects of climate change. An interesting feature of the GCF is that it also provides technical assistance to developing countries, especially for the development of their institutional capabilities, so they may be better prepared to access the GCF funding schemes.

An important second group of players, considered one of the major delivery channels for climate finance, is the Development Finance Institutions (DFIs), which accounts for a significant share of climate finance management. Multilateral Development Banks have an important role that goes beyond mere financial intermediaries between Climate Funds and countries. They also generate qualified knowledge and relevant information on regional experiences, foster replicable best practices, help build institutional capacities in recipient countries, assist them in developing their national and sectorial plans, create financial mechanisms more suitable for countries with capacity gaps, among other things.

Countries and Implementing Agencies (National or Regional) are also part of this core group of players. They are on the recipient side of the equation, accessing funding from Trust Funds and, generally, through Development Finance Institutions, to invest on their programs and projects. Although Countries and Implementing Agencies usually feature as recipients, they also have the role of 'donors' since a part of the funds raised internationally is often redirected to Civil Society Organizations that are the players operating the projects.

Image 01: **Landscape of Climate Finance in 2015/2016**



Source: Climate Policy Initiative

Climate Finance

Climate finance generally refers to the financial resource flows used to support a broad spectrum of initiatives related to climate change and sustainability.

They may foster both adaptation and mitigation activities. Adaptation activities focus on actions that reduce the impacts from the current climate change risks and consequences that are bound to happen. Adaptation efforts aim to improve the resilience of human and natural systems to such changes. Mitigation, in the other hand, seeks to moderate and alleviate the consequences of the climate change, mainly by reducing or limiting the emissions of Greenhouse Gases.

There is no single definition of climate finance

While there is no single definition of climate finance, the one provided by the United Nations Framework Convention on Climate Change (UNFCCC) offers a helpful insight into its meaning: *"finance that aims at reducing emissions, and enhancing sinks of greenhouse gases and at reducing vulnerability and maintaining and increasing the resilience of human and ecological systems to negative climate change impacts."* [1]

This definition refers to the financing channeled by local, national, regional and international entities for climate change projects and programs. They include climate-specific support mechanisms and financial assistance for mitigation and adaptation activities to spur and enable the transition towards low-carbon, climate-resilient growth and development through capacity building, R&D and economic development. The term has been used in a narrow sense to refer to transfers of public resources from developed to developing countries, in light of their UN Climate Convention obligations to provide "new and additional financial resources", and in a wider sense to refer to all financial flows relating to climate change mitigation and adaptation initiatives, from both private and public actors.

The massive volume of resources and its multiple financing channels have posed an enormous challenge

The international flows of capital aimed to fund climate initiatives have gained a lot of attention recently and have been at the center of the climate change debate. The massive volume of resources and its multiple financing channels have posed an enormous challenge in managing and guaranteeing the efficiency of the funding. To operate this large stream of climate resources, a wide array of mechanisms and financial instruments are necessary, aimed to fund the climate change initiatives (Forstater, 2012). Among the Mechanisms, the National Climate Funds are a fundamental tool. National Funds are generally the way in which countries assemble, blend and manage all the resources incoming from national sources and international grants, loans, etc.

These resources will then be allocated accordingly to the country national strategy, funding multilevel programs and projects, which will be carried out by either National Implementing Agencies or Civil Society Organizations.

Carbon Market is also an important Mechanism. It was the first international financial mechanism developed to mitigate global greenhouse gas emissions, by efficiently reducing emissions by setting limits on emissions and allowing the trading

1 United Nations Framework Convention on Climate Change. UNFCCC Standing Committee on Finance 2014 Biennial Assessment and Overview of Climate Finance Flows Report. 2014.

of emission units. The Carbon Market established the conditions to a whole new trading environment that created innovations such as: carbon and emissions trading, emissions allowances, carbon offset, etc.

Regarding financial instruments, among the most popular ones we could highlight: i. Multilateral and Bilateral Grants, which are non-repayable funds that are generally directed to non-economic activities; ii. Non-Concessional and Concessional loans, which are mainly operated by the private sector and development financial institutions, and have played a critical role in supporting large projects and sustainable economy initiatives; iii. Insurance Instruments, often related to risk management from both investments and natural disasters; and iv. Guarantees, also a tool to mitigate risk, generally involving the government role in creating a safer environment to attract investments to ensure the viability of a given program or public policy (Transparency International, 2017).

Beyond the traditional financing approaches, currently it is possible to identify different innovative climate finance instruments and products. Those innovative ideas generally aim to seek funding for new initiatives that manage to overcome the ordinary risks and close market gaps, and usually have a difficult time in accessing traditional climate funds. Equity Funds, for example, are generally more flexible instruments, allowing, for instance, to fund smaller projects that are usually not eligible for Climate Funds due to their size. Equities are also able to invest in a wider range of asset classes. Eco-Enterprises and Davos Timberland are two interesting examples from this alternative. Bond issuance is also a flexible alternative that manages to mobilize long-term capital, and it could easily be accessed by a large variety of funding sources, such as pension funds, hedge funds, governments, and other investors. The Climate Awareness Bonds from the European Investment Bank is an interesting example of Green Bonds.

Despite the variety of institutions, mechanisms and instruments, accessing climate funds is a burdensome process that only a few of players are able to grasp, generally due to their capacity gaps – a scenario that has strengthened the role of intermediary institutions. The process of a given country accessing directly resources from the Trust Funds is long and complex. The accreditation process of the country or its designated National Implementing Agency requires their ability to demonstrate that they have adequate institutional, technical, and financial performance to implement the projects, properly manage the project resources and the capacity to comply with the Fund´s fiduciary standards. These processes require the applicant to have an organizational structure and a qualified team to provide extensive supporting documentation for the accreditation and the bid, which conditions are generally absent in developing and least developed countries.

Table 01: **Minimum Fiduciary Standards from the Global Environment Facility (GEF)**

Audit, Financial Management and Control Framework	Project/Activity Processes and Oversight	Investigations
• External Financial Audit • Financial Management and Control Frameworks • Financial Disclosure • Code of Ethics • Internal Audit	• Project Appraisal Standards • Procurement Processes • Monitoring and Project-at-Risk Systems • Evaluation Function	• Investigation Function • Hotline and Whistle blower • Protection

Source: Druce, Gruning and Menzel, 2013

Despite the leading role that intermediaries institutions, such as UN Agencies and International Development Banks, have in facilitating the access to Trust Fund resources and distributing them to countries and their Implementing Agencies, many countries have shown desire to access those resources directly. That aspiration was met with decisions by most Trust Funds to not only facilitate and simplify the processes of accreditation and of direct access to funding, but also to provide capacity building for countries with institutional and technical capacity gaps. In addition to the principle of Direct Access, the concept of Enhanced Direct Access has been gaining ground in the last few years. This concept resides in the idea that the delegation of decision-making power to sub-national/local level entities, capable of making those decisions and implementing actions, may provide a greater level of ownership and need-driven to projects funded by climate resources.

Sectors

Regarding sectors, renewable energy generation is becoming a regular "winner" in capturing investment both from public and private sources.

Both in 2015 and 2016, the amount of private investment in renewable energy generation has far surpassed the investment in fossil fuel energy generation. In 2015, US$ 299 billion were directed to renewables, versus US$ 111 Billion for fossil fuel. Following the trend, in 2016, once again, renewables investment managed to double the amount invested in fossil fuels, US$242 billion against 118 US$ billion (Buchner, Oliver, Wang, Carswell, Meattle, Mazza, 2017).

Shepherds Flat Wind Farm

The levels of spending in climate finance have been steadily increasing in the last few years, although it was possible to identify a significant decrease from the 2015 to the 2016 levels. In the 2015, a record high was achieved in terms of climate finance flows, reaching US$ 437 billion dollars. This surge was largely driven by the private investment, especially in China, the US and Japan.

Although we watched a decrease in the investment levels in 2016, the scenario could not be considered all pessimistic. According to the Global Landscape of Climate Finance 2017, two main reasons helped to explain the lower levels of investment of this year. The first reason is connected to the falling costs of the renewable technologies, which decreased by 10% in average. The second reason is related to the capacity of many countries to assimilate further investments in their economies. Positive expectations, thus, arise from the fact that only recently few players started to operate at nearly their full capacity, such as the Green Climate Fund, which was launched in 2015 and the New Development Bank, which funded its first activities in 2016.

Mitigation efforts have been receiving the lion's share of the climate investment. In the 2015/2016 period, it accounted for nearly 93% of the total investment. From the volume directed to mitigation activities, the largest beneficiary was the renewable energy sector, having received 74% in the same period. This was a considerable increase, if compared to the last few years. This increase was propelled by heavy investments by United States, Japan and especially China, who was responsible for a surge in investment on its generational renewable capacity (Buchner, Oliver, Wang, Carswell, Meattle, Mazza, 2017).

Conversely, despite the fact that Adaptation initiatives received a considerably smaller share of climate investment, according to the Global Landscape of Climate Finance 2017 report, some of the decrease in investment could be explained due to methodological changes in climate finance reporting done by Development Finance Institutions. In the Adaptation case, water and wastewater projects were the most "popular" allocations for the public finance, accounting for 51% of the adaptation investment.

Challenges

The nature of the Climate Finance ecosystem brings with it several central issues that must be addressed presently.

As noted before, the climate finance environment has grown tremendously in complexity, due either to the volume flow of money, or to the increasing number of players – each of them operating in a dense web of rules, standards and processes. In this highly complex and rapidly growing environment, some challenges arise as stumbling blocks, hindering the chances of success of the international efforts. Among these major challenges, we could highlight:

1. Standards and Definitions

To date, there is no universally agreed definition on what should count as 'Climate Finance'. The lack of definition and standards is a byproduct of the multitude of players, each one with its own rules and procedures. This issue lies in the foundation of the problem, since it affects several others important topics and hinders the coordination efforts. This matter affects how each player processes: the funding operation, the initiatives eligible for funding, the reporting system, etc.

2. Transparency and Accountability

One of the biggest concerns for the climate finance environment is the transparency of the resource flows and operations. Here several dimensions must being highlighted, such as: assess the fulfillment of the pledges made by the developed countries and thus ensuring 'Additionality'; access to better data, which would be paramount to the assessment of the initiatives and to better inform agents responsible for decision making; avoid waste and misuse of the resources; and combat corruption.

3. Monitoring/Tracking and Evaluation

Both issues 1 and 2 have a direct impact on M&E initiatives. The lack of definitions and transparency make it very hard to identify the path that the climate finance resources have taken and their final destination. All this heavily impacts the consolidation of data (and its quality) – much needed to conduct evaluation processes and to assess the efficacy and efficiency of the initiatives.

4. Overlapping and Double Counting

In a scenario with a wide array of players, each of them following their own rules and procedures and with limited exchange of information between them, funding overlapping and double counting contributions is not that rare. The lack of transparency (from donors and recipients) coupled with the difficulty to track the financial flows, allow that different funding players end up supporting the same initiative. Or, on the other hand, also allow that the same resource be accounted for twice.

The Urgency in spending to curb the environmental impact in time; the Fragmentation of the players involved in funding and operating climate resources; and the Volume of resources necessary to promote change in a global scale are fundamental characteristics of the Climate Finance process. Those are unchangeable features. Combined with the aforementioned issues, they provide a serious combination that allows inefficiency and corruption to thrive in the way Climate Finance is currently managed. In that sense, tackling those issues seems paramount to the success of the international efforts to deal with climate change.

2

Blockchain Technology

Blockchain is a technology designed to work as a trust machine[2]. There are three key elements needed to establish trust: identity, ownership and verification. Blockchains allow users to easily prove their identities, protect ownership of digital assets and verify transactions without intermediaries.

Identity:

Blockchain is based on the use of digital signatures through asymmetric cryptography. Each user is given a set of two digital codes: a "public key," similar to an account number, and a "private key", similar to a password.

Ownership:

Blockchain maintains a continuously growing database of records, protecting the whole transaction history of what is operating from being tampered with, even by their operators. In addition to the huge computational power that usually protects the database accounting the values each user possesses, there are also economic disincentives, making frauds financially pointless in most cases.

Verification:

For each Blockchain network, there is a common database to which all parties can propose changes and the network itself will validate, rejecting fraudulent or wrong data from being recognized as valid and propagating only the proper information, periodically establishing consensus throughout the whole network. Everyone connected to the network sees the same information, as each and every peer has the exact same copy of the database, with verified new information being added to it. This public audit capability provides the system with an indisputably groundbreaking level of transparency.

How Blockchain Technology Works and Why It Was Created at First

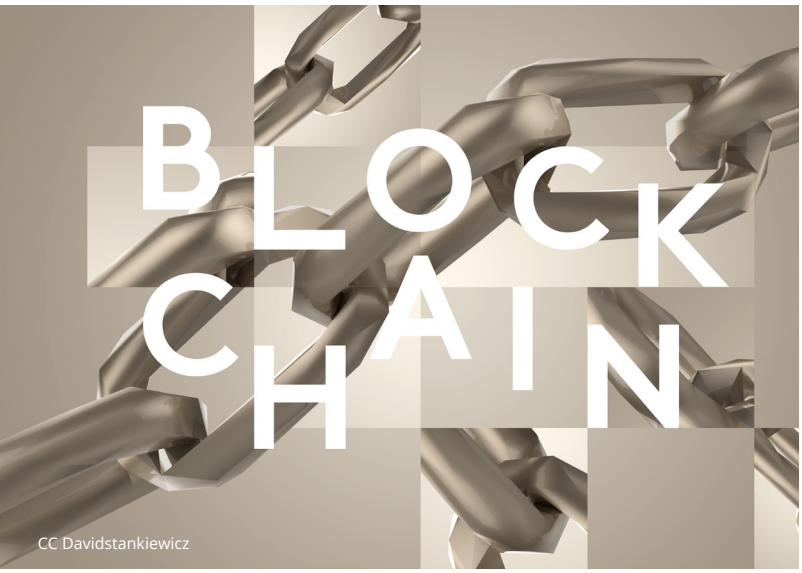
In October 31, 2008 an individual or group of people using the pseudonym Satoshi Nakamoto started a discussion in the cypherpunks mailing list, an online tech forum devoted mostly to computer scientists and alike, focused on social transformation through encryption tools. Satoshi said that he had been working on a novel system for electronic cash named Bitcoin, allegedly capable of working in an entirely decentralized way, in the sense that it did not rely on any trusted third party (like banks or States) to function properly. These ideas were put together and firstly introduced in the form of the whitepaper Bitcoin: a Peer-to-Peer Electronic Cash System, with direct references to predecessors like Wei Dai's b-Money and Adam Back's Hashcash. Satoshi was clear about the main intentions behind his creation at that time, by emphasizing that Bitcoin would allow any two or more parties to interact financially without any kind of intermediary, as trust would be automatically established by Bitcoin's distributed network of computers running the same piece of software to maintain the system.

Two months after publishing the Bitcoin whitepaper in a Cryptography mailing list, Satoshi Nakamoto released the first version of the Bitcoin software as an entirely open source protocol. For the first time in more than 25 years of research (Lamport, Pease, Shostak, 1982) and theoretical proposals in the field, the electronic cash idea was successfully implemented as a real protocol. With limited use cases for the first 4 years of its existence, it was in 2013 that Bitcoin reached the mainstream, through a combination of macroeconomic, political and media factors. Since then, it has been evolving by the attention and the investments of large enterprises, startups and hedge funds focused

2 https://www.economist.com/leaders/2015/10/31/the-trust-machine

on developing the Bitcoin ecosystem of financial applications. Moreover, especially from 2015 on, many markets (Bheehmaiah, 2015)[3] have been showing an even larger interest on the underlying technology that made it possible for Bitcoin to work as a digital currency under a distributed network of nodes, with no public or private intermediary needed: the Blockchain.

Blockchain is a technology that relies on cryptography to maintain a continuously growing database of records, protecting all the registered information from being tampered with, even by their operators. Blockchain requires a software that allows computers to communicate with each other directly through a distributed network of peers, where no one has special powers over the others. Thus, these databases are periodically updated with new information comprising new transactions or registries, and consensus is automatically reached, guaranteeing that everyone connected to the network sees the same information. In other words, each and every peer has the exact same copy of the database, with verified new information being added to it after passing through a decentralized validation process.



Blockchain is a technology that relies on cryptography to maintain a continuously growing database of records

Taking Bitcoin as an example, its Blockchain works as a sort of public ledger that accounts the number of coins that belongs to each user. A new block of transactions added to the chain resembles new pages being filled on an accounting book, in order to preserve both the whole history of all the coins that changed hands in the network and the current holdings of all the users (i.e., the final sum that they possess at any given time). Blockchain is the term commonly used to describe the technology itself and the public database it generates and maintains. As mentioned, it is focused primarily on the maintenance of consensus between any users connected through its decentralized network.

In practical terms, consensus means that there is a common database to which all parties can propose changes and the network itself will validate, rejecting fraudulent or wrong data from being recognized as valid and propagating only the proper information, periodically establishing consensus among the whole network. The main achievement of this technology is to be constructed from an intricate mechanism that, based on computational power and economic incentives, makes any attempt to circumvent the validation process prohibitively costly. Basically, there are no intermediaries responsible for ensuring the integrity or the trustworthiness of the data, since this systematic is regulated by software voluntarily executed by users from any part of the globe connected to the network.

As explored in the aforementioned example, Blockchain was originally programmed in Bitcoin (Nakamoto, 2008) in the form of a shared database that represents a public record of the whole history of its transactions, by constantly counting how many bitcoins (the system's digital value units) are owned by each user of the system at any given time. In legacy systems, strictly speaking there are one or more institutions, generally considered intermediaries, responsible for taking care of this permanent update. In systems based on the Blockchain technology, this process is operationalized by ensuring that the network is updated by the users themselves, and they are the only ones responsible for adding the information that accounts for new exchanges being made and the consequent changes that must be made to the copy each one holds of the Blockchain.

3 Further information at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2596465

In addition, there is a mechanism based on asymmetric cryptography[4] which uses pairs of public and private keys (Nakamoto, 2008), ensuring that, roughly speaking, only the proper user can change the information concerning him in the network. That is, only the holder of that balance in bitcoins can propagate to the network the information needed to transfer them to another person, since any other (malicious) attempt will be rejected by the code that regulates the system. From this, it is possible to conclude that the consensus between the parties is maintained even in a very dynamic sphere, since this common database also grows whenever new exchanges of information (such as Bitcoin transaction) are performed.

In short, what Blockchain provides is based on a sequence of factors:

1. "Proof-of-Work":
It means that if you are a miner (a jargon for the users that connect to the network as a validating node), you need to offer a solution to a mathematical puzzle that demands a lot of computational power to be solved, in order to be able to add new information to the database that constitutes a Blockchain per se.

2. Encryption:
This is based on cryptographic functions, ensuring an important feature of the system: information, as well as its authenticity and authorship, is easy to verify, but it is practically impossible for a single entity or individual to circumvent it, as massive computational power would be needed and there are also huge economic disincentives to do so.

3. Audit:
Once validated by the system's code, run concurrently by a whole network of thousands of peers and propagated over the network in order to be added to their own copies of the Blockchain, this information has its validity publicly audited by everyone, according to the information itself, its author and also the date and the time it was created.

4 For further information, refer to: Hirsch, Frederick J. "SSL/TLS Strong Encryption: An Introduction". In Apache HTTP Server.

It is precisely because of this technical rigor and the consequent open possibilities that it becomes possible to see Blockchain as a foundational technology with real transformative potential, especially due to what it allows in terms of transparency, reliability, security and efficiency of transactions. New uses for Blockchain, whose code or motivations owe much to the original implementation launched in Bitcoin, begin in the financial field but extend across the most varied fields in which intermediation had been an absolute necessity. The potential of Blockchain technology lies in its ability to offer censorship-free in a decentralized fashion, guaranteeing new fields for a more equitable set of digital institutions (Radu, 2015), no matter if they allow to carry out votes, payments or one of its most promising features: smart contracts.

For Blockchain researchers Aaron Wright and Primavera De Filippi (2015), the paradigm shift brought by the diffusion of the Blockchain, followed by the increasing implementation of decentralized systems based on it, will lead to the rise of *lex cryptographia* (De Filippi, Wright, 2015), which means a set of rules administered through self-executing smart contracts. If, instead of data corresponding to numbers or financial information, as in the case of Bitcoin, a database built and generated by Blockchain technology stores data of other kinds, it is possible to maintain a wide range of new services, much wider than those strictly monetary, with the same qualities of Bitcoin: inviolable, irreversible, secure, independent and decentralized. The report *Blockchain Technology and Legal Implications of 'Crypto 2.0'* from Bloomberg BNA indicates that this growing trend started to get traction in 2015, with the phenomenon dubbed "Blockchain 2.0" impacting major industries.

Property records, proofs of authorship and intellectual property, digitization and automation of contracts, international remittances, issuance of private titles, mechanisms for decentralized control of institutions, remote and distributed storage of cloud data and various financial products are some of the first among a diverse set of markets being transformed. The logic behind these new Blockchain-based technologies that have been emerging, in addition to being responsible for making them operational in most cases, is written in the form of

smart contracts. In different cases and moments, they should be responsible for disrupting certain a lot of ineffective or inefficient processes.

In *Formalizing and Securing Relationships on Public Networks* (1997), American cryptographer and lawyer Nick Szabo introduced the seminal idea of smart contracts and what they could become. Since 2014, it has been going from mere vision to practical implementations, mostly with the emergence of Ethereum. It is a decentralized system that operates a Blockchain-based network to be a global supercomputer whose smart contracting capabilities are jointly maintained by its users.

American cryptographer and lawyer Nick Szabo introduced the seminal idea of smart contracts and what they could become

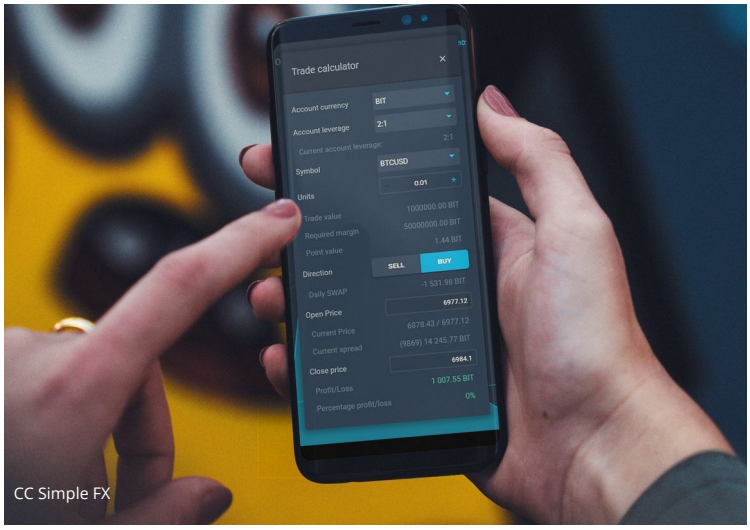
A relationship between two minds (Szabo, 1997), as well as its formalization, is the starting point for the concept of "contract". In practical terms, it can be understood as the establishment of actions and the possible criteria applicable to judge or regulate them, once a common agreement has been made between two or more parties. In this case, adding "intelligence", in the computational sense, to contracts consists of the ability to make them digital, more automated and based on commonly used hardware and software (Szabo, 1997). This could significantly reduce human failure, making the control protocols surrounding contracts less costly, as in smart contracts they are automatically designed to assess whether certain clauses were complied with or not. In a digital environment marked by large automation, control procedures such as auditing, for example, would require much less time and financial resources than traditional options. This would also make room for the "self-execution" of digital contracts, arguably the main benefit of a smart contract, whenever the validation of its clauses had been automatically processed. As pointed out by De Filippi and Wright, the Blockchain is closely related to the implementation of smart contracts:

> *Using a distributed database, like the blockchain, parties can confirm that an event or condition has in fact occurred without the need for a third party. As a result, the technology has breathed life into a theoretical concept first formulated in 1997: digital, computable contracts where the performance and enforcement of contractual conditions occur automatically, without the need for human intervention [...]. In some cases, smart contracts represent the implementation of a contractual agreement, whose legal provisions have been formalized into source code. Contracting parties can thus structure their relationships more efficiently, in a self-executing manner and without the ambiguity of words. Reliance on source code enables willing parties to model contractual performance and simulate the agreement's performance before execution. In other cases, smart contracts introduce new codified relationships that are both defined and automatically enforced by code, but which are not linked to any underlying contractual rights or obligations. To the extent that a blockchain allows for the implementation of self-executing transactions, parties can freely transact with one another, without the technical need to enter into a standard contractual arrangement.*
> *(DE FILIPPI, WRIGHT, 2015).*

In terms of large open networks based on Blockchain today, the main highlights are the Bitcoin and Ethereum protocols. In different but equally valid ways, both allow the implementation of smart contracts. Ethereum allows any user to create and run smart contracts deployed in its Blockchain, associated with its own programming language, aimed to make the whole process as straightforward as possible. While each of the dozens of serious Blockchain projects operating nowadays has particular advantages and limitations, it is especially important to emphasize that Ethereum was the first to be created explicitly in order to maintain a Blockchain on top of which it is easy to deploy smart contracts or to create an entire decentralized application based on them. What Ethereum maintains, in short, is a Blockchain network optimized for general use cases. The opening section of the original Ethereum whitepaper, describing the project, includes points of special interest for the present report:

> *Commonly cited alternative applications of blockchain technology include using on-blockchain digital assets to represent custom currencies and financial instruments ("colored coins "), the ownership of an underlying physical device (" smart property "), non-fungible assets such as domain names (" Namecoin "), ("smart contracts") [...] What Ethereum intends to provide is a blockchain with a fully-fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code. (https: //ethereum.org)*

Beyond the native platform, given that it operates as a kind of backbone on which large-scale projects can be built, new applications are already beginning to affect markets once dominated by few players: Augur (decentralized prediction markets), Maker (stable digital currencies and standalone banking services), Dharma Protocol (a permissionless protocol for issuing, underwriting, and administering debt instruments as cryptographic tokens), DAOstack (an operating system for massive collaboration) and Aragon (a project that aims to disintermediate the creation and maintenance of organizational structures), to name a few.



Ethereum allows any user to create and run smart contracts deployed in its Blockchain, associated with its own programming language

Why Blockchain and the Decentralization it Promotes are Important

From 2000 onward, greater decentralization proved to be paramount for the resilience of many innovative technologies. Services such as Napster, which although decentralized had a central company as co-responsible, ended up being completely shut down as a result of legal battles involving copyright and other issues. Some of these services were stopped regardless of the nature of the content being shared, thus harming the full range of users, including those who made legal use of them. However, successor alternatives were created with a focus on greater decentralization, providing users with point-to-point connection without the need for large fault-prone central points, making tools such as the Gnutella network "unstoppable" from a technological perspective, although the illegal use of these and other networks is duly combated in the traditional legal sphere.

Entrepreneurs and activists set some opposition to the way certain businesses were traditionally conducted

With regard to the evolution of decentralized networks from the 2000s onwards, it is important to recognize the permanent legacy that such systems have left in the digital economy universe. By proposing changes in a way that became known as "permissionless innovation", entrepreneurs and activists set some opposition to the way certain businesses were traditionally conducted. Either by the inefficiency of the old models on which they were based or by ideological issues which led some to propose a greater democratization in the access to culture and information. The accelerated cycle of innovation that has marked the growth of the internet in the last decade and its consequences are largely responsible for the inevitable assimilation of some of the recent changes by the mainstream.

The yearning for constant user innovation, combined with the challenges of decentralized technologies, whether fair or otherwise, has forced large businesses to adapt their models and practices completely. Thus, it can be said that the new model of streaming multimedia content, such as music and movies paid by monthly subscription, as proposed by companies such as Spotify or Netflix, was a response largely influenced by the assimilation of recent changes in the consumption of these goods impact on market demands. Or, clearly pointing out: without the controversial transformation initiated by Napster, it is likely that, even with the advent of the Internet, the market would still be stuck in old-fashioned models for trading multimedia content, emulating the analog world in the digital

CC Christiaan Colen

Without the controversial transformation initiated by Napster, the market would still be stuck in old-fashioned models for trading multimedia content

universe, and without taking full advantage of the advantages brought by the latter. Thus, even with the alternation of companies or projects as market leaders or referrals, decentralization and its impact on business models are configured as growing trends. The strongest wave and the new frontier of this phenomenon at the moment are precisely the diffusion of services based on Blockchain, given the substantially broader impact it can generate in a wide scope.

In *Why Business Schools Need to Teach About the Blockchain*, researcher Kariappa Bheemaiah (2015) clearly exposes the pillars that make Blockchain a great asset to innovation, both for the unprecedented technical aspects it has and for the power it has to accelerate and amplify the positive effects of other decentralized arrangements that preceded it:

> *[...] the Internet of Everything is increasingly becoming part of business reality. Today businesses and societies are noticing that the line between physical and virtual existence is beginning to blur at an increasing rate. A secondary effect of the internet of everything is that it will also create an economy of everything (Panikkar, 2015), the every device capable of connecting to the internet becomes a point of transaction and economic value generation for consumers and prosumers in a sharing economy . [...] the possibilities that are offered by the Blockchain technology begin to make economic sense. [...] In addition, decentralized architectures offer better cost benefits to companies as the peer-to-peer sharing of resources in the distributed network removes dependency on a central server, optimizes resource use and reduces costs. [...] The distributed networks begin to act as channel of value-based transactions and in light of the aforementioned advantages, a new breed of Blockchain-based businesses are now beginning to show signs of disruption in various domains of the market.*
> *(Bheemaiah, 2015)*

The transformative potential of Blockchain technologies, however, is not limited to promoting a closer approximation, or in some cases even the merger itself, between the figures of the service provider and the consumer of the service provider. Nor is it limited to the enormous economy and consequent simplification in the cost structure of any given application, made possible by the elimination of several intermediaries, expensive auditors or related services. By impacting new business dimensions, such as customer relationships (from automation via smart contracts), value proposition (by enabling services that were not possible before) and revenue sources (given the reach digital currencies can have), Blockchain is clearly being singled out as a top trend, providing the world with new services, as well as the potential it has for improving traditional services that assimilate and implement it.

Blockchain is clearly being singled out as a top trend

3

Blockchain Contributions Applied to Climate Finance

a. Public and Private Blockchains

A DLT (distributed ledger technology) is a general acronym referring to a group of technologies capable of maintaining, updating and storing a database by multiple independent parties. Even though Blockchain has been considered a pioneer and foundational technology in many aspects, technically speaking it is nowadays understood as one out of a few DLTs. More specifically, a subset of this macro category, which at the same time comprises completely different informational architectures such as IOTA's Tangle or R3's CORDA, for example. We should note that this does not stop, however, some people from labelling everything related to these topics, both the multiple technologies involved and the benefits from its adoption, as simply "Blockchain" instead of DLTs, as the second term can be confusing to some at the time being.

Transfers on a distributed ledger are generally made final when the ledger is updated. In this sense, a Distributed Ledger can be permissioned or permissionless[5]. Permission refers to how the system works with respect to validating transactions. In a permissioned system, you need to be verified to validate a transaction, which means that, to some degree, the nodes know each other. On the other hand, for permissionless Blockchain such as Bitcoin and Ethereum networks, all the peers can act freely (entering or leaving the network at any time), without identifying or authenticating themselves, without causing any disruption. The single major exception being the security of a permissionless Blockchain, which is generally accepted to be greater: the more distributed it its, the more nodes/peers it has as part of the network[6].

b. Blockchain Main Technical Features

Blockchain's potential is rooted in providing data with the following qualities:

i. Key Benefits

The key benefits are related to the promotion of transparency, security and accountability, thus reducing fraud and corruption, as well as adding to a stronger traceability. Immutability, inviolability, and resilience are one of the key factors that fuels excitement about technology. The decentralization character of the system allows only data verified by independent nodes to be accepted, which makes it impractical and prohibitively costly to attempt an inconsistent data entry or fraudulent changes to already confirmed transactions.

CASE

CarbonX (Cost Efficiency)

CarbonX offers financial incentives for individuals to reduce their carbon footprint. The Canadian startup CarbonX first buys carbon offsets, then converts the carbon credits into a cryptocurrency token called CxT. It then sells the tokens to retailers and manufacturers, who in turn use them to encourage consumers to make more sustainable choices. Consumers using the CarbonX platform might earn tokens for choosing locally-grown produce instead of flown in from a distant country, or for buying an energy-saving washing machine. These tokens can then be exchanged for carbon-friendly goods and services, other reward program points, or other digital currencies. The loyalty scheme uses Blockchain technology to seamlessly keep track of the transactions. Retailers will decide how many tokens a given purchase will earn, and the tokens will be tradable on the CarbonX platform. Retailers and service providers signing up to CarbonX will also be able to take advantage of transaction data and information on customers' energy usage to help them target products and services to customers who are most likely to purchase them.

CARBONX
PERSONAL CARBON TRADING INC.

5 http://coala.global/uploads/COALA-GLOSSARY-DEC-2015.pdf

6 https://www.bis.org/publ/arpdf/ar2018e5.pdf

ii. Transparency

Anyone with access to the network can view the history of all transactions operated and being operated in real time. Blockchain records work through a common database, to which all parties can propose changes. The network automatically validates new information at the same time everyone connected to it can audit the entire process, securing the rejection of any wrong data and the propagation of proper information, periodically re-establishing the public consensus. Everyone sees the all the data, as each and every peer has the exact same copy of the database, with verified new information being added to it. This public audit capability makes for the system indisputable groundbreaking level of transparency. Potential impact: the money trail can be tracked and monitored more accurately in areas like aid distribution.

iii. Privacy (and Opacity)

Usually, participants of a Blockchain can be pseudonymous by default, without putting the network and its operations at risk, even though they can choose to reveal their real-world identities at different levels, according to the needs of the technology being used or of any application built on top of it. They can communicate their decisions merely by using of their pairs of public and private keys, disclosing any information tying these keys to any specific individual or organization being optional, at the technical level. In Bitcoin's Blockchain for example, the user does not have to be identified a priori, by giving away any personal data, whereas this is needed when the Blockchain application touches traditional institutions, which is the case when you are exchanging bitcoins for dollars in your regular bank account. Just as some degrees of privacy are perfectly possible, the exact same opposite is also true, with full transparency being reachable to all the three pillars mentioned before: identity, ownership and verification. We can even ensure the identity of any set of specific members without risking the privacy of the others. Because each participant has access to one or more unique private keys that identify them, anyone can digitally sign their transaction using it so that it is only possible to mathematically conclude that whoever executed this signature was the holder of that key. Authentication is a field that undoubtedly presents a wide range of applications.

CASE

BNDES Token & TruBudget (Transparency)

The Brazilian Bank for Economic and Social Development (BNDES) held its first experience with Blockchain in early 2018. After a long period in which the bank had been studying the potential use cases, both in national and international fields, the Blockchain Initiative is being developed through two projects. The first is based on a private network developed in partnership with the German Development Bank KfW, whereas the second is creating tokens for the Bank's public financing processes using the Ethereum network. BNDES established a MoU with KfW in February 2018, allowing them to use and improve the German's Blockchain based tool called TruBudget. KfW provides BNDES with consulting and technical support, working in parallel with the National Institute of Information Technology. KfW also intends to consolidate its open source software licenses. As a proof of concept, the new Amazon Fund website was announced in mid-April. The idea is to use tokenized assets for money transactions originated from non-refundable foreign funds, which is exactly the case of the Amazon Fund. In their new portal, citizens can access the summarized project and the respective procedures, in line with the indicators of effectiveness.

The BNDES Token was started with a simple but very impactful idea. When a loan is released, it is done through a tokenized backed asset, in such a way that the monitoring of all transactions can be done in real time, both by BNDES agents and by civil society as a whole. It is important to emphasize that, although there are some trade-offs in any application like this, the use of Blockchain technology in this case guarantees the added transparency and full traceability benefits for everyone involved in these processes. That is, these benefits are not only restricted with regard to financial operations at national and supranational levels, but also have clear and positive impacts for all the final beneficiaries.

CASES

BVRIO Institute (Immutability)

The BVRio Institute is an organization with a mission to promote the use of market mechanisms to facilitate compliance with environmental laws and support the green economy in Brazil. The creation of the BVRio is part of a strategy to contribute to the development of an ecosystem of players involved in activities related to environmental economics. Since 2016, BVRio has been using the Ethereum blockchain as part of its risk analysis tool for the acquisition of Brazilian tropical timber. Risk analysis allows timber buyers to have detailed information about the exploration, processing and transportation activities related to the product they are purchasing. BVRio consolidates the public information on the extraction, processing and negotiation of timber and identifies if there are risks of illegality on the products acquired by Brazilian and foreign buyers. Blockchain technology serves as an indicator of confidence in the information they consolidate.

Imagine that a timber buyer has used the BVRio platform to generate a risk assessment report for the supply chain of a given timber product. After some time, this same buyer questions the information that was used in the calculation of a report. In this case, BVRio presents a consolidated report on the timber market to the date of the report generated by the buyer. The consolidated report contains all assessments made for all timber sources known to the BVRio at that time, so that the origin of the buyer's timber can be compared to other sources. But how do you know if the consolidated report was generated on that date and not produced after? That's where the blockchain comes in. At the end of each day, when a consolidated report is generated, BVRio generates a hash (a sort of digital fingerprint) of the report and saves it in the Blockchain of the Ethereum network. Once the transaction in which the hash was saved is confirmed by the network, it can no longer be changed. So, if the buyer wants to confirm the date of issuance of the consolidated report, they can request the report from BVRio, generate the hash from the contents of the report and compare it with the hash that is stored in the Ethereum network. The information is guaranteed to not change, given the immutability of Blockchains, and is publicly available. In addition, BVRio does not need to maintain an infrastructure to keep records or worry about server downtime, since the Ethereum Blockchain has no single point of failure.

BVRIO

iv. Immutability

Unlike traditional accounting systems, Blockchain is based on the concept of triple-entry accounting, in which the time variable is inserted and attached to all transactions so that they are located and sorted in a specific order. This temporality, that is, the fact that each transaction is coded and "stamped" with date and time, allows the tracking of all "blocks of the chain", in addition to ensuring that transactions cannot be easily changed. In fact, for public Blockchains, the cost of attempting to cheat on such networks is prohibitive to the point that it is considered impractical for any rational economic agent. This chaining logic of blocks that have past transaction information added to the system's immutability allows any good or value transacted via Blockchain to be traced from its first to its last state.

v. Trust-minimizing

Blockchains allow anyone to send money to anyone without an expensive or corrupt intermediary, with a deeply decentralized consensus mechanism, which relies solely on the machines connected by the network running the same piece of software, regardless of who their owners are. Potential impact: money sent across borders or into natural disaster zones will move quickly. In addition, many critical elements of our economy allow people to trade with each other without fear that the other party will back out. Banks perform this function, but often add high administration costs and slow processing times into the system. Blockchain smart contracts guarantee that a contract will be fulfilled when a specific action is completed. Potential impact: eliminating intermediaries reduces counterparty risk, thus reducing costs.

vi. Reliable Data Storage & Compliance

Among other promoted features of the Blockchain are the possibility of elaborating self-executable "code pieces" in the form of smart contracts and decentralized autonomous organizations. In such a way, programmability can also be considered as a benefit of Blockchain technology and thus enabling predictability. In fact, this technology allows not only the creation of automation in different fields, but also the creation of layers where it is possible to create other systems that run in parallel applications.

Since they are highly programmable and automated, the scale gains of the network also become evident. Blockchains have huge potential with increasing scale gains and decreasing costs according to the size of their structure.

vii. Identity (information) Management

Blockchains can create and manage identities for people in a less costly, secure way through digital signature technology, which gives people a public key (similar to an account number) and a private key (similar to a password). Potential impact: underserved populations, like the unbanked, receive access to services never before possible. The advantages of using a Blockchain are intrinsically related to the elements that make up the technology. This technology allows cost and bureaucracy reduction, increasing at the same time the reliability and efficiency of payment systems. It is important to note that while the benefits are tied to the technology, applications mentioned here as examples comprise the most important use cases today, being the factor of extreme relevance for its use in the scope of Climate Finance.

CASES

Zug, Switzerland (Identity (information) Management)

The town of Zug, self-titled the "Crypto Valley" due to their business-friendly environment for Blockchain entrepreneurs, launched a trial Blockchain voting system that could be rolled out to cover public votes in future years. The trial period took the form of a very simple questionnaire at first. Citizens were asked whether they would like to see fireworks at the annual town festival and similar low-key issues. The purpose of an exercise like this is to see to which extent a system like that works. According to SwissInfo, however, the mayor of Zug Dolfi Müller made it clear that the town could, in the near future, build new use cases based on Blockchain technologies to store and distribute data for bigger purposes in a few years. Müller believes that Blockchain offers enhanced security over other e-voting systems, including better protection against hacks and misuse of personal data, as its decentralized nature means there is no single point of entry for hackers to manipulate vote results, according to Zug authorities. Voters can access the system via Zug's Blockchain eID system and it has also been employed for Zug's Blockchain bicycle hire and library service.

View over Lake Zug

CASE

Everledger (Traceability)

Blockchain could be applied to various sectors of the supply chain economy. For example, in agriculture, the authentication and possibility of following every route of a particular crop, from its planting to the final destination, guarantees transparency and benefits not only for the end user, since they would be sure of the stages and origin of that product, but also for the enforcement authorities. With regard to industry, the process of recording every step of the manufacturing process in a Blockchain would make the work of the professionals in the segment much more efficient. This could be even stronger, due to the additional uses of geolocation records and data collected directly from sensors. In this exact sense, Everledger operates in diamonds registration and tracking. In the project, each diamond has its measures recorded in the Blockchain, being assigned to it a corresponding serial number. Once you have registered the information on the diamond in the Blockchain, you can carry out all diamond tracking to protect the end consumer against informational frauds about the product. This project allows transparency in matters of public interest, such as the working conditions during the productive process and the ways of exploring natural resources, as well as adding value to the service provided by the company that exploits diamonds registered in Blockchain.

everledger

viii. Timestamping & Traceability

Not only does Blockchain guarantee the integrity of the main data being recorded, but it is also added to the database with a correspondent timestamp pointing out when it was done (date and time) and a digital signature cryptographically identifying its author(s). Potential impact: timestamping and authorship capabilities are essential to easily identify any inconsistency in transactions, preventing frauds or errors from being propagated and causing temporary disruptions in Blockchain-based systems. Moreover, these tools make for a robust system of proof of ownership, keeping permanent track of who is adding new information, as well as who is making requests to access or change anything, contributing to an even more incorruptible system to manage strategic funds globally.

ix. Decentralization and Democratic Use

One feature that guarantees the uniqueness of the Blockchain in relation to other databases is the current consensus mechanism and its recurrent update by highly decentralized means. This underscores the point of diffuse trust in the network, so that unknown participants can trust each other unequivocally, a fact that is strongly secured by the use of cryptography and distributed consensus algorithms, mostly proof-of-work and proof-of-stake. These are basically an algorithm that ensures that the data of the network are the same for all participants and crucial for legitimizing transactions. In this regard, it is important to emphasize that the debate on decentralized and distributed governance is directly related to this consensus mechanism (usually influenced by economic incentives). In the case of large databases, structured using Blockchain technology, such as Bitcoin and Ethereum, there has been no occurrence of total network outage or attacks that have actually compromised its operation to date. The main mechanism that provides this is the direct result of the strong decentralization of these networks. Without central points of failure to be attacked, they are able to operate even in extreme situations.

CASES

Power Ledger (Decentralization)

Created to empower individuals and communities to co-create their energy future and foster the development of a power system that could grow in an autonomous, resilient and low-cost way, the Power Ledger platform was started as an ecosystem focused on enabling interoperability between diverse market management/pricing mechanisms and units of electricity (kWh) by way of pre-purchased tokens. The Power Ledger platform provides a transparent governance framework that allows the ecosystem to seamlessly interface with energy markets all over the world, bringing a new reality to consumers. It is basically a trustless, transparent and interoperable energy-trading platform that supports an ever-expanding suite of energy applications, with exchangeable frictionless energy-trading tokens, which can be purchased and redeemed using fiat currencies with individual trading platforms hosting closed-loop exchanges for energy and tokens. Energy trading applications are not just conceptual, they are proven and deployed in a few communities and energy markets including Australia, New Zealand, Europe and Asia. Its P2P trading applications give retailers the ability to empower consumers to simply trade electricity with one another and receive payment in real-time from an automated and trustless reconciliation and settlement system. There are many other immediate benefits, such as being able to select a clean energy source, trade with neighbors, receive more money for power surplus, benefit from transparency of all trades being recorded on a Blockchain and very low settlement costs, all leading to lower power bills and improved returns on investments in distributed renewables.

POWER LEDGER

Mudamos (Democratic Use)

The Mudamos application is an initiative of the Institute for Technology and Society of Rio de Janeiro (ITS Rio), awarded by the Google Social Impact Challenge in 2016, and is a tool for signing popular initiative bills in a safe and simple way. Mudamos is an application that turns any smartphone into a digital pen, making it easier, safer and more transparent to put signatures on popular initiative bills, making it possible for Brazilian citizens to exercise this essential right, bringing voters and their representatives closer. The architecture provided by Mudamos also paves the way for the expansion of these concepts and the creation of a sovereign identity for the civic exercise in manifestation of the political will of any citizen.

When a user registers in the application, he is also creating a Blockchain "wallet", with a public cryptographic key that digitally identifies him. The Mudamos app recognizes the identity from the data that the user provides, such as their social security number, voter's registration, name and ZIP code. By signing a bill in the application, the user does so through a key that could only be contained in their mobile phone. The content of the subscription, as submitted through the Mudamos Blockchain System, is stored, as well as data regarding the origin of this signature, the cellphone ID and other metadata that could be used in an audit process, whenever a possible fraud is detected. In the analogous process, when it is done an analogical way (paper), any attempt to identify the date, time and place, or even the pen that signed the form, would be impossible, as these traces are not recorded.

The difference in having a digital process in which it is possible to give unity to the actions of the users is that the interaction of these users with the network can produce information that strengthens their digital identity. The more interactions with different applications or services, the more credible this digital identity becomes. In this regard, at the same time that the Mudamos app experiences the use of cryptographic keys to certify signatures on popular initiative bills, it also becomes an application capable of authenticating certain identity information of its users, especially the ones needed for the exercise of other political rights or access to governmental services in the foreseeable future.

MUDAMOS

Table 02: **Current Blockchain Applications Focused on Climate**

PROJECT	ADDITIONAL INFORMATION	MAIN BENEFIT
Carbon Coin	https://carboncoin.cc/	Cost Efficiency
CarbonX	https://www.carbonx.ca/	Cost Efficiency
Climate Ledger	https://www.climateledger.org/	Transparency
Climate Chain	http://www.theclimatechain.org/	Transparency
Earth Token	https://www.earth-token.com/	Transparency
Energy Blockchain	http://www.energy-blockchain.com/	Cost Efficiency
Energy Web	http://www.energyweb.org/	Decentralization
Fintech4Good	https://www.fintech4good.co/	Transparency
Grid+	http://www.gridplus.io/	Automation
DAO Integral for Climate	http://ipci.io/	Transparency
Poseidon	https://poseidon.eco/index.html	Transparency
Power Ledger	https://powerledger.io/	Decentralization
Redd Chain	www.climateledger.org/resources/5.pdf	Automation
Solar Coin	https://solarcoin.org/	Cost Efficiency
Veridium	https://www.veridium.io/	Accountability
Volt Markets	https://voltmarkets.com/	Decentralization
Xpansiv	https://www.xpansiv.com/	Immutability

Source: Adapted from: https://www.ieta.org/resources/Resources/GHG_Report/2017/Using-Blockchain-to-Achieve-Climate-Change-Policy-Outcomes-Baumann.pdf

4

Blockchain Limitations

a. Legal Framework

The emergence of every groundbreaking technology creates an environment of uncertainty as it changes the status quo, bringing a new set of players, relationships and possibilities. Along with all those changes, these new technologies also pose fundamental challenges for any society, from a legal to an ethical nature.

The Internet, which also had a groundbreaking impact in all societies, is a very interesting predictor for some of the challenges that lie ahead for the Blockchain. The Internet brought with it several (legal) tensions that even now have not been completely solved. The regulation of the new cyberspace brought to the table not only old tensions, such as geographical boundaries, but also new ones such as the distinction between two normative systems: the legal code and the technical code.

This distinction is better illustrated as the legal code being the group of regulations that determine legal obligations. Legal code is extrinsic, as Lessig (1999) would put it, for those rules can be broken, and a legal agent (generally the government) would act accordingly to ensure compliance. The technical code, which works through protocols and software, has, on the other hand, an intrinsic nature. That is because if rules are "broken" in this environment, an error occurs and no activity happens, so compliance is an inherent part of the process. Pioneers and enthusiasts in the early days of the Internet (as it is often compared to the current days regarding Blockchain technology) believed that the technical code could somehow overcome the legal code in the Internet. That the rules determined by protocols and systems would suffice to regulate this environment, which would lead to greater individual freedom and emancipation (De Filippi and Wright, 2018). This rationale is intimately related to the idea that the Internet was (and now Blockchain is) supposed to be unregulated and uncontrolled by governments.

Eventually, governments managed to extend their control to the Internet, although they are still struggling in some sectors. They ultimately found out that the best way of regulating the Internet was through its "intermediaries", such as internet providers, data centers, companies, programmers – so those intermediaries would have to abide to the legal code as they develop the technical code. The Blockchain is the 'second chance' for those pioneers and enthusiasts, as it fosters the development of automated and self-regulated systems. Ultimately, this *lex cryptographica* (Di Filipi and Wright, 2018) would allow people to engage with others (peer-to-peer) in many different levels, from exchanging values to validating documents, without intermediaries. The Bitcoin software is currently the most notorious example of this dynamic. It functions solely by technical code, in which for every transaction every player must follow the rules determined by the code. Here the technical code was able, without following or being controlled by any country, to determine the issuance of a currency (or a reserve of value, as many regard Bitcoin as the Gold 2.0), the total availability of coins, transaction validations, among other necessary processes.

As emerging technologies began to be adopted, they started to pose challenges which were soon confronted with regulations. Nonetheless, Regulations could have both positive and negative impacts on those technologies. In that sense, regulations could be grouped in two categories: Enabling and Prohibitive. Considering the Blockchain as an example, enabling regulations would be considered those that allow and support the use of Blockchain-based solutions in our daily lives, such as digital signatures. That means that as the legal code recognizes the legitimacy of digital signatures, it would lay the legal ground for smart contracts to operate through digital authentication and digital transaction validation. Conversely, the prohibitive category would generally outlaw certain initiatives or constrain the conduct of certain players. The ban of the Initial Coin Offerings (ICOs), as a way to access resources to fund initiatives, by China is an illustrative case in this scenario.

As seen before, the Blockchain could be either permissioned or permissionless. In the case of a permissioned Blockchain, the application is likely to have an internal and operational nature, in the sense that it would work more as a software emulating an "interlinked database" to be used by a company or a group of companies to exchange and store information in a more efficient way. Here, the legal

code would have fewer situations to regulate, since we would be generally talking about more controlled inside processes. The legal code would probably apply to cases that the permissioned Blockchain is used as a platform for smart contracts between a group of companies that is part of this particular network.

In the case of the permissionless Blockchain, the legal code would have more situations to cover. Here, the most notorious example is the Bitcoin. Applications that share some features with Bitcoin would be decentralized in nature and open to participation. Those features would invite a series of questions of how to frame this given application in order to verify how to regulate it. Some of the possibilities are:

1. Securities Law, which would regulate its issuance and transactions;

2. Money Transmission Law, which would be applied to monitor (and possibly control) the fluxes of money;

3. Tax Regulations, which would target gains from those solutions that emulate currency or reserve of value;

4. Privacy and Data Ownership, which would try to ensure the user has legal rights regarding its own information;

5. Restrictions and prohibitions, which would simply restrict or ban certain applications that government authorities deem to be harmful (such as the aforementioned case of the ICOs in China).

Blockchain technology is still immature and most sectors have yet to use it at its full capacity

Blockchain technology is still immature and most sectors have yet to use it at its full capacity. In that sense, there is a tangible danger to overregulate the field in these early stages, since it could constrain unpredictable (positive) developments and innovation. In the other hand, a complete lack of regulation also delays the mainstream adoption of the technology, given the uncertainties that this scenario generates and could create situations in which some players might use loopholes to benefit themselves. Careful and flexible rules, such as “Regulatory Sandbox Approaches”, could offer a way out from this difficult dilemma.

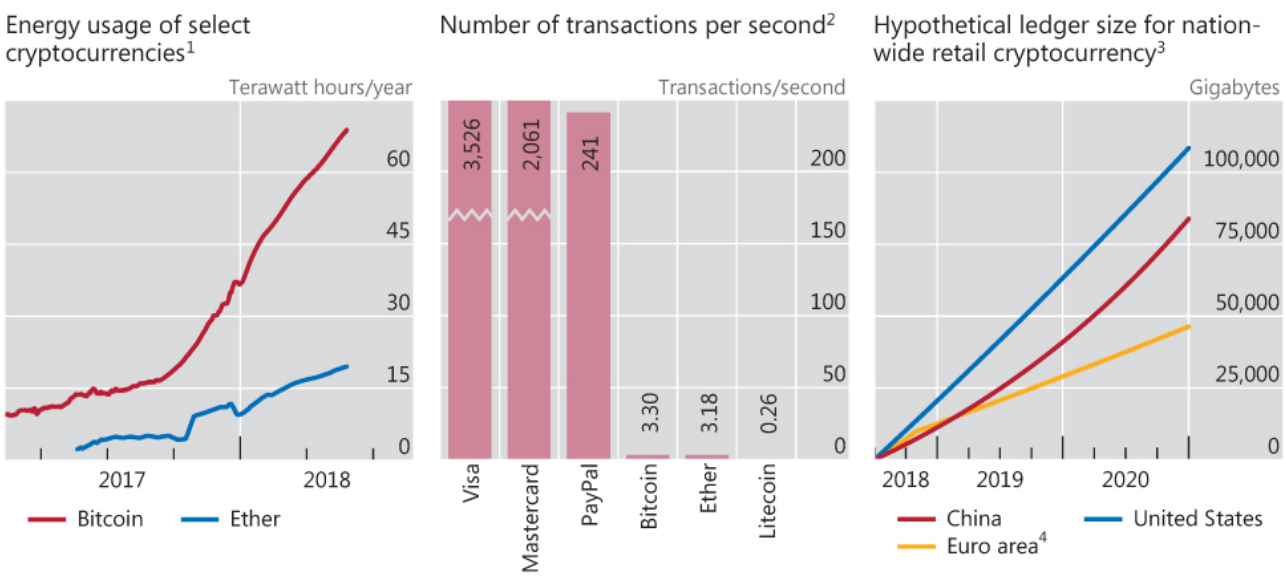
b. Environmental Impact

Energy Consumption and Scaling Issues

The Bitcoin price hikes in 2017 had drawn a great deal of attention towards the cryptocurrency. Most of it focused in its financial dimension, whether or not it was a bubble and/or whether it could really replace fiat currencies. In parallel, from the sustainability point of view, the most controversial issue was the escalation of the energy consumption, necessary to power the Bitcoin. By early December 2017, when Bitcoin was near its all-time high value (in US dollars), its energy consumption peaked– which was, at that time, surpassing the consumption of countries like Ireland and Nigeria[7].

7 Further information at: https://www.bis.org/publ/arpdf/ar2018e5.pdf

Image 02: **Energy Consumption and Scaling Issues**



[1] Estimated. [2] 2017 data. [3] The displayed hypothetical size of the blockchain/ledger is calculated assuming that, starting from 1 July 2018, all non-cash retail transactions of either China, the United States or the euro area are processed via a cryptocurrency. Calculations are based on information on non-cash transaction numbers from CPMI (2017) and assume that each transaction adds 250 bytes to the ledger. [4] BE, FR, DE, IT and NL.

Source: Annual Economic Report 2018 from BIS[8]

The issue about the massive energy consumption raised a lot of concerns about the sustainability of the Bitcoin and other Blockchain applications and their impact on the environment. Those concerns are generally grouped in two poles. The first group worried about the economical sustainability of all Blockchain solutions, since if most of them presented the same levels of energy consumption of Bitcoin, they would be economically impracticable. The second group focused on the environmental sphere caused by the impact that this technology would provoke in the global energy matrix, in special regarding the incentives to use non-sustainable sources of energy (as coal power plants).

The Bitcoin´s energy consumption derives from the process of cryptography called Proof-of-Work. In short, it manages to collect a given amount of data (transactions, in the case of the Bitcoin) and encrypt it in the form of a "hash", after solving a highly-complex mathematical problem. The process of solving this mathematical problem demands a great deal of computational power, and therefore electrical energy. Proof-of-Work was the first consensus algorithm that succeeded in creating a trustless network. When Bitcoin was created, the low number of transactions did not require such computational effort. In fact, originally, Bitcoin was supposed to be "mined" by individuals in their own personal computers – since the idea of Bitcoin's creator was to achieve maximum decentralization for the network. In this early days scenario, the amount of energy needed to power the network would be residual.

As the network grew and the number of transactions increased, the original solution became insufficient. Soon after, miners started to used computer graphic cards due to their capacity to perform considerably better, not only in terms of speed hash, but also because they also consumed less energy. In 2011, the newly-born Bitcoin mining industry developed mining devices that drastically improved one´s capacity to mine Bitcoins. Those new mining hardware devices, developed specifically to this purpose, basically took over the mining business (especially in the case of the Bitcoin). Today, it is possible to find real "mining farms" in places that offer cheap electrical energy to power these machines.

8 Available at: https://www.bis.org/statistics/ar2018stats.htm

Despite the fact that the Bitcoins´ energy consumption matter took many observers by surprise, given the dimension it took in late 2017, the mining industry and the Blockchain developer community were already trying to address this issue. So far it is possible to divide these efforts in three different directions. The first direction has been carried out by the mining industry. Companies invested considerably to improve the technology behind the new mining hardware, in order to make them more cost-effective. The table 03 offers a simple, but illustrative, comparison between the solutions already used to mine Bitcoins.

Table 03: **Hardware Efficiency in Mining Bitcoins**

Mining Hardware	Hash Power	Energy Efficiency	Started to Operate
Personal Computer (Intel(R) Core(TM)2 Duo)	2.5 Mh/s	N/A	2009
Graphic Card (NVIDIA GeForce GTX 1080 8 GB)	30 Mh/s	180 W	2011
Antminer S1	180 Gh/s	360 W	2013
Antminer S9	13.5 Th/s	1.375 W	2016

Source: Authors

The second and third directions are led by the developer community. The second relates to protocol innovation. As mentioned before, the Proof-of-Work protocol was the first consensus algorithm to be developed, and remains the most popular protocol, operating most of the cryptocoins. As the hash power efficiency and energy consumption started to become an issue on scalability debate, new solutions started to be developed. To date, the most popular alternative to the Proof-of-Work is the Proof-of-Stake protocol. The difference between them is based mostly on who solves the complex mathematical problem; while the former depends on miners, the latter counts with the coin owners to create the blocks – which requires significant less energy consumption. Despite the near dominance from those two solutions, there are other alternatives already being tested or being developed. Reports from universities such as MIT and Cornell, and large tech firms, such as IBM and Intel, show us that a new generation of sustainable Blockchain solutions, aiming to cope with the energy efficiency issue, is being developed.

The third direction is not directly concerned with Blockchain´s energy efficiency, but with applications' scalability (whether or not Bitcoin is able to go mainstream, for instance). But since the scalability is directed related to the energy efficiency of a given application, the solutions from this group also impact the environmental sustainability sector. This direction comprehends a wide array of technological advancements that are supposed to upgrade a given Blockchain application. A notorious example, in the case of the Bitcoin (although not specifically), is the development of the Lightning Network, which would, in short, create a second layer at the top of the Blockchain, which would enable instant transactions.

Energy consumption is still a major limitation for Blockchain applications. The Proof-of-Work is still the dominant protocol and solutions like the Lighting Network are still in testing stages. Nonetheless, the Blockchain development industry has proven to be a vibrant, innovative and fast-paced environment. In order to remain economically viable, new technological advancements will probably remain a top priority. Since every Blockchain is a ledger (and therefore a file or database) that exists in many copies, the computer resources and the energy required for the calculation, transmission and storage of the information increases as the Blockchain grows in complexity and use. One academic study showed that the cost of bitcoin mining was comparable to the whole of Ireland's electricity consumption[9]. The energy footprint, therefore, needs to be a significant consideration in decisions on whether and how to roll out the technology.

9 Karl J. O'Dwyer and David Malone, Bitcoin Mining and its Energy Footprint, Hamilton Institute, National University of Ireland Maynooth, 2014. Available at: http://karlodwyer.com/publications/pdf/bitcoin_KJOD_2014.pdf

The senior executives we interviewed were divided on whether Blockchain will contribute to net energy saving or whether it will add to energy demand. 40% of interviewees believe that Blockchain adds to total energy demand, while 47% think that it brings net savings on energy demand (the rest of interviewees did not answer). The actual costs of how Blockchain applications will develop cannot, of course, be fully projected today. Improvements in the technology may reduce energy costs, and there are cost differences between private and public Blockchain. Private Blockchain usually involve lower transaction costs and operate on the basis of simplified verification processes (for instance, proof-of-work verification uses up more energy than the proof-of-stake process), which decreases costs.

The actual costs of how Blockchain applications will develop cannot, of course, be fully projected today

c. Quality of Data

As any database system, the quality of data inserted on system is paramount for its operation. Here, the human factor is permanently a major issue, since human error is always a constant in this equation.

With Blockchain it is no different, in fact this issue is even more pressing, since one of its main features is the near immutability of the data inserted on the Blockchain. Even though is impossible to eliminate the impact of the human factor on the accuracy of data input, there are already some alternatives that could mitigate its impact on many Blockchain applications.

Probably one of the major alternatives is the Internet of Things technology (IoT). IoT sensors enable devices to communicate with themselves, allowing them to monitor and record readings from a given situation/environment, in an accurate and unbiased manner. Here, the nanotechnology could even boost the IoT sensors solutions through nanosensors. As an example, IoT sensors could be used to monitor and record, safely in the Blockchain, weather conditions from a given locality or even the levels of greenhouse gases emissions from factories.

Even in those cases, where is impossible to rely solely on technology to insert data in the Blockchain, is possible to diminish human error even when the human factor is present. The most important element here is the education and capacitation of those handling the information. Well-trained staff, regular training courses, well-defined guidelines, and clear handbooks would probably generate a positive impact on error and confusion during the process.

A second solution, when dealing with the human factor, is the use of redundancies and confirmations in the system. Here, the idea is to develop a set of processes in which before the information is inserted in the Blockchain, it would have to comply with some procedures, for instance: confirmation by more than one person, double entry of data, cross confirmation from two different entries, etc. Data quality will always be a central issue in any Blockchain application, due to its immutability feature. In situations of permissioned Blockchain solutions, such as an application used by a Developing Finance Institution to monitor, track and store the information of its funding schemes to their local partners, the focus would probably be on human factor issues. In cases of a permissionless Blockchain network that uses sensors from multiple players to gather information from CO2 emissions levels in the atmosphere from all over the world, it would require a different approach to ensure the accuracy of its data.

Data quality will always be a central issue in any Blockchain application

d. Privacy Dilemma

Paradoxically, the Blockchain technology has been hailed both for its ability to offer a transparent decentralized network and, at the same time, guarantee a high level of privacy for its users through pseudonyms and hash addresses.

The interesting combination of transparency and privacy in the Blockchain is possible because: when a given transaction information is inserted in the Blockchain, this information will be in the hash format, therefore impossible to read without a private key – but, at the same time, the information will be there, immutable and available for verification. This assertion, however, is inaccurate. One limitation of the Blockchain technology regarding privacy relies on the possibility of identifying information from users and transactions. One possible way to do it is to identify transactional patterns to link transaction addresses to real-world identities. Additionally, web trackers and cookies used by most websites leak pieces of transactions information that could be used when trying to connect addresses and identities.

For many cases, smart contracts are supposed to store a fair amount of sensitive/confidential information from the business conducted by the parties that use them. This is the case of applications such as Ethereum, which powers most of the smart contracts in use for now. In cases like this, although some information could be encrypted, many sensitive information still goes to the transparent layer of the Ethereum Blockchain. In that sense, despite the fact that there are some uses of the Blockchain technology in which privacy is not an issue, such as monitoring the emissions in the atmosphere or sea tides patterns, others are highly dependable of stronger privacy levels, for example: financial documents, terms of contracts, password and credentials, user's identity, among others.

To cope with this issue, the developer community has already presented some alternatives that could mitigate the privacy issue. One example is the 'Elliptic Curve Diffie-Hellman-Merkle (ECDHM)' addresses. In short, the ECDHM creates a secret key and masks the true address of the transactions, and only those who have that secret key would be able to know the true address. A second example is the 'tumbler', which consists in grouping a number of payers into a pool, and then enable the pool to spend afterwards. Theoretically, the only information that would be 'traceable' in the Blockchain would be a particular amount of coins from the pool to a particular receiver. Moreover, there are a few other solutions being developed. Many are popular amidst the cryptocurrency community, since they offer important solutions for them, among those we highlight: the zero-knowledge proof, zkSTARKs and Code Obfuscation.

There is also a second and serious problem concerning privacy when it comes to the use of Blockchain. One of the key features of a Blockchain, the immutability of its data, contrasts directly with the concept of the 'right to be forgotten', which became critical after the internet. Here, the storage (in datacenters or websites) and the use of private information were and still are a key point of concern in the internet debate.

One of the major reactions to this matter was the General Data Protection Regulation (GDPR), a comprehensive legal framework for personal data privacy recently approved by the European Union, which could have the ability to reshape how information is handled in the virtual world. The GDPR objective is to develop a data regulation framework for the European Union that would enhance individuals´ control regarding the storage and the use of their personal information and data. The initial focus of the GDPR was the regulation and control of cloud services and social media/networks, which seemed to be living an information "gold rush", in the sense that they tried to acquire as many data as they were able, generally from their users, and faced few constraints in how to benefit from it.

Blockchain-based solutions are being developed in a different context. Many of the applications that work with personal information exchange and/or storage have had to deal with regulations such as the GDPR since its inception. That is the case of the Blockchain platform being developed by the Spanish bank consortium Niuron. This platform aims to record the information of their new clients in order to enhance the user's experience (through reducing the time

and bureaucracy of the processes) and to fight crime, such as fraud and money laundering. Here, the idea is that once the new client registers with a given bank, his/her information would be shared with the other banks – which would expedite processes if this particular client decides to acquire products from other banks of the consortium, since the first bank already did the due diligence necessary by the 'Know Your Customer' regulations. The Niuron Consortium stated that its project is already in conformity with the new GDPR regulations, which means that privacy rights from its clients should already be protected.

Despite Blockchain's inherent paradox between confidentiality and transparency, privacy has been, from the beginning, a central concern of the original Blockchain project. Its signature project, the Bitcoin, aimed to "give back to the people" their control over money or limit individuals' reliance on governments. For that, being able to keep the privacy of one's transactions and information is a necessary issue. Starting from this point, the real question is less about how to guarantee privacy for users, but how to reach a middle-ground in which the user may have control of his/her information, but at the same time being bound to not withhold his/her information from the government - which has the attribution to investigate, fight crimes and enforce the rule of law to its perpetrators.

In this sense, report "*Blockchain – an opportunity for energy producers and consumers?*" published by PwC offers an interesting use case of Blockchain's inherent transparency for energy markets, balancing its risks and benefits:

> *[The] use of blockchain technology would ensure greater transparency for consumers. It would allow consumers to track exactly where the electricity they purchase was produced. Direct transactions between energy providers and energy consumers would enable the parties to specify exactly the "contractual counterparty", i.e. the wind or solar farm delivering the energy. This would make it possible to determine precisely the source of the electricity supplied, for example in terms of the percentage share of renewable energy. Every energy consumer would specify these aspects individually and to an unprecedented level of granularity. Accordingly, the entire transaction history stored on the blockchain (energy consumed and payments made) would also become transparent. The availability of a full transaction history and the possibility of running analyses on this basis would afford customers an as yet unrivalled level of clarity. Commercial and large customers who already have such data at their disposal today would be charged less for them, whilst probably having more details available on which they could base their analyses. A point to be critically reviewed in this context is what drawbacks this level of transparency would entail, as under the basic blockchain model all transactions are publicly accessible. The individual users would use aliases, but it is theoretically possible to "decrypt" a certain number of aliases without authorisation, which might pose a risk. (PwC, 2016)*

5

Considerations Regarding Adoption

a. Technical Dimension

i. Maturity of the Technology and its Features

According to some experts, such as the IBM Watson IoT Executive Architect, David Noller, "... 2018 will be a milestone year that we will see the adoption of a first set of Blockchain solutions in enterprise applications - from securing the pharmaceutical supply chain to eliminating inefficiency in international logistics." (Scott, Post, Quick and Rafiq, 2018). Most of the Blockchain early adopters were companies that started to pay attention to the technology between 2013-15. Most of their pilots and trials started to operate by 2016-17. Therefore, the following years will be paramount to observe the level of success and impact that Blockchain applications will present.

Despite of the relatively broad consensus that the Blockchain still is in its early stages and its first use cases are going live now, it is very difficult to assess the level of the maturity of the technology for its applications. The Blockchain is an incredibly versatile technology, which may be designed in many different ways to power different architectures, networks, processes, platforms, etc. Therefore, is extremely hard to generalize Blockchain's application to business, in its many different sectors. Discussing the use of the Blockchain technology should be on an individual basis, taking into account the particularities of the sector in question and the kind of solutions it aims for. In fact, an earlier decision is whether you should/need to use or not the Blockchain tech. In cases that there are centralized, do not have multiples participants, do not wish/need to track transactions or keep record and trust is not an issue – Blockchain might not be the adequate solution.

Even if the Blockchain would be a perfect fit for the use case in question, it is necessary to identify what kind of Blockchain would be more appropriate. For example, it is regarded as a consensus that no more than just a few Blockchain solutions for business purposes would rely on the Bitcoin Blockchain. The Bitcoin network is unregulated, considerable slower than its peers, has scalability issues and it is quite expensive to run a program in its network. In fact, many Blockchain-based solutions do not even have to rely in cryptocurrencies to operate properly, such as the Hyperledger case.

The decision to adopt the Blockchain technology is not to be considered only a technological matter. According to a Deloitte report, this adoption can "transform business models and processes, and reshape the set of stakeholders and their roles" (Chew, Killmeyer and White, 2017), therefore it might have deeper implications. Despite the obvious technological challenges of methods of validations, data standardization, scalability, infrastructure, systems integrations and personal capacitation, there are also some managerial issues to be dealt with, such as incentive structure, network governance, power and privileges structure, among others.

Currently, it is difficult to determine which sectors are more mature to harbor Blockchain applications. Nonetheless, some of them, such as the financial sector, have been leading the charge with many use cases leaving the piloting process and starting to launch phases. Sectors that have large conglomerates relying on supply chains and need cutting edge tracking systems could benefit greatly. As such, initiatives that have multiple participants and constantly share information (for example marketplaces) also might feel a significant impact. Other areas, such as the energy sector, medicine, education, insurance and government are already developing applications and running pilots as well. This phenomenon is especially interesting in the case of the public sector. Starting from several years ago numerous governmental (both on federal and local level) agencies have been trying to apply Blockchain solutions both to their public services (i.e. Land Registry and Identification Management) and their own internal administration (i.e. Procurements and Record Keeping).

Image 03: **Blockchain in the public sector (as for march 2017)**

Blockchain experiments in the public sector are accelerating globally, with a concentration in the US and Europe.

Source: Deloitte and Fletcher School as Tufts University

ii. Institutional Capacity Gaps (Small Civil Society Organizations and Large Banks) and Direct Link Between Donor and Local Projects

As mentioned before, accessing resources from Climate Funds is not an easy feat, since it requires from the applicant country, or its implementing agency, a considerable degree of institutional capacities. The level of fiduciary standards required from the Climate Funds is sometimes a barrier for many countries, which have to resort to the Multilateral Development Banks, as intermediaries, to "repack" the Funds' funding schemes to make them accessible to them. The level of complexity to comply with the standards sometimes raises concerns, since some of the smaller funding schemes from the Climate Funds occasionally require a burdensome and time-consuming process that does not justify the application, even for countries that have some Institutional capacity.

On another level, Civil Society Organizations are also subject to a similar process when applying for Climate funding from National Development Banks, National Implementing Agencies and even Multilateral Development Banks. At the local level, Civil Society Organizations and Grassroots Groups are often leading the efforts of implementation for many projects. Quite frequently, projects led by CSOs are regarded as reference in terms of effectiveness, and are those that better represent people's concerns. Nonetheless, due to their level of informality and lack of infrastructure, some CSOs are not even within the "funding ecosystem" at the national level. Frequently, more robust organizations are also not able to access funding due to their lack of capacity and/or due to the complexity of the requirements compliance form the donor institutions.

Civil Society Institutions, especially those that are based on the ecosystem in which they operate, such as the Amazon Forest, lack a number of features that constrain their development and considerably diminish the array of funding options at their reach – putting them in a vulnerable position.

Civil Society Organizations often present a number of cross-cutting institutional gaps. Among the most frequent ones, we could highlight: i. Human Resources, which refers to the general lack of staff and skills. Often the CSO team does not have personal with finance or accounting skills and have to rely on interns or volunteers to manage the bulk of their paperwork; ii. Fund Raising and Resource Management; few CSOs have people dedicated specifically to fundraising and have proper financial systems and provide a high level of auditing of their disbursements; iii. Strategic Planning; most the CSOs have limited capacity to provide clear audited accounts from its projects and from the organization for longer than 3 years. Furthermore, their staff generally has a high turnover rate and their funding covers short-term projects – a combination that hinders any institution's long-term strategy.

Strengthening Civil Society Institutional Capacity could prove to be an interesting solution for decentralizing the funding distribution and for reaching alternative and innovative projects. More capable CSOs are instrumental to: engage in data collection on the field, identify priorities, establish greater coordination between other CSOs and even with the governmental agencies, build stronger coalitions and partnerships and hold the government accountable for their policies and provide better feedback.

Despite the fact that institutional capacity building activities are paramount for CSOs ability to access Climate Funds and to better implement their projects, many times this lack of capacity in following the donor's compliance requirements are born from the inefficiency of the public power (at all levels, local and federal) in providing the minimum access to civil services – this issue gains dramatic contours with CSOs operating in remote areas such as the Amazon Forest. The difficult access to notaries, burdensome bureaucracy and even lack of banking services create a significant barrier that even hinders CSOs capacity to reach the donor´s accreditation stage.

Confronted with this scenario, Blockchain applications could be useful to power solutions that could help bridging this capacity gap. Despite the aforementioned technology maturity issues, there already are relatively simple applications based on Blockchain that could help to target some of those problems. The technology features could be instrumental to both substituting several procedures in the accounting and management processes, such as tracking disbursement and financial audit, and also bypass the need for proximity to "physical" notary offices and banking agencies.

Designing Blockchain-based solutions could take the Direct Access and Enhanced Direct Access concepts to a new level. This alternative could be beneficial for both countries and implementing agencies trying to access climate funds from Trust Funds and from Civil Society Organizations trying to access it from governments and its agencies. There already are several developmental banks, such as the Brazilian Development Bank, that already have pilots on Blockchain applications, mostly for their internal operations, therefore creating solutions to facilitate the access to their funding programs should be the natural consequence.

b. Social Dimension

i. Civil Society Role and Addressing Needs

Blockchain, along with other emerging technologies, such as Internet of Things and Artificial Intelligence, is a part of the forthcoming Fourth Industrial Revolution, or the Digital Revolution. Each industrial revolution, until now, has caused considerable gains in production efficiency, economic expansion and even some social development. But they also generated negatives externalities by deepening income concentration, creating pockets of exclusion and alienating several economic sectors by making some professions obsolete.

Each Industrial revolution demanded a different approach from the governments and society to mitigate their consequences, ranging from expanding social protection networks, creating new legal codes, or even rethinking ethics and codes of conduct. The Fourth Industrial Revolution will

probably demand from us a similar trial, although probably the scale of its consequences should be unprecedented. The emergence and mass adoption of those digital technologies will definitely greatly impact our society – but they also have an unprecedented capacity to mitigate their own negative externalities. The Digitization phenomenon will play an important role in a wide range of areas, including education, health, security, energy, environment and climate change, humanitarian aid, microfinance, public services, governance, transparency and accountability, to state a few.

In fact, digital technologies have become a powerful tool for the civil society organizations that manage to exponentially increase their ability to collect data, monitor, oversee, disseminate and mobilize the society – activism has reached a whole new level. They also create a very fertile environment for mass collaboration, which allows a higher level of social engagement. The Blockchain technology, in particular, is well positioned to allow the population and the organized civil society to participate in and address some government weakness. Blockchain-based solutions could guarantee transparency and security to applications/initiatives that would allow citizens to monitor public policies or project results and provide feedback for impact assessment. Here, the Blockchain technology could contribute in both ends. It could first be used by the government as a platform where the results of a given social policy are registered, making it available for the society´s oversight. This contribution would ensure: transparency, accountability, security and quality of data. In the other end, a Blockchain-based solution could offer a decentralized platform where citizens could input their feedback in a safe and reliable way, while making it available to others.

Another interesting contribution would be in the financial realm. Blockchain technology is well positioned to foster the development of initiatives that are able to empower social and solidarity-based finance. One of the major tenets behind the Bitcoin project is the idea of empowering people by bringing them together in a peer-to-peer process. That logic allows or facilitates the connection among the network participants, reducing the need for intermediaries, thus reducing transaction costs.

Using this logic, Blockchain-based solutions could power collaborative economy initiatives, such as developing cryptocurrencies coins to foster local economies. Alternative local cryptocurrencies could be issued by local governments or a funding entity, in order to ensure that the resources of a given funding would only be able to circulate within a given community – between the local recipients of the program and the accredited local business. This would address two complex issues that usually constrain this type of initiative: falsification of the local currency or hefty fees charged by banks or financial institutions to operate the project resources. That solution is closely connected with a famous Blockchain-based application that has already several pilot projects, especially in the Middle East and Africa – that is: addressing the Unbanked problem.

To date there are still hundreds of millions of people that do not rely on banking services to meet their daily needs. Unable or unwilling to have banking accounts, those people are somehow marginalized from the financial system and consequently are able to access many financial services. Here, the crypto currencies are well positioned to "bank the unbanked" by offering the possibility to make financial transactions through online cryptocurrency exchanges, smartphone apps and even directly through their virtual wallets. Currently, it is even possible to identify several startups that are developing applications that offer financial services for cryptocurrency owners, such as micro-credit and insurances.

A third financial possible contribution is regarding new fundraising alternatives. The Blockchain technology could enhance existing models such as the crowdfunding, adding transparency and traceability to the process. Additionally, it generates new funding models, such as the Initial Coin Offerings (ICO). Popular especially among startups that generally have difficulties in raising money through traditional financial institutions, the ICO initiatives allow those startups to circumvent intermediaries and regulatory compliance. Originally created to allow 'fans' and supporters to fund a given project, the ICO generally works by selling a token that, once the project is launched, would represent a cryptocurrency of a functional unit to be used in project service or platform. The ICO solution became popular in 2017 by raising billions of dollars for several hundred different projects. Half of those were unable to live

for more than six months. The lack of regulatory compliance and institutional oversight permitted many weak projects and scams to have easy access to those resources. Due to its young age and novelty, the ICOs are still a risk and vulnerable application; nonetheless if proper enabling regulations are adopted, ICOs could prove to be a powerful tool for civil society groups and startups to access resources that are generally out of their reach.

Aside from fostering direct social action and participation, Blockchain technology could address people's need through helping development aid programs, both public and private. Development aid experts have long drawn our attention to several issues that had hampering aid efforts and reducing their impact of the recipient communities. Among them: corruption, the large number of intermediaries, the overlapping among different donors, etc. are some of the commonly highlighted issues. In that sense, more and more aid experts have being turning their attention to possible contributions that the Blockchain technology might have to offer to mitigate the hurdles that have been challenging development aid programs (Pisa and Juden 2017). Blockchain solutions could also have a positive impact on aid distribution systems and logistics and enhance its auditing capabilities.

The ongoing digital technology revolution has already provided certain baseline conditions for Blockchain solutions to advance, such as the evolution in the mobile phones, especially the mass adoption of smartphones and the increasing coverage of the internet, sometimes even in remote areas. There are already projects using existing technologies that are trying to alleviate poverty and financial inclusion, through offering financial services via smartphones with considerable success (Konner 2017). The adoption of Blockchain might increase the efficiency, scale and cost-effectiveness of such projects.

Within the UN System, the World Food Program (WFP) has taken the lead and has been developing Blockchain solutions for several years. One of its flagship projects, called Building Blocks, uses the technology to power a cash transfer program aimed to aid Syrian refugees In Pakistan. The Project objective is to empower its participants by allowing them to make their own decisions regarding ways to alleviate hunger. Despite the original objectives of create a safer, faster, cost-effective and empowering tool, the project also managed to authenticate and register all the transactions that used the program resources, therefore creating a trustworthy database that now would give the WFP material to better prepare future programs (United Nations World Food Program Innovation Accelerator Annual Report 2017).

Currently, there are other UN Agencies that are also developing their pilots powered by the Blockchain Technology. Among them, it is worth mentioning the United Nations Office for the Coordination of Humanitarian Affairs (OCHA), the United Nations Children's Fund (UNICEF), the UN Women and the newly-launched Climate Chain Coalition.

c. Political Dimension

i. Trust and Advocacy

Money, stocks, bonds and other financial assets, deeds, votes and identities are different kinds of assets with a common ground: public institutions have to originate, register or protect them to some extent. One step ahead, the transaction involving them are even more important to global economies, and as Blockchain emerges as a real trend with large potential to disrupt many of them it starts to gain attention from governments, lawyers and others. Financial regulators have been taking steps to understand everything involved in these changes:

> *"The Bank of England's top economist, Andrew Haldane, has proposed a national digital currency for the United Kingdom. The Deputy Chief of the Bank of Russia, Olga Skorobogatova, said that it was "time to develop national cryptocurrencies", and the People's Republic of China has been experimenting with Ethereum to develop digital Yuan. However, governments around the world are uncoordinated in their approach to blockchain - some favoring laissez-faire policy [...]. Some regimes are openly hostile, increasingly a fringe response. Even those stakeholders who resist government intervention acknowledge the merit of regulator participation in governance debates." (WEF, 2018).*

Moreover, it is important to emphasize that there is a growing policy network emerging. Coin Center is a nonprofit established in Washington DC with the aim to focus on how cryptocurrencies can foster innovation, consumer protection and privacy, at the same time as they combine their advocacy with a strong research on anti-money laundering and know-your-customer practices. The Chamber of Digital Commerce is a trade organization focused on the acceptance and use of digital currencies, something critical when they started their activities in 2014:

> *"The US Senator was calling for a ban on bitcoin. [...]. Since then, the Chamber has made huge strides in educating the community. 'In the past 12 months, we have held over 100 briefings for policy-makers at the state, federal and international level. Today, we have many bitcoin and blockchain champions across the world's policy community; we even have a Congressional Blockchain Caucus.' The United Kingdom has its own Digital Currency Association, as does Australia and Canada, who speak for industry. Promoting and uniting many strong voices in the policy arena will ensure that blockchain has a better chance of fulfilling its potential." (WEF, 2017)*

As also pointed out by the World Economic Forum's recent report on Blockchain Technologies, hopes that the Blockchain communities will share everything they have been learning so far will guide developers and policy makers with regard to what needs to be fixed in the architecture of these decentralized networks. Knowledge networks are presented as the support for this, especially for what they give in terms of potential specifications for the whole markets of distributed ledger technologies.

In this context, the COALA network is an interesting initiative, whose research aims "to ensure that Blockchain-based applications operate in the current regulatory framework and interact with existing institutions governed by the rule of law". Their list of achievements includes the following Blockchain based projects:

COALA-ID:
A framework for credential management and access control in collaboration with MIT;

COALA LEX:
An interface between smart contracts and legal contracts to bridge the gap between traditional legal frameworks and Blockchain technologies.

Elethron:
Blockchain-based system for renewable energy trading in collaboration with the Commonwealth Bank of Australia and Hewlett-Packard

The Coalition intends to elaborate upon "meta-languages for hybrid techno-legal agreements" and develop "an open-source library of standardized and certified smart contract modules". It has representation in technical standards setting bodies such as W3C and IETF, and has partnered with Harvard, Stanford, Cambridge and Oxford universities, University of California at Berkeley, University College London, National Center of Scientific Research, and Hong Kong University of Science and Technology. This fact shows how scientific-driven and factual research institutions have been seriously embracing partnerships in the Blockchain ecosystem, in hopes of addressing its challenges and spreading its real benefits.

ii. Power and Privileges

Where the internet democratized information, the blockchain democratizes value and cuts to the core of legacy industries like banking. It also pertains to the management of money, wealth, intellectual property and other forms of value for which many societies expect government to protect the public interest. So we need to acknowledge that, while governments and regulators alone lack the knowledge, resources and mandate to govern this technology effectively, government participation and even regulation will likely have greater influence over blockchain technologies to ensure that we preserve both the rights and powers of consumers and citizens. People in free societies have the right to free speech and have the power to express it on the internet of information but not the power to protect it from piracy, hacking or censorship. One of the defining characteristics of an open permissionless blockchain is that no one has the right to anything. There are really just powers, what you have the power to do, what you can do. (WEF, 2017).

With regard to Blockchain technologies, people will have the power to express themselves and preserve their expression without many of the possible restrictions and constraints of other digital means. But these differences do not require government to control, oversee or somehow govern the Blockchain applications, because distributed ledgers are and must be distributed. Therefore, power is also distributed.

The World Economic Forum approach presented in their latest report on the topic recommends self-organizing, bottom-up and multi-stakeholder governance as a way to control Blockchain. According to Primavera de Filippi, faculty associate at the Berkman Center for Internet & Society at Harvard and a permanent researcher at the National Center of Scientific Research in Paris, the absence of a formalized governance structure has two possible effects: either Blockchain-based communities have to be acting and reacting expeditiously or else informal and invisible power dynamics emerge, often more centralized than they appear. Which means that invisible powers could be emerging if these technologies are not built on top of sovereign governance systems.

iii. Rules and Bureaucracy

By being tamper-proof in practice and adding by default a high degree of transparency regarding the data it carries in its blocks, Blockchain can become a strong ally in the accessibility of government information at its different levels. More innovative uses of Blockchain technology in the public sector can make room, for example, for greater citizen participation in the political process at different levels. As a digital and open platform, it supports accountability in political and voting systems. By allowing the registration of signatures on a reliable, immutable and verifiable database, it enables support for petitions, traceability of public money and creation of online proposals for participatory budgets. This idea can also be applied to multi-annual plans of budgeting or in the financial dimensions of electoral campaigns, for example. In the private sector, smart contracts could be used to automatically ensure that companies are acting in accordance with current legislation, guaranteeing compliance in a much more efficient way.

We should once more emphasize, however, that smart contracts both define and manage ownership rights without subjective or additional interpretations other than the ones hardcoded. Their code makes no assumptions about the assignment of rights, and code cannot arbitrarily seize, divest or transfer these rights. For example, if during the process of land registration, government officials assigned the ownership of a parcel of land to someone who was not the legal owner of that parcel, that person would have absolute sovereignty over the parcel, and the legal owner could not simply reverse the assignment. Right now, there is a lack of legal recourse in a world of irrevocable transactions and unavoidable smart contracts. According to researchers De Filippi and Wright, “people are, indeed, free to decide the particular set of rules by which they want to abide, but - after the choice has been made – may no longer deviate from these rules”. It delivers greater efficiencies and effectively eliminates nonperformance risk because we have no choice to breach, no choice of damages. But that is also a potential downside and should be used carefully.

6

Recommendations

The overall aim of the present report was to introduce the debate on the possible contributions that the Blockchain technology could offer to the Climate Finance environment, bridging the gap between Blockchain experts and the Climate Finance community of practitioners.

The report benefited not only from research, but also from interviews and especially from two workshops that gathered experts on both fields. By having an introductory nature, this report does not provide conclusions, but offers concrete recommendations – divided into several areas. The main idea here was to propose initiatives that would cover a wide array of players, such as the Climate Trust Funds, Multilateral and National Developmental Banks, Implementing Agencies, Governments, Business (and startups) and Civil Society Organizations.

a. Bridging the Institutional Gap

Bridging the gap between recipients and donors could be one of the most important and representative contributions that Blockchain-based solutions could offer to Climate Finance. A major obstacle in connecting the funding sources to the recipient players (either a country or a Civil Society Organization) is the institutional and technical capacity gaps presented by some, which represents their difficulties to access funding due to their limited capacity to comply with the Climate Funds compliance standards.

In this context, Blockchain applications could be applied to **improve direct access and enhanced direct access concepts**. For instance, the development of a **toolbox** could simplify the compliance standards processes for certain funding modalities, making it easier for recipients to access the funding. This example of solutions would not only be beneficial to the recipient, but also to the Donor that could include in this toolbox important features, such as the project impact assessments and monitor elements. By adopting Blockchain-based solutions, it would also be possible to reduce the number and the scope of action of the intermediaries, which in the end would also diminish the transaction cost of the projects.

b. Strengthening the Political Debate

Blockchain, as any emerging technology with comprehensive applications, is often subjected to a certain degree of distrust and doubt. Quite frequently, some of the early users take advantage of the unregulated scenario to engage in questionable or illegal activities. That dynamic tends to weaken the position of emerging technologies toward legislators.

Therefore, Blockchain technology is currently in a transition process. At this point, it is highly important to **foster an informative and high-quality political dialogue** with public authorities and legislators, in order to stimulate **enabling legislations** rather than only prohibitive ones. That would be the case of ICOs. Prohibitive regulations would create disincentives to innovative ways of alternative funding – which could address the needs of groups marginalized from the Climate Finance environment and traditional financing sources.

Blockchain-based solutions could be instrumental in fostering Transparency, Accountability and Answerability from the governmental authorities, prompting them to be more responsive toward public demands.

c. Enhancing Civil Society Role

One of the original concerns of the Blockchain technology was how to enhance the role of the civil society. Decentralization is a key feature of the technology, which enables us to develop a number of solutions designed for large groups, therefore creating value for the communities.

One interesting solution could be the development of a **feedback application** in which the civil society could monitor and evaluate the process of a given public policy or a project in a transparent and trustworthy manner. This solution could not only give voice to the affected community, but also generate need information for the evaluation of the policy or program.

Blockchain based solutions could also **balance power relations** in some localities, where small players have difficult access to certain services due to the monopoly of interested groups or associations. Using cryptocurrency, utility tokens and even designing a platform to build a virtual marketplace could provide a useful alternative to avoid this concentration of power.

However, innovative solutions could also enhance the **inclusion of groups in remote areas** that are usually in the margin of the climate finance environment. The design of solutions to "bank the unbanked" is key to give access to bank account, financial and notary services. Startups are already developing Apps for smartphones that near substitute physical bank branches and the need to sign paper contracts. Those advances would greatly enhance the inclusion of small Civil Society Organizations and indigenous people.

d. Fostering New Solutions

Allied with other emerging technologies, such as the Internet of Things and Artificial Intelligence, Blockchain technology is currently well positioned to power a number of solutions to present-day obstacles, or even increase the efficiency of established mechanisms.

The **development of new financial services**, either using cryptocurrency or the technology to build platforms, is an obvious place to start the Climate Finance environment. A second possibility is using the Blockchain technology to **enhance Know Your Costumer (KYC) processes**. Insurance companies, in particular, are already exploring this option to reduce the risk of fraud and corruption and to **enhance their compliance standards**.

Blockchain technologies could also greatly enhance the means to operate **crowdfunding projects** and **reward systems**. Regarding rewarding systems, a given project could reward players for behaving in a certain way, by compensating them with an utility token to be used for a specific purpose (Amazon landowners could be rewarded with utility token for preserving a larger part of their properties). This sort of solution has the added value of allowing the project manager to keep transparent and trustworthy records of all the transactions using the token; this would not only reduce corruption but also generate valuable information that might be used to enhance the project.

Initial Coin Offerings (ICOs) are a very innovative and new format to engage in crowdfunding activities. They could be used by smaller startups and Civil Society Organizations to raise money for their projects, bypassing the obstacles posed by traditional funding sources. A word of caution is need here – ICO is a very new funding scheme, therefore it is not regulated by most countries, with some having even prohibited it. It is advisable to check the host country regulations to avoid legal hurdles.

e. Caveats

Despite the original idea of the Blockchain technology having been to empower the civil society, it still only a technology, thus it is not virtuous in essence. Therefor a fundamental element of the Blockchain tech is its **governance** – the set of rules, determined by the technical code, that will ensure its functioning. The Governance of a given application is what determines the participants of the network, the reward system, what information to record, etc. Therefore, a key element when developing a Blockchain application is to keep in mind the importance of designing its governance, in order to curtail future power relations complications and disincentive its use.

A second important caveat concerns Blockchain´s applications that could reproduce old system problems, such as the **gatekeeper concept**. Depending on its governance rules, a given application could provide some participants with "filtering" powers, thus becoming gatekeepers of the network. Such power is more concerning in decentralized platforms in which all participants are to partake in the network sharing information/transactions freely.

f. Collateral Benefit

Beyond the already mentioned benefits that the Blockchain technology might offer to the Climate Finance ecosystem, it is possible to also identify "collateral benefits" that are not directly related to the technology, but would be fostered by its adoption.

The first relevant collateral benefit is the **digitization** of documents. In many cases, much of the documentation derived from process, be it a country or Civil Society Organization, is still in paper. That is especially true for smaller and more remote CSO and least developed countries. The application of Blockchain-based solutions would foster incentives to the digitization of those documents, thus enhancing security against mistakes, corruption and loss of information.

A second collateral benefit related to the Climate Finance environment is the debate concerning the **definition of assets**. The definition of what is an asset and which could be owned, traded or shared still is quite controversial. These definitions are paramount to the adoption of the Blockchain technology. An example would be to consider carbon as an asset – by consequence, the Blockchain technology could power applications that would contribute to the functioning of the Carbon Market.

7

Glossary of Concepts and Players

Sustainability Glossary

Adaptation

Adaptation comprehends a range of activities that are intended to reduce the vulnerability of human and natural systems to the consequences of the climate change. They generally aim to increase the capacity and resilience of those systems in order to adjust to the unavoidable impact of the climate.

Additionality

The term Additionality generally causes some confusion, since it could have two different meanings, both related to climate change. The first refers to its relationship with the ODA. The idea of Additionality here indicates the additional amount of resources, in excess of the ODA, that would be destined from developed countries to developing countries to fund mitigation and adaptation projects. The logic behind it is to prevent the ODA money from being relocated to climate change initiatives.

The second meaning of Additionality is related to emissions offset. It determines that Additionality is the amount of emissions reduced as a result of a given project – compared to the baseline assumption of the project. That means that whenever a project generates an impact by reducing the emissions, it would have Additionality. The main challenge here is the future calculation of the Additionality, since it is only present if it is attested that the emissions would not have been reduced regardless of the implementation of the project.

Carbon Credits/ Carbon Markets

Carbon credit refers to a certificate or a permit that allows its holder to emit 1 ton of carbon dioxide (or the equivalent of a different greenhouse gas) in excess of the holder's original quota. That is because this permitted amount given by the carbon credit is being offset elsewhere. The idea is that some players may acquire/buy credits in carbon markets from other players that are not using their allowance.

Climate Debt

Climate debt refers to the idea that developed countries owe to developing countries for having being the leading players that caused the imbalances in climate change (due to their disproportionate emissions) that impacts the latter more severely. This concept works through two elements: Adaptation debt, which stands for the compensations that developing countries should receive for the damages suffered and lost opportunities due to the current climate change environment. The second element is the Emission Debt, which refers to the compensation that developing countries should receive for not being able to use its "share of atmospheric space", since the emissions from the developed countries already taken most of the finite atmospheric space.

Climate Funds

Climate Funds are the mechanisms created to administer resources for climate finance and fund projects and initiatives in this area. They may be multilateral, bilateral and even national.

Conference of the Parties (COP)	COPs are annual conferences organized by the UNFCCC to assess the progress of the international efforts to cope with climate change. Often, during the COP meetings the parties negotiate agreements and protocols that determine obligations to the parties. One of the most famous actions born within the COP meetings was the Kyoto Protocol.
Mitigation	Mitigation refers to initiatives that aim to mitigate climate change consequences, by reducing the greenhouse gas emissions and preserving the environmental features that absorb carbon from the atmosphere. Mitigation projects intend to reduce the speed of the climate change and, therefore, ease its impacts on the environment.
Nationally-Determined Contributions (NDCs)	The NDCs are self-imposed targets of GHG emission reduction determined by countries in the run-up to the COP 22 in Paris 2015. It was the first time that developed and developing countries alike committed to defined targets of emission reduction under the UNFCCC.
United Nations Framework Convention on Climate Change (UNFCCC)	UNFCCC is an international treaty signed during the Rio 92 Summit, the object of which was the stabilization of the greenhouse gas concentration in the atmosphere, resulting from manmade interference, in order to prevent drastic climate imbalances. Despite the fact that the Convention does not have binding limits for emissions, it sets an outline for protocols and agreements that are often achieved in the annual meeting of the Convention parties, the COPs.

Blockchain Glossary

Asymmetric Cryptography (Public and Private Keys Cryptography)

Using what are called public and private key pairs, this technology allows a message to be encoded so that it becomes readable and/or assigned by specific parties. To do this, we only need to address it to a certain public key, known and associated with the person in question, making decoding possible by using the corresponding private key.

Hence the concept of inseparable pairs of keys, as in a (public) safe in which money could safely be deposited, certain that only its legitimate holder has the (private) key needed to open the padlock that protects it. This last example helps in understanding how the operation of cryptographic applications goes far beyond "keeping secrets", in the ordinary sense of the term. It can represent a crucial dimension for the integrity of information in systems that digitally ensure the operationalization of digital currencies, utility tokens, identities and smart contracts.

Blockchain

Public ledger containing the transaction history that is verified and stored by all the machines in the decentralized network that maintains it. The computational power is what allows this ledger to be reliably updated with its multiple copies knowing when to add trustworthy information and when to reject incorrect or fraudulent data. Transaction blocks have cryptographic links to ensure the order of transactions. It is impossible to change information recorded in one block without changing all subsequent blocks. This makes cheating unfeasible. In a general sense, it refers to a database organized in a decentralized way, with multiple copies distributed automatically, which are constantly being updated with new information, synchronized with the other copies and integrally ensured by powerful distributed networks. The term "Blockchain" is commonly used to describe both this innovative database and the technology that makes it work without depending on a particular company, entity or individual.

Consensus

A term that refers to the way in which transactions in a Distributed Ledger are validated and truth is periodically established, so that everyone has the same information as valid, and inconsistent information is rejected beforehand. This may be done automatically, according to the rules of one or more protocols.

Consensus Algorithm

Algorithms specifically designed to perform the tasks associated with the validation process in a Blockchain, running in form of a computation code through all the nodes that are part of the network. Variations of these algorithms include Proof of Work (the one commonly attributed to the so-called resource-intensive mining process), Proof of Stake, Byzantine Agreement System and Federated Byzantine Agreement, among others.

Cryptoasset

A proof of right to something of value, represented in the form of a token in a Blockchain. It can be 1 bitcoin, 1 ounce of gold or anything along these lines.

Cryptocurrency

A digital representation of value designed to work as virtual money, where accounting and transactions are made possible by tools derived from applied cryptography, generally in the form of distributed ledger technologies (DLTs). In a broader sense, the term cryptocurrency can be understood as a computer protocol designed to establish a transactional and registering system for monetary values and its correspondent users. The current technologies in this category combine mathematical cryptography, open-source software, digital networks and economic incentive structures.

Cryptography / Encryption

In a broader sense, it represents the study of the principles and techniques by which information can be encoded and decoded. It is precisely the tools of cryptography that are responsible for taking information in its original form and making it unintelligible to any individual who intercepts it, with the exception of one or more previously defined recipients. In general, the recipient is understood to be the holder of a "secret key", capable of unraveling the encrypted message. Without this key, it is impossible to derive the original message from the unreadable data block resulting from the encryption mechanism.

Fintech

A "fintech", using the general term to name a company that works in this field, will be synonymous with a startup in the area of financial technology focused on growth in scale. If the fintech's focus is on a non-accelerated growth model, then it will be synonymous with a traditional company in the financial technology field. In both cases, however, an attempt is made to increase the efficiency of existing businesses in this industry, especially in relation to costs and deadlines.

Hash / Hashing Function

When we enter our password on various websites, for example, this data cannot be transmitted in its original state by the network, at the risk of any intermediary being able to see and use it improperly. To solve this problem, these data pass through a cryptographic hash function and only the information resulting from that process is transmitted later. It is known in the technical jargon as a hash function digest, and as a consequence of the points explained before, the only way to get to a given digest is to always re-enter the same data (in this case, your password); so that, from the same cryptographic hash function, the digest in question is generated.

That is, what sites store is never (or should ever be) a pure text list containing the passwords of its users, as this would be catastrophic in the event of a hacker attack or a leak. What you save is just a list of undecipherable digests, whose original data that generate them are unknown to the site, its employees, and the multiple intermediaries who process this information over the Internet. Therefore, the only way to authenticate a user is to require him to enter a secret (his password), in order to know if this data generates in the device of the individual the digest corresponding to his login, the only piece of information that the site has stored.

Ledger

A ledger is a way of producing consensus about the facts that are necessary for commerce to function. Ledgers are the basic transaction recording technology at the heart of all modern economies. In this sense, a Blockchain is a whole new approach to building and using ledgers, i.e. to producing consensus. Indeed, Blockchains are increasingly known as the distributed ledger technology (DLT). The new part is to have figured out the way to securely and effectively use distributed ledgers, and thus to produce consensus without requiring centralized trust, overturning the old technology of ledgers that needed to be centralized in order to be trusted. A block is a trustless distributed ledger. The significance of this new technology follows from the fact that modern economies and societies are ultimately built upon ledgers. Moreover, the institutional and organizational outline of a modern economy is to a significant degree a consequence of those ledgers needing to be centralized (i.e. in government, in layers of bureaucracy, in large corporations, etc.).

Node

The role of a node is to support the network by maintaining a copy of a Blockchain and, in some cases, to process transactions. Each cryptocurrency has its own nodes, maintaining the transaction records of that particular token and, in some cases, additional information like data for multiple purposes, like smart contracts.

Smart Contract

A concept first formulated theoretically in 1997: digital, computable contracts where the performance and enforcement of contractual conditions occur automatically, without the need for human intervention. In some cases, smart contracts represent the implementation of a contractual agreement, whose legal provisions have been formalized into computational code. Contracting parties can thus structure their relationships in a self-executing manner and without ambiguity. Reliance on computational code allows willing parties to model contractual performance and simulate the agreement's performance before execution. In other cases, smart contracts introduce new codified relationships that are both defined and automatically enforced by code, but which are not linked to any underlying contractual rights or obligations. To the extent that a Blockchain allows for the implementation of self-executing transactions, parties can freely transact with one another, without the technical need to enter into a standard contractual arrangement.

Startup

Startups are nascent companies marked by the capacity for large growth in scale, in a relatively short term and in general with fewer initial resources than traditional businesses. Contrary to what most people believe, a startup does not need to be necessarily related to technology, although it is the case of most of them, given the breakdown of borders and the logistical advantages of the digital economy.

Token

Unit of account registered and operable in a Blockchain. It can be a coin, a vote, a contract, etc.

Bibliography

AMANI, Sharon Mei. The Case of the United Nations World Food Programme's Purchase for Progress. PhD Dissertation. Arizona State University, May 2016. Available at: https://repository.asu.edu/attachments/170674/content/Amani_asu_0010E_16029.pdf

BAUMANN, Tom. Using Blockchain To Achieve Climate Change Policy Outcomes. IETA Insights. Available at: https://www.ieta.org/resources/Resources/GHG_Report/2017/Using-Blockchain-to-Achieve-Climate-Change-Policy-Outcomes-Baumann.pdf

BAUMANN, Tom. Using Blockchain To Achieve Climate Change Policy Outcomes. IETA Insights. Available at: https://www.ieta.org/resources/Resources/GHG_Report/2017/Using-Blockchain-to-Achieve-Climate-Change-Policy-Outcomes-Baumann.pdf

BHEEMAIAH, Kariappa, Why Business Schools Need to Teach About the Blockchain. February, 2015. Available at SSRN: https://ssrn.com/abstract=2596465

Blockchain: projects and products from ITS Rio. July, 2018. Available at: https://itsrio.org/en/projetos/blockchain-projects-and-products-from-its-rio/

BUCHNER, Barbara K; OLIVER, Padraig; WANG, Xueying; CARSWELL, Cameron; MEATTLE, Chavi; MAZZA, Federico. Global Landscape of Climate Finance 2017. Climate Policy Initiative. CPI Report, October 2017. Available at: https://climatepolicyinitiative.org/wp-content/uploads/2017/10/2017-Global-Landscape-of-Climate-Finance.pdf

CHEW, Bruce; WHITE, Mark; KILLMEYER, Jason. Will blockchain transform the public sector? Blockchain basics for government. Deloitte University Press, 2017. Available at: https://www2.deloitte.com/content/dam/insights/us/articles/4185_blockchain-public-sector/DUP_will-blockchain-transform-public-sector.pdf

Cryptocurrencies: looking beyond the hype. BIS Annual Economic Report 2018. May, 2018. Available at: https://www.bis.org/publ/arpdf/ar2018e5.pdf

DE FILIPPI, P. and Wright, A. Blockchain and the Law: The Rule of Code. Cambridge, Harvard University Press, 2018.

DE FILIPPI; Hassan, Blockchain Technology as a regulatory technology: From code is law to law is code, First Monday. December, 2016. Available at: http://firstmonday.org/ojs/index.php/fm/article/view/7113/5657

DRUCE, Laura; GRUNING, Christine; and MENZEL, Carola. Key messages on direct access to international. Policy Brief, Frankfurt Scholl and UNEP Collaborating Center, July 2013. Available at: http://fs-unep-centre.org/sites/default/files/project/1/policy_brief_direct_access.pdf

FORSTATER, Maya. Towards Climate Finance Transparency. Aidinfo Report, 2012. Available at: http://www.publishwhatyoufund.org/files/Towards-Climate-Finance-Transparency_Final.pdf

Groupe Speciale Mobile Association (GSMA). Blockchain for Development: Emerging Opportunities for Mobile, Identity and Aid. GSMA Report, 2017. Available at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/12/Blockchain-for-Development.pdf

KO, Vanessa and VERITY, Andrej. Blockchain for the Humanitarian Sector: Future Opportunities. Digital Humanitarian Network and UN-OCHA Report, 2016. Available at: https://drive.google.com/file/d/0B--8okvw4smiNnFEWjF1M2NSaW8/view

LEE, Judith et al., Blockchain Technology and Legal Implications of 'Crypto 2.0', 104 Banking Rep. (BNA) No. 654, at 4. March, 2015.

LESSIG, Lawrence. Code and Other Laws of Cyberspace. Ed. Publishing Systems PTY, 1999.

PISA, Michael and JUDEN, Matt. 2017. "Blockchain and Economic Development: Hype vs. Reality." CGD Policy Paper. Washington, DC: Center for Global Development. https://www.cgdev.org/publication/blockchain-and-economic-development-hype-vs-reality

Satoshi Nakamoto. Bitcoin: A Peer-to-peer Electronic Cash System. October, 2008. Available at: https://bitcoin.org/bitcoin.pdf

SCOTT, Tracie; POST, Armand L.; QUICK, Johnny; and RAFIQI, Sohail (2018) "Evaluating Feasibility of Blockchain Application for DSCSA Compliance," SMU Data Science Review: Vol. 1 : No. 2 , Article 4. Available at: https://scholar.smu.edu/datasciencereview/vol1/iss2/4

SZABO, Nick. Smart Contracts: Formalizing and Securing Relationships on Public Networks By First Monday, Volume 2, Number 9 - 1. September, 1997. Available at: http://ojphi.org/ojs/index.php/fm/article/view/548/469

Transparency International. A Tale of Four Funds. Transparency International Report. 2017. Available at: https://www.transparency.org/whatwedo/publication/a_tale_of_four_funds

United Nations Development Programme. A Capacity Assessment of CSOs in the Pacific. UNDP Pacific Centre Report. 2009. Available at: http://www.undp.org/content/dam/rbap/docs/Research%20&%20Publications/democratic_governance/UNDP_PC_DG_A_Capacity_Assessment_of_CSOs_in_the_Pacific.pdf

United Nations World Food Programme Innovation Accelerator. Annual Report 2017. Available at: https://innovation.wfp.org/year-review-2017/docs/WFP-innovation-accelerator-2017-annual-report.pdf

Wood, Gavin. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. February, 2015. Available at: http://gavwood.com/paper.pdf

WORLD ECONOMIC FORUM, Realizing the Potential of Blockchain, A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies, White Paper. June, 2017. Available at: http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf

WRIGHT; De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia, March, 2015. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664

Websites:

https://ethereum.org
https://www.bvrio.org
https://www.carbonx.ca
https://powerledger.io
https://www.mudamos.org
https://www.bitcoindesigned.com

Image and Source References:

Front cover: < Earth Blue Planet > by WikiImages. Licenced under Creative Commons CC0 via Pixabay - https://pixabay.com/photo-11015/

Page 13: < Landscape of Climate Finance in 2015/2016 > by Climate Policy Initiative - https://climatepolicyinitiative.org/wp-content/uploads/2017/10/171026-GLCF-Sankey@4x.png

Page 16: < Shepherds Flat Wind Farm, Oregon, USA, seen from the Empire Builder train route. > by Steve Wilson. Licenced under CC BY 2.0 via Wikipedia - https://en.wikipedia.org/wiki/Renewable_energy#/media/File:Shepherds_Flat_Wind_Farm_2011.jpg

Page 20: < Blockchain Grid > by Davidstankiewicz - Own work. Licenced under CC BY 4.0 via Wikimedia Commons - https://upload.wikimedia.org/wikipedia/commons/thumb/2/22/Blockchain_Grid.jpg/800px-Blockchain_Grid.jpg

Page 23: < Trading with SimpleFX WebTrader > by SimpleFX. Licenced under CC BY 2.0 via Flickr - https://c2.staticflickr.com/2/1861/42659710630_bf58f06a42_o.jpg

Page 24: < Napster settings > by Christiaan Colen. Licenced under CC BY 2.0 via Flickr - https://c1.staticflickr.com/1/255/18409023820_c3ca9dc2ca_o.jpg

Page 30: < View over Lake Zug with the old town of Zug and the Zytturm > by Schulerst - Own work. Licenced under CC BY-SA 3.0 via Wikipedia - https://en.wikipedia.org/wiki/Zug#/media/File:Zug_Zytturm_1.jpg

Page 37: < Energy Consumption and Scaling Issues > by Annual Economic Report 2018 from BIS - https://www.bis.org/publ/arpdf/ar2018e/images/graph-V4.jpg

Page 44: < Blockchain in the public sector (as for march 2017) > by Deloitte and Fletcher School as Tufts University - https://cdn-images-1.medium.com/max/1600/1*Q4MLhOFb64Qcep145L_xjw.png

8

Annexes

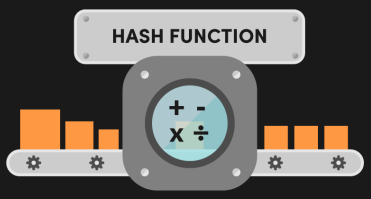
Educational Infographics

What is a hash?

bitcoindesigned.com

The hash function

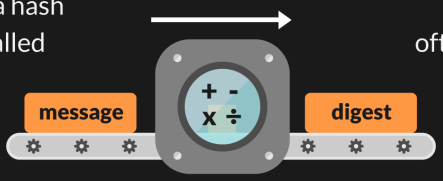
A hash function is a **math algorithm** that turns an arbitrarily-large amount of data into a **fixed-length representation**.



Hashes are usually written in a **hexadecimal** notation.

Decimal:
10000000000000
↓ to hexadecimal
9184E72A000

The input data to a hash function is often called the **message**.



And the output is often called **digest** or simply **hash**.

What about a cryptographic hash?

A cryptographic hash function is a **special class of hash** function with useful properties for cryptography.

Besides the usual hash features, here are some **extra properties** of an ideal cryptographic hash function:

Efficient

It is quick to compute the hash for any given message.

Trap-door

It is infeasible to calculate a **message from its hash**.

No collision

it is infeasible to find two **different messages** with the **same hash**.

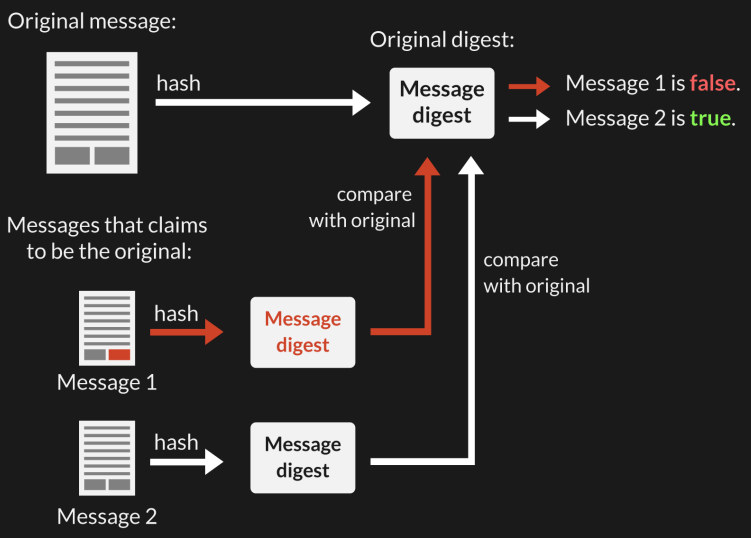
"Unbreakable"

it is resistant to all **known** crytoanalytics attacks.

Some of the applications

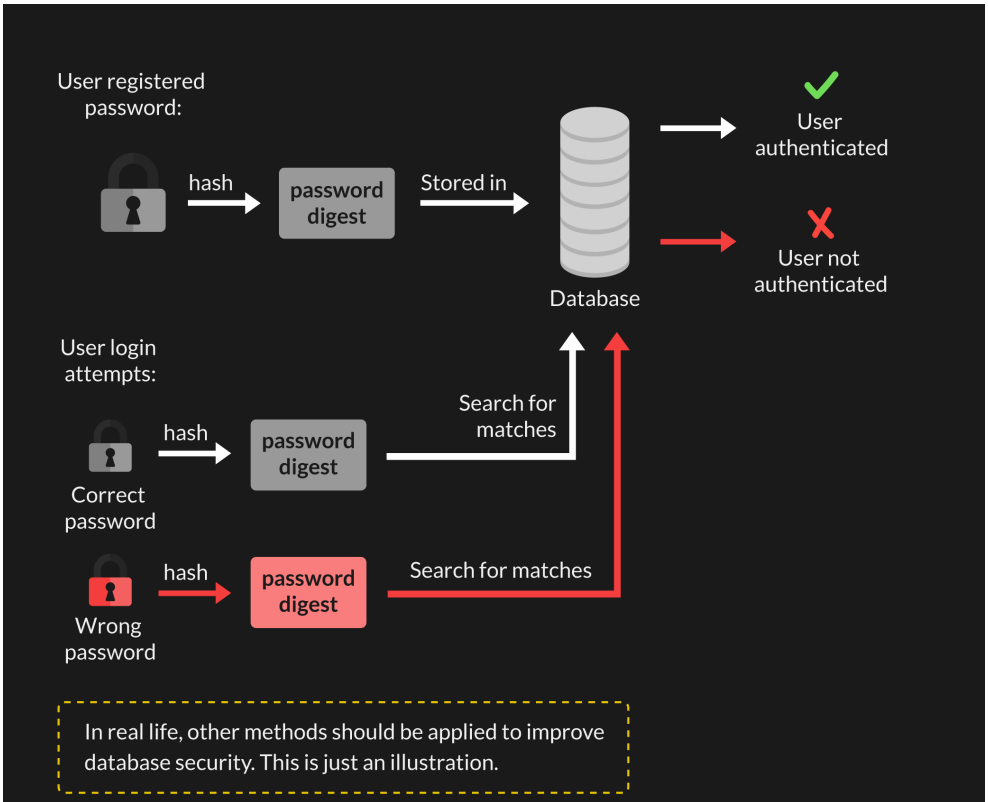
Verifying the integrity of files or messages

If you calculate the hash of a message in the moment of its creation and anytime after, you'll be able to verify the content integrity. If one byte has been altered, the two hashes will be completely different.



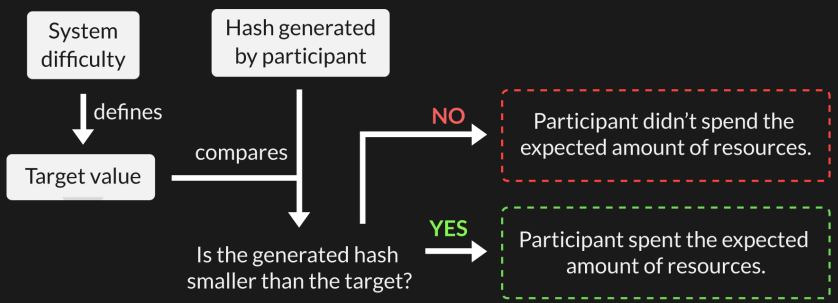
Password verification

Storing plain passwords in databases is extremely insecure. If you store the hashes of passwords, you can still authenticate the correct inputs, but if the database is compromised, the passwords will not be directly available for an attacker.



Proof-of-Work (PoW)

The generation of a cryptographic hash can be predictably costly, while the verification of the result is easier. With PoW, we want to verify if a participant spent an estimated amount of computational resource to perform an operation.



Bitcoin hash functions

Bitcoin uses two different cryptographic hash functions in its inner workings:

SHA-256

- Results in a 256-bit number. It means it's a really big number and it looks like this (just an example from a file in my computer):

  af7e22ad9fcc57e0104f1d7a084a009827a59708558cb69f5847c0be9bef3dae

- Used in mining as the Proof-of-Work algorithm and in the creation of bitcoin addresses.

RIPEMD-160

- Results in a 160-bit number. It's still large, but smaller than the SHA-256. Here's an example of how it looks:

  7c159364c3f2f03edc9e0aee508b5092c0f56a21

- Used in the creation of bitcoin addresses.

Some special paranoia...

In Bitcoin, everytime you use one of these functions you double it with an extra round of SHA-256; it's a security reinforcement.

This means that when you hear:

"Uses SHA-256 on X."

↓ It actually means:

Uses SHA-256 on X and uses SHA-256 again on the first result. Or, simply:

SHA-256 (SHA-256 (X))

"Uses RIPEMD-160 on X."

↓ It actually means:

First uses SHA-256 on X and then uses RIPEMD-160 on the first result. Or, simply:

RIPEMD-160 (SHA-256 (X))

Author: Patrícia Estevão

Editor: Marco Agner

Main sources:

https://en.bitcoin.it/wiki/Hash

https://en.wikipedia.org/wiki/Cryptographic_hash

https://en.bitcoin.it/wiki/SHA-256

Public Key Cryptography in Bitcoin transactions

bitcoindesigned.com

Public key cryptography is also known as **Asymmetrical Encryption** because it uses **2 different keys** – a pair of a public and a private key – instead of one to encrypt data.

Symmetrical encryption

Only 1 encryption key (both communicating parties have to know it)

When you receive a message:

Sender's message

Encrypts with key

Cipher text

Sends to

You

Decrypts with key

Message

Asymmetrical encryption

Public key (show to people you want to communicate with) + **Private key** (keep it a secret, only you know it)

When you receive a message:

Sender's message

Encrypts with your **public** key

Cipher text

Sends to

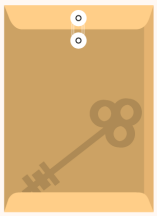
You

Decrypts with your **private** key

Message

The general goal of public key cryptography is to **prove you have a secret without having to show it** to anyone. And the secret is your private key.

Not having to share your private key is one of the advantages of this type of encryption.



Digital signature

When you use your private key to sign a message you create a **digital signature**.

That can prove the message was written by the **owner of the private key**.

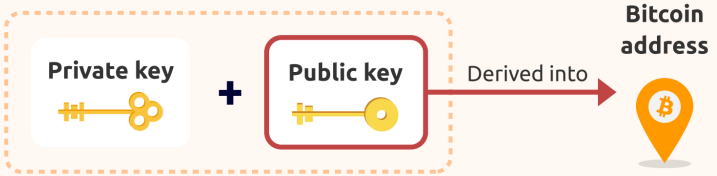
It's a type of **authentication**.

Bitcoin Address

The address we use in Bitcoin to receive money is actually a **derivation from your public key**.

When you send money to an address, you are saying "the bitcoins can be used by the **owner of the keys** correspondent to this address".

Bitcoin ownership:



Bitcoin Transactions

The most common type of Bitcoin transaction is called **Pay to Public Key Hash** (P2PKH), which basically means "**Pay to an address**".

A **transaction is essentially a message** that uses Public Key Cryptography to make sure the right person can unlock it.

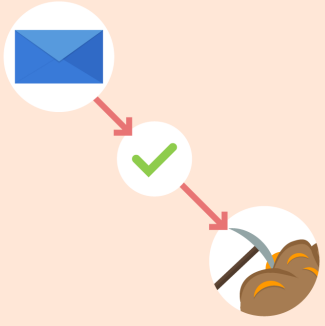
Payment to Bob:

So here's an example with the simplified dynamic of how Public Key Cryptography acts **in a Bitcoin P2PKH transaction**:

Bob sends you bitcoins:

Bob **"locks" the bitcoins** with the condition that the correct signature is presented.

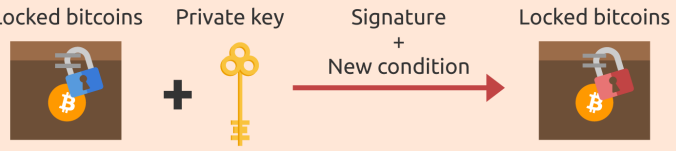
He transmits the transaction to the network.



The transaction is validated by network nodes and mined.

You spend the bitcoins:

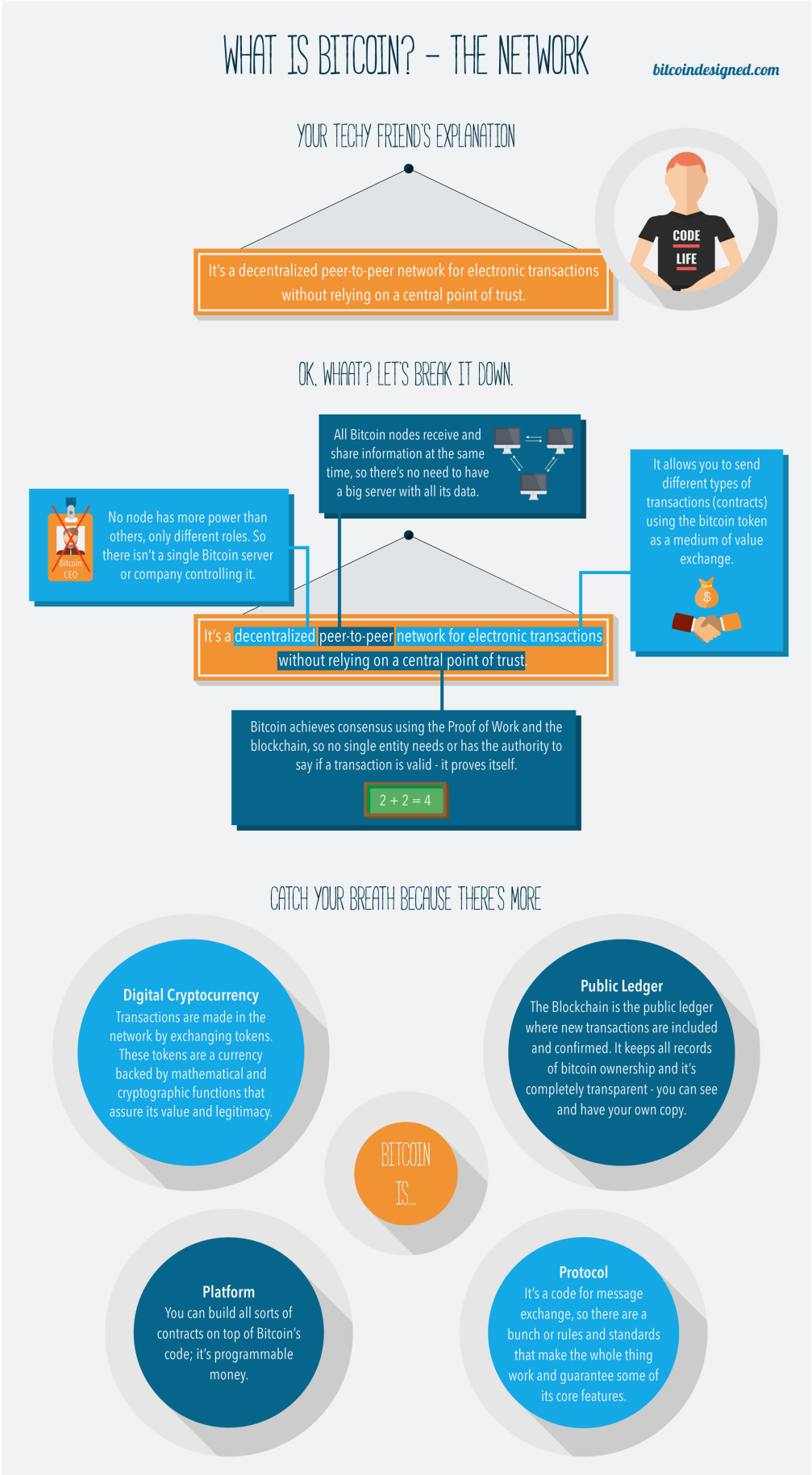
You unlock the bitcoins by **answering to the previous condition** (signing the transaction) and then you lock the funds with a **new condition** (that the signature of the recipient is presented).

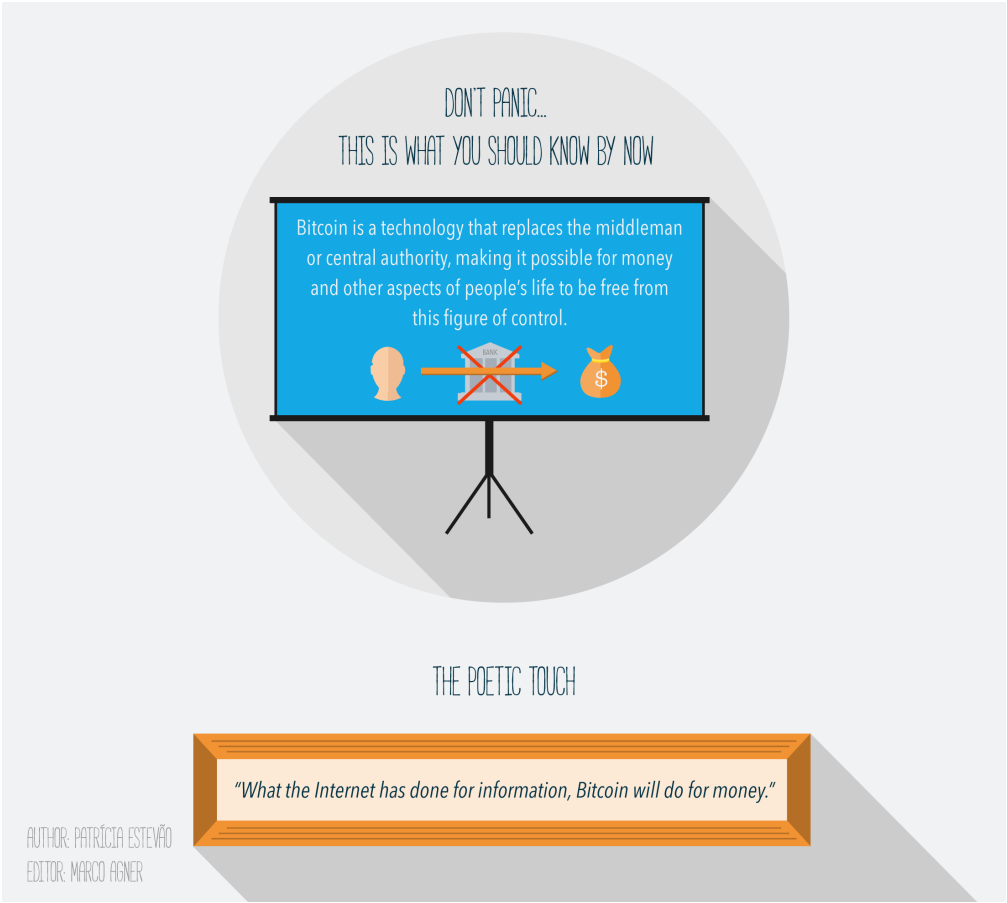


You transmit the transaction to the network.

The transaction is validated by network nodes and mined.

Author: Patrícia Estevão
Editor: Marco Agner
External source:
https://en.wikipedia.org/wiki/Public-key_cryptography


WHAT IS BITCOIN? - THE NETWORK
bitcoindesigned.com
YOUR TECHY FRIEND'S EXPLANATION
It's a decentralized peer-to-peer network for electronic transactions without relying on a central point of trust.
CODE
LIFE
OK. WHAAT? LET'S BREAK IT DOWN.
All Bitcoin nodes receive and share information at the same time, so there's no need to have a big server with all its data.
No node has more power than others, only different roles. So there isn't a single Bitcoin server or company controlling it.
Bitcoin CEO
It allows you to send different types of transactions (contracts) using the bitcoin token as a medium of value exchange.
It's a decentralized peer-to-peer network for electronic transactions without relying on a central point of trust.
Bitcoin achieves consensus using the Proof of Work and the blockchain, so no single entity needs or has the authority to say if a transaction is valid - it proves itself.
2 + 2 = 4
CATCH YOUR BREATH BECAUSE THERE'S MORE
Digital Cryptocurrency
Transactions are made in the network by exchanging tokens. These tokens are a currency backed by mathematical and cryptographic functions that assure its value and legitimacy.
Public Ledger
The Blockchain is the public ledger where new transactions are included and confirmed. It keeps all records of bitcoin ownership and it's completely transparent - you can see and have your own copy.
BITCOIN IS...
Platform
You can build all sorts of contracts on top of Bitcoin's code; it's programmable money.
Protocol
It's a code for message exchange, so there are a bunch or rules and standards that make the whole thing work and guarantee some of its core features.


DON'T PANIC...
THIS IS WHAT YOU SHOULD KNOW BY NOW
Bitcoin is a technology that replaces the middleman or central authority, making it possible for money and other aspects of people's life to be free from this figure of control.
THE POETIC TOUCH
"What the Internet has done for information, Bitcoin will do for money."
AUTHOR: PATRÍCIA ESTEVÃO
EDITOR: MARCO AGNER

Fundação Getulio Vargas
International Intelligence Unit

210 Praia de Botafogo – 12th floor
Rio de Janeiro
Brazil

https://iiu.fgv.br/

Konrad-Adenauer-Stiftung e.V. (KAS)
Regional Programme Energy Security and Climate Change in Latin America (EKLA)

Address: Calle Cantuarias 160 Of. 202
Miraflores, Lima 18 - Perú

Tel: +51 (1) 320 2870

energie-klima-la@kas.de
www.kas.de/energie-klima-lateinamerika/