

Blockchain



Unpacking the disruptive potential
of blockchain technology
for human development

WHITE PAPER



IDRC | CRDI

International Development Research Centre
Centre de recherches pour le développement international

Canada

Researcher and author

Raúl Zambrano

raul@ictdegov.org

International expert on technology and development, New York

Editing and research support

Ruhiya Kris Seward and **Phet Sayo**, Senior Program Officers from Networked Economies, International Development Research Centre

Design

Claudio Mendonca

ccmdesign.ca

The authors would like to thank Katie Clancy and Allie Wilson for proofreading and research support in the production of this White Paper.

August 2017

© International Development Research Centre 2017



Licensed under the [Creative Commons Attribution 4.0 license](https://creativecommons.org/licenses/by/4.0/)

The research presented in this publication was carried out with a grant from the International Development Research Centre, Ottawa, Canada. The views expressed herein do not necessarily represent those of IDRC or its Board of Governors.

Contents

EXECUTIVE SUMMARY	5
Blockchain technology	6
Blockchain applications	7
Blockchains and human development	9
Conclusions	12
Recommendations	14
1 INTRODUCTION	16
2 WHAT IS BLOCKCHAIN TECHNOLOGY?	18
Brief history	18
A look inside blockchains	21
Blockchain key traits	30
Blockchains limitations	31
3 BLOCKCHAIN APPLICATIONS	33
Public goods	34
Private goods	39
Conclusion	44
4 BLOCKCHAINS AND HUMAN DEVELOPMENT	45
Infrastructure and infostructure	46
Capacity development	46
Policy and regulation	47
Institutions	48
The governance of blockchains	50
5 CONCLUSIONS	53
6 RECOMMENDATIONS	55
Research	55
Programming	56
Networking and partnerships	56
ANNEX I: ANALYTICAL FRAMEWORK	57
ANNEX II: BLOCKCHAIN TECHNOLOGIES AND INNOVATION	59
ENDNOTES	68
REFERENCES	78

ABBREVIATIONS

Dapps	Distributed applications
DAO	Decentralized autonomous organization
DLT	Distributed ledger technology
DNS	Domain Name System
ICTs	Information and communication technologies
ICTD	Information and communication technologies for development
IP	Intellectual property and Internet protocol
PKC	Public key cryptography
SDGs	Sustainable development goals

FIGURES AND TABLES

Figure 1: Blockchain trends 2012-2017.....	19
Figure 2: Country interest in blockchain 2012-2017.....	20
Figure 3: Network typologies	21
Figure 4: Blockchain schematic representation.....	22
Blockchain 101.....	23
Blockchain for Development 101.....	24
Figure 5: Distributed ledger technology and blockchains.....	29
Figure 6: Bitcoin blockchain top miners market share 2017	32
Figure 7: Bitcoin blockchain hash rates Jan 2015-April 2017.....	64
Table 1: Blockchain types.....	28

Executive Summary

Technologies old and new are propelling the current wave of innovation around the world. Artificial intelligence, robotics and machine learning are all gaining new ground and being deployed in a wide variety of contexts globally. One of the more cryptic but oft-hyped technologies is blockchain, an emergent technology developed as part of Bitcoin, the cryptocurrency invented in 2008. Whereas Artificial Intelligence and robotics innovations seem to have a dark side, many perceive blockchain technology as a platform for positive and even radical change.



Yet for developing countries, the high sophistication and complex infrastructure requirements (bandwidth, connectivity and high operating costs) of this technology might prove challenging if countries intend to be active players and not just end users or consumers. Exploring the relevance of new technologies to address existing socio-economic gaps and support internationally agreed development targets including the globally-recognized Sustainable Development Goals (SDGs) is critical for countries in the global South. The question for developing countries is not only how this could be workable but also who could be involved in harnessing blockchain technologies to close development gaps, foster social inclusion and promote democratic governance.

This white paper explores the potential blockchain technology could have in fostering human development in developing countries. The first part (after the executive summary) provides a non-technical overview of blockchain. It then moves to illustrate the range of applications in development areas and sectors from a public/private goods perspective. The third section examines the actual relevance of blockchains in developing countries. The paper concludes with a series of recommendations for additional research and potential development programming using blockchain technologies. The annexes lay out the information and communications technology for development (ICTD) framework and a more technical presentation of blockchain technologies.

This paper centers on blockchain applications that go beyond cryptocurrencies. The core focus is thus on the use of blockchain technology as a generic application platform in developing countries.

BLOCKCHAIN TECHNOLOGY

The blockchain is one of the core underlying technologies supporting Bitcoin, the first successful decentralized, peer-to-peer cryptocurrency in history. As a financial platform, Bitcoin required a digital ledger to record all transactions. The blockchain is the technology that furnishes such a ledger and records all transactions that take place on the cryptocurrency network. Initially overshadowed by Bitcoin, blockchains gained relevance in the past few years as a standalone technology that could be deployed in sectors other than finance.

In layperson's terms, **blockchains can be defined as a public spreadsheet that sequentially records transactions among users operating within a decentralized peer-to-peer network.** Every network node stores an up-to-date copy of the data and updates automatically diffuse among all nodes.

One of the key innovations of blockchain technologies is the way records are interlinked. Each row, comprised of a block of transactions, has a unique identifier linked to the previous one. The unique identifier of the previous block is used to compute the identifier for the new block thus creating a mathematical link between blocks in the chain. Changing or deleting rows in the database is nearly impossible as it requires changing all records in the chain.

Adding new rows to the data requires node consensus - achieved with the help of the proof of work algorithm which nodes must run. Proof of work resembles the traditional 'guess the number' puzzle but has much higher complexity. The outcome of proof of work is shared among network nodes that can then validate the result. Once this happens, the block is added to the existing blockchain.

More Info

Need a little more detail about blockchain?

See Annex II on page 59 for a more thorough explanation



Blockchain technology uses cryptographic tools. First, each block unique identifier is a cryptographic hash of the inputs provided. The block of transactions included in each block is also the result of a hash operation. Second, all nodes and users must use public key cryptography to be part of the network and interact with each other. Creating a profile or providing personal information is not required, in sharp contrast with existing social media platforms.

Key attributes of blockchain technology

Privacy

Pseudo-anonymity

Integrity

Distributed trust, governance

Transparency

Security

Sustainability

Open source

Blockchain issues and limitations

Scalability

Limited block size

High operating costs

Environmental impact

Mining centralization

High bandwidth requirements

Usability

Complexity

Use of cryptography

Immutability as liability

BLOCKCHAIN APPLICATIONS

Keeping abreast of blockchain innovation and development is not an easy task as the sector is evolving at a rapid pace on a global scale. What matters for this paper, however, is how this is taking place in developing countries. From a development perspective, introducing the concepts of public and private goods and their provision by the public and private sectors is essential. This paper highlights blockchain developments in relation to these two types of goods and services.

In most developing economies, governments are in principle the main providers of public goods from justice and security to health and education, among others. This does not imply, however, that governments themselves deliver such goods. Much of the time, implementation is outsourced to private partners, both for-profit and non-profit. This is how blockchain technologies are being deployed in most developing countries.

Areas and sectors impacted by blockchain technologies include:

- ▶ Government services, especially in programs related to e-government and smart government
- ▶ Land titles, one of the first areas of blockchain technology deployment
- ▶ Identity services, including personal reputation management
- ▶ Freedom of speech
- ▶ Anti-corruption
- ▶ Electoral processes
- ▶ New forms of governance in terms of both virtual and global governments
- ▶ Aid and development, supported by international donors and multilateral organizations

Examples and evidence compiled by this paper suggest blockchain technology deployments for the provision of public goods in developing countries are still in their infancy. Many of these efforts are supply driven with local institutions playing a passive role with limited ownership of initiatives. Blockchain technology initiatives engaged in smart government programs and identity services likely have the best chance for success in the medium run.

On the other hand, private goods provision of blockchain technology has an internal financial sustainability component that works like a magnet in attracting suppliers - as long as prices are at a certain level. Yet billions of people around the globe do not have access to such goods – such as banking services – to which the poor rarely have sustained access. In this light, the paper examines five areas where private goods and services provision is lagging. They are:

- ▶ Banking for the unbanked
- ▶ Remittances (a.k.a. Rebittances)
- ▶ Agriculture
- ▶ Food security
- ▶ Intellectual property rights

Most of the blockchain technology initiatives targeting this selected group of private goods show potential but have yet to take off. Some have already stopped or suspended operations altogether while others continue to struggle to generate solid revenues. Remittances and digital money are the most promising areas here.



BLOCKCHAINS AND HUMAN DEVELOPMENT

Regardless of the relative success of ongoing blockchain technology initiatives, development practitioners and researchers should have at least an adequate non-technical understanding of the technology's potential in supporting and enhancing development programming and democratic governance. The analysis of the impact of blockchain technology on human development is based on a four pillar analytical framework (see Annex I for more details): Infrastructure, capacity development, policy and regulation, and institutions and governance.

In terms of **infrastructure**, recent data suggests nearly four billion people do not have access to the Internet, most of whom live in the developing world. It thus seems unlikely that people living with no access will become blockchain network nodes, or could run wallet software to at least benefit from the technology as end users. A second infrastructural issue relates to what can be called **infostructure**, or public key infrastructure. This encompasses the roles, policies and procedures needed to secure the electronic transfer of information, and is not yet in place in many developing countries. This poses serious obstacles to the systematic use of blockchain technologies for any purpose, as it relies on the use of these cryptographic tools.



In terms of **capacity development**, two key issues emerge. One is the use of these multifaceted, complex tools. Recent research suggests using cryptographic tools is still difficult, and has significant room for improvement to appeal to and be understood by a wide range of users. The second issue relates to the management of end user private and public keys. Blockchain technology wallets and client software can and have provided friendly interfaces that facilitate public key cryptography. But users need to manage their private keys and safely store them somewhere, somehow. These two issues together might prove too demanding for populations with relatively low levels of education and literacy and who otherwise face socio-economic exclusion.

As with other technologies fostering the platform economy, blockchain technologies are running ahead of local policies and regulation. While industrialized countries are catching up, this is not the case in most developing



countries where policy and regulatory capacities are still incipient. This gap facilitates a disorderly deployment of blockchain technologies in the global South not only for local startups but also by corporations or other institutions from the North, who bypass local development priorities or exploit the lack of regulatory knowledge. In addition, as most startups using blockchain are sticking to Bitcoin, policy and regulation of cryptocurrencies is also becoming increasingly important. Local policies and regulations are also crucial for security reasons in countries where conflict and violent extremism are rampant, and the financing of such activities should be more closely monitored to prevent global spread.

In the same fashion as previous Internet technologies, the deployment of blockchain suggests possibilities for reducing some forms of (central) government. The distributed nature of the technology coupled with a new form of decentralized trust and distributed consensus provide the fodder for such views. This does not, however, mean that blockchain is (or should be) inextricably linked to such views. As described in the previous section, many blockchain technology startups are working with governments to deploy the technology at the state level. But an issue largely ignored is the potential of blockchain technologies to support and enhance the devolution of government within nation-states. There is a genuine opportunity for blockchain technologies to support local governments, which usually have limited access to fiscal and human resources.

To harness new technologies, besides fiscal resources, developing countries require institutional capacities that can facilitate their deployment. Such capacities are not limited to knowledge of technology alone. To ensure their long-term sustainability, blockchain deployments and initiatives need to end up strengthening institutional capacities. Factoring in how blockchain technologies should be deployed in the public sector is thus essential.

While the prevailing view suggests blockchain should replace current processes, it is rather more important to consider how the technology can complement or supplement governing processes while also promoting innovation within the public sector.

In terms of governance, blockchain technologies raise a variety of questions including: Who is in charge, who drafts smart contracts (algorithmic transactions that execute pre-defined contractual agreements), and how can all voices be included? A quick response from the blockchain camp is straight forward: No one is in charge as, by default, no need for this exists – and everyone is in charge as governance happens by consensus only. Such consensus is based on algorithms that allow users and nodes to almost automatically agree on the outcomes of the process. It thus seems the software takes control, placing individuals, who need not interact among themselves anymore, in the background. This raises issues related to:

- ▶ **Software coders:** Who does the actual coding? How were they selected?
- ▶ **Code comprehension:** While the code is open source, end users must have the capabilities of reading and understanding the code. Most do not so they require intermediaries to do so.
- ▶ **Scalability:** Blockchain technology is still not scalable (though many in the blockchain community are actually working on this). Until scalability is dealt with, how will the growth in blockchain technologies to billions of user and nodes impact decentralized consensus?
- ▶ **Trust vs. governance:** Decentralized and depersonalized trust does not imply enhanced governance.



Though decentralized and distributed, these issues point to the fact that blockchain technology cannot guarantee that hierarchies and inequality among peers will not take place. This is already happening with the mining of blockchain technologies. The same goes for blockchain coders, developers, and techno-entrepreneurs, all of whom seem to have a privileged position in the networks and can muster substantial power over all other nodes and users. Inequality within a decentralized network is thus feasible and real.

CONCLUSIONS

Adoption and widespread use of blockchain technologies face challenges already familiar to ICT for development practitioners. Perhaps a new ingredient in the mix is the **complexity of blockchain technology itself**. This introduces new issues and obstacles in terms of both technology deployment and its diffusion to end users and stakeholders.

Blockchain technology is still in its infancy and supported by a relatively small but highly qualified group of innovators and techno-entrepreneurs. Together, they could address most if not all the limitations and challenges highlighted in this paper. Blockchain's innovation potential is thus large. While this speaks volumes for blockchain technologies, it is early to draw final conclusions on how the technology will evolve in the next five years or so. At the moment, as is often the case with technologies, **hype is leading the charge, but current evidence suggests blockchain technology deployments are still in a proof-of-concept stage.**

Replacing ongoing initiatives or launching new ones on standalone blockchain technology platforms will only delay blockchain adoption. The best approach for developing countries is to **deploy blockchain technology to complement or supplement ongoing programs.** This could lower entry barriers while increasing the chance of making initial investments in blockchain technologies sustainable in the medium term while catering to local needs and development gaps.

Broader **blockchain initiatives linked to smart government seem to be best positioned to make blockchain technology a key catalyst in delivering public goods.** Remittances and digital money in the private goods area also have potential; however, it is critical to understand how this might not promote economic and financial inclusion of those sitting at the bottom of the pyramid.

Usability issues might also limit blockchain technology diffusion in developing countries. Widespread use of cryptographic tools in poor countries face formidable challenges, especially if blockchain technology initiatives target the poorest sectors of the population. The assumption that every single beneficiary must use and manage private and public keys is not realistic, and the lack of public key infrastructure in most developing countries will only exacerbate this. The only way to break out of this impasse is to devise alternatives that furnish end users with access to cryptographic tools via intermediaries such as community based organizations, small enterprises and/or local governments. The key point here is that **end users do not need to own or directly use the technology to benefit from its deployment.**



While blockchain technology thrives in decentralized settings, this paper shows that **mining is prone to centralization and concentration**. In the early days of Bitcoin blockchain, anyone with a laptop or PC could mine the network; today, this can only be accomplished by a few who have the financial resources and hardware to do so and who can afford to pay high energy bills.

Similarly, for notions of consensus, blockchain technologies replace human consensus with algorithmic consensus. **The issue here is not just of consensus automation but also of representation and scale**. Decentralized autonomous organizations and blockchain networks are small in terms of the number of people involved. Most blockchain users are clients using wallet software and are not part of any consensus building process, algorithmic or not. As it stands today, given its lack of scalability and other limitations highlighted in this paper, blockchain technologies seem more ideal for small scale operations.

Blockchain technologies could disrupt development soon. Indeed, the Internet and mobile technologies have – and continue to - trigger positive disruption in development practices, though not to the degree expected when they first emerged. Similarly, it is still early days of blockchain, and the technology continues to rapidly evolve. **Success in terms of deployment of new technologies like blockchain in developing countries depends on its effectiveness to tackle the human development challenges highlighted above.**

In this light, an additional and pertinent question is whether blockchain technologies can foster deeper levels of disruption in development processes than its predecessors. For sure, the potential is there but more targeted action is required to have such impact in development processes.

RECOMMENDATIONS

Based on the analysis and findings of this paper, the following recommendations emerge.

RESEARCH

Undertake a series of selected case studies on ongoing blockchain technology initiatives that are taking place in developing countries. While some anecdotal information on such initiatives can be found, little in terms of academic or developmental research is currently available. Indeed, a large vacuum exists here that has helped spread blockchain hype even more.

Undertake further research and analysis on both blockchains for governance and the governance of blockchains vis-à-vis governments and the provision of public goods. In particular, the links between trust, consensus building and representation have not been explored in the existing literature.

Link current and future work on blockchain technology to Artificial Intelligence as the latter is being systematically introduced into the technology and related “decentralized applications” or Dapps. This points back to blockchain technologies’ governance issue and the governance of algorithms in general which are not participatory, nor transparent. Is blockchain part of the solution?

Consider opening new and pioneering research on the governance of algorithms and the impact they can have in society, especially in developing countries. This theme is in turn linked to the notion that technologies are social products. In the end, society ends up shaping how technology is harnessed. However, the prevailing view today seems to be the opposite, blockchain technologies included.

Explore innovative approaches and solutions to facilitate blockchain technology access to those sitting at the bottom of the pyramid, focusing on access and use of cryptographic tools. Here, distinguishing technology use and ownership from its benefits is crucial. Previous technology deployments have shown that poor communities can benefit from them without directly using or owning a particular technology. Community networks and shared mobile telephone use are well-known examples here.

PROGRAMMING

Explore the role of ongoing innovation initiatives and existing tech hubs in developing countries to support blockchain technology deployments. Africa and Asia, in particular, have a considerable number of technology hubs which can furnish adequate expertise to deploy blockchain technologies with local knowledge and to target the provision of public goods.

Consider funding or supporting small blockchain technology pilots or prototypes focused on specific development themes, the SDGs or local priorities in developing countries. Funding need not be large but special attention should be placed on the human development impact. As mentioned earlier, identity and government services using blockchain technologies are the most relevant at this point and have already been implemented in other contexts.

Support or help create a network of blockchain technology innovators and entice them to support applications that foster public goods provision. Attracting local innovators in emerging and developing economies is of critical importance here.

NETWORKING AND PARTNERSHIPS

Support the creation of a blockchain for blockchain-related projects in developing countries, or consider the creation of a related sustainable knowledge base. Partnering with international experts and other innovators on a global scale should be part of such initiative.

There has been some action by **multi-laterals and overseas development funding agencies on linking blockchain technologies to the implementation of the SDGs.** Development agencies and development practitioners should join these efforts to track the latest developments and eventually undertake further research on the topic.

Launch or help organize a ‘blockchain for development’ network, or a decentralized autonomous organization with key donor countries and organizations. The main goal of such a network could be to keep the development perspective atop, and above blockchain itself.



1

INTRODUCTION

Nasa

Introduction

The *fourth industrial revolution*.¹ The *second machine age*.² The *zero marginal cost society*.³ These are some of the metaphors used to describe the current wave of technology innovation⁴ that is rapidly evolving.

Robotics and artificial intelligence are surging in use, being deployed en masse in production processes by the private sector. Newer technologies are also part of the innovation wave. At the forefront here is the blockchain, a new technology developed as one of the core pillars of Bitcoin, the cryptocurrency invented in 2008 by a still anonymous author.⁵ Whereas artificial intelligence and robotics seem to have a dark side,⁶ many perceive blockchain technology as a platform for positive change - one that could disrupt the global economy and address many of the socio-economic and political issues that countries are facing nowadays.⁷ While such claims are certainly not new, blockchain technology is attracting the attention of a wide range of actors, from governments and international donors to the private sector and venture capitalists.

These technologies share a common trait: High sophistication, not only in terms of software and hardware requirements but also in relation to capital requirements, human capacity and institutional environments. In contrast with the mobile ‘revolution’,⁸ the current innovation wave might prove to be more challenging for developing countries if they intend to be active players - and not just end-users or consumers of these technologies. Exploring the relevance of new technologies to address existing socio-economic gaps and support internationally agreed development targets such as the SDGs is critical for countries in the global South.⁹

Initially linked to financial applications, blockchain technology is now being deployed in many other areas and sectors, including development and humanitarian aid. The question for countries in the global South is not only how this could be workable but also *who* could be involved in harnessing blockchain technologies to close development gaps, foster social inclusion and promote democratic governance.

The purpose of this white paper is to explore the potential blockchain technology could have in fostering human development in developing countries. The paper first provides a non-technical overview of blockchain technologies. It then moves to illustrate the range of blockchain technology applications in development areas and sectors from a public/private goods perspective. The following section presents an examination of the actual relevance of blockchains in developing countries, using an ICT for development (ICTD) framework presented in Annex I. The paper concludes with a series of recommendations and actions for additional research and potential development programming using blockchain technologies. Note that this paper is exclusively focused on blockchain applications that go beyond new cryptocurrencies. The core focus is thus on the use of blockchain technologies as a generic application platform in developing countries.¹⁰

Blake Wheeler





Sebastien Gabriel

What is blockchain technology?

This section details the inner workings of blockchain technology from a non-technical perspective.¹¹ It starts with a short history of the genesis of blockchains, and then describes what the technology can do and how it works. Understanding how blockchains function will help development practitioners unpack the hype, and recognize its potential relevance and benefits in current and future research and development programming.

More Info

Still a little unclear about blockchain technology?

Please see Annex II on page 59

BRIEF HISTORY

The blockchain is one of the core underlying technologies supporting Bitcoin, the first successful decentralized, peer-to-peer **cryptocurrency**¹² in history.¹³ Bitcoin was created in 2008 by Satoshi Nakamoto whose real identity remains a mystery.¹⁴

As a financial platform, Bitcoin required a digital **ledger**¹⁵ to record all transactions taking place among cryptocurrency users. The blockchain is the technology that furnishes such a ledger. The way this ledger was designed is what led to the emergence of blockchain technologies.¹⁶ The Bitcoin software created by Nakamoto was released on the internet as Open Source Software (OSS), which has helped propel its diffusion on a global scale since its inception.

In its early years, Bitcoin operated in the fringes of the economy as few merchants were willing to accept the cryptocurrency as a legal form of payment. The **dark web**¹⁷ however saw things in a different light. Bitcoin

provided an anonymous form of payment that could not be used to track buyers and sellers. The now infamous [Silk Road](#)¹⁸ website, an online black market platform, extensively used Bitcoin, while Bitcoin exchanges facilitated cryptocurrency conversion into U.S. dollars.

Bitcoin was thus linked to a number of illegal activities, from the drug trade to money laundering. Law enforcement entities and regulators took notice and promptly began prosecuting those involved in such activities. The Bitcoin community then had to rebuild the reputation of the cryptocurrency, an effort that paid off a couple of years later.¹⁹ This is still an issue that remains relevant for Bitcoin and all other cryptocurrencies,²⁰ but is not as important for blockchain technologies as the latter can be fully functional without Bitcoin.

Bitcoin initially overshadowed blockchains, being thus ignored by pundits and technologists. But things changed around 2014 when its potential as a standalone technology working in sectors other than finance was recognized by innovators, and soon thereafter, by venture capitalists. Figure 1 depicts this evolution, using Google Trends. Note the exponential growth starting in 2016.

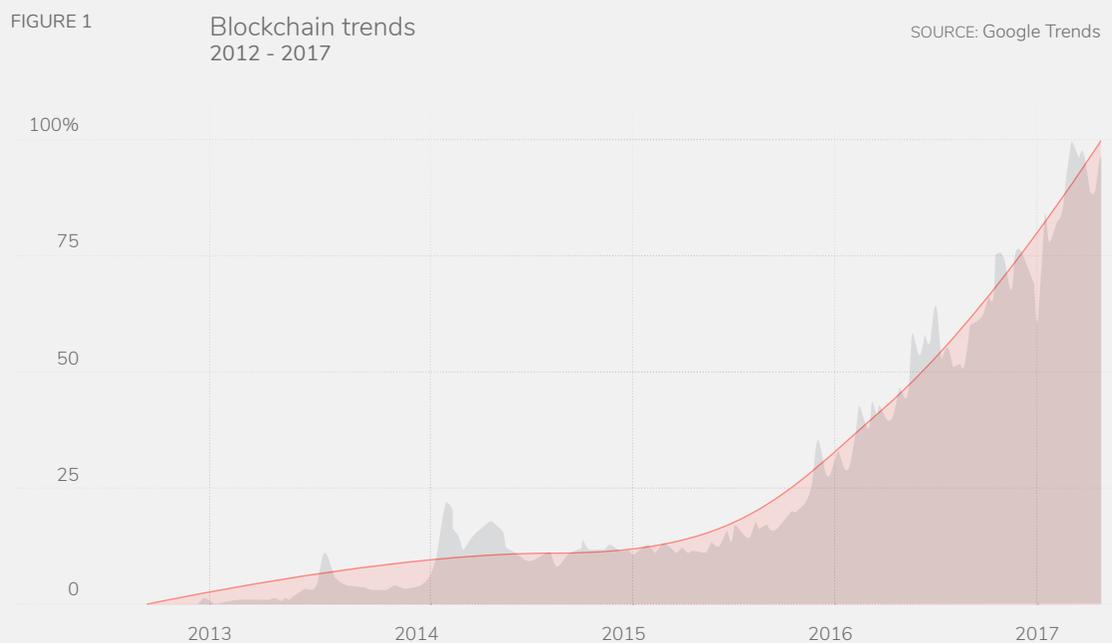


Figure 1 depicts the evolution of blockchain using Google Trends, when its potential as a standalone technology for sectors other than finance was recognized by innovators and venture capitalists. Note that the Y axis represents the share of monthly searches relative to the highest month for the whole period, and it can never be more than 100%. Please see footnote 21 for clarification.

Joel Filipe



Figure 2 below shows interest in blockchain technologies by country.²¹ Note that a few developing countries are leading the pack.

Blockchain is not only surging but is also being deployed in several countries for a wide variety of purposes, as described below. Even large and traditional financial institutions are now on the verge of embracing blockchain technologies, though not without first trying to reshape it to support current business processes and practices.

FIGURE 2 Country interest in blockchain 2012 - 2017

SOURCE: Google Trends

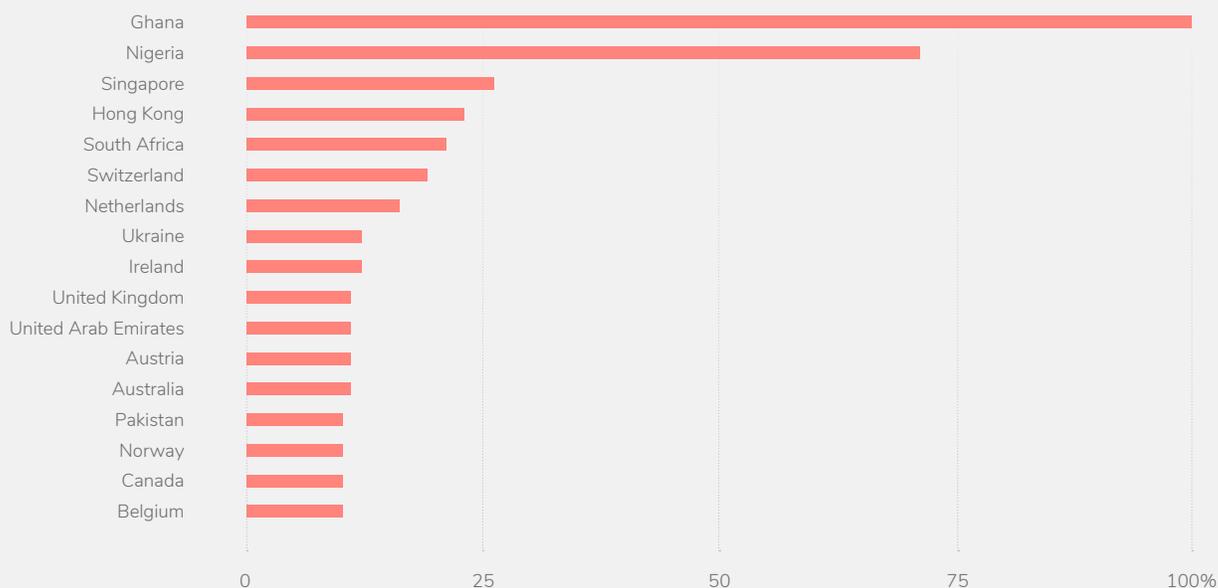
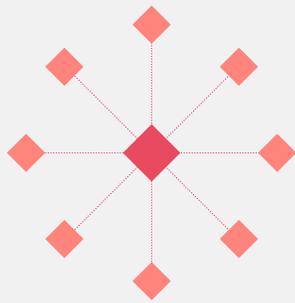
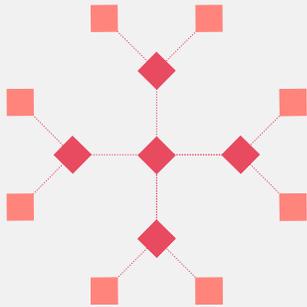


Figure 2 shows interest on blockchain technologies by country. The paradox is that while most of the action is taking place in developed countries, most searches on blockchain technologies are happening in developing countries. Note that Google trend numbers are relative, not absolute. For any keyword search, it identifies the maximum number of searches on a given day or year and divides all others by it. The maximum is thus always 100. It is clear that Google searches for blockchain technologies are still on the rise. See footnote 21 for more details.

FIGURE 3 Network typologies²⁵



Centralized



Decentralized



Distributed

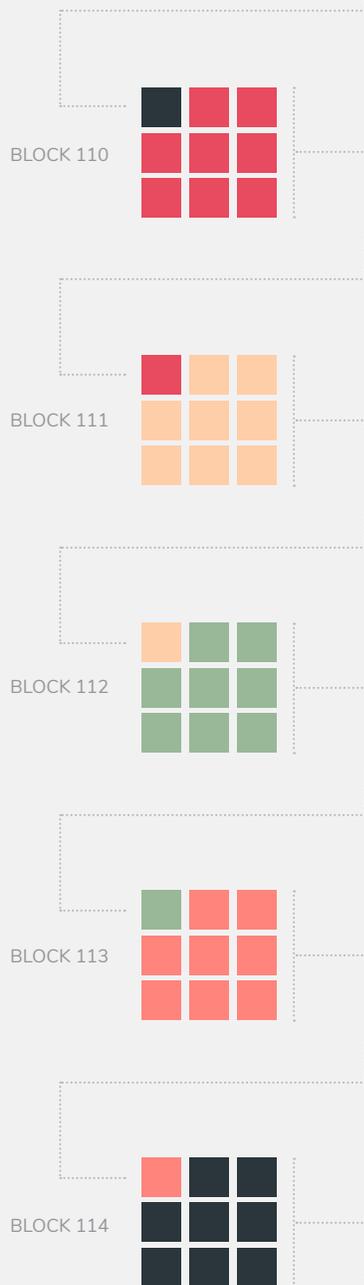
A LOOK INSIDE BLOCKCHAINS

In layperson terms, the blockchain can be seen as a spreadsheet that sequentially records transactions among users operating within a **peer-to-peer network**.²² By default, the spreadsheet is public: all network users or nodes have real-time and full access to data recorded in the database. Previous authorization or permission granted by third parties or a pre-existing central authority is not required. The spreadsheet is also distributed.²³ Every network node stores an up-to-date copy of the data. By the same token, data updates automatically diffuse to the network every time a new row is added. No central computer or server handling or directing traffic is thus needed.²⁴

Raphael Koh



FIGURE 4
Blockchain
schematic representation



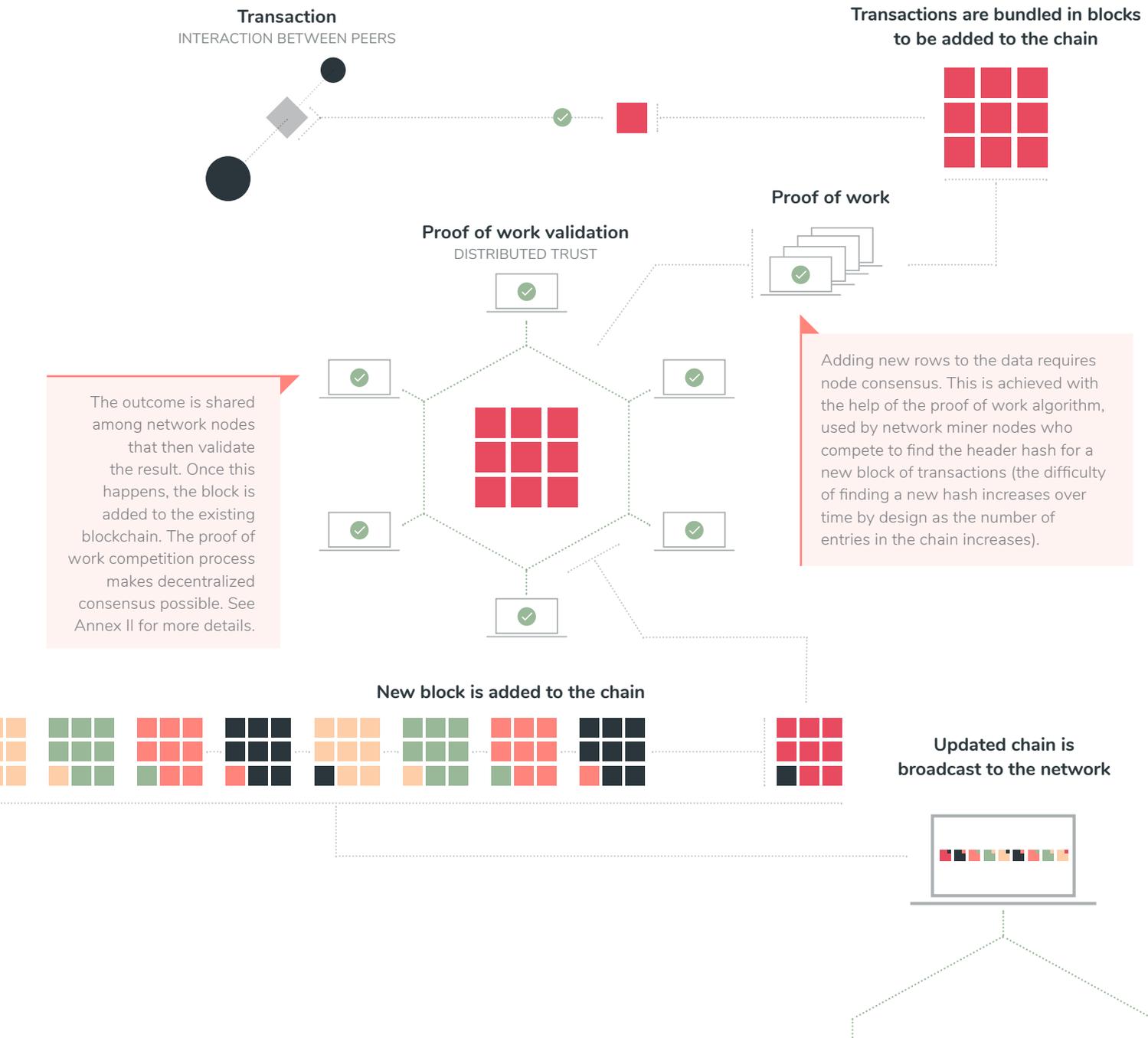
One of the key innovations of blockchains is the way records or rows are interlinked. Each entry in the public database is comprised by a *block* of transactions²⁶ and has a *unique identifier*. Each block of transactions is linked with the previous or, in computer speak, is a *child* of the previous block thus creating a *chain* between blocks.

How is this accomplished? Each block *unique identifier* is used to generate the unique identifier of the next block. This creates a chain of linked blocks, or a blockchain, where changing the content or the order of the rows is virtually impossible. Any block is thus the mathematical child of the previous one. The only exception here is the so-called “genesis block,” the first block or row in the data, which is an *orphan*, as it lacks “parents.”

Figure 4 shows a schematic representation for three random blocks in a fictitious blockchain. Block 112 for example has its own unique ID and includes its own set of transactions. It also includes the unique ID of the previous block and a unique time stamp which registers the date and time the entry was added to the blockchain.

Clearly, blockchains are much more complex than regular spreadsheets. This is perhaps best reflected in the way records are added to a blockchain.

Blockchain 101



Main actors

Core developers have write access to the source code.

Full nodes have up-to-date copies of the blockchain, validate new blocks and propagate them across the network.

Miners are dedicated to running proof of work.

End users use the network to do their transactions by using client or wallet software.

Service nodes such as wallets, storage, exchanges, and cloud services.

P2P Technology

In a peer-to-peer network all interconnected nodes are in principle equal. No central server exists, therefore no central point of failure. If one node goes down, all others remain interconnected - and data and information flowing through the network is preserved. Examples: BitTorrent and Napster.

Cryptography

Blockchain uses public key cryptography: a private key known only to its owner and a public key which is shared with the world. A private key is first generated in random fashion, and is then used to create a public key. The private key is used to encrypt the transaction which can then be decrypted by the intended recipient using the sender's public key. It is mathematically impossible to use a public key to decipher a private one.

Blockchain for Development 101

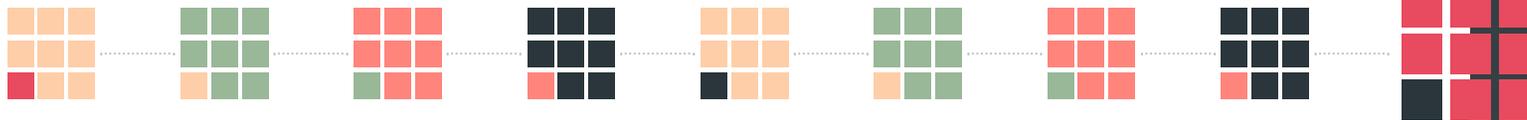
POTENTIAL AND CURRENT USES OF BLOCKCHAIN

Public or government services

- Landtitles
- Identity services
- Anti corruption
- Electoral processes
- Aid distribution and development

Private sector services

- Rebittances
- Agriculture
- Food security
- Intellectual property rights



MAIN REQUIREMENTS FOR BLOCKCHAIN

Infrastructure & infostructure

The blockchain ecosystem requires infrastructure - from telecommunications to the electrical grid, to health and education - all of which need both private and public investments. But it also requires infostructure - such as public key infrastructure, which includes the roles, policies and procedures needed to secure the electronic transfer of information. This kind of infrastructure is often not yet in place in many developing countries.

Capacity development

Countries require human capacity to develop and deploy new technologies - not only technical capacities but also cross-cutting functional capacities that go beyond ICTs. Users need to be able to manage their private keys and safely store them, which could prove demanding for populations with low levels of education and literacy.

Policy & regulation

The capacity of government at all levels to develop, implement, and enforce policies within the territory under their control is key. Agile policy environments can facilitate the use of technologies and enable countries to become places where pilots and prototypes are deployed, enhancing expertise and competitive advantage on a global scale.

Institutions

This includes the 'rules of game' that allow people to undertake activities within a given institutional context. Governance mechanisms are part of this, especially new models based on multi-stakeholder engagement. Blockchain can help improve or support better state institutions, facilitating state decentralization which is a core development issue.

MAIN VALUES OF BLOCKCHAIN

Immutable data

Blockchains offer data and user integrity. First, it is virtually impossible to change and falsify blockchain blocks, and this offers a high degree of data integrity, or immutability. Second, metadata about the transactions undertaken by a node and/or end user are recorded on the blockchain and can be linked to the user undertaking them. This means users cannot fool the network or try to complete an invalid transaction. However, though full anonymity cannot be achieved, blockchains store no personal information and use private/public encryption to authenticate users undertaking transactions. Nodes and users do not need to provide names or personal details to be part of the network, and mining blockchains to obtain personal information that could be sold to third parties for a profit is not feasible.

Distributed trust

The blockchain successfully bypasses the need for a trusted central authority. Instead, trust is spread across the network. The same goes for governance mechanisms where, in principle, different types of users and nodes have the same political leverage.



Photo via Visualhunt

ADDING A NEW BLOCK TO THE CHAIN

Unlike other traditional ledgers and transactional platforms, new blocks can only be added once network nodes reach consensus. This is called decentralized consensus, which supersedes the need for a central trust authority. This is why the blockchain is characterized as a technology where trust is decentralized: The network itself provides trust among all peers. Third parties certifying or approving ongoing transactions are not needed as they are with traditional financial operations and many other transactional networks.²⁷

Such consensus is not accomplished via voting but rather by using the computing power of nodes in the network.²⁸ Decentralized consensus is achieved with the help of the proof of work algorithm that nodes must run to add a new block to the database.²⁹ Proof of work resembles the **guess the number puzzle**³⁰ but has much higher complexity. The outcome of proof of work is shared among network nodes that can then corroborate or validate the result. Once this happens the block is added to the existing chain of records and subsequently distributed among all nodes.

Note that nodes must compete among themselves to solve the puzzle. However, only specialized nodes running sophisticated hardware have a realistic chance of solving the puzzle.

CRYPTOGRAPHY

Blockchain technology systematically uses cryptographic tools.

In the first place, the unique identifier for each block is a *hash of the inputs provided*.³¹ The block of transactions included in a blockchain record is also the result of a hash operation. However, the hash function used in the latter differs from that used for generating the unique block ID.³² Transaction information is encoded thus revealing little of its actual content to the naked eye other than some basic metadata.³³

Second, all nodes and users must make use of public key cryptography to be part of the network and interact with each other. Users and node must generate both private and public keys, the latter being shared across the network to identify them. Creating a profile or providing personal information is not required. A valid public key will suffice. In this context, blockchain technology is *pseudo-anonymous, in sharp contrast with existing social media platforms*.



BUILT-IN INCENTIVES

Blockchain technologies have built-in economic incentives for nodes entering the proof of work competition, and for those that want to provide additional services specific to either Bitcoin or blockchains, or both.

For example, nodes solving proof of work on the Bitcoin blockchain get newly minted Bitcoins. In addition, nodes can also charge a fee for every transaction paid in Bitcoins by users undertaking such transactions. In principle, these incentives should be large enough to support the increasing hardware, energy and other associated costs of running proof of work.

Converting Bitcoins into US dollars and other currencies was one of the first services that nodes provided. As the market price of Bitcoins rapidly increased over time, exchanges have become a key source of revenue for network nodes.

Blockchain has created a sophisticated ecosystem of services which so far has proven to be profitable. The recent upsurge in the price of Bitcoin and other blockchain-based platforms will accelerate such growth.

BLOCKCHAINS AND GOVERNANCE

The decentralized nature of blockchain technology, combined with the emergence of distributed network trust, could lead to significant disruption in traditional governance processes,³⁴ for instance ushering in more horizontal and personalized forms of governance. Other ideas bandied about in the literature include:³⁵

- ▶ New forms of direct democracy where all network members can take part in decision making processes. One example here is the idea of Liquid Democracy that predates blockchain but has now found its perfect platform.³⁶
- ▶ Empowerment of individuals by decentralizing and diffusing authority among them. This can be accomplished with software agents that act on behalf of people, based on protocols previously agreed and coded into the blockchain.³⁷ Decentralized autonomous organizations³⁸ are a good example as well as other forms of decentralized organizations that operate via smart contracts.³⁹
- ▶ Global public services customized and delivered to clients regardless of location or nationality. Not all versions of this idea call for the demise of the nation-state. Blockchain can in fact complement or supplement government services while simultaneously enhancing transparency and accountability.⁴⁰
- ▶ Creation of blockchain-based nation-states such as [Bitnation](#).⁴¹
- ▶ Generating a new and more inclusive social contract.⁴²

Thomas Kvistholt





Ferdinand Stohr

BLOCKCHAIN TYPES

While Bitcoin’s blockchain is public and open to all, blockchains do not necessarily need to have such characteristics to be deployed and effectively used.

First, blockchains can either be *public* or *private*.⁴³ In the latter case, only a set of pre-selected nodes can be part of the overall network and process transactions. Second, blockchains can be *permissionless* or *permissioned*. The latter requires node authentication via passwords, digests and/or digital signatures to read and/or add new records to the blockchain.

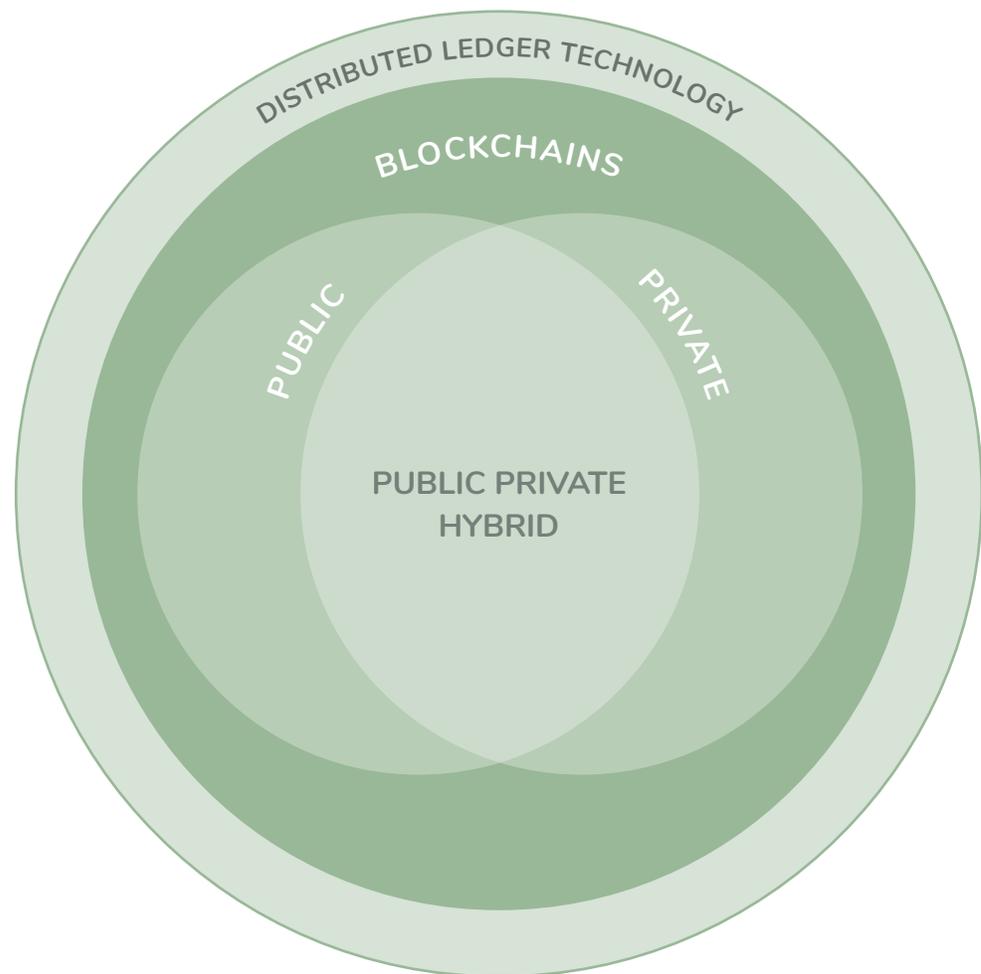
As a result, a private blockchain could be permissionless while a public one could demand previous authentication before granting write permissions to the blockchain. In this case, only authenticated nodes can add new entries to the database. The above is summarized in Table 1.

Table 1: Blockchain types

	Permission-less	Permissioned
Public	All peer-to-peer network nodes have full access to the blockchain.	Nodes need to be authenticated to get write access to the blockchain.
Private	All nodes in a previously defined private network have full access to the blockchain.	Nodes must authenticate to have read and write access to the private blockchain. Alternatively, only some authorized nodes can write to the blockchain, while all others have read access only.

Private permissioned blockchains are being promoted by some in the private sector. On the other hand, governments could opt to consider public permissioned blockchains to deliver specific services to citizens while avoiding the use of expensive and unsustainable proof of work algorithms.⁴⁴

Note that using public-private or hybrid blockchains is also feasible.⁴⁵ Finally, some observers have labelled blockchain technology as “distributed ledger technology” (DLT) to highlight its non-currency nature.⁴⁶ However, not all DLTs make use of blockchains. *Corda*⁴⁷ and *Ripple*⁴⁸ are examples of DLTs that do not use blockchains.⁴⁹ Figure 5 puts all the above together and provides a schematic representation of all such variations.



BLOCKCHAIN KEY TRAITS

The above presentation provides the necessary background to identify the key characteristics and principles of blockchains. These are the following:

Privacy: Blockchains store no personal information and use private/public encryption to authenticate users undertaking transactions. Mining blockchains to obtain personal information that could be sold to third parties for a profit is not feasible.

Pseudo-anonymity: Nodes and users do not need to provide names or personal details to be part of the network. However, full anonymity is not achieved as linking users to network activity is feasible and can thus lead to revealing their identities.⁵⁰

Integrity: This works in two ways. First, data integrity: it is virtually impossible to change and falsify blockchain blocks. This is also called *immutability*. Second, user integrity: metadata about the transactions undertaken by a node and/or end user are recorded on the blockchain and can be linked to the user undertaking them. Users cannot fool the network or try to complete an invalid transaction.

Distributed trust, governance: The blockchain successfully bypasses the need for a trusted central authority. Instead, trust is spread across the network. The same goes for governance mechanisms where, in principle, different types of users and nodes have the same 'political' leverage.

Transparency: All blockchain metadata and information is available to all nodes and users in real-time. It is not possible to hide or redact blockchain information.⁵¹ Distributed transparency is thus feasible, but also introduces new issues.⁵²

Security: Use of blockchains requires cryptographic tools and public/private keys by all participants, being nodes or end users.

Sustainability: Built-in economic incentives provide a clear path for network economic sustainability.

Open source: Software required to use blockchains is freely available to all, including cryptographic tools. Furthermore, users with adequate capacities can actually help enhance and refine blockchain technologies, in addition to catching bugs. This can also facilitate the spread of blockchain innovations.

BLOCKCHAIN LIMITATIONS

As an emerging technology, blockchains face a series of limitations that might prevent widespread adoption not only in the financial sector but also in other areas. These can be summarized as follows:

Scalability: As it stands today, Bitcoin blockchain can only add a new block of transactions every ten minutes or so. This translates into a low volume of transactions per second (less than five), a far cry from the volumes reported by traditional transactional networks.

Block size: The above is the result of the small block size defined by the original Bitcoin source code. The maximum size for each block is one megabyte which can accommodate 2,200 transactions. Increasing block size is currently under discussion but so far no final decision has been reached.⁵³

High costs: Miner nodes use sophisticated and expensive hardware to run proof of work algorithms. Consequently, only certain nodes in the network can effectively compete in this process, even though in theory all nodes have the software required to mine the network. Nakamoto's notion of "one-CPU-one-vote" is no more as hardware and electricity costs prevent most nodes from participating in this process.

Environmental impact: A by-product of the above is also proof of work's inefficiency in terms of energy resources. Some estimates on energy consumption suggest that, by Spring 2017, Bitcoin use of electricity was comparable to that of 280,000 US households per year.⁵⁴

Centralization: Mining is now centralized with a few nodes controlling a large share of the market.⁵⁵ Figure 6 below depicts market shares of the top miner nodes or companies. Note that the top five companies alone control over 50 percent of the market.⁵⁶

Bandwidth: Full nodes that want to be active in the network must have access to the right Internet bandwidth. Slow, unreliable connections are not welcome, especially when the current size of the blockchain is over 120 gigabytes.⁵⁷

Usability: Blockchain technology requires the secure management of public and private keys by end users and nodes. While existing wallet software has come a long way, losing private keys is still a serious risk. None of the existing solutions are resistant to physical theft and only a few can protect users from malware.⁵⁸

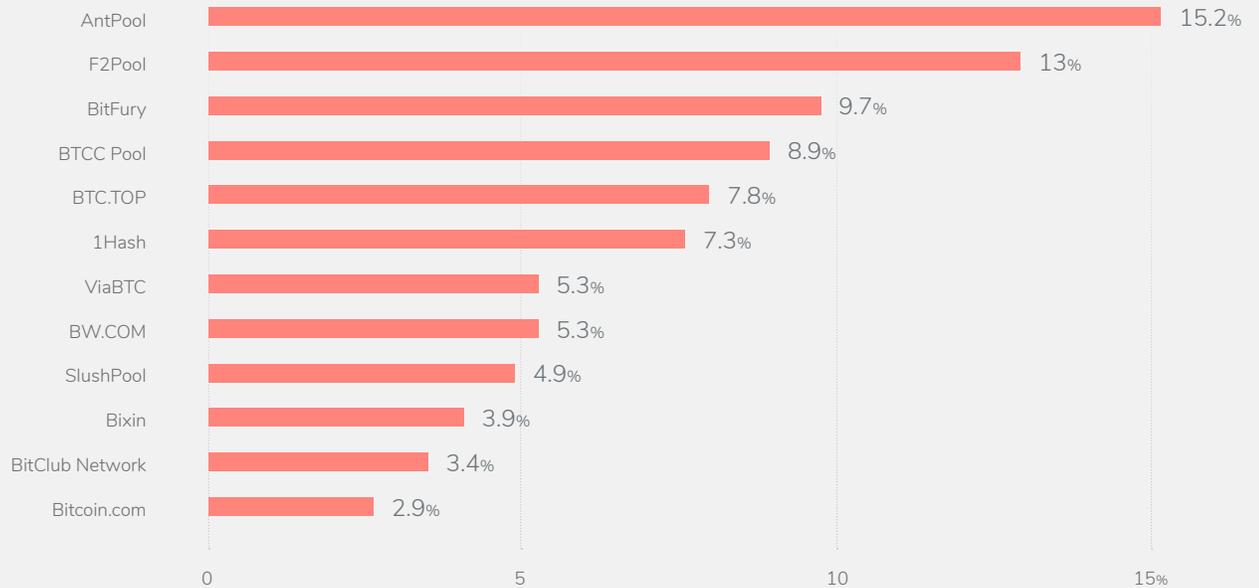
Complexity: Blockchain technologies appear to be almost incomprehensible to the average person and the tech speak around it does not help. Only a selected few seem to understand the technology.

Cryptography: Use of cryptographic tools is still incipient and the average Internet user cannot be expected to embrace its use in the short term.

Immutability as liability: If the blockchain is hacked or the software code has a bug that allows a particular exploit, then its immutability can in fact become a liability. This was the case for example with the Ethereum hack of last year where one rogue node was able to seize over 64 million dollars.⁵⁹

The blockchain technology ecosystem is indeed proactive and already working to address some of these limitations. The fact that the code is open source is critical here. On the other hand, changes to both the code and blockchain operations can only be accomplished by either consensus or if a majority of nodes agree on a way forward.

FIGURE 6 Bitcoin blockchain top miners, market share
1 April, 2017



Blockchain applications

In spite of being a base layer, blockchains do not require the Bitcoin protocol to be operational. Blockchain technologies can be used in other areas and sectors where transactions, interactions, and events among actors take place. This includes both tangible and intangible assets.

Keeping abreast of blockchain innovation and development is not an easy task as the sector is rapidly evolving on a global scale.⁶⁰ But what matters for this paper is how this is taking place in developing countries.

From a development perspective, introducing the concepts of public and private goods and their provision by the public and private sectors is essential.⁶¹ This paper highlights blockchain developments in relation to these two type of goods and services.

Before getting into specifics, it is critical to distinguish between delivery of the service and the recording and storage of such transaction on blockchains. Distributed ledger technology is not geared towards providing the actual service. Rather, it furnishes a secure, private, transparent and immutable record of transactions occurring during service provision.⁶² For example, the UK is already using blockchain to make welfare payments for instance. In addition, the government has set up blockchain as a service in the cloud, available only to public institutions.⁶³ The latter could be seen as a ‘best practice’ for developing countries. With land titles, the relevant public entity still has to issue the title to the owner. This issuance, and a digital fingerprint or hash of the land title, can be recorded in the blockchain to show proof of ownership and title legitimacy. Fraud prevention or title alteration by third parties can be addressed in this fashion.

The following subsections explore this evolution using the aforementioned categories of private and public goods and their provision by the private and/or public sector.

Guillaume Bolduc



BitFury

Founded in 2011 as a Bitcoin mining operation, BitFury now offers a full suite of hardware and software services for the blockchain ecosystem. The company has become quite profitable, with estimated revenues of US\$93.7 million in fiscal year 2017. BitFury works with a number of public and private sector actors, through its headquarters in Amsterdam and offices in San Francisco, Washington, DC, Riga, Latvia and Hong Kong.

BitFury is working with the Georgian Ministry of Justice, the National Agency of Public Registry, and economist Hernando DeSoto to manage land titles and notary services through blockchain, aiming to make it faster and easier for Georgians to register land titles in a fair and responsible way. The Government of Ukraine's new blockchain initiative is also supported by BitFury, with pilot projects in state registers, public services, social security, public health, and energy. BitFury has begun to develop AI on Blockchain for the healthcare industry.

PUBLIC GOODS

In most developing and emerging economies, governments are in principle the main providers of public goods such as justice, security, health and education, among others.⁶⁴ However, this does not imply that governments themselves deliver such goods. Most times, implementation is outsourced to private partners, both for-profit and non-profit.

This is the case for the design and current implementation of blockchain technologies in the global South. The fact that local regulations are way behind new technologies has provided fertile ground for this to take place as has already happened with other technologies.⁶⁵

GOVERNMENT SERVICES

In principle, blockchain technologies could be used for providing government services that involve the overall handling and management of public documents which, at least in many developing countries, people have a hard time obtaining. More generally, blockchains could be used to support the overall provision of most public goods to citizens and stakeholders, especially those that demand personal interaction and require individual identification.⁶⁶

An implicit link between blockchain technology and e-government⁶⁷ does exist, and it is now being explored by a selected group of blockchain startups. **ProCivis**,⁶⁸ a Swiss startup, will be soon launching a blockchain-based app store delivering selected government services to the public. It will also offer identity services to clients.⁶⁹ Recently, Ukraine signed an agreement with **BitFury**⁷⁰ to support the provision of public services to citizens, among other activities.⁷¹ Dubai has also joined the blockchain technology wave and is now planning to become a fully-fledged Blockchain City by 2020 as part of its ongoing Smart Dubai initiative.⁷²

Being an information rich area, health services could particularly benefit from distributed ledger technologies.

BitLand

Bitland is an experimental platform in Ghana using a blockchain to bridge the gap between the government and the undocumented areas lacking land titles. Bitland, which is voluntary, seeks to get personal and/or community consent and approval, time-stamps and government approval. Despite positive media, the project has run into a number of issues which have delayed its ability to be rolled out. It remains to be seen if the initiative will be able to successfully roll out its services, though a global offering was to be launched in the Fall 2017.

Several blockchain startups are now supporting these areas and doing work in countries such as the Philippines and Estonia, among others.⁷³ As mentioned before, health is one of the key targets for Hyperledger. In contrast, the education sector has not been able to attract a lot of interest from blockchain technology startups and consortia.⁷⁴ Most of the examples that follow show how blockchain technologies could support a wide variety of smart government programs and initiatives.

LAND TITLES

Land titles were perhaps the first area where blockchain technology planning and potential deployment took place in a developing country. In 2015 the government of Honduras signed an agreement with **Factom**,⁷⁵ a US startup, to use blockchains to manage land title registration and help manage fraud and corruption.⁷⁶

How did this happen? A local foundation promoting libertarian values initially approached the startup and then proactively built the bridge between the tech company and the central government. A confidential agreement was subsequently signed. However, a few months later the project came to a halt for reasons that are still unclear.

Last year, similar initiatives were also launched in Georgia⁷⁷ and Ghana.⁷⁸ In the case of Georgia, world-renown economist Hernando de Soto is involved as a member of the advisory board of BitFury, the blockchain startup implementing this initiative.⁷⁹ The case of Ghana is perhaps more interesting as a local not-for-profit startup, **BitLand**,⁸⁰ is using Bitcoin's blockchain to manage land titles and settle land disputes. BitLand is closely working with local institutions whose mandate is to issue land titles and are willing to try new technologies to solve issues that has been outstanding for decades. **BenBen**⁸¹, is yet another startup in Ghana working on the same topic.

Namecoin

The management of Internet Protocol addresses and names - the Domain Name System (DNS) - has given rise to issues around internet governance.

At the moment, internet governance is led by a multi-stakeholder coalition, currently heavily centralized although globally distributed. ICANN, the Internet Corporation for Assigned Names and Numbers, plays a key role in this structure.

Namecoin, created in 2012, is the first ever altchain whose main goal was to decentralize the management of the DNS. By modifying the original Bitcoin source code, creating its own blockchain, and allowing the systematic capture of key/names pairs, Namecoin provided the required tools to manage domain names and personal identities. However, its success has been relatively limited vis-à-vis the large DNS registrars.

The platform only caters to .bit domains which in turn can only be reached via specific add-ons or extensions in standard browsers. Furthermore, and perhaps more importantly, Namecoin has had little to no influence on Internet Governance debates.

Given the immutability inherent to blockchains, issues related to DNS squatting, domain names without relevant Internet Protocol addresses, and potential name seizures, Namecoin seems to be struggling.

While the initiatives in Ghana seem to have fizzled out, Sweden is successfully moving ahead with its own land titles project, thus moving beyond the proof-of-concept stage.⁸² In any event, this seems to suggest that blockchain deployments in developing countries face complex challenges.

IDENTITY SERVICES

As previously mentioned, [Namecoin](#) developed key technology for potentially protecting and authenticating personal identity, fostering freedom of speech and preventing surveillance.

Several startups are already working on blockchain identity services.⁸³ For example, [OneID](#)⁸⁴ provides multiple-factor authentication and Single Sign On services, among others.⁸⁵ This seems to be one of the most promising fields for the successful application of blockchain technologies as reflected by the increasing number of startups working in this area. Blockchain technology-based identity can be effectively used for managing passports, birth and wedding certificates, national and electoral IDs, and handling e-residence programs, among others.

However, some critics argue that existing digital ID technologies are working fine and are far more scalable than those using blockchain platforms.⁸⁶ Blockchain technology scalability limitations could prevent massive deployments in countries with large populations such as India and China.⁸⁷

FREEDOM OF SPEECH

Startups such as [FlorinCoin](#)⁸⁸ and [Publicism](#)⁸⁹ promote freedom of speech in different ways.⁹⁰ The former has created a distributed ledger application (Dapp) called *Alexandria* that aims to be a decentralized repository of knowledge and information managed directly by end users. One of its applications is the preservation of



Avel Chuklanov

censored digital content that usually quickly disappears from the Internet. Floricoïn has enhanced the blockchain by introducing the possibility of attaching comments to blocks in the chain. Publicism offers support to journalists that face censorship in many countries, allowing journalists to use pseudonyms to protect their identities.⁹¹ [MazaCoin](#),⁹² whose goal is to support native and indigenous US communities, recently started using its platform to protect freedom of speech and store protest photos on the blockchain.⁹³

ANTI-CORRUPTION

The US National Democratic Institute (NDI) has partnered with [BitFury](#),⁹⁴ the same startup doing land titles in Georgia, to promote anti-corruption efforts with a platform called Blockchain Trust Accelerator.⁹⁵ The purpose is to promote the development of blockchain applications that can foster open government and transparency. Launched in June 2016, there is not much information available yet on how the accelerator is evolving.

ELECTORAL PROCESSES

Electoral processes of various sorts have also benefited from the deployment and use of blockchain technologies. [Follow My Vote](#)⁹⁶ is a startup using distributed ledgers to run voting processes and prevent fraud and identity theft. One of the potential advantages is that voters using blockchains can verify their voting choices using their private keys at any point in time.⁹⁷ Ukraine is one country that has jumped into this area. The country will use [E-vox](#),⁹⁸ an Ethereum-based distributed ledger for local elections. Implementation has already started in a couple of towns.⁹⁹

One of the core issues however is access to the private keys which hackers could acquire in a variety of ways,¹⁰⁰ or voters could offer to loan or sell their private keys for economic benefit. Once it emerges as a viable method, it will be interesting to compare blockchain voting with Internet voting, which is already in use in Estonia.¹⁰¹

Bitnation

BitNation, founded in 2014, is a “Virtual Nation”, a decentralized nation not linked to any territory and only existing in the blockchain. BitNation aims to provide the same services as a traditional government, but in a way that is not bound by geography – rather, education, health services, and notary services are provided through the chain or through local contractors. BitNation has developed agreements with Estonia to support notary services for their e-Residents project. In 2015, BitNation developed a “Blockchain Emergency ID” as a response to the refugee crisis, allowing refugees who could not get other identity documents to receive an ID recorded on their identification documents and to receive Bitcoin Visa cards with funds that can be used in Europe. Bitnation has received a significant amount of media coverage since its inception, and represents a very libertarian position towards statehood.

9Needs

9needs, based in South Africa and started in 2012, uses blockchain and identity technology to tackle post-Apartheid social issues. Their most developed project is Amply, with aims to help the government use blockchain to manage Early Childhood Development Services. In 2016, 9needs received funding from the UNICEF Innovation Fund, and is being piloted at 50 centres in South Africa to help strengthen registration, contracting, and information management systems.

NEW FORMS OF GOVERNMENT

Some blockchain platforms aim at replacing or at least emulating government. The best example is [Bitnation](#)¹⁰² which allows users to create their own borderless countries that offer a series of services to its citizens. These countries have their own constitutions and some even offer basic income to its citizens.¹⁰³

AID AND DEVELOPMENT

Aid:Tech, a London based company is perhaps the first blockchain technology startup that supported humanitarian and development efforts in the Middle East.¹⁰⁴ The company provides a voucher system that can be used in even the most challenging contexts and helps ensure that financial resources securely reach their final destinations. Bitnation is now also offering support to [refugees](#).¹⁰⁵

On the UN side, UNICEF (UN Children’s Fund) disbursed USD 100,000 to support a startup, [9Needs](#),¹⁰⁶ and has plans for doing the same for another five to ten startups.¹⁰⁷ 9Needs works on health and development innovations. UNDP (UN Development Programme) is supporting cash transfers and financial tools in Serbia and Moldova, and has plans to expand to other countries soon.¹⁰⁸

UNWFP (UN World Food Programme) announced a blockchain technology pilot using Ethereum to disburse financial support to those in need in Jordan, building on the results of a smaller initiative in Pakistan.¹⁰⁹ According to one report, seven UN agencies are exploring and/or using blockchain technologies to support their operations and programs.¹¹⁰

RECAP

Deployments of blockchain technology in developing countries are not yet delivering any major disruptions on a sustained basis. Most are supply driven, operate as standalone initiatives not linked to ongoing programs, and local institutions play only a passive role with little sustained ownership. Local economic and political challenges are still formidable and will remain so unless blockchain technology deployments adopt a more comprehensive approach. In this light, blockchain technology initiatives engaged in broader smart government programs and identity services likely have the best chance for success in the medium term.



Clark Young

PRIVATE GOODS

The provision of private goods in the blockchain ecosystem has an internal financial sustainability component that works like a magnet for attracting suppliers - as long as prices are competitive. Even so, billions of people around the globe do not have access to such goods, particularly in the case of banking services. When they do have some minimal access, poor people must pay extraordinarily high fees to use private services, as we see with remittances.¹¹¹ Agriculture is another sector where private goods are pervasive - and a sector that provides livelihoods to most of the world's poor population.¹¹² Intellectual property rights are also an area where blockchain technologies could be effective for protecting digital and non-digital assets and ensuring royalties flow towards creators and innovators.

BitPesa

Bitpesa, a quickly growing company, has merged mobile money and blockchain technology. From the early pilot in 2013, it has received significant startup funding to serve emerging markets that include Nigeria, Kenya, Tanzania, Uganda, the Democratic Republic of the Congo and Senegal, as well as the UK. Bitpesa takes Bitcoin payments and exchanges them for local currencies which are then deposited into bank accounts or mobile money wallets. Bitpesa promises to be a cheap way to transmit money and remittances internationally, especially for underserved markets in the mobile money space in Africa.

BANKING FOR THE UNBANKED

M-Pesa, a product of mobile innovation in Kenya, was the first successful attempt to furnish basic banking services to those sitting at the bottom of the pyramid. Today, more than 90 countries are using similar schemes, serving nearly half a billion people. However, close to two billion people still remain without access to basic banking services.¹¹³

This is where entrepreneurs are hoping blockchain will help, via **BitPesa**.¹¹⁴ A Kenya-based startup run by expats, BitPesa supports transactions and payments between African businesses and the rest of the world using Bitcoin blockchain. In principle, the platform is open to anyone, including small and micro enterprises that could use these services to increase their businesses. BitPesa is thus markedly different from M-Pesa – but even so a legal dispute between the two has been ongoing for the last few months.¹¹⁵ BitPesa is active in the Democratic Republic of Congo, Kenya, Nigeria, Tanzania and Uganda, and has partners in the US and China. In addition to payments, BitPesa also exchanges Bitcoins into local currencies, as well as US dollars and other currencies.

BitSoko¹¹⁶ is another Kenyan startup that furnishes an Android-based Bitcoin wallet to reduce the relatively high transaction costs of other mobile money platforms, such as M-Pesa. Such costs oscillate between four to ten percent and BitSoko aims to reduce these fees to less than half a percent. It also offers a more secure and transparent platform by capitalizing on the benefits of Bitcoin blockchain. In 2015, BitSoko received support from the Gates Foundation to essentially create the portfolio of services the startup offers today.¹¹⁷ Although they plan to support feature phones in the near future, the application platform is only available for smartphones, which limits its coverage and usability to those able to afford the more expensive smart phone. In this context, it is still far behind M-Pesa and other mobile money platforms. Note that both BitPesa and **BitSoko** also support remittances.

In April 2017, the Gates Foundation launched its own initiative that will support the provision of financial services to the poor. The initiative will provide frameworks for government on how to use blockchain technology but also show its limitations in terms of scale and governance.¹¹⁸

REMITTANCES (A.K.A. REBITTANCES)

Remittances are probably one of the most competitive areas in the blockchain ecosystem due no doubt to its sheer market size and profitability. In 2015 alone, remittances were well over 500 billion USD, with 25 percent coming from the US alone.¹¹⁹ This year, the global average cost of transacting remittances was nearly seven and half percent, with Africa having higher average costs. Using traditional banks entails much higher costs, up to 11 percent, while prepaid cards remain the most affordable, at an average of 1.75 percent.¹²⁰

Clearly, this is an area where blockchain technology competition is already intense. Indeed, close to 30 startups and companies are already offering rebittance services in many countries.¹²¹ A good example here is [Abra](#),¹²² a Philippines-based startup that recently got financial support from international venture capital. Using Bitcoin's blockchain, the startup is now planning to expand to other countries. Note that the current app is only available for smartphones, so users who lack access to such devices must use a computer or similar device to access its services.

Another example is [Rebit](#),¹²³ also based in the Philippines, which is backed by a larger company whose goal is to promote Bitcoin in the country¹²⁴ and can be used to send money to the Philippines from anywhere in the world. The company says it does not charge user fees but requires users to buy Bitcoins to use the service. Recipients get local currency as Rebit does the conversion (thus keeping the Bitcoins) and are notified by both email and SMS.

On the development side, UNDP recently announced the launch of a blockchain remittances pilot in Serbia,¹²⁵ while UNICEF is exploring blockchain technologies for cash transfers.¹²⁶

As a result of the relatively large market share the sector has, remittances seem to be one of the most attractive and thus competitive sectors when it comes to blockchain technology deployment. Abra and BitPesa¹²⁷ are two of the current top six blockchain technology remittances companies, but could easily be displaced as other companies start to grow and gain market share.

AGRICULTURE

While the agricultural sector in industrialized countries rely heavily on the use of technologies of various sorts, this is certainly not the case in most developing countries. In fact, the sector has one of the lowest levels of technology investment, especially among small holder farmers. Mobile technologies have changed this a bit by providing information and services to producers, including pricing. So there are no shortage of blockchain startups emerging to support this sector. Common applications include: Tracking products and supply chains; facilitating payments to producers; keeping an eye on prices to ensure fair payment for produce; and enhancing community-supported agriculture.¹²⁸ For example **Skuchain**¹²⁹ uses smart contracts to keep track of agriculture supply chains (and is also used in many other sectors too).¹³⁰ However, it also seems to require a level of sophistication that might be beyond the average poor small holder farmer in much of the global South.

Farmshare¹³¹ supports community based agriculture which promotes communal forms of property and collaborative labor processes for developing local economies. Farmshare also uses smart contracts and Dapps to promote local products and ensure payments are distributed among participating communities.¹³²

Bitmari¹³³, another African Bitcoin wallet service for sending money, is supporting an accelerator and trust for female farmers in Zimbabwe.¹³⁴ The project is using crowdfunding to collect Bitcoins and then provide funding to 100 women farmers who are expected to receive technical assistance from experts.

Zbysiu Rodak



FOOD SECURITY

When it comes to food security and supporting small farmers and cooperatives, [AgriLedger](#)¹³⁵ seems to be the indisputable leader. Using blockchain and a mobile app that runs on smartphones, AgriLedger allows farmers to keep track of all transactions while providing unique IDs to each end user. Needless to say, the app requires access to mobile networks with data access. It is not clear if the startup has any plans to offer offline access.



Jenny Hill

INTELLECTUAL PROPERTY RIGHTS

As an immutable, distributed and transparent platform with built-in financial tokens, blockchain technology seems ideally positioned to support the protection of intellectual property rights. One clear example is the creation of blockchain technology-based intellectual property (IP) registries where IP owners can keep hashed digital certificates of their IP and even use the platform to get royalties from those who make use of their inventions using smart contracts.¹³⁶ Curiously, this is an area that so far has received relatively little attention from the blockchain technology ecosystem.

[Ascribe](#)¹³⁷ is one of the startups working in this area, focusing on protecting the IP of artists. The company uses Bitcoin's blockchain but has developed an open source protocol that interacts with the former and allows users to register intellectual property.¹³⁸ Artists can get certificates of attribution, certificates of ownership and manage licensing of their work to third parties.

Issues of piracy could be effectively addressed in this fashion but blockchain technology-based IP protection will need to work in sync with governments and legislators to make it enforceable in legal terms – and it could be this that is deterring the development and deployment of blockchains in this area. On the other hand, issues related to fair use of IP could be impacted negatively by a blockchain technology-based IP regime.¹³⁹

RECAP

Most blockchain technology initiatives targeting this selected group of private goods have a lot of potential but have yet to take off.¹⁴⁰ Some have already stopped or suspended operations altogether while others are struggling to generate solid revenues. This may be a symptom of intense startup competition in a market that is still incipient and where much-needed venture capital is scarce. Blockchain technology-driven progress in areas such as banking for the poor and agriculture is scant and overshadowed by other technologies such as mobiles. In this light, remittances and digital money seems to be most promising areas at this point.

CONCLUSION

The review of blockchain technology applications indicates that barriers to entry remain high in comparison to other technologies such as mobile apps. Mobile innovation diffused rapidly to developing countries in spite of lower technology skills and limited Internet access – and the emergence of over 100 tech hubs in the African continent is hard evidence of this.¹⁴¹

Blockchain technology innovation seems to demand higher levels of knowledge and capacity. While tech hubs and techno-entrepreneurs have been active in developing countries for many years, local blockchain uptake has been relatively slow - and certainly not as impressive as that of mobile technologies. But this does not mean blockchain initiatives are bound to fail in the global South. On the contrary, in most cases the technology is being tested in several sectors, and for the first time. Some startups in the global South have indeed harnessed blockchain technologies but are deploying vanilla platforms developed in the North; and while current trends suggest that blockchain innovation is mostly happening in the North, deployment is taking place globally which will quickly impact innovation ecosystems in the global South too.

Andrew Branch

Blockchains and human development

The previous section provided a glimpse into a gamut of blockchain technology applications with potential relevance to development. While it is possible to conclude that the range of applications is wide, the overall depth is still shallow. Many of the initiatives described above are still on paper or about to begin while others are fully operational but serving only very few clients and stakeholders, and many have also failed. This is perhaps the result of the fact that the technology is still in its infancy, and just entering its take off stage.

Regardless, development practitioners looking for innovative solutions to tackle traditional development gaps should have an adequate non-technical understanding of the potential blockchain technologies could have in supporting and enhancing development programming. This section explores this by using the analytical framework presented in Annex I, with an additional 'governance' perspective to further elucidate blockchain's potential to enhance democratic governance.

INFRASTRUCTURE AND INFOSTRUCTURE

Recent data indicates that almost four billion people do not have access to the Internet, and most happen to live in the developing world.¹⁴² In addition, while urban centers in the global South have the latest access to technologies and broadband at their disposal, those living in rural and marginalized communities, and those too poor to buy either access or technology tools do not. It thus seems unlikely that people living in such conditions will be able to become blockchain technology network nodes, or could effectively run wallet software to at least benefit from the technology as end users.¹⁴³ Granted, this is not unique to blockchain, but it does affect the way the technology should be deployed and harnessed if the final goal of interventions is to foster human development among those who are socially excluded.

What is unique to blockchains is the required and extensive use of cryptographic tools which demand the development of a different kind of infrastructure, or infostructure: **public key infrastructure**.¹⁴⁴ Public key infrastructure, which encompasses the roles, policies and procedures needed to secure the electronic transfer of information, is not yet in place in many developing countries. This poses serious obstacles to the systematic use of blockchain technology and is especially relevant for the effective and transparent provision of public goods in a distributed fashion. Not surprisingly, advocates have already suggested the deployment of *decentralized* public key infrastructure using blockchain technology, thus bypassing the traditional centralized model.¹⁴⁵

CAPACITY DEVELOPMENT

From the end user perspective, using cryptographic tools on a regular basis can be a formidable challenge. A recent study of U.S. college students - many of whom are 'digital natives' - suggests that even among this population enormous obstacles need to be overcome before cryptographic tools become mainstream.¹⁴⁶ Similarly, whistleblower Ed Snowden had a difficult time communicating with journalists because most could not use such tools, never mind install the appropriate software in their laptops.

Two separate issues emerge here. One is the use of such tools. The second relates to the management of end user private and public keys. As mentioned before, blockchain wallets can and have certainly provided friendly interfaces that facilitate the creation and use of public key cryptography, even though

the end user might not fully understand how this works.¹⁴⁷ But users need to be able to manage their private keys and safely store them somewhere, somehow. These two issues together might prove to be too demanding for populations that have relatively low levels of education and literacy, and who face social exclusion.

As discussed in section 3 above, a few startups from developing countries have been relatively successful in harnessing blockchains, despite limited uptake on the client side. Most of them are using Bitcoin's blockchain. However, none of these startups are introducing innovations to adapt the code to local contexts or develop new features, and unlike mobile technologies apps, Dapps are not being developed either. This strongly suggests that higher level technical skills are required to make this happen at the local level.

Countries such as Ghana and Kenya have benefited from existing tech hubs and networks to harness blockchains and thus have an incipient innovation ecosystem that could support its local development. This could then become a launching pad for blockchain innovation in the global South in the medium run, especially if venture capital or other external financial mechanisms become available, including development assistance.

POLICY AND REGULATION

As is the case with many other technologies fostering the so-called sharing economy,¹⁴⁸ blockchain technology, spearheaded by Bitcoin's rise, is running ahead of local policies and regulation. While industrialized countries have already started to catch up, this is certainly not the case in most developing countries where policy and regulatory capacities are still incipient. This gap facilitates the use of distributed ledger technologies in the global South not only for local startups but also by those based in the North. In terms of the latter, this group of countries can become places where proof-of-concept pilots and prototypes are deployed, and enhance startup expertise and competitive advantage on a global scale. This is in fact what is already taking place in several developing countries.

The lack of national public key infrastructure policies in these countries can also initially be seen as further propelling blockchains, though on the other hand it may also become a liability should security issues related to public key management emerge, such as key theft or key trafficking.¹⁴⁹ If this is the

case, public key infrastructure policies are indeed needed, even if the actual implementation is done via decentralized models using blockchain technologies.

As most startups using the blockchain are sticking to Bitcoin, then policy and regulation of cryptocurrencies are also important. This includes services offering the conversion of Bitcoins or altcoins into local currency as well as the use of cryptocurrencies as legal tender. Furthermore, local policies and regulations are also important for security reasons in countries where conflict and violent extremism are rampant and financing of such activities should be closely monitored to prevent their global spread.

INSTITUTIONS

DISTRIBUTED NETWORKS AND THE STATE

As is the case with some of the previous Internet technologies, Blockchains can also promote further reduction of some, if not all, forms of central government. Indeed, one of the motivations that drove Nakamoto to develop Bitcoin was the response by governments to the 2007/2008 global economic crisis.¹⁵⁰ Many of the early supporters of Bitcoin blockchain were libertarians who saw the new technology as the most effective tool to eliminate state interventionism for good.¹⁵¹ The distributed nature of the technology coupled with a new form of decentralized trust and distributed consensus provide the fodder for such views.

However, this does not necessarily mean that blockchain is inextricably linked to such views, nor is anyone seriously expecting the state to vanish any time soon. As a matter of fact, and as described in the previous section, many blockchain startups are working directly with government to deploy the technology at the state level. More recently, the creator of Ethereum has changed his perception about the relevance of libertarian philosophy in the current political juncture.¹⁵²

An issue which has been largely ignored up until now is the potential blockchain could have in supporting and enhancing the devolution of government within a given nation-state. State decentralization, also called local governance, has been a core development issue, and many developing countries already have overarching decentralization policies. However, local governments face serious fiscal and capacity issues and are unable to deliver public goods. Blockchain



Zi Jian Lim

technology could thus furnish real benefits to local governments. The argument for decentralized or distributed government services blockchain pundits promote could become an excellent win-win opportunity.

INSTITUTIONAL CAPACITY

Harnessing new technologies by developing countries requires, in addition to fiscal resources, institutional capacities that facilitate their deployment on a sustained basis. Such capacities are not limited to knowledge of technology but also include administrative and managerial capacities as well as clear rules of the game established by law and enforceable throughout. Many developing countries are still building and developing such capacities which seriously limits their ability to jump on board when technology innovations such as blockchains and others emerge. As seen in the examples examined in section 4, this has not prevented them from using the latest technologies. On the contrary, developing country institutions can embrace the use of blockchains by either importing know-how and expertise and/or using local expertise, if available, outside government. The real issue here is that such initiatives might not be sustainable in the medium run. They are usually done in isolation, delinked from other public institutions and operate outside policy processes that allocate fiscal resources to public institutions.

From an institutional perspective, it is also important to factor in how blockchains should be used in the public sector. While the current view suggests that blockchain technologies should entirely *replace* current processes, it is also possible to consider the technology as complementing and supplementing processes,¹⁵³ in addition to introducing innovation within the public sector.

Finally, distinguishing between design and implementation of blockchain initiatives is essential. While public institutions need to be involved in the former, the latter can be undertaken by private partners (profit and non-

profit) that are better qualified to do so. This is what indeed happened with mobile app development in developing countries. However, this does not seem to be the case for current blockchain technology pilots, and this could have negative implications for scaling up such pilots and ensuring their long-term sustainability.

THE GOVERNANCE OF BLOCKCHAINS

Calls for a new social contract raise key questions about blockchain: who is in charge, who is going to draft such a contract, and how can all voices be included?¹⁵⁴ A quick response from the blockchain camp is straight forward: No one is in charge as, by default, no need for this exists.¹⁵⁵ In fact, everyone is in charge as governance is done by consensus only. Such consensus in turn is based on algorithms¹⁵⁶ that allow users and nodes to almost automatically agree on the outcomes of the process.

One of the core ideas of this *governance by algorithmic consensus* is the decentralized autonomous organization (DAO). Groups of individuals seeking to promote a common outcome, a business objective or a political intervention get together and agree on a series of principles that are coded into software. The software then takes control of the overall operation, and places individuals, who now do not need to interact among themselves anymore, in the background. Several issues emerge here and can be highlighted as follows:

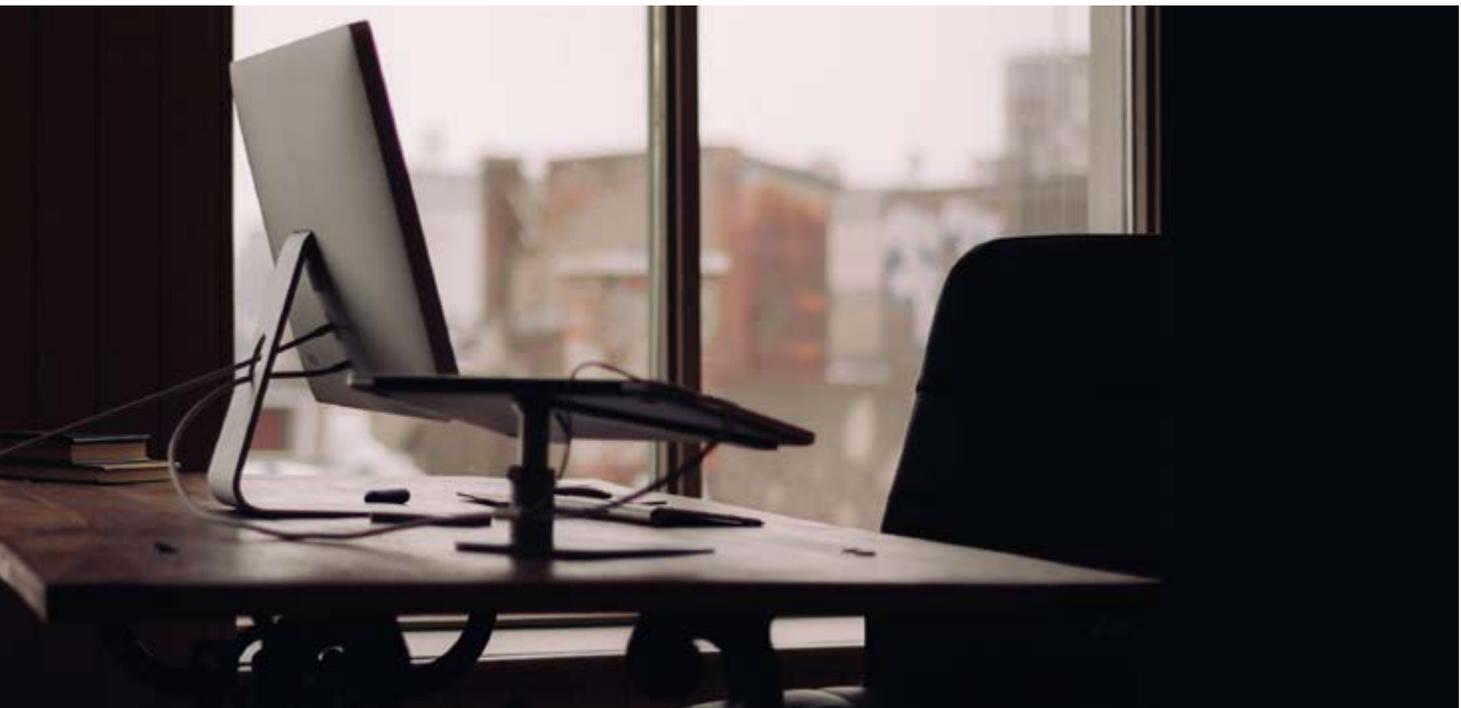
Coding: Who is doing the actual coding? How were they selected? Coding envisages the translation of the agreements between DAO members into a particular programming language, including machine learning, which runs the smart contract and automatically triggers particular events when certain conditions are met.

Code comprehension: Who can actually read and audit the code? Most blockchains use open source software which means that anyone has access to the code. But users must be able to read and understand the code itself. By analogy, reading a free book in say Chinese requires that the reader knows the language. Otherwise, the free book lacks value for the potential reader, regardless of the cost. Those who cannot read code will then have to seek trusted third parties who can ensure the code does reflect what has been agreed.¹⁵⁷

Scalability: As described in section 2, blockchains have well-known limitations when it comes to scalability. While upcoming innovations in the sector could help address the issue, the push to keep the number of blockchains to a

minimum could be counterproductive. If this number increases instead then interoperability among blockchains becomes a larger issue.¹⁵⁸ Furthermore, how will the growth in blockchain technology to billions of user and nodes impact on reaching decentralized consensus? Issues of democratic representation within the network might emerge in the near future.

Trust vs. governance: The fact that trust is decentralized and depersonalized and placed instead on a distributed network does not automatically imply enhanced governance.¹⁵⁹ For example, nodes and users that were not part of the original design of the blockchain did not participate in the process and were not part the governance decisions made by those who were. Users either join under given conditions but are also free to go somewhere else if they do not like it.



Luke Chesser

These issues point to the fact that blockchains, even though decentralized and distributed, cannot guarantee that hierarchies and inequality among peers will not take place. In fact, this is exactly what seems to be happening now when it comes to blockchain mining.¹⁶⁰ The same can be said about blockchain coders, developers and techno-entrepreneurs, all of whom seem to have a privileged position in the network and can muster substantial power over all other nodes. Inequality within a decentralized network is thus feasible.

Finally, some blockchain enthusiasts seem to endorse the view that algorithms, programmed by a selected few, could or should rule society and perhaps even replace individual interactions.¹⁶¹ However, algorithms are not neutral, nor immediately transparent to most.¹⁶² What is perhaps needed is a decentralized network ensuring the transparency and democratic governance of algorithms.

From a governance and development perspective, most of the above presupposes a considerable level of development of democratic institutions and democratic values. Actual relevance to a specific developing country should be assessed on a case-by-case basis. But in principle, the lower the level of human development, the more complex it would be to implement blockchain technology in systematic fashion.

Conclusions

Adoption and widespread use of blockchain technologies face challenges that are already familiar to ICT for Development practitioners. Perhaps a new ingredient in the mix is the complexity of blockchain technology itself. This brings in additional issues and obstacles in terms of both technology deployment and its diffusion to end users and stakeholders. This is certainly the case in contexts where both infrastructure development and local capacities are below world averages.

Blockchain technology is still in its infancy and supported by a relatively small but highly qualified group of innovators and techno-entrepreneurs. Together, they could address most if not all the limitations and challenges highlighted in this paper. Blockchain's innovation potential is thus large. While this speaks volumes for blockchain technology, it is still early to draw final conclusions on how the technology will evolve in the next five years or so. At the moment, hype is leading the charge. But current evidence on blockchain technology deployments shows the technology is still in a proof-of-concept stage.¹⁶³

Many blockchain applications examined in this paper are already on the ground. But most are operating on a small scale, have few clients and/or cover a few stakeholders, particularly in developing countries. A few governments have taken the leap and are trying to harness blockchain technology to tackle gaps in public goods provision. However, most are running as pilots and lack clear long-term strategies.

Replacing ongoing initiatives or launching new ones on standalone blockchain platforms will only delay blockchain adoption. The best approach for developing countries is to deploy blockchain technologies to complement or supplement ongoing programs and initiatives. This could lower entry barriers while increasing the chances of making initial blockchain technology investments sustainable in the medium term while catering to local needs and development gaps.

Usability issues might also limit blockchain diffusion in developing countries. Widespread use of cryptographic tools in poor countries face formidable challenges, especially if blockchain technology initiatives target the poorest sectors of the population. The assumption that every single beneficiary must use and manage private and public keys is not realistic. The lack of public key infrastructure in most developing countries will only exacerbate this. The only way to break out of this impasse is to devise alternatives that furnish

end users with access to cryptographic tools via intermediaries such as community-based organizations, small enterprises and local governments. The key point here is that end users need not own or directly use technology to benefit from its deployment.

Broader blockchain technology initiatives linked to smart government seem to be best positioned to make blockchain a key catalyst in delivering public goods. Remittances and digital money in the private goods area also have great potential; however, they might not promote economic and financial inclusion of those sitting at the bottom of the pyramid.

While blockchain technology is a standard bearer of decentralization, this paper has shown that mining is prone to centralization and concentration. In the early days of Bitcoin blockchain, anyone with a laptop or PC could mine the network. Today, this can only be accomplished by a few who have the financial resources and hardware to do so and can afford to pay high energy bills. The same goes for the notion of consensus. Blockchain technology replaces human consensus with algorithmic consensus. The issue here is not only consensus automation, but also one of representation and scale. Decentralized autonomous organizations and blockchain networks are small in terms of the number of people involved.¹⁶⁴ Most blockchain users are clients using wallet software and thus not part of any consensus building process, algorithmic or not. As it stands today, blockchain technology seems ideal for small scale operations, given its lack of scalability and other limitations highlighted in this paper.

Blockchain technologies could disrupt development soon. However, it is still early days as the technology is rapidly evolving. Success in developing countries will depend on blockchain effectiveness to enhance human development. And this, in turn, will depend on how the themes highlighted in the previous section are tackled. Algorithms alone will not suffice.

Both the Internet and mobile technologies triggered positive disruption in development practices but not to the degree expected when they first emerged. In this light, the other relevant question is if blockchain technologies can foster deeper levels of disruption in development processes than its predecessors. The potential is there. But more targeted action will be required to have such impact in development processes.

Recommendations

Based on the analysis and findings of this paper, these are the recommendations [repeated from the Executive Summary].

RESEARCH

Undertake a series of selected case studies on ongoing blockchain technology initiatives that are taking place in developing countries. While some anecdotal information on such initiatives can be found, little in terms of academic or developmental research is currently available. Indeed, a large vacuum exists here that has helped spread blockchain hype even more.

Undertake further research and analysis on both blockchains for governance and the governance of blockchains vis-à-vis governments and the provision of public goods. In particular, the links between trust, consensus building and representation have not been explored in the existing literature.

Link current and future work on blockchain technology to Artificial Intelligence as the latter is being systematically introduced into the technology and related “decentralized applications” or Dapps. This points back to blockchain’s governance issue and the governance of algorithms in general which are not participatory, nor transparent. Is blockchain part of the solution?

Consider opening new and pioneering research on the governance of algorithms and the impact they can have in society, especially in developing countries. This theme is in turn linked to the notion that technologies are social products. In the end, society ends up shaping how technology is harnessed. However, the prevailing view today seems to be the opposite, blockchain technology included.

Explore innovative approaches and solutions to facilitate blockchain technology access to those sitting at the bottom of the pyramid, focusing on access and use of cryptographic tools. Here, distinguishing technology use and ownership from its benefits is crucial. Previous technology deployments have shown that poor communities can benefit from them without directly using or owning a particular technology. Community networks and shared mobile telephone use are well-known examples here.

PROGRAMMING

Explore the role of ongoing innovation initiatives and existing tech hubs in developing countries to support blockchain deployments. Africa and Asia, in particular, have a considerable number of technology hubs which can furnish adequate expertise to deploy blockchain technologies with local expertise and to target the provision of public goods.

Consider funding or supporting small blockchain pilots or prototypes focused on specific development themes, the SDGs or local priorities in developing countries. Funding need not be large but special attention should be placed on the human development impact. As mentioned above, identity and government services using blockchain technologies are the most relevant at this point and have already been implemented in other contexts.

Support or help create a network of blockchain technology innovators and entice them to support applications that foster public goods provision. Attracting local innovators in emerging and developing economies is of critical importance here.

NETWORKING AND PARTNERSHIPS

Support the creation of a blockchain for blockchain-related projects in developing countries, or consider the creation of a related sustainable knowledge base. Partnering with international experts and other innovators on a global scale should be part of such initiative.

There has been some action by **multi-laterals and overseas development funding agencies on linking blockchain technologies to the implementation of the SDGs.** Development agencies and development practitioners should join these efforts to track the latest developments and eventually undertake further research on the topic.

Launch or help organize a ‘blockchain for development’ network, or a decentralized autonomous organization with key donor countries and organizations. The main goal of such a network could be to keep the development perspective atop, and above blockchain itself.



NASA

ANNEX I

Analytical Framework

The field of Information and Communication Technologies for Development (ICTD) furnishes the core analytical framework for this paper, drawing together these four different perspectives under one umbrella analysis. For the purposes of this paper, the emphasis is on the 'development' part of the ICTD framework.

Perhaps the best known dimension of ICTD is the so-called digital divide which is still wide in many developing countries. Not surprisingly, the digital divide is just a reflection of existing socio-economic and gender gaps in the global South. However, the link between these seemingly different divides is not usually acknowledged. In this light, attempts to close the digital divide without taking into account socio-economic and other intersectional gaps usually translate into endeavors that cannot be sustained in the medium to long run.

But even if such attempts are successful, as one might argue has been the case with mobile technologies in developing countries, they do not automatically foster social inclusion or new economic opportunities for those sitting at the bottom of the pyramid. Recent research on the topic¹⁶⁵ has shown that while the horizontal diffusion of new technologies has accelerated around the globe in the last 15 to 20 years, its *vertical penetration* within developing countries is still incipient. And this quintessential distinction demonstrates that effectively harnessing new technologies in many developing countries is a more complex issue that transcends the traditional digital divide.

Most developing countries have no option but to import or use technologies developed elsewhere, usually from industrialized nations. They must allocate a wide variety of resources to adopt and adapt the new technologies to the local context and needs. This is certainly the case for the productive sector of the economy (including the service sector) or in government investments in technology, as is the case of e-government for example.

As a new and potentially disruptive technology, blockchains will not be exempt from the diffusion patterns that other equally disruptive technologies such as the Internet have experienced in most developing countries. It is of course feasible that blockchains will expand as fast as say mobile technologies in the last 20 years or faster. But even so, the conditions and environment under which this is feasible still need to be examined. In this light, this paper places the focus on the following pillars as they relate to the diffusion of new technologies:

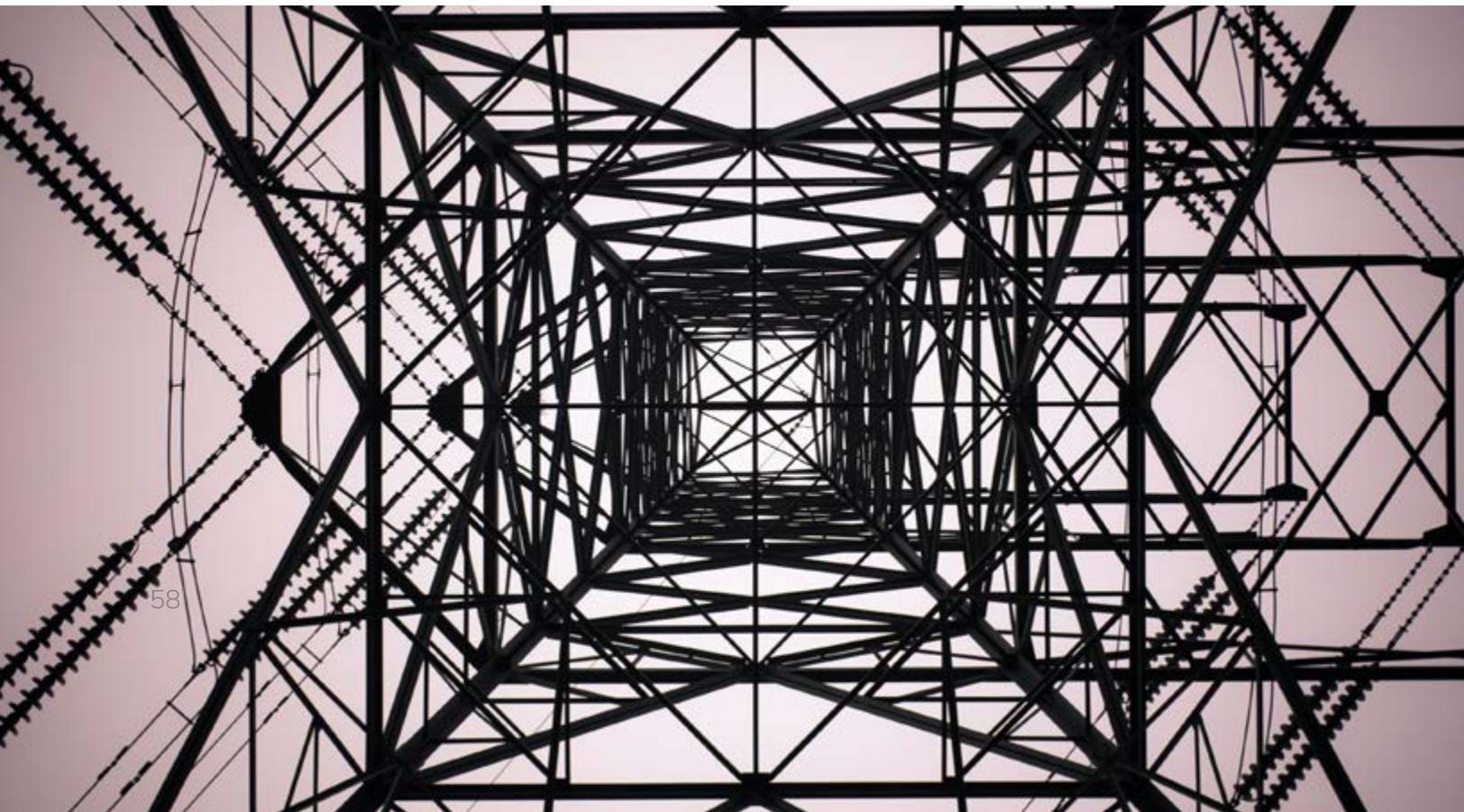
Infrastructure: Private and public investments that support overall infrastructure development in a country but not limited to ICTs only. For example, access to the electrical grid, and health and education infrastructure are also included.

Capacities: The human capacities that countries should have to develop and deploy new technologies. This is not limited to technical capacities but also includes functional capacities which are cross-cutting and go beyond ICT.

Policy and regulation: The capacity of government at all levels to develop, implement, and enforce policies within the territory under their control.

Institutions: The “rules of game” environment that allow people to undertake activities within a given institutional context, including the private sector and civil society organizations. Governance mechanisms are part of this, especially new models based on multi-stakeholder engagement.

Shane Rounce





Cargo Cult

ANNEX II

Blockchain technologies and innovation

OVERVIEW

Blockchain technologies are based on four different technologies initially brought together under one umbrella by the creator of Bitcoin. They are:

- ▶ Peer-to-peer networks
- ▶ Decentralized, distributed databases
- ▶ Cryptography
- ▶ Proof of work algorithm (to solve the so-called double-spending issue)

PEER-TO-PEER NETWORKS

In a peer-to-peer network all interconnected nodes are in principle equal. No central server exists, nor is there need for one. These networks are thus characterized by the lack of a *central point of failure*. *If one node goes down, all others remain interconnected - and data and information flowing through the network is preserved.* Nodes are thus both *clients and servers* at the same time.

In the Internet era, the now defunct music-sharing site Napster, created in 1999, is perhaps the best example of a peer-to-peer network. Napster was effectively used for decentralized file sharing: Once on the network, a particular file could be located in thousands of nodes, if not more. Nowadays, BitTorrent is one of the largest peer-to-peer networks on the Internet.¹⁶⁶ Both Napster and BitTorrent use their own protocols for network communication and interaction.¹⁶⁷ The [Interplanetary File System \(IPFS\)](#)¹⁶⁸ is the most advanced incarnation of a peer-to-peer network using [distributed hash tables](#).¹⁶⁹

WHO IS WHO IN BLOCKCHAINS: USER/NODE TYPES

As open source software, blockchains are available to anyone who downloads the software into a computational device. Once running, the device becomes one more node or user in the peer-to-peer network. In principle, anyone with a device connected to the Internet can join the network. Five generic types of actors are part of a Blockchain peer-to-peer network:

Core developers: The group of people who have write access to the source code of blockchain technologies. Code changes however must be approved by the network community.

Full nodes: These are the nodes that have up-to-date copies of the blockchain, validate new blocks and propagate them across the network.

Miners: Nodes dedicated to running proof of work, competing with each to find the required header hash to add a new block of transactions to the blockchain.

End users: Users who use the network to do the transactions they need by connecting the network node using client or wallet software. End users need not have full copies of the blockchain to be active on the network.¹⁷⁰

Service nodes: Nodes providing services to other nodes such as wallets, exchanges, mixers, storage, and cloud services, among others.

In Bitcoin's case, a [foundation](#)¹⁷¹ was created to raise public awareness and influence government policy and regulation, among other things.

DECENTRALIZED, DISTRIBUTED DATABASES

In simple terms, a database running on a peer-to-peer network is decentralized as by default nodes store copies of the structured data. The distributed attribute refers to the way database processing is undertaken within the network. A database is distributed if the computations required to modify the data are executed by a set of network nodes - and not by one central server (Raval, 2016).¹⁷²

Note that a centralized database can also be distributed - this is in fact the prevailing model used by leading Internet companies.¹⁷³

CRYPTOGRAPHY

Extensive use of cryptographic tools is one of the distinctive characteristics of blockchain technologies, which use public key cryptography. *Public key cryptography (PKC)* uses key pairs: a private key known only to its owner and a public key which is shared with the world. PKC allows for the asymmetric creation of private and public keys. A private key is first generated in random fashion. The private key is then used to create a public key. The private key is used to encrypt the transaction which can then be decrypted by the intended recipient using the sender's public key. Note that it is mathematically impossible to use a public key to decipher a private one.

In Bitcoin, the public key is used to create a Bitcoin address.¹⁷⁴ Bitcoin and other wallet (client) software usually provides the functionality to easily create such keys, as well as to store private keys in digital devices, paper or in other nodes who provide such services. End users can generate multiple Bitcoin public keys to process transactions.¹⁷⁵

HASHING

Blockchains store information in structured fashion. *Each block in the chain has a defined structure that includes four columns or fields. One of them is the block header which is in turn comprised of six different fields. The block header is used to generate a unique identifier or block hash for the current in question and includes the unique identifier from the previous block.*

A hash is a cryptographic function that can take any input of variable length and convert it into a fixed-length output. The probability of two different inputs having the same hash output is close to zero: Any single input has a unique hash output. Guessing the value of the original input from a resulting hash output is not feasible. Reverse engineering is not possible here.

However, verification that a hash is the output of an input can be easily accomplished: hashing is computationally efficient. This is the hashing property that allows network nodes to validate or corroborate the outcome of the proof of work competition process which in turn makes decentralized consensus possible.

A block hash is actually the digest of the six fields that comprise the block header, serving as a unique identifier for the block in question. Computation of the block hash for the uses the block hash of the previous block thus creating a mathematical link between the two.¹⁷⁶

To generate a block hash, the block header is encoded using a **cryptographic hash function**¹⁷⁷ that generates a string of alphanumeric characters presented in **hexadecimal**¹⁷⁸ format, instead of the regular decimal notation. Reading a Blockchain record with the naked eye will consequently not reveal a lot as most of the content has actually been hashed.¹⁷⁹

In a nutshell, a cryptographic hash function encodes data or text of any size and produces a unique fixed-length output called a **digest**¹⁸⁰ or **digital fingerprint of the input furnished**. Blockchains use **SHA-256**^{181, 182} which generates a digest comprised of 256 bits or 32 bytes or characters.

Hashing Example

As an example, using SHA-256 on the phrase “Blockchain: Disrupting Development?” produces the following digest in hexadecimal format:¹⁸³

a86b5ca5e16b840d152779b7c8378a01ae441d211¹⁸⁴

Adding the letter **s** at the end of the word Blockchain yields

66a1cc69b0dbb6d7d0ae27c18c87a8c5648dc5af1b3091ed093bb02437dd50aa

which is totally different from the first one, even though only one character was changed.

In principle, it is almost impossible for two different inputs to have the same digest. By the same token, it is not possible to select beforehand a particular digest for any given input. Finally, it is not feasible to guess or decipher the content furnished to a hash function from the resulting digest.

Blocks can also be identified by their position in the Blockchain or row number. This is called the *block height* which is not part of the block data structure itself but is rather generated dynamically.¹⁸⁵ Block height allows for indexing of Blockchain entries for faster retrieval and effective search for particular block entries.

PROOF OF WORK ALGORITHM

Proof of work is a *brute force algorithm* used by network miner nodes who compete among themselves to find the header hash for a new block of transactions. By design, the difficulty of finding a new hash increases overtime, as the number of entries in the chain increases. Similarly, miners rewards tend to decrease overtime in terms of new Bitcoins created.

As mentioned in section 2 (and the Executive Summary), proof of work has some similarities with the *guess the number puzzle that kids play*. However, *proof of work* is certainly much more complex.

For starters, proof of work must find a hexadecimal number that has 256 alphanumeric characters. Secondly, the first 8-9 characters of that number must all be zeros. Third, the number sought must be below a previously defined threshold. And finally, miners must use as input the solution found in the previous proof of work process, alongside a number which is used to perform the calculations.¹⁸⁶

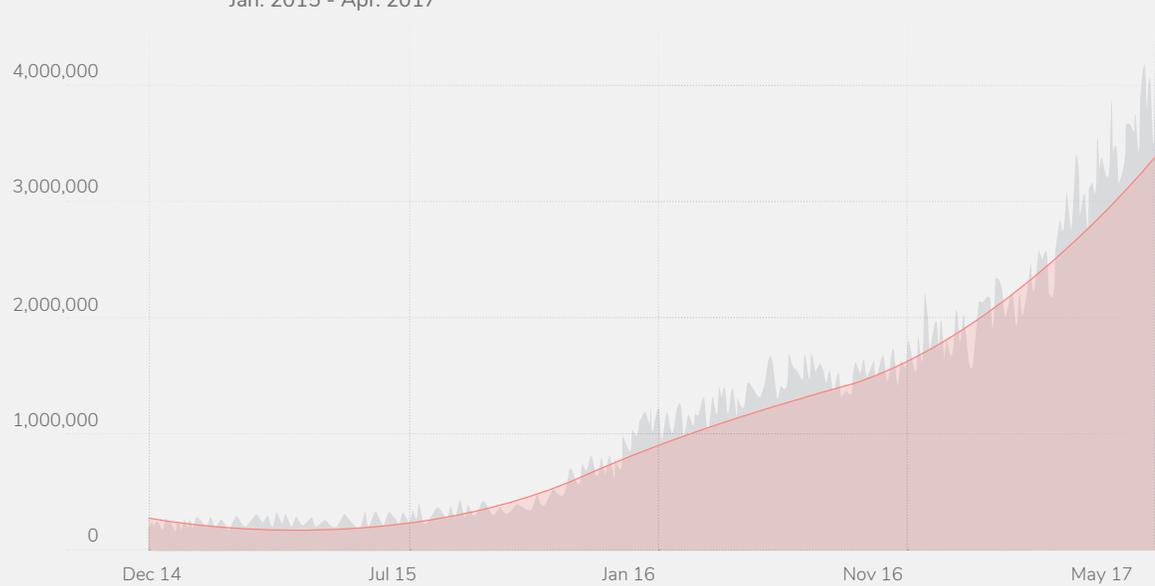
Entering this race demands heavy computing power, and even so, finding the result might take billions of iterations. Specialized and expensive hardware has been developed to tackle blockchain technologies' proof of work algorithm.¹⁸⁷ In similar fashion, mining is mostly undertaken by *mining pools* which essentially use peer-to-peer distributed computing to find the solution to the puzzle. Large and small miners can be part of a pool and distribute the rewards according to the amount of work completed if they win the competition.

Figure 7 shows the absolute growth of hash rates in the last couple of years. While actual growth seems to be decelerating, the actual value is still large and demands huge computing power and energy resources. In this light, proof of work is not one of the most efficient or smart algorithms.

FIGURE 7

Bitcoin blockchain hash rates
Jan. 2015 - Apr. 2017

Source: blockchain.info



Being that as it may, proof of work solves long standing issues such as **double-spending**¹⁸⁸ and the **Byzantine Generals' problem**.¹⁸⁹ It also protects the peer-to-peer network from **Sybil attacks**.¹⁹⁰



BLOCKCHAIN INNOVATIONS

Blockchain innovations transcend new cryptocurrencies.¹⁹¹ This does not mean that such applications do not create new cryptocurrencies. Most do and in fact use it as part of the incentive for miners to solve proof of work or other similar algorithms. Nodes offering services to end users and other nodes in the network can also benefit from such incentives via fees or other arrangements.¹⁹²

As in many other technologies, innovation is the driving force in the evolution of blockchain. Overall, three broad types of innovation have taken place:¹⁹³

- 1 **Cryptocurrency innovation** aimed at improving the overall functions and limitations of Bitcoin. Applications that focus on creating alternatives to Bitcoin as cryptocurrency are known as *altcoins*. So-called colored coins also fall under this header. Most of these platforms use Bitcoin's Blockchain.
- 2 **Consensus innovation** aimed at addressing the high costs and seeming inefficiency of proof of work algorithms. Proof of stake and variations on the original proof of work algorithm are part of this.
- 3 **Blockchain innovation** *per se* aimed at expanding the use of blockchain beyond cryptocurrencies and into many other areas. Examples here include **Namecoin**¹⁹⁴ and **Ethereum**.¹⁹⁵ Some authors have labelled this set of applications as *altchains* as they use blockchains that are independent from Bitcoin.¹⁹⁶

Nowadays, many altcoins and altchains are operational.¹⁹⁷ Overtime, the focus of overall blockchain innovation has shifted away from cryptocurrencies to innovations leading to improved and expanded use of distributed ledger technology across the board. A complementary innovation whose initial goal was to foster the interoperability of Bitcoin Blockchain with other altcoins and altchains is *sidechains*.¹⁹⁸ Current trends suggest that distributed ledger innovations will continue to lead the pack while alternative cryptocurrencies or altcoins will experience further decline in the medium term.¹⁹⁹ In any event, looking a bit more closely at the first altchain platforms can shed light as to how blockchains have evolved overtime.

NAMECOIN

The management of Internet Protocol addresses and names, or the Domain Name System (DNS) has given rise to the issue of Internet governance which at the moment is led by a multi-stakeholder coalition. The current system is heavily centralized although globally distributed. **ICANN**,²⁰⁰ the Internet Corporation for Assigned Names and Numbers, plays a key role in this structure.

Namecoin, created in 2012, is the first ever altchain whose main goal was to decentralize the management of the DNS.²⁰¹ By modifying the original Bitcoin source code, creating its own blockchain, and allowing the systematic capture

of key/names pairs, Namecoin provided the required tools to manage domain names and personal identities. However, its success has been relatively limited vis-à-vis the large DNS registrars. The platform only caters to *.bit* domains which in turn can only be reached via specific add-ons or extensions in standard browsers.²⁰² Furthermore, and perhaps more importantly, Namecoin has had little to no influence on Internet Governance debates.²⁰³

Given the immutability inherent to blockchains, issues related to DNS squatting, domain names without relevant Internet Protocol addresses, and potential name seizures, Namecoin seems to be struggling.²⁰⁴



ETHEREUM

Ethereum is usually closely associated with smart contracts. This however is only partially true as the platform can support a wide range of applications where the interaction and/or coordination among peers in a given network can be programmed and automated.²⁰⁵ The key point here is that peers themselves agree on how this should happen and can then code this into the blockchain. This is called a smart contract and is supported by a Decentralized Autonomous Organization or DAO. But in reality Ethereum is a programmable blockchain²⁰⁶ that can serve as a basis for the development of a wide variety of decentralized applications or Dapps.²⁰⁷

Ethereum also addresses the potential centralization inherent to the Bitcoin protocol where only miners with sophisticated hardware can effectively run proof of work algorithms. Ethereum uses instead the proof of stake algorithm.²⁰⁸ In a nutshell, proof of stake requires nodes that want to compete in the mining process to post a bond or security deposit in Ethereum's currency, the ether. This potentially eliminates the need for expensive hardware and the associated energy costs.

Ethereum can also have built-in artificial intelligence components, including deep learning algorithms for example, to implement smart contracts and support Dapps development. In recent weeks, Ethereum has gained substantial ground and is now becoming one of Bitcoin's main competitors, although the platforms clearly have distinct functionality and goals.

Hyperledger

Hyperledger is an inter-industry collaboration space to develop open protocols and standards for distributed ledger technologies. It aims to improve the performance and scalability of blockchains. Hyperledger is currently supporting financial and health applications.

HYPERLEDGER

More than an innovation in blockchain per se, **Hyperledger** is an inter-industry collaboration space to develop open protocols and standards for distributed ledger technologies. Initially created by the Linux Foundation in 2015, Hyperledger now has over 100 industry members, including companies from across Asia. It also aims at improving the performance and scalability of blockchains.

At the moment, Hyperledger is supporting financial and health applications and will soon start work on supply chains.²⁰⁹



Lee Ferrell

RECAP

In contrast with Namecoin, Ethereum has had a relatively greater impact on the blockchain ecosystem, while Hyperledger is one of the many new blockchain technology consortia that have recently emerged.²¹⁰ In any event, these examples show the quick evolution of distributed ledger technology in recent years. The pace has barely slowed since and innovation in this space continues to take place at a rapid pace.

ENDNOTES

- 1 <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>
- 2 <http://secondmachineage.com/>
- 3 <http://thezeromarginalcostsociety.com/>
- 4 In this paper, technology is used as a synonym of Information and Communication Technologies (ICTs) and excludes all other technologies.
- 5 Nakamoto (2008).
- 6 Dark side in terms of potential negative impact on jobs and income, and also in terms of the so-called singularity in which intelligent machines eventually end up controlling the human race. As an example see: <http://time.com/3614349/artificial-intelligence-singularity-stephen-hawking-elon-musk/>.
- 7 See for example Tapscott (2016: 25): “The result can be an economy of peers with institutions that are truly distributed, inclusive and empowering - and thereby legitimate. By fundamentally changing what we can do online...the new platform may even create the technological preconditions to reconciling some of our most vexing issues.”
- 8 Developing nations were part of the mobile innovation wave of the last decade. Mobile apps created in Kenya and other developing countries started to be deployed on a global scale. From one perspective, mobile apps can be seen as micro-applications with low entry barriers requiring basic technical and coding skills, pretty much unlike older web applications that required a greater degree of knowledge and higher technology skill sets. See UNDP (2013).
- 9 See: Ashish Gadnis (2016) “Opinion: Blockchain offers poorest a real economic identity — and a shot at the SDGs.” Devex blog (7 November). <http://bit.ly/2hP8HdT>
- 10 Blockchain technologies could be considered as a **General Purpose Technology**. See Kane (n.d.).
- 11 Technical details are included in Annex II below.
- 12 <https://en.wikipedia.org/wiki/Cryptocurrency>
- 13 The history of digital currencies in general and of Bitcoin in particular is beyond the scope of this paper. For details on such history see Popper (2016).
- 14 It should be noted that in his pioneering paper, Nakamoto (2008) did not use the word ‘blockchain.’ Rather, the author made reference to a chain of blocks running on a ‘timestamp server.’
- 15 <https://en.wikipedia.org/wiki/Ledger>
- 16 Swan (2015) argues that Blockchain is the base layer for Bitcoin or any other similar protocols that run on it.
- 17 https://en.wikipedia.org/wiki/Dark_web
- 18 https://en.wikipedia.org/wiki/Silk_Road
- 19 See Popper (2016) for additional details.
- 20 The recent hacker attack on over 100 countries using ransomware is one example: Hackers are demanding payments in Bitcoin to ‘liberate’ the information they have encrypted. See Gautham (2017). “Bitcoin Ransomware Makes Global IT Infrastructure ‘WannaCry.’” NewsBTC, 13 May. <http://www.newsbtc.com/2017/05/13/bitcoin-ransomware-makes-global-infrastructure-wannacry/>.
- 21 Google trend numbers are relative, not absolute. For any keyword search, it identifies the maximum number of searches on a given day or year and divides all others by it. The maximum is thus always 100. In any event, it is clear that Google searches for blockchain technologies are still on the rise.

- 22 <https://en.wikipedia.org/wiki/Peer-to-peer>
- 23 There seems to be some confusion on the difference between decentralized and distributed networks. For a clear conceptual definition see the classic paper by Baran (1962). In this light, blockchain could be characterized as a *decentralized distributed network*.
- 24 Contrast this with the current Internet-based information and services paradigm where centralization is a core feature that generates substantial value for the companies furnishing such services.
- 25 Source is Baran (1962).
- 26 In Bitcoin, a new block of transactions is added every ten minute or so. A block added to the chain can have a maximum of 2,200 transactions, give or take.
- 27 Some authors have defined blockchains as “the trust protocol.” See Tapscott (2016: 3 & ff)
- 28 “One-CPU-one vote,” Nakamoto (2008: 3); and the majority of CPUs prevail.
- 29 There are other algorithms that can achieve the same result. For example, Ethereum has proposed proof of stake. See Annex II for more technical details.
- 30 http://www.abcya.com/guess_the_number.htm
- 31 Technical details are in Annex II.
- 32 A binary hash or **Merkle Tree** is used here. See appendix II for details. Note that hashing a hash is also feasible and is actually widely used in blockchain.
- 33 The record of recent Bitcoin transactions can be seen [here](#).
- 34 For example Swam (2015). References to Hayek et.al. are also common in this literature.
- 35 This is partly based on Atzori (2015). **Futarchy** and **Franchalutes** are not included here as they do not seem relevant in developing country contexts.
- 36 Consensus (2016). “Liquid democracy and emerging governance models.” 24 August. <https://media.consensus.net/2016/08/24/liquid-democracy-and-emerging-governance-models/>.
- 37 This in fact is the definition of a “smart contract.”
- 38 For a concise typology of decentralized organizations see Raval (2016).
- 39 **Smart contracts** (also known as self-executing contracts, blockchain contracts, or digital contracts) are algorithmic transactions that execute pre-defined contractual agreements. The terms of the agreement are coded into a blockchain and are automatically executed by the software. Some smart contracts make use of AI to ensure contracts can have some adaptability. Smart contracts enable two or more pseudo-anonymous parties to conduct business (usually over the internet), without the need for a centralized authority. For more, see: <https://blockgeeks.com/guides/smart-contracts/>.
- 40 See for example <http://www.reform.uk/reformer/government-in-blockchains-ii-disrupting-bureaucracy/>
- 41 <https://bitnation.co/>
- 42 This is one of the clarion calls of Tapscott’s book.
- 43 Consortium blockchains can be seen as a third type. Here, a preselected number of nodes run the consensus process which is thus private. See Buterin, V. (2016). “On public and private blockchains.” Ethereum, 7 August. <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>
- 44 Some discussion on the feasibility of centralized blockchains is now taking place. See Buntinx, JP (2016). “A centralized blockchain solution will not solve financial fraud.” The Merkle, 22 May. <http://themerke.com/a-centralized-Blockchain-solution-will-not-solve-financial-fraud/>.

- 45 Hybrid blockchains are distributed ledgers that combine aspects of public, consortium and private blockchains.
- 46 See for example Walport (2016).
- 47 <https://www.corda.net/>
- 48 <https://ripple.com/>
- 49 See Corda's [white paper](#) for further details.
- 50 Mixer services are developing innovative alternatives to ensure full anonymity. For additional details see Novetta (2015). "Survey of Bitcoin Mixing Services: Tracing Anonymous Bitcoins." Novetta, September. https://www.novetta.com/wp-content/uploads/2015/10/NovettaBiometrics_BitcoinCryptocurrency_WP-W_9182015.pdf.
- 51 This applies only to public and permission-less blockchains.
- 52 Brenig, C. (2017) "Transparency through Decentralized Consensus: The Bitcoin Blockchain and Beyond." Albert-Ludwigs-Universität Freiburg. Unpublished Ph.D. Dissertation. <https://freidok.uni-freiburg.de/fedora/objects/freidok:11559/datastreams/FILE1/content>.
- 53 For more on the block size debate, see: Lester Coleman (2017). "Extension Block Proposal Stumbles In Attempt to End Bitcoin Block Size Debate." Cryptocoins News, April 4. <https://www.cryptocoinsnews.com/extension-block-proposal-stumbles-trying-end-block-size-debate/>.
- 54 Deetman, S. (2016) "Bitcoin Could Consume as Much Electricity as Denmark by 2020." Motherboard, March 29. <http://motherboard.vice.com/read/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020>.
- 55 Zambrano, R. (2017). "Blockchain mining: Competition and (de)centralization." April 24. <http://blog.raulza.me/blockchain-mining-competition-and-decentralization/>.
- 56 Data for Ethereum shows similar patterns: <https://etherscan.io/stat/miner?range=7&blocktype=blocks>.
- 57 Ethereum's Blockchain is about half that size. Downloading such a large file over a slow connection can be cumbersome. <https://bitinfocharts.com/>
- 58 The Morning Paper (2017).
- 59 For more, see: Coleman, Lester (2016) "Ex-Ethereum Developer: How the DAO Hack Happened and What Comes Next." Cryptocoins News. (July 30th) <https://www.cryptocoinsnews.com/ex-ethereum-developer-dao-hack-happened-comes-next/> or Ore, Jonathan. 2016. "How a \$64M hack changed the fate of Ethereum, Bitcoin's closest competitor." CBC News (Aug 28). <http://www.cbc.ca/news/technology/ethereum-hack-blockchain-fork-bitcoin-1.3719009>
- 60 One report indicates that at the beginning of this year there are over 1,200 blockchain active startups. See Michalik, V. & L. Lundy. (2017). "Frost & Sullivan identifies the 2017 global blockchain startup map". Marginalia, March 31. For a list of the 2017 top 250 blockchain companies see Blockchain Daily News. (2017). "Top 250 blockchain companies and startups". http://www.blockchaindailynews.com/Top-250-blockchain-companies-startups_a24712.html.
- 61 See Kaul (2003) for a definition of public goods more relevant to the age of globalization than the traditional one.
- 62 Higgins, S. (2016). "UK Government Trials Blockchain Welfare Payments System". Coindesk, 7 July. <http://www.coindesk.com/uk-government-trials-Blockchain-welfare-payments-system/>.

- 63 Prisco, G. (2016).
- 64 This is based on Kaul's definition of public goods. Kaul (2003).
- 65 The Economist (2016) "Uberworld: The world's most valuable startup is leading the race to transform the future of transport." September 3. <http://www.economist.com/news/leaders/21706258-worlds-most-valuable-startup-leading-race-transform-future>.
- 66 Mougayar, W. (2016) "The Blockchain is Perfect for Government Services." Coindesk. September 3. <http://www.coindesk.com/Blockchain-perfect-government-services-heres-blueprint/>.
- 67 Included here are: e-governance, open government, and smart government.
- 68 <https://procivis.ch/>
- 69 Ngo, D. (2017) "Procivis Set to Release Blockchain-Powered e-Government 'App Store' This Year." Bitcoin Magazine. February 8. <https://bitcoinmagazine.com/articles/procivis-set-release-blockchain-powered-e-government-app-store-year/>.
- 70 <http://bitfury.com/>
- 71 Chavez-Dreyfuss, G. (2017) "Ukraine launches big blockchain deal with tech firm Bitfury." Reuters. April 19. <http://www.reuters.com/article/us-ukraine-bitfury-blockchain-idUSKBN17F0N2>.
- 72 Lohade, N. (2017) "Dubai Aims to Be a City Built on Blockchain." Wall Street Journal. April 24. <https://www.wsj.com/articles/dubai-aims-to-be-a-city-built-on-blockchain-1493086080>.
- 73 Dyrda, L. (2016) "8 blockchain healthcare startups to know." Becker's Health IT & CIO Review. August 30. <http://www.beckershospitalreview.com/healthcare-information-technology/8-Blockchain-healthcare-startups-to-know.html>. Healthcoin, a Dutch startup, is focused on personal health only.
- 74 See Watters, A. (2016) "The Blockchain for Education: An Introduction." Hackededucation.com. April 7. <http://hackededucation.com/2016/04/07/Blockchain-education-guide> and Tierion (2016).
- 75 <https://www.factom.com/>
- 76 See Colindres (2016) for details.
- 77 Forbes (2016) A recent update is here: <https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/#1281b034dcdc>.
- 78 Mwinsuubo, N. (2017) "Bitland Ghana Land Title Protection News." Bitland Global. March 7. <http://bitlandglobal.com/cadastral-land-registry-news-ghana/>.
- 79 See: <http://bitfury.com/team>.
- 80 See: <http://www.bitland.world/oracle/index.php>.
- 81 See: <http://benben.com.gh/>.
- 82 Latest developments are here: Keane, J. (2017) "Sweden Moves to Next Stage With Blockchain Land Registry." Coindesk. March 30. <http://www.coindesk.com/sweden-moves-next-stage-blockchain-land-registry/>.
- 83 Mesropyan, E. (2017) "21 Companies Leveraging Blockchain for Identity Management and Authentication." Let's Talk Payments. 13 February. Also: <https://letstalkpayments.com/22-companies-leveraging-blockchain-for-identity-management-and-authentication/>.
- 84 <http://www.oneid.com/>

- 85 See Swan (2015) chapter 3 for additional details.
- 86 Cooper, A. (2016) "Does digital identity need blockchain technology?" Gov.uk. August 15. <https://identityassurance.blog.gov.uk/2016/08/15/does-digital-identity-need-Blockchain-technology/>.
- 87 India's national ID programme, Aadhaar, puts the issue of scale in the forefront.
- 88 <http://florincoin.org/>
- 89 <https://steemit.com/blockchain/@pieterhaasnoot/publicism-blockchain-based-free-press>
- 90 A startup company recently announced a new Internet router that uses Blockchains to prevent surveillance and beef up security. See Young, J. (2016) "Blockchain Router Solution to Government Surveillance, Nodio Believes." Coin Telegraph. November 4. <https://cointelegraph.com/news/Blockchain-router-solution-to-government-surveillance-nodio-believes>.
- 91 Cobben, I. (2016) "Blockchain technology to improve press freedom." World News Publishing Focus. August 2. <http://blog.wan-ifra.org/2016/08/02/Blockchain-technology-to-improve-press-freedom>.
- 92 <https://www.mazacoin.org>
- 93 Rogoff, Z. (2016). "Blockchain versus pipeline: uncensorable protest against fossil fuel development." Medium. October 16. <https://medium.com/@zakkai/Blockchain-versus-pipeline-uncensorable-protest-against-fossil-fuel-development-bc03412f9229#sgdbxd24a>.
- 94 <http://bitfury.com/>
- 95 Swislow, D. (2016) "What the blockchain could mean for democracy in the digital age." National Democratic Institute. June 23. <https://www.demworks.org/what-Blockchain-could-mean-democracy-digital-age>.
- 96 <https://followmyvote.com/>
- 97 Follow My Votes uses bitshares, a financial oriented blockchain platform, as its main technology.
- 98 <http://e-vox.org/>
- 99 See: <http://e-vox.org/e-vox-memo/> and <http://e-vox.org/balta-installs-e-voxnarada/>.
- 100 Burns Koven, J. (2016) "Block The Vote: Could Blockchain Technology Cybersecure Elections?" Forbes, August 30. <http://www.forbes.com/sites/realspin/2016/08/30/block-the-vote-could-Blockchain-technology-cybersecure-elections/>.
- 101 An evaluation of Estonia's platform is here: Springall, D. et.al. (2014). "Security Analysis of the Estonian Internet Voting System". ACM, November. <https://estoniaevoting.org/findings/paper/>.
- 102 <https://bitnation.co/>
- 103 Comparing Bitnation to the 13 year old Second Life platform could be the source for a case study in alternative forms of national government.
- 104 Clark, A. (2016) "Blockchain In Humanitarian Efforts Leads To Award Nomination." Aid:Tech. August 2. <https://aid.technology/charity-digital-news-Blockchain-in-humanitarian-efforts-leads-to-award-nomination-for-aidtech/>.
- 105 See: <https://refugees.bitnation.co/>.
- 106 See: <http://9needs.net/this-is-results-lab/>.
- 107 Higgins, S. (2016) "UNICEF Just Invested in its First Blockchain Startup." Coindesk. 15 November. <http://www.coindesk.com/unicef-just-invested-first-blockchain-startup/>.

- 108 Begovic, M. et.al. (2016) "UNDP Alternative Financing Lab - the next big thing is a lot of small (and smart things)!" UNDP Croatia. September 19. <http://www.hr.undp.org/content/croatia/en/home/blog/2016/9/19/UNDP-Alternative-Financing-Lab-the-next-big-thing-is-a-lot-of-small-and-smart-things-.html>.
- 109 del Castillo, M. (2017) "The UN Wants to Adopt Bitcoin And Ethereum – And Soon." Coindesk. April 24. <http://www.coindesk.com/the-united-nations-wants-to-accept-ethereum-and-bitcoin-and-soon/>.
- 110 Higgins, S. (2017) "Seven United Nations Agencies Are Now Investigating Blockchain Applications." Coindesk. April 27. <http://www.coindesk.com/7-united-nations-agencies-are-now-investigating-blockchain-applications/> and <https://www.blockchain-expo.com/2017/04/blockchain/un-launches-request-information-blockchain-based-international-assistance/>.
- 111 As mentioned before, this paper does not focus on financial services. But for a detailed analysis on these services vis-a-vis innovation and blockchain, see Skinner, 2016.
- 112 Agriculture employs 40 percent of the world's working population and up to 75 percent in poor countries in Africa and Asia. http://www.momagri.org/UK/agriculture-s-key-figures/With-close-to-40-%25-of-the-global-workforce-agriculture-is-the-world-s-largest-provider-of-jobs-_1066.html.
- 113 Data from GSMA's 2015 Mobile Money global report: http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/04/SOTIR_2015.pdf.
- 114 <https://www.bitpesa.co/>
- 115 See: <https://www.bitpesa.co/blog/bitpesa-v-safaricom/>.
- 116 <https://bitsoko.wordpress.com/about/>
- 117 Caffin, G. (2015). "Meet the Kenyan Startup Trying to Change Bill Gates' Mind on Bitcoin". Coindesk, July 23. <http://www.coindesk.com/meet-the-kenyan-startup-trying-to-change-bill-gates-mind-on-bitcoin/>.
- 118 Woyke, E. (2017). "How Blockchain Can Bring Financial Services to the Poor". MIT Technology Review, April 18. <https://www.technologyreview.com/s/604144/how-blockchain-can-lift-up-the-worlds-poor/> and Gates Foundation. (n.d.). "Financial Services For The Poor - Strategy Overview". <http://www.gatesfoundation.org/What-We-Do/Global-Development/Financial-Services-for-the-Poor>.
- 119 Pew Research. (2016) "Remittance Flows Worldwide in 2015." August 31. <http://www.pewglobal.org/interactives/remittance-map/>.
- 120 World Bank. (2016) "Remittance Prices Worldwide." September 19. https://remittanceprices.worldbank.org/sites/default/files/rpw_report_sept_2016.pdf. The SDGs include a target that calls for the reduction of remittances costs to three percent maximum. See: <https://sustainabledevelopment.un.org/sdg10>.
- 121 See: <http://themoneywiki.com/wiki/alternative-currency-rebittance-bitcoin-remittance>. Note that some of the links here are already dead.
- 122 <https://www.goabra.com/>
- 123 <https://rebit.ph/>
- 124 Satoshi Citadel Industries: <http://sci.ph/about.html>.
- 125 Begovic et.al. (2016), cited above,
- 126 Higgins, S. (2016) "UNICEF Eyes Blockchain as Possible Solution to Child Poverty Issues." Coindesk. February 3. <http://www.coindesk.com/unicef-innovation-chief-Blockchain-child-poverty/>.
- 127 Buntinx, JP. (2017) "Top 6 Bitcoin and Blockchain Remittance Companies." The Merkle. April 18. <https://themerke.com/top-6-bitcoin-and-blockchain-remittance-companies/>.

- 128 Additional examples are in this web page: <http://www.ccgrouppr.com/practical-applications-of-Blockchain-technology/sectors/agriculture/>.
- 129 <https://www.skuchain.com/>
- 130 Alisson, I. (2016) "Skuchain: Here's how blockchain will save global trade a trillion dollars." International Business Times. February 8. <http://www.ibtimes.co.uk/skuchain-heres-how-Blockchain-will-save-global-trade-trillion-dollars-1540618#>.
- 131 <http://farmshare.us/>
- 132 Farmshare's white paper is here: https://www.academia.edu/16673793/FarmShare_Blockchain_Community-Supported_Agriculture. Farmshare's web site says the project is now on hold which probably means it has hit a dead end.
- 133 <http://bitmari.com/>
- 134 Campbell, R. (2016) "BitMari's Farmers Accelerator Program Aims to 'Decolonize African Agricultural Economies.'" Bitcoin Magazine. November 8. <https://bitcoinmagazine.com/articles/bitmari-s-farmers-accelerator-program-aims-to-decolonize-african-agricultural-economies-1478638863>.
- 135 <http://www.agriledger.co/>
- 136 Cawrey, D. (2014) "How Bitcoin's Technology Could Revolutionize Intellectual Property Rights." Coindesk. May 8. <http://www.coindesk.com/how-block-chain-technology-is-working-to-transform-intellectual-property/>.
- 137 <https://www.ascribe.io/>
- 138 Higgins, S. (2015) "Blockchain Startup Raises \$2 Million for Intellectual Property Solution." Coindesk. June 24. <http://www.coindesk.com/blockchain-startup-2-million-intellectual-property/>.
- 139 Rogers, B. (2015). "How the Blockchain and VR Can Change the Music Industry, Part 1." Medium. November 24. <https://medium.com/cuepoint/bc-a-fair-trade-music-format-virtual-reality-the-blockchain-76fc47699733>.
- 140 Micro-finance and micro-credit are yet another areas where blockchain technologies could be used, as is happening in Burma. See Dhaliwal, S. (2016) "Blockchain Makes Microfinance Accounting Foray in Burma Led by Infoteria and Tech Bureau of Japan." Cointelegraph. June 28. <https://cointelegraph.com/news/Blockchain-makes-microfinance-accounting-foray-in-burma-led-by-infoteria-and-tech-bureau-of-japan>.
- 141 Kelly, T. (2014) "Tech hubs across Africa: Which will be the legacy-makers?" World Bank. April 30. <http://blogs.worldbank.org/ic4d/tech-hubs-across-africa-which-will-be-legacy-makers>.
- 142 ITU (2016). <http://www.itu.int/en/mediacentre/pages/2016-PR30.aspx>. This number includes those who access the Internet via mobiles phones.
- 143 Note that M-Pesa for example was not limited by Internet connectivity. It allowed users with feature phones to benefit from mobile money via SMS. SMS-based wallets for Blockchains will probably be a bit more difficult to implement, given the required use of public key cryptography on the client side. In addition, the security risks could be much higher.
- 144 https://en.wikipedia.org/wiki/Public_key_infrastructure
- 145 Allen, C. et. al. (2015) "Decentralized Public Key Infrastructure: A White Paper from Rebooting the Web of Trust." December 23. <https://danubetech.com/download/dpki.pdf>.
- 146 Routi, S. et. al. (2015) "Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client." Arxiv. October 29. <https://arxiv.org/pdf/1510.08555v1.pdf>.

- 147 See The Morning Paper (2017).
- 148 The Economist. (2016) "The Rise of the Superstars, Special report." 16 September. <http://www.economist.com/news/special-report/21707048-small-group-giant-companiessome-old-some-neware-once-again-dominating-global>.
- 149 A dark market for private keys, for example.
- 150 Popper (2015).
- 151 Ibid.
- 152 Pearson, M. (2017) "Ethereum's Boy King Is Thinking About Giving Up the Mantle". Motherboard. April 24. https://motherboard.vice.com/en_us/article/ethereums-boy-king-is-thinking-about-giving-up-the-mantle.
- 153 Werback (2016) provides further details.
- 154 This discussion is focused in distributed ledger technologies that could be used to enhance human development and it thus ignores Bitcoin and all other altcoins.
- 155 Recall Nakamoto's "One CPU, one vote" principle.
- 156 Such as proof of work which is a brute force, inelegant and inefficient algorithm.
- 157 A rental lease is a good example for a smart contract. The contract can be easily put on a blockchain and every month rental payments happen on an automatic basis until the contract expires. However, renters should not be expected to be able to read the computer code to sign the contract so they must trust the algorithm by default. Opacity trumps transparency here.
- 158 Sidechains could be seen as a partial solution to this issue.
- 159 Blockchain technology does not really eliminate the need for trust. Rather, it changes the way trust functions within a distributed network.
- 160 See: <https://blockchain.info/pools>
- 161 This perspective, accompanied by the re-emergence of Artificial Intelligence in the age of big data, are triggering the development of the so-called black box society. See Pasquale (2015).
- 162 O'Neill (2016) dwells into this particular topic and brings forward real life examples on how algorithms can indeed destroy people's lives.
- 163 For implementation issues related to this stage see: Harris, P. (2017) "Despite the Success of Blockchain POCs, Deploying Pilots Won't be Easy (Part One)." Distributed. May 4.
- 164 M-pesa for example has over 20 million users in Kenya. Facebook has over one billion users. Could we have the same scale for a blockchain application?
- 165 Comin (2013).
- 166 BitTorrent history and details are summarized here: Johnsen, J.A. et. al. (2005) "Peer-to-peer networking with BitTorrent." NTNU, Department of Telematics, December. <http://web.cs.ucla.edu/classes/cs217/05BitTorrent.pdf>.
- 167 BitTorrent uses [Distributed Hash Tables](#) (DHT).
- 168 <https://ipfs.io/>
- 169 https://en.wikipedia.org/wiki/Distributed_hash_table
- 170 Simplified Payment Verification or SVP is used for such clients. SVP was part of Nakamoto's original Bitcoin design.

- 171 <https://bitcoinfoundation.org/>
- 172 Proof of work mining via mining pools is thus distributed.
- 173 Many blockchain technologies observers use distributed and decentralized as synonyms.
- 174 This is a rather complex process summarized here on the Bitcoin Wiki: https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses
- 175 Bitcoin uses [Elliptic Curve Cryptography](#).
- 176 The block header is actually hash two times with SHA-256. In other words, the resulting digest from the first SHA-256 operation on the block header becomes an input for the second hash operation. This reduces the possibility of attacks by increasing the security of the final digest.
- 177 https://en.wikipedia.org/wiki/Cryptographic_hash_function
- 178 <https://en.wikipedia.org/wiki/Hexadecimal>
- 179 Most blockchains store metadata or data about data. And the metadata is in turn encoded.
- 180 An encrypted digest becomes a digital signature.
- 181 SHA stands for Secure Hash Algorithm and was created by the US National Security Agency, NSA.
- 182 <https://en.wikipedia.org/wiki/SHA-2>
- 183 The digital signature actually has 64 hex characters. Bear in mind that a regular character is represented by two contiguous hexadecimal symbols so the total number of actual characters is 32.
- 184 Online hashing tools are available. Check <http://www.fileformat.info/tool/hash.htm> for example. It is also possible to hash files, documents, photos, etc.
- 185 A quick glimpse of Bitcoin's blockchain in real time can be seen here: <https://Blockchain.info/>. To see the data structure of say block 436132 see <http://bit.ly/2e040Pm>.
- 186 This number is called a *nonce*.
- 187 For the evolution of Bitcoin mining hardware, see Szmigielski (2016).
- 188 <https://en.bitcoin.it/wiki/Double-spending>
- 189 http://www-inst.eecs.berkeley.edu/~cs162/fa12/hand-outs/Original_Byzantine.pdf
- 190 https://en.wikipedia.org/wiki/Sybil_attack
- 191 “*Forking*” of the original Bitcoin software base is what, to a large extent, has led to such innovations. The fact that the original software is open source implies that all forks must remain as such.
- 192 One of the core issues for innovators is if they should endorse Bitcoin or create a competing currency. While many new cryptocurrencies have been created, nowadays the high price of Bitcoins has become a magnet towards its use. Bitcoin has also become a valuable financial asset.
- 193 This is based on Antonopoulos (2015).
- 194 <https://namecoin.org/>
- 195 <https://www.ethereum.org/>
- 196 Antonopoulos (2015).
- 197 A comprehensive list with financial data is available here: https://bitinfocharts.com/index_v.html. Note that there are many small players competing side by side with a few large and dominant ones. However, the rapid increase in Bitcoin price has permeated all other altcoins and altchains.

- 198 Sidechains can improve the usability and scalability of blockchains, as well as their interoperability. This paper will not pursue this topic in systematic fashion as it falls beyond its original scope. See Back, A. et. al. (2014) "Enabling Blockchain Innovations with Pegged Sidechains". 22 October.
- 199 This does not necessarily mean that altcoin innovation is about to disappear. *Zcash*, a new altcoin that promises true anonymity, is a recent example.
- 200 <https://www.icann.org/>
- 201 Bear in mind that Namecoin can also be used for other purposes such as identify protection, etc.
- 202 Namecoin was also able to successfully address *Zooko's triangle* which was previously thought as being unsolvable.
- 203 Namecoin was invited to the latest ICANN meeting held in Copenhagen last March.
- 204 Further details in Kaldoner (n.d.).
- 205 This introduces the potential of software bugs into the blockchain as shown by the Ethereum hack where one node stole over \$64 million. See Siegel, D. (2016) "Understanding the DAO attack". Coindesk, June 25.
- 206 See Ethereum's intro paper: <http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html>.
- 207 Ethereum is a *Turing-complete* platform; that is, it has universal applicability, in computing terms. See Buterin (2013).
- 208 Casper proof of stake is being developed by Ethereum: <https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/>. Ethereum is also exploring other alternatives at this time.
- 209 See: <https://www.hyperledger.org/industries>.
- 210 There are over 25 global blockchain technology consortiums. See Mougayar, W. (2016). "The State of Global Blockchain Consortia". Coindesk, December 11. <http://www.coindesk.com/state-global-blockchain-consortia/>

REFERENCES

- Aitken, R. (2016) "Bitland's African Blockchain Initiative Putting Land on the Ledger." *Forbes*. April. <https://www.forbes.com/sites/rogeraitken/2016/04/05/bitlands-african-blockchain-initiative-putting-land-on-the-ledger/#57fff9e67537>
- Antonopoulos, A. M. (2015) *Mastering bitcoin: Unlocking digital cryptocurrencies*. Sebastopol, CA: O'Reilly.
- Asharaf, S., & Adarsh, S. (2017) *Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities*. doi:10.4018/978-1-5225-2193-8
- Atzori, M. (2017) "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?" *Journal of Governance and Regulation*, 6(1). doi:10.22495/jgr_v6_i1_p5
- Baran, P. (1962) *On Distributed Communications: I. Introductions to Distributed Communication Networks*. The RAND Corporation. Santa Monica. http://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf
- Bithub (2016) *The Blockchain Opportunity in Africa*. Nairobi: Bithub. <http://bithub.co.ke/booksale/>
- Böhme R, N. Christin, B. Edelman and T. Moore (2015) "Bitcoin: economics, technology, governance." *Journal of Economic Perspectives*, 29(2): 213 -38.
- Buterin, V. (2013) "A Next-Generation Smart Contract and Decentralized Application Platform." *Ethereum*. www.ethereum.org/pdfs/EthereumWhitePaper.pdf
- Catalini, C., and Gans, J. (2016) *Some Simple Economics of the Blockchain*. NBER. doi:10.3386/w22952
- CoinDesk (2017) "A Branch of the UN Just Launched Its First Large-Scale Ethereum Test." May 02. <http://www.coindesk.com/the-united-nations-just-launched-its-first-large-scale-ethereum-test/>
- CoinDesk (2017) "Mauritius: The Tropical Paradise Looking to Become a Blockchain Hub." May 08. <http://www.coindesk.com/mauritius-the-tropical-paradise-looking-to-become-a-blockchain-hub/>
- CoinIdol (2017) "Decentralization: Who Should Decide on the Blockchain?" <https://coinidol.com/who-should-decide-on-the-blockchain/>

- Coleman, Lester (2016) "Ex-Ethereum Developer: How the DAO Hack Happened and What Comes Next." Cryptocoins News. (July 30th) <https://www.cryptocoinsnews.com/ex-ethereum-developer-dao-hack-happened-comes-next/>
- Collindres, J., M. Regan and G. Peña Painting (2016) "Using Blockchain to Secure Honduran Land Titles." http://internationalpropertyrightsindex.org/casestudy_collindres
- Comin, D. and Mestieri, M. (2013) "Technology Diffusion: Measurement, Causes and Consequences." NBER. doi:10.3386/w19052. <http://www.nber.org/papers/w19052.pdf>
- Davidson, S., Filippi, P. D., and Potts, J. (2016) "Economics of Blockchain." SSRN Electronic Journal. doi:10.2139/ssrn.2744751
- De Filippi, P. (2015) "The Interplay between Decentralisation and Privacy: The Case of Blockchain Technologies." Journal of Peer Production, Issue 7. <http://bit.ly/2e1r1Tp>
- De Filippi, P. and B. Loveluck (2016) "The invisible politics of Bitcoin: Governance crisis of a decentralised infrastructure." Internet Policy Review, 5(3). DOI: 10.14763/2016.3.427.
- Dickey, M.R. (2017) "Algorithmic accountability." April 30. <https://techcrunch.com/2017/04/30/algorithmic-accountability/>
- Ekblaw, A. et.al. (2016) "A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data." MIT Media Lab: Cambridge. https://www.healthit.gov/sites/default/files/5-56-onc_Blockchainchallenge_mitwhitepaper.pdf
- Fargo, S. (2015) "The Economics of Bitcoin Mining Centralization." April. <http://insidebitcoins.com/news/the-economics-of-bitcoin-miningcentralization/31833>
- Forbes (2016) "Bitland's African Blockchain Initiative Putting Land On The Ledger." Forbes. April 5. <http://bit.ly/2druN5A>
- G-20 (2017) "The G20 Countries Should Engage with Blockchain Technologies to Build an Inclusive, Transparent, and Accountable Digital Economy for All." http://www.g20-insights.org/policy_briefs/g20-countries-engage-blockchain-technologies-build-inclusive-transparent-accountable-digital-economy/

- Gadnis, Ashish (2016) "Opinion: Blockchain offers poorest a real economic identity — and a shot at the SDGs." Devex blog (7 November). <http://bit.ly/2hP8HdT>
- Garrod, J.Z. (2016) "The Real World of the Decentralized Autonomous Society." *tripleC* 14(1): 62-77. https://www.academia.edu/22154529/The_Real_World_of_the_Decentralized_Autonomous_Society
- Goldman Sachs (2016) *Blockchain: Putting Theory into Practice*. New York: Goldman Sachs. <http://www.the-Blockchain.com/docs/Goldman-Sachs-report-Blockchain-Putting-Theory-into-Practice.pdf>
- Golumbia, David (2016) *The Politics of Bitcoin: Software as Right-Wing Extremism*. Minneapolis: University of Minnesota Press.
- Hileman, G. & M. Rauchs. (2017) "Global Cryptocurrency Benchmark Study." University of Cambridge. Judge Business School. <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/global-cryptocurrency/>
- Kavanagh, D., Miscione, G. (2015) "Bitcoin and the Blockchain: A coup d'état in Digital Heterotopia?" *Critical Management Studies Conference*. Leicester.
- Kaldoner, H. et.al. (n.d.) "An empirical study of Namecoin and lessons for decentralized namespace design." Princeton University. <http://randomwalker.info/publications/namespaces.pdf>.
- Kane, E. (n.d.) "Is Blockchain a General Purpose Technology?" *SSRN Electronic Journal*. doi:10.2139/ssrn.2932585
- Karlstrøm, H. (2014) "Do libertarians dream of electric coins? The material embeddedness of Bitcoin." *Distinktion: Scandinavian Journal of Social Theory*, 15(1), 23-36. doi:10.1080/1600910x.2013.870083
- Kaul, I. (2010) *Providing global public goods: Managing globalization*. New York: Oxford Univ. Press.
- Kostakis, V. & Giotitsas, C. (2014) "The (a)political economy of bitcoin." *tripleC* 12(2), pp.431-440. <http://triplec.at/index.php/tripleC/article/view/606>.
- Kshetri, N. (2017) "Will blockchain emerge as a tool to break the poverty chain in the Global South?" *Third World Quarterly*, 1-23. doi:10.1080/01436597.2017.1298438
- Lemieux, V. L. (2016) "Trusting records: Is Blockchain technology the answer?" *Records Management Journal*, 26(2), 110-139. doi:10.1108/rmj-12-2015-0042

- Lundy, L. (2016) "Five Things We Learned from Analysing the Location of 950 Blockchain Startups." July. <https://medium.com/outlier-ventures-io/5-things-we-learned-from-analysing-the-location-of-950-blockchain-startups-96daa788560c#.f4mby72h5>
- Maras, Elliot. (2016). UN paper claims Bitcoin Solutions for Developing Countries Could Be Interpreted as Neo-Colonialism. <https://www.cryptocoinsnews.com/will-bitcoin-Blockchain-build-finance-developing-economies/>.
- May, T. (1988) The Crypto Anarchist Manifesto. <http://www.activism.net/cypherpunk/crypto-anarchy.html>.
- Mettler, M. (2016) "Blockchain technology in healthcare: The revolution starts here." 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom). doi:10.1109/healthcom.2016.7749510
- Metz, C. (2016) Why Bitcoin Will Thrive First in the Developing World. Wired. February 02. <https://www.wired.com/2016/02/why-bitcoin-will-thrive-first-in-the-developing-world/>
- Miscione, G., & Kavanagh, D. (n.d.) Bitcoin and the Blockchain: A Coup D'tat in Digital Heterotopia? SSRN Electronic Journal. doi:10.2139/ssrn.2624922
- Morabito, V. (2017) Blockchain Governance. Business Innovation Through Blockchain, 41-59. doi:10.1007/978-3-319-48478-5_3
- Nakamoto, Satoshi (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>
- NewsBTC (2015) Developing Countries Adopting Blockchain for Land Titles. May 19. <http://www.newsbtc.com/2015/05/19/countries-adopt-Blockchain-land/>
- O'Dair, Marcus (2016) Music on the Blockchain. Blockchain for Creative Industries Research Cluster. Report N° 1. Middlesex University. <http://eprints.mdx.ac.uk/20574/1/Music%20On%20The%20Blockchain%201.0.pdf>
- O'Neal, C. (2017) Weapons of Math Destruction. S.L.: Penguin Books.
- Ore, Jonathan. 2016. "How a \$64M hack changed the fate of Ethereum, Bitcoin's closest competitor." CBC News (Aug 28). <http://www.cbc.ca/news/technology/ethereum-hack-blockchain-fork-bitcoin-1.3719009>
- Outlier Ventures. (2016) Five things we learned from analyzing the location

of 950+ Blockchain startups. <https://medium.com/outlier-ventures-io/5-things-we-learned-from-analysing-the-location-of-950-blockchain-startups-96daa788560c#.f4mby72h5>.

Pasquale, F. (2015) *The black box society the secret algorithms that control money and information*. Cambridge: Harvard University Press.

Pilkington, M. (n.d.) "Blockchain technology: Principles and applications." *Research Handbook on Digital Transformations*, 225-253. doi:10.4337/9781784717766.00019

Popper, N. (2016) *Digital gold: Bitcoin and the inside story of the misfits and millionaires trying to reinvent money*. New York: Harper.

PriceWaterHouseCoopers (2016) *Blurred lines: How FinTech is Shaping Financial Services*. *Global FinTech Report 2016*. http://www.pwccn.com/webmedia/doc/635936368926159575_fs_fintech_mar2016.pdf

Prisco, G. (2016) "UK Government Awards Framework Agreement to Blockchain-as-a-Service

Company Credits." *Bitcoin Magazine*. August 8. <http://bit.ly/2eNZvl0>.

Raval, S. (2016) *Decentralized applications: Harnessing Bitcoin's blockchain technology*. Beijing: O'Reilly.

Reijers, W., O'Brolcháin, F., and Haynes, P. (2016) "Governance in Blockchain Technologies & Social Contract Theories." *Ledger*, 1, 134-151. doi:10.5195/ledger.2016.62. <https://www.ledgerjournal.org/ojs/index.php/ledger/article/view/62/51>

Schermer, M. (2017) "FinTech in Afrika is much more than just mobile money and remittances." May 4. https://thenextweb.com/afrika/2017/05/04/fintech-afrika-much-just-mobile-money-remittances/#.tnw_8LMKdmUb

Schiller, B. (2017) "The Fight for the \$400 Billion Business of Immigrants Sending Money Home." <https://www.fastcompany.com/3067778/the-blockchain-is-going-to-save-immigrants-millions-in-remittance-fees>

Scott, B. (2014) *Visions of a Techno-Leviathan: The Politics of the Bitcoin Blockchain*. *EInternational Relations*. June. <http://www.e-ir.info/2014/06/01/visions-of-a-techno-leviathan-the-politics-of-the-bitcoin-blockchain/>

- Shin, Laura (2016) "Republic Of Georgia to Pilot Land Titling on Blockchain with Economist Hernando De Soto, BitFury." *Forbes*. April 21. <https://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/#6751e06b44da>
- Shrier, D., D. Sharma & A. Pentland. (2016) "Blockchain & Financial Services: The Fifth Horizon of Networked Innovation, Part 1." White Paper. MIT: Cambridge. <http://bit.ly/2d8Wq28>
- Skinner, C. (2016) *Valuweb: How fintech firms are using mobile and blockchain technologies to create the Internet of Value*. Singapore: Marshall Cavendish.
- Strelenko, O. (2017) E-Government of the future – eGaaS. *Medium*. <https://medium.com/egaas/e-government-of-the-future-73c8c35abcf7>
- Sullivan, C., & Burger, E. (2017) E-residency and blockchain. *Computer Law & Security Review*. doi:10.1016/j.clsr.2017.03.016
- Swan, M. (2015) *Blockchain: Blueprint for a new economy*. Beijing: O'Reilly.
- Szmigielski, A. (2016) *Bitcoin essentials*. Packt Publishing Limited.
- Tapscott, D., & Tapscott, A. (2016) *Blockchain revolution: How the technology behind bitcoin is changing money, business and the world*. London: Portfolio Penguin.
- Tapscott, D., & Tapscott, A. (2017) *The Blockchain Corridor: Building an Innovation Economy in the 2nd Era of the Internet*. The Tapscott Group. <http://dontapscott.com/BlockchainCorridorReport.pdf>
- The Economist (2015) "The Trust Machine." 31 October. <http://www.economist.com/news/leaders/21677198-technology-Behind-bitcoin-could-transform-how-economy-works-trust-machine>
- The Economist (2017) "The world's most valuable resource is no longer oil, but data." 06 May. <http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource?frsc=dg|e>
- The Morning Paper (2017) "A first look at the usability of Bitcoin key management." 22 February. <https://blog.acolyer.org/2017/02/22/a-first-look-at-the-usability-of-bitcoin-key-management/>

- Tierion (2016) *Blockchain Healthcare 2016 Report – Promise & Pitfalls*. <https://tierion.com/blog/Blockchain-healthcare-2016-report/>
- UNDP (2013) *Mobile Technologies and Empowerment: Enhancing human development through participation and innovation*. UNDP: New York. http://issuu.com/undp/docs/mobile_technologies_and_empowerment_en?download
- UNRISD (2016) *How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?* Working Paper 2016-1. UNRISD: Geneva. <http://www.unrisd.org/brett-scott>
- Vigna, P., and Casey, M. (2015) *The age of cryptocurrency: / how bitcoin and digital money are challenging the global economic order*. New York: St. Martin's Press.
- Wagner, A. A. (2016) *Developing Countries Adopting Blockchain for Land Titles*. November. <http://www.newsbtc.com/2015/05/19/countries-adopt-blockchain-land/>
- Walport, Mark (2016) *Distributed Ledger Technology: Beyond Blockchain*. Report by the UK Government Chief Scientific Adviser. Government Office for Science: London. <http://bit.ly/2drf0DG>
- Wattenhofer, Roger (2016) *The Science of Blockchain*. Inverted Forest Publishing.
- Werback, Kevin (2016) "Trustless Trust." SSRN. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2844409_code355061.pdf?abstractid=2844409&mirid=1
- World Economic Forum (2016) *The future of financial infrastructure: An ambitious look at how Blockchain can reshape financial services*. http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf
- Yarvin, C. (n.d.) *The DAO as a lesson in decentralized governance*. Urbit. <https://urbit.org/blog/dao/>
- Young, J. (2017) *How South Korea Has Become Largest Ethereum Market Above US, China*. May 8. <https://cointelegraph.com/news/how-south-korea-has-become-largest-ethereum-market-above-us-china>

Blockchain

Unpacking the disruptive potential
of blockchain technology
for human development

WHITE PAPER



IDRC | CRDI

International Development Research Centre
Centre de recherches pour le développement international

Canada