



# The Legal Aspects of Blockchain



Anand · Audia · Busstra · Gort · Hartog  
Van Heukelom-Verhage · De Kok · Makala · Marani · Naves  
Oude Luttighuis · Rikken · Stack · Yamamoto · Zoet

# Table of contents

## The Legal Aspects of Blockchain

<b>Preface</b> .....	005
<i>Sigrid Kaag</i>	
<b>01</b> Introduction .....	007
<i>Benedetta Audia, Yoshiyuki Yamamoto and Koen Lukas Hartog</i>	
<b>02</b> Blockchain and Distributed Ledger Technology: definitions .....	011
<i>Olivier Rikken, Sandra van Heukelom-Verhage and others</i>	
<b>03</b> Some general remarks about blockchain and the law .....	025
<i>Jeroen Naves and Olivier Rikken</i>	
<b>04</b> Human Rights .....	041
<i>Marjolein Busstra</i>	
<b>05</b> Implications of blockchain / DLT on the UN System .....	065
<i>Benedetta Audia</i>	
<b>06</b> Legal aspects of smart contracts .....	089
<i>Sandra van Heukelom-Verhage, Olivier Rikken and others</i>	

<b>07</b> Identity (SSID) .....	101
<i>Giulietta Marani, Steven Gort and André de Kok</i>	
<b>08</b> Data, information & citizen control .....	109
<i>Paul Oude Luttighuis en Steven Gort</i>	
<b>09</b> Blockchain and Land Administration .....	131
<i>Baloko Makala and Aanchal Anand</i>	
<b>10</b> Blockchain Market Microstructure Implements the 100% Reserve Chicago Plan – Now What? .....	151
<i>Matt Stack</i>	
<b>11</b> ICOs: “Understood and Misunderstood” .....	177
<i>Mona Zoet</i>	
<b>12</b> Open Source Development .....	193
<i>Steven Gort and Giulietta Marani</i>	
<b>Author Biographies</b> .....	205

For more information please contact:

**Benedetta Audia**  
[benedettaa@unops.org](mailto:benedettaa@unops.org)  
**Yoshiyuki Yamamoto**  
[yoshiyuki@unops.org](mailto:yoshiyuki@unops.org)  
**Koen Lukas Hartog**  
[koen@blockchainprojects.nl](mailto:koen@blockchainprojects.nl)  
**Marloes Pomp**  
[marloes@blockchainprojects.nl](mailto:marloes@blockchainprojects.nl)

Unless indicated otherwise, the contents of this book are published under Creative Commons Attribution 4.0 International.



The views reflected in this book are personal and do not necessarily reflect those of the United Nations, including UNOPS.

# PREFACE

*Sigrid Kaag*

Minister of Foreign Trade and Development  
Cooperation, The Netherlands



*I strongly suggest that we, as public sector, should be explicitly involved in technological developments.*

The fourth industrial revolution is underway, and organisations in the public domain – on both the national and international front – are being confronted with numerous new technologies. Separately, but especially in combination with each other, the Internet of Things, robotisation, cloud computing, Blockchain, and 3D-printing are causing society to change in rapid tempo.

Blockchain, the technology that questions the position of trusted third parties, is rightly getting a lot of government attention in several countries. In the Netherlands, for instance, a large number of blockchain projects has been initiated by government organisations. Through the Dutch Blockchain Coalition, business, government and the academic world work together on the most important building blocks of the blockchain ecosystem. Especially now that the technology is still under development, we, as public organisations, can investigate how we can pre-sort for new forms of service and a different relationship between citizens and government.

I strongly suggest that we, as public sector, should be explicitly involved in technological developments. In our modern network society, many boundaries are disappearing: between analogue and digital (the Internet of Things), physical and virtual (virtual reality), and between countries (cyberspace). In order to stand firm as government in the midst of these developments,

experiments, fast learning, and modern coordination are needed. We must be able to quickly identify how technologies can have the greatest positive social impact and gain insight into the role the government can play in that. That role may vary: sometimes we have to create space, sometimes we have to take control.

In order to fulfil a positive role as government in the context of these technological changes, cross-border cooperation is of crucial importance. We are proud of the way in which the Netherlands is paving the way when it comes to blockchain. But if we join forces, we can achieve much more within a shorter time frame. That is why I support this book about the legal implications of blockchain. When examining and implementing a technology of which the impact on society can be so great, we will encounter numerous legal issues. To stimulate blockchain innovation and optimise its social return, we need a lot of thinking power. It is a positive sign that the UN, the World Bank, and representatives from the public and private sector from Singapore, the Netherlands, and the U.S. have decided to provide a first joint legal interpretation of blockchain.

# 01

## Introduction

*Benedetta  
Audia, Yoshiyuki  
Yamamoto and  
Koen Lukas Hartog <sup>1</sup>*

<sup>1</sup> Benedetta Audia is the Corporate Legal Advisor and Head of the Commercial and Institutional law practice at UNOPS. Yoshiyuki Yamamoto is the Special Advisor for UN Engagement and Blockchain Technology, UNOPS. Koen Lukas Hartog is the Programme Manager of Blockchain Projects for Dutch governmental organizations, [Blockchainpilots.nl](http://Blockchainpilots.nl).

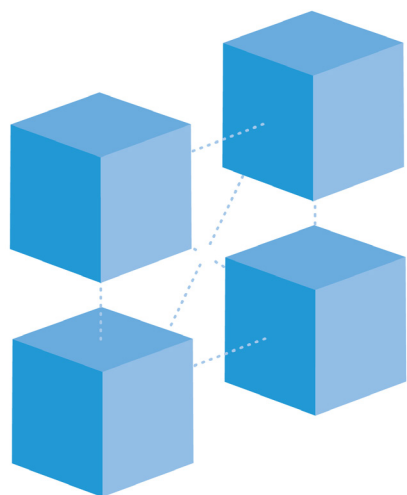
While the majority of mainstream news coverage is still focusing on the price swings of bitcoin and other cryptocurrencies or on the question whether we are (or were) in a crypto bubble, a silent tech revolution has started within several governmental organizations worldwide. These organizations focus on the application of blockchain beyond the use case of digital money (cryptocurrencies).

Without trying to diminish the significance of bitcoin, it is important to underline that it is yet the first use case of blockchain or distributed ledger technology. Blockchain questions one of the foundations of our modern society, the role of trusted third parties. Blockchain makes it possible to develop decentralized services and applications. As a result, the technology that could replace (specific roles of) banks, notaries, accountants and the government has been coined the ‘trust machine’.

As one of the primary trusted parties, governments are confronted with the challenge to picture themselves in a more decentralized society. To better comprehend what the opportunities and threats of blockchain for society are, several countries and international organizations have started exploring blockchain projects. In the Netherlands, more than 35 governmental organizations have launched blockchain pilot projects since May 2016. By developing use cases and prototypes, these organizations got a better understanding of the potential use of this technology and its impact on society and their own organization.

At the beginning of 2017, there were only few UN organizations that were actively exploring the potentials of blockchain technology. However, the landscape of blockchain space made a rapid change in 2017 and 2018; UNOPS is in the process of establishing a fund enabling

the receipt and disbursement of cryptocurrency; WFP and UNDP piloted proofs of concepts of blockchain-based work in their mandated areas; UN Women organized a hackathon in Oslo in May 2017; and the World Bank launched a Blockchain Lab in June 2017.



A common denominator for blockchain prototypes developed by governmental organizations is that their management questioned at some point in time: do we comply with legal rules and regulations if we would launch this service for the public? Giving an answer is not always easy. Several legal experts tried to provide clarity. In the Netherlands, a consortium of lawyers wrote a report about the legal significance of smart contracts. Pels Rijcken, a technology-focused law firm in The

Hague, developed the first legal assessment for blockchain prototypes. The Monetary Authority of Singapore (MAS) and the Swiss Financial Market Supervisory Authority (FINMA) were amongst the first financial authorities that tried to provide clarity on the legal meaning of ICOs specifically for blockchain tokens, and in which cases these should be seen as a form of stock in a company. A lot of legal questions remain, and a large part of the legal community within the public sector still have not dealt with blockchain (yet).

For blockchain to reach its full potential within the context of the public administration and international organizations, a clear understanding of the legal implications involved is required. Governments could shape emerging norms and

rely on blockchain technology itself to achieve several policy objectives through a blockchain-based network and associated smart contracts.

This book is a not-for-profit initiative by UNOPS and Blockchainpilots.nl which explores the emerging use of the blockchain technology, describing its perceived benefits and challenges and its potential use in the United Nations system and development community at large. We are grateful for the intellectual contributions made by several legal, finance and blockchain experts and hope that this book can be a starting point for further legal discussions on blockchain.

*“For blockchain to reach its full potential within the context of the public administration and international organizations, a clear understanding of the legal implications involved is required.”*

# 02

## Blockchain and Distributed Ledger Technology: definitions

*Olivier Rikken,  
Sandra van  
Heukelom-Verhage  
and others <sup>2</sup>*

<sup>2</sup> This chapter was published earlier in “Smart contracts as a specific application of blockchain technology” by O. Rikken, S. van Heukelom, S. Mul, J. Boersma, I. Bijlloo, P van Hecke, A. Rutjes, F. Stroucken, J. Linnemann, H. Terpoorten and R.R. Nederhoed.

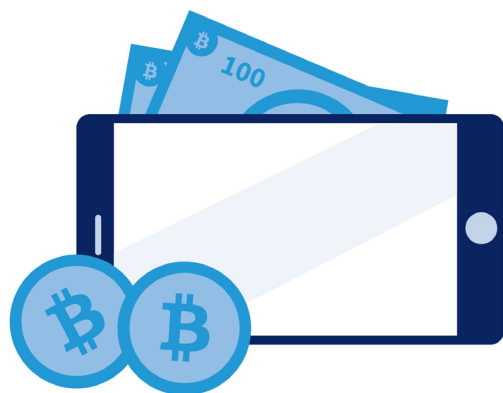
### 2.1 BLOCKCHAIN

Blockchain is the collected term for technologies created with the purpose of synchronizing data that has been stored on different computers and/or servers via a network in a way that enables it to remain the same. A consensus protocol is used to guarantee the integrity of the content of the data, in which cryptography plays a big part.

The essence of blockchain technology is that synchronization takes place in a peer-to-peer fashion, which means that no single computer in the network has control over the system. In time, this means that certain tasks of so-called “trusted third parties”, such as a cadastral agency or a central bank, can be implemented differently or could even become redundant. This would mostly concern irrefutable registration of specific data and executing standard checks.

Every participating computer will only accept a proposed change in the data set after it itself has ascertained that the change takes place in accordance with predetermined rules (typically, such a rule would be: “was the change made by the party registered as a party with a right to make this change”). Because it concerns a peer-to-peer system and there is no “authoritative” party in the network, it is possible that changes are made at several locations in the network, that participants each individually report that they comply with the rules, but that they are actually in conflict with each other (i.e. that they result in different data sets). The mechanism recorded in the blockchain software that ensures that the network of computers eventually reaches a consensus on the “real” data set is called the consensus protocol. The exact implementation of this protocol can differ per blockchain.

## 2.2 BITCOIN - THE FIRST BLOCKCHAIN IMPLEMENTATION



Blockchain's origin lies in bitcoin, a so-called cryptocurrency. The designer of bitcoin wanted to create a system in which parties could pay each other online without the mediation of banks or other financial institutions(!). The question remained who, with the absence of a so-called trusted third party (see the next paragraph), ends up checking whether the paying party has sufficient balance and whether or

not this party illicitly tries to spend the same value twice (double spending problem). The solution was for the network to do this itself; every participating computer checks if a transaction can take place and witnesses that the balance cannot be spent twice. This was the birth of the blockchain: a register (often compared to a ledger) containing the history of all bitcoin transactions trusted by the network. If a computer in the network fails, then this is not a problem; after all, there are many other computers with a copy of the register, and every computer can check proposed transactions independently. A special property of blockchain is that all data is stored and cannot be changed unilaterally later; data is essentially only added and not removed or changed.

## 2.3 BLOCKCHAIN AS A REPLACEMENT OF TRUSTED THIRD PARTIES

We just explained that blockchain technology enables safe payment with bitcoin without the mediation of a bank. Others quickly realized that the blockchain is essentially

a generic technology that can be used in all situations in which there is a need for a jointly managed data set that cannot be unilaterally manipulated by any of the parties. In other words, blockchain makes it possible to create a shared single source of truth between two parties for which these parties do not have to use the services of a neutral trusted third party.

Naturally, it is possible to record whatever you want in this data; besides ownership of bitcoins<sup>3</sup> it is also possible to register ownership of an asset, an authorization, a degree certificate, a license, medical data, etc. Blockchain technology can also be used to transfer value (symbolic or otherwise). For instance, if it is possible for a specific asset (a house for instance) to be uniquely identifiable on a blockchain, this also makes it conceivable for that house to change ownership via the blockchain (bearing in mind the following caveats, however).

There are some caveats, though: the intention of one or more parties to execute and possibly also create a legal act via a blockchain application does not mean that all requirements have been met legally. For instance, the sale of a house through a smart contract is technically and economically relatively easy to achieve, but it does raise the question whether or not a valid agreement has been created. Furthermore, the transfer of ownership of a house requires the mediation of a notary, according to current legislation (in the Netherlands).

The possibility of recording data without the mediation of trusted third parties and possibly transferring value means that the speed of such matters can be increased, while the costs are reduced by not just avoiding transaction fees, but also, for instance, the costs of security, supervision

*“...blockchain makes it possible to create a shared single source of truth...”*

<sup>3</sup> Even though it might look like coins change ownership, behind the scenes there are only debit and credit transactions.

and enforcement. It could, additionally, enable a self-organizing group of people/bodies to draw up their own set of rules for making transactions and executing them without the use of a third party. This explains the disruptive potential of blockchain technology applications, especially when combined with the application of smart contracts.

We have already indicated that certain tasks of trusted third parties with regard to administration and standard checks could disappear or be implemented differently. At the same time, we would do well to remember that TTPs are often more than just glorified administrators. They can play a part in protecting the parties involved or the rights of third parties. This can prevent conflicts, which is also in the government's interest.

#### 2.4 PERMISSIONED VS PERMISSIONLESS BLOCKCHAINS

A very important aspect with relation to blockchains is the phenomenon of permissioned versus permissionless blockchains. Both are essentially the same: data storage takes place in a comparable way, by way of building blocks. The difference lies in participation and rights. This in turn leads to discussions of an entirely different nature and to facts regarding privacy and governance.

A permissionless blockchain is a blockchain in which everyone is completely free to participate (anonymously). This means that everyone who wants to can participate in this blockchain as a standard user or as a so-called full node. There is no identification or authentication in the case of permissionless blockchains. In that sense, participants are virtually anonymous, though it would be more accurate to

state that participants have a pseudonym. In order to execute transactions, so-called cryptographic key pairs are used: a (hash of a) public key and a secret private key. All transactions and all information in the blockchain in question is public. Everyone can make proposals for software updates, but an upgrade of the network only takes place if (the majority of) the participants voluntarily update the software on their own machines. In a permissionless blockchain not a single party is "in control" and the chain does not have any super users or comparable positions. If a software update is not accepted by part of the network, then a network split (also called a fork) could occur, resulting in two different blockchains that have a common prior history up to the point of the split. A permissionless blockchain is also called a public blockchain. Bitcoin and Ethereum are the most well-known permissionless blockchains.



Permissionless blockchains have issues regarding sustainability (energy consumption), costs (energy, hardware, processor power), processing speed and scalability (one block per 10 minutes for Bitcoin) and governance (distributed).

A permissioned blockchain is protected by means of a so-called access control layer. A permissioned blockchain is a blockchain that not everyone can participate in, but which requires an access request/approval and for which read/write rights, for example, can differ from user to user. In theory, it is even possible that the data is only stored on one computer ("node") and that a type of super user can be created. Permissioned blockchains are also called hybrid,



consortium or private blockchains depending on the number of different nodes and types of users. Various software projects to build permissioned blockchains work under the Hyperledger project started by the Linux Foundation (e.g. Hyperledger Fabric, which was originally contributed by IBM, or Hyperledger Burrow that builds on Ethereum).

There is a significant difference between permissioned and permissionless blockchains with respect to governance and compliance. In terms of governance, for instance, it is possible to appoint a person or group of people responsible for the blockchain, whereas everyone and at the same time no one seems to be responsible in a permissionless blockchain.<sup>4</sup> For example, different read/write rights in a permissioned blockchain can be used to allow for easier safeguarding of privacy; this is not as easy to achieve in a permissionless blockchain due to its transparent nature.

## 2.5 CONSENSUS MECHANISMS AND IMMUTABILITY

Like all computer networks, blockchain applications also have to take network attacks into account. It is conceivable, for instance, that a number of computers in the network might be working together to present an inaccurate version of the truth to the other computers. This primarily seems to be a hazard for so-called permissionless blockchains for which access is free to everyone and in which anyone in the world with a computer and an internet connection can participate anonymously in both using the application (e.g. paying someone) and maintaining and securing the blockchain in the context of this use. This means that the design needs to take into account anonymous malicious people who will try to compromise the system.

<sup>4</sup> Many permissionless blockchains do have “core development teams” that make the biggest contributions in terms of further development of the open source software and have a de facto governance role within the community. Examples are the Bitcoin Core team and the Ethereum Foundation. However, everyone can add to the software or take part in the community.

In order to fend off attacks, Bitcoin and many other permissionless blockchains currently opt for a so-called proof-of-work system. This system appoints a “random”<sup>5</sup> computer about every 10 minutes<sup>6</sup> that is allowed to propose a block of transactions to the other computers in the network.<sup>7</sup> For the other computers, it is very easy to determine via mathematical proof (cryptography) that:

1. This computer has indeed earned the right to make the proposal.  
*Proof: proof-of-work*
2. The proposed transactions do indeed exist, come from a party that is permitted to execute these transactions, and the contents have not been tampered with.  
*Proof: digital signature*
3. The proposed transactions can indeed be executed according to the applicable rules (e.g. sufficient balance). This means that it must also be demonstrated that the transaction history has not been tampered with.  
*Proof: blockchain in the shape of inextricably linked Merkle trees*

A consensus process based on proof-of-work costs (a lot of) money in terms of energy, write-offs of hardware and processing power that could have been used for other things (at a higher yield). The fact the process costs money is not a coincidence: the costs deters “spammers”. On the other hand, there’s no such thing as a free lunch: in order to convince benign people to spend money on the process of managing and securing the blockchain, the computer used to approve a block of transactions is rewarded. In the case of Bitcoin, new bitcoins are awarded (this is how bitcoins are created). Other methods use so-called

<sup>5</sup> Random in the sense that every computer has an equal chance of being chosen depending on processing power; a computer with more processing power (and thus a higher investment) has a higher chance, of course.

<sup>6</sup> For other blockchains this average time can differ; Ethereum switches every 15 seconds, for example.

<sup>7</sup> For the manner in which blocks of transactions are “published” see, among other things: <https://blockchain.info/nl>

transaction fees. For proof-of-work systems it is assumed that the transactions have better protection (and cannot be undone) the longer they are registered. In practice, a Bitcoin transaction is considered to be permanent after one hour.

The proof-of-work mechanism is much older than blockchain technology itself. This currently makes it the proven mechanism to achieve consensus in a decentralized environment. That is also why most permissionless and some permissioned blockchains use this mechanism. However, there are several downsides to this method, which is why many other consensus mechanisms are common as well. The most prevalent alternatives<sup>8</sup> are:

1. Proof-of-Stake
2. Proof-of-Capacity
3. (P)BFT
4. PAXOS
5. RAFT

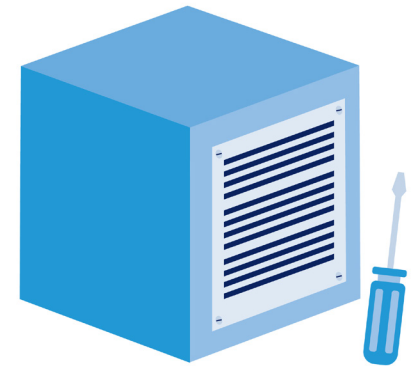
For permissionless blockchains, the proof-of-work and proof-of-stake mechanisms are most common. For permissioned blockchains there is more diversity.

One of the primary elements of a blockchain is the so-called immutability. Once something has been placed on a blockchain it is no longer possible to undo it. This needs to be more nuanced, however: it cannot be undone unilaterally. If there is general consensus between all nodes that something must be undone, then it is definitely possible. Proof of this is the so-called hard fork of Ethereum in 2016.<sup>9</sup> The challenge lies in the fact that if the same is to be achieved in a permissionless blockchain, then all the nodes in the network will have to cooperate to

<sup>8</sup> <http://www.coindesk.com/short-guide-blockchain-consensus-protocols/>

<sup>9</sup> <https://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds/>

prevent a split in the network. The problem is that not all nodes in the network are known to everyone, which means that convincing everyone in the network is a difficult process. In a permissioned blockchain, all full nodes – the network's accountants – are known. This makes undoing transactions in a permissioned blockchain for which everyone needs to agree much easier than achieving the same in a permissionless environment.



Finally: immutability simply means that it is certain that a specific piece of data was once registered on a blockchain. It does not mean that this data is also correct. For example, an incorrect owner is registered in an ownership register of bicycles due to a human error, which cannot be deleted. This does not make the person in question the legal owner. For applications that want to use a blockchain to represent real-world assets (also see the next paragraph) it is important to construct the application in such a way that the representation in the blockchain can also be synced with the legal reality (by including exception procedures, for example).

## 2.6 NATIVE CURRENCIES VERSUS ISSUED ASSETS

The application of (permissionless) blockchains that is the most well-known to the public is the so-called cryptocurrencies like bitcoin, ether, dash, etc. There are currently over 750 blockchains with their own currency that allow for public trading.<sup>10</sup>

Each of these currencies is inherent, or native, to the blockchain they operate on: the currency is a way to

<sup>10</sup> <https://coinmarketcap.com/currencies/views/all/>

*“ This means that the value of these currencies is inextricably linked to the use this blockchain has for the user. ”*

connect a cost price to transactions. After all, if transactions were free, the network would be spammed excessively in a permissionless blockchain, which has happened before on an Ethereum test network.<sup>11</sup> It is also the tool used to compensate parties that secure the network (through proof-of-work or proof-of-stake). The currency can only exist in conjunction with the corresponding blockchain. This means that the value of these currencies is inextricably linked to the use this blockchain has for the user.

Blockchain applications that go beyond trading the native currency were found rather quickly. With a few tricks (techniques like “colored coins” or Omni and Counterparty) you can make your own “coins” in Bitcoin and trade them via the blockchain. Other blockchains, such as Nxt (assets) and Ethereum (tokens) make this even easier. The number of popular crypto-assets is currently running into the hundreds.<sup>12</sup>

Assets can represent monetary value, such as a claim on goods (assets that represent gold in a safe are popular!), a share, or another type of security. Contrary to the native currency, the value of which is intrinsically linked to the functioning of the underlying blockchain, the value of an asset solely depends on the issuer of that asset. As the holder of the asset you implicitly or explicitly agree with the issuer that you can claim the underlying value. However, assets can also represent abstract things, such as membership or the right to use specific software. In these cases, the issuer often is not a legal entity, but a pseudonymous group of developers. Especially the world of Ethereum tokens and smart contracts is prone to experimentation, with many new business models and forms of organization, particularly in cases where token holders form a type of virtual company (a Decentralized

<sup>11</sup> <https://www.coindesk.com/ethereum-spam-attacks-back-time-test-network/>

<sup>12</sup> <https://coinmarketcap.com/tokens/views/all/>

Autonomous Organization) because every holder has an incentive to increase the value of the token.

## 2.7 SMART CONTRACTS AND ORACLES

Smart contracts are applications that can be placed on a blockchain. A smart contract is basically a deterministic computer program that is replicated and executed on a blockchain. A computer program is deterministic when it always generates the same output for a specific input and specific start values. In other words, its effect is completely predictable. Even though the name suggests otherwise, a smart contract does not necessarily create or execute a contract or other legal acts. For example, a collection of interacting smart contracts and oracles can also manage an operational process in a chain.

In order to determine if the conditions for the execution of a smart contract have been met, generally data (input) mostly from outside of the blockchain will be required, such as package delivery confirmation. A blockchain is “deaf and blind”: the blockchain software is not able to retrieve external information (other than what has been instructed by the protocol).<sup>13</sup> This is where the so-called oracles come in. Oracles can provide input to a smart contract.

An oracle is a party (or a technical source, such as a database, or a person who has been issued this role) that takes up the role of “source of truth” for a smart contract. The other parties that use the smart contract trust that the oracle will provide the correct information for the execution (of a function) of the smart contract, but cannot verify that this was actually the correct information “on

<sup>13</sup> Security is an important reason for public blockchains: the software is “sandboxed” and smart contracts, for example, do not have access to the network or hard drive. Consensus would be impossible, because every node is located in a different environment and “sees” different things.

chain”. If parties do not want to put their trust in one source, they could have multiple sources “vote”.

The role of an oracle is similar to that of a trusted third party. An oracle can only be a source of information and cannot be involved in the execution of the contract. Furthermore, an oracle does not even have to have knowledge of the further use of the provided information. An oracle does not have to be a technical source, such as a database; it could also be tied to a notary, or a mediator whose signature is required for the execution of (a specific function in) the contract. Generally trusted institutions, such as the Royal Netherlands Meteorological Institute, the Dutch Directorate-General for Public Works and Water Management, etc. could provide digitally signed data feeds for use by oracles in various blockchains in order to automatically handle insurances, for example. However, as indicated above, an appointed person with the proper authorization could also take up this role (in the form of binding recommendations, for instance).

As stated before, smart contracts can also be used to transfer value (symbolically or otherwise). If cryptocurrencies or assets/tokens are used as payment, then these can be “locked” in a smart contract until it has been determined that the payment conditions have been met, or until a specific period of time has expired after which the deposited sum can be returned again. In some cases, tokens can even be made a condition for exercising a certain right. Think of a rental car that will not start before people enter a specific virtual key, for example.

Smart contracts are used to an increasing extent for the transfer of value, on the so-called Ethereum blockchain, for example. When looking at what a smart contract consists

of on the Ethereum blockchain, you can find these three main elements:

1. A balance (on which a varying sum of the ether cryptocurrency can be stored).
2. An option for data storage (that can be overwritten or otherwise) – Here statuses can be stored, for instance if a package is en route or has been delivered. It is also possible to keep track of virtual tokens and of the amount of tokens, with a token representing a share, for example.
3. The contract code – this code determines, combined with values in the data storage or otherwise, whether the data storage needs to be adjusted or if cryptocurrencies need to be transferred based on the message sent to a smart contract.

These smart contracts have an address (similar to an “account number”) to which a message or a sum of cryptocurrency can be sent. Smart contracts are reactive. This means that they do not do anything until they receive a message (transaction). After receiving the transaction, the code is activated and decides whether or not something needs to be done with the message.

Once registered on the blockchain, the contract’s code cannot be changed. Furthermore, the balance or storage also can no longer be manipulated other than via a specific message that can be sent to the contract by means of a transaction. This, too, is only possible if the code contains functions that permit a change.

*“ The role of an oracle is similar to that of a trusted third party. An oracle can only be a source of information and cannot be involved in the execution of the contract. ”*

# 03

## Some general remarks about blockchain and the law

*Jeroen Naves and  
Olivier Rikken* <sup>14</sup>

<sup>14</sup> Jeroen Naves works as an attorney at the Dutch law firm Pels Rijcken & Droogleevers Fortuijn. Jeroen specializes in the legal aspects of disruptive technologies. Olivier Rikken MSc MBA is director blockchain and smart contracts at AXVECO working on sustainable blockchain innovation implementations. Furthermore active for the Dutch Blockchain Coalition, member of the ISO smart contract standardization workgroup, advisor to various (blockchain) startups and entrepreneur.

### 3.1 INTRODUCTION

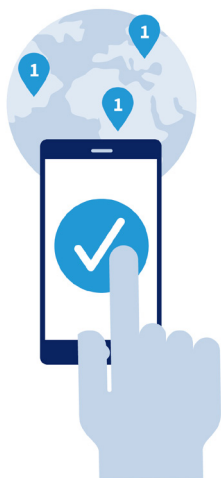
Blockchain is more than just technology. The decentralized nature of the blockchain makes it possible to view existing structures, which are often based on central databases, in a different light. This is evidenced by the rise of bitcoin and other cryptocurrencies; in a relatively brief period, a financial system worth hundreds of millions of dollars was created without the involvement of any bank or government. It is a system that is difficult to grasp within our current legal frameworks, which is exactly why it is interesting from a legal perspective. The first part of this chapter explores this in more detail.

At the same time, we should not overestimate the current impact of blockchain technology. There are regular calls for changes in legislation and regulations due to the existence of blockchain technology. However, when looking at blockchain at a transaction level, it is clear that many legal questions about the blockchain can be answered within the current legal frameworks. The second part of this chapter explores this in more detail.

### 3.2 LAW IN A DECENTRALIZED WORLD

#### 3.2.1 A new legal system

Our current legal frameworks are based on national borders. We are used to the idea that crossing a border has consequences for the applicable rules. Differences in rules that range from which side of the road you need to drive on to fundamental rights stemming from the Charter of the United Nations.



The internet results in a fading of national borders. It is possible to perform a (legal) act in another country with the press of a button on your computer. Because our legal frameworks are based on national borders, it is highly relevant from a legal perspective in which country these (legal) act have been performed; this is relevant for which law applies and which government has the authority to enforce this law. Actual relevance is limited, however. For instance, if I order a new pair of shoes in Italy via the internet from the Netherlands, then only the fact that I can get a good pair of shoes for a great price really matters. Where the shoes come from is not that relevant.

Blockchain technology is the superlative of the internet in the sense that its decentralized nature ensures that the system in itself no longer needs to be linked to any legal system. The nodes that together form a blockchain could theoretically be located in any country in the world. However, a specific country could decide to declare that their rules apply to the nodes located in their country. Should the other nodes in the network refuse to accept the applicability of these rules, then the action of the government in question means nothing. In other words: the lack of a central database and a corresponding central party means that governments only have a limited say about what does and does not happen in a blockchain. It is interesting to see how such a society deals with legal and organizational issues. We have proceeded to shed light on this based on three examples.

#### The DAO

The DAO or Decentralized Autonomous Organization was the first ever organization on the blockchain that had humans truly placed in the margins and where smart

contracts were designed to run the company. Once deployed, humans were to play a minimum role, if any, in running the company. This includes decision-making and execution. Smart contracts were designed to take over this role. Although the Ethereum blockchain at that time had only been running in a live environment for approximately one year, the token sale of the DAO became one of the most successful crowdfunding actions ever. It raised almost \$160 million in a month's time, way before ICOs were hyped in the general audience. The DAO hack was the result of unexpected behavior of a command in a smart contract of the DAO. This hack resulted in a loss of a \$60 million equivalent in Ethers, at that time representing about 10% of the total value of the Ethereum blockchain. Bear in mind that there is no central authority in the Ethereum blockchain that monitors suspicious activities, nor are there compliance officers.

Within an hour of the first activities by the hacker and despite the lack of officially appointed persons to monitor any abnormalities, the first reports were shared via various forums and social media like Twitter and Reddit, warning for strange behavior of the DAO and possible loss of funds.

Even though the DAO was designed to run autonomously, within hours the community connected to the DAO – officially not organized – came up with a recovery plan and the hack could be stopped. It is an interesting example of quick governance in an officially ungoverned and decentralized environment.

This also resulted in the hard fork of Ethereum ending up splitting into Ethereum and Ethereum Classic. The hard fork was necessary to basically undo (a large part of) the transactions and refunding the almost \$60 million in

*“Blockchain technology is the superlative of the internet in the sense that its decentralized nature ensures that the system in itself no longer needs to be linked to any legal system.”*

funds to the rightful owners. This shows that although a blockchain is thought of as being completely immutable, these malicious transactions can be reversed as long as the “whole” community agrees.

#### Parity MultiSig Wallet

The Parity MultiSig wallet was a wallet created to be very secure. This wallet is a so called M of N wallet, which means that it requires a minimum amount of the total entitled signatures before funds can be transferred out of this wallet.

In July 2017, a black hat hacker – a hacker with malicious intentions – discovered a flaw in the Parity MultiSig wallets. Basically the “names” (Externally Owned Account Numbers) of the signatories could be overwritten without any checks, meaning that the hacker was able to overwrite him/herself as signatory multiple times. This led to the fact that the hacker could sign the minimum required M times by him/herself and thus transfer funds unauthorized. This hack began on July 17th 2017.

However, the first victim of the hack was an Ethereum startup that was actually tied to some white hat hackers – ethical hackers who hack to find flaws in systems and warn others about any vulnerabilities. This start-up immediately warned the white hat hackers of these suspicious activities. This resulted in a race between the white hat hackers and the black hat hacker(s).

An important element of blockchain – its transparency – played a crucial role in the counter-actions. Just as it is possible to see all transactions in permissionless blockchains, it is also possible to search for smart contract code, which means that the addresses of other Parity

MultiSig wallets could be found easily. This is what the white hat hackers did and, using the flaw found by the black hat hacker, they transferred the funds from these wallets to safe accounts. They then posted on various online platforms that if the rightful owners were missing their funds, they should prove that these wallets actually belonged to them after which the funds would be transferred to new, secure, accounts. The race ended in approx. \$35 million for the black hat hackers with the white hat hackers recovering almost \$360 million. This is yet another example of unexpected governance actions due to the characteristics of blockchain and the cooperation of the blockchain community, even though this community hardly knows each other in person. With regards to the \$35 million that the black hat hackers were able to transfer to their own accounts: even if they are in control of it, it is pretty much useless to them. Which is best illustrated by the last example, the CoinDash hack.

#### CoinDash

CoinDash is a start-up that planned to do an Initial Coin Offering in July 2017. After all the preparations for the ICO, on the date of the ICO, CoinDash got hacked. Instead of the smart contract address for the CoinDash token, an address of an externally owned account of the hacker got displayed. Thus, funds that investors were sending for the ICO were not sent to the CoinDash address, but directly to the hacker’s address. This resulted in an approximate first loss of \$7 million in Ether.

At this point, the transparent nature of blockchain started to play a crucial role. Due to the fact that all accounts are public, even if they are behind a pseudonym, the funds were easily traceable. At this point, these “hot” accounts were flagged on all block browsing sites. As a result,

*“ The blockchain community in general believes that individuals in themselves are largely responsible for their own actions, ... ”*

other participants in the network were warned that they should not interact with these accounts. The exchanges were also warned about these accounts, leading to the hacker being unable to trade or exchange their Ethers for goods or fiat currencies. Furthermore, transferring funds to other accounts will not help, as these transactions would be noticed immediately. Although the hacker was theoretically in full control of the funds, in practice these funds were actually frozen due to the hacker's inability to use them as these funds had been marked.

After several weeks of this status quo something happened that nobody expected. The hacker, unable to move the funds, felt remorse and refunded (part of) the funds to CoinDash.

#### Unexpected governance behavior and a possible steps forward

As stated, there are few formal governance structures, especially with respect to permissionless blockchains. Nevertheless, due to the characteristics of blockchain and the attitude of the community, swift action could be taken in a lot of cases even though nobody is in control and all major decisions need to be taken with (almost) 100% consensus. Furthermore, in multiple cases the full transparency led to unexpected behavior that would be unimaginable for a centralized environment where a lot of information is kept from the general public.

There are some important elements that various communities and governments can work on in order to improve this behavior and the governance structures in permissionless environments. One important example relates to the Parity hack. Formally speaking, the white hat hacker group was committing a crime with the salvage

action as they moved funds without authorization, even though their ethical intentions were good. It is recommended to investigate the option, under the right circumstances, to give white hat hackers the authority to perform these actions without the risk of being prosecuted after the fact.

Another important sentiment within the permissionless blockchain communities is that they believe that individual responsibility should be increased, whereas individual responsibility has declined by increasing rules and regulations worldwide over the past decades. The blockchain community in general believes that individuals in themselves are largely responsible for their own actions, including actions that will result in loss of assets or data that they have could prevented themselves. Even though governments must protect individuals to a certain degree, the debate could be reopened to see how far the ever-increasing duty of care in various areas must go.

#### 3.2.2 Opportunities for solving existing problems differently

The blockchain technology offers the possibility of creating a digital society that is difficult to define within our current legal frameworks, but that nevertheless seems capable of solving its own problems. This does not mean that the blockchain technology also offers alternatives for the solutions that are currently being implemented within the existing legal systems. This is explained on the basis of three examples.

The General Data Protection Regulation is the legal framework for the protection of personal data within the European Union. This regulation focuses primarily on data minimization. Under the GDPR, parties are no longer



permitted to process personal data that is not required for the realization of the goal for which the personal data is collected. Blockchain technology seems to be in conflict with this principle. After all, the decentralized nature of the technology means that if personal data is processed in a blockchain, it is then stored in many more different locations than if it were to be processed in a central database. However, one of the primary goals of the right to privacy is that citizens have control over the data that is processed about them. Even though blockchain technology may be in conflict with the basic principles of data minimization, the blockchain does present options for citizens to maintain control over their personal data, which prevents abuse and unnecessary processing of data. As such, blockchain technology offers a solution that seems to be in conflict with the GDPR, but which does ensure that one of the primary goals of the right to privacy can be realized. Chapter 4 discusses the relationship between privacy and blockchain in more depth.

A second example is the smart contract. Many countries require certain types of agreements to be recorded in writing and then signed. Blockchain technology offers the option of recording (parts of) agreements in smart contracts. This has major benefits: a well-programmed smart contract ensures that the parties are certain that specific actions will take place automatically under specific circumstances. This would mean that a breach of contract becomes impossible, which in turn significantly saves on costs, for instance for insurance or bank guarantees. For many parties, these savings will take prevalence over the certainty of written recording or a signature. Chapter 6 will further explore the topic of smart contracts.

A third example is the topic of supervision. In principle, the

blockchain could make supervision easier and possibly superfluous. After all, the information it contains cannot be changed, which means supervisory bodies would only need to consult a blockchain to see what happened in a specific situation. It is conceivable that a supervisory body will no longer have to supervise, and that smart contracts on the blockchain will take over this task. For example, in the future, it is possible for the auditing tasks of an accountant to be reduced significantly.

However, in practice, this does not yet seem to be the case. Supervisory bodies are facing the fact that it is difficult to ascertain which legal entities are behind the public keys acting in a blockchain. Naturally, this makes it more difficult for supervisory bodies to supervise a blockchain as such. One issue that has presented itself around the world is whether or not governments can supervise so-called Initial Coin Offerings and, if so, how they would go about this. Chapter 11 will further explore this topic.

### **3.3 A FEW LEGAL QUESTIONS AND ANSWERS FOR THE USE OF BLOCKCHAIN TECHNOLOGY IN CURRENT LEGAL PRACTICE**

Blockchain offers a different perspective of looking at the current legal system. This does not mean that blockchain technology does not raise questions within the current legal frameworks that need to be answered. A number of general legal questions will be answered below. Not all legal limitations for the application of blockchain technology in practice will be removed by answering these questions. It is possible that industry-specific regulations apply to the blockchain depending on the industry in which that blockchain is used. For instance, a blockchain in which

*“Blockchain offers a different perspective of looking at the current legal system.”*

electricity is traded must meet the specific legislation and regulations that apply within the energy industry. A blockchain that is used in the healthcare industry will have to meet the regulations that apply within that specific industry.



### 3.3.1 Applicable law

The decentralized nature of blockchain technology means it is not possible to determine which law applies to a blockchain in a general sense, because every field of law sets different conditions for applicability within the legal field in question. Thus, it is conceivable that Dutch civil law applies to a transaction in a blockchain, but that the German tax authorities are authorized to levy taxes on this transaction based on the German tax laws. Imagine that this could apply to all transactions in a blockchain. This could mean that regulations from many different legal systems could apply depending on the context of a blockchain.

However, at the transaction level it is usually quite clear which law applies to the transaction. If a transaction in a blockchain is executed between two parties from the same country, then generally the civil law of the country in question will apply.<sup>15</sup> The rules of international private law will have to determine which civil law applies to a transaction between parties from different countries. The Regulations regarding the law applicable to obligations from agreements (Rome I) determine which law applies, for example, if a transaction is executed between two parties from two different countries in the European Union. The main rule is that parties can decide amongst themselves which law applies to the transaction executed in the blockchain. If they did not determine this, then generally the law of the country where the characteristic

<sup>15</sup> Deviation from this is only possible if the parties have agreed by contract that a different law applies.

performance is executed will apply.

Let us take the example of a Dutchman who via the internet purchases a bicycle from a Belgian. The transaction takes place on the blockchain, because the Dutchman pays for the bicycle with bitcoins. The delivery of the bicycle is the characteristic performance in this case. After all, payment is not the thing that distinguishes this transaction from other transactions. The distinguishing aspect is the delivery of the bicycle. For this reason, Belgian law applies to the transaction of the bitcoins.

The question of where the characteristic performance takes place is only relevant to determine the civil law that applies to a transaction in a blockchain. Whether for example the tax laws, general administrative laws or financial laws of a specific country apply to a transaction in a blockchain depends on other conditions.

If the civil law applicable to a transaction in a blockchain has been determined, then the question remains how such a transaction is qualified on the basis of the national law. This strongly depends on the specific circumstances of the case itself and the rules that apply within the national system of law.

### 3.3.2 Ownership of a blockchain

A blockchain consists of various components: infrastructure (nodes) that provides storage capacity and processing power, and software that ensures the blockchain does what it is supposed to do.

The question of who owns a node that is part of a blockchain can generally be determined based on the property law of the country where the node is situated. For

most blockchains, the infrastructure (nodes) that are part of the blockchain will be owned by different parties. This is, after all, the strength of the blockchain: because the infrastructure (nodes) is controlled by different parties that verify each other, one single party is not able to manipulate the system and security is provided based on technology.

In most legal systems, it is not possible to be the owner of software in the sense of property law. However copyright is generally placed on software. The blockchain at the foundation of the bitcoin consists of open source software that has been built by a group of programmers. Every programmer holds the copyright to the part of the blockchain they built.

<sup>16</sup> The MIT license is a software license for open source software. It was created at the Massachusetts Institute of Technology. Like the BSD license, the MIT license permits almost anything. The only condition is that the copyright statement must be retained in all copies. Furthermore, the software can also be used as part of proprietary software.

<sup>17</sup> The legal entity behind a public key is generally known to the party that exchanges bitcoins or other cryptocurrency into euros or dollars. Investigative services, for example, could find out who is behind a transaction in the bitcoin blockchain through this exchange office.

For the blockchain that is at the basis of bitcoin, all programmers have made the part of the blockchain they built available as open source under the MIT license.<sup>16</sup> Under this license, anyone can use the software. The MIT license does state that anyone who wishes to distribute (an adjusted version of) the software must state who holds the copyright in the software itself. Chapter 12 will further explore the topic of open source.

### 3.3.3 Identity in a blockchain

All transactions in a public blockchain are public. This does not mean that it is always clear who executes the transactions in the public blockchain. In the bitcoin blockchain for example, all users have a public key, and there is no way to directly determine which person hides behind that key. Because there is no central organization that regulates the bitcoin blockchain, it is also not possible to determine which person is behind a specific account through a central organization.<sup>17</sup>

This could lead to problems in practice. If you do not know who it is you are transacting with via a blockchain, then it is practically impossible to take that party to court if something went wrong with this transaction. It is conceivable, for instance, that you make a payment with bitcoin in which you accidentally enter an additional zero, which means ten times as many bitcoins as intended are transferred to the receiving party. If such a transaction had taken place via a bank, then it would be relatively simple to find out the identity of the receiving party and enforce a repayment judicially. For a transaction in a blockchain, finding out the identity of the receiving party is much more complicated.

There are several initiatives aimed at developing a way to link the biological identity of a person to a digital identity by means of a blockchain and otherwise.<sup>18</sup> Chapter 7 explores this topic in more detail.

### Legal significance of smart contracts

Smart contracts are often inextricably linked to blockchains or considered as such. This is due to the fact that smart contracts require objective circumstances that can trigger the execution of a smart contract. Such objective circumstances can be provided by a blockchain.

The use of smart contracts results in many legal questions. Can a smart contract also be a legal contract? What if the will of the parties does not correspond to how it is recorded in the code? And what if the smart contract does not act as intended by the parties?<sup>19</sup> And is it possible to agree that this is not possible (code = law)? Chapter 6 will answer some of these questions.

<sup>18</sup> <https://kennisopenbaarbestuur.nl/thema/digitale-identiteit/>

<sup>19</sup> An example of this is the DAO hack. Even though the word hack suggests otherwise, this hack did not involve a breach of security. Instead, an error in an open source smart contract was abused and 55 million dollars was diverted.

*“A characteristic of blockchain technology, for instance, is that information that is processed in a blockchain is immutable in principle, whereas European data protection law introduces the right to be forgotten.”*

#### **3.3.4. Processing personal information in a blockchain**

A question that is interesting, at the very least with respect to European law, is whether or not it is possible to process personal information in a blockchain. This is not a theoretical question; many parties are experimenting with processing personal information in a blockchain. Moreover, it is conceivable that the information that is processed in a public blockchain like the bitcoin blockchain on the basis of the General Data Protection Regulation can be flagged as personal information, which means that this Regulation would also apply to blockchains like the bitcoin blockchain.

This is true even though the blockchain technology seems to be irreconcilable with European data protection law in some extents. A characteristic of blockchain technology, for instance, is that information that is processed in a blockchain is immutable in principle, whereas European data protection law introduces the right to be forgotten.

Even more problematic might be the fact that European data protection law focuses on a central figure that is basically responsible for compliance with the law (“the controller”).

If a company processes employment-related data for their own purposes, for example, then that company is the controller. If a government body processes personal information in the context of the execution of a legal task, then the government body is the controller.

In principle, a blockchain does not have such a key figure, which directly gives rise to some questions. Who is responsible for securing a blockchain? And what if there is a data leak? Must all participants of a blockchain report

this data leak to the supervisor?

In our experience, in a closed blockchain that allows for a form of governance, it is possible for the blockchain to comply with European data protection law. After all, in such a blockchain the participants can jointly make agreements on the way in which compliance with the obligations based on the General Data Protection Regulation is implemented. The consequence is that this does form a type of (trusted) third party that should have been superfluous by using blockchain technology.

A public blockchain in which these agreements cannot be made or in which these agreements are not made will be more difficult to comply with European data protection law. This does not prevent people from using such blockchains, however.

### **3.4 CONCLUSION**

Blockchain technology forces us to look at the law from a different perspective as does it to our traditional view of governance. At the same time, it turns out that a lot of the existing legal frameworks can more or less be applied to blockchain technology. Both topics are explored in more detail later in this book.

# 04

## Human Rights

*Marjolein Busstra*<sup>20</sup>

<sup>20</sup> Marjolein Busstra works for the international law section of the Dutch Ministry of Foreign Affairs on human rights and cyber related issues

<sup>21</sup> See, inter alia, the following introductory websites or documents: <http://www.ohchr.org/EN/pages/home.aspx> (UN human rights treaties), <http://www.ohchr.org/Documents/Publications/training9chapter3en.pdf> (regional human rights treaties), [https://eur-lex.europa.eu/summary/chapter/human\\_rights/1301.html?root=1301](https://eur-lex.europa.eu/summary/chapter/human_rights/1301.html?root=1301) (EU human rights law), [https://eur-lex.europa.eu/summary/chapter/information\\_society/3104.html?root=3104](https://eur-lex.europa.eu/summary/chapter/information_society/3104.html?root=3104) (EU data protection law) and <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR-EN.pdf> (UN Guiding Principles on Business and Human Rights).

### 4.1 BLOCKCHAIN AND HUMAN RIGHTS

Blockchain technology and related concepts such as smart contracts and autonomous organizations have the potential of profoundly changing societies and economies, causing a next revolution in the way human interaction is organized. As such, they are bound to have a profound impact on human rights and it is worth exploring in which way human rights could, or rather should, inform the design and implementation of blockchain applications. However, any discussion on human rights aspects of blockchain technology will heavily tilt towards the ‘maybe’ and the ‘what if’, as the technology is still in its infancy stage. There clearly is still a lot of thinking to do, and this introductory article only offers a tasting menu of some of the issues that call for further exploration.

For reasons of expediency, this article does not go into detail on definitions or technical aspects. A basic knowledge of blockchain technology is presupposed. Neither does it go into definitional questions regarding human rights. A broad and inclusive understanding of the term is employed, referring to the internationally agreed canon of human rights, as it is contained in a number of international and regional instruments, as well as in authoritative soft law norms such as the UN Guiding Principles for Business and Human Rights.<sup>21</sup>

This article briefly looks at potential applications of blockchain technology that may benefit or harm the cause of human rights and subsequently considers in which way human rights should inform the application of blockchain technologies.

## 4.2 BLOCKCHAIN APPLICATIONS AND HUMAN RIGHTS

Blockchain promises more transparency, more security and more efficiency. All good, so it would seem. Indeed, numerous applications come to mind that could positively affect the cause of human rights. Just a selection of examples:

- Blockchain's property of storing information in such a way that no one can alter or delete it afterwards can be very useful in countering corruption or arbitrariness in public services. Elections by blockchain are for instance much harder to manipulate than paper ballots.
- Blockchain technology offers a tamper-free and reliable way of tracking activities and entitlements or assets. This can be especially beneficial in countries with immature governance systems, acting as a catalyst for economic activity and growth. A much-cited example is blockchain registry of land rights in countries where official registration of land ownership is unreliable or non-existent. Community members can register their claims to land and the underlying documentation in a reliable and transparent way, which makes it more difficult to deny their rights and seize their property unlawfully.
- The ability to share data quickly and securely could benefit human rights defenders, journalists and other persons investigating and reporting on human rights violations. The International Bar Association has for instance recently launched an app that allows people to share information about human rights violations in a secure way.<sup>22</sup> Blockchain technology

<sup>22</sup> <https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=f8ff99f9-43e4-4301-b1a4-9935a25f0fdd>

could take this a step further, by making it more difficult for human rights violators to interfere or change data once uploaded.

- Cryptocurrencies based on blockchain technology offer opportunities in terms of financial inclusion, by giving access to financial services to people in countries with immature or inaccessible financial infrastructure. Small-scale farmers or entrepreneurs can get access to global cryptocurrency markets and acquire loans or insurance in order to boost their business. Poor communities could benefit from cooperative insurance schemes against failing crops or disability. With these and similar applications blockchain technologies can contribute to the fight against poverty.<sup>23</sup>
- The transparency offered by blockchain technology makes for interesting possibilities for opening up supply chains, helping businesses in carrying out the human rights due diligence that is required of them in the framework of Business and Human Rights. Blockchain technology makes it easier to accumulate and share reliable information about where products come from and which journey they make until they end up on the shelves or racks for consumers to buy. Such supply chain blockchains could further include data about, for instance, labour conditions, tax returns or environmental protection safeguards. In this way, businesses not only gain more insight in the human rights risks in their supply chain, but they can also show to the public how they prevent or mitigate the materialization of these risks, by storing information in the blockchain about the measures they have taken. Similar supply chain initiatives have

<sup>23</sup> Hack the future of development aid, by inter alia the Danish government, <http://sustainiaworld.com/wp-content/uploads/2017/12/hack-the-future.pdf>, at 12. See for a much more elaborate exploration of potential financial applications of blockchain technology in Brett Scott's Working Paper for the United Nations Research Institute for Social Development *How can cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?*, <http://www.unrisd.org/brett-scott>

been launched in the cobalt sector in Congo and the fishing sector in the Pacific.<sup>24</sup>

Exciting as these possible applications may be, blockchain technology is not more than an instrument. It can equally engender unwanted or negative effects, or not deliver on its promise if used in the wrong way or by the wrong people. After all, the aforementioned applications all require some extent of reliable human input and verification in order to be effective. A blockchain application recording land property rights can only benefit people if they already have some form of evidence of ownership that is recognized by the blockchain. The chain cannot create land rights, only record them. This may be problematic for indigenous communities who do not have any legally valid title documents for land they own by tradition. Similarly, for supply chain blockchains to function, one needs not only data about the origin and location of the product, but also someone to check that the information added is actually true.

Even if blockchains function perfectly they can still lead to unwanted outcomes. Commentators have pointed to the risk of loss of jobs caused by the elimination of intermediaries in supply chains and by increased automation of production processes. Another potential risk lies in the lack of control of authorities over certain types of blockchains. Levying taxes on blockchain applications may for instance prove to be difficult, which could undermine public finances and result in lower levels of public service or public investments. Not to mention the risk of abuse of blockchain applications by repressive regimes or criminal or terrorist organizations.

<sup>24</sup> <https://business-humanrights.org/en/dem-rep-of-congo-blockchain-technology-can-help-improve-cobalt-supply-chain-say-experts-and-the-developers-of-this-new-solution> and <https://business-humanrights.org/en/fiji-blockchain-technology-joint-pilot-project-launched-to-address-illegal-fishing-practices-and-human-rights-abuses-in-pacific-islands-tuna-industry>

Despite, therefore, the great potential that blockchain technology holds, it would be naïve to assume that it is automatically a force for the good. Especially since so much about the possibilities and impossibilities of this new technology is still unclear. This is exactly why it is important to discuss ethical and legal issues surrounding blockchain, now that the technology is still in its infant stage. Which brings us to the core question of this article: how should human rights regulate or condition the use of blockchain and related technologies?

### 4.3 HOW SHOULD HUMAN RIGHTS REGULATE BLOCKCHAIN TECHNOLOGY

There is broad international consensus that human rights apply in the digital domain and that persons should have the same rights online as they have offline.<sup>25</sup> To the extent, therefore, that blockchain technology is used by humans or impacts on the lives of humans,

human rights standards have to be complied with. This not only raises questions as to how to translate human rights norms to the new technical realities introduced by blockchain, but also as to how to enforce rights in a blockchain context. Three major themes come up in this respect: access, privacy and remedy.

#### 4.3.1 Access

As the development and use of blockchain technology takes flight, more and more services and benefits will become available, perhaps exclusively, in the form of



<sup>25</sup> See UN Human Rights Council Resolution The Promotion, Protection and Enjoyment of Human Rights on the Internet, para. 1, UN Doc. A/HRC/32/L.20 (June 2016) and UN General Assembly Resolution The Right to Privacy in the Digital Age, GA Res. 68/167, para. 3, UN Doc. A/RES/68/167 (December 2013).



this technology. This in turn will make it increasingly relevant for individuals to have access to these services or benefits. There may come a time that access to blockchain applications is deemed so fundamental that it merits a right in itself, in a comparable way to the right to internet access that is currently debated.<sup>26</sup> Even in the absence of a self-standing right, human rights law has relevance for a number of issues related to access to blockchains.

First, the right to non-discrimination requires that access to blockchains is provided in a non-discriminatory manner. Individuals may not be excluded from a blockchain application or offered less favourable treatment because of their ethnicity, religion or sexual preference or other legally recognized discrimination grounds. Insofar as it entails a prohibition of direct discrimination, using prohibited grounds directly as selection criteria, this norm is quite straightforward. Fully permissionless blockchains, which allow anyone to participate and do not impose any conditions for entry, appear to be inherently not directly discriminatory. Even for regulated permissionless blockchains and permissioned blockchains the prohibition of using certain selection criteria should not be too complicated to comply with. One simply makes sure that the software does not select according to ethnicity, or sexual preference, or religion, and so forth. Note in this respect that the prohibition of discrimination does allow for the use of certain specified discrimination grounds as selection criteria, as long as there is a legitimate justification for using them. Factors such as gender or age are relevant in certain circumstances. Think of health checks for age related illnesses or gender specific diseases. In case of such legitimate use of a particular selection ground, it is important that the service provider is transparent and clearly explains how and why this ground is used.

<sup>26</sup> See for instance [https://en.wikipedia.org/wiki/Right\\_to\\_Internet\\_access](https://en.wikipedia.org/wiki/Right_to_Internet_access). Note that human rights law does not entail a right to internet access as of yet.

A more complicated issue arises with respect to the so-called prohibition of indirect discrimination, which is based on the reality that discrimination can occur even when no prohibited ground is used as a selection criterion, because of a particularly - disproportionately - damaging effect on a protected group. For instance, in many countries ethnic minorities live in relatively poorer neighbourhoods. If an online shop charges more for delivery to the postcodes of such neighbourhoods, or if a government selects such postcodes in catchment areas for lower quality schools, the ethnic minority living there is disproportionately disadvantaged compared to persons of the general population. Absent a reasonable justification for such disproportionate effect, it amounts to indirect discrimination. So, if a smart contract or algorithm in a blockchain application factors in characteristics that are more or less connected to a particular minority group, it could, perhaps unintentionally, disproportionately filter out persons of that minority group and produce discriminatory results. The potentially discriminatory outcomes of automated decision-making is a concern increasingly highlighted by human rights experts.<sup>27</sup> With reason: various instances of bias have already been found in facial recognition software, internet search engines and other algorithmic applications.<sup>28</sup>

All of this calls for thorough research into potentially discriminatory effects of proposed designs of blockchain applications and commensurate adjustments. However, the problem with indirect discrimination is that it often cannot be predicted in advance and is only established afterwards, by discovering a disproportionate negative effect on a particular group of people. Self-learning AI applications seem particularly capable of producing unforeseen forms of disproportionate negative impact,

<sup>27</sup> How to prevent discriminatory outcomes in machine learning, Global Future Council on Human rights, World Economic Forum, Algorithms and human rights, study on the human rights aspect of automated data processing techniques and possible regulatory implications, Council of Europe study DGI(2017)12, <http://www.ohchr.org/EN/pages/home.aspx> (22 March 2018), at 26; Report of the Special Rapporteur on the right to privacy (advance unedited version), A/72/43103 (October 2017), at 15. Big Data's Disparate Impact, Solon Barocas, Andrew D. Selbst, 104 California Law Review 671 (2016), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2477899](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899)

<sup>28</sup> <https://business-humanrights.org/en/new-study-reveals-racial-bias-in-facial-recognition-software>; <https://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html>; [https://en.wikipedia.org/wiki/Algorithmic\\_bias](https://en.wikipedia.org/wiki/Algorithmic_bias)



*“...it is vital that persons from minority or other underprivileged groups are included in design and development processes and in governance discussions on blockchain and related technologies.”*

as they are programmed to find and use correlations and causations that are not immediately obvious. So applications should not only be checked beforehand, at the design stage. The results produced by software should be continuously monitored and mechanisms should be put in place to undo or remedy potentially discriminatory results. Moreover, it is vital that persons from minority or other underprivileged groups are included in design and development processes and in governance discussions on blockchain and related technologies. This is also why the open source working method is to be preferred with regard to the further development of blockchain, as it maximizes transparency and allows broad scrutiny, in particular by users that may otherwise be overlooked.

The argument also holds true at a country level. Blockchain has the ability to reduce the costs of transaction processes significantly, and as transaction costs generally tend to be higher in developing economies, these have relatively much higher profits to reap from a transition to blockchain technology than developed economies. It is essential to include these countries in the debates and trials that are currently taking place, and especially in any discussions on governance and regulation. Otherwise, there is a real risk that these countries fail to reap the benefits of these new technologies and end up lagging even further behind, reinforcing global inequality.

Reasoning further along the lines of non-discrimination and access: the practice of digital profiling, which is likely to be used in many blockchain applications, especially in smart contracts and similar phenomena, poses a real concern. It entails recording patterns of behavior and making profiles of persons based on seemingly unconnected and unnoticed digital activities of individuals. This is problematic because

the premise of the prohibition of discrimination is that persons are to be treated as individuals, not as categories. There is also a problem from a privacy perspective, because more information about personal choices may be revealed and recorded than persons are aware of or even have consented to. In addition, digital profiling can undermine individuals' ability to freely make personal, autonomous choices that shape their identity, a core element of privacy. Simplistically stated: I may not mind that people see me going into an ice cream shop one particular day, but I do mind if someone records each time I go into the ice cream shop, finds out I always go on Thursdays after the gym and subsequently offers me a discount for low-fat ice cream, as this is the type of ice-cream most popular with people going to the gym. There is a real risk that blockchain applications coupled with certain algorithms or AI abilities will distinguish between individuals based on perceived trends and correlations, without checking their real profile or giving them a real choice. As a result, individuals may feel treated unfairly on the basis of some profile that is based on their own or someone else's behavior: what if I prefer to get a discount on full-fat ice cream? Getting ice cream is of course trivial, but more important interests may be at stake.<sup>29</sup>

At the same time, digital applications cannot exist without making use of trends and profiles. Indeed, many applications using big data and algorithms greatly enhance the quality of life, by offering tailored healthcare or fitness solutions, helping people to work more efficiently or giving consumers personalized offers that saves them a lot of money. So using big data and algorithms in itself may not be problematic, but it may become a problem when people are not aware of their existence and don't have a real choice as to whether they want to benefit from

<sup>29</sup> See for a very enlightening yet disconcerting discussion of what a world governed by autonomously operating algorithms may look like: Decentralized blockchain technology and the rise of lex cryptographia, Aaron Wright, Primavera de Filippi, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2580664](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664) (accessed February 2018), at 40-44.

<sup>30</sup> See articles 13(2)f, 14(2)g and 22(1) of the EU General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679> (GDPR). Read together, these articles recognize the right not to be subject to a decision based solely on automated processing and require that individuals should be notified about (1) the fact that their data is being used for profiling purposes and (2) the logic that is used in the profiling process. See furthermore the following recommendation of the Council of Europe on data profiling: Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, <https://rm.coe.int/16807096c3> (23 November 2010).

them or not. This calls for maximum transparency from providers of such applications about when and how they use algorithms and data profiling. Moreover, individuals should have the opportunity to choose whether they want to participate in applications that use this type of profiling and they should be able to change or correct profiles made of them. In Europe, both the European Union and the Council of Europe have elaborated guidelines and even legislation in this respect.<sup>30</sup>

Another issue that comes up in the context of non-discrimination is the question whether vulnerable groups should get extra assistance in gaining access to certain blockchain applications. This is particularly relevant for blockchain based services operated by governments, as they have the obligation to provide for special measures for certain vulnerable groups.<sup>31</sup> Just as governments must provide access for persons with disabilities to public buildings and infrastructure, they should arguably assist digitally vulnerable groups in access to blockchains offered by the government. Think of applications in the field of education or healthcare. If these are too complicated for certain social groups, the human rights to education and to health require that they are assisted in accessing them. A final word about access, or rather about non-access. What if individuals do not wish to have access to a particular blockchain application? In other words: if a service or benefit that hitherto was offered in a physical form is transposed to a blockchain application, do persons have a right to claim to continue to use the physical alternative? What if a person wants to continue to communicate with a company or government through post or telephone instead of an application on their smartphone? Do human rights say anything about a right not to go digital?

Two lines of thought are relevant here. First: if the introduction of digital applications threatens to lower the previously existing level of protection of human rights in a particular state, there is an argument to be made that states should provide for an alternative.<sup>32</sup> For instance, if the state introduces tax returns through blockchain applications for smartphones, they should arguably continue to offer the option of tax return through paper and mail for the group of people who don't have such phones or do not know how to operate them. This argument closely resembles the one of the need for special measures for vulnerable groups. More fundamentally, there is an argument to be made for a right not to go digital based on the right to privacy. This has to do with the fact that digital applications seem to necessarily involve some degree of digital tracing, which means that certain data about users is recorded and stored for at least some period of time. If the right to privacy is interpreted as including a right to remain anonymous or a right to be forgotten, this may mean that at least some essential or fundamental services have to be offered in a physical or analogous way, parallel to the digital application.<sup>33</sup> Both suggested lines of thought are open for debate. But it is an important debate to have, as more and more aspects of human life are usurped by the digital realm.

#### 4.3.2 Privacy

The right to privacy carves out a personal space, in which individuals have the freedom to determine and develop their own identity, relationships, ambitions and choices. In addition, the right to privacy grants the individual the right to decide to which extent they share information about this personal space with others. Privacy is, in short, about identity and about ownership of data concerning that identity. The right to privacy is not absolute, and it depends on the specific circumstances of a case whether

<sup>31</sup> See for instance the following general recommendations of UN treaty bodies with regard to persons with disabilities, racial and ethnic minorities and women respectively: General comment (2018) on equality and non-discrimination, CRPD/C/GC/6 (March 2018), General recommendation No. 32 The meaning and scope of special measures in the International Convention on the Elimination of All Forms Racial Discrimination, CERD/C/GC/32 (September 2009), General recommendation No. 25: Article 4, paragraph 1, of the Convention (temporary special measures), [https://tbinternet.ohchr.org/\\_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCEDAW%2fGEC%2f3733&Lang=en](https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCEDAW%2fGEC%2f3733&Lang=en) (2004)

<sup>32</sup> At least in the field of economic, social and cultural rights the UN monitoring bodies have recognized

<sup>33</sup> In EU data protection case law, the 'right to be forgotten' has been recognized. This has been codified in article 17 of the GDPR.



an infringement of someone's privacy actually amounts to a violation of their right to privacy. Different legal texts give different names to the test that needs to be performed to establish a violation, but they are more or less comparable.<sup>34</sup> Interferences are required to be legitimate and proportionate, meaning that they should pursue a legitimate aim and the severity and nature of the interference

should be proportionate to this aim. If an interference with a person's privacy complies with these conditions, it is not unlawful and qualifies as a legitimate limitation.

Even though it can be argued that blockchain applications can empower people and therefore contribute to their construction of their identity, adding to their right to privacy,<sup>35</sup> there are equally a number of concerns that deserve consideration.

First, there is the aforementioned problem of the impossibility of participating in blockchains on an anonymous basis: even if one takes on a pseudo-anonymity when participating in a blockchain, it is still technically possible to connect that pseudo-anonymity to a person or location. At least at this stage of technological development. That means that not only a person's actions on a blockchain are visible to all participants, but also that they can always be traced back to the person. As said before, it is important to consider whether there are certain services that are so sensitive or essential that individuals should be offered the choice for a physical or analogous alternative. This would make sense, for instance, for democratic elections or referendums, giving people the option of a paper ballot instead of a digital vote.

<sup>34</sup> Article 17 of the International Covenant on Civil and Political Rights prohibits unlawful or arbitrary interferences of privacy; article 8 of the European Convention on Human Rights requires interferences to be "in accordance with the law" and "necessary in a democratic society".

<sup>35</sup> Hack the future of development aid, Sustainia, Danish Ministry of Foreign Affairs and others, <http://sustainiaworld.com/wp-content/uploads/2017/12/hack-the-future.pdf> (accessed March 2018), at 7.

For voluntary blockchain applications that do not offer essential services there seems to be less of a problem, as it is up to persons themselves to decide whether they want to give up their anonymity for a particular application or not. People already do that all the time, by making use of social media networks, apps on their smartphone or internet search engines. However, one could wonder how much this argument is still worth in scenarios where blockchain is so omnipresent that not participating comes down to not being able to participate normally in society. It therefore seems important to keep looking for technical solutions that make anonymous participation in blockchains possible.

If anonymous participation becomes possible, however, new dilemmas come up. Governments have very valid reasons to consider anonymous participation in blockchains undesirable. Think of issues to do with taxation, national security or fighting crime. Taking measures to limit anonymous participation in blockchains for legitimate reasons is not necessarily problematic from a privacy viewpoint, as long as the conditions for legitimate limitations are respected. Indeed, as will be argued below, it is even desirable that governments start thinking about regulating blockchains in such a way that the potential benefits are maximized and risks are minimized.

Coming back to the current state of affairs, where anonymous participation is not possible: it is essential that access to personal data on blockchain applications is controlled and monitored.<sup>36</sup> This means that developers of blockchain applications have to carefully circumscribe which persons have access to personal data and which data they have access to. In line with the legitimate limitation test for privacy interferences, access should only

<sup>36</sup> Compare article 5 (b) of the GDPR, which determines that personal data may only be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".

be permitted to the extent necessary. What is needed, is a clear regime with regard to access to personal data and a controlling mechanism to monitor whether this regime is adhered to in practice. This may for instance mean that access is provided to certain people on a temporary basis. Or perhaps it is possible to close down access to certain personal data after a particular date, working with offline cryptokeys that are destroyed after some time. The point is: attention need to be given to find ways that restrict access to personal data as much as possible.

The second problem that comes up in the context of blockchains and privacy: at the current stage of technological development, blockchains do not allow for altering data once recorded, which can undermine individuals' freedom to shape their own identity. Take a transgender person who wants to retroactively change references to their gender in official documentation. This is not possible in a blockchain context, where the option of altering or deleting data has been traded for more secure and transparent data sharing. Clearly, there is strong tension here with the right to privacy, which in some jurisdictions has been interpreted as entailing a right to be forgotten and a right to change personal data about oneself in public or private databases.<sup>37</sup>

A number of considerations are relevant here. First, the impossibility of changing or deleting data calls for very careful consideration of which personal data are stored in the blockchain in the first place. To the extent that individuals have a choice whether to participate in a blockchain application or not, this is primarily their own responsibility. If, for instance, a blockchain application that rents out cars records locations and routes taken, a person using such blockchain arguably accepts that information

about their whereabouts is being recorded and stored. The right to privacy does, however, require that the application explicitly informs users about which data is recorded and asks for their consent, so that they have a real opportunity to reflect on privacy implications.<sup>38</sup>

Individual consent holds less value in situations where the choice not to participate is not a realistic option, for example where the only way to rent a car is through a blockchain application. So the responsibility for carefully considering which personal data is recorded in the blockchain cannot solely lie with individual persons. It is essential that designers and developers of blockchain applications afford sufficient attention to this question and only record and store personal data that is actually needed for the smooth running of the application. They should actively look for ways to safeguard privacy from the very beginning of the design process - this is the so-called principle of privacy by design.<sup>39</sup>

This brings us to the second point: when it comes to recording and storing personal data, the rule is: less is more. In the same way that the legitimate limitations test of the right to privacy requires that access to personal data is allowed only to the extent necessary, it requires that only those pieces of personal data that are necessary for the smooth operation of the technology or application are recorded. This calls for an active search for ways to minimize the amount of personal data needed for an application. An interesting example is the development of the concept of zero knowledge proof, which allows applications to run on the basis of verifiable 'yes' or 'no' questions about individuals' personal situations. For instance, if a bank wants to know whether an applicant for a mortgage earns enough to be able to pay the monthly

*“ Individual consent holds less value in situations where the choice not to participate is not a realistic option, ... ”*

<sup>37</sup> Articles 16 and 17 of the GDPR for instance requires that processors of data offer individuals the opportunity to request to delete or alter information about them and that they delete data as soon as they no longer (legitimately) need it.

<sup>38</sup> Compare article 6(1)a of the GDPR, which provides that personal data may only be processed with the consent of the individual concerned.

<sup>39</sup> Compare article 25 GDPR, which lays down the principle of data protection by design and by default.

installment, a zero knowledge proof application allows checking whether the applicant earns more than a certain minimum amount without needing to know the exact salary. Thus, zero knowledge proof allows keeping the amount of personal information needed for transactions at a minimum level.

Thirdly, the impossibility of deleting data once recorded means that it is essential to make sure that personal data submitted to a blockchain is accurate.<sup>40</sup> Safeguards must be put in place for verification of personal data and adjustment of incorrect or incomplete data, before the data is recorded in the blockchain. As a general rule, the final decision as to the accuracy of personal data lies with the person whom it concerns, in line with the principle that individuals have ownership over their own identity. Exceptions to this rule may be necessary where personal data reflect decisions or actions of others who have a stake in the accuracy of the data. Think of official registers of civil status or health statistics. In such cases, it is reasonable that the responsible authority has the ultimate say on the accuracy of data submitted, but individuals should at least have the option to review data concerning them and request alteration if they consider the data inaccurate.

This is closely related to the fourth and final consideration regarding the inability to alter or delete data: it makes it all the more important to keep looking for technical or legal ways to enhance individuals' ownership of personal data. In this respect there are some promising initiatives to create digital identities or digital passports for individuals, based on blockchain technology. The idea is to create blockchains of digital safes for storing personal data, the keys of which are held by individuals themselves.<sup>41</sup> In this way, individuals can create their own digital identity and

<sup>40</sup> Compare article 5(d) of the GDPR, which requires personal data to be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay".

<sup>41</sup> <https://www.forbes.com/sites/rogeraitken/2018/01/07/blockchain-to-the-rescue-creating-a-new-future-for-digital-identities/#483c62ee5492>; <https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity/>; <https://www.investopedia.com/news/blockchain-could-make-you-owner-data-privacy-selling-purchase-history/>

decide who they want to give access to which particular aspects of that identity. From a privacy perspective, such solution is preferable over a solution where governments or private organizations provide for (centrally stored) digital passports or identities.

#### 4.3.3 Remedy

As said before, persons have the same human rights online as they have offline. This means that states have to respect human rights when using digital technologies such as blockchain. It also means that states have the obligation to protect individuals against violations of their human rights in the digital world. Acting against cybercrime is as much a task of the government as acting against home burglary or physical abuse.

The argument for online and offline equation arguably holds not only for human rights, but for all legal rights that persons have. If I rent a car through a blockchain-powered application, I expect to have the same level of consumer protection that I would have if I rented a car from a physical car rental agency. Seeing that human rights law requires that states provide access to an effective and accessible remedy for people whose rights, human rights or other rights, have been infringed, it can be argued that states have to make sure that their citizens' rights are as well protected online as offline. States are therefore advised to scrutinize their laws and regulations for digital – or blockchain - compatibility and update these if necessary. It should not matter whether the infringement originates with a real person in the physical world or with a blockchain application.

This does call for some flexibility. Contrary to the digital world, law is essentially not binary. Indeed, a fundamental

*“As long as digital activities involve some extent of human input or control, it would seem that the law can regulate them, ...”*

characteristic of law is that it recognizes that reality is unpredictable. This is why it employs open concepts such as ‘reasonability’, ‘proportionality’ and ‘necessity’, which make sure that all particularities of a specific case are taken into account. This is also why law generally allows for hardship clauses that allow making exceptions in extraordinary circumstances. Such open terms require a human mind that is capable of considering and weighing all relevant circumstances.

As long as digital activities involve some extent of human input or control, it would seem that the law can regulate them, either directly or by proxy, through regulation of the relevant human actor. It was after all not too difficult for legal systems to adapt to the reality of email and smartphones. Even activities on the internet, a complicated structure that cannot be tied to a specific location or actor, generally proved to be governable through the regulation of activities of internet providers and tech companies.<sup>42</sup>

Thus, in order for law to be able to regulate blockchains and other new technological applications, they are ideally designed to involve some extent of human input or control, which can subsequently be regulated. This involves, for instance, making use of ‘oracles’ in the blockchain process, who can add data to the blockchain, check the operation of the blockchain and intervene if necessary. Think of a certification institute that can verify claims about labour conditions or environmental safeguards in local factories and whose authorization is needed for recording the relevant data in a supply chain blockchain. Another option is to require that applications of blockchain technology are accompanied by legally valid (e-)written agreements, that spell out the various responsibilities and rights of the participants.<sup>43</sup> This would for instance mean that if

I wanted to rent a car through a blockchain rental app, I would have to sign a written rental contract with the provider of the car.

It is questionable whether these solutions of adjusting blockchain applications and other technological innovations to the current legal paradigm will suffice in the longer run. Technology that does not need any human input after being created already exists. Indeed, the very concept of a smart contract is that it runs on its own, executing predetermined outcomes when predetermined conditions are met. Self-learning and -thinking AI applications go even further, not producing predetermined outcomes yet without needing human input. How can such applications be expected or forced to respect legal norms? Furthermore, even if there is a person or group of persons behind a blockchain or comparable application, it may be impossible to identify or locate them, which makes it very difficult to enforce legal norms against them. This is particularly the case with unregulated, permissionless blockchains. There can be informal groups of dedicated users that de facto manage the blockchain, but they are most likely not organized to such extent that they can be held accountable for the functioning of the blockchain.

The same goes for distributed autonomous organizations (DAO). In order for these entities to be accountable under national law, they would have to be recognized as legal persons. But this presupposes some sort of founding act by one or more natural persons in a particular legal jurisdiction, according to the rules of that jurisdiction, whereas DAOs can simply be created online by any person without adhering to any rules. In a scenario where a great deal of digital interaction takes place with no immediately identifiable human actors, expecting digital applications

<sup>42</sup> Wright and De Filippi, at 49.

<sup>43</sup> This is for instance suggested in [https://www.ibe.org.uk/userassets/briefings/ibe\\_briefing\\_58\\_business\\_ethics\\_and\\_artificial\\_intelligence.pdf](https://www.ibe.org.uk/userassets/briefings/ibe_briefing_58_business_ethics_and_artificial_intelligence.pdf), at 5.



to adjust to the existing legal paradigm does not work. Neither would denying legal effect to transactions or actions on blockchains that do not comply with the current legal paradigm, as this would lead to unwanted levels of uncertainty and impunity, undermining the rule of law.

Therefore, new, innovative solutions are needed, focusing on adjusting the legal system to make it compatible with the realities of blockchain and related technologies. This is very much unexplored territory and calls for creative thinking. Perhaps a form of collective insurance can protect against damage caused by blockchain applications that do not have an identifiable owner or manager. Perhaps providers or other intermediaries that offer access to a blockchain should be vicariously liable for the blockchains in their portfolio. Perhaps certain legal principles or rules can be translated into code language that can be used in the software of blockchain applications or in smart contracts.<sup>44</sup> Going further, perhaps some fundamental concepts of law need adjusting. Take for instance one of the central concepts of civil law: property or ownership. It is conceivable that at some point in time, with the advancement of the internet of things, persons will hardly 'own' any objects anymore, but will only use or share them.<sup>45</sup> Instead of a right to property, will they rather need some form of right to access? This article does not presume to be able to answer these and similar questions that need consideration but simply points out that there is a great need for further research. Given the complexity and multifaceted nature of the matter, a multidisciplinary approach is necessary, involving lawyers, technical experts, policymakers, as well as private stakeholders. As said before, it is advisable to aim for a discussion involving as many different stakeholders as possible, in order to ensure inclusiveness and coherence.

<sup>44</sup> Wright and De Filippi, at 55, mention the so-called nearest person-theory, which would imply for instance liability of creators for damage caused by the blockchain applications they created or vicarious liability of users of blockchain applications.

<sup>45</sup> [https://www.nytimes.com/2015/08/31/business/dealbook/bitcoin-technology-piques-interest-on-wall-st.html?\\_r=0](https://www.nytimes.com/2015/08/31/business/dealbook/bitcoin-technology-piques-interest-on-wall-st.html?_r=0)

A final word on remedy, more particularly on who is responsible for remedying violations of rights. The primary bearers of this responsibility are states. They have to comply with human rights standards when making use of blockchain technology and they have to ensure that users of blockchain technology within their jurisdiction both respect human rights themselves and are protected against violations by others. Given the potentially far-reaching implications of blockchain technologies for societies, it is therefore essential that states take an active role in the debates surrounding these technologies and perhaps even take part in the design process. This needs to be done both at the national and the international level, as blockchain technology, like any digital technology, does not respect boundaries. However, not only states have human rights obligations; private actors, including tech companies, have a responsibility as well. Especially in the field of blockchain and other technologies, where most of the innovations originate with the private sector. According to the UN Guiding Principles for Business and Human Rights, businesses have to carefully examine their planned activities and projects for potential human rights impacts and take measures to prevent or remedy any negative impacts. It does not suffice to wait for government regulation or actions by the public: an active effort to comply with and advance human rights is required.<sup>46</sup> Quite rightly, some commentators have therefore called for a human rights by design approach, which means that human rights are taken into account at the earliest time, when blockchain technologies are being planned and conceived.<sup>47</sup> Moreover, developers of technological applications need to be as transparent as possible with regard to what they plan to make and how their products work, and they need to make an effort to explain this in a way that people from other disciplines understand. Only

<sup>46</sup> This obligation is not (yet) legally binding at the international level; the UN Guiding Principles constitute so-called soft law. However, discussions on an international legally binding instrument are ongoing and more and more states adopt national legislation regulating businesses' responsibility with regard to human rights.

<sup>47</sup> <https://www.bsr.org/en/our-insights/blog-view/human-rights-by-design>

then a meaningful discussion can take place with regard to how these technologies can benefit human rights rather than harm them.

#### 4.4 CONCLUSION

Blockchain is both a gift and a threat from a human rights perspective. In order to make sure that the positive impact



greatly outweighs the negative, it is necessary that human rights are taken into consideration from an early stage in the development and implementation process of blockchain applications, as well as in broader discussions on governance of blockchain and related technologies. Human rights by design is a crucial principle, as many of the human rights issues identified in this article

can only be tackled in the beginning phase of a new application. The right to privacy is especially vulnerable in this context. This is because of the special characteristic of blockchain that data once submitted cannot be changed or deleted, which means that mistakes made with regard to personal data cannot be undone. But also because the right to privacy requires informed consent by consumers with regard to personal data and there is a real risk that blockchain applications are so technically complex that they easily defy the average person's understanding.

Even though businesses and other private actors have the responsibility to respect human rights, they probably need encouragement from governments, especially where human rights-friendly solutions cost money. This means that states should actively participate in the debates and

trials currently taking place and that they should act timely to get their regulatory bodies in order. They have to make choices that promote and reinforce human rights before the technical reality makes choices on their behalf.

A closer look on the points made in this article reveals that a considerable part of them are not exclusively relevant for human rights, but rather stem from a more fundamental, general unease between the current legal paradigm, which is adapted to analogous realities and applies a human focus, and the digital paradigm, which is binary in nature and applies a logical, mathematical focus. This tension will only increase, as blockchain technology enters the phase of autonomously operating smart contracts and autonomous organizations. Not all technologies are the same, however. There is for instance a fundamental difference between permissioned blockchains and unregulated, permissionless blockchains. As permissioned blockchains or regulated permissionless blockchains run by certain rules, they can more easily be regulated and forced to fit into current legal systems. Unregulated, permissionless blockchains, however, pose some fundamental challenges in terms of governability and accountability that cannot easily be solved. They call for a multidisciplinary, multi-stakeholder debate about how to make sure that they live up to their revolutionary potential in a way that is consistent with human rights and the rule of law. Technological experts and lawyers have so far each operated more or less independently. The challenges outlined in this article make clear that this can no longer continue. Legal and technical expertise need to team up in order to devise solutions that are technically feasible and respectful of human rights.

*“Blockchain is both a gift and a threat from a human rights perspective.”*



# 05

## Implications of blockchain / DLT on the UN System

*Benedetta Audia*<sup>48</sup>

<sup>48</sup> Benedetta Audia is Corporate Legal Advisor and Head of the Commercial and Institutional Law Practice at the United Nations Office for Project Services (UNOPS). The author gratefully acknowledges the contribution of Nathaniel Green. The views reflected in this paper are personal and do not necessarily reflect those of the United Nations, including UNOPS.

Distributed ledger technology, or DLT, has rapidly earned a reputation as a groundbreaking mechanism allowing for a range of complex interactions between entities, be they individual persons or complex organizations, without the verification and authentication practices traditionally provided by trusted third parties. Blockchain is nearly synonymous with DLT, and is perhaps best known for its critical functionality within the basic software protocol for the cryptocurrency bitcoin. That said, DLT mechanisms offer other possibilities for the re-orientation of existing social, economic and political systems vis-à-vis traditional oversight mechanisms. As such, blockchain systems (a term here used interchangeably with DLT)<sup>49</sup> suggest new pathways for international development practices, but simultaneously open up new legal questions where existing regulatory mechanisms are potentially bypassed.

However, a blockchain protocol is not a panacea. Blockchain can be a valuable tool in allowing established needs to be met with greater efficiency and, in some cases, greater security and democratization, but it will not solve underlying problems related to, for example, lack of governance capacity or lack of access to secure internet connections in a given country or region. In this light, the use of blockchain in the UN System and in development contexts more generally must be tempered by an understanding that use of blockchain protocols must work in tandem with more traditional mechanisms, and must begin with carefully-selected tools designed to address clear administrative obstacles in well-understood and clearly defined circumstances.

The following chapter discusses potential uses of blockchain protocols in the international development context, coupled with the legal issues likely to accompany

<sup>49</sup> Blockchain is in actuality one permutation of DLT technology, but its rise to prominence in international media discourse allows and encourages its use as a synonym for DLT generally. See Blemus, Stéphane, Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide (January 17, 2018). *Revue Trimestrielle de Droit Financier (RTDF)* (Forthcoming). Available at SSRN: <https://ssrn.com/abstract=3080639>

extensive deployment of this technology. More specifically, we discuss possibilities within the UN System for use of blockchain-based transactional protocols and address how legal questions involving blockchain-enabled processes and entities will fit within the UN regulatory framework. In addition, we address the question of blockchain's likely future in international development contexts, and ask whether the UN System is prepared to address the changes in financial, political, and other practices that may accompany such a development. This chapter ultimately argues that UN System regulators and administrators should be prepared to develop new approaches to the use of cryptocurrencies and to the formation and management of "smart contracts" and other blockchain-enabled protocols that are likely to enter into UN practices.

## 5.1 FORMS AND USES FOR BLOCKCHAIN IN THE DEVELOPMENT CONTEXT



Within the UN system as a whole, an interest in the streamlining and democratizing potential of blockchain systems has given rise to a great number of individual programs and initiatives.

In the development arena specifically, blockchain protocols have found their way into new platforms for addressing a range of development problems. Uses for blockchain-based tools in the UN system can be roughly divided into two categories: 1) those that use cryptocurrencies to address challenges in financial practices, and 2) those that seek to use blockchain to build social and governance structures meant to

directly address a range of well-recognized challenges in development work. Both tracks present in turn their own challenges in implementation and corresponding legal issues to be considered, among them being privacy issues, donor restrictions, and lack of governance/technical capacity in developing regions. We begin with a discussion of the potential for use of cryptocurrency within the UN system.

Cryptocurrency is the heart of blockchain development. Bitcoin, still the most recognized and largest cryptocurrency in terms of market size, is built on the first blockchain protocol, and in a real sense is the origin point for all further blockchain developments. The bitcoin blockchain protocol created the first instance of scarcity in a purely digital, information-based and non-physical sense. The creation of new bitcoin units are managed through a consensus protocol termed "proof of work," which involves using computer power to run through complex mathematical problems, in the course of which activities simultaneously providing a node, or transaction validator, in the bitcoin distributed ledger. Each bitcoin uses two keys for ownership and identification, one key being public and the other private. Each key is verified by being matched across a network of distributed ledgers, where each bitcoin transaction is recorded in individual "blocks." Once a transaction is recorded in a block on the blockchain the transaction becomes indelible, and is checked and verified across an entire distributed network of ledgers, making forgery or alteration nearly impossible. Scarcity in bitcoin circulation is created through the amount of computing power needed to create new bitcoin units, which increases with each new generation of bitcoins and miners (nodes) that join the system.

*“Whilst the bitcoin platform is by its nature public, permissioned or permissionless blockchain platforms have a wide range of uses beyond the cryptocurrency model.”*

Because each bitcoin transaction is verified through participation in the bitcoin blockchain, traditional trust mechanisms including banks and other third-party actors are unnecessary, making bitcoin transactions less expensive and more efficient, and in some cases more accessible to individuals and organizations who are either not wealthy enough to take part in complex international financial flows, or who are seen as too high a risk by the larger financial institutions. The public nature of the blockchain protocols that host most cryptocurrencies is essential to its working as an alternative currency. Because the blockchain protocol is open to use by any member of the public, the consensus mechanism providing for the verification of transactions remains, in principle, evenly distributed.

Whilst the bitcoin platform is by its nature public, permissioned or permissionless blockchain platforms have a wide range of uses beyond the cryptocurrency model. A semi-private, or consortium blockchain is a member-restricted platform in which an administrator grants permission to one group of members to make transactions, and grants permissions to another group to perform block validation.<sup>50</sup> There may be some overlap between the two groups. Like public blockchains, consortium blockchains use synchronized distributed ledgers instead of central registries.<sup>51</sup> Thus, both types of blockchain protocols are attractive for similar reasons, arising from the bypassing of intermediaries and providing for more direct and efficient transactions. Fully private blockchains also exist, where the blockchain is not necessarily used to facilitate financial or other types of transactions between distinct entities, and instead where a single organization replaces its central database with distributed ledgers.<sup>52</sup> Fully private blockchains potentially have their place in development

practices, but because of their insular framework are more limited in their effects across extensive systems.

## **5.2 BLOCKCHAIN AND THE NEED FOR TRUSTED INTERMEDIARIES: BANKING, FINANCE, CRYPTOCURRENCIES AND CONSORTIUMS**

A blockchain protocol is a type of trust mechanism, this being a role traditionally given to neutral third parties in financial and other sensitive transactions. In development, the need to manage transactions through trusted third parties creates a number of bottlenecks, where for example complex financial transactions are managed by banking institutions

which add their own fees to any given process, leading to increased costs and a bias towards larger institutions whose resources allow for extensive international financial flows. In the development arena, the appeal of blockchain arises from its ability to eliminate the need for trusted third parties, since the blockchain algorithm itself provides for the verification of a financial transfer or other transaction. This then provides the opportunity to both greatly reduce the costs associated with securing development funding, and to potentially open up the process to entities and organizations traditionally marginalized through lack of sufficient resources.



<sup>50</sup> Takahashi, 2

<sup>51</sup> Id

<sup>52</sup> Id., 3.

### 5.3 BANKING: BITCOIN AND BLOCKCHAIN CONSORTIUMS

In the case of activities pursued by UN system organizations, blockchain systems have the potential to replace banks as financial intermediaries for the transfer and exchange of funds. Cross-border international financial flows are the lifeblood of development work, and are often rendered inefficient by the lack of any coordinated global payment infrastructure.<sup>53</sup> A number of blockchain-based payment structures, including bitcoin itself, have been proposed as a means of developing such an infrastructure. The use of bitcoin or other cryptocurrencies, or the use of more ambitious platforms such as complex smart contracts (such as those built on the Ethereum protocol) or interledger protocols, could do much to streamline international payments by limiting the number of banking instructions and accounts necessary for such transactions.

In addition, the high cost of “de-risking,” associated with “Know Your Customer” (KYC) practices and increased scrutiny of money-laundering practices, might be ameliorated through the use of blockchain.<sup>54</sup> Blockchain protocols used in this capacity are most likely to be semi-private in structure and to connect opt-in consortiums comprising institutions united by a common industry or practice. Those institutions involved in international financial flows, for example banks and international aid donors, could use such blockchain platforms to share information regarding financial records and transactions in the process of standardized due diligence practices. The exercise of due diligence in regards to prospective donors is a major part of international development work, given the primacy of public mandate and the corresponding need to manage reputational and compliance risks. At present, KYC practices require a great amount of redundancy,

as each new customer-bank relationship must be independently evaluated. Blockchain could potentially allow for a centralized KYC process, where a centralized authority allows access to blockchain-stored client data to approved banking agencies. For example, in October 2017 the Infocomm Media Development Authority of Singapore (IMDA) completed initial tests of an ASEAN-regional KYC blockchain proof-of-concept in collaboration with HSBC, Japan’s Mitsubishi UFJ Financial Group, and OCBC Bank.<sup>55</sup> The Singapore KYC blockchain protocol allows banks, customers and regulators to opt in to a regulatory system that verifies identities and background data in real time. In this context, banks and associated regulators can record, access, and share customer data across a distributed network, with each recorded transaction validated near-instantly via the blockchain’s specific consensus protocol. While such blockchain-based data consortiums are still in development, the potential for increased efficiency and collaboration between actors in international finance is readily apparent.

However, such solutions give rise to legal concerns centered on privacy and sovereignty. To participate in a blockchain-based consortium such as that being tested in Singapore, customers must transition from the ad hoc, transaction-by-transaction process of validating the customer’s identity and credentials, to one where the customer must allow a central authority to manage disbursement of credentials to approved entities. Such a process causes a significant shift in the ability of the blockchain participant to manage release of sensitive information on an incremental basis, and also places said information in the possession, more or less permanently, of an entity (this being the blockchain-based consortium itself) that at this time is uncertain in its legal identity. The Singapore model so far appears to have

<sup>53</sup> Michael Pisa and Matt Juden. 2017. “Blockchain and Economic Development: Hype vs. Reality.” CGD Policy Paper. Washington, DC: Center for Global Development. <https://www.cgdev.org/publication/blockchain-and-economic-development-hype-vs-reality>, 16.

<sup>54</sup> Id, 18

<sup>55</sup> <https://www.ccn.com/singapore-regulator-banks-complete-kyc-blockchain-prototype/>

withstood security testing, and it may be that the IMDA is to serve as the liable party and de facto legal personality for the consortium should a major breach occur. Still, the legal question remains and must be addressed through relevant rules and regulations. In the case of UN system organizations, should international aid donors opt in a KYC consortium based on a semi-private blockchain protocol similar to that used in the Singapore model, it could make for a far more efficient KYC process overall, requiring fewer resources and allowing for closer collaboration between donors and respective programs. In particular, a UN-developed and managed protocol would help to establish a new regulatory landscape for such financial data consortiums, and given the UN established public mandate and framework deriving from such documents as the UN Charter, the UN Suppliers Code of Conduct, and the UN Global Compact, UN system organizations are in an ideal position to ensure that semi-private financial consortiums develop according to relevant international norms.

#### 5.4 RECEIVING FUNDS: CONTRIBUTIONS IN CRYPTOCURRENCY

Within the UN system the use of cryptocurrency is attractive for a number of reasons. As referenced above, by providing an automated trust mechanism, the use of cryptocurrency on the part of donors could bring greater efficiency to the delivery and implementation of development funds. In the public sector reasons for interest are related to those expressed in the private sector, but characterized by a few important differences related often to the need to consider widely differing levels in terms of local capacity and services. The approaches for receiving donor funds

in development activities in this context involve both use of cryptocurrencies and use of more complex blockchain-based consortiums.

As noted earlier, the use of remittances is a major source of financing in development work. As is noted in World Bank studies, percentage fees on the sending of remittances to developing countries on average remain roughly 4.5 percentage points higher than the UN Sustainable Development Goals target of 3 percent, despite conventional industry efforts to bring these prices down.<sup>56</sup> A number of start-ups are working to develop ways of lowering the cost of international payments through use of blockchain, some being focused on the use of retail remittances, while others focus on business to business (B2B) payments.<sup>57</sup>

A few distinct approaches to the use of cryptocurrency for the donation of funds for development exist. For the purposes of this chapter we assume the use of bitcoin, this being the dominant cryptocurrency in common use today. All development approaches use cryptocurrency to avoid excess charges associated with the correspondent banking system by exchanging traditional currencies or other exchange mechanisms for bitcoin or another cryptocurrency at some or all stages of a transaction. In international development practices, such innovative approaches to finance are certainly attractive because they streamline the process and reduce expenses. In regions where UN system organizations work to develop a host of programs, ranging from capacity-building in governance to infrastructure development, savings may be directed to the implementation of additional project activities. Furthermore, any financial exchange using bitcoin is free of localized trust mechanisms, most of which are subject

*“... by providing an automated trust mechanism, the use of cryptocurrency on the part of donors could bring greater efficiency to the delivery and implementation of development funds.”*

<sup>56</sup> Pisa and Juden, 17.

<sup>57</sup> Id.

to political or social shifts.

In the case of UN system organizations, the development of a UN bitcoin Wallet might be an important first step in allowing donors to fund UN programs via cryptocurrency exchange. A UN wallet service could allow for individual or groups of donors to provide funds in bitcoin that are aimed directly at certain projects, or paid into a central bitcoin pool.

A number of practical and legal issues arise when considering large-scale donations handled in bitcoin. For one, obviously in most places it is not yet possible to use cryptocurrency in day to day transactions, and in many places where UN system organizations carry out activities, communications infrastructure and internet access do not provide a stable enough platform for easy management of bitcoin transactions. For this reason, the UN System organizations may need to work with bitcoin exchanges. These services provide for the management of bitcoin transactions and exchange to and from local or fiat currencies. Bitcoin exchanges are also closely regulated in most countries, which may help to mitigate legal issues associated with working in a currency that is at present not backed by any sovereign entity.

Legal issues concerning the streamlining of financial transactions used in economic development practice stem in part from the current lack of uniform regulation for virtual currencies, although numerous jurists have cited the possibility of building new regulatory frameworks to account for their use. Still, in legal practice the use of bitcoin and other cryptocurrencies introduces issues of due diligence that affect the actors in the development world particularly. At present, the regulation of

cryptocurrencies is fragmented but also in near-constant flux. Many countries in which bitcoin transactions take place have promulgated regulations that require bitcoin exchanges to comply with domestic anti-money laundering and KYC laws. Such states include Canada, Australia, and Japan.<sup>58</sup> In the United States, regulation of bitcoin exchanges is still uncertain and bitcoin regulation itself is fragmented between the individual states, though the Federal Securities and Exchange commission views bitcoin as a commodity and regulates the cryptocurrency accordingly.<sup>59</sup> A few countries, such as Bolivia and Bangladesh, have expressly outlawed bitcoin transactions. Meanwhile, in South Korea and China, bitcoin exchanges are under increasing regulatory scrutiny, although recent reports that South Korea is exploring the possibility of building joint bitcoin exchanges with Japan and China may signal a shift in this landscape.<sup>60</sup> Taken as a whole, these developments present varying degrees of uncertainty, and as a result regulatory risk is a major consideration for any program based on use of cryptocurrencies.<sup>61</sup>

Another form of risk associated with the use of bitcoin is that associated with fraud and money-laundering. This is especially true of the public development sphere, where reputational risk carries particular weight. Legal scholars have suggested that, in many cases, use of bitcoin falls into a grey area not anticipated by domestic anti-money laundering (AML) statutes. The United States itself appears to be one such jurisdiction.<sup>62</sup> Players in the international finance industry observe that bitcoin can be used to bypass traditional regulatory choke-points, such as international banking institutions, and therefore help some individuals



<sup>58</sup> <https://www.coindesk.com/information/is-bitcoin-legal/>

<sup>59</sup> <https://www.wsj.com/articles/who-regulates-bitcoin-trading-no-u-s-agency-has-jurisdiction-1514116800.wi>

<sup>60</sup> <https://www.coindesk.com/report-south-korea-eyes-joint-crypto-regulations-with-china-japan/>.

<sup>61</sup> <https://www.ft.com/content/e561743a-dec4-11e7-a8a4-0a1e63a52f9c>

<sup>62</sup> Danton Bryans, Bitcoin and Money Laundering: mining for an effective solution ( Indiana University Law Journal, Winter 2014) Available at: <https://www.repository.law.indiana.edu/ilj/vol89/iss1/13/>

and entities avoid scrutiny under post-2008 AML statutes. Risk management in this area requires intense scrutiny, as demonstrated in January 2018, where the Metropolitan Bank Holding Corp., a major provider of bitcoin services, halted all international wire transfers in response to an instance of possible fraud.<sup>63</sup> In addition, some countries such have introduced the concept of cryptocurrency as a means of bypassing international sanctions, the most recent and prominent example being Venezuela's "Petro," an oil-backed cryptocurrency. General consensus argues that there is simply not enough cryptocurrency available to make widespread avoidance of sanctions possible, but the association may restrict use of bitcoin among international donors.

## 5.5 DISBURSEMENT OF FUNDS: SMART CONTRACTS AND PROCUREMENT

Cryptocurrency is only one form of blockchain protocol with potential to change the nature of development work. Blockchain structures also allow for complex legal and financial relationships to be layered into base DLT protocols.<sup>64</sup> These automated systems are popularly known as "smart contracts," and typically reflect the semi-private or consortium approach to building blockchain protocols. The cryptographic redundancy and distributed nature of blockchain protocols allows the management of and participation in a smart contract to occur entirely online, without requiring such "real world" processes such as the exchange of physical copies or signatures.<sup>65</sup> Also, basic follow-through on the terms of a smart contract can be automated, and not require separate and potentially delayed initiative on part of human actors. As such, a smart contract can monitor business or other

developments remotely, and, for example, disburse funds under prescribed circumstances without requiring direct human input.

Whole systems can be built on the model of the smart contract, and these are often termed Decentralized Autonomous Organizations, or DAOs. In public discussions regarding possible uses for blockchain protocols, particularly in the economic sphere, there is as yet no firm differentiation between the terms DAO and smart contract. As a practical matter, we might understand a DAO to be a form of smart contract, characterized by an extensive community of participants, often acting without shared goals but with shared interest in the value created by the workings of the central blockchain protocol.<sup>66</sup> In this sense, a DAO takes on some of the characteristics of traditional corporate entities, though the legal status of a DAO, meaning in part whether it should be treated as a contract or as a legal personality, and if so under what legal standards, is a matter of recent debate. The DAO itself as a term is derived from the Ethereum-based DAO, which once essentially operated as a virtual, decentralized venture capital firm and famously fell to an exploit on part of a member who used a coding flaw to withdraw one third of the DAO's fund in 2014. While the failure of the original DAO does not take away from the usefulness of complex smart-contract structures generally, it does point directly to the due diligence and liability issues that will take center stage at any rollout of blockchain protocols. As these form radically centralized systems (in that a failure affects a range of players and activities previously handled by multiple actors), it is of vital importance that the code running such protocols be developed and managed according to strict guidelines.

*"The cryptographic redundancy and distributed nature of blockchain protocols allows the management of and participation in a smart contract to occur entirely online, without requiring such "real world" processes ..."*

<sup>63</sup> <https://www.thetimes.co.uk/article/bitcoin-bank-metropolitan-bank-holding-corp-halts-transfers-over-money-laundering-fears-lw8979kfm>

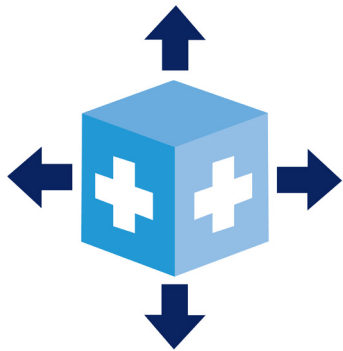
<sup>64</sup> Carly L. Reyes et al., Distributed Governance, William and Mary Law Review Online, v.59 (2017) 11.

<sup>65</sup> Id, 12.

<sup>66</sup> See Czarnecki, 10.



Much of the nascent exploration of blockchain-enabled programming in the UN system is based on or envisions the use of smart contract or DAO-type protocols for large-scale coordination. Such coordination can also rely on existing protocols, such as cryptocurrencies, especially in the case of financial transactions. Blockchain is attractive within the UN space for a number of reasons. In the context of development funding and the distribution of said funds, blockchain-based platforms could lend themselves to greater transparency stemming from the fact that all transactions in a blockchain are recorded and immutable.<sup>67</sup>



A DAO-type blockchain structure, for example, could allow numerous international aid actors to better coordinate the disbursement of funds in response to short- and longer-term challenges, potentially by feeding into a neutral centralized and contractual structure that cannot be altered by any single entity, and yet being open to all international aid operators. Such an organization could do much to speed access to aid and to simultaneously avoid unnecessary duplications.<sup>68</sup>

In doing business with non-UN entities, for example it is appropriate to ask whether such a virtual and legally ambiguous (in its identity at least) entity as a DAO is a legitimate potential partner under UN rules and regulations. The answer to this question is mixed: in practice, UN organizations enjoy broad authority in the choice of partners. However, regulations generally stipulate that entities engaging with UN organizations shall obey the laws of their respective home jurisdictions, while other regulations assume the fact of a partner or vendor's

<sup>67</sup> <https://www.unops.org/news-and-stories/insights/could-Bitcoin-technology-revolutionize-aid-distribution>

<sup>68</sup> Id.

physical presence somewhere in the world. Regardless, the trend in digital commerce is moving toward a reality where more commercial companies and foundations will have no physical presence.

Taking the United Nations Office for Project Services (UNOPS) by example, provisions discussing vendor eligibility make no mention of the need for national registration or for adherence to specified national laws. Meanwhile, UNOPS procurement rules do require that prospective vendors adhere to certain international norms, which in the case of work with or through DAO structures could be said to take the place of the regulatory structures that typically affect corporate entities through national registration. To illustrate, Section 2: Ethics of the OI on Vendor Sanctions provides that, "UNOPS expects all vendors who wish to do business with UNOPS to embrace the United Nations Supplier Code of Conduct. Furthermore, UNOPS expects all its suppliers to adhere to principles of the United Nations Global Compact." These cited rules, being the Global Compact and the Supplier Code of Conduct, also do not require that a contracting entity be a traditional, physically-located and incorporated legal personality. However, other procedural requirements might complicate this picture.

While UN regulations do not explicitly disqualify DAOs from taking part in procurement activities, some procedural requirements might lead to delay or confusion in the process. For example, all vendors wishing to contract with UNOPS must register with the UN Global Marketplace service (UNGM). The registration process for the UNGM allows for individual consultants, traditional company/NGO structures, trade missions, and UN organizations. For future work with DAOs as prospective vendor



organizations, UN system procedures would need to expand to deliberately accommodate these types of virtual entities.

As with prospective procurement partners, the UN system lacks specific requirements dictating the legal form or personality of organizations whose funding provides for the activities of UN organizations. Again, the problem here in working with DAOs stems from the question of fitting UN contracting procedures to the decentralized nature of a DAO. As required by UN general rules on contracting, UN organizations must have contact with individuals in a funding organization who are authorized to formally agree to UN and the organization's terms and conditions. Therefore, while DAO structures comprised of funding organizations could do much to streamline the deployment of funding especially in times of crisis, it is likely that new regulatory structures concerning DAOs specifically must be developed in order to establish consistent solutions for such gaps.

Scholars have noted that a solution to the lack of direct, hierarchical representation within DAO systems could be the creation of third-party entities to serve as contractual intermediaries between DAO-based communities and regulatory mechanisms or third-party partners, and some have suggested that UNCITRAL play a central role in outlining a regulatory framework for this process.<sup>69</sup>

## 5.6 SOCIAL AND GOVERNANCE-ORIENTED APPLICATIONS FOR BLOCKCHAIN

Beyond strictly financial matters, other blockchain-enabled initiatives in the UN system have been proposed, and some

implemented. Strong possibilities exist for governance, for example where DAO-type approaches could be used to build voting systems in areas where existing systems either do not exist or are fundamentally compromised. Because blockchain systems are able to bypass traditional regulatory bottlenecks, public trust once invested in such a system is difficult to upset through, for example, distrust of vote-counting. The built-in transparency available through blockchain is in this context another significant benefit. Generally DAOs do require human oversight at the fringes of their respective activities, to ensure that failures relating to programming are promptly addressed or that a DAO's founding mandate remains central to its operations. In the case of governance-related DAO platforms, UN system organizations could learn to fill this role.

Scholars have noted that, in the private sphere, blockchain-based structures have the potential to change the way corporate governance decision-making works at a fundamental level.<sup>70</sup> In the public sphere these changes may be especially welcome given the mandates common to UN organizations and other participants in the development arena. However, in the UN context a range of issues exist as to the ambiguous legal identity of smart contracts and DAO-type communities.

## 5.7 ISSUES OF REAL AND INTELLECTUAL PROPERTY

Access to real property is a matter of central importance in international development work. For UNOPS in particular,

<sup>70</sup> Reyes, 19.

<sup>69</sup> Riccardo de Caria, A Digital Revolution in International Trade? The International Legal Framework for Blockchain Technologies, Virtual Currencies and Smart Contracts: Challenges and Opportunities (2017).



infrastructure development is a central part of the organization's mandate. As noted at the beginning of this chapter, blockchain by itself is a tool for simplifying and streamlining, and in some cases democratizing financial and other transactional relationships. This fact is especially important in the case of using blockchain to improve land registration systems.

This is also a distinct problem as a legal issue, since in many regions it is difficult to obtain adequate property records, and legal proof of ownership is often uncertain. Blockchain can provide a solution to this problem in some contexts. Several pilot projects have been launched in recent years using blockchain to secure property rights, notably in Georgia, where the country's already very strong land registration system has successfully transitioned to a blockchain platform, with corresponding gains in security and transparency.<sup>71</sup> In Ghana, also, two startups have recently begun to develop blockchain-based land registries, going by the names BenBen and Bitland.<sup>72</sup> Both companies have seen some success in connecting rural, largely undocumented regions with central government registries, and both speak of international expansion in the near future.

However, obstacles exist to the development of such systems. Blockchain systems must after all rely on existing records, and where legacy record systems are inadequate the blockchain transition will be difficult, expensive, and provide still-uncertain data. Such transition, therefore, must be accompanied by some type of governance capacity building in the field. In the case of Georgia's successful blockchain-based land registry, the country began with a traditional type of centralized bureaucratic land registry that was consistently updated, well managed, and did not

<sup>71</sup> Pisa and Juden, 30.

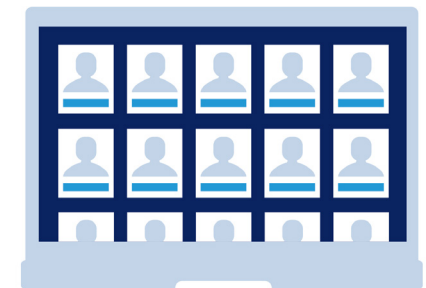
<sup>72</sup> <https://www.devex.com/news/opinion-7-ways-to-use-blockchain-for-international-development-90839>

lack for public trust. The underlying data, then, patched into the blockchain protocol was about to provide a stable foundation for the new, centralized system. In states where land registries are less well-managed, blockchain is only the second step after reform of the data-collection mechanisms themselves.

The first steps in such a transition can therefore be very challenging and costly, and require great expertise in governance capacity development. In the case of UNOPS, however, the process may well be worth the effort, central as it is to the infrastructure development mandate. Aid given for the blockchain-based systematization of land registries, for example, might be predicated on preparatory efforts to assemble a reliable and transparent land registry archive. This is the beginning of a conversation, but one with far-reaching implications for the fundamental workings of development practices.

## 5.8 PERSONAL IDENTIFICATION AND VOTING: PRIVACY AND OTHER CONSIDERATIONS

Real Property registration is related to another possible role for blockchain in development, this being the registration of personal assets, and by extension the creation of tamper-proof identification systems for marginal, displaced, and otherwise vulnerable populations. While blockchain systems for these purposes would mark significant improvement for eliminating the problem of fatal weak links (being decentralized) and being resistant to tampering, the privacy implications are problematic.



*“UN system organizations can offer a solution based on a hybrid approach to the basic decentralized systems model that typically defines blockchain technology.”*

The concept of an “identity wallet” has been widely discussed, making individual identity practices dependent on decentralized networks rather than states. However, this aspect is also problematic from a privacy standpoint, in that the information on individuals is widely shared across many access points. In the UN system, the General Assembly’s Resolution 69/166 places strict scrutiny on the mass collection and distribution of personal data on digital frameworks. Identity wallet protocols, therefore, should be very carefully constructed with adequate safeguards.

UN system organizations can offer a solution based on a hybrid approach to the basic decentralized systems model that typically defines blockchain technology. It seems clear that user-centric ID systems, while they may run on blockchain and so be open to all the benefits listed above, must rely on the active participation of central authorities in order to be effective.<sup>73</sup> In this sense, the semi-private blockchain protocol described earlier may have uses beyond the financial sphere, and may open up another niche for UN regulatory leadership.

With such obstacles in mind, the UN High Commission for Refugees (UNHCR) has initiated a program for the issuing of international, universal identification credentials: 1) to quickly determine what services a given person needs; 2) to provide secure identification; and 3) to improve documentation to help refugees find long-term solutions.<sup>74</sup> This project has moved ahead in the past year, with a centralized system built by Accenture and a prototype blockchain digital ID network developed by Accenture and Microsoft and designed to run on the UNHCR ID management system.<sup>75</sup> Specifically, if a blockchain system were developed for international identification, but confined to dedicated systems and subject to an assigned

<sup>73</sup> Id., 27.

<sup>74</sup> Pisa and Juden, 27.

and neutral third-party auditor, privacy risks could be greatly mitigated. Another exercise in the development of blockchain-based universal ID concerns the narrowly-targeted issue of child trafficking in Moldova, a country where lack of identification credentials often makes the area a target for human traffickers. UNOPS, in conjunction with the World Identity Network and other agencies, is currently involved in developing a blockchain-based identification protocol for children in the region, which due to the properties of the platform will allow for universal credentials verification that can be incorporated in local practices, and might therefore be up and running much more quickly.<sup>76</sup> Such efficiency is a vital improvement given the immediacy of the problems involved.

Universal identification for high-risk populations and the improvement of property registration both involve the problems of source material and technological access. Each is needed to make the new system work, and each is likely to be difficult to achieve where the new system is needed most. In many cases, such as in the context of international business and finance, the opportunities are slim and the need to improve circumstances on the ground may often outweigh opportunities for growth. In the case of UNOPS, however, the strength of the organization’s public mandate makes such targeted blockchain projects worth the resources involved. Moreover, UNOPS holds the expertise and, again, mandate needed to pursue corresponding work in capacity development at the social and governance sectors in participating regions.

<sup>75</sup> Id.

<sup>76</sup> <https://www.reuters.com/article/us-moldova-blockchain-child-trafficking/moldova-eyes-blockchain-to-end-child-trafficking-idUSKBN1DF2GQ>

## 5.9 CONCLUSION: A NORMATIVE ROLE FOR UN ORGANIZATIONS IN BLOCKCHAIN DEVELOPMENT

Use of blockchain protocols in development is as new as it is promising, and the UN system is in a unique position by way of the reach of its operations, and by way of its independence and institutional experience. Because UN system organizations show enough regulatory flexibility to work with and refine blockchain platforms under current circumstances, UN activities might serve as a kind of test lab both for blockchain systems and for new regulatory approaches to blockchain-based international transactions. As noted at several points in this chapter, a solution to the lack of direct, hierarchical representation within complex blockchain systems could be the creation of third-party entities to serve as contractual intermediaries between DAO-type communities and regulatory mechanisms or third-party partners.

Some have suggested that UNCITRAL could play a central role in outlining a regulatory framework for this process.<sup>77</sup> Within existing UNCITRAL works, including the Model Law on Electronic Commerce, the Model Law on Electronic Signatures, the Convention on the Use of Electronic Communications in International Contracts, the Model Law on Electronic Transferable Records, and others, it appears that these existing structures can account for use of blockchain exchange systems with some amount of flexibility. However, enough exceptions exist to provide incentive for UNCITRAL to develop new works to account directly for cryptocurrencies and other blockchain-enabled transactions. For example, Koji Takahashi notes that the ST Model Law defines the word “money” as legal tender authorized by a state.<sup>78</sup> Bitcoin and other cryptocurrencies could meet this definition if

a state legally adopted it as valid currency, but looking further a cryptocurrency cannot qualify as a “tangible asset” under ST Model Law Article 2(II), and therefore cannot be treated directly as money under this regulatory model.<sup>79</sup> It is therefore recommended that UNCITRAL develop new works specifically to provide an international model for the regulation of cryptocurrencies. While current frameworks regulating international financial transactions do not tend to disallow use of cryptocurrencies per se, if such mechanisms are to become a stable and widespread source of development funding it is inevitable that more fine-tuned regulatory structures will arise to deal with the inevitable conflicts that arise.

UNCITRAL, with its resources and history of legitimacy in this area, is ideally situated to step into this niche.<sup>80</sup> Given that the UN public mandate puts UN system organizations in a position to be early developers for a range of blockchain protocol types, it is especially appropriate, and reflective of its international accountability, that the UN system takes on a corresponding normative role.

<sup>77</sup> Riccardo de Caria, *A Digital Revolution in International Trade? The International Legal Framework for Blockchain Technologies, Virtual Currencies and Smart Contracts: Challenges and Opportunities* (2017).

<sup>78</sup> Koji Takahashi, *Implications of the Blockchain Technology for the UNCITRAL Works*, 9.

<sup>77</sup> Riccardo de Caria, *A Digital Revolution in International Trade? The International Legal Framework for Blockchain Technologies, Virtual Currencies and Smart Contracts: Challenges and Opportunities* (2017).

<sup>79</sup> *Id.*, 10.

<sup>80</sup> *Id.*, 9.

# 06

## *Legal aspects of smart contracts*

*Sandra van  
Heukelom, Olivier  
Rikken and others* <sup>81</sup>

<sup>81</sup> This chapter has already been published in “Smart contracts as a specific application of blockchain technology” by O. Rikken, S. van Heukelom, S. Mul, J. Boersma, I. Bijlloo, P van Hecke, A. Rutjes, F. Stroucken, J. Linnemann, H. Terpoorten and R.R. Nederhoed.

### 6.1 INTRODUCTION

The conclusion of chapter 2 is that a smart contract is firstly deterministic computer software that is replicated and executed on a blockchain. This chapter is concerned with the legal questions regarding smart contracts.

The term smart contract in this respect is not only unfortunate because a smart contract does not always have legal significance, but also because the term suggests a contract is formed. As we will explain below, smart contracts can play a part in various legal domains, and their use needs to be considered carefully: as a source of rights and obligations, or only as an execution thereof. Whether this is the case will need to be determined for each legal system.

If smart contracts do have manifestations that represent a legal act according to the applicable law, or that can have meaning for the law or the legal relationship in which the smart contract is deployed, it must be made sure that the smart contract is programmed in such a way that the applicable legal requirements placed on the legal act for which the smart contract provides are met, or at least the requirements placed on the law or legal relationship that the parties have. In other words, the smart contract will have to represent a legal situation, and the transaction generated by the smart contract must be legal. The standards according to which the smart contract must be lawful depends on applicable law and jurisdiction. This will be discussed later.

## 6.2 CONCEIVABLE LEGAL MANIFESTATIONS

It is not inconceivable that the smart contract represents a legal act or has meaning for the law or legal relationship in which the smart contract is deployed. Depending on the applicable law, the following legal acts or meanings are conceivable:

1. Contract and/or execution of a contract
2. Suspensive condition or dissolving condition in contract
3. Unilateral legal act
4. Decision under public law
5. As (a means of) evidence
6. Automatic execution of a (legal) process
7. Obligation of compliance with (fiscal) law

There are likely (many) more legal manifestations to be identified depending on the applicable legal system. Therefore, the above list is not exhaustive. It only serves to indicate the most prevalent legal acts that are executed in a smart contract.

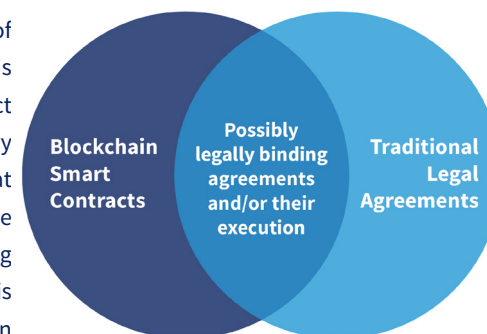
### 6.2.1 A closer look: The smart contract as a contract

Take the contract and/or the execution of a contract. A contract is a type of agreement. A smart contract, however, is firstly “just” a program on a blockchain. There will be a collection of smart contracts that are not intended for the formation of an agreement. Vice versa, there is a collection of written agreements that have nothing to do with smart contracts. In the cross-section between these two collections, there is a subset that uses smart contracts for the automated execution of (part of) an agreement. And also to possibly establish obligations.

*“It is conceivable for smart contracts to be used to an increasing extent in a way in which the code is inextricably linked to statements in a natural language.”*

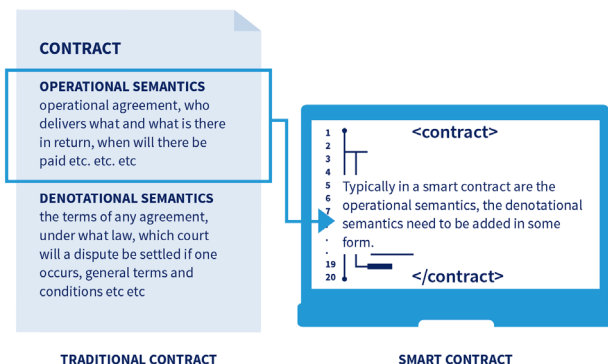
Every legal system has its own set of requirements on the basis of which it is possible to determine whether a contract has been concluded. One of the primary requirements of an agreement is that it is clear to the parties what they have agreed. In this context, and depending on the legal system, more meaning is attributed to the written representation of the agreements between parties or

the intentions of the parties. If the written representation of the agreements between the parties is decisive, then these agreements can be more easily programmed than the intentions of the parties. Moreover, smart contracts are written in a programming language like Solidity or Go and are often published on the blockchain in a “compiled” form that can only be read by computers. That is why it is recommended that the agreements written in programming language are provided to the parties in an understandable language. The benefit of this is that this also allows recording of agreements that cannot be automated or are less suitable for automation. A possible downside to agreements in standard language next to code is that there can be a discrepancy between the two.



It is conceivable for smart contracts to be used to an increasing extent in a way in which the code is inextricably linked to statements in a natural language. The natural language can serve to record matters that cannot be expressed in code (general terms and conditions, applicable law, agreement as to burden of proof, more open standards, etc.) and possibly to explain the purpose of the code. A hybrid contract combining code (or executable data structures) and prose is also called a Ricardian contract.<sup>82</sup>

<sup>82</sup> <http://iang.org/ricardian/>



Smart contracts are often based on payment in a native cryptocurrency, like bitcoin or Ether. This raises the question whether or not a cryptocurrency is a currency or a medium of exchange. This, too, depends on the legal system and will have to be properly investigated each time. According to Dutch

law, bitcoin is not a currency, it is a medium of exchange. One of the consequences is that payment with bitcoin for the delivery of goods or services is not considered to be a “purchase” as defined by law. In the Netherlands, this has been solved by declaring that the rules of purchase also apply to exchanges, but this will also differ per legal system.

### 6.3 GENERAL LEGAL ISSUES

Apart from the different manifestations, there are general legal issues with respect to smart contracts, such as applicable law, jurisdiction, liability, dispute resolution, privacy and identity.

#### 6.3.1 Applicable law

Applicable law in this case concerns: “which country’s law applies?” It needs to be said that this question only arises if a jurisdictional choice has not been made beforehand. In order to clarify which law applies, in general, a number of steps need to be taken:

1. Which legal manifestation is involved? This question is answered below.
2. What are the nationalities of the parties involved?
3. To which (international) regulations (treaty, acts, etc.) is the commitment between the parties subject?
4. Which national law is designated as the applicable law in the specific case?

Every legal manifestation of a smart contract will have its own regimen for handling these questions. Subsequently, with respect to smart contracts, there are multiple relationships; (i) the person organizing the coding of the smart contract, (ii) the programmer, (iii) in some cases, the person providing input for the smart contract, and (iv) in some case, the “beneficiary” of the output of the smart contract. A different law can apply for each of these relationships. From a technical perspective, the different aforementioned people can also be embodied in a single person. Finally, as far as we can tell, there is the complicating factor that all smart contract activities are performed by or use nodes. The location of the node(s) involved and the domicile of the person involved with an expression of will and that legal act need not always be one and the same.

#### 6.3.2 Jurisdiction – international <sup>83</sup>

Jurisdiction relates to the area over which a governmental body has authority. The legislative, executive and judicial powers all have their own specific jurisdiction. In this report, we will only discuss the judicial powers: courts.

Should it come to a dispute concerning a smart contract, then the question that follows the question of applicable law is: which court is competent? Here too, this question

<sup>83</sup> This chapter concerns the question of the court appointed from an international perspective. The question of which court is competent (absolute authority) and how proceedings are conducted is not discussed. This question can also result in additional challenges.



will only arise if no choice of jurisdiction has been made beforehand with respect to the competent court (or any other judicial body, such as an arbitration institute).

To answer the question of which court is competent, the same steps must be taken as with the question about applicable law:

1. Which legal manifestation is involved? This question is answered below.
2. What are the nationalities of the parties involved?
3. To which (international) regulations (treaty, acts, etc.) is the commitment between the parties subject?
4. Which court has been designated as the competent court by international regulations to settle the dispute in the specific case?

The first problem, or challenge, regarding the question of the competent court, like the question about applicable law, is that various legal manifestations can have a different regimen in this respect. When looking at a commitment between parties each of whom have their domicile<sup>84</sup> in a different EU member state, for instance, then the EEX regulation will generally apply. However, this regulation only applies to civil and trade matters. Moreover, article 1 of this regulation explicitly states that the regulation does not apply to tax matters, customs matters or administrative law matters. This means that the legal manifestation in which the smart contract is cast must be clear (and whether this has been done). This does not resolve the challenge; it is possible that the outcome leads to the competence of multiple courts. In this case, it is possible to select the court before which the dispute will be heard.

<sup>84</sup> Domicile with respect to a natural person is intended to be: “their place of residence” and lacking that, their actual location. With respect to a legal entity, domicile is intended to be their place of business according to statutory regulations or their own articles of association or regulations.

<sup>85</sup> Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

The second challenge has also been mentioned before: the location of the node(s) involved and the location (or domicile) of the parties involved in the smart contract are not necessarily the same. However, the question is to what extent this leads to problems. After all, the question of which court is competent to hear a dispute will only present itself once it is clear which (legal) entity against whom proceedings are initiated. Moreover, in such a case, proceedings will only (and up to now, could only) be initiated and measures will only be taken against a (legal) entity and not against a node or, in a broader sense, a system. Sometimes, this raises the question whether a system as such should not be able to participate in legal relationships or have an independent position. Currently, this is not the case and is not legally possible.

### 6.3.3 Liability

The question of the exact meaning of liability is a question that must be answered based on applicable law. The matter of (legal) liability often occurs in the context of an illegal act or breach that can be attributed to a person or company. In this case, that person or company is liable and they must compensate the damage caused. The first challenge is the fact that blockchain technology allows for activities under a pseudonym. In this case, it is difficult to determine the liable party. The question is whether or not the cryptographic signature of a party interacting with a smart contract offers sufficient certainty with respect to a physical party that can be made liable. After all, this cryptographic signature guarantees that this party can and is permitted to appeal to the smart contract, but it does not mean that the identity of that party can be established with certainty. Another question is whether there can even be a breach between parties in the first place. It is expected that exact agreements have been made regarding what would

happen in case of a specific input; it has been recorded in a piece of code. As such, the outcome is fixed and known, at least to the parties in the smart contract.

#### 6.3.4 Dispute resolution

In case of a dispute regarding the correct execution of a contract or other legal agreement, there are multiple forms of dispute resolution one can turn to, such as the decision of a court or mediator.

This also holds true for a dispute between parties that have a legal agreement in the form of a smart contract. The difference being that smart contracts can offer additional functionality to significantly simplify identifying a dispute. Moreover, in case of a value transfer through a smart contract, a guarantee for the value transfer or a refund of value could be made possible because a party is unable to destroy the value in the meantime. In these cases, a smart contract is comparable to an escrow account or third-party bank account for which the value can be released if both parties indicate via a message (a voting mechanism) that the agreements for the final value transfer have been met. If anyone does not wish to provide such a voting mechanism, for which parties' opinions exclusively lead the transaction, then alternatively the parties involved can appoint an oracle that is used to determine whether or not the transaction requirements have been met. It is possible, for instance, to agree that if a database of a weather service indicates that there was a storm at a specific location at a specific time, then automatic payment of an insurance sum occurs, for example, instead of meeting to determine whether the storm actually occurred. In such a case, it is agreed beforehand, upon drawing up the smart contract, that the status of the agreed oracle is a refutable presumption or binding proof, if so agreed in an evidentiary

agreement.

In the absence of consensus, dispute resolution can be provided by means of, for example, a signaling function the parties can use to present their dispute immediately before a third party. This third party can then offer mediation or make a binding decision. In the period of time during which the conflict is unresolved, the value can remain in the smart contract. It is conceivable that the dispute resolving body is given the authority to determine which party will be (re)granted the value recorded in the smart contract. This does mean that, in case of a protracted conflict, the parties cannot access the value in the smart contract.

It is therefore important that the parties agree beforehand how conflicts are resolved, who will take up the role of mediator or dispute resolver and what their authority is. In other words, clear agreements when drawing up smart contracts are extremely desirable.

#### 6.3.5 Privacy

Privacy concerns the protection of personal information. Personal information is data that can be directly or indirectly traced to a living natural person. In Europe, on the basis of the General Data Protection Regulation, European citizens have (as of May 2018) various rights with respect to their personal information. Among other things, this includes the right to correction of personal information, deletion thereof and the right to be forgotten (GDPR).

Personal information can be processed in smart contracts. In this case, qualification issues will arise initially as a result of the applicable laws. For instance, the law makes a distinction between a data controller and a data processor.

*“ In Europe, on the basis of the General Data Protection Regulation, European citizens have (as of May 2018) various rights with respect to their personal information. Among other things, this includes the right to correction of personal information, deletion thereof and the right to be forgotten (GDPR). ”*

Different legal requirements apply to the data controller and the data processor. It is conceivable, for example, that all participants in/users of a blockchain and smart contract in which personal information is exchanged are data controllers and have to meet (all) legal requirements (independent from one another). It is less clear, however, whether or not the other parties that participate in the blockchain (all parties that run the nodes) also have a specific status based on the Dutch Personal Data Protection Act. We can imagine that those nodes must be considered to be processors of personal information. If this is the case, then they, too, must meet the basic principles of the Dutch Personal Data Protection Act and enter into processing agreements with the data controllers, for example.

As discussed earlier, with respect to compliance with privacy law requirements it is relevant to make a distinction between permissionless and permissioned blockchains. The latter makes it possible to influence governance of the blockchain and (among other things) control who is responsible for compliance with the GDPR requirements. Accordingly, in these cases a determination can be made of who safeguards the citizen's rights, such as the right to correction, and in which manner this is done. When starting up the blockchain, the participants can agree on this accordingly. This is different for permissionless blockchains where nobody and everyone has control and for which these kinds of agreements are much harder to make due to the free-access possibility and the lack of governance control. The possibility of protecting privacy in such situations will have to be investigated further.

### 6.3.6 Digital identity

In order to give smart contracts meaning in the legal world, there must be a reliable system for digital identification (of natural persons and legal entities) and authorization. At the same time, the blockchain itself can be a platform for recording and anchoring the identity and authorization of persons.



In order to guarantee reliability, it is desirable and necessary to (inextricably) link (the physical manifestation of) a person to a digital identity, and to reliably record this link and to (be able to) audit the requirements for each transaction. This requires constant matching between (the physical manifestation of) a person and their digital identity. Among other methods, this can be achieved by enriching a person's digital identity with their biometric data, or to use their biometric data when obtaining access to digital systems.

Many countries currently do not have such a digital identity. The current identification and authorization methods for digital systems are limited to entering and checking digital proof of access without constant state-of-the-art links to (the physical manifestation of) the person who holds the digital proof of access. This makes it impossible to determine if the holder of the digital proof of access is the person to whom this proof has been issued, or if the holder of the digital proof of access is actually the person authorized to view or influence the data in a smart contract.

# 07

## *Identity (SSID)*

*Giulietta Marani,  
Steven Gort and  
André de Kok* <sup>86</sup>

<sup>86</sup> Steven Gort works for ICTU, a not-for-profit foundation within the Dutch Government. As the assigned “data whisperer” he is one of the driving forces behind Discipl, an information platform for a future digital society in a resource based economy. Giulietta Marani works as advisor and account manager at ICTU. Her main areas of expertise are innovation, new technologies, security and organization’s learning ability. She is part of the Discipl team. André de Kok works as an architect working at the National Office of Identity of the Netherlands ministry of Interior and Kingdom Relations.

Over the past decades, the rate of development in the field of identity management has increased. Governments have realized that identity management is crucial to their operations and that a reliable identity infrastructure is a necessary precondition for a successful implementation of identity management. But changes, especially in the digital domain, happen so fast that further development and improvement of the identity infrastructure is a constant topic of attention and sometimes of concern to governments.

The number of countries that issue electronic passports and electronic identity cards and that also offer electronic services to citizens is growing rapidly. The questions that arise here are: what is the impact of these developments on identification and ID verification, on the documents and tokens, on the application and issuance processes, on document control, on the instruments to be used and on their interoperability?

The concept of identification will evolve towards a relative, quantitative and dynamic definition of identification relying on evidence of identity. An International Identity Management Organization will be created to harmonize and coordinate ID management at a global level. In each country, a National Civil Registration Authority will develop efficient and trusted ID management services based on Unique Personal Numbers. A global identity chain will grow from trusted ID information and not from the illustrated information of breeder documents. Quality and integrity will only be achieved in the identity chain by collaboration and cooperation. The enforcement of data protection and privacy regulations will be crucial in increasing trust regarding ID management. A set of minimum common criteria needs to be defined to achieve



a general acceptance of biometric technology in ID management. Tokens will be multi-purpose and cost-effective and integrated in widely accessible objects, and finally, a new balance between efficiency and flexibility for digital ID management will be discussed at the political level.

By 2030, roles and mandates regarding ID management will have been clarified. In 2030, the NCRAs will be in charge of, and responsible for, the ID management policy,

the implementation of digital infrastructures supporting ID management processes compliant with recommended practices and making trusted ID management services available digitally to users, public and international organizations, and private partners at a national level. The NCRAs focus in particular on the following tasks: the enrolment of individuals, the management of the identities including the integrity of the personal and biometric data, the security and logistics of the tokens (issuance, control and destruction), the ID control and terminating the identities. The NCRAs fully exercise their national sovereignty in fulfilling these prerogatives, but the challenge consists of fulfilling them in line with international recommendations, specifications and standards of the IIMO.

The IIMO guarantees the availability of a trusted digital ID infrastructure at an international level, ensuring the scalability, the interoperability and the integrity of ID management processes (enrolment, control and end), of the tokens, and of the personal and biometric data used. These requirements of scalability, interoperability and integrity are necessary for the IIMO to fulfil its role of

international coordinator, managing the international requests of the NCRAs, and of all the other public or international organizations and private partners operating digital infrastructures and managing ID processes. These organizations are active, inter alia, in the fields of migration (e.g. the International Organization for Migration – IOM), of transportation (e.g. the International Civil Aviation Organization – ICAO and the airline companies), of tourism (e.g. the United Nations World Tourism Organization), of law enforcement (e.g. Interpol) and more generally in the fields of international trading and business (e.g. import-export companies, credit card issuance companies and other financial institutions).

Before the creation of the IIMO and due to its leading role in the field of international civil air transportation, the ICAO was historically de facto in a central position by providing guidance, standardization and coordination at a global level in the field of ID management. The creation of the IIMO has created the opportunity for the ICAO to refocus on its core business regarding ID management. In 2030, the ICAO will concentrate on guidance, standardization and coordination in the field of air transportation in order to mitigate the risks linked to ID management activities in this field. More generally, the international bodies involved in ID management operate similarly, concentrating on their area of activity and interacting with the IIMO for guidance and coordination of the ID management between areas of activity.

In 2030, there will be a balance between privacy and trust. In 2030, technology-driven data protection and privacy regulations will be in place all around the world. Their enforcement increases the trust of citizens and users regarding the organizations managing ID processes.

*“ In 2030, technology-driven data protection and privacy regulations will be in place all around the world. ”*

The regulation focuses particularly on the ownership, collection, custody and processing of the personal and biometric data. At national, regional and global levels, mechanisms are in place to foster swift legislation to oversee and, if necessary, address through legal means, the rapid and sometimes undesirable developments in ID technology and ID management. In 2030, the IIMO will have set up an accreditation system as a quality management tool to accredit the public, private, national and international organizations operating digital ID infrastructures and managing ID processes. The aim is to certify the competence of their staff, to assess the compliance of their data, technology and processes with the regulations and to assess the validity, reliability, neutrality and the impartiality of the collection, custody and processing of personal and biometric data. Concretely, these quality management activities are organized and supervised jointly by the NCRAs and by the National Accreditation Bodies (NABs). These are performed nationally for national organizations and regionally for international organizations. The international Standardization Organization (ISO) and the IIMO are also involved, providing the framework of standards and specifications necessary for quality management.

### 7.1 SELF SOVEREIGN IDENTITY & BLOCKCHAIN

Humanity's notion of trust is shaped by new platforms operating in the emerging sharing economy, acting as intermediate matchmakers for ride sharing, housing facilities or freelance labor, thus effectively creating an environment where strangers trust each other. While millions of people around the world rely on online sharing activities, such services are often facilitated by a few

predatory companies that manage trust relations. This centralization of responsibility raises questions about ethical and political issues, such as regulatory compliance, data portability and monopolistic behavior. Recently, blockchain technology has gathered a significant amount of support and adoption due to its inherent decentralized and tamper-proof structure. In *Laws for Creating Trust in the Blockchain Age*,<sup>87</sup> Delft University of Technology & The National Office for Identity Data present a blockchain-powered blueprint for a shared and public programmable economy. This architecture's focus lies on four essential primitives: digital identities, blockchain-based trust, programmable money and marketplaces. Trust is established using only historical interactions between strangers to estimate trustworthiness. Every component of the proposed technology stack is designed in accordance with the defining principles of the Internet itself: self-governance, autonomy and shared ownership. Real-world viability of each component is demonstrated with a functional prototype or running code. The vision is that the highlighted technology stack devises trust, new acts, principles and rules beyond the possibilities in current economic, legal and political systems.

For the purpose of this book, we will give two examples worth mentioning in this field:

In January of this year, Sovrin delivered a thorough paper from over 20 contributors describing the state of the art for self-sovereign identity.

In February of this year, a Proof of Concept for a Blockchain-based Self-Sovereign Identity has been published by the Delft University of Technology.<sup>88</sup> The system allows users to make claims about their identity, get an attestation

<sup>87</sup> <https://www.degruyter.com/view/j/eplj.2017.6.issue-3/eplj-2017-0022/eplj-2017-0022.xml>

<sup>88</sup> <https://tools.ietf.org/html/draft-pouwelse-trustchain-01>

*“The issues of digital identity are so diverse and complex in nature, however, that they require new approaches.”*

for these claims from an authority (the government, for example), and then use their attested claims to prove they are allowed to use a service offered by a provider. The system makes use of blockchain technology to publish the attestations made by authorities. An authority publishes the public parameters of a zero-knowledge proof (ZKP) and the key of the claim it is attesting. By publishing this on the blockchain, the authority acknowledges that the user has the claimed attribute, after which the user can prove the ZKP to a provider, which verifies the proof with the information on the blockchain.

Both examples illustrate the ground-breaking work being done in this field. The issues of digital identity are so diverse and complex in nature, however, that they require new approaches. Combining operational issues, organizational issues, public values, partnerships, different target audiences and legal issues cannot be done from behind a desk. That is why the Dutch Ministry of the Interior and Kingdom Relations (BZK) and the National Service for Identity Data (RvIG) came up with the idea of starting a policy lab. The policy lab's approach assumes that complex social issues will often be different in practice than in theory, meaning the best possible approach is to focus on the target group experience while working alongside various government bodies. That is the core of the policy lab: defining problems, coming up with solutions and testing them, and doing so in collaboration with stakeholders. In the lab, BZK/RvIG want to work with a number of testable identity concepts in the shape of MVPs/prototypes based on the aforementioned examples of technologies that can be used in a focus group or expert session.

In 2030, there will be a balance between control and facilitation. By 2030, substantial experience of managing ID processes will have been accumulated by the NCRA's and all the other public or international organizations and private partners operating digital ID infrastructures. The information related to the traceability of events and to decisions that have been made are of particular interest in establishing a balance between control and facilitation in operation, knowing why, when, who and what needs to be checked (and what should not be checked). This information is used to monitor the mobility of people and their access to services and benefits, with the aim of improving and streamlining the service, but also to detect threats linked to irregular immigration, public health or security. This information also helps to determine if and for whom checks can be anticipated and performed remotely. For example, border preclearance processes are intended to streamline border procedures on the spot. After all, a traveler's health and travel history, financial records, criminal record (or absence thereof) and even the content of their luggage are potentially informative of their intentions.



# 08

## *Data, information & citizen control*

*Paul Oude  
Luttighuis en  
Steven Gort* <sup>89</sup>

<sup>89</sup> Paul Oude Luttighuis works for Le Blanc Advies as an advisor architect for various clients in various fields. Steven Gort works for ICTU, a not-for-profit foundation within the Dutch Government. As the assigned “data whisperer” he is one of the driving forces behind Discipl, an information platform for a future digital society in a resource based economy.

### 8.1 INTRODUCTION

#### 8.1.1 Cause

In order to act, a government is highly dependent on information. In turn, the government appears to citizens and businesses in the shape of information. That is why the government’s information landscape requires constant care and continued development.

Current developments of distributed technologies like blockchain technology give new importance to a vision on how the information landscape is arranged. New importance, because the traditional registration and administration of data at the government that was formed in accordance with purpose limitation based on legal tasks do not and cannot relate to the current access to and flow of information, for which both citizens and businesses need to be able to enter into a dialogue with the government within the intention(s) of both legislation and regulations. Or, indeed, for which both citizens and businesses are put in control by that same government! That is why we are introducing purpose limitation by design, or: dimensioning.

### 8.2 CONTEXT

#### 8.2.1 Trends

##### *8.2.1.1 Digitization*

Society is digitizing. In a vibrant game of adulation and disillusionment, trendy information technologies are passing us by. However, under the surface of this dynamic there is a significant change that is more tied to computer information than technology. Much like the industrial technology a century ago reminded us that humans



and society, too, worked like gears fitting together, the idea that information is what the computer makes of it slowly takes root: something digital, a fragment that can be moved, stored and processed en masse and rapidly at almost no cost. Thinking digitally is no longer viewed as just a tool for people, and it hasn't been for a while; it is about to be viewed as the standard for people's lives and society.

#### *8.2.1.2 Data drift*

Because of the fact that information has always been the living tissue that kept society and cooperation together, it must have far-reaching consequences. Especially for the public embodiment of a society: the government. Data that historically was held by the government for executing actions is drifting; it is on its way to being reused in unanticipated contexts. Two forces are pulling at this data in opposite directions. One wants to reuse the data for the administrative, decision-making and executive branch of the law (for instance, a home address as the basis for the composition of the household). The other wants to reuse the data for the production of private value (for instance, the same home address for discount through the organizer regarding noise pollution of an event just around the corner). In some places, these forces are blending and causes the line between public and private to shift or fade.

#### *8.2.1.3 Daily experience*

In the interplay of forces between legal and private reusing forces, citizens are only limitedly capable of ensuring that all this data still reflects their daily experience, because it is so charged with formal and/or commercial ulterior motives. For a government that wishes to include all its

citizens and wants all its citizens to be included this is an additional worry that transcends its formal charge of executing laws.

Everyday life is so much more than the digital dimension, as long as we are willing to acknowledge this. This does not mean that information technology does not have its place; far from it. But if information technology wants to acknowledge everyday life, then it will have to change its tone.

### **8.2.2 Opportunities**

This same data drift can just as well allow for a host of new ways of cooperating, if it is guided properly.

#### *8.2.2.1 Reuse*

Reusing data formally – between legislation and execution – can help the government become smarter, or get clearer ideas, make better judgements and make better decisions. What passes for “better” and for truth must continue to be formulated by democratic forces. Logic and statistics (in the context of this book, this primarily concerns smart contracts combined with blockchain) should be no more than a tool, never a replacement. This form of reusing data is also preferably tailored to the situation of the citizens and businesses and not just to the formality of a law, no matter how unavoidable it is. A government solidifies its connection with society wherever this is possible.

Reusing data functionally – between supply and demand – can help the government add social value by means of servitude to citizens and businesses. What passes for value does need to be formulated by democratic forces. Money or other quantitative measures can play a part in this, but can never replace value. Moreover, a condition for this

form of reusing data is that it is accessible and tailored to the situation of the party involved, not just tailored to efficiency. A government solidifies its connection with society wherever this is possible. Functional reuse of data can also be placed in private hands for a major part; after all, revenue models form wherever value is added.

No matter for which of these two approaches data is reused, dimensioning is the key to the quality of reusing. Both methods differ fundamentally in what drives them: law and truth, versus importance and value. These two forces will only meet each other based on situation specific conditions. On larger scales, further removed from social reality, they are a risky combination, though.

#### 8.2.2.2 Innovation

Innovations in the data landscape can also be an important impulse for legal, organizational and technical innovation. Because the government, like society, is permeated with information, information itself is a driving force for change in legal, organizational and technical terms. Taking information to be a belonging that can be contained with a combination of legal, organizational and technical measures is a risky misconception.

That is why this vision is a vision of information, of data, above all. Insofar as legislation, organization and technology are included, the question is how they relate to information. Not how information relates to legislation, organization and technology. Moreover, this vision will not wait for legal, organizational or technical innovation and will not propose it. It will trust that proper handling of information will cause these changes automatically wherever and whenever they are required.

In cases where coherence with regard to information technology temporarily or permanently reaches across organizational borders, the tactical implementation of the information landscape will first be decided by means of information technology agreements between these parties before it will result in a technological solution, if any.

#### 8.2.3 Challenges

Anyone looking to guide these changes properly faces at least three challenges: semantic confusion, complexity and alienation.

##### 8.2.3.1 Semantic confusion

Firstly, the topic is plagued by semantic confusion. This vision will also not define what data is and will at the same time also use the related term information. It will also talk about information as if it were synonymous with language. The semantic confusion is understandable; it also exposes differences in perspective.

Procedural behavior views information as logistics objects that can be collected, distributed, stored and edited at will. The meaning of such information is whatever it is considered to indicate. Many technologists share this view, as do many business experts. A lot of legislation, including parts of the GDPR share this classic logistics view. Nevertheless, in doing so it fails to account for the ways in which and for which purposes, both intentionally and unintentionally, data is used. And it is missing the tools to properly guide this usage.

Rational behavior adds something to the procedural view: a specific type of information use, and thus a specific type of idea of what data is. It attaches truth, or untruth, to data. Data is viewed as a fact from which you can draw

*“ Taking information to be a belonging that can be contained with a combination of legal, organizational and technical measures is a risky misconception. ”*

conclusions. The meaning of such information is whatever it is deemed to claim. The aforementioned form of reusing data applies this view. Logic and statistics use data in this way.

Functional behavior uses data in an entirely different way: as value. Data is viewed as a product for which a party can have a need, on which a party depends to a certain degree. The meaning of such information is whatever it is deemed to satisfy. The aforementioned functional form of reusing data applies this view. Economics and business administration often take this view.

Facts and products are two valid ways to use data that are incompatible. When facts are treated as products, the truth becomes subject to needs, as is the case with fake news. When products are treated as facts, value becomes subject to constraint logic, as is the case with filter bubbles.

A fourth view of data transcends this contrast by viewing data as expressions of language in a dialogue that have different interpretations in specific situations. The meaning of such information is whatever it is deemed to intend. This view is the most powerful and natural view that approaches the human daily experience better than any of the other three. We will call this view intentional hereinafter.

#### *8.2.3.2 Complexity*

Semantic confusion contributes significantly to the complexity of implementation issues in the data landscape. But even if that confusion were solved, there still is a large amount of inherent complexity left. The complexity of the data landscape cannot be smaller than the complexity of the government's task. And this, unlike private domains,

takes place at a social scale.

At this scale, the differences between data are as important as the similarities. For implementation issues regarding standardization and centralization versus variation and decentralization, it concerns a deliberation between the weight of the similarity versus the weight of the difference. One size fits none, no matter how often differences are unnecessary. Cohesion and mutual understanding (interoperability) also do not primarily depend on standardization, but on joint insight into both similarity and differences. More effective and safer standardization is possible in any case where the actual differences are clear.

The fact that the data landscape is at odds with organizational, legal and technological divides does not make things any easier. In the trade-off between differences and similarities, information content and information use should play a leading role. Organizational, legal and technological parceling preferably play a secondary role. An argument for the (re)valuation of differences is explicitly not an argument for the continuation of existing discord. On the contrary, it is an even more powerful argument for a revised arrangement, much more powerful than a unilateral appeal for centralization or standardization could ever be.

Three measures – (1) unravelling the semantic confusion regarding data, (2) weighing the differences and similarities, and (3) letting information content take prevalence over organizational, legal and technological parceling – can combat the unnecessary complication of the data landscape and contain the inevitable complexity. This alone will result in an adequate control of the transparency, openness and quality of the data landscape.



#### 8.2.3.3 Alienation

Rational and functional reuse of data is of vital importance, but also a source of risks. The widespread “networking” of facts to form judgements can obfuscate the truth and alienate it from the daily lives of citizens. The large-scale exchange of data to serve a wide range of needs can obfuscate the value of that data and alienate it from the daily lives of citizens. As stated, combining these two forms of reusing data creates additional risks.

These risks require a guarantee that the intentions with which the data has been created or collected fit the intentions for which that data is used. This purpose limitation differs from how purpose limitation was originally viewed in at least two ways. Firstly, the purpose here is not synonymous with a task domain or legal domain, but is viewed in a more intricate and nuanced way. Secondly, purpose limitation is not viewed as a legal concept that limits implementations, but as a quality aspect of implementation and design itself that stretches beyond privacy alone.

You could call it purpose limitation by design, or dimensioning. A general guideline for this could be that data is meaningless outside of the purpose for which it formed. Data cannot be used outside of its context. So, the question is not: Is reusing data allowed or not?, it is: How do we design these connections?

Eventually, a data landscape will prove itself when it is confronted with the daily lives of citizens and businesses in their specific situations. This confrontation will prove the data to be cohesive and clear (or not). And whether the data respects both citizens and businesses. Proper

dimensioning, (rational) transparency and (functional) accessibility are key. A meaningful flow of information for citizens and businesses would be an illusion without them.

## 8.3 VISION

### 8.3.1 Why create a new model?

This vision will put forward a new model, a new way of arranging government data. Because numerous models and architectures are already available, there need to be good reasons for yet another model. The burden of proof lies with the “new kid on the block”, even if the established views have already shown their limitations.

#### 8.3.1.1 Information emancipation

First of all, none of these existing models take information itself as the starting point; instead

- they project a technological, organizational or legal arrangement onto a problem that cannot directly handle it;
- or they are, usually unintentionally, limited to one of the first three perspectives (procedural, rational, functional) and thus not only forget about an intrinsic part of the government, but also lose track of the daily lives of citizens and businesses.

#### 8.3.1.2 Use and intention

Existing models often separate information (objects, facts, products) from its use, and firstly focus on the information “itself” instead of on its use. But the essence of information is how it is used. The meaning of specific information is the answer to the question: What could or must it be used for? Without looking at use, information means absolutely nothing, which means it is no longer information.

Purpose limitation boils down to the question: Does the use of information fit the intentions with which the information was created? This applies to all information, not just personal information. Existing models barely offer any direction for tailoring new-style purpose limitation on the actual dimensions of the information's use. Thus, the purpose limitation discourse is stuck in a debate regarding the technical possibilities and legal limitations, stuck between the accelerator and the brake. The "drives" of the driver are not deemed important.

Purpose limitation is not primarily a legal matter; it is an information principle. This principle is subsequently reflected in legal, organizational and technological arrangements. A technological force that categorically ignores this invokes a legal counterforce; a technological force that embraces it could make a lot more progress. And better progress.

### 8.3.2 The information tetralogy

The model in this vision consists of four fields, each corresponds to the four perspectives of information mentioned earlier in this publication: ritual (objects), rational (facts), functional (products) and intentional (expressions). But as such they are also four materially different forms of:

- information use, leading to different types of purpose limitation;
- information processes;
- information control, and thus citizens' control over information;
- information quality;
- information rights and duties;
- information technologies and architectures.

*“Purpose limitation is not primarily a legal matter; it is an information principle.”*

The four fields are organized in a two by two table (Figure 1). In a government context, the vertical fields can be considered to be ranging from legislation (top) to execution (bottom), the horizontal fields can be viewed as ranging from demand (right) to offer (left).

It is important to note that the four areas are not depicted as separate blocks. They link up with each other in a way we will discuss later.

Both axes are equally important. The horizontal axis is about how the government meets the social demands of citizens and businesses. The vertical axis is about how the government meets the social justification for citizens and businesses. Both axes touch the core of the government's *raison d'être*. Letting one dimension be ruled by the other is tampering with the foundations of the government's data landscape. Both dimensions will need to be attended to in a cohesive and balanced way.

This also applies to each of the four fields individually. They all occur within the government, they have to. There are differences in effectiveness and efficiency between the fields, but none of them is the best or the worst. It is not a matter of choice, but (firstly) of properly separating them and (secondly) correctly choosing and connecting them.

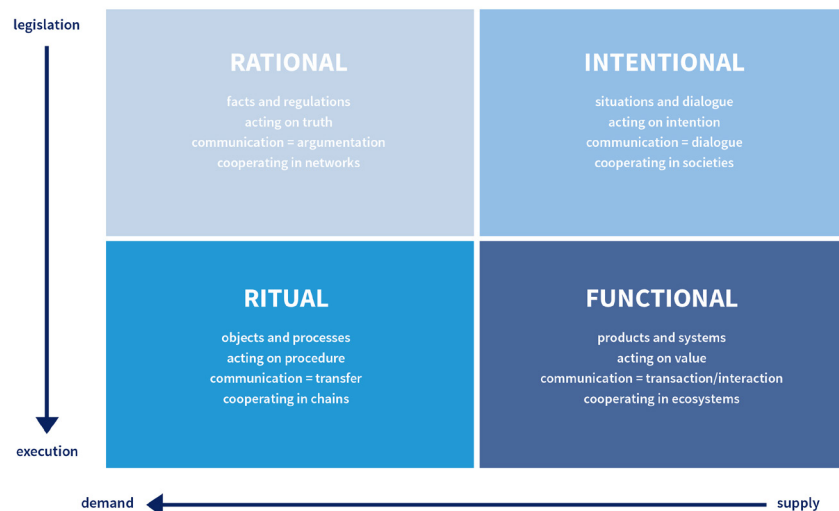


Figure 1 –  
The information tetralogy

### 8.3.3 Performance and relationships

#### 8.3.3.1 Efficiency and effectiveness

The four fields each perform differently in terms of effectiveness and efficiency of information. Effectiveness is distinguished in terms of cohesion and flexibility. Cohesion is the extent to which information and the corresponding actions and means can be mutually combined; flexibility is the extent to which it can adapt to changing situations.

Efficiency is distinguished in terms of efficiency in use and efficiency in adjustment. Efficiency not only corresponds to the use of financial means, but also to the use of energy and time. Figure 2 shows how the fields perform in terms of these indicators with respect to each other.

The intentional field is most effective; it combines a level of cohesion and flexibility the other fields cannot offer, not by themselves and not when combined with others. It is the broadest approach and the most powerful in how it deals with complexity. Moreover, it encompasses the other fields

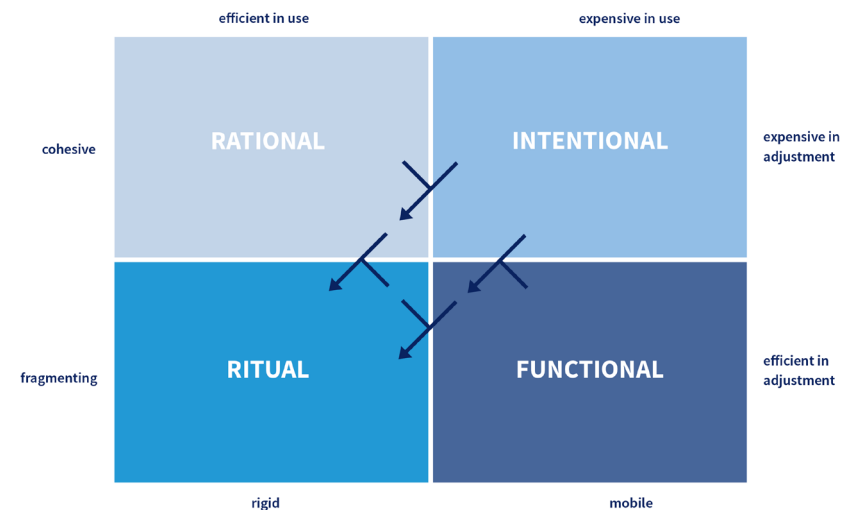


Figure 2 –  
Performance of the four fields

and allows itself to be limited to them if need be. This is not possible the other way around. However, the intentional field represents the most expensive approach in both use and adjustment. Use and adjustment are strongly linked to each other and eventually merge in the intentional field. The two are categorically separate, however, in the ritual field.

#### 8.3.3.2 The power of weakness

No matter how weak ritual thinking may be, it is the most efficient way of implementing a large-scale information system that mediates between rational forces from a legislation standpoint and functional forces stemming from social demand. It is not surprising that the government's basic registrations are based in ritual; it simply has to be like that. This quality cannot simply be sacrificed to rational or functional forces. The ritual field deserves its place amidst the other three, or better yet: within the other three.



Take the trade register that registers notarial deeds, for instance. If a notary were to make an error in representing the truth when drawing up a deed, then this is also included in the register. Within the ritual process this is not an error, however. If the registration procedure has been followed correctly, then the registration is correct. Deed well done. That data can be viewed as an error is not the fault of the register, but of an assessment process that wants to use this information. This assessment always uses a specific view of the truth and cannot be entrusted to the ritual field. It belongs to the rational field that can fully reuse the ritual data (objects), but which has to promote this data to facts itself in light of a specific view of the truth.

Such a consideration is required if the administrator of the trade register wants to provide custom information products to businesses. This projects a specific need on the data from the trade register. Responsibility for this projection lies in the functional field. Promotion of a ritual information object to a functional information product can only be a functional task.

**8.4 CONSEQUENCES**

In the above, we are making an argument for seeing information itself as the key for the implementation of the data landscape of the government. The division into four fields is a principled ordering of information that evades attempts to control information through legislation, governance or technology. In fact, this division into four fields, with information as a starting place, stretches across legislation, organization and technology. Not the other way around; that is not possible.

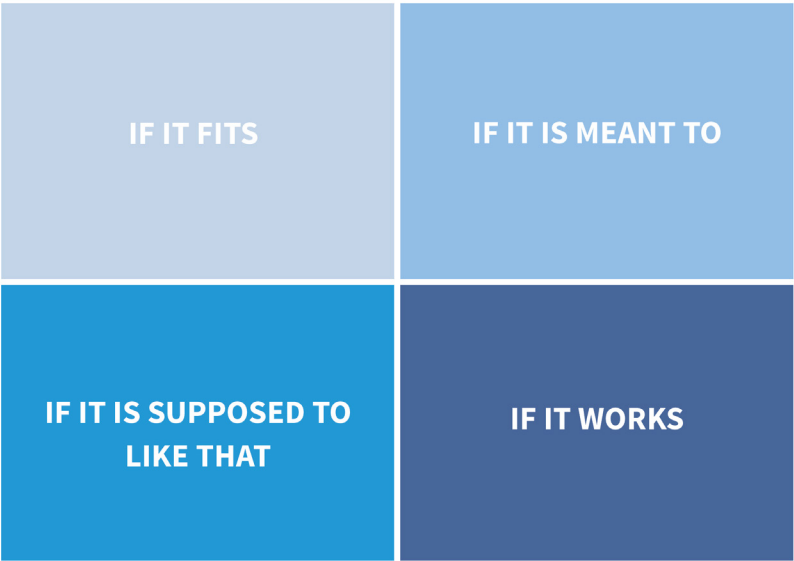
**8.4.1 Organizational consequences**

There are numerous organizational consequences. The division into four fields also applies to the character of the government’s implementation and the patterns in the corresponding policy. The four fields are also operational fields that require a different approach, management, expertise and even culture.

*8.4.1.1 Data management*

A more concrete example of an organizational consequence is caring for the data itself: data management. This understanding of quality of information itself differs between the four fields as shown in the following figure.

*Figure 3 –  
Quality of information*



*“ The administration federation share, among other things, the meaning and purpose of the data with each other; the custodian federation share details about structure and access with each other. ”*

This difference in the interpretation of quality also causes different implementations of governance in the data landscape. The discussion about this is often held in terms of centralized and decentralized approaches. However, this means a proper solution is unattainable. After all, the decentralized part needs to prove itself to the centralized part because it is a denial of that part. Moreover, the fact that a decentralized governance is still responsible for connecting with the other players in the governance to guarantee cohesion in the full data landscape is conveniently left out.

The cause of this unfortunate discussion is that it starts with centralization. Without it, the decentralized alternative cannot even be considered. Fitting governance of a data landscape is always federated. It is executed by players that at the same time have their own mandates and have mutual responsibilities. They are more estate managers than the owners of information. Centralized governance is not in conflict with this at all, it is only an extreme form of it. Centralized governance is a coarse federation. The other end of this spectrum is a highly distributed federation.

#### 8.4.1.2 Data atlas

Every data federation that is even slightly distributed requires that all parties involved can inform each other of the data they are responsible for as administrators or custodians, but that the other parties in the federation need to or can use. The administration federation share, among other things, the meaning and purpose of the data with each other; the custodian federation share details about structure and access with each other.

This information on information is also important to parties outside of the federation that do not have any

administrative or custodian responsibilities, but could nevertheless use the information, including privately, or that at least would like to know what information is circulating in the data landscape. Thus, the data federation also have a responsibility for the transparency and accessibility of the data landscape.

Sticking with the metaphor of a data landscape, a jointly organized data atlas could provide support. Such a data atlas is purposefully positioned as a support facility for a data facility; an organizational tool, in other words. Demand for such a tool will depend on the extent to which and on the way in which the data federation functions.

Figure 4 – Data atlas



In any case, the data atlas takes a different shape depending on the field in which it is used. This also means that the technology used for a data atlas, and the way in which it is managed, need to be tailored to the field in question. The rational part of the data atlas primarily

contributes to the transparency of the data landscape; the functional part contributes to the accessibility thereof. The four fields also each have their own use and target group. Anyone working on the implementation of legislation will take a top to bottom approach through the atlas, whereas anyone working on the application of open data will move from the functional field to the ritual field, for example.

8.4.1.3 Citizens' control

Because local and international developments explicitly entail some form of control for citizens over their own information, we also want to show that there is a range of different forms of this citizen control, represented in the four fields of the information tetralogy reflecting a wide-ranging view of what this individual citizen actually is or can be.

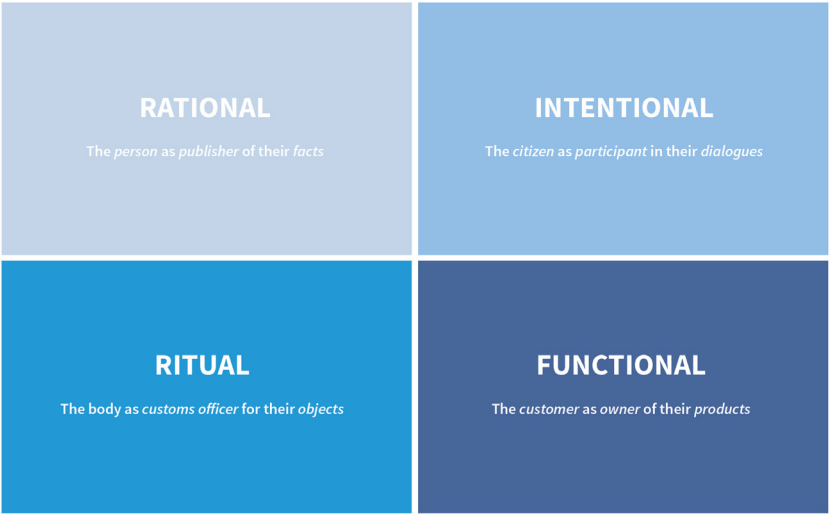


Figure 5 –  
Citizens' control over  
information

In the ritual field, the individual citizen only takes the role of a customs officer, who is permitted to know that their objects are being moved from one process to the other process, and who may be permitted to stop this flow. Cohesion and change of this data are outside of their field of vision or control. One example is the permission a patient needs to give for healthcare providers to share the citizen's medical data with each other.

This is different in the rational field where a citizen becomes a person who has the right to get their facts from certain sources and share them with their readers. This is comparable to the role of the free press in a society, but at an individual level. One example of this is MedMij, a project of the Dutch Ministry of Healthcare that intends to enable citizens to manage their own health data. Here, citizens have control over the cohesion of the information, but not over any changes.

True ownership in an economic sense offers the citizen – now acting as a customer – the option of turning their data into transactions as a medium of exchange. This is already the case in the private domain, even though it largely occurs implicitly. An example of a service that wants to give citizens the opportunity to manage their information as a product is DataIsMe. Here, citizens are given control over changes to information, but not over the cohesion of the information.

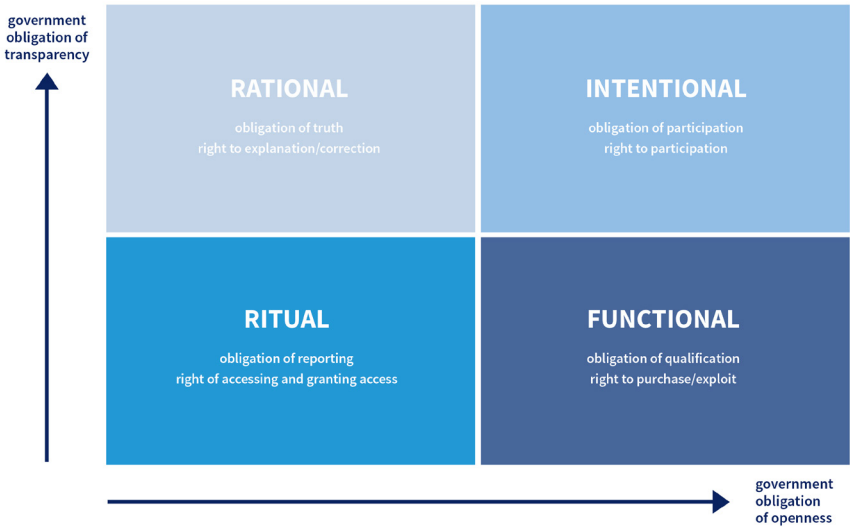
For an example of intentional control, we do not have to come up with innovative concepts: our own democratic elections are the clearest example of this. As a participant in society – a full-fledged citizen – a voter decides on the content of his or her own vote.

For the application of blockchain, it should be clear that it is very relevant to acknowledge these different roles (customer journeys, if you will) as soon as this technology is used to permit and/or (help) facilitate citizens' control over their own information!

8.4.1.4 Information rights and obligations

Rights and obligations also fully apply for any form of citizen control over information. Some of these rights are also part of the GDPR. A problematic aspect is that the GDPR, along with the lion's share of legislation and regulations regarding information, primarily uses ritual idioms. The question remains whether this also means that the non-ritual rights and obligations intended by that same legislation can be established properly. An example of this is the right to data portability established by the GDPR. This is a ritual phrasing of meaningful communication, while ritual thinking actually fails in giving meaning and purpose to information, because it only does so through indication.

Figure 6 – Information rights and obligations



8.4.1.5 New-style purpose limitation

In paragraph 8.2.3.3, we already stated that purpose limitation is an information technology principle first, and a legal principle second. Nevertheless, we will discuss it again here under the legal consequences.

In its role as an information technology principle, purpose limitation belongs in the design of the data landscape even before it is a matter of justifying reuse. This can be achieved by attaching context to the information. This context is also information like any other information and describes the context in which that information formed. This context is both spatial and historical in nature. If, for example, a specific piece of data is collected in the context of a specific request, then this request is part of the context including the moment in which it occurred.

Subsequently, using information without its context should be discouraged; in other words, it must not be taken out of context. This can be achieved in multiple ways. If the information is copied, then this is possibly by also copying (a reference to) the context and requiring that the context limits the reuse of that information in the design of the data use. An even more fundamental approach would be to not simply copy the information, but to use compatibility with the context as an access requirement.

For personal information, this could be combined with a form of citizen control (paragraph 8.4.1.3). For example, if a citizen is granted control over their own data via the rational model (as a publisher), then a party that wants to access that data could be obliged to first commit to the context in which it formed.

*“... if a citizen is granted control over their own data via the rational model (as a publisher), then a party that wants to access that data could be obliged to first commit to the context in which it formed.”*

Although they do so coarsely, the four fields themselves already delineate intended purposes of data. Information can be reused ritually, rationally (for an assessment), functionally (for interests), and intentionally (for a purpose).

Finally, it is not relevant for this description whether it involves personal information or otherwise. All information is given meaning from its context. The fact that purpose limitation is for now mostly associated with privacy is more due to the special rights people enjoy than it is due to information technology considerations.

# 09

## *Blockchain and Land Administration* <sup>90, 91</sup>

*Baloko Makala and Aanchal Anand* <sup>92</sup>

<sup>90</sup> This Chapter is published under Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO)

<sup>91</sup> The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent. The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work ▶

### 9.1 BACKGROUND ON BLOCKCHAIN TECHNOLOGY

Blockchain is the technology that powers the much-talked about cryptocurrency, Bitcoin. However, Bitcoin is just one application of the blockchain. Blockchain is essentially a “chain of blocks,” where each block represents a set of records. Each such record could, in turn, represent a cryptocurrency, a land plot, a diamond, or even an identity. In this sense, if the traditional Internet is an Internet of information, blockchain is considered the “Internet of value.” Therefore, the technology has the potential to revolutionize the way value is stored and exchanged.

The technology has been evolving for the most part unregulated as lawmakers and regulators are yet to fully understand the cryptocurrency phenomenon on the one hand and on the other hand, they are being called upon to review current regulations to integrate blockchain technology and protect consumers against fraud. Even though there are doubts about the viability of cryptocurrencies, the unanimous opinion is that the underlying technology Blockchain will revolutionize the way value is stored and transferred. Therefore, this chapter does not focus on cryptocurrencies and looks instead at the wider usability and applicability of blockchain in international development.

Notable papers and articles have been published by academics and legal practitioners to explain blockchain technology in terms that can be understood by non-technology experts. International Development Organizations such as The World Bank Group through its Technology and Innovation Lab and other UN organizations are also working on unpacking and analyzing the various concepts behind the blockchain ecosystem to derive

< do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.)

<sup>92</sup> Baloko Makala is the Policy and Legal stream Lead at the World Bank Group Technology and Innovation lab. Aanchal Anand is a Land Administration Specialist in the Global Land and Geospatial Unit of the World Bank.)

relevant questions as blockchain is being considered for solving development challenges. New terminologies such as “consensus mechanisms” or “smart contracts” are making their way into our everyday vocabulary. Such novel concepts need a legal interpretation and assessment of their potential impact in a real-world situation. The following is an attempt to explain how blockchain technology works and the key components relevant to the field of international development with specific focus on land administration.

## 9.2 HOW DOES BLOCKCHAIN TECHNOLOGY WORK

Blockchain technology is an instance of a Distributed Ledger Technology (DLT). DLTs fall into two broad categories: permissionless (open DLTs) such as Ethereum or the Bitcoin blockchain, or permissioned (closed DLTs) that tend to exist between entities that know each other such as commercial banks. Hybrids of both categories have also been developed.<sup>93</sup>

In a blockchain environment, the information is stored in a distributed fashion on computers called “nodes” by way of consensus between participating nodes. Given that blockchain is a decentralized peer to peer system with no central decision-making mechanism, a dynamic mechanism of reaching agreement known as consensus stands in lieu of a central entity of authority. Multiple types of consensus mechanisms are found, the most notable ones are *proof of work* and *proof of stake*. In proof of work, the consensus mechanism consists of solving a complex computational challenge to add a block to the blockchain and a reward is given to the first computer or “miner” capable of solving the challenge. This process is known

<sup>93</sup> Global Benchmarking Study [https://www.jbs.cam.ac.uk/fileadmin/user\\_upload/research/centres/alternative-finance/downloads/2017-09-27-ccaf-globalbchain.pdf](https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-09-27-ccaf-globalbchain.pdf) page 22

to be particularly energy intensive, to the extent that is becoming an issue of concern on a global level. This is not only due to the substantial amount of energy consumed by the process of mining and climate change implications when it is powered by dirty energy, but also because only nations with access to large and relatively cheap energy sources will be able to enjoy the economic incentive of mining.

A proof of stake model, on the other hand, uses the amount of stake a user has as a determining factor for new blocks creation. The methods the blockchain system usage of stakes can vary – from random selection of staked users, to multi-round voting, to a coin aging system. Regardless of the exact approach, users with more stake are more likely to produce new blocks.<sup>94</sup>

Virtually anything can be recorded on a blockchain. One of the key strengths of distributed ledger technology is that the technology guarantees the validity of the information once stored provided that the information encoded is correct. If any data is tampered in one of the nodes, the error will be recognized by the remaining nodes.

In a blockchain environment, two parties can transact without knowing each other and without the need of a trusted intermediary. The privacy of users is a particularly challenging to regulators in operations involving financial transactions. The principle of “know-your-customer” (KYC) goes against “privacy,” one of the key founding principles of blockchain technology.

### 9.2.1 Smart Contracts

The Technology and Innovation Lab at the World Bank developed several proofs of concept (POCs) using smart

<sup>94</sup> Blockchain Technology Overview <https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf>

contracts for land administration. These were developed using the Ethereum blockchain and solidity as the coding language.<sup>95</sup> The following are some of the preliminary observations:

Smart contracts are auto-executing programs encoded on a blockchain that are triggered once predefined requirements or conditions are met. They are comparatively low on memory as they are replicable over multiple nodes. Security is a key consideration when developing smart contracts. Furthermore, the signing mechanism is guaranteed by a combination of public keys and private keys. Should a user lose the private key or make it public, she/he may not be able to recover the key or render his assets on the blockchain vulnerable to theft or permanent loss.<sup>96</sup>

Smart contracts are deterministic in the sense that when provided with specific input and specific start value, the outcome remains predictable.<sup>97</sup> Therefore, smart contracts are not “smart” and cannot perform any intelligent action such as the performance of any contract or legal act. It is important to mention that the blockchain cannot access information beyond the confines of its own environment. If the data source is corrupt, the blockchain does not have any mechanism to correct it or ascertain the reliability of the data source. Once the code has been deployed on a blockchain, it can no longer be changed unless the code contains functions allowing it to be changed or by way of a correcting transaction or by encouraging the other participants in a blockchain network to initiate a “hard-fork” or a split into two blockchains.

Smart contracts can also be used as a source of storage of value while waiting for the terms of a contract to be fulfilled.<sup>98</sup>

Smart contracts are not fool-proof and the code itself is subject to human error that can lead to dire consequences and loss of substantial financial value. Nevertheless, when properly designed, smart contracts have the potential to remove the inefficiencies and weaknesses found in real world systems

### 9.3 BLOCKCHAIN AND LAND ADMINISTRATION

The following sections are devoted to blockchain and land administration,<sup>99</sup> an area that has attracted attention from blockchain developers and international development experts alike. Therefore, these sections aim to demonstrate the opportunities and challenges associated with blockchain technology in a field that has a significant impact on governance.

In order to better understand the blockchain’s applicability to land, the following features should be kept in mind. What makes blockchain unique is that it is a decentralized, distributed, and immutable ledger.<sup>100</sup> Its decentralized processing on several “nodes” or computers connected to the blockchain network ensures that there is no one single deciding authority validating transactions. This, in turn, means that transactions are peer-validated (on public blockchains) or validated by multiple authorized users (on private blockchains<sup>101</sup>), thereby reducing the opportunity for corruption or rent-seeking behavior by a single actor or entity. In some cases, the decentralized nature could also decrease transaction cost and possibly transaction time on public blockchains where peer-validation takes over functions of third-party intermediaries.

The distributed aspect has significant implications for

<sup>99</sup> Land administration is a broad concept that was first coined in 1993 by the United Nations Economic Commission for Europe (UNECE) and is broadly defined as the “process of determining, recording and disseminating information about ownership, value and use of land and its associated resources. These processes include the determination (sometimes called ‘adjudication’) of land rights and other attributes, surveying and describing these, their detailed documentation, and the provision of relevant information for supporting land markets.” <http://www.fao.org/in-action/herramienta-administracion-tierras/introduction/concept-land-administration/en/>

<sup>100</sup> The Internet of Value-Exchange, Deloitte Report: <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-internet-of-value-exchange.pdf>

<sup>101</sup> It is important to note that “blockchain” is not a monolith and there are different types of blockchains with different levels of access. ▶

<sup>95</sup> Mahesh Chandras Karajgi (Smart Contract Developer) interviewed Baloko Makala on 03/19/2018

<sup>96</sup> ‘I forgot My Pin: An epic tale of losing \$30,000 in bitcoin’ <https://www.wired.com/story/i-forgot-my-pin-an-epic-tale-of-losing-dollar30000-in-bitcoin/>

<sup>97</sup> Smart Contract as specific Application of Blockchain Technology <https://www.pelsrijcken.nl/media/591947/smart-contracts-eng-report.pdf>

<sup>98</sup> Blockchain Demystified [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3091218](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091218)



◀ Public blockchains are the most secure but may not allow land registries to have full control of the blockchain whereas private or hybrid blockchains are tailored to specific functions but are not as secure. This trade-off would need to be further explored through discussions with interested governments and other stakeholders.

<sup>102</sup> A gentle introduction to immutability of blockchains, Bits on Blocks, <https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains/>

<sup>103</sup> Ibid.

<sup>104</sup> The Blockchain Immutability Myth, Multichain, <https://www.multichain.com/blog/2017/05/blockchain-immutability-myth/>

<sup>105</sup> Swedish Mapping Authority Pioneering Blockchain-Based Real Estate Sales: <https://www.nasdaq.com/article/swedish-mapping-authority-pioneering-blockchain-based-real-estate-sales-cm935347>

<sup>106</sup> Blockchain Virtual GovHack video: <https://www.youtube.com/watch?v=y0WGwzKaxI>

disaster recovery as the data can be spread across different nodes. If one node is destroyed (say, in an earthquake or a flood), the data can be recovered from other nodes on the blockchain.

Perhaps, the most attractive feature of the blockchain is its immutability. Each block is connected to the previous block through an algorithm that is cryptographically secure and contains information on the previous block.<sup>102</sup> Therefore, unlike an ordinary ledger, which is organized by page numbers that are unrelated to the contents of the page, the blockchain's "blocks" contain a hash that represents the contents of the previous block. This means that it is mathematically nearly impossible to change a record in the past without disrupting the entire chain. Even if such a thing were to happen, it would not escape the notice of other nodes. At the same time, it is important to note that blockchain immutability is a relative concept,<sup>103</sup> and that collusion and "51% attacks," while prohibitively expensive and time-consuming, are possible.<sup>104</sup>

In the context of land administration, virtual authentication is the simplest application on a public blockchain. Instead of requiring a notary to certify previous ownership while transferring an asset, the public blockchain could theoretically process the virtual authentication at a lower cost due to disintermediation.

However, it appears that most land registry applications are likely to be on private blockchains, where only authorized institutions or individuals have access to the system and have pre-defined roles to clear transactions per their legally-defined function. This can be seen in the cases of the second phase of the Chromaway pilot in Sweden<sup>105</sup> and the Consensus pilot with the Dubai Land Department

<sup>106</sup> which register land titles and transactions respectively on the blockchain. While the public blockchain is more transparent and tamper-resistant, the private blockchain comes with the stamp of approval of piloting Governments that would uphold the legality of transactions on the blockchain platform. Without Government recognition, transactions are unlikely to be considered valid.

A description of how blockchain may help resolve some of the land administration challenges is presented in greater detail in the next two sections. The first one provides theoretical foundations of blockchain's uses and the second describes the land administration use cases conducted at the World Bank Group's Technology and Innovation Lab. It is important to note that these proofs of concept were developed under laboratory conditions and they have not been tested in any jurisdiction. Proofs of concept customized to fit certain jurisdictions requirements may be developed in the future.

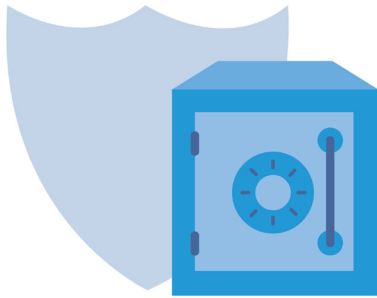
### 9.3.1 Can Blockchain Improve Land Administration?

Being a relatively new technology, blockchain's uses, advantages and challenges across different sectors, including land administration, are still being discovered and debated. This section looks at some of the biggest land administration challenges and how blockchain technology may make a difference.

#### 9.3.1.1 Corruption in the Land Sector

Corruption in the land sector can be considered "pervasive and without effective means of control."<sup>107</sup> Lack of transparency and asymmetric information allow elite capture and create opportunities for corruption. While digital systems have already improved access to information and increased transparency, blockchain

<sup>107</sup> Corruption in the Land Sector, Transparency International and FAO, 2011, [http://files.transparency.org/content/download/70/279/file/2011\\_4\\_TI\\_FAO\\_LandAndCorruption\\_EN.pdf](http://files.transparency.org/content/download/70/279/file/2011_4_TI_FAO_LandAndCorruption_EN.pdf)



may be able to offer further advantages over existing digital systems. Due to its immutable nature, once a transaction has been processed, it cannot be removed from the blockchain thus creating a tamper-proof record. Any alteration to an existing record or transaction would make the hash value or unique identification of the tampered block inconsistent with other blocks in the chain. As discussed earlier, tampering with a public blockchain will be both expensive and time-consuming, thereby creating disincentives around altering records.

Land registries, however, are expected to operate on private blockchains. These private blockchains provide more control to authorized users. More control also means that such blockchains could be more susceptible to tampering by colluding participating nodes, thereby nullifying the immutability aspect. However, a private blockchain could be designed in a way that citizens have view-access to anonymous parameters like transaction time and cost, creating an extra layer of accountability even on a public blockchain. This approach would not only afford a blockchain-based land registry the main benefits of a public blockchain—such as faster transaction verification, error correction, and greater security from external attacks<sup>108</sup>—but also create room for greater transparency and accountability by adopting elements of peer-to-peer validation through citizen engagement. This is a clear advantage over existing systems where paper and digital records can be tampered without much consequence. Therefore, if harnessed properly, blockchain has the power to boost transparency and reduce corruption in the land sector.

<sup>108</sup> How Safe Are Blockchains: It Depends, Harvard Business Review, March 7, 2017, <https://hbr.org/2017/03/how-safe-are-blockchains-it-depends>

### 9.3.1.2 Cybersecurity

It is estimated that in most countries, between 50% to 75% of a country's wealth exists in the form of land or real estate.<sup>109</sup> Land is also an important factor of production that contributes to different sectors of the economy. In addition, land can often be the only asset of the poor. Therefore, as land administration ICT systems and records are being digitized, cybersecurity becomes more and more important with respect to safeguarding people's ownership of their single most important asset. When digital systems come under attack, there is a threat that land and property records could be hacked and manipulated. Blockchain technology offers an added layer of security through its immutable nature and the advantage that records generally cannot be tampered with.<sup>110</sup> This feature of the blockchain is expected to become more prominent in land administration.

### 9.3.1.3 Disaster Recovery

Blockchain's distributed nature enables a very important application for land administration: disaster recovery of land records and information.<sup>111</sup> As of now, in the case of natural disasters and wars, servers containing land rights information need to be physically guarded to protect valuable information. While disaster recovery centers are increasingly common, they too consist of servers that face similar threats as the original databases. Blockchain's ability to distribute data across all participating nodes greatly reduces the threat of data loss. In the event of disasters, blockchain could enable data recovery and help the country and the market return to normal functionality more swiftly than with current available means. This would be critical for smooth post-disaster recovery, which can often be slow and challenging. Pilots would need to be conducted to test the robustness and feasibility of

<sup>109</sup> The Effects of Land Registration on Financial Development and Economic Growth, Frank Byamugisha, 1999.

<sup>110</sup> See earlier discussion on circumstances when public and private blockchains may be tampered with.

<sup>111</sup> Note: the reliance on physical in-country servers is also being reduced by cloud technology. One disaster recovery solution could involve marrying blockchain with cloud technologies.

blockchain-based disaster recovery.

#### 9.3.1.4 Property Rights of Women and Vulnerable Groups

Blockchain can enable “multisignature” transactions wherein more than one user’s private key is needed to complete a certain transaction. This can create significant advantages for the property rights of women and vulnerable groups. For example, women’s property rights, while guaranteed by law in most countries, are not always exercised due to strong cultural norms that favor male property ownership. In the case of marital property, women often lose out if the husband wants to sell the

property. However, requiring the wife to also sign off on a transaction through her private blockchain key would provide an added layer of security for her property rights. While “off chain” coercion is still possible, blockchain would make it nearly impossible for the transaction to progress without the wife’s knowledge. Similar applications can be thought of for the registration and protection of indigenous peoples’ lands rights wherein a multisignature transaction can safeguard community rights and ensure that fair

payments are made during any sale to all members of the community.

#### 9.3.1.5 Access to Affordable Services

Another significant challenge in the field of land administration is that roughly 70% of the world’s population does not have access to affordable land administration services<sup>112</sup> e.g. land or property registration. While the fee structures vary across countries, notarization and registration fees can often amount to several months’ income.

It is still unclear if and how blockchain may be able to bring down transaction costs. On public blockchains, the hypothesis is derived from disintermediation. If the consensus mechanism can perform the function of a third-party intermediary e.g. a notary, then the cost to the citizen is expected to decrease. It is more difficult to estimate the impact of transaction costs on private blockchains. Pilots would need to be conducted to look at the marginal cost of executing common land administration services on the blockchain. Furthermore, the fixed costs of setting up and maintaining a private blockchain-based land registry would also need to be considered.

## 9.4 LAND ADMINISTRATION USE CASES

### 9.4.1 Proof of Concept: Design

The World Bank’s Global Land and Geospatial Unit (GSULN)<sup>113</sup> and the World Bank Group Technology and Innovation Lab (TI) are collaborating on exploring use cases for land administration. This work focuses not only on the technological solutions but also looks at “off chain” issues such as governance, legal and regulatory framework, enabling conditions (e.g. data accuracy, digitized records, digital signatures), and institutional and capacity questions.

As part of this work, the GSULN and TI teams partnered to carry out a “proof of concept”<sup>114</sup> (PoC) or simulation under laboratory conditions for three use cases: (a) first registration of a parcel; (b) transfer of ownership; and (c) virtual authentication. All three cases were selected as they are some of the most common services in land administration.

<sup>113</sup> The GSULN team also received input from the Food and Agriculture Organization.

<sup>114</sup> A proof of concept is Assessing or demonstrating the viability / feasibility of trending emerging/disruptive technologies in the context of our business environment.

<sup>112</sup> Enhancing Public Sector Performance: Malaysia’s Experience with Transforming Land Administration, World Bank Group, November 2017, <http://documents.worldbank.org/curated/en/928151510547698367/pdf/121243-REVISED-World-Bank-Report-06-Land-Administration-FA-FULL-Web-V2.pdf>

The teams implemented the PoC using Microsoft Azure Blockchain-as-a-Service. A private Ethereum blockchain was chosen, which provided the teams the ability to configure the blockchain, specifically the proof-of-work consensus and transaction costs. The PoC simulated transactions between owner/possessor, buyer, private surveyor, and the land registry office. Each transaction was submitted to the transaction node, which was broadcasted to the mining nodes in a peer-to-peer fashion. When a mining node validated and confirmed a transaction, it was added to the blockchain and broadcasted to the peer-to-peer network for confirmation. Smart contracts were coded using Solidity language, which allowed the teams to implement the transactions securely. Each transaction captured the parameters of properties e.g. parcel details, status, documents on/off-chain storage and the signatures of the involved actors.

#### 9.4.1.1. First Registration of a Parcel

While parcel registration is a common service, the use case focused on the simpler first registration. This was done for simplicity as first registration (the first record of a parcel registration) does not require the existence of a parcel history on the blockchain. As the technology develops, more complex registration scenarios can be tested under the POC stage.



#### 9.4.1.2 Transfer of Ownership

Another important land administration service is the transfer of ownership where a buyer and seller come together and complete a transaction on the blockchain platform. This use case is being tested with a client country and initial results show the opportunity to use smart contracts

to reduce the time associated with the transaction while simultaneously improving transparency in the process and increasing trust between the interacting parties. The next round of POCs could include adding commercial banks (for linking mortgages) to this scenario to broaden its usability.

#### 9.4.1.3 Virtual Authentication

As discussed in Section 3, blockchain can be used for virtual authentication. In this use case, the use case explored the “notarization” of a transaction by a notary and the creation of a time-stamped record on a blockchain platform. As of now, this POC did not look at the cost of the service to the citizen though this could be studied in future POCs.

### 9.4.2 Proof of Concept: Outcomes

The POC exercise has enabled the GSULN and TI teams to better understand how blockchain technology works as well as the opportunities and challenges associated with blockchain solutions. As a result of the POC work, the teams are better equipped to ideate and create use cases beyond the three that have been developed. The teams are also investing time in understanding off-chain issues that affect the applicability, viability, and effectiveness of blockchain solutions in specific country contexts. This exercise has been helpful to better understand the enabling conditions and operational constraints. Overall, the teams have created, applied, and shared knowledge to have meaningful discussions with client countries interested in exploring blockchain technology. The teams plan to take this work forward by conducting POCs on additional use cases. Subject to the availability of funds, the next phase of POCs may also include interested client countries. Over time, the teams will start exploring the cost-benefit aspects of applying blockchain solutions.

*“ The POC exercise has enabled the GSULN and TI teams to better understand how the blockchain technology works as well as the opportunities and challenges associated with blockchain solutions. ”*

## 9.5 OTHER CONSIDERATIONS IN BLOCKCHAIN TECHNOLOGY AND LAND ADMINISTRATION

Land rights remain fundamental to poverty reduction. For example, in Africa, the productivity of the land is directly linked to poverty reduction. It leads to access to basic services such as health care and education. Land ownership implies access to shelter and basic infrastructure, employment and financial services.<sup>115</sup> While land rights are fundamental to the livelihood of people, land ownership remains nonetheless a complex process and subject to a wide range of legal agreements subject to laws at local and national levels including international treaties.

As the policy and lawmakers' community is in the process of building its capacity in addressing the inner workings of blockchain technology, many questions have started to emerge, challenging previous assertions that have been made on the benefits or drawbacks attributed to blockchain technology. Given the various ongoing pilots, it appears that blockchain may well contribute towards resolving some of the challenges that have been plaguing land administration systems. However, if deployed in the absence of a satisfactory legal and governance framework, the technology may be used to exacerbate the existing challenges. This section attempts to unpack legal and governance considerations in Blockchain and Land administration.

### 9.5.1 Applicable Legal Systems

Legal systems vary from jurisdiction to jurisdiction. Most nations follow one of the following two legal systems: Common Law or Civil Law. While legal systems in each category may share a common legal heritage, each jurisdiction has its own specificities. In blockchain-enabled

environment where systems are expected to operate across borders, the design of such system could prove to be challenging.

Given that Blockchain technology is distributed by nature and that participating nodes in the recording of a transaction may be located across multiple jurisdictions should a permission-less system be used, therefore, the major challenge is that several jurisdictions may need to be considered when addressing the legal questions surrounding the transactions being carried out over the blockchain.<sup>116</sup>

Specifically, to land administration, challenges may arise in the appropriateness of a technology characterized by immutability in areas where customary law apply in the administration of land rights. In fact, in Africa, 90% of land is held under customary tenure. Customary laws have a great impact in matters regarding marriage, inheritance and traditional authority, usually in a context characterized by patriarchy.<sup>117</sup> Indigenous peoples and other minorities have been traditionally marginalized. Women in particular have often been excluded from inheriting land from their fathers or husbands. Often, the name of the wife or daughter would not appear on the land titles. These women may find themselves further disenfranchised in a decentralized world characterized by immutability of records.

### 9.5.2 Principle of Digital Development and Ethical Design

The introduction of digital tools to solve development challenges is not novel. However, they have often been marked by failure. The digital principles for development are nine living guidelines that are designed

<sup>116</sup> Blockchain: background, challenges and legal issues <https://www.dlapiper.com/en/uk/insights/publications/2017/06/blockchain-background-challenges-legal-issues/>

<sup>117</sup> African Customary Law, Customs and Women's Rights <https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?referer=http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjBz5edmczZAhXipVkkHT8oCmlQFggnMAA&url=http%3A%2F%2Fwww.repository.law.indiana.edu%2Fcgi%2Fviewcontent.cgi%3Farticle%3D1437%26context%3Dijgls&usq=AOvVaw2se8KksARyAJalfTB6Mv&httpsredir=1&article=1437&context=ijgls>

<sup>118</sup> Principles for digital development <https://digitalprinciples.org/>

<sup>119</sup> Blockchain Ethical Framework for Social Impact – Executive Summary (Beech Center for Social Impact/ Georgetown University)

<sup>115</sup> The Impact of International Treaties on Land and Resource Rights, <http://www.ielrc.org/content/a0407.pdf>

to help integrate best practice into technology-enabled programs.<sup>118</sup> Blockchain Technology could benefit from these guidelines to avert repeating the mistakes of the past technology solutions.

Ethical design should be central to blockchain technology to ensure the best outcome for end user and particularly when these are the most vulnerable members of society such as refugees, children, the disabled and women. Important question should be asked in the process of designing a blockchain solution including the governance model, how identities are established, the authentication and verification method, data ownership and access, security.<sup>119</sup>

### 9.5.3 Data Governance

Blockchain technology as an open, permission-less system was designed so as not to rely on a centralized governance system. Participants do not need to know or trust each other in order to transact. This system was built in such way that no intermediary institutions such as government, banks etc. would be needed to verify the transactions and records automated on the blockchain through consensus and cryptographic means.<sup>120</sup>

One of the roles of land administrators is to provide opportunities for all rights holders to be explicitly recognized and be included in all legal documents as appropriate within the existing legal framework<sup>121</sup> In most countries, cadastres and land registries contain geographic and legal information regarding land and property. Contrary to other information systems, data can be created and retrieved but virtually impossible to alter without significant resources and control of computing power. As in the case of most information systems, one of

the key legal issues is data governance.

From a process standpoint, recording a land title on a blockchain raises a number of questions. The system does not consider potential “off chain” issues that may arise prior to the recording of transactions on the blockchain. Land ownership is often contested and land titles do require often correction as a result of dispute resolution or any other outcome from a judicial process. Should the wrong transaction be recorded on the blockchain, it would potentially require more resources to have it changed. This could further hurt the rights and interests of poor and marginalized communities. Therefore, countries interested in blockchain-based land registries must be mindful of addressing “off chain” aspects such as completion of records, data quality and accuracy, dispute resolution etc.

In the context of Blockchain technology and land administration, the process of recording land titles on the Blockchain may prove to be a source of exacerbation of the disenfranchised nature of minority groups because of the quasi- immutability of records on the Blockchain when compared to current recording systems, thus placing vulnerable groups at even greater risk of not being able to restore their right to land.

### 9.5.4 Pseudo anonymity vs. Identity

One of the principles of Blockchain technology is the preservation of the privacy of its actors. The data breach suffered by Equifax<sup>123</sup>, a US based-credit reporting company is often cited when debating the need to decentralize identity information and that people should be in control of their identity data and how it is shared. In the context of land administration, privacy may be an impediment to the management of land rights and it may

<sup>119</sup> Blockchain Ethical Framework for Social Impact – Executive Summary (Beeck Center for Social Impact/ Georgetown University)

<sup>120</sup> Blockchain Technology and Decentralized Governance: Is State Still necessary? [http://nzz-files-prod.s3-website-eu-west-1.amazonaws.com/files/9/3/1/blockchain+Is+the+State+Still+Necessary\\_1.18689931.pdf](http://nzz-files-prod.s3-website-eu-west-1.amazonaws.com/files/9/3/1/blockchain+Is+the+State+Still+Necessary_1.18689931.pdf)

<sup>121</sup> The Role of Land Administrator Professionals <http://www.fao.org/docrep/005/Y4308E/y4308e08.htm>

<sup>123</sup> 2017 Cybersecurity Incident & Important Consumer Information <https://www.equifaxsecurity2017.com/>



<sup>124</sup> Peter Zhou interviewed by Baloko Makala on 03/20/2018

<sup>125</sup> Blockchain and Smart Contract by Josephus Van Erp (The Maastricht University), Land Conference 2018 (03/1/2018)

<sup>126</sup> ITSO/TC 307 Blockchain and Distributed ledger technologies <https://www.iso.org/committee/6266604.html>

<sup>127</sup> Press release, Ministry of Industry and Information Technology of the People's Republic of China <http://www.miit.gov.cn/n1146290/n1146402/n1146440/c6081357/content.html>

not be an option depending on the existing laws. In the case of a public blockchain, various options of identity management solutions are being explored but still in infancy stages. In the use cases explored in the Technology and Innovation lab, identity has been managed in a centralized fashion while others are experimenting with new solutions.<sup>124</sup>

#### 9.5.5 Data ownership and Data Access

Whilst a private blockchain is more likely to be used in the context of land administration, data ownership and data access remains nevertheless a relevant issue. The quality of record on the onset would need to be up to standard and error-free, which is hardly the case with land cadaster including legacy geographical data impact both the issue of ownership and access. There is a new form of privatization of the registration of land rights which will create a new challenge on who should own the data.<sup>125</sup> Furthermore, the multiplicity of copies of the ledger in several nodes begs the question on whether all nodes should have the same data and which data should be accessible e.g. private information on land owner would be shared across all nodes.

#### 9.5.6 Standards

Blockchain technology and smart contract are relatively new artifacts. There is no prevalent standard at this point on blockchain technology although several institutions are looking at standards for blockchain including ITSO<sup>126</sup> where the ISO/TC 307 working group has been set up to explore the said standards. Recently, the Chinese government launched an initiative to develop standards.<sup>127</sup>



#### 9.5.7 Electronic Signatures

The legal recognition of digital signature or e-signature is an important aspect to be taken into account should a blockchain solution be envisaged. Many countries are yet to fully recognized digital signatures as valid form of signatures.

#### 9.5.8 Security

The now infamous DAO breach is a perfect example that demonstrate that Blockchain systems may not be completely shielded from breaches. The DAO stands for Digital Decentralized Autonomous Organization and rested on the premises of organizing both commercial and for-profit enterprise with no conventional management system. A vulnerability in the DAO code exposed the organization and a third of its funds were stolen as result of a bug in its smart contract code. There has been a number of instance of “security breaches” affecting the blockchain ecosystem.

### 9.6 THE WAY FORWARD ON BLOCKCHAIN TECHNOLOGY AND LAND ADMINISTRATION

Blockchain technology and its applications in the field of land administration remain new and relatively untested. As discussed in this chapter, there are several “on chain” and “off chain” considerations that still need to be explored, studied, and tested. Furthermore, for blockchain technology to be widely adopted, it would need to demonstrate clear and quantifiable advantages over existing digital systems.

The World Bank continues to explore this technology to determine its fitness and applicability in ending extreme

*“Blockchain technology and its applications in the field of land administration remain new and relatively untested.”*

poverty and boosting shared prosperity in many areas, including land administration. Some of the next steps on the land administration front include: (a) conducting more POCs e.g. mortgage registration, which is expected to have a positive impact on commercial banks and urban housing; (b) testing the POC with interested client countries to learn more about adapting the POC to specific jurisdictions; (c) exploring the possibility of marrying the blockchain technology with other technologies e.g. cloud, AI to develop innovative client solutions; and (d) continuing to study the legal and policy implications of blockchain-based land administration services. Additionally, the World Bank Group continues to invest in knowledge and learning activities and studying the growing number of blockchain-based land administration pilots across the world. The World Bank Group also seeks partners with whom these issues can be explored in greater depth and breadth.

# 10

## *Blockchain Market Microstructure Implements the 100% Reserve Chicago Plan – Now What?*

*Matt Stack* <sup>128</sup>

<sup>128</sup> Matt Stack is a founder of XLP Capital, the founding manager of the Lambda Prime Venture Funds, and the Chief Investment Officer of XLP's technology equity and credit investments at Devonshire Capital Funds. He serves as the lead cryptocurrency and blockchain advisor to the United Nations, where he advises governments on technology and central banking policies.

### THE TECHNO-LEGAL CONNECTION BETWEEN BLOCKCHAIN, THE FEDERAL RESERVE, AND THE GREAT DEPRESSION

BLOCKCHAIN IS FULL RESERVE BANKING:  
ARE WE PREPARED FOR THIS?

Cryptocurrency, on the surface, is a family of technologies and associated systems of dedicated hardware that appear to be ripe for proof of concepts at the government, monetary policy, and even macro-economic domains. We see this in current events with the turbulent launching of the Venezuelan El Petro asset backed currency, the ebb and flow of funding into geopolitical pilots, and the prospective defensive tactics taken by the Chinese government against cryptocurrency. Is a blockchain based currency or commodity an asset or a liability at the geopolitical level, and what core issues should policy makers have in mind when framing their countries' exploration of blockchain and cryptocurrency pilots? Is blockchain a friend of government monetary policy makers that stands to lower costs, revolutionize local financial sectors, or is it a driver of decentralized threats and loss of control? Blockchain stands at the intersection of technology, economics, and monetary regulation and policy – too few understand all three sufficiently well enough to appreciate the issues that rest at the intersection of these disparate domains. What is needed is a better system of integrating and designing blockchain pilots with contract law, monetary policy, and blockchain's technological limitations.

These issues, and others, stand at the forefront of many today, without appropriate framing – and perhaps more troublesome – without careful consideration of the long term implications of blockchain backed assets and currencies. While the superficial interpretation of



blockchain in financial services and bitcoin currencies seem friendly in their applications to governments, monetary policy, and economic exchange given the association with core internet principles of decentralized, democratization, and distribution – are these the criteria for a successful and robust financial system? This makes sense to ask today, as the global economic system is run on money, and generation, exchange, and interaction of money appears at the center of many international and governmental agendas. Blockchain is said to be primed for adoption at the policy level for this reason, and it has enjoyed numerous pilots and projects throughout the world. It is my position and expectation that most of these projects will fail, not for lack of enthusiasm, funding, but rather for a core misunderstanding of the true nature and characteristics of the system of generating and sustaining the an asset based monetary supply.

We focus this paper on addressing three core issues that stand at the center of technology, economics, and legal policy: 1) how do modern monetary policy systems evolve over time? 2) where does money come from, and 3) how should we structure blockchain pilots?

### **10.1 HOW SHOULD A MODERN MONETARY SYSTEM EVOLVE OVER TIME?**

Modern monetary theory is imposed and upheld by a series of tightly orchestrated interactions between a core set of organizations, domestic and foreign banks, etc. It is brought into the scope of law through the passage of regulatory policy and code of law and statutes often associated with large monetary policy decisions enacted by leading government officials. The financial system of

most developed economies, and especially in the United States, was not invented and defined in one process, but rather has been repeatedly modified and upgraded, altered, and changed – especially frequently over the course of the past 100 years. In order to change the modern monetary system in place within a country, its regulators and policy makers enact modifications and changes to rules, tariffs, reserve levels, and interest rates at all levels of the system, and against transactions, entities, and even asset classes. The modern system seen in the United States, has undergone multiple severe structural changes, ranging from the introduction of the Federal Reserve Act of 1913 to the modern acts of legislation associated with the short and long term recovery from the Financial Crisis of 2008. Enacting this evolving system are a series of institutions, and people following the legal statutes, and interpreting what is out of scope through processes and market forces. Blockchain currency assets replace these mechanisms by permitting individual software developers to choose digital policies or “features” concerning the administration of the asset or currency, and then permitting the market to adopt – or not – a specific blockchain software based on how adopters like these rules. Adoption of the blockchain is often closely linked to whether others elect to dedicate their own compute resources and power to computing hashes, blocks, and proofs of work on behalf of the blockchain. If no one adopts the blockchain, and no one is willing to compute for the chain, the system collapses. Once launched, however, if members of the blockchain dedicate compute resources and download and run the software required of the blockchain, the system thrives. This raises the important question: what happens if changes are sought in the blockchain software, or if new features are deployed, optimizations made, of structural changes made to the blockchain? Changes to the blockchain require

*“Adoption of the blockchain is often closely linked to whether others elect to dedicate their own compute resources and power to computing hashes, blocks, and proofs of work on behalf of the blockchain.”*

<sup>129</sup> This has led to forks and new blockchains, including bitcash, bitgold, Ethereum classic, etc.

the downloading of new software – often, this software includes new features, enhancements to the interface, or how members interact with the blockchain. Other times, however, changes to the blockchain involves core structural changes – such as the block size and complexity of the hash computing algorithms. When this happens, tight coordination must be in place so that all parties simultaneously upgrade their software and agree to behave differently. Coordinating these mass, synchronized upgrades is expensive and high transaction cost – and so many in the recent years have failed. Occasionally, these lead to “hard forks” in the blockchain, in which some members follow the new features, while others continue on in support of the original blockchain.<sup>129</sup>

Herein lies a central challenge and question blockchain raises for the mature monetary policy practitioner: modern monetary policy has changed and adapted over the years through the introduction and passage of regulation and laws moderating the behavior of the institutions that enact the capital economy, while a blockchain approach

to monetary policy front-loads the decision making, and forces programmer-oriented forks to upgrade or alter the mechanism of behavior of the cryptocurrency. The mechanism of forking remains controversial, poorly understood, and would be one of the most central issues of contractual and policy law in any blockchain asset.

## 10.2 Where does money really come from?

We begin with the seemingly simple question of where money comes from, in order to gain a better appreciation of the often obscure and misunderstand sources of resilience and market

forces at play in our current monetary system. To the cryptocurrency enthusiast, blockchains appear to offer a well-thought out alternative to the generation of money by a central banking system. However true this may appear on the surface, it obscures the rich complexity and resilience of the system currently enacted in most developed economies. Specifically, in the US, we must understand the subsystems of the Federal Reserve, monetary supply metrics of M1 and M2, Treasury bank auction process, fractional reserve banking, and cash reserve ratios. Once we have gained an appreciation of these core concepts, we will examine their existence or absence in blockchain, and extrapolate implications.

At regularly scheduled intervals, the US Treasury holds auctions in which it sells securities, typically in the form of notes, bills and bond products in intervals ranging from months to years. Domestic and International banking institutions purchase these obligations, upheld by the central government, who promises to repay these obligations at a later time, honoring both the principle and the interest rate. Banks do not hold on to these notes, but typically resell them to other investors, for a marginal fee called a “spread” – at which point the bank will hold cash, and the investor(s) will hold promissory notes or securities documents (electronic and printed) informing them of ownership of the bond or other Treasury product. The Treasury is regulated in the amount of products it sells by policy regulations enforced on it, which will direct the maximum number of current outstanding obligations (debt ceiling) it is allowed to sustain at any time. In addition, the Treasury is subject to supply and demand of banks and investor willingness to buy, and may adjust its interest rates to respond to the ebbing and flowing of investor interest in holding treasury securities, which are thought



to be lower yielding, but safer investments than other investments may be (including real estate, commercial equity and credit, foreign exchange currencies, derivatives, etc.).

The US Treasury market is roughly \$14.5T USD, anticipated under current government policy to expand to \$15.5T USD by the end of the 2018 calendar year. Three primary parties purchase these US Treasury products: Foreign Governments, US banks, and the Federal Reserve Bank. Foreign governments as of the end of January, 2018 hold in aggregate around \$6.2604T USD.<sup>130</sup> US Commercial Banks hold in aggregate \$2.499T<sup>131</sup> as of February 2018. This leaves approximately \$3.3T USD in Treasury held by other US domestic investors, including individuals, institutional investors, State level institutional balance sheets, and corporations.

When foreign governments purchase US Treasuries, they must purchase with assets converted to US currency (subject to foreign exchange currency rates), and then purchase the Treasury notes, bills, and other securities. When US domestic investors, individuals, institutions, States, and corporations purchase US Treasuries, they do so by transferring US dollar currency from bank accounts, usually electronically, through the auction process – or from US commercial banks who in turn purchased the Treasuries. When the Federal Reserve Bank accumulates assets, including bonds, or Quantitative Easing assets, it does so ex nihilo by crediting its own internal balance sheet.

The activities of the US Federal Reserve Bank are strictly regulated by US government policy, e.g. through changes implemented to it through the passage of US Law. This

<sup>130</sup> United States Treasury Monthly Report: <http://ticdata.treasury.gov/Publish/mfh.txt>

<sup>131</sup> Federal Reserve Bank of St. Louis reporting via FRED: <https://fred.stlouisfed.org/series/USGSEC>

includes a recent – if not subtle – change to the Federal Reserve Bank cash on hand dividend policy passed as part of the Fixing America’s Surface Transportation Act or “FAST Act”:

#### SEC. 32203. DIVIDENDS OF FEDERAL RESERVE BANKS.

(a) IN GENERAL.—Section 7(a)(1) of the Federal Reserve Act (12 15 U.S.C. 289(a)(1)) is amended—

(1) by amending subparagraph (A) to read as follows:

“(A) DIVIDEND AMOUNT.—After all necessary expenses of a Federal reserve bank have been paid or provided for, the stockholders of the bank shall be entitled to receive an annual dividend on paid-in capital stock of—

“(i) in the case of a stockholder with total consolidated assets of more than \$10,000,000,000, the smaller of—

“(I) the rate equal to the high yield of the 10-year Treasury note auctioned at the last auction held prior to the payment of such dividend; and

“(II) 6 percent; and H. R. 22—429

“(ii) in the case of a stockholder with total consolidated assets of \$10,000,000,000 or less, 6 percent.”; and

(2) by adding at the end the following:

“(C) INFLATION ADJUSTMENT.—The Board of Governors of the Federal Reserve System shall annually adjust the dollar amounts of total consolidated assets specified under subparagraph (A) to reflect the change in the Gross Domestic Product Price Index, published by the Bureau of Economic Analysis.”.

(b) EFFECTIVE DATE.—The amendments made by subsection (a) shall take effect on January 1, 2016.

Numerous changes to the behavior and restrictions of the Federal Reserve have been introduced, imposed, and modified over the past ~100 years. It is likely that restrictions will continue to evolve over time, as restrictions

*“Of importance to our understanding of the origination of new currency in the modern monetary system is the requirement for cash-on-hand imposed on commercial banks by US legal statutes and the membership rules imposed on banks that participate as members of the Federal Reserve central banking system.”*

on the Federal Reserve – and other Central Banks – are often policy makers’ principle levers in implementing changes to monetary policy.

The many and varied ways in which commercial banks earn profit from financial activities is beyond the scope of this article. A critical function of the commercial bank is the management and maintenance of a balance sheet comprising of cash on hand, as well as a cumulative amount of assets and liabilities spanning multiple lines of business. These lines of business can include spreads earned from reselling Treasuries, investment returns, advisory service revenue, and interest gained on lines of credit or checking accounts. Of importance to our understanding of the origination of new currency in the modern monetary system is the requirement for cash-on-hand imposed on commercial banks by US legal statutes and the membership rules imposed on banks that participate as members of the Federal Reserve central banking system. The requirement, in short, mandates that banks maintain a certain minimum amount of cash on-hand and on-site depending as a function of the total balance sheet size.

A poorly understood – and often mischaracterized mechanism of the monetary generation system – is the requirement for all commercial banks participating in the central banking system to continuously hold a percentage of their balance sheet with the Federal Reserve. This amount is mandated as a percentage of total assets at any time, and is described under the Federal Reserve Act, Section 5. Stock Issues; Increase and Decrease of Capital:

Shares of the capital stock of Federal reserve banks owned by member banks shall not be transferred or hypothecated.

When a class member bank increases its capital stock or surplus, it shall thereupon subscribe for an additional amount of capital stock of the Federal reserve bank of its district equal to 6 per centum of the said increase, one-half of said subscription to be paid in the manner hereinbefore provided for original subscription, and one-half subject to call of the Board of Governors of the Federal Reserve System. A bank applying for stock in a Federal reserve bank at any time after the organization thereof must subscribe for an amount of the capital stock of the Federal reserve bank equal to 6 per centum of the paid-up capital stock and surplus of said applicant bank, paying therefor its par value plus one-half of 1 per centum a month from the period of the last dividend. When a member bank reduces its capital stock or surplus it shall surrender a proportionate amount of its holdings in the capital stock of said Federal Reserve bank. Any member bank which holds capital stock of a Federal Reserve bank in excess of the amount required on the basis of 6 per centum of its paid-up capital stock and surplus shall surrender such excess stock.

The Federal Reserve Act, Section 7. Division of Earnings, (a) Dividends And Surplus Funds Of Reserve Banks provides that a bank holding 6% of their assets at the Federal Reserve shall gain 6% tax-exempt interest on their contribution, unless the member bank is large and holds consolidated total assets in excess of \$10B, this interest rate will be “the rate equal to the high yield of the 10-year Treasury note auctioned at the last auction held prior to the payment of such dividend” if this number is smaller than 6%. At the time of this publication, in April 2018, the yield of the 10-year Treasury note is 2.776%, so large member banks with greater than \$10B in assets are receiving this small yield, and not 6%. The central purpose of this requirement is to ensure a sharing of cash and assets

across all banks, so that a “central bank” may provide additional balance sheet in the event that any member bank runs into difficulty or faces stress on its balance sheet (more on this later). It is worth noting that this central feature of behind-the-scenes risk sharing across the banks mitigates risk in any one bank, and is a crucial – and yet missing – feature from blockchain and crypto-exchanges today. Large balance sheets and large pools of capital tend to absorb economic shocks better than smaller balance sheets. This tends to result in more stable and less volatile asset prices. Blockchain promotes a highly distributed set of wallets, and therefore rejects the creation of a central “large pool of cash” (aka balance sheet) that a central bank may provide. We observe the implications of the absence of this central behind-the-scenes balance sheet daily with the price volatility in most crypto currencies.

The Federal Reserve is an integral member of the monetary system, as it also participates in Treasury auctions, Financial Crisis asset purchasing programs, Quantitative Easing and Tightening programs, and is permitted to purchase and hold bills, bonds, notes, etc. at its discretion. In other words, the Federal Reserve Bank buys and holds money issued by the Treasury. As we shall discuss later, this amounts to a significant portion of Treasury originated bills, bonds, etc. Without the Federal Reserve, the monetary system would be missing a critical counterparty in the system of currency supply, and would require alternate structures or institutional processes to generate currency. Despite the relative complexity of the modern currency creation system, it ensures that policy makers and capital market supply and demand forces are closely linked to the decision processes.

The Federal Reserve is owned by its member contributors

– e.g. commercial banks that place deposits with the Federal Reserve. Commercial banks that are members of the Federal Reserve are required to hold a portion of their liabilities – net transaction accounts – in cash or deposits on-hand. The rest of their liabilities may be held elsewhere, leant elsewhere, etc. The requirement to have cash on hand is known as the “Reserve Requirement,” is mandated by the Federal Reserve Bank, and administered through the policy practices stated and summarized in materials to member banks:

Reserve requirements must be satisfied by holding vault cash and, if vault cash is insufficient, also by a deposit maintained with a Federal Reserve Bank. An institution may hold that deposit directly with a Reserve Bank or with another institution in a pass-through relationship. Reserve requirements are imposed on “depository institutions,” defined as commercial banks, savings banks, savings and loan associations, credit unions, U.S. branches and agencies of foreign banks, Edge corporations, and agreement corporations.

Under the Depository Institutions Deregulation and Monetary Control Act of 1980, the bill:

Requires all depository institutions to maintain reserves in the Federal Reserve System. Imposes a three percent reserve ratio on the first \$25,000,000 of an institution’s total transaction accounts (any account upon which withdrawals may be made by an instrument, payment order, telephone, automatic transfers from savings, share draft or other means determined by regulation of the Board). Requires reserves to be maintained against an institution’s total transaction accounts over \$25,000,000 in the ratio of 12 percent or at a ratio between eight and

14 percent prescribed by the Board. Adjusts the base level figure of \$25,000,000 each year according to the change in total transaction accounts held by all depository institutions. Imposes a three percent reserve requirement on all time deposits in which any interest is held by a depositor who is not a natural person. Authorizes the Board to adjust the reserve ratio on nonpersonal time deposits between zero and nine percent solely for the purpose of implementing monetary policy.

The Garn–St Germain Depository Institutions Act of 1982 exempted the first \$2.1 million of liabilities from reserve requirements, for banks that are members of the Federal Reserve banking system, and specified that the exemption amount is changed annually by a formula. The Garn-St Germain Act specified that a bank having net transaction account liabilities between \$2.1 and \$26M would be required to hold only 3% of this liability as cash on hand, while the rest could be leant out, or held elsewhere. These numbers have changed annually since this Act, and now require the 3% holding for net transactions of between \$16 - 122.3M. When net transaction account liabilities exceed \$122.3M, the Federal Reserve requires member banks to keep 10% of liabilities on hand in cash accounts. The concept of a cash reserve ratio is therefore the minimum amount of total liabilities a bank must hold in cash on site (or in deposits with the central bank, e.g. the Federal Reserve Bank). This contributes to the widely quoted and discussed figure that the US economy is based on a fractional reserving system of 10%.

As an aside, a cursory review of international policy at the time of this publication shows a diverse set of international requirements for cash reserve ratios (e.g. the percent of funds required on hand vs. the total balance sheet size

of a bank), ranging generally from 0% to 45%, with the majority falling between 5-10%. Exceptions to this would include Australia, New Zealand, Sweden for which the ratio is 0%, but limitations on reserves and the size of bank balance sheets are enforced through different mechanisms (e.g. specifying and limiting the maximum total liabilities owned by the banks). Some countries have seen significant historical fluctuations in this number depending upon financial regulatory policies: the UK evolved from 20.5% to 5.0% to the current 0% (limitations on banks enforced via other regulation), Turkey from ~60% to 5-10% (depending on maturity date of liabilities), Germany from 20% to 12% before the European Central Bank, and around 1% after the ECB regulations were enacted.

The concept of cash reserve ratio is critical for the modern monetary system because it permits a single bank to loan out against its on-hand cash in a multiplying ratio effect that magnifies the amount of capital over the amount of physical cash required. If a borrower approaches a bank and asks for a loan, the bank is permitted to issue that loan ex nihilo by electronically debiting a depository account without crediting this same amount in any other account. Instead, it credits a fraction of this amount on its balance sheet. For every \$100 held on hand and held at the Federal Reserve Bank, a US bank may lend another \$900. Most of this system of accounting is conducted electronically, with on-hand requirements for physical printed cash settled through an order process between the banks and the Mint; a periodic process by which a bank may request delivery of physical printed cash from the Mint to provide or issue requests by customers. Since most banking customers handle cash through electronic transfers to credit cards, checking systems, electronic transfers, etc. the physical printed cash currency requirement is rarely stretched. If

*“ The concept of cash reserve ratio is critical for the modern monetary system because it permits a single bank to loan out against its on-hand cash in a multiplying ratio effect that magnifies the amount of capital over the amount of physical cash required. ”*



the system were at any point to be tested, for instance if all owners of the  $\$100 + \$900 = \$1,000$  in the aforementioned example were to ask for printed physical currency at the same time, the banks would be required to solicit the Mint for additional cash to distribute. If the request for

cash were to accelerate across multiple accounts and multiple banks - causing the so-called “bank run” - the banks would fall back to a central bank to petition for funds to cover the run. Prevention of this form of crisis was one of the primary reasons for the Federal Reserve Act of 1913 which established

12 regional Federal Reserve Banks, and introduced the 6% depository rule for bank funds.

In practice, under the processes of the modern monetary policy system, money is created whenever commercial banks lend money to borrowers. No process akin to cryptocurrency mining is conducted, and no balanced general ledger accounting is performed. Instead, capital market supply and demand principles dictate how much money is lent out, and at what interest rate, preventing a runaway multiplier effect. In other words, the amount of money created is a function of the number of borrowers willing to borrow money at a given interest rate. There is only a demand side to the modern monetary system - there is no supply constraint. If there is marginal cost to providing a new loan, why then, don't banks lower interest rates and lend an unlimited amount of money by underwriting an unlimited number of loans? There is no simple linear answer to this question. Rather, the answer is dependent upon the fact that banks would suffer reputationally if their loans failed at high rates (see stock prices of mortgage bond lenders during the mortgage

crisis), and to the fact that banks are often engaged in multiple lines of business at any time that provide greater profitability from utilization of their balance sheet than underwriting loans. Once a depository account has been debited with money, the lending commercial bank's requirement to keep a portion of cash on hand increases slightly (in accordance to the cash reserve ratio).

While most blockchains originate new currency through programmatic mining or timed release of funds, the modern monetary system originates new money through a competitive and resilient process of reputational and demand-side driven loan origination that generates currency through policy-defined fractional reserving. Trusting blockchain's method of currency generation requires having faith in the bug-free, transparent nature of a coded methods and algorithms in the blockchain code base. On the other hand, trusting modern monetary policy requires trust in banks following opaque loan market equilibrium.

The net effect of the cash reserve ratio is to permit the virtual creation of spending power and econometric velocity of cash that is greater than the sum of physical printed cash. In the days of gold-backed cash (so called the “gold standard”), the introduction of regulation enabling the invention of the cash reserve ratio, and the system of fractional reserve banking it created, was argued to be a crucial development for economic growth. It was argued that a large portion of currency remained dormant in savings and bank accounts, not performing an economically useful activity, such as the promotion of trade, pricing and exchange of services. Fractional reserve banking increased the effective utilization of all printed physical currency.



Critics of the fractional reserve banking system, and its underlying reliance on the cash reserve ratio accounting system, generally point to the “run-away” effects: including the difficulty with tracking and measuring the amount of money actually in circulation or deployment at any time. The same mechanism that permits a bank to lend a multiple of its cash on hand could in theory lead to unintentional run-away effects if that bank were permitted to lend \$100 to another bank, who in turn could fractional reserve and lend another \$900. This magnification effect might result in a multiplying effect whereby the fractional reserve rate of \$100 may turn into \$1000 and then in theory again into \$100,000 or more. While in theory this is possible, in practice this is limited by market supply and demand pressures between banks, and the practical auditing of bank balance sheets.

In response to criticisms of run-away currency generation, various measurements were proposed to track monetary supply, including the well know Currency, M1, M2, and M3<sup>132</sup> indexes. M1 was established to measure the amount of physical printed cash, plus the amount of money held in demand deposits (immediately available, liquid asset deposits). M2 was defined as the sum of M1 plus the addition of time deposits, savings deposits, and some money-market funds. M3 expands upon M2 inclusively to include longer time deposits and other forms of money. The progression of M1 to M2 and M3 may be viewed as the increase in virtual currency associated with the US Dollar, as driven and empowered by the magnifying effects of fractional reserve banking and the cash reserve ratio. For every \$1 US Dollar measured as currency, M1 was approximately 2.26 as of end of 2017, M2 approximately 8.67 as of the end of 2017, and M3 if measured in accordance to the way it was reported through 2006,

<sup>132</sup> United States Treasury Monthly Report: <http://ticdata.treasury.gov/Publish/mfh.txt>

<sup>133</sup> In 2006, the ratio of M2 to US Currency was 9.45, and the M3 to Currency ratio was 13.77. In 2018 as of the end of 2017, the M2 to US Currency ratio is 8.67, reflecting a general deleveraging between M2 and Currency. Assuming the same deleveraging might hold between M3 and US Currency across the same time, we arrive at an approximate 2018 M3 to US Currency ratio of between 12 and 13

would be between a number likely between 12 and 13.<sup>133</sup> Additional measures of progressively more expansive tiers of M4, M5, M6... etc. could in theory be estimated but lose precision and approach back-of-the-envelope estimates. Suffice it to say, the 12-13x multiplier of Currency-to-M3 is a far cry from the worst-case scenario of runaway currency generation, but suggests that the currency multiplier is a very real phenomenon.

We argue here that the details and precision of estimated M1, M2 and the now-defunct M3 are irrelevant in the face of the conclusion we wish to draw: that the power of the cash reserve ratio serves to amplify the practical currency velocity and spending power on goods and services in an economy as a multiple of the total amount of physical currency in circulation. This seems to be the case, and appears to be practically manageable across most major mature monetary systems. If we presume to take the role of architect of a modern monetary system (as many blockchain programmers and development teams have become), it might be prudent to ask the question: what is the ideal cash reserve ratio for a currency system?

While it is not in the scope of this paper to expound on the intricacies of the capital markets, their structure, and the details of structured financial products, it may be possible that legal and regulatory-enforced reserve ratios have optimal ranges of values. If the cash reserve ratio is too low (e.g. <5%), it is likely that the tolerance for faults in the economic system are high if not otherwise mediated – otherwise banks have less reserve to absorb financial stresses or shocks. If the cash reserve ratio is too high (e.g. >30%), there is an implicit reduction on the rate at which money is leant out, which may have the consequence of slowing the rate of economic development.



We turn our attention now to looking for analogies to other examples of asset and currency systems that have similar mechanisms of reserve ratios, or insurance mechanisms – in order to establish a viable and sustainable range of cash reserve ratios. Here we discover that collateralized mortgage backed securities (CMBS) of the well-known 2008 Financial Crisis have similar mechanisms and measurements. Specifically, when a tranche of mortgage backed securities is created, a group of mortgages of varying quality is assembled and placed in a single structured entity. The ability of that entity, or group of mortgages, to meet its aggregate cash flow requirements, is a function of the ability of the group of mortgages to stay solvent in aggregate, and to meet the ability to pay the periodic interest rate coupons issued by the entity. If mortgages within the group collapse and are no longer paying their mortgage obligations, a certain percentage of other mortgages in that tranche must continue to pay in order for the coupon to be issued. The subordination level is defined as the “proportion of principal outstanding of the junior tranches who will absorb initial credit losses”<sup>134</sup> and in practice, represents an analogy to the amount of cash on hand required of banks in the event of crisis – an effective cash reserve cushion. While the savvy financial engineer will point out myriad differences between the cash reserve ratio and the subordination level, we stress that each acts in principle as a level of insurance against a set of assets on a balance sheet.

In 1995, AAA rated CMBS tranches contained around 30-32% subordination levels, and riskier A tranches contained ~20%, while the even more risky BBB- tranches contained 15% levels. In 2007, one year before the financial crisis, AAA rated CMBS tranches held on average ~12% subordination levels, A held ~10%, and BBB- tranches held between

3-4% levels. These were discovered within a year to be unsustainable, and 2008 required severe intervention and “bailing out”. A similar effect to fractional reserving in M1, M2, and M3 was observed in CMBS as tranches of mortgage securities were subsequently re-tranched and derivatives against these underwritten multiples of the underlying securities. Attempts to formalize volumes of CMBS rehypothecation and derivative volumes are difficult and poorly documented, but estimates have ranged anywhere between 10-50x underlying assets depending on the tranche (compare this to 12-13x multiplier of Currency to US M3). Prior to the Financial Crisis of 2008, this re-tranche process was regarded as beneficial in helping to accelerate velocity of investment in real estate. After 2008, it was regarded as unsustainable, unnecessary, and excessively risky.

Is it possible to abstract and generalize learning from macro-economic stability measures as well as micro-economic risk measures, to estimate that a sustainable cash reserve ratio might exist somewhere in the range of 10-20%? If we take CMBS subordination levels as a proxy measure of risk and fragility, we may argue that cash reserve ratios below 10% are deemed too risky for the system to absorb shock, economic turbulence, surprise, or the unexpected. Meanwhile, if the cash reserve ratio is greater than 20%, it may be argued that the currency system sub-optimizes the rate of currency velocity, liquidity, and deployment required for a stable economic system.

We conclude this section with the observation that sustainable cash reserve ratios that strike the balance between systemic fragility and promotion of growth appear to take place within the 10-20% range. Below this

*“Prior to the Financial Crisis of 2008, this re-tranche process was regarded as beneficial in helping to accelerate velocity of investment in real estate. After 2008, it was regarded as unsustainable, unnecessary, and excessively risky.”*

<sup>134</sup> What is Subordination About? Credit Risk and Subordination Levels in Commercial Mortgage-backed Securities (CMBS). Xudong An, Yongheng Deng, Joseph B. Nichols, Anthony B. Sanders. 2014

number, additional tiers of control are required (perhaps those architected into blockchain are sufficient, but this is not time-tested). Above this number, and one may argue the fundamental nature of the monetary system is changed, and the central purpose of currency proliferation is slowed.

What, then, is the cash reserve ratio of a blockchain asset? At the heart of blockchain is a crypto-hashing technique that guarantees that only one hashed currency amount may exist in any wallet at any given time – this is known in the blockchain community as defense against the “double spending attack”. Once a currency amount has been mined and introduced onto the blockchain, it can not be duplicated, replicated, etc. It can only be transferred to other wallet addresses, and there is a total conservation of crypto-currency at all times on the blockchain (whether or not wallets remain accessible is beyond the scope of this paper).

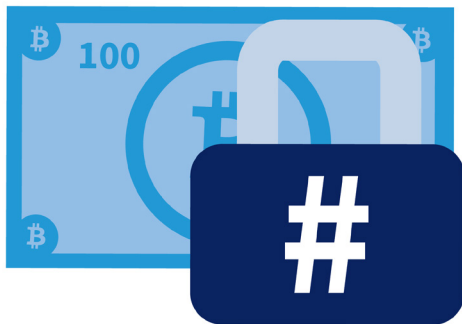
Consequently, it stands to reason that blockchain represents a monetary system that prohibits ex nihilo currency creation, and therefore inhibits fraction reserving in its current implementation. Said differently, a currency implemented on blockchain has a cash reserve ratio of 100%. This is sometimes referred to as a “full reserve banking” system.

We have already discussed that at the heart of most modern monetary systems is a cash reserve system practically bound to between 5-15%. The core features that promote blockchain immutability and security, authenticity, etc. required of a purely electronic medium of currency or

asset registry, also impose severe limitations on – if not outright reject – the ability of the blockchain system to promote fractional reserve banking. More concretely, at the time of this paper’s publication, of the 1,000’s of crypto currencies in deployment, none provides a mechanism for fractional reserving. No current cryptocurrencies provide a mechanism for cryptocurrency reserve ratios other than 100%. Instead, all blockchain assets and currencies require that lenders of crypto currency only lend out exactly the amount of money in possession, and no more. Blockchain inhibits the creation of depository accounts upon the issuance of a loan, up to an amount protected by the cash reserve ratio.

Fractional reserving requires a temporary suspension of the general ledger of a bank’s balance sheet to permit the debiting of an account with a monetary amount that does not exist on site, but is rather a function of the cash reserve ratio requirement the bank is required to honor. To map this process against a cryptocurrency operating on a blockchain would require a technology to take a tally of blockchain assets, and then suspend the proof of work, mining, and transaction validation algorithms momentarily, and create new assets – in effect either replicating the blockchain hash multiple times – or creating what is known as “side chains” which might represent other chains forking off from the primary hash block. Multiple attempts have been proposed as of the time of this publication, including the arguably controversial algorithm of “proof of proof of work” which would support side chain expansion and collapsing.<sup>135</sup> This technology is too new and too early to determine its long-term viability or susceptibility to method or algorithmic hacks.

We pause momentarily to ask a question: is it possible that



<sup>135</sup> Proofs of Proofs of Work with Sublinear Complexity. Aggelos Kiayias, Nikolaos Lamprou, and Aikaterini-Panagiota Stouka. National and Kapodistrian University of Athens. - and - Non-Interactive Proofs of Proof-of-Work. Aggelos Kiayias, Andrew Miller and Dionysis Zindros. University of Edinburgh. University of Illinois at Urbana-Champaign. National and Kapodistrian University of Athens. December 4, 2017

the essence of cryptocurrency implementation on top of blockchain stands at odds with one of – if not the most important – lever by which government policy asserts influence on its monetary system and economic growth rate, via the policy set cash reserve ratio? While interest rates are often the dominant and frequently changed value on a short term basis, changes in cash reserve ratios are arguably more systemic and have far wider implications. Here we rewind the clock to the Wall Street Crash of 1929, and recall the backlash against the financial system that led to such a widespread systemic collapse in the asset pricing system. Multiple opponents of the financial system emerged, including the now largely popularized work of John Maynard Keynes. Milton Friedman is also said to have advocated for 100% reserve banking on selected bank accounts, including retail consumer checking and short-term deposits.<sup>136</sup> Above all, however, the work of Irving Fisher stands out; Irving was a long proponent of 100% cash reserve banking, an argument that was largely ignored and regarded as impractical. Irving and Henry Simons proposed a system known as the “Chicago Plan”<sup>137</sup> that promoted the benefits of 100% reserving as: control over business capital cycle trends, elimination of bank runs and bank issued currency, and general reduction in consumer and government debt. In contrast to the current system of monetary creation, in which currency is created whenever commercial banks issue loans, the Chicago Plan proposed the effective segmentation of debt from the currency creation process. Banks would make loans only of the currency and assets they had in reserves, and no more. Currency creation would proceed under government policy processes, but debt would be replaced by a series of investment trusts that would facilitate lending. The role of banks, and central banks, would be fundamentally different and more limited than they are today.

<sup>136</sup> Solow, Robert M. (March 28, 2002), “On the Lender of Last Resort”, *Financial crises, contagion, and the lender of last resort*, Oxford University Press, p. 203, ISBN 978-0-19-924721-9

<sup>137</sup> IMF Working Paper – Research Department. Jaromir Benes and Michael Kumhof. *The Chicago Plan Revisited*. 2012

### 10.3 HOW SHOULD WE STRUCTURE BLOCKCHAIN PILOTS?

The long-term ramifications of an economic structure and asset and liability exchange system in which the Chicago Plan is enacted are unknown. We may study the speculations of the authors and proponents of the Chicago Plan from the first half of the 20th century, examining their proposed implications and end-state. Regardless of the outcome, we are clearly entering a period in which blockchain pilots, economic experiments involving cryptocurrencies, proof of concept projects investigating crypto-unique assets, and entrepreneurial endeavors building unique and immutable smart contracts will closely mirror the system described by the authors of the Chicago Plan. We must accept that blockchain isolates the creation of currency and asset from the process of lending and debt creation or facilitation, in such a way as to isolate the lending process entirely. What implications does this have?

We can extrapolate impacts on policy and law from the basic observation that any blockchain system does not inherit the same counterparty financial obligations seen with modern financial regulation or corporate contract. Blockchain assets and contracts pertaining to instruments of debt or obligation – at their core – relate to an economic system that bears nearly no resemblance to our current modern system, but rather to a speculative system imagined over 90 years ago during the peak of the Great Depression. Transactions and blockchain “contracts” should be viewed instead as highly experimental, and not founded on the same legal standing as current modern monetary system policy. Taken to the logical extreme, we will find that most arguments pertaining the contractual

*“ The more blockchain currencies gain adoption, the increasingly adversarial or irrelevant the classic monetary debt creation process will become. ”*

obligation of a blockchain contract involving obligations between two parties will fail the test of modern debt law in most jurisdictions. While it appears safe to argue for blockchain's treatment and standing in contracts as currency, it is not obvious that blockchain-based investments, loans, microfinance, coin offerings, crowd funding, or debentures have any standing in existing case law, because the core mechanism of blockchain as a 100% currency reserve system necessarily precludes its integration with loan based monetary policy.

Looking forward, it seems clear that blockchain forces a priori decisions about currency generation and asserts strict rules and limitations on currency reserving and rehypothecation. Many of these decisions will be left to software developers and the democratic adopters of cryptocurrency and blockchain platforms – and not to policy makers and regulators. Legal professionals, regulators and policy makers, therefore, will find it increasingly difficult to assert control over currency restrictions in blockchain without changing software code and driving adoption of new “forks” in currencies. As the authors of the Chicago Plan foresaw, the opportunity for legal professionals and policy makers may rest in the clarification, definition, and illustration of the newly orphaned statutes of commercial contract, debenture, loan origination, and central banking. The more blockchain currencies gain adoption, the increasingly adversarial or irrelevant the classic monetary debt creation process will become. This will require a complete audit of many legal statutes governing the interaction of central banks, banks, and reserves to fully appreciate the long term, at-scale implications of successful blockchain pilots. Too often, blockchain startups, pilots, and programs are launched with no consideration as to the

economic implications; this is dangerous and potentially catastrophic to monetary policy. At the time of this paper's writing, most blockchain currency pilots the author has reviewed at the international policy and government level may be deemed unsustainable or “dead on arrival” due the simple fact that they have ignored the implications of de-coupling currency generation from debt origination. An economy that operates at a 100% reserve ratio has not proven successful or sustainable in the past century, and no leading economy has demonstrated monetary policy segmented from commercial lending. To state this opportunistically rather than critically, policy and law makers should focus attention on two primary goals as they move forward with blockchain pilots: 1) defining new processes for managing contractual debt issuance and contracts that involve blockchain currency, or 2) investing in technology solutions that permit fractional reserving, or cash reserving at less than 100% on blockchain.

# 11

## *ICOs: “Understood and Misunder- stood”*

*Mona Zoet* <sup>138</sup>

<sup>138</sup> Mona Zoet is the founder & CEO of RegPac Revolution (a Knowledge Sharing / Ecosystem Building Platform for Thought leadership and Networking).

Imagine you are a blockchain startup looking to raise funding for your project. You don't have enough money to fund an IPO, which can easily run into the millions for legal, investment banking and accounting fees. You don't have a long-standing, proven product that you can pitch to VCs. All you have is a brilliant idea, and maybe a prototype. This is where you can use an ICO – an initial coin offering, where you develop your own crypto currency and sell it to anyone who believes in your idea.

Just in the past 14 months ICOs have raised nearly \$4.5 billion for blockchain and related startups, blowing the \$1.3billion from VCs out of the water, and it is easy to see why. Not only do ICOs have the potential to provide much larger amounts of funding than VCs, with Telegram anticipating \$2.55 billion from their ICO after three rounds of coin offerings, but too it offers a simpler route to the funds. Many VCs expect a functional, fully developed product before they invest any money, which can often be difficult for a startup to achieve, but with an ICO all you need is an excellent idea and a little bit of marketing to build up hype around your product, and the investors will come.

### **11.1 UTILITY TOKEN**

With this said, an ICO hold great potential as a source of funding for a firm, and there are a number of different ways it can be done, depending on what works best with the specific firm's business model. The first of these that we will consider, and likely the most common, is the offering of a Utility Token – a form of crypto currency that holds some redeemable utility in a firms platform once they are set up. The best way to understand this is to consider a

Case Study of a Utility Token that is currently available, so we will look at UKG (Unikoin Gold), a cryptocurrency built on the Ethereum platform that can be used for gambling on e-sports events (competitive video gaming).

UKG - Utility Token Example:

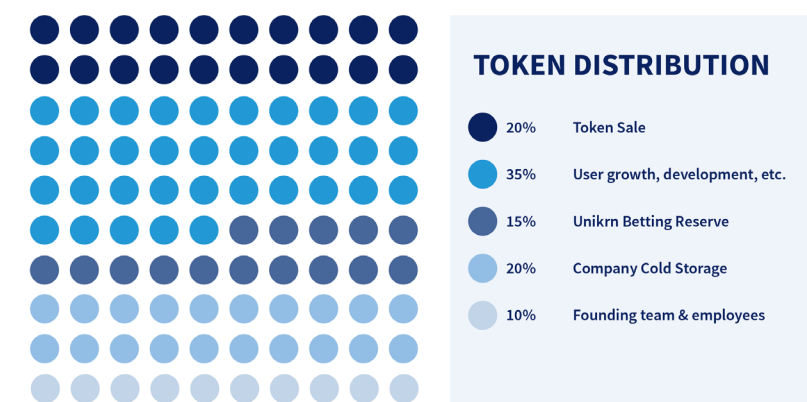
UKG is a cryptocurrency developed by UniKrn, an esports entertainment and betting platform. The UniKrn platform originally used an internal token system that was redeemable for products such as jackpot tickets, but in the dawn of blockchain saw an opportunity to improve the efficiency of these transactions by using a cryptocurrency. By developing it on the Ethereum blockchain, it could make use of the platform's additional utilities such as smart contracts, they created UKG – a cryptocurrency that is redeemable on the Unikrn platform for jackpot tickets and wagering, just as in the old system, but also with its own cryptocurrency that can be redeemed for Ether.

In total there are 1 billion UKG tokens that exist, and as shown in figure 2, 20% of these were distributed via an ICO in September 2017. The price at the time of the ICO was:

1 UKG ≈ 0.00115 ETH  
 ≈ 0.3 USD

This means in total Unikrn raised approximately 300,000 ETH from their ICO, worth 60 million USD. Beyond this Unikrn had already been operating successfully for 3 years before the ICO, so this was merely additional capital to facilitate international expansion of their firm.

Figure 2



Since the ICO the price of UKG has settled at about 0.315 USD, meaning the founders and employees also have 31.5 million USD worth of UKG between them, and even a further 63 million USD in cold storage – an offline reserve of UKG that could potentially be distributed at a later date.

An additional benefit to offering a Utility Token is that there is nothing stopping a firm from expanding the Token's use in the future. For example, Unikrn have said that as they grow their platform they will be looking into new products that UKG could be used for, such as premium features on their website, or tournament hosting. This could then cause further growth in the currency's value, increasing the value of the firm's assets in cold storage and offer even more potential for funding.

11.2 OTHER FORMS OF ICOS

Aside from Utility Tokens, ICOs can offer cryptocurrencies that behave similar to more traditional investments,

*“But why would a firm choose to use an ICO rather than an IPO, if they are essentially the same thing? The obvious answer is that a share sold in the form of a cryptocurrency will benefit from all the advantages of DLT, such as their incredibly fast transfer times, and the ground-breaking security of the blockchain.”*

so these are perhaps easier to understand if you have a financial background. This could be as a CIS (collective investment scheme), debenture or security. If we consider the example of using a token as a security, this will mean the crypto currency will imply ownership of equity of the firm. In this case the ICO will very closely resemble an IPO, where the firm sells equity in exchange for funding for their business, except in this case they are selling the equity as a crypto currency, rather than for fiat currency on a traditional exchange. Again, this process is best understood through a real-life example, so we will look at LKK (Lykke Coin), developed by Lykke.

#### LKK – Equity Token Example

Lykke is a Swiss FinTech firm building a currency and asset exchange using coloured coins – a form of crypto currency that is a representative of a real asset. Essentially, instead of trading the actual asset, which is slow and costly, you exchange the coloured coins, making use of the speed and security of blockchain technology, and then redeem the coloured coins when you need the asset. As a means of funding their project, Lykke developed LKK on the bitcoin blockchain, itself a coloured coin, that not only represented a share of equity in the firm, but also offered a means of voting on important company issues, with one coin representative on one vote, just as a normal share in a company would do. These coins were initially distributed to employees and private investors, and then were offered to the public in October 2016 via an ICO. The price of LKK at the time of ICO was:

1LKK ≈ 0.05 USD

And a total of 23,226,753 LKK were sold, meaning a total of 1,239,670 USD was raised, which when combined with the

private investments (some of which accepted the payment in LKK too), certainly left Lykke with a good amount of funding.

But why would a firm choose to use an ICO rather than an IPO, if they are essentially the same thing? The obvious answer is that a share sold in the form of a cryptocurrency will benefit from all the advantages of DLT, such as their incredibly fast transfer times, and the ground-breaking security of the blockchain. If built on the Ethereum platform for example, they can also benefit from smart contracts, further increasing efficiency of trade and therefore offering significant improvements in liquidity.

The less obvious answer, and perhaps one that won't be true for too much longer, is that they avoid much of the regulation that ordinary securities at an IPO undergo, because crypto is a new industry and regulators have not had enough time to adapt. This saves a lot of time and money for the firms running the ICO, as they don't have to worry about complying with the relevant regulations that they would if they were selling ordinary shares. According to a PWC report an IPO cost a firm on average more than \$1million in initial costs, and then a further \$1.5million in recurring costs as a result of being public, compared to an ICO costing around \$50-\$500,000. Not only this, but IPOs are slow, typically taking 2-3 years from the beginning of the process until the company is public; whereas ICOs can be set up in a matter of months. All a startup has to do is create the currency on a blockchain of their choosing, write a white paper of their business plan, and generate interest in the currency, which with the buzz around ICOs right now is always going to be easy.

While great for the firm running the ICO and found good quick solutions for funding their innovative ideas, this could be a major liability for the financial industry as a whole, and therefore this is something regulators are beginning to react to.

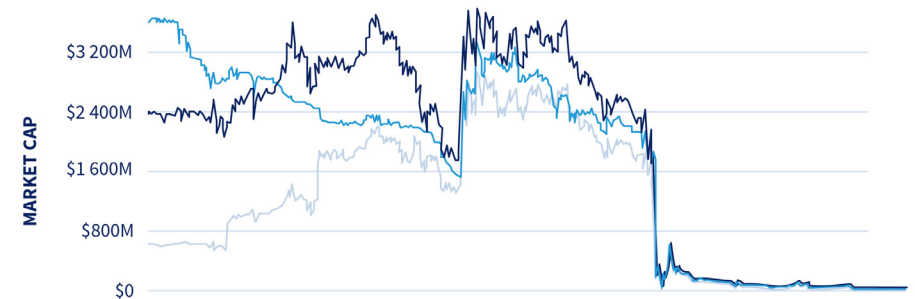
### 11.3 THE NEED FOR REGULATION

As Jeff Garzik, Co-founder of BloqInc, points out, due to the lack of regulation on ICOs and their vulnerability for fraud, “99% of these ICOs will be garbage”. Ordinarily a firm would have to gain approval from the Securities and Exchange Commission before going public with their company, involving detailed checks on the firm’s financials, prospects and potential risks. However, by offering an ICO firms are able to completely bypass this, leaving investors vulnerable to buying into poorly functioning businesses, or even scams.

One of the most famous examples of this was Bitconnect, a crypto currency-lending platform that used its currency, BCC (Bitconnect Coin) as a means of funding via an ICO. The product was marketed well, making use of popular YouTube personalities to advertise, and fuelled by community hype managed to reach a peak of 470 USD per BCC. The firm’s business model was that a user would loan their crypto currency to Bitconnect, and you would get returns back depending on how long the loan was for. It supposedly generated these returns using a volatility trading software – admittedly a legitimate method of generating revenue, but Bitconnect was promising unreasonably high returns of up to 40%, which clearly is unfeasible given normal standards. This led to fears of a Ponzi scheme, and in January of 2018, supposedly due to

“bad press”, Bitconnect shut down its lending platform, essentially making its currency useless. Unsurprisingly the price of BCC crashed, as shown below in Figure 3, falling all the way to just 3.13 USD per BCC. Clearly anyone who invested in BCC will have made significant losses. Under adequate regulation, a firm such as Bitconnect would never have been allowed to go public, and this complete loss of assets for investors could have been avoided.

Figure 3



You could argue that like an IPO investors should do their own homework and due diligence as well and if something seems to be too good to be true, it probably is. The other thing to state here is that it differs quite a bit from country to country or even from continents. As for example in Singapore gambling is a big thing and with ICOs at this early stage, it is more or less a gamble, so the men on the street are easy to persuade to buy into especially with an idea of getting rich very quickly and easy. The other thing to note is that the VC culture in Singapore is quite tough for startups who need funding, most VC’s are reluctant to buy into an idea (alone), they first would like to see the full product before investing, which of course in some cases really is the chicken and egg story.



#### 11.4 THE RESPONSE FROM REGULATORS

In any case, regulators have started to respond. On August 1st 2017, the MAS (Monetary Authority of Singapore) clarified their position of ICOs, and have since published a detailed 13-page guideline ICOs.

The first issue they deal with is the provider of ICOs, attempting to protect against the threat of another Bitconnect. Now, if the MAS considers a coin/token as a security, the provider must:

- Publish a regulation-compliant investment prospectus
- Register it with the Central Bank
- Hold capital markets services license

It is still possible for small ICOs to be exempt if:

- The total offering is < 5 million SGD
- A private placement offer is made to < 50 people
- The offer is only to institutional investors
- The offer is to accredited investors

This mirrors the regulation for an ordinary security, and is immediately a massive burden for small firms. Under this regulation, it is more likely that only legitimate firms with well designed business plans will be willing to face the costs of compliance, and thus should help introduce some confidence to ICO investors.

Another vulnerability in the ICO space is the trading platforms (crypto-exchanges) that the currencies are traded on. Many of these were scams, stealing currency from its users, so clearly regulation was necessary here too. Now any crypto trading platform must be approved by the MAS as a recognised market operator under the SFA

(Securities and Futures Act). If any of you have ever used a crypto-exchange, you will know this involves significant KYC, especially if you want to trade in large volumes.

Similarly, there was no regulation on who could offer advice on crypto currencies, meaning there is no way for consumers to know if the information they are reading is legitimate, so now any firm offering advice on digital tokens will require a financial advisor's license.

To help understand specifically whom this impacts, the MAS have offered some examples.

##### *Example 1 – A Utility Token*

A company is going to use an ICO to raise funds for the development of its platform. The token can be used to access the company's platform, and renting computer power provided by other platform users.

This token will not constitute a security under the SFA, and will not be subject to any requirements under the SFA.

##### *Example 2 – An Equity Token*

A company is going to use an ICO to raise funds for the development of its platform. The token will be a digital representation of a token holder's ownership in the company.

The token will constitute a security under the SFA. The ICO will need to comply with Prospectus Requirements, and the company will need a capital markets service license.

##### *Example 3 – A CIS (collective investment scheme)*

A company is going to use an ICO to raise funds, which will be pooled and invested in a portfolio of shares. The

*“Another vulnerability in the ICO space is the trading platforms (crypto-exchanges) that the currencies are traded on.”*

company will manage the portfolio, and will distribute the profits among the token holders.

This will be considered a CIS, so will constitute a security under the SFA, meaning the ICO will have to comply with Prospectus Requirements, and the company will need a capital markets service license. Additionally, this will have to be authorised under section 286 of the SFA, or recognised under section 287 of the SFA depending on whether the arrangement is constituted in Singapore or outside Singapore, and will be subject to the applicable requirements under Division 2 of Part XIII of the SFA, the SF (OI)(CIS) R and the Code on CIS.

#### *Example 4 – A debenture*

A company is setting up a platform that helps startups raise funds through digital token offerings. Investors will invest by issuing a loan to the company, and in exchange will be given a digital token specific to the start-up that will represent the rights of an investor as a creditor of the loan. The token will be considered a debenture, so will constitute a security under the SFA. The company will need to comply with Prospectus Requirements, and requires a capital markets service license.

On a side note, an interesting development in Singapore is that there are firms who now looking into the KYC processes for ICO's and virtual exchanges. One example is the traceto.io ICO, as it is almost impossible to get sufficient funding through VCs to build this platform the people behind traceto.io decided to do an ICO, the whitepaper promises to assist in the whole KYC process for ICO's and exchanges through the use of blockchain technology, their AML RegTech solution platform and AI, which makes sense since there are so many ICO's going on

and from a risk management perspective, of course ICO's and virtual exchanges need sufficient KYC but in a much faster and secure way. This form of "self regulation" could also become a way to distinguish so called bad ICO's from the good ones.

### **11.5 IN SIMPLE TERMS**

The quick summary is that most forms of tokens in an ICO, whether they are shares, CIS's or debentures, will now be regulated just as an ordinary security would. The exception to this rule is the Utility Tokens, such as UKG, which will remain exempt from such regulations.

It is worth mentioning however that the tokens that fall outside of this regulation, i.e. the utility tokens, may still be subject to AML and anti-terrorism legislation. In particular the MAS highlights two things: the first is that you must report suspicious transactions with the Suspicious Transaction Reporting Office, Commercial Affairs Department of the Singapore Police Force, complying with section 39 of the Corruption, Drug Trafficking and Other Serious Crimes Act, and second is that you must not use the ICO to fund terrorism, complying with the Terrorism (suppression of financing) Act.

The MAS also allows creators of digital tokens to apply for their 'FinTech Regulatory Sandbox', which offers relaxation of certain regulatory requirements for the duration of the sandbox. For a successful application you must use technology in an "innovative way", and obviously have done your due diligence.

*“China and South Korea have taken the most drastic approaches to ICOs in out-right banning them.”*

### 11.6 RECENT NEWS FROM THE MAS

Interestingly, as of March 2018, there has been a push by the MAS to enforce the relevant regulation on ICOs. Extending an initiative to conduct investigations into financial crime set up in March of 2015, the MAS have teamed up with the CAD (Commercial Affairs Department) to enforce compliance with the SFA and FAA, claiming that this will “allow for greater efficiency and more effective enforcement of capital markets and financial advisory offences”. Up until now the focus has been traditional financial misconduct such as insider trading, with a total of 3 convictions being made, but now, with the MAS’ clarified position on digital token offerings, ICOs will be under threat. If tokens that constitute a security are not fully compliant, expect them to be investigated, and similarly crypto-exchanges that do not comply with KYC – a surprisingly common phenomenon - to be shut down.

This is only Singapore’s response however, and in fact regulators globally have come up with very diverse responses to ICOs, so it is worth having a look at the rest of the world too.

### 11.7 WHAT ABOUT THE REST OF THE WORLD?

If we begin by considering the US, we can see their policy is in general quite similar to Singapore. If a token is considered a security, then it will be treated as a security, meaning an ICO will have to register with the SEC and comply with disclosure obligations. However, one interesting difference is that in the US, a token can also be considered a commodity. This regulation stems from the idea that similar other commodities e.g. gold or

silver, a cryptocurrency hold some inherent value (it is able to utilise blockchain technology), and there is usually a scarce, finite supply of the coin. This offers an interesting regulatory coverage for those tokens that escape the security laws – something not yet addressed by Singapore.

In the UK, the FCA (Financial Conduct Authority) has warned that “many ICOs will fall outside the regulated space”, but has said that it will consider each ICO on a case-by-case basis and see if it falls under any relevant regulation. Similar to the US and Singapore, if a token resembles a security it will be treated as a security, and more generally say that if the token issuer’s activities fall under a regulated activity then they will be required to comply.

In mainland Europe the ESMA (European Securities and Markets Authority) have again advised that certain tokens may be considered as securities or financial instruments, and so will be regulated as such. However, there are also specific regulations between different European countries, such as in Germany where crypto currencies are all considered to be financial instruments, or in Sweden, where the central bank is considering the development of a national e-currency.

China and South Korea have taken the most drastic approaches to ICOs in out-right banning them. In September 2017, China published a report saying, “No organisations or individuals shall engage in illegal fundraising through coin offering”, and even required anyone who had raised funds through an ICO to return the funds. Later that month South Korea introduced similar policy, entirely outlawing token offerings for funding. However, just as we write this chapter, South Korea is contemplating another direction and may allow allow ICOs under certain circumstances

Perhaps the most comprehensive regulatory framework exists in Japan. Similar to most countries, Japan has said that if a token resembles a security then it may fall under Japanese security law. However beyond this, as of April 2017 Japan have given a formal definition of a 'virtual currency' and began to regulate them under an amended Payment Services Act. This means ICO operators must register as a 'virtual currency exchange business'. The Japanese FSA admitted there could theoretically be exceptions to this regulation, but that would require the token to be both untradeable and nonredeemable for any other virtual currency or good/service, so realistically this offers a complete coverage of all ICOs.

At this point in time it is safe to say there is significant diversity in regulation throughout the world. One common theme is that most countries are recognising certain types of tokens as securities; however, regulation beyond this is inconsistent. Some countries are more supportive of crypto, such as Sweden and Singapore, even looking to develop their own e-currency, while others are much less so, such as China and South Korea outright banning ICOs.

Meanwhile Japan appears to be leading the way with the most developed regulatory framework at this point in time, offering an official definition of a 'virtual currency' and amending their payments and services act to include them instantly. Naturally then this leads to the question of what the future of ICOs will be like. Will countries take the route of Japan and develop cryptocurrency specific regulations? Or will they stick to the simpler option of reusing existing regulation that they can put ICOs under?

## 11.8 FUTURE

For the short-term future at least it seems that regulators will continue the pattern of trying to find existing regulation that they can put ICOs under. This is what we have seen worldwide with the tokens that resemble a security, where they will simply be required to follow the relevant rules for ordinary securities. However, looking more long-term it is possible that ICOs are better understood by regulators and more countries will follow suite Japan and develop specific crypto currency regulations.

Crypto specific regulations may be necessary because under many current regulatory frameworks the Utility token remains largely unregulated. The positions of the firms offering these tokens is that a Utility Token does not provide a form of investment, as it is simply a redeemable voucher for some products or services, so it should not be treated as such. However, these tokens still exist as a tradable crypto currency that can be exchanged and redeemed for fiat currency, with a variable price level that can go up as the platform expands or the utility of the coin goes up, meaning many people are in fact buying these tokens as investments for the future. This is definitely one of the main reasons why Singapore has put up this detailed ICO guideline and stipulated almost all tokens as 'security' as well as regulating the providers and platforms, however, it remains to be seen whether this will keep people from fraudulent dealings.

Ultimately we can safely say that ICOs are in their infant stage and that further development of the global regulatory framework is necessary, and for sure it will change a lot in the coming years. In the short-term, regulators will likely stick to the trend of applying existing regulation to

ICOs where possible, but long-term it would make sense to develop specific regulations for virtual currencies to offer a more comprehensive coverage of all ICOs. The only certainty seems to be that change is coming, and firms will have to be much more careful if they are considering an ICO in the future.

# 12

## *Open Source Development*

*Steven Gort and  
Giulietta Marani* <sup>139</sup>

<sup>139</sup> Steven Gort works for ICTU, a not-for-profit foundation within the Dutch Government. As the assigned “data whisperer” he is one of the driving forces behind Discipl, an information platform for a future digital society in a resource based economy. Giulietta Marani works as advisor and account manager at ICTU. Her main areas of expertise are innovation, new technologies, security and organization’s learning ability. She is part of the Discipl team.

Distributed technologies (such as blockchain technology) are catalysts that force authorities to view the everyday situation from other perspectives. Force them to employ other paradigms. It challenges these authorities to reconsider all known and trusted (legal) frameworks, institutions and interests of the system world that is being created. Back to the drawing board. Back to the government’s intentions and their constitutional basic principles.

The technological developments are advancing at a rapid pace and many new concepts and technologies follow each other in quick succession. Software products resulting from this are protected on the basis of copyright and, as such, cannot be reused without the permission of the rights holder. To protect their economic position, the rights holder also often chooses to make the software products available as closed source even when these products have been developed by order of a government. In contrast, open source is actually an important driving force behind many successful technologies. Open source technologies lie, among other things, at the foundation of what we now know as the internet. Moreover, many of the programs we use on a daily basis have been developed on the basis of open source technologies. Android OS and Apple MacOS, for instance, are based on the kernel and Unix open source technologies respectively.

For the entire range of public services we argue in favour of arranging the intellectual property and reuse of software in such a way that everyone can reuse, alter and share the source code for free. In short, of only allowing open source. If it involves public funding, then it should also involve public code!

We want to create an open source ecosystem, an informal network that revolves around solutions that are already available or that can be reused in different context(s) with some adjustments.

This will be created around the platform Discipl<sup>140</sup>:

1. a platform for automated information services for and by society;
2. it allows for exploration of a new socio-economic environment with innovative business models that support all manners of cooperation;
3. it works towards a new generic digital infrastructure (GDI) that is future-proof and in which information is processed, shared and stored via a virtual source in real time;
4. it guarantees privacy and security by design and offers points of reference for far-reaching ethical issues that are approaching slowly but surely.

Contributing and participating in the Discipl open source ecosystem first and foremost means working with the same moral compass:

1. We create sustainable, highly automated solutions that provide for the needs of people;
2. Solutions can be produced, installed and used (for free) relatively easily;
3. Solutions are open source, with a Creative Commons licence or GPL version 3.01;
4. Solutions apply the Discipl Pattern;
5. We respect current legal frameworks.

<sup>140</sup> <https://www.ictu.nl/nieuws/discipl-technologie-voor-een-samenleving-van-de-toekomst#>

## 12.1 DISCIPL PATTERN

The Disciple Pattern is not about a foundation for the business logic and information management attempted to be safeguarded by legislation and regulations with respect to privacy and digital human rights. We feel that this open government will be created when we create solutions from the ground up according to a non-violent need fulfilment pattern.

This begins with acknowledging the fact that solutions are always universal transactions between sovereign people whose existence cannot be denied and on whom you can never impose anything. Need fulfilment is the focus.

This takes place through universal peer-to-peer transactions for which there is always a transfer of something with true value, yet which does not involve money. The nature of this value is determined by the context of applicable legislation and regulations. The transaction is executed by means of a decision made in a group discussion between all parties involved via Convergent Facilitation<sup>141</sup> and on which everyone is actually prepared to agree.

If such transactions are automated in an extensively automated economy of abundance, then it makes sense that parties involved mostly use distributed applications on their own devices, such as smartphones, to interact with others and share information.

In situations in which all people in society need to be represented in the decision to be made, the application can automatically guide the conversation in a transparent manner towards only the decisions that can be made according to the automatic but uniformly interpreted

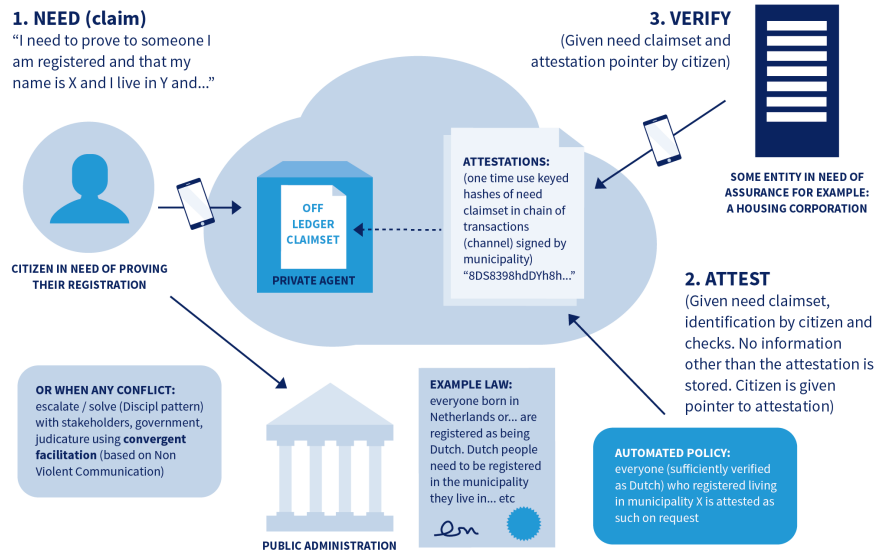
<sup>141</sup> Organisations, communities, neighbourhood groups, political parties or any entity we can think of where people meet (as in our suggested open source ecosystem); there is a universal need for cooperation that is both inherently human and effective. In a brief video Miki Kashtan explains (<https://youtu.be/I12WUUD96Es>) what convergent facilitation is.

It should, however, always be possible for parties involved to disagree, after which it should be possible to automatically escalate the transaction to a suitable committee consisting of peers from, for example, the local community. For example, a randomly selected group of enthusiasts who are experienced with the context and can help come to a supported decision, or so-called circles as intended in the proposal for a global governance system<sup>142</sup> submitted by Miki Kashtan in the context of a call for this by the Global Challenges Foundation.

<sup>142</sup> <http://thefearlessheart.org/resources/local-to-global-collaboration/>



196



More information can be found on:

<https://discipl.org/proof-of-registration-haarlem/>

The aim is to work towards a 'GitHub' and 'AppStore' for innovation of public service provision.

See: <http://discipl.org>

## 12.2 OPEN SOURCE ECOSYSTEM

Government organisations try to amass knowledge and experience with service provision and business operations of the future from many different places. In the open source ecosystem, ICTU wants to help governments to innovate in an inter-administrative manner with a learn-do-share environment and a collective intelligence network in which government organisations together can explore

new impactful developments and defining technologies, amass (cross-industry) knowledge, create prototypes, and use the knowledge, prototypes of learning experience of others.

The ecosystem determines what can be explored and invests – with people, money and/or tools. ICTU offers a (legally) safe experimentation environment and connection with the market and knowledge institutions should these be missing. Together, the ecosystem develops new methods and techniques (Proof of Concept, knowledge products, training, etc.) for the government. Participating parties offer different stages to each other for the ecosystem in order to share ideas as well as learning and practical experiences.

In ICTU's experimentation environments, governments are free to develop new ideas to solve a problem and to look into new technologies (use cases). Moreover, they can use the existing digital building blocks, such as the identity framework.

Based on the administrative experiences with the various blockchain pilots initiated by Marloes Pomp and Koen Hartog, we had to idea of creating an administrative Tech Team. The team consists of high-level civil servants and, if necessary, external experts. It helps, among other things, the Council for Public Administration to come up with answers with respect to a fundamental reorientation of the political culture.

The ecosystem provides know-how to guarantee the quality of experiments and solutions and to steer towards reuse (and even which solution could be the new standard for the government). The administrative Tech Team filters,

*"The ecosystem determines what can be explored and invests – with people, money and/or tools. ICTU offers a (legally) safe experimentation environment and connection with the market and knowledge institutions should these be missing."*



prioritises, takes final responsibility and guarantees the necessary care in public service provision and legitimacy of changes.

### **12.3 CHANGE IN SYSTEM CONTROL**

This requires a different perspective of administrative responsibility. The advice of the Council for Public Administration states that it is important to change from system responsibility to system control; from a hierarchical system with one person with final responsibility to shared responsibility of all parties involved in the system. In which each party, irrespective of it being a public or private party, can be made accountable for their contribution to the whole. It means that parties need to discuss their tasks and roles in the whole much more. Everyone's contribution to the whole is the focus, contrary to, for example, the traditional approach in which parties behave like partners in a chain. In which input and output between chain partners are at the centre instead of the effects they wish to achieve in the service provision through the chain.

This also applies to fast prototyping of new ideas in beta states. The intended permanent beta is the new foundation for the efficacy and efficiency of the government's business operations. At the same time, it lies at the basis of the customer experience of good public service provision. In short, there are no more distinctions between mass primary processes and individual customised solutions. And the supporting tools for this public service provision are never 'finished'.

The route to be followed to achieve this is a route along making the whole bigger than the sum of its individual

parts. It is what has come up briefly in the introduction of the desired ecosystem and what Nick Szabo formulates nicely in his blog Money, blockchains, and social scalability. He outlines which mental efforts are required to achieve such an ecosystem in the first place. Social scalability, as he calls it, is the power to leave the institutions, to shed ourselves of cognitive limitations and to let go of the ingrained behaviour patterns.

### **12.4 MANIFESTO ON SHARED INNOVATION FOR PUBLIC SERVICE PROVISION**

Cooperation with shared responsibility requires new rules, especially within a government that follows the Public Enterprises (Market Activities) Act. ICTU has formulated rules that allow for combined and radically transparent public-private open source innovation without any compromises.

#### **12.4.1 The game and the rules**

##### *Objective*

1. The goal is to improve public service provision by reusing solutions. To this end, together with everyone who wants to participate, we are building a library filled with open source government software that is accessible to everyone without restrictions and free of charge.
2. The software in question never stops developing (permanent beta).

##### *Basic idea*

3. New initiatives for the development of software are published on the Disciple website.

4. These initiatives will also be announced via leading IT websites.
5. All products end up in the Discipl library.
6. In case of personal data, every participant complies with the relevant legislation and regulations.
7. All other information that becomes available during development is public.
8. No single party can exercise intellectual property rights.
9. A participant makes their knowledge, experience and time available at their own initiative.
10. The parties are free to donate to make the activities in this manifesto possible.
11. When information and/or results are lost during the development, then this is at the risk of the participating parties.
12. If parties have a conflict, they must work it out amongst themselves.

*Registration and cooperation without financial consideration*

13. Every company can register for participation in an initiative or can start their own initiative.
14. Companies need to be prepared to execute projects with other participants.
15. Companies can be linked to other companies via Disciple to improve cooperation.
16. Every company can stop participating in the development and/or work with other companies on the same initiative.
17. Participation in development is performed by a participant without financial considerations.

*Registration for development that requires an incentive*

18. If the development of a specific initiative does not advance, then a one-time subsidy with a maximum of € 50,000 can be granted over a period of two months.
19. In most cases, the government organisation benefiting from the initiative in question will grant this subsidy.
20. The company or combination of companies that registers and that is most distinctive in a number of criteria announced beforehand on the Discipl website for the initiative in question will be granted the subsidy.

**Note**

*This manifesto contains the description of the current playing field. If it turns out that new elements are required, then the community manager will introduce these in deliberation with all participating parties.*

# Author

## biographies



**Aanchal Anand** is a Land Administration Specialist in the Global Land and Geospatial Unit of the World Bank. She has worked on Bank-financed land projects and analytical studies in over 15 countries across Eastern Europe, Central Asia, Middle East, and East Asia. She has been leading her team's work on blockchain applications for land. Prior to the World Bank, she worked as an investment banker in London and as a corporate strategy professional in New Delhi. Aanchal has a BSc in Economics from the London School of Economics and an MA in Economics and International Relations from the Johns Hopkins University School of Advanced International Studies.

**André de Kok** works as an architect working at the National Office of Identity of the Netherlands ministry of Interior and Kingdom Relations. His ambition is to give every human being a save and secure place in the digital world.



**Baloko Makala** is the Policy and Legal stream Lead at the World Bank Group Technology and Innovation lab. She has worked extensively in Technology and Public policy fields.

**Benedetta Audia** has been in the UN system for twelve years and is currently working with the United Nations Office for Project Services (UNOPS) as Corporate Legal Advisor and Head of the Commercial and Institutional Law Practice. Benedetta is also an Adjunct Professor of Procurement in International Development at George Washington University and a Visiting Professor of Public International Law at LUISS University.





**Giulietta Marani** works as advisor and account manager at ICTU - a not-for-profit foundation that operates as independent digital services consultant and executor within the Dutch government. Her main areas of expertise are innovation, new technologies, security and organization's learning ability. She is part of the ICTU's Discipl team.

**Jeroen Naves** works as an attorney at the Dutch law firm Pels Rijcken & Droogleever Fortuijn. He specializes in IT and data protection law and is known for his knowledge about the legal aspects of disruptive technologies, as blockchain, artificial intelligence and Internet of Things. Jeroen regularly publishes on technology and law. The whitepaper he co-wrote about the legal aspects of blockchain has been rewarded with the PON Essay Award 2017.



**Koen Lukas Hartog** is the program manager of Blockchain-projects.nl, the blockchain program that was developed in collaboration with the Dutch government. Since 2016, Blockchainprojects.nl developed more than 40 blockchain projects for more than 30 governmental organizations. In addition, Blockchainprojects.nl has organized several blockchain missions to Singapore and the US.

**Marjolein Busstra** holds a PhD in human rights law. She has extensive experience in foreign policy and international relations, having fulfilled a number of roles in the Netherlands diplomatic service. She currently works for the international law section of the Dutch Ministry of Foreign Affairs on human rights and cyber related issues. Marjolein has a special interest in the interplay between technology and human rights.



**Matt Stack** is a founder of XLP Capital, the founding manager of the Lambda Prime Venture Funds, and the Chief Investment Officer of XLP's technology equity and credit investments at Devonshire Capital Funds. He is an experienced early and seed stage investor in high tech hardware and analytics companies with over \$250M in completed deals, and serves as a technology advisor to a variety of institutions and family offices overseeing and directing over \$800M in assets. In addition, he serves as the lead cryptocurrency and blockchain advisor to the United Nations, where he advises governments on technology and central banking policies.

**Mona Zoet** is the Founder and CEO of RegPac Revolution Pte. Ltd, a Regulatory Technology Ecosystem builder and Digital Knowledge Platform. After working for more than 15 years around the globe in top tier Financial Institutions, such as JP Morgan (Hong Kong), State Street (Boston, USA), Lloyds Banking Group (NYC, USA) and Bank of America Merrill Lynch (Singapore), she set up her own company ThinkMola, a boutique regulatory compliance & risk management consultancy firm, in Singapore. Furthermore, Mona is an Executive Board Member, Southeast Asia Lead and Singapore Chapter President of the International RegTech Association (IRTA) which exists to ease and accelerate the evolution of the RegTech industry.





**Olivier Rikken** MSc MBA graduated at Delft University of Technology on Simulation of Logistics Systems and later did his Executive MBA At Nyenrode Business University/ Kellogg School of Management/Stellebosch Business School on the effect of strategy changes on various business elements. Starting his career in transport and logistics, later in consulting and finally in the financial sector, always responsible for strategy, process improvement (Lean Six Sigma) and IT development. Nowadays he is director blockchain and smart contracts at AXVECO working on sustainable blockchain innovation implementations. Furthermore active for the Dutch Blockchain Coalition, member of the ISO smart contract standardization workgroup, advisor to various (blockchain) startups and entrepreneur.

**Paul Oude Luttighuis** works for Le Blanc Advies as an advisor architect for various clients in various fields.




**Sandra van Heukelom-Verhage** is a lawyer at Pels Rijcken & Droogleevers Fortuijn, the State Advocate of The Netherlands. She heads the Digital Transformation team, which main goal is to improve the Dutch innovation climate. The team published the whitepaper Legal Aspects of Blockchain. Sandra also heads the Project Board of the Dutch Blockchain Coalition, a public-private initiative. The Dutch Blockchain Coalition tries to stimulate the large scale deployment of blockchain technology in The Netherlands. Sandra is co-writer of the Report Smart contracts as specific application of blockchain technology.

**Steven Gort** works for ICTU, a not-for-profit foundation that operates as independent digital services consultant and executor within the Dutch government. As the assigned “data whisperer” he is one of the driving forces behind Discipl, an information platform for a future digital society in a resource based economy.



**Yoshiyuki Yamamoto** is the Special Advisor for UN Engagement and Blockchain Technology at UNOPS, and the most senior UN official working in this field. He explores the application possibilities of blockchain technology for the United Nations and international aid work. Yoshiyuki is the former Director of UNOPS Peace and Security Centre. He has more than 25 years of experience in the United Nations system, mainly in humanitarian assistance and peacekeeping operations, and has spent 15 years working in various fields in Pakistan, Afghanistan, Jordan and Iraq.



15 authors from around the world  
discuss the legal implications that  
blockchain has – and may have –  
on humanitarian and development  
work as well as existing regulatory  
frameworks, data and identity.