Ohnesorge, Jan

**Working Paper**

# A primer on blockchain technology and its potential for financial inclusion

Discussion Paper, No. 2/2018

**Provided in Cooperation with:**
German Institute of Development and Sustainability (IDOS), Bonn

*Suggested Citation:* Ohnesorge, Jan (2018) : A primer on blockchain technology and its potential for financial inclusion, Discussion Paper, No. 2/2018, ISBN 978-3-96021-057-3, Deutsches Institut für Entwicklungspolitik (DIE), Bonn, https://doi.org/10.23661/dp2.2018

This Version is available at:
https://hdl.handle.net/10419/199522

d·i·e

Deutsches Institut für Entwicklungspolitik

German Development Institute

Discussion Paper 2/2018

# A Primer on Blockchain Technology and its Potential for Financial Inclusion

*Jan Ohnesorge*

# A primer on blockchain technology and its potential for financial inclusion

Jan Ohnesorge

Bonn 2018

Discussion Paper / Deutsches Institut für Entwicklungspolitik
ISSN 1860-0441

Die deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at http://dnb.d-nb.de.

ISBN 978-3-96021-057-3 (printed edition)

DOI:10.23661/dp2.2018

Printed on eco-friendly, certified paper

**Jan Ohnesorge** is an associated researcher in the research programme "Economic and Social Systems" at the German Development Institute / Deutsches Institut für Entwicklungspolitik (DIE).

*Published with financial support from the Federal Ministry for Economic Cooperation and Development (BMZ)*


Tulpenfeld 6, 53113 Bonn
☎ +49 (0)228 94927-0
🖷 +49 (0)228 94927-130
Email: die@die-gdi.de
http://www.die-gdi.de

## Acknowledgements

Peter Wolff and Kathrin Berensmann provided guidance at a very early stage of this report and encouraged me to focus my research on blockchain technology. Peter Wolff, moreover, provided support and guidance during the entire research process.

At an internal presentation of preliminary findings, Jakob Schwab, Christoph Sommer, Jonas Keil, Peter Wolff and Kathrin Berensmann provided valuable feedback. In addition, I am grateful to my colleagues at the DIE Sören Hilbrich, Heiner Janus, Kathrin Berensmann and Peter Wolff for providing very valuable comments on various drafts of this paper. Special thanks go Nick Gogerty for commenting on Section 2 of this paper and providing indispensable feedback on technical issues. Robert Furlong edited the text and greatly improved its reader-friendliness. Finally, I would like to thank Verena Kauth, Kira Petters and Lea Jechel for formatting the references and Cornelia Hornschild for coordinating the entire publishing process.

Bonn, January 2018 Jan Ohnesorge

Contents

# Abbreviations

| | |
|---|---|
| AML/CFT | anti-money laundering/combating the financing of terrorism |
| ASICS | application-specific integrated circuit miners |
| DAO | Decentralized Anonymous Organization |
| GPU | graphics processing unit |
| IOT | internet of things |
| IOU | promise of payment (abbreviated from the phrase “I owe you”) |
| MTO | money transfer operator |
| NEM | New Economy Movement |
| SDG | Sustainable Development Goal |
| PoI | proof of importance |
| PoS | proof of stake |
| PoW | proof of work |
| UNL | unique node list |
| USD | United States dollar |
| USDT | crypto currency version of the US dollar |

## Executive summary

The development of Bitcoin marked the advent of blockchain technology in 2008/2009. The pseudonymous developer of Bitcoin was the first person to solve the "double-spend problem" (i.e. the problem that simple digital files representing monetary units can be copied and spent twice). In conventional digital payment systems, the central actor (e.g. a bank) ensures that monetary units can only be spent once. By inventing a blockchain-powered solution to the double-spend problem, Bitcoin was able to create the first international payments network that does not need a central party. The crypto currency operates on a peer-to-peer basis.

In all blockchains, transactions (or other forms of data) are bundled in blocks, which are cryptographically interlinked. Due to this, the manipulation of a certain block is visible in every block that is created on top of this block. Additionally, the blockchain is stored on the computers of a large number of network participants, so manipulation is made even harder due to the sheer number of copies of the ledger. Since the advent of Bitcoin, blockchain technology has rapidly progressed, and today hundreds of functional crypto currencies exist. In fact, blockchains are today only a subset of "distributed ledger technologies". All functional distributed ledger technologies guarantee a high level of immutability and are stored on many computers across the network. This is not always achieved by bundling transactions in blocks, however. Nevertheless, the shorter term "blockchain" is often (including in this paper) used when distributed ledgers are meant, and the differentiation between the two terms is not relevant for the argument being made. This discussion paper gives an overview of some important forms of distributed ledger technology, using concrete crypto currencies as examples. It thereby aims to equip the reader with an intuitive understanding of the different technologies as well as their benefits and drawbacks.

In the early days of Bitcoin, the full potential of the technology behind it was not yet clear. Today, distributed ledger technology is often characterised as the "internet of trust", referring to its usefulness for a very broad range of applications. This discussion paper focusses on (i) the role of crypto currencies to enable international payments, and (ii) blockchain-powered land registries. Note that the former use case is the "traditional" form of blockchain technology. Existing distributed ledger networks enable very low-cost international remittances, while the exact rates depend on the concrete currency pair. The latter use case – blockchain-powered land registries – covers a more recently developed field of application: the use of blockchain technology to improve government services. The advantages of both types of use cases include a high level of immutability and a reduction in transaction costs. Although international payments are an essential part of financial inclusion, there are reasons to believe that blockchain-powered land registries could also foster financial inclusion. In fact, a reliable stewardship of land titles enables their use as collateral. This is essential for increasing credit access for people in developing countries.

The flip side of blockchain technologies' innovative nature is that it comes with new types of risks. An important part of these risks stems from the fact that many blockchain networks (including Bitcoin) are not organised as decentrally in practice, as was originally envisioned. Quasi-central entities in the network face the same IT risks as banks (e.g. the risk of getting hacked by cyber thieves). In addition, these actors were sometimes not as professionally organised, at least in past years. Due to this, many crypto currency investors lost (parts of

their) investments. Regulators' efforts to address these issues by applying consumer and investor protection measures to the field should be intensified. It is also important to counter the illicit use of certain crypto currencies and concealing services that claim to offer anonymous digital transactions. On the other hand, regulators should not ignore legitimate needs for privacy, as the entire transaction history (but not the personal details of network members) of many crypto currencies is publicly available. Keeping in mind the universal, indivisible and interlinked nature of the Sustainable Development Goals, an environmental risk of blockchain technology should not be omitted: certain types of blockchains (including Bitcoin) have extremely high energy consumption levels. Government agencies and other actors can avoid this environmental externality by using low energy-intensity variants of the technology (Sections 2.2-2.4). The high levels of volatility of many crypto currencies are an economic risk, which can also be avoided by using less-volatile alternatives (e.g. crypto currencies that are pegged to the US dollar).

When aiming to use distributed ledgers to foster financial inclusion, it is essential to keep in mind the diversity of the technologies and their properties. Efficiency losses and a suboptimal user experience are the likely consequences of solely focussing on the most well-known forms of distributed ledgers. Regulators should follow a proportionate approach that balances the benefits and risks of the many forms of this groundbreaking technology.

# 1 Introduction

In 2008, an individual or a group that used the pseudonym Satoshi Nakamoto published the article "Bitcoin: A Peer-to-Peer Electronic Cash System". The article outlines the functional principle of the first crypto currency, whose software would be released in 2009. The creation of a truly peer-to-peer (i.e. without a trusted central party) electronic cash system was, up to that point, an elusive task for software developers. One of the main challenges for developers was the effortless duplicability of digital files, which leads to the "double-spend problem": conventional digital files meant to be used as monetary units can, unlike physical forms of money, be easily copied and given to multiple recipients, thus completely compromising the scarcity – and thereby the value – of the currency. In the absence of a technical fix to the double-spend problem, trusted central parties such as banks, money transfer operators (MTOs) (e.g. Western Union), internet payment companies (e.g. PayPal) and mobile network operators (e.g. Safaricom[1]) are needed to ensure that money can only be spent once within their respective electronic systems. Satoshi Nakamoto solved the double-spend problem for Bitcoin by inventing what was later to be called a "blockchain", thereby eliminating the need for a trusted central party.[2]

The name "blockchain" refers to the fact that all transactions are bundled in blocks. The Bitcoin network, which is not only home to the first crypto currency, but also the first application of blockchain technology, produces new blocks about every 10 minutes. These blocks are cryptographically interlinked, so that a manipulation of a certain block is visible in every block that is created on top of this block. Additionally, the blockchain is stored on the computers of a large number of network participants, so manipulation is made even harder due to the sheer number of copies of the ledger.

In addition to blockchains, the advent of Bitcoin has inspired the development of diverse "distributed ledger technologies", which share a high level of immutability and security. Blockchains are actually a subset of distributed ledger technologies (see Figure 6), but the terms are often used interchangeably. Unless the distinction is relevant for analytical purposes, this paper uses the shorter term "blockchain technologies" more often.

Due to this solution to the double-spend problem, crypto currencies, which are enabled by distributed ledgers, seem to have the potential to revolutionise the finance sector. One of the lowest-hanging fruits is (international) payments. Access to payments and the ability to safely store money are surely essential parts of financial inclusion. If crypto currencies were a widely accepted form of payment internationally, people could just transact across borders, and the beneficiaries could spend the crypto currency on the products and services they demand. This way, they could avoid paying high fees to MTOs, such as Western Union. Currently, one does not observe universal acceptance of crypto currencies in any country, but there are blockchain-powered innovations in the remittance market that create benefits under current market conditions (Section 3.1). In addition, blockchain technology is

1 Safaricom operates the mobile payment system M-Pesa in Kenya (Safaricom, 2017).

2 Two noteworthy precursors of Bitcoin were Wei Dai's b-money and Nick Szabo's Bitgold, which were both conceptualised in 1998. Neither of the two concepts was implemented, but especially Bitgold is conceptually similar to Bitcoin. Important innovations of Bitcoin over Bitgold were the incentivisation of transaction processing and increased security, that is, resistance to sybil attacks (Bitcoinwiki, 2016a; Peck, 2015).

beginning to spur innovation in the insurance and lending sectors (e.g. Ether World, 2017; Lorenz et al., 2016).

However, blockchain technology has a broad potential that goes beyond purely financial applications. The technology effectively enables people who do not trust each other to transact with each other without the need for a trusted third party.[3] Due to this feature, *The Economist* (2015) described blockchain technology as a "trust machine". The trust creation is made possible by a high level of immutability and can potentially lead to large reductions in intermediation costs. Examples of sectors that the technology may substantially change include value chain management (IBM, 2016), various services of the sharing economy or even the automation of firms (Tapscott & Tapscott, 2016). Blockchain technology could also improve government services such as identity management (e.g. Bitnation, 2017), humanitarian aid (Tapscott & Tapscott, 2016) or land registries. The quality of land registries in many developing countries in particular could benefit from the high level of immutability that blockchain technology offers. A trustworthy land title is not only important for securing the rights of private and business property owners, but also to further their financial inclusion (Section 3.2).

The remainder of this paper is structured as follows: Section 2 simplifies the operating principles of different distributed ledger technologies and aims to convey an intuitive understanding of how they work, without diving so deep as to explain mathematical formulas. Nevertheless, the section does contain some level of technical detail, because the author believes that understanding some details is necessary to be able to judge realistically the potential and risks of the technology. All too often, blockchain technology is seen as a trust-creating black box, which may lead to incorrect expectations.

Building on this foundation, the potential of the technology for financial inclusion is analysed in Section 3 by using the examples of (international) payments and land registries. Whereas payments are an important part of financial inclusion, the connection to land registries is indirect. However, there are convincing arguments as to why land registries are very important for fostering access to credit. This example was chosen because it illustrates the broad potential of blockchain technology.

In most cases, new technologies not only come with unexplored potentials, but also with new types of risks. Section 4 discusses the security, immutability and privacy of distributed ledger systems, focussing on security risks as well as the externality of high levels of electricity consumption and price volatility of crypto currencies. Section 5 concludes and gives some regulatory recommendations. An important general finding of this paper is that the potential as well as the risks of blockchain technology vary widely across the different types of distributed ledgers and their concrete implementation.

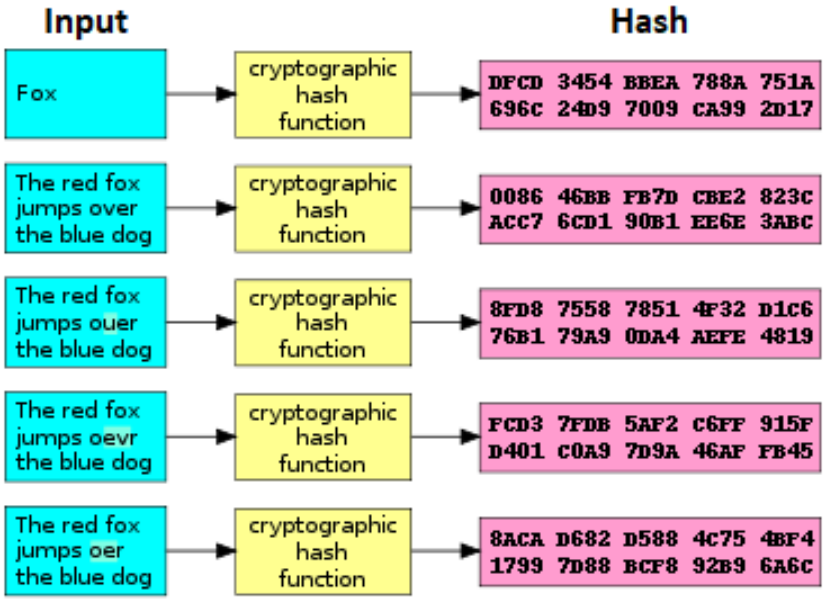
3 Whether this holds true in practice depends on the concrete design of the blockchain (see Section 4.1).

## 2 What are blockchains and distributed ledgers?

All distributed ledgers use "consensus mechanisms" to reach agreement over "shared data in peer-to-peer networks" (this definition is a slightly modified version of the one from Van Valkenburgh, 2017). There are closed distributed ledgers, but with the exception of ledgers for land registries, this paper focusses on open forms, which are fully accessible to the public. As mentioned in the introduction, blockchains are a subset of distributed ledgers.

To prevent the manipulation of data stored in the ledger, cryptographic techniques that link all pieces of data are applied. An important element of distributed ledgers are hashing functions. A hash is a fingerprint of data. It is generated using mathematical rules that convert an input of any length into a fixed-sized string of letters and numbers. Figure 1 illustrates how similar inputs are transformed – by using the cryptographic "secure hash algorithm 1" (more commonly known as SHA-1) hash function[4] – into hashes that look very different from each other. To verify that a given hash correctly represents the input, one only has to run the hash function on the input, which is easy to do, computationally. However, it is practically impossible to find out what the original input is if one only possesses the hash.[5]

**Figure 1: A cryptographic hash function**




Source: Wikipedia (2017, slightly modified)

Distributed ledger systems differ significantly, and especially so regarding their consensus mechanisms. Therefore, it seems more useful to describe some actual approaches rather than explain the general idea of distributed ledgers in more detail. In the following, it is explained

4 This particular hash function is no longer secure (see footnote 5), but it is still useful for illustrative purposes.

5 This is true as long as the cryptographic hash function is secure. Some hash functions have been shown to be insecure in the past. Future developments such as the advent of quantum computers could make several more of them insecure (Castor, 2017).

how Bitcoin, Ethereum, NEM, Ripple and IOTA work in order to equip the reader with a sense of different distributed ledger technologies.

## 2.1 Bitcoin

This section illustrates the functioning principle of Bitcoin using an example that largely builds on information provided in Nakamoto (2008) and Bitcoin.org (2017).

To transfer an amount of Bitcoin, user Alice needs to know a Bitcoin address[6] of the desired recipient, Bob, and sign the transaction with her private key. The private key functions as a password that is cryptographically associated with her Bitcoin address. To make sure that her transaction is processed (in a timely manner), she includes a variable transaction fee. The price of the transaction fee is determined by supply and demand. Thus, Alice signs the transaction, which specifies Bob's address, as well as the transaction fee and broadcasts it to the network.

In the next step, so-called miners[7] individually collect all valid transactions that they would like to process and bundle them into a new block proposal. Blocks may not exceed the maximum block size, which is currently 1 megabyte (Madeira, 2017). All miners transform their respective block proposal into hashes, aiming to be the first miner to create a hash that fulfils a certain rule: to make it difficult to calculate a permissible hash, there is a requirement that the hash has to start with a certain number of zeroes. To enable this, a "nonce" (a **n**umber that is **o**nly used o**nce**) is part of every block. The only known way to calculate the hash of a block in accordance with the required number of zeroes is to change the nonce to a discretionary number, calculate the hash and repeat the procedure until the hash meets the requirement. This proof of work (PoW) consensus algorithm is purposefully computationally intensive in order to deter attackers (see the section on network forks below).

When a valid hash of a new block is found, the miner broadcasts his or her new block, and the other miners normally accept the block, provided it adheres to all the rules (e.g. the block size limit). The successful miner receives a reward that is made up of a bounty of newly "mined" Bitcoins, as well as the combined fees of all the block's transactions. If Alice's transaction to Bob was included in this block, Bob receives the payment. However, in order to not have the transaction end up in a network fork, he waits until a sufficient number of blocks are mined on top of the block that contains Alice's transaction before confirming the payment. The more blocks he waits for, the more confident he may be that his block is not part of a network fork (six blocks is often deemed sufficient).

6 It is standard practice to use a new Bitcoin address for every transaction one receives in order to enhance security and privacy. In addition, if an address is used to send Bitcoin to another address, the remaining balance does not remain at the original address, but is transferred to a newly created address. This is normally done automatically by Bitcoin wallets (Bitcoinwiki, 2016b, 2017c).

7 This simplified example omits the role of full nodes, which distribute new transactions to Bitcoin miners and check the validity of transactions and blocks (Bitcoinwiki, 2017b). In the Bitcoin white paper, the roles of full nodes and miners are not split, but this division of labour emerged later (Nakamoto, 2008).

**Box 1: A short history of Bitcoin mining**

When Bitcoin was created in 2009, the mining was typically done on regular PCs using the central processing unit (CPU). Oftentimes, Bitcoin users ran the mining software on their computers when they had spare capacity. However, it was quickly discovered that graphics processing units (GPUs) were more efficient at Bitcoin mining, and the first computers were outfitted with up to six GPUs to maximise the income generated by mining.

In 2012, the first specialised computers for Bitcoin mining were introduced. The application-specific integrated circuit miners (ASICS) increased the efficiency of Bitcoin mining by a factor of 10. ASICS quickly pushed GPUs out of the market and fuelled the building of big data centres that are specialised to mine Bitcoin (ForkLog, 2016). These datacentres were predominantly built in China, where they are powered by a cheap and coal-dominated energy mix. ASICS are constantly optimised, and their typical lifespan is only a few months, after which they are replaced by the next generation of more-efficient devices (Down & Hutchinson, 2015). The casual observer may be tempted to think that the rapid efficiency gains of mining hardware should at least bring down the levels of electricity usage of Bitcoin, but this is not the case. Instead, the rising Bitcoin price is motivating more actors to invest in Bitcoin mining, which is fuelling extremely high and rising levels of electricity consumption (Section 4.2).

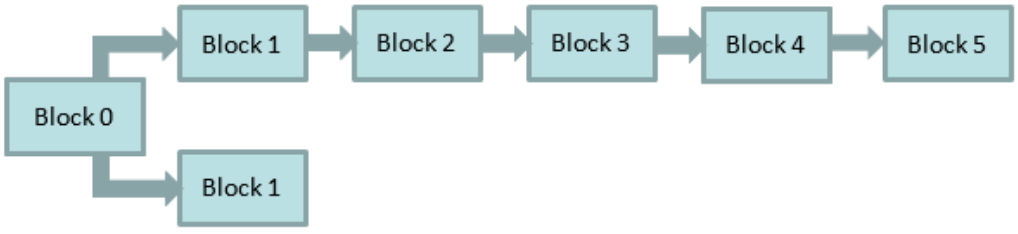
Along with technical improvements, the organisational level of the miners also rose. Today, most mining is done through mining pools, that is, associations of miners that are formed to generate a relatively steady stream of income for miners, instead of getting a big reward occasionally (Coindesk, 2014). An increasingly popular way to invest in Bitcoin mining is to engage in so-called cloud mining, which means renting part of a Bitcoin mining data centre to receive the Bitcoins it mines.

## Network forks

Instead of forming a part of the main chain, a block can also turn out to be part of a fork. This happens quite regularly by coincidence, but forks may also be created purposefully in order to attack the system.

When two miners (almost) simultaneously broadcast a new block, a temporary fork appears (Figure 2). The information about the two new blocks may not be distributed evenly across the network, so that some miners will receive the upper block 1 first, whereas others will be informed about the lower block 1 first.

**Figure 2: Normal occasional forking**

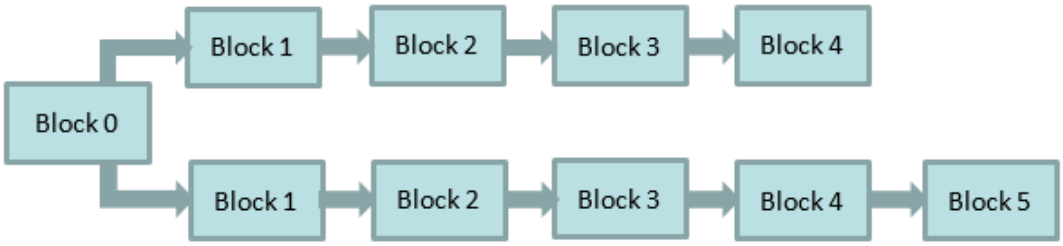



Source: Based on Bitcoin.org (2017)

Miners will typically start mining on top of the block that they received first. When the next valid block is mined, the stalemate is resolved, and any miner who mined on top of the unsuccessful branch will switch to the successful one. This procedure is called the "longest chain rule". Stale blocks may be a nuisance to miners because, if they happen to mine a block that turns out to be stale (i.e. part of a fork), they will not be able to spend their mining reward. However, they are not a security threat as long as they are not deliberately produced to attack the network.

It is purposefully made difficult to find new blocks in order to avoid attacks that aim to rewrite part of the transaction history and double-spend an amount of Bitcoin. Such an attack is called an "alternative history attack", and it is feasible if a miner controls a significant portion of the computational power of the Bitcoin network. To see how this would work, consider Figure 3.

**Figure 3: Rare extended forking**




Source: Based on Bitcoin.org (2017)

Let us assume the attacker spent 10 Bitcoins in the upper block 1 of the blockchain and immediately received a good or service in return. He could subsequently create a fork by mining the lower block 1 and include a transaction that spends the same 10 Bitcoins again. This is possible because, in this fork of the blockchain, the funds have not been spent by him yet. The chances of successfully completing this attack by making the lower branch the longest chain are dependent on the share of computing power that the attacker controls. Additionally, the more blocks that are mined on top of the upper block before the attacker has received the goods or services and can start to create the fork, the harder it is to successfully conduct such an attack. If the attacker consistently controlled the majority of the mining capacity, he could enlarge his fork of the network up to the point in block 5, whereby his branch would become the longest chain. Under the stated conditions, this is ultimately possible no matter how long the lead of the main network is that he has to catch up with.

It should be noted that there can be extended forks, which are legitimate. For example, forks can also be formed as a result of a split of the network on the question of which new rules to introduce. Bitcoin Cash, which can be seen as another version of Bitcoin with slightly different features (see Table 1 in Section 2.4), is the most prominent example of such a fork (The Economist, 2017a). Another reason for a non-fraudulent fork is disagreement on whether to rewrite the transaction history to undo a malicious transaction (Section 4.1).

*Future development*

Bitcoin developers plan to introduce the "Lightning Network", which will provide pre-funded payment channels that are rooted in the blockchain. Alice and Bob may, for example, decide to put one Bitcoin in their shared channel (this would be recorded on the blockchain). Each time Alice wants to pay Bob (or vice versa), they both have to sign the transaction, but this is not recorded on the blockchain, but only in the Lightning Network. Each party can unilaterally end the payment channel, and the current balance is recorded on the blockchain (Lightning Network, s.a.). Due to the designation of funds to a specific payment channel, the Lightning Network is best suited for small and recurrent transactions. Its advantages include reduced transaction fees and increased transaction speed (Section 2.4).

## 2.2 Ethereum and NEM

*Ethereum*

Ethereum ranks second among crypto currencies after Bitcoin in terms of market capitalisation (Coinmarketcap, 2017). However, it is more than a crypto currency due to the network's strong ability to host smart contracts.

**Box 2: Smart contracts**

Smart contracts are digital programs that embed contractual clauses. Their performance is mediated by technological means, and they are irrevocable. Smart contracts can fully replace the functionality of conventional written contracts or complement them by automating a certain aspect of a contract (R3 and Norton Rose Fulbright, 2016).

Perhaps the simplest example of a smart contract is a vending machine (Szabo, 1997). A more recently implemented example that was also foreseen by Szabo (1997) is the automatic accessing of (rental) cars. As soon as you fulfil your contractual obligation (e.g. submit your credit card information and agree to let the car rental block a certain amount on it), a program recognises this fact before technological elements of the car (e.g. an automated lock) enable you to access it using your smartphone. These examples clearly show that smart contracts function independently of blockchain technology. However, the concept is seen as a very interesting complement to blockchain technology, because it enables blockchains to decentrally organise more complex issues than exchanging a virtual currency. To stay with the above example, blockchain-enabled smart contracts could enable an automated peer-to-peer car rental. Car owners would only need to specify the availability and rental price of their car, build in an automated lock and leave collecting the payment and proving access to the car to the smart contract. However, the example of a peer-to-peer index insurance is more relevant for developing countries in the short term. Index insurances pay out a certain premium if a certain index (e.g. a certain number of days without rain) hits a certain level, regardless of actual outcomes for insurance takers (e.g. if the harvest of a farmer was compromised by the insufficient rainfall). This type of insurance is often feasible when other forms are not, because it does not suffer from adverse selection and moral hazard problems (Banerjee & Duflo, 2012). A blockchain-powered smart contract that enables an automated (peer-to-peer) index insurance could increase competition and drive down prices for index insurances. In fact, a "hackathon" challenge to design such a system on a non-peer-to-peer basis was published by Swiss Re (2017). The high irrevocability of smart contracts is especially important in this context, because it gives unknown insurance providers a means to credibly guarantee full payout in case the index hits a certain level. In fact, payout is completed automatically, so insurance takers do not need to trust individual insurance givers, but only the accuracy of the smart contract and the weather station. On the other hand, insurance givers also do not need to trust insurance takers to pay their instalments in time, because the smart contract could automatically inactivate it in case of unpaid instalments. These examples show that smart contracts enable blockchain technology to decentralise a broad array of services, including internet of things (IOT) devices such as smart locks and smart weather stations.

A discussion of smart contracts would be incomplete without touching upon the risks of the technology. Relatively simple contracts are often very hard to translate into computer code, and small coding errors can have disastrous consequences (see Section 4.1 for an example). In addition, the legal status of smart contracts is unclear in many jurisdictions. An example in German law is that highly complicated smart contracts (e.g. contracts where you transfer certain decisions to an artificial intelligence) are facing legal scrutiny because, according to the Federal Supreme Court, "machines/ software cannot make [the obligatory] valid declaration of intent" (R3 and Norton Rose Fulbright, 2016, p. 42). Thus, a legal person has to take responsibility for the actions of an artificial intelligence and has to act as a contracting party (which poses some limits on the automation of the contract). In addition, legal ambiguities may also arise if it is questionable whether a contracting party has more than a "vague appreciation of what the smart contract does or provides for" (R3 and Norton Rose Fulbright, 2016, p. 43). The short-term relevance of these limits and ambiguities may seem to be low, but a fully automated organisation that worked on the basis of smart contracts already existed (and failed) in 2016 (see below). It follows that these insecurities are already starting to matter today. One can argue that very complicated smart contracts ought to be forbidden, but regulators should definitely provide legal certainty.

Ethereum's current consensus algorithm is PoW. Although the consensus mechanism is technically different from Bitcoin's, it requires the solution of difficult-to-solve mathematical problems (Github, 2017). However, its developers are planning to slowly shift to a proof of stake (PoS) system. PoS essentially awards the right to create a block to users, depending on their committed funds in the respective crypto currency. If you, for example, stake 0.1 per cent of the coins of a pure PoS crypto currency, you would be allowed to create one block in a thousand. This would give you the right to collect the transaction fees as well as a possible block creation reward. The exact mechanism that determines who gets to create which block varies from implementation to implementation. However, in general, "stakers" select the transactions they would like to include and electronically sign them. In contrast to PoW, this process requires fewer calculations, and therefore less energy.

The Ethereum developers plan to introduce a PoS system in the near future called Casper, which will initially only be used to create every 100th block in the blockchain, while the rest of the blocks will still be mined using PoW (Edwards, 2017). Two whitepapers that describe the technical and economic features of the shift were published in 2017 (Edwards, 2017). A problem with a very simple PoS system is that, unlike in PoW systems, it is not costly to create blocks on different forks of the network simultaneously. This would enable double-spend attacks. Casper solves this problem by financially penalizing forbidden behaviour such as signing blocks on different branches of the blockchain. This is done by requiring potential block creators to contribute a large sum of "Ether" (Ethereum's crypto currency) into a security deposit. Should any user of Ethereum notice fraudulent behaviour, they may red-flag this and automatically receive a small share of the offender's security deposit. The rest of the offender's security deposit will automatically be destroyed. Thus, if an attacker aims to conduct an alternative history attack, she would have to repeatedly invest a large amount of money. This seems to be a convincing system, and time will tell whether it functions reliably. If Ethereum successfully manages the transition to a PoS system, this would drastically reduce the energy consumption levels of the network (Section 4.2). In addition, this could also increase the transaction capacity of the network and reduce transaction costs (Edwards, 2017). A successful shift to PoS could potentially also spark interest in the Bitcoin community, which is consuming even more electricity and is experiencing higher transaction costs as well as lower transaction capacity.

*NEM*

A consensus algorithm that builds on PoS has been demonstrated to work well for the crypto currency NEM (New Economy Movement). NEM ranks 10th among crypto currencies in terms of market capitalisation, as of 19 November (Coinmarketcap, 2017). Its consensus mechanism is called proof of importance (PoI) and takes into account the amount of XEM (the currency of NEM) a user owns, but also net transfers to and from other NEM members, as well as other graph theoretic[8] measures of importance in the network (NEM, 2015).

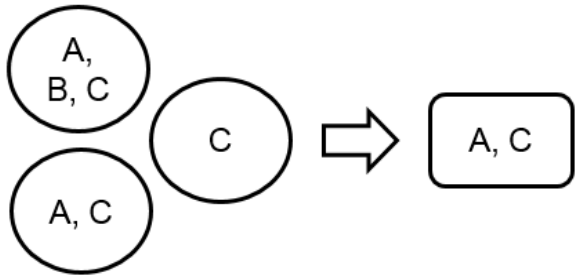
8 Graph theory is used in such diverse fields as social network research and neuroscience to determine the importance of nodes.

## 2.3 Ripple and IOTA

*Ripple*

Ripple and IOTA (ranked fourth and eighth, respectively, among crypto currencies in terms of market capitalisation; Coinmarketcap, 2017) are distributed ledger systems, but not blockchains (see Figure 6 for an overview). Ripple works with a voting-style consensus mechanism that allows gateways (mainly banks and other public institutions) to vote on the veracity of the transactions proposed by users. Gateways check the veracity of transaction proposals that they receive from users and put all valid transactions up for vote. Then they vote on all transactions that their unique node list (UNL) approves of. This list is a subset of all gateways chosen by the Ripple algorithm, or by gateways themselves in order to minimise the likelihood that the members of that group collude to attack the system. Voting is normally done automatically using an algorithm that is controlled by each gateway. The process of voting takes place in several rounds, in which transaction proposals are distributed in the network and any mutually conflicting transactions are eliminated. Transactions that do not meet the minimum quorum of approval, which increases each round, are discarded. In Figure 4, for example, the quorum of approval is 60 per cent, and the UNL consists of three gateways. As transaction proposals A and C fulfil this quorum, they pass this round and are voted upon again in the next round, whereas transaction proposal B is discarded.

**Figure 4: Voting-style algorithm**




Source: Author, based on Cohen, Schwartz and Britto (2017)

All transactions that at least 80 per cent of a gateway's UNL approve of in the last round are added to the ledger. To ensure that all UNLs of the network come to the same result in the last round, a minimum level of connectivity between gateways needs to be ensured (Schwartz, Youngs, & Britto, 2014).

Another noticeable feature of the Ripple network is that it not only allows for the trading of its native currency, Ripple, but it also allows gateways to issue digital representations of (fiat) currencies or other assets of value. These so-called IOUs (abbreviated from the phrase "I owe you") may then be traded freely among participants of the network. The settlement of IOUs takes place outside of the Ripple network, so the acceptance of issuances requires trust in the issuer. However, the Ripple network automatically creates trust paths to exploit the fact that even people who do not trust each other can pay each other if they are connected through intermediaries, which form a line of trust. For example, if Alice accepts Bob's IOUs and Bob accepts Carol's IOUs, then Carol can automatically give an IOU to Alice through Bob. However, if Alice later wants to swap the IOU for actual money, she would ask Bob to pay her outside of the Ripple network in exchange for deleting the IOU. If he does so and Carol does not live up to her IOU to Bob, Bob will have to bear the loss. Thus, participants

must carefully choose which actors they trust up to which amount, because otherwise they may incur losses, even without actively taking part in any transactions. For this reason, IOUs from reputable institutions are preferred by many users. Ripple allows these institutions to collect a transfer fee (e.g. 0.2 per cent of the amount transferred; Ripplewiki, 2014).

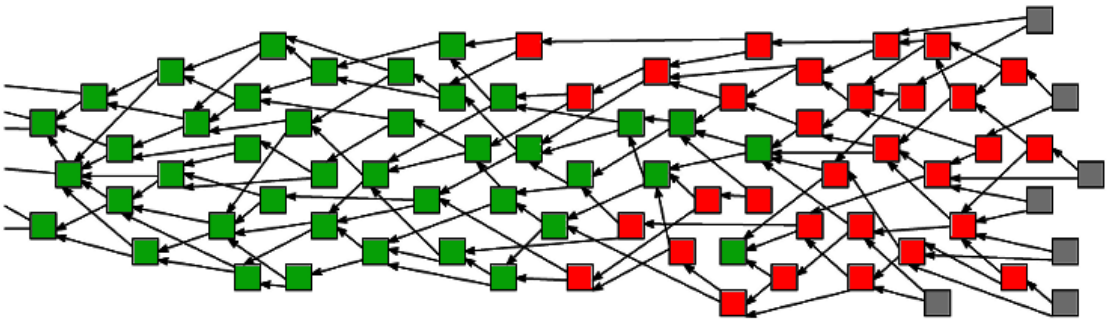
In reality, the trust paths that Ripple establishes are much longer than in the above example, and many users accept IOUs as they would accept money – thus rarely, if ever, asking to swap IOUs for money outside the Ripple network. As long as all trusted parties honour their IOUs, Ripple is an efficient and universal system to transfer any currency (or other type of intangible asset) internationally.

Ripple is set up as a company and cooperates intensively with banks, which has raised some criticism in parts of the blockchain community, due to their aim to decentralise financial services completely. However, Stellar works very similarly, but it is set up as a non-profit organisation and has a broader focus regarding cooperation partners (Stellar Development Foundation, 2017). Stellar ranks 17th among crypto currency in terms of market capitalisation, as of 23 November (Coinmarketcap, 2017). NEO also uses a voting-style algorithm, but, in contrast to Ripple and Stellar, it focusses on the provision of smart contracts (Table 1).

*IOTA*

IOTA uses a directed acyclic graph – better known as the "Tangle" – as a consensus mechanism. In contrast to a blockchain, there are no blocks; instead, each transaction confirms two previous transactions. In Figure 5, all the grey blocks are unconfirmed transactions, which each confirm two other transactions. In contrast, the green blocks are confirmed by the entire network, while all the grey blocks indirectly confirm all the green blocks. The red blocks are confirmed by parts of the network. The level of confirmation the receiver requires to accept payments is subjective, but for very large transactions, 99 or 100 per cent is advisable.

**Figure 5: The "Tangle"**



Source: Schiener (2017)

The system secures transactions using PoW. However, in contrast to Bitcoin and Ethereum, the levels of difficulty and associated electricity consumption levels of calculating hashes are so low that transactions can be completed on simple transacting devices (e.g. on a smartphone) in a few minutes. So although there are no reliable estimates regarding the power consumption of an IOTA transaction, it is clear that IOTA is – by magnitudes – more energy-efficient than Bitcoin, Ethereum or any other major PoW-powered blockchain. A reason for this low level

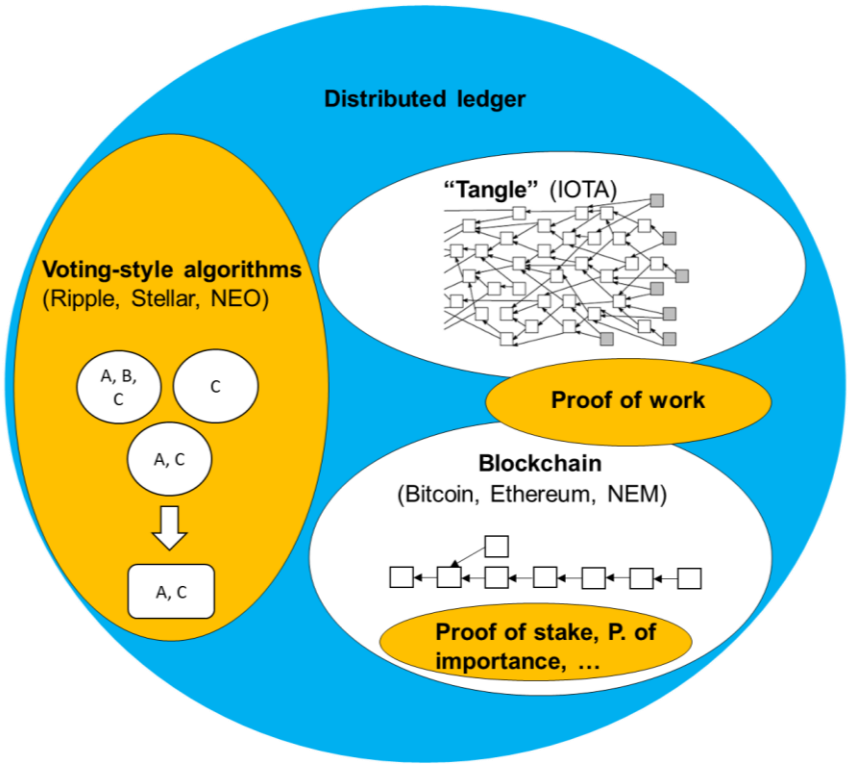
of energy consumption is that there is no competition to be the first to complete the PoW, as it is computed by each network participant for every transaction (Falls, 2017; Popov, 2017).

Because there are no intermediaries involved to bundle and verify transactions, IOTA works without any transaction costs, which makes it suitable for micro transactions. In addition, it has a high transaction capacity due to the absence of block size limits. Another remarkable feature is the high partition tolerance of the network. It is possible for devices that are connected by local networks to transact between them and only register their transactions a few times a day with the main Tangle online. These features enable IOTA to process the transactions of IOT devices, which are expected to pay very small sums to each other (e.g. to pay for short-term internet access) without being connected to the internet at all times (IOTA Foundation, 2017). On the other hand, the zero cost and high-capacity features are also appealing to human users (e.g. remittance senders).

## 2.4 Comparing different distributed ledger technologies

Figure 6 gives an overview of different distributed ledger systems.[9] Relatively widely used consensus algorithms (coloured orange) and data structures (coloured white) are displayed.

**Figure 6: Venn diagram of distributed ledgers**




Note that all arrows represent confirmations (of blocks or transactions respectively). Thus, their direction is opposite to the arrows in Figures 2 and 3.

Sources: Author, based on Bitcoin.org (2017), Cohen et al. (2017), Github (2017), NEM (2015), NEO (2017a), Scott (2017), Stellar Development Foundation (2017)

9 The Venn diagram is bound to be incomplete due to the dynamic developments taking place in this field.

The most frequently used consensus algorithm is PoW, which is used in many blockchains, including Bitcoin (Section 2.1), but also in the Tangle, as implemented in IOTA (Section 2.3). In PoW systems, one has to perform complex calculations in order to be able to create ledger entries. Alternative consensus algorithms, which are used in blockchains, include PoS and PoI. In PoS systems, one has to stake a certain amount of crypto currency to be able to create ledger entries. PoS is planned to be introduced in Ethereum (Section 2.2), but this will not be the first PoS implementation. For example, the crypto currency Nxt (ranked 28th in terms of market capitalisation, as of 13 December 2017) was designed to accommodate for PoS. PoI systems aim to gauge the importance of a user to the system and allocate the right to create ledger entries accordingly. PoI is implemented by NEM (Section 2.2.). Voting-style algorithms, in contrast, let validators vote on the validity of transactions in several rounds until a threshold of agreement is reached.

Data structures displayed in Figure 6 include the blockchain and the Tangle. In blockchains, validators (miners in the case of PoW blockchains) confirm transactions by creating blocks on top of the last block that is created (Section 2.1). In the Tangle, every participant of the network validates two previous transactions (Section 2.3). The data structure of voting-style algorithms is similar to that of a blockchain, in that transactions are bundled and recorded in cryptographically linked ledger entries. However, using voting-style algorithms, no forks may appear, because each voting round has only one unambiguous outcome.

To illustrate the differences in performance of different distributed ledger systems, concrete crypto currency networks are analysed in the following. Table 1 compares the main features of the top 10 crypto currencies in terms of market capitalisation. Differences across currencies are considerable in all dimensions. Whereas transaction fees and average transaction times are indicators that influence customer satisfaction, transaction capacity is an important indicator of the ability of a crypto currency to scale up and become a mainstream payment mechanism. An often-cited – and up to now unreached – benchmark is the transaction capacity of the VISA payment network, which can process up to 45,000 transactions per second (Coindesk, 2017a).

In terms of electricity consumption, PoW blockchains are wasteful when compared to conventional payment systems or all other described distributed ledger systems. This includes the Tangle, which also uses PoW but is not structured as a blockchain. From a sustainable development perspective, the extremely high levels of electricity consumption of the two largest crypto currencies – Bitcoin and Ethereum, the latter of which is at least planning to switch to PoS – is particularly worrying. The additional feature column shows that some of the biggest crypto currencies go far beyond the enabling of payments. Especially Ethereum and NEO are more accurately characterised as universal platforms for smart contracts that also provide a crypto currency functionality. It should be mentioned that smart contracts can also be implemented on other distributed ledgers, including Bitcoin, but the support for smart contracts on these platforms is limited. The only additional feature that is not unambiguously positive is the increased level of privacy that the crypto currency Monero provides. There are, of course, legitimate reasons for demanding these features, but an anonymous digital form of money is obviously appealing to many sorts of criminals, too (Section 4.1).

Table 1 shows, that the biggest crypto currency, Bitcoin, is constantly grouped among the currencies with the worst characteristics. An important reason for this could be that Bitcoin was the pioneer, and its successors were able to optimise their currencies after analysing Bitcoin's strength and weaknesses. One can imagine that it is easier to build an improved

crypto currency from scratch than to upgrade an existing system. However, it is not surprising when a pioneer is overtaken by competitors, but rather that it is technically superseded, yet continues to dominate the market. Bitcoin is the number one crypto currency and has a market share of about 55 per cent, as of November 2017. This is in spite of average transaction fees of USD 7.32, which make the currency more expensive than some conventional international remittance services, let alone the national payment options. For example, eight conventional remittance providers offer cheaper rates for sending USD 500 from the United States to the Philippines (World Bank, 2017a). This makes the crypto currency look more like an investment vehicle than a competitive payment mechanism (Section 4.3). However, the introduction of the Lightning Network may change this situation, as it would at least drastically improve performance in terms of all four dimensions for small and recurrent transactions (Section 2.1).

Table 1 highlights the enormous performance differences between the 10 biggest crypto currencies.

**Table 1: The 10 biggest crypto currencies**

| Crypto currency | Average transaction fee in USD | Average transaction time | Transaction capacity per second | Energy efficiency | Additional features |
|---|---|---|---|---|---|
| 1. Bitcoin | 7.32 | 9-10 minutes | 7 | Low (PoW blockchain) | |
| 2. Ethereum | 0.22 | 14 seconds | 20 | Low (PoW blockchain) | Supports smart contracts |
| 3. Bitcoin Cash | 0.32 | 9-10 minutes | 50 | Low (PoW blockchain) | |
| 4. Ripple | 0.0000024 (+ IOU fee)[10] | 3.5 seconds | 1,000 | High (Voting-style algorithm) | Enables IOU transactions in any currency |
| 5. Litecoin | 0.15 | 2 minutes | 56 | Low (PoW blockchain) | |
| 6. Dash | 0.30 | 2-3 minutes | (4,000)[11] | Low (PoW blockchain) | |
| 7. NEO | None (+ variable fee)[10] | A few seconds | 1,000 | High (Voting-style algorithm) | Supports smart contracts |
| 8. IOTA | None | No data available | 500-800 | Rather high (PoW Tangle) | Especially suited for IOT devices |
| 9. Monero | 2.43 | 2 minutes | 1,700 | Low (PoW blockchain) | Advanced privacy features |
| 10. NEM | 0.21 | 30 seconds | (3,000)[11] | High (PoI blockchain) | Integrated reputation system |

Note that this table is based on data from 20 November 2017. It represents a snapshot and may be subject to significant changes within short time spans. Furthermore, the accuracy of the data on transaction times and capacities varies and is in some instances only based on estimates. It should, however, give the reader a feeling for the rough dimensions of the speeds and capacities of the listed crypto currencies.

Sources: Alfaroq (2017), BitInfoCharts (2017), Cyberblock (2017), Mastermined (2017), NEM (2015, 2016), NEO (2017c), Steemhoops99 (2017)

10 The transaction fees are set to zero/ a fraction of a cent in NEO and Ripple, respectively, but users may choose to pay a fee to prioritise their transaction (NEO, 2017b) or to use IOUs of trusted organisations (Ripplewiki, 2014).

11 For Dash and NEM, no current data on current transaction capacity is available. The data refers to the transaction capacity of planned improvements (Alfaroq, 2017; Mastermined, 2017).

## 3 The potential of distributed ledger technologies for financial inclusion

The 2030 Agenda for Sustainable Development puts a focus on financial inclusion as a means of alleviating poverty; several Sustainable Development Goals (SDGs)[12] address this issue. The empirical case for the effectiveness of promoting broader development goals by fostering financial inclusion has been getting stronger in recent years. Robust studies that demonstrate an impact on poverty reduction (Banerjee & Duflo, 2012; Suri & Jack, 2016) are beginning to emerge: "Financial inclusion means that individuals and businesses have access to useful and affordable financial products and services that meet their needs – transactions, payments, savings, credit and insurance – delivered in a responsible and sustainable way" (World Bank, 2017b).

This definition encompasses a broad spectrum of basic financial services. Crypto currencies generally enable transaction, payment and store-of-value (i.e. savings without interest payments) services. Transaction costs and price volatility vary from implementation to implementation though (Table 1 and Section 4.3). Distributed ledger technology also has the potential to reform services such as interest-earning savings (B2BPay, 2017), credit and credit ratings (Bloom, 2017; Lee, 2017) and insurance. An important tool to program such systems are smart contracts (see Box 2, also for an exemplary blockchain insurance service). In addition, blockchain technology could revolutionise identity-management systems, thus overcoming an important impediment to financial inclusion.

Access to a transaction account is of special importance for financial inclusion, as it provides a possibility to store money as well as send and receive payments, and it serves as a gateway to other financial services (World Bank, 2017b). In 2011, 2.5 billion people did not have an account,[13] according to World Bank estimates. By 2014, financial inclusion expanded rapidly, reducing the figure to 2 billion people. The advent of mobile banking contributed to this success, particularly in sub-Saharan Africa, where 12 per cent of adults were using mobile money accounts. In the region, 45 per cent of mobile money account holders did not have an account at a bank or financial institution, so their only access to financial services was mobile money (Demirguc-Kunt, Klapper, Singer, & Van Oudheusden, 2015).

A good replacement for access to a transaction account could be access to a universally accepted and secure crypto currency. It would enable payments, offer the possibility to store money and could also provide a gateway to other financial services (blockchain-powered or not). Crypto currencies do not generally have formal access restrictions, but user-friendliness (e.g. password recovery mechanisms) could be improved. This might also increase adoption rates, which are arguably the biggest hindrance to fulfilling the game-changing potential of distributed ledgers. Nevertheless, blockchain technology has a home advantage concerning national as well as international remittances, which are discussed in Section 3.1. Simple financial services (i.e. payments and a store-of-value) are both (i) relatively easily provided through existing blockchain technologies and (ii) an indispensable part of financial inclusion. Moreover, the emerging distributed ledger and blockchain technologies are often viewed as being the most significant universal innovations since the

12 According to my count, six of the seventeen SDGs (Goals 1, 2, 3, 5, 8, 9) directly address issues of financial inclusion. The respective targets are 1.4; 2.3; 3.8; 5a; 8.10; 9.3 (United Nations, 2015).

13 This includes accounts at a bank or another type of financial institution, or with a mobile money provider.

advent of the internet (Lorenz et al., 2016). To also showcase a non-financial application of the technology, blockchain's potential for improving land registries is analysed. The connection of land registries to financial inclusion may not be obvious, but officially registered property is a very important form of collateral. Thus, better land registries may contribute towards improving access to credit (Section 3.2).

## 3.1 National and international remittances

International remittance flows to developing countries (USD 440 billion, as of 2015) are responsible for about three times the amount of official development assistance flows (USD 131 billion, as of 2015) (Organisation for Economic Co-operation and Development, 2017; World Bank, 2017c). Do these large funds also have an impact on development outcomes? A literature review (Adams, 2011) shows that "international remittances generally have a positive impact on poverty and health in the developing world", whereas their effect on labour supply, education and economic growth can be negative. The development outcomes of poverty alleviation and health improvements are clear ends in themselves, whereas labour supply and economic growth are means rather than ends. Education has important means as well as ends components, but it should be clear that, on an individual level, the absence of severe illnesses and the absence of extreme poverty are preconditions for attaining any meaningful level of education. Thus, the total positive development impact of remittances is quite clear, despite possible negative side-effects. Even if one disagrees with this reasoning, one should support low remittance prices, as long as one is committed to achieving the SDGs: Target 10.c aims to "reduce to less than 3 per cent the transaction costs of migrant remittances" by 2030 (United Nations, 2015).

Mobile banking drastically reduces the cost of offering payment services by avoiding the costs of brick-and-mortar branches. At the same time, it offers obvious benefits of convenience and reduces transport costs, especially in villages (people no longer have to go to town to handle their financial affairs). It seems reasonable to expect that mobile banking has further contributed to bringing down the number of people without an account since 2014. Are crypto currencies able to further reduce the costs of payments and migrant remittances in the face of such a recent and impactful technological revolution in the sector?

The answer very much depends on the crypto currency one has in mind, as the average transaction fee varies from more than USD 7 to absolutely free (Section 2.4). A disadvantage that all currently available crypto currencies share is that they require an internet connection, possibly through a smart phone, whereas mobile payment systems only require a regular mobile phone. In addition, using crypto currencies is sometimes not very user-friendly and requires a relatively high level of technical know-how, although this is quickly changing (see the example of Abra below); the technical barriers for usage are definitely higher for crypto currencies than for mobile payment systems. In addition, the regulatory capacity of a government and its willingness to accept a certain level of risk under a proportionate approach to regulation are important factors. Regulators will not only influence adoption levels of crypto currency-powered payment mechanisms, but also the development of a crypto-financial-services ecosystem.

The higher technical barriers for using crypto currencies also apply in the field of migrant remittances. Mobile money companies are increasingly adding international remittances to

their services. The average cost reductions they offer vis-à-vis conventional MTOs range from 50 to 21 per cent, depending on whether the recipient makes use of the cash-out service or keeps the money in a mobile account (GSMA, 2016). Despite this positive development, in the third quarter of 2017, the global average cost of sending remittances was 7.21 per cent of the amount sent (World Bank, 2017a). These high costs mean that the disruptive potential of crypto currencies is much higher in the remittances market than in the payments market.

Could blockchain technology lead to substantial cost reductions in the remittances market? The most important cost driver of remittance companies is the operation of cash collection and distribution locations. These costs may come in the form of commissions to local agents or as salaries and rents, depending on the business model (Kalan & Aykut, 2005). Although a blockchain-powered money transfer can operate without branches, this is also possible with digitised transfers that do not use a blockchain. In fact, incumbents such as Western Union as well as start-ups such as TransferWise and WorldRemit offer cashless services that rely entirely on sending money online or through a mobile phone, thus circumventing the costs for running brick-and-mortar branches. However, blockchain solutions offer another advantage over conventional digital solutions. Remittance services working through the internet or using mobile money both use the banking system (typically correspondent banks) to settle cross-border transactions (Committee on Payment and Settlement Systems & World Bank, 2007; Daly, 2010). Due to this, it takes several days to settle transactions. MTOs nevertheless offer (premium-priced) express services, which guarantee same-day or nearly instant delivery. By holding large amounts of local currency, the local MTO representative is able to give out funds to recipients and gets refunded some days later. Although it enhances convenience for the consumer, this pre-funding increases capital costs. Blockchain-powered cross-border payments do not rely on the banking system to transfer money across borders, so transactions are settled within minutes – or even seconds – instead of days. This brings down capital costs and lowers entry barriers for start-ups, which intensifies competition.

On the other hand, blockchain-powered solutions that use a crypto currency to transfer money require two currency conversions instead of one (e.g. euro to Bitcoin to Indian rupee, instead of euro to Indian rupee). Blockchain transaction fees may also be an issue, depending on the crypto currency one uses. The currency conversion fees are not necessarily large, as exchange rate markups of intermediaries can be very low if the market is highly liquid.

The peer-to-peer payment service Circle proves that blockchain-based cross-border payments for zero fees and zero exchange rate markup are possible today. The service is currently only available in the United States, Great Britain and several euro zone countries, but the company plans to expand its network to China. Circle states that it is able to offer its Ethereum-based service for free (they offer the mid-market rate to their customers) due to its crypto currency treasury and trading operations (Neville & Allaire, 2016, 2017). This makes sense if one considers that currency treasury and trading require the ability to purchase currency as cheap as possible and sell it as expensive as possible. Thus, Circle profits from being able to buy/sell currency from/to their customers, because they would otherwise have to pay higher/ sell for lower prices. Cashaa has a similar business model and offers its low-cost crypto currency-powered service in 141 countries.

In addition, Stellar offers the transfer of IOUs in any currency globally for a fraction of a cent (Ripple works with a similar technology but markets it primarily to banks instead of end users; see Section 2.3). Although the payment app Abra charges somewhat higher fees,

it provides an innovative technical solution for customers who prefer to use cash to pay for the remittance or who want the receiver to get the money in cash. The system is based on Bitcoin transactions, but users do not necessarily have to buy Bitcoins on their own. Instead, they can use the services of "Abra tellers", who act as one-person exchanges between Bitcoin and local currency cash in sending and receiving countries, respectively (Light, 2017).

National – and especially international – remittances is an area where transformational change is already happening with existing distributed ledger technologies. The first user-friendly apps and online services that offer international payments for free or for very low costs exist. These and other innovative distributed ledger companies that have yet to present their solutions to the public may be expected to attract a considerable share of the remittances market in the coming years. However, as of now, the technology is only suitable for remittance senders and receivers that are connected to the internet.

## 3.2 Land registries

The Peruvian economist Hernando de Soto is a seasoned proponent of strengthening property rights in developing countries to fight poverty. He coined the term "dead capital" to describe assets that lack formal property rights, and therefore cannot be easily traded or used as collateral for credit (de Soto, 2000). Due to the missing titles, dead capital is also subject to a looming threat of expropriation, which may discourage investment. De Soto's early work on property rights and informality – for example, the empirical finding that it took 289 days to open a small business in Peru in 1983 – has inspired the development of the World Bank's "Doing Business" report. Since its second edition in 2004, the report contains a section on registering property (World Bank, 2016). In this area, digitising the land registry turned out to be an especially effective measure for speeding up transfer processes. Between 2010 and 2015, 37 economies digitised their land registry. This led to a 38 per cent reduction in the time needed for registering a property transfer in these countries, compared to a 7 per cent reduction in countries that did not digitise their land registries (World Bank, 2016). The next promising step that builds on digital data could be to put (parts of) the land registries on a blockchain.

Even small improvements may have a considerable effect in this field, as the volume of global dead capital is estimated by de Soto to be USD 20 trillion, which is held by 5.3 billion people worldwide (Arsenault, 2016; Bne IntelliNews, 2017). This massive lack of property rights has far-reaching economic consequences. Fixing this issue could, according to de Soto, lead to "Chinese or Indian growth rates worldwide" (Casey, 2016). However, this enthusiasm is not undisputed. Williamson (2010) splits de Soto's reasoning into two hypotheses and conducts a survey of the empirical literature to test both: "1) Property rights impact development by altering the ability and incentives for capital formation, 2) Land titling provides the means to secure property rights."

Whereas the first hypothesis is largely uncontested in the empirical literature, the evidence on the second hypothesis is mixed.[14] Kerekes and Williamson (2010) identify a potential

14 Williamson (2010) explains that three out of six studies that investigate whether or not land titles lead to higher investment rates find significant effects.

reason for the limited effectiveness of land titles: private banks in Peru do not trust land titles enough to grant their holders any advantages over holders of untitled land. In fact, Peruvian private banks use informally and formally owned land as collateral. To compensate for the perceived insecurity of the collateral, banks charge interest rate premiums, irrespective of the existence of land titles. Kerekes and Williamson (2010) argue that a failure of the state to enforce property rights could be the reason for this surprising finding.

It is therefore important to stress that a blockchain land registry must be embedded in functioning enforcement mechanisms to effectively secure property rights. These conditions are currently not being met in many developing countries, where the situation is characterised by disputed land rights and dysfunctional legal enforcement mechanisms. Note that crypto currencies do not typically have to rely on enforcement mechanisms other than their own code-based mechanisms against malicious activities. The virtual token (e.g. Bitcoin) itself is the valuable object, which enables software to protect it. Only if this protection fails – for example, if an attacker succeeds in stealing the private key of a Bitcoin address – are state enforcement mechanisms (i.e. the police and courts) needed. In contrast, a land registry contains titles, that is, abstract representations of physical valuables that are outside the registry. Thus, all current proposals for distributed ledger land registries that the author is aware of (sometimes implicitly) rely on state enforcement mechanisms to function properly.

The alternative to this would be a software- and hardware-enabled enforcement mechanism of property titles, that is, to digitise the access to properties. This could potentially be achieved using so-called proplets: electromechanical devices that "control physical objects with digital protocols" (Szabo, 2001). In the case of buildings, proplets could be integrated in doors to digitally restrict access to anyone who is not the owner. The owner would be identified on the blockchain. However, a critical attribute of proplets, as described by Szabo (2001), is entanglement. The proplet should be so entangled with the property it protects that it is prohibitively costly to remove it from said property. This requirement seems to be difficult to fulfil, given the high value of buildings and the land they are built on. It is indicative that Szabo (2001) mentions cars and even weapons of mass destruction, but not property as being exemplary use cases for proplets. Thus, in the foreseeable future, property registries will depend on state enforcement mechanisms.

In addition, the initial creation of ledger entries cannot be fully automated and requires a functioning judicial system to guarantee that conflicting claims to a given property are legally settled before the property enters the distributed ledger. Arruñada (2017) points out that producing reliable information is indeed the main challenge for property registries and that blockchain technology does not seem to be able to solve this problem. Once the ledger is set up, the transfer of property tokens could theoretically be handled analogously to the transfer of Bitcoins or other crypto currency tokens. However, this would lead to enormous problems if a cryptographic key to a property token were to be lost or stolen (Mizrahi, s.a.). Due to this and other reasons, projects that aim to migrate the land registry of a country to a distributed ledger usually try to design a more sophisticated system that does not fully rely on users keeping their cryptographic keys safe (see below).

However, even if functioning land registries exist, politically motivated transfers of land (primarily state land) to political elites and their cronies are an important concern in many developing countries (Deininger & Feder, 2009). Against this background, blockchain

technology can be seen as a tool for governments to credibly self-bind themselves to not interfere with the land registry. As distributed ledgers have a high level of immutability, corrupt bureaucrats and politicians would hardly be able to assign land titles to their cronies, as long as the system is not dominated by a group of colluding block creators or abandoned by the government.

In addition, Arruñada (2017) cautions that the automated exchange of property on a blockchain is only conceivable in a system that records deeds (e.g. employed by France and a majority of US states), as opposed to a system that registers rights (e.g. employed by Germany and Australia). The main difference between the systems is that the former system dates and keeps documents, whereas the latter system additionally "[verifies] as a necessary condition for entry into the register, that the intended transactions respect all other rightholders' rights on the specific asset" (Arruñada, 2017, p. 28). Therefore, the latter system is able to provide an indefeasible title of the land, whereas in the former system, the titleholder has to prove its legitimacy in court if there are conflicting claims. Thus, in the case where a fraudulent transaction of a title (e.g. an attacker steals the private key and transfers the property to themselves) is done on a fully automated blockchain under a land registration system, the attacker would, in principle, hold an indefeasible title of the land. In contrast, the attacker could be challenged in court under a deeds registration system. Arruñada (2017) therefore argues that blockchains will likely not be able to fully automate land transactions in systems that register rights.

The Republic of Georgia and Sweden are hosting two of the most advanced projects (by BitFury and ChromaWay, respectively) that aim to optimise the national land registry using blockchain technology. Hernando de Soto actually serves as a board advisor to BitFury (BitFury, 2017). Georgia is not a country that desperately needs reforms of its land registries. In fact, the country ranked third in the "Registering Property" dimension of the World Bank's 2017 "Doing Business" report. BitFury is said to have chosen the small Caucasian country precisely due to its efficient land registries, so that a well-functioning land registry on a blockchain can serve as a role model for other countries (Smith, 2016). The stalling of a similar project by Factom in Honduras lends some credit to their approach (Rizzo, 2015). As of April 2017, 100,000 documents were registered on the blockchain that BitFury created for Georgia (Smerkis, 2017).

The project that ChromaWay is conducting in Sweden has, up to now, only completed the testbed stage. Despite this, they are ahead of the project by BitFury, in that they have already published a report that broadly describes how their solution works and what benefits are to be expected (Kempe, 2017). The report clarifies that the system will not enable fully automated transactions of property titles on the blockchain and replace the Swedish land registration authority's role in the process. Rather, the project aims to build a solution that simplifies and speeds up the cooperation of the different actors involved in property transfers (the land registration authority, seller, buyers and their respective agents and banks), while increasing transparency for the parties involved.

This is realised using a private blockchain that restricts access to the documents of a transaction to those involved in it. Additionally, hashes of the contract can be uploaded into an existing blockchain (e.g. Bitcoin or Ethereum) as an additional security mechanism that further guards against undetected manipulation. If the project lives up to its ambitions, the

time between writing the purchasing contract and registration at the land registration authority will, for example, be reduced from four months to a few days.

This indicates that distributed ledger technology has the potential to increase the efficiency and user-friendliness of land registry systems in all countries. Furthermore, distributed ledgers could be even more valuable in countries that struggle with unreliable land registries. This potential is subject to the following conditions:

- Existing problems are due to difficulties with maintaining the registries, as opposed to the initial creation of ledger entries.
- The land registry is supported by adequate executive and judicial enforcement mechanisms.
- National governments are willing to self-bind themselves by impeding future manipulations of the ledger.

However, as a reliable land registry is an indispensable precondition for "reanimating" the enormous sums of dead capital globally, even solutions that only work in specific contexts should not be underrated.

## 4 Risks and externalities

Despite their potential for financial inclusion and other purposes, distributed ledgers are a new technology that comes with new risks and externalities. The following three subsections focus on security risks, the externality of high levels of electricity consumption and price volatility of crypto currencies.

### 4.1 Security, immutability and privacy of distributed ledger systems

There is no consensus in the crypto currency community about which consensus mechanism is theoretically the most secure (see e.g. Buterin, 2016a; Demeester, 2017; Kiayias, Russell, David, & Oliynykov, 2017). Section 2 provided simplified explanations on how the different mechanisms secure the ledger, but the technical details of this debate are beyond the scope of this paper. In the following, the security and immutability of distributed ledgers are instead examined by analysing experienced security threats in Bitcoin and immutability concerns in Ethereum.

Under Bitcoin's PoW system, attaining the bulk of available computational power to successfully conduct an alternative history attack is very expensive. Until now, such attacks have only been successfully conducted if the receiver accepted the payment without waiting for any confirmations (i.e. blocks that were mined on top of the block that contained the payment). In fact, the mining pool (see Box 1 for a definition) "Ghash.io" conducted double-spend attacks against an online gambling site in 2013 (Hearn, 2015). In addition, Gash.io controlled at least 51 per cent of the available computing power for about 12 hours in June 2016 (without conducting double-spend attacks). These incidents showed that alternative history attacks are not only a theoretical threat. The emergence of mining pools has created a considerable degree of centralisation in a system that is designed to be decentralised.

Satoshi Nakamoto, the pseudonymous founder of Bitcoin, argued that it would not make sense economically to attack the system in this way, because an attacker who owns enough computing capacity to attack the system would undermine their own wealth (Nakamoto, 2008). This could refer either to the hardware investment of the miner or to an expected collapse of the value of Bitcoin after a successful attack. However, Down and Hutchinson (2015) point out that one should not rely on this intuitive argument too much, because mining hardware (ASICS) only has a useful lifespan of a few month. Thus, towards the end of this cycle, the value of the ASICS could be smaller than the gains of a large double-spend attack. In addition, the possibility of cloud mining even allows attackers to control mining power without owning any hardware.

Despite the existence of large mining pools, which increase the risks of double-spend attacks, more conventional attacks have caused much greater losses. Attacks in which the private keys of individual users or centralised institutions, such as crypto currency exchanges, are stolen, are similar to the hacks of online bank accounts of individuals or corporations. A popular way to steal a private key is to install a conventional keylogger program or device[15] on the victim's computer. Knowledge of the private key enables the attacker to transfer the Bitcoin held in the address to their own account. Unlike with online banking, this transaction cannot be recovered because there is no central entity that can undo the transaction[16] or refund the victim of the attack. The hacks of large centralised entities within the Bitcoin and Ethereum networks have led to massive losses of crypto currency. The largest Bitcoin theft, which consisted of Bitcoins worth USD 500 million, targeted the exchange Mt. Gox, which subsequently could not pay out its users' funds and collapsed (Wieczner, 2017). However, there are technical means that individual users can employ to prevent key thefts (Bitcoinwiki, 2017a).

In the Ethereum network, the hack of the Decentralized Anonymous Organization (DAO) has brought the immutability of blockchains into question. The DAO was an automated venture capital fund without any management staff. All investors were supposed to be able to take a vote on investing in projects that were proposed to the fund. After the DAO raised the equivalent of USD 150 million in Ether (the currency of the network Ethereum), an attacker exploited a code error and was able to withdraw about a third of the funds (del Castillo, 2016). The Ethereum community, some of whom had invested in the DAO, was split on the question of whether the withdrawal of the funds was a theft that needed to be corrected or the legitimate exploitation of a faulty smart contract. The lead developers did not want to accept that such a large investment by many members of the community was lost, so they implemented a fork just before the block that contained the disputed withdrawal of DAO funds (Buterin, 2016b). This had the effect that everybody who had invested in the DAO could safely withdraw their investment. The fork quickly gained the support of a clear majority of Ethereum miners, but a minority refused to accept the change in the transaction history. Due to this, Ethereum Classic was created, which still works with the original transaction history, including the disputed withdrawal of DAO funds. Today, Ethereum

15 Keyloggers are computer programs or hardware devices that track every keystroke of a computer (Landesman, 2017).

16 It is technically possible to freeze transactions that are mistakenly sent on distributed ledger networks, but Bitcoin does not support this feature. Stellar allows its users to freeze transactions so that the recipient cannot use the unintentionally sent funds but can send them back to the sender (Stellar Development Foundation, 2017).

Classic is traded for USD 30, whereas Ethereum is traded for USD 480 (Coinmarketcap, 2017, as of 28 November 2017).

This discussion shows that distributed ledgers are not technically immutable, but they offer a relatively high degree of protection against malicious network attacks by individuals. However, if the majority of decision-makers agree to rewrite the transaction history, this is possible. Thus, one has to trust the group of decision-makers of the respective distributed ledger not to collude in order to defraud its users. This should be easy as long as the decision-makers are a large and diverse group of actors who also have a stake in the success of the currency. However, with the emergence of large mining pools and cloud mining, neither of the two conditions are necessarily true for all PoW blockchains.

The privacy features of crypto currencies are ambiguous. Like the creator of Bitcoin, most crypto currency transactions can be described as being publicly visible but pseudonymous. In Bitcoin and Ethereum, for example, the entire ledger of transactions can be scrutinised by anyone, but instead of seeing names of senders and remitters, you see their crypto currency addresses. Associating these with people or companies is complicated, but it is possible by linking publicly available information to a Bitcoin address (see e.g. Meiklejohn et al., 2013; Monaco, 2015). Thus, public ledgers offer the option to track payments, which is a feature that is not provided by conventional electronic payment mechanisms. Although this has advantages for law enforcement agencies, the desire of users to have more advanced privacy features is understandable. After all, there is a looming threat that somebody could publicly link users' names to their public transaction histories.

The crypto currency Monero addresses this need by offering advanced privacy features and untraceable transactions (Monero, 2017). In addition, there are automatic crypto currency mixers that confuse the trails of transactions in any currency. These mixers work well, unless one aims to disguise the whereabouts of very large sums (see Buterin, 2013, for an enthusiastic description). It is obvious that these privacy features can be misused for criminal activities. Traditionally, a preferred form of payment among criminals who handle large amounts of money is cash, due to the high privacy level it offers. However, cash has several disadvantages. For example, it creates high transaction costs if the physical distance between sender and receiver is large, and it is easily lost or stolen. Crypto currency has the potential to solve both problems. Combined with the advanced privacy features of some crypto currencies and concealment services, the digital versions of cash-stuffed suitcases may encourage money laundering and the financing of illicit goods.

To combat these illegal activities, regulations focussed on anti-money laundering (AML) and combating the financing of terrorism (CFT) exist. Applying these regulations to crypto currencies is difficult due to their peer-to-peer nature. Regulators are usually able to regulate central entities. In fact, crypto currency exchanges are subject to know your customer (KYC) regulation. However, it is possible to use crypto currencies without ever interacting with exchanges. A very anonymous way to achieve this is to engage in mining the currency. To balance the legitimate privacy needs of users with security needs and the associated prosecution requirements of law enforcement agencies is not easy, and Section 5 can only give some hints.

## 4.2 Electricity consumption of proof of work blockchains

Financial inclusion is primarily a means to achieve developmental ends, such as the SDGs, which are outlined in the 2030 Agenda. The SDGs and its targets are "universal, indivisible and interlinked". This implies that financial inclusion should not be achieved at the expense of environmental goals, such as SDG 13, which aims to combat climate change (United Nations, 2015). Section 3 highlighted the potential of blockchain technology to foster financial inclusion. However, PoW blockchains have a high level of – often coal-powered – electricity consumption. Against the background of environmental externalities associated with fossil fuel-powered electricity generation, this section discusses the electricity consumption of PoW blockchains. In addition, the rationale for using this consensus algorithm is scrutinised.

Although the Bitcoin mining hardware is quickly getting more energy-efficient (Box 1), the total energy consumption level that PoW requires is continuing to rise. In fact, the difficulty of calculating the hash for each block is adjusted to the computing power of the network, so that it always takes about 10 minutes for the next block to be mined. Under these conditions, efficiency gains only increase competition and lead to a higher rate of hardware exchange, but they do not reduce the total consumption level of energy. The electricity consumption level of the Bitcoin network has exploded in recent years, fuelled by the currency's skyrocketing price. As of 17 November 2017, a single Bitcoin transaction is estimated to consume 277 KWh.[17] This is equivalent to the daily consumption of about nine American households. The total electricity consumption of the network is a remarkable 0.13 per cent of worldwide consumption (Digiconomist, 2017a). The Ethereum network is estimated to consume 61 KWh per transaction, which is equivalent to the daily consumption of two American households, which is extremely high for a payment service, although the figure pales in comparison to Bitcoin's 277 KWh. Ethereum's share of global energy consumption is estimated at 0.05 per cent (Digiconomist, 2017b).

The alternative consensus mechanisms PoS and PoI (Section 2.2) as well as voting-style algorithms (Section 2.3) have very low energy consumption levels. Also, the Tangle's version of PoW is relatively energy-efficient. Thus, there are many alternatives that already have proved their viability. After all, four out of the top ten crypto currencies use (relatively) energy-efficient consensus mechanisms. From a sustainability perspective, it is unfortunate that the top three crypto currencies (Bitcoin, Ethereum and Bitcoin Cash) are still using PoW. Therefore, it is of particular importance that Ethereum's switch to PoS is successfully completed. This might then also encourage the developers of Bitcoin and other PoW blockchains to switch to a sustainable consensus algorithm.

However, at the moment, Bitcoin developers seem to have no such plans, except for the introduction of the Lightning Network, which would improve the situation for small and recurrent transactions (Section 2.1). A popular argument for PoW blockchains is that the costliness of their creation, using a gold analogy, gives Bitcoins their value. This idea can be traced back to 1998, when Nick Szabo wrote the concept for Bitgold, which was an intellectual precursor of Bitcoin. The pseudonymous creator of Bitcoin also referred to this

17 This does not take into account the energy used to produce the hardware, which is typically replaced at a high frequency (see Box 1; Digiconomist, 2017a).

idea by stating: “The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation” (Nakamoto, 2008).

In the following, a possible explanation for the reluctance to retire PoW is given. It is part of the crypto-anarchic attitude that gave rise to the creation of crypto currencies to stress the weaknesses of fiat money (money that is legal tender but not backed by any commodity). Indeed, fiat money has led to many hyperinflation periods due to its over-issuance by the government. The consequence was usually the replacement of the failed fiat currency with a new one. However, there are counterexamples of currencies that have not failed for very long time spans, with the record-holder being the British pound, which was introduced in 1694[18] (Galland, Mack, & Clark, 2011).

The history of frequent hyperinflation-created currency crises indicates that there were insufficient governance mechanisms in place to regulate the supply of money in all such instances. It is also true that such crises can be avoided by using something that is costly to produce as a monetary unit, because a drastic oversupply of money is infeasible if it is costly to produce. Note, however, that Bitcoin uses a fixed schedule to issue additional amounts of currency, so that production is not subject to market forces at all. Therefore, although costly-to-produce tokens can be used to guard a currency against inflation, this is not the mechanism Bitcoin uses.

However, the author argues that protection against any given money-supply-driven inflation level can be achieved through any secure system that guarantees a rules-based money-creation process. PoS, voting-style algorithms or any other secure mechanism that guarantees that any additional quantities of money are only issued in accordance with a pre-defined schedule fulfils this condition, just as PoW does. In fact, the security of the algorithm determines the level of trustworthiness of a crypto currency. Using electricity costs to secure an algorithm seems to be a very inelegant and inefficient solution. Thus, it seems unconvincing that Bitcoins and similar crypto currencies are valuable just because real resources were used to create them. Crypto currencies rather derive their trustworthiness from secure mechanisms that guarantee their scarcity.

The claimed security advantages of PoW are disputed in the distributed ledger community (Section 4.1). Against this background, there does not seem to be a compelling reason, other than path dependencies, to continue using PoW as a consensus algorithm. If, for some reason, PoW does have some unique features that make it superior to alternative algorithms, one should at least try to use the enormous computing power that it uses to solve real problems and further the advancement of science. The relatively small crypto currencies Primecoin and Gridcoin follow this approach and use their PoW systems to find special prime number chains or do the computing work for various research projects in diverse fields such as epidemiology, climate science and astrology (Gridcoin, 2017; Primecoin, 2014).

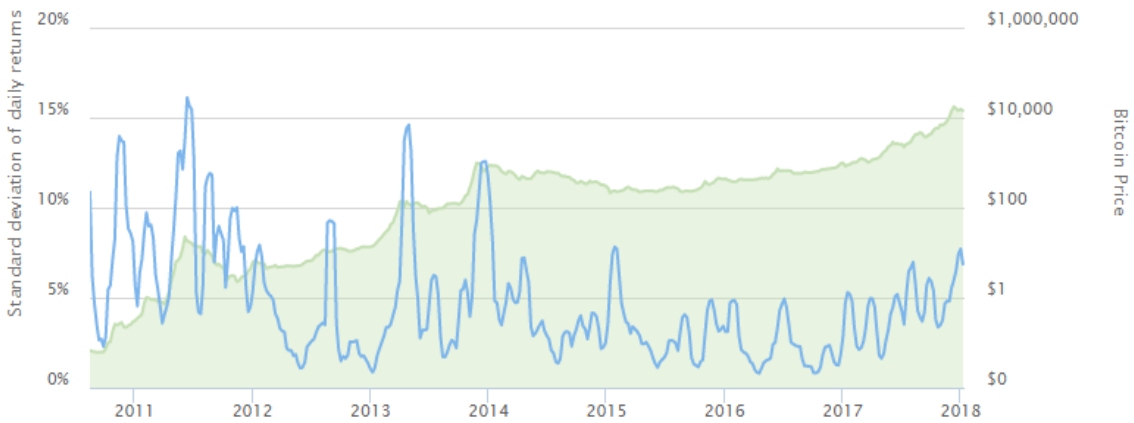
18 To paint the complete picture, one has to point out that even the British pound, due to regular inflation, is only worth about 0.5 per cent of its original value, which was 20 ounces of silver (Galland, Mack, & Clark, 2011).

## 4.3 Volatility of crypto currencies

Since the US soap opera "The Good Wife" of mainstream television network CBS aired an episode on "Bitcoin for Dummies" in 2011, the crypto currency has attracted increasing levels of media attention (99Bitcoins, 2017). A recurrent theme throughout the years has been Bitcoin price explosions. The phenomenon has also frequently been described as a Bitcoin bubble, cautioning against a belief of ever-rising prices (see e.g. Browne, 2017; The Economist, 2013). Media coverage also plays an important role in the short-term price variations of Bitcoin, but in the long run, fundamental factors such as Bitcoin's velocity, equity market indices and exchange rates are determining factors, according to Bouoiyour, Selmi, Tiwari and Olayeni (2016).

As a result of short-term and long-term factors, the exchange rate of Bitcoin skyrocketed from USD 0.05 in July 2010 to more than USD 13,000 in January 2018 (Coindesk, 2017b). This explosion in value went hand in hand with very high – but slowly declining – levels of volatility. At the time of publishing, the 30-day volatility of Bitcoin against the US dollar is still fluctuating around 6 per cent (Figure 7), as compared to the average volatility of other major currencies (0.5-1 per cent) or gold (1.2 per cent).

**Figure 7: Bitcoin price and 30-day volatility**




Note that prices are measured on a logarithmic scale.
Source: Buy Bitcoin Worldwide (2017)

Most other crypto currencies are also experiencing high levels of volatility, but this section focusses on Bitcoin, because its volatility has been more thoroughly analysed in the literature than any other crypto currency.

Its high level of volatility seriously impedes Bitcoin's functionality as a currency. Baur and Dimpfl (2017) assess to which degree Bitcoin is able to fulfil the three economic functions of a currency, namely to be used as (i) a medium of exchange, (ii) a store-of-value and (iii) a unit of account. Although a high level of volatility obviously impedes functions two and three, it may also affect function one indirectly. Risk-averse consumers will strive to minimise their exposure to a currency with a high level of volatility, thus they will have to buy Bitcoin immediately before using the currency to purchase something. This pushes up

transaction costs and drives down Bitcoin's usefulness as a medium of exchange. As a consequence, Baur and Dimpfl (2017) conclude that its high level of volatility prevents Bitcoin from properly fulfilling any of the three functions. It follows that Bitcoin might better be classified as an investment than a currency at present. This is backed by the analysis of Glaser, Zimmermann, Haferkorn, Weber and Siering (2014), which demonstrates that new users of Bitcoin predominantly keep their newly bought Bitcoins on the exchange they bought them. The transaction volume of the crypto currency is unrelated to the transaction volume of Bitcoin exchanges in their sample.[19] Thus, peoples' primary motivation for buying Bitcoin seems to be investment rather than usage as a means of payment.

However, there are fiat-pegged crypto currencies that circumvent volatility almost entirely. Perhaps the simplest solution to achieve this is provided by Tether, which backs its crypto currency version of the dollar (USDT) 100 per cent with US dollars, so that one USDT can always be exchanged for one USD (Tether, 2017). In addition, the central banks of Canada and China are exploring the launch of crypto versions of the legal tenders of their countries (The Economist, 2017b). Furthermore, distributed ledger-based payment systems such as Ripple and Stellar allow the user to directly transfer fiat IOUs. Thus, a high level of volatility does not apply to all crypto currencies.

## 5 Conclusions and regulatory recommendations

This paper illustrates the diversity of distributed ledger technologies by explaining two major data structures – the blockchain and the Tangle – as well as the four major consensus algorithms: PoW, PoS, PoI and voting-style algorithms (Section 2). Across these different categories – and to a lesser degree also between different networks within the same category – performance indicators, additional features as well as risks vary greatly.

Finance is the most obvious field of application for distributed ledgers. Evidence for the great potential of blockchain technologies to bring down remittance costs and provide a secure store of money is presented in Section 3.1. It is indicated as well that crypto currencies may act as a gateway to more sophisticated financial services. The field is developing dynamically with rapid advances in user-friendliness and lowering costs: some international distributed ledger-powered remittance services are already available for free. The remaining challenge of achieving mainstream adoption does not seem to be hindered by existing regulations in any major way. In general, blockchain-powered remittance services should be regulated analogously to conventional remittance services to retain a level playing field.

Fields of application outside the finance realm have gained attention in recent years. The considerable potential of blockchain technology to improve the efficiency and reliability of land registries is discussed in Section 3.2. The usefulness of the technology in this sector depends on certain conditions, such as functioning executive and judicial enforcement mechanisms. If these conditions are met, blockchains can also help to revive dead capital

19 As Glaser et al. (2014) point out, transactions at the exchange are not recorded directly on the blockchain, as the funds remain at the Bitcoin addresses of the exchange. Thus, the Bitcoins are not transferred to a Bitcoin address of the buyer, unless the buyer transfers the funds.

by enabling the use of property as collateral. As only a few approaches have been successfully tested, further efforts to develop better blockchain-based land registries could lead to even more benefits. Therefore, countries that commission a blockchain-based restructuring of their land registry not only increase the efficiency of their system by orders of magnitude, but also contribute to worldwide progress in this field. Policy-makers should be encouraged to follow the examples of the Republic of Georgia and Sweden. Furthermore, the potential of the technology for other public services should also be considered. It is essential to compare different technologies in order to gain high levels of efficiency while avoiding negative externalities.

The innovativeness of blockchain technology goes hand in hand with new types of security threats. These as well as the implications of different anonymity features of crypto currencies are analysed in Section 4.1. Regulatory issues related to these topics are consumer protection and AML/CFT. Crypto currencies are still in their infancy, and over-ambitious regulation could harm their development in the respective judicial area. On the other hand, funds worth more than USD 260 billion have already been invested in crypto currencies (Derousseau, 2017), which are subject to some unique risks. The mandatory provision of information about risks from exchanges would be a regulatory requirement that constitutes only a minimal market intervention. On the other hand, it would nudge customers to make informed decisions about whether they are willing to take the risks associated with crypto currency usage and investment. The information should be standardised and written in a way that is comprehensible for the general public. Mandatory topics could include possible attacks against the network, possible attacks against individual users, data on the volatility of the respective crypto currency, and technical as well as behavioural means to manage and mitigate these risks.

How can the dilemma of letting users protect their privacy – while at the same time providing law enforcement with sufficient information – be addressed? Regulating exchanges, which is already standard practice, is not sufficient, because it is also possible to use crypto currencies without having any direct or indirect connection with exchanges. This may be too cumbersome for most users, but criminals have a higher motivation for keeping their transactions anonymous. Regulating every user is obviously impractical, because effectively controlling a sufficient share of users would put a large burden on law enforcement agencies. A proposal of Australia to make wallet providers subject to AML/CFT regulations is interesting in this context and should also be considered by other regulators (Australian Government, 2016). This, as well as any other regulation on AML/CFT, should ensure that the advanced privacy features of some crypto currencies and mixing services are adequately considered and cannot be used to circumvent the regulations.

The extremely high energy consumption levels of PoW blockchains (Section 4.2) are another reason for concern. However, instead of regulating the energy consumption levels of blockchains separately, this issue should be addressed by reforming and harmonising existing emission-trading schemes and carbon taxes.

The volatility of Bitcoin has decreased over the years, but, in combination with very high transactions fees, it still compromises its usefulness as a currency (Section 4.3). However, there are other crypto currencies that guarantee a fixed exchange rate to the US dollar (e.g. Tether) or enable the transfer of IOUs in any currency (e.g. Ripple and Stellar).

Considering the great potential, but also the significant risks, of distributed ledger technologies, a proportionate approach to regulation is indispensable. Regulators should also accommodate for the diversity of distributed ledgers and the differences in types of risks they entail.

## References


99Bitcoins. (2017). *Bitcoin price history chart with historic events*. Retrieved from https://99bitcoins.com/price-chart-history/

Adams, R. H. (2011). Evaluating the economic impact of international remittances on developing countries using household surveys: A literature review. *The Journal of Development Studies, 47*(6), 809-828. http://dx.doi.org/10.1080/00220388.2011.563299

Alfaroq, U. J. (2017). *NEM's next generation core (codename "catapult") unveils its power for productive use – confirmed in a live environment with >10m accounts*. Retrieved from https://medium.com/nem-distributed-ledger-technology-blockchain/nems-next-generation-core-codename-catapult-unveils-its-power-for-productive-use-confirmed-e1888b2a92bf

Arruñada, B. (2017). *Blockchain's struggle to deliver impersonal exchange*. Retrieved from https://econ-papers.upf.edu/papers/1549.pdf

Arsenault, C. (2016). *Property rights for world's poor could unlock trillions in "dead capital": Economist*. Retrieved from https://www.reuters.com/article/us-global-landrights-desoto/property-rights-for-worlds-poor-could-unlock-trillions-in-dead-capital-economist-idUSKCN10C1C1

Australian Government. (2016). *Regulating digital currencies under Australia's AML/CTF regime*. Retrieved from https://www.ag.gov.au/Consultations/Documents/AML-CTF/Regulating-digital-currencies-under-Australias-aml-ctf-regime.pdf

B2BPay. (2017). *Blockchain saving account.* Retrieved from https://www.b2bpay.co/blockchain-saving-account

Banerjee, A., & Duflo, E. (2012). *Poor economics: A radical rethinking of the way to fight global poverty*. Reprint edition. New York, NY: Public Affairs.

Baur, D. G., & Dimpfl, T. (2017). *Realized Bitcoin volatility*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2949754

Bitcoin.org. (2017). *Bitcoin developer guide*. Retrieved from https://bitcoin.org/en/developer-guide#stratum

Bitcoinwiki. (2015). *From address*. Retrieved from https://en.bitcoin.it/wiki/From_address

Bitcoinwiki. (2016a). *Bit gold proposal*. Retrieved from https://en.bitcoin.it/wiki/Bit_Gold_proposal

Bitcoinwiki. (2016b). *Address*. Retrieved from https://en.bitcoin.it/wiki/Address

Bitcoinwiki. (2017a). *Hardware wallet.* Retrieved from https://en.bitcoin.it/wiki/Hardware_wallet

Bitcoinwiki. (2017b). *Full node*. Retrieved from https://en.Bitcoin.it/wiki/Full_node

Bitcoinwiki. (2017c). *Address reuse*. Retrieved from https://en.bitcoin.it/wiki/Address_reuse

BitFury. (2017). *Meet the team*. Retrieved from http://bitfury.com/team

BitInfoCharts. (2017). *Cryptocurrencies*. Retrieved from https://bitinfocharts.com/; for Bitcoin: https://bitinfocharts.com/bitcoin/; for Ethereum: https://bitinfocharts.com/ethereum/; for Bitcoin Cash: https://bitinfocharts.com/ethereum/; for Litecoin: https://bitinfocharts.com/litecoin/; for Dash: https://bitinfocharts.com/litecoin/; for Monero: https://bitinfocharts.com/monero/

Bitnation. (2017). *World citizen*. Retrieved from https://bitnation.co/join-bitnation/

Bloom. (2017). *Say hello to inclusive credit.* Retrieved from https://hellobloom.io/

Bne IntelliNews. (2017). *FINTECH: Blockchain to get its own global business council*. Retrieved from http://www.intellinews.com/fintech-blockchain-to-get-its-own-global-business-council-113368/

Bouoiyour, J., Selmi, R., Tiwari, A., & Olayeni, O. (2016). What drives Bitcoin price? *Economics Bulletin, 36*(2), 843-850.

Browne, R. (2017). *Bitcoin price bubble "will collapse" while the tech that underpins it lives on, Kenneth Rogoff predicts*. Retrieved from https://www.cnbc.com/2017/10/09/bitcoin-price-bubble-will-collapse-kenneth-rogoff-predicts.html

Buterin, V. (2013). *Trustless Bitcoin anonymity here at last*. Retrieved from https://Bitcoinmagazine.com/articles/trustless-Bitcoin-anonymity-here-at-last-1377737692/

Buterin, V. (2016a). *A proof of stake design philosophy*. Retrieved from https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51

Buterin, V. (2016b). Hard fork completed. *Ethereum Blog*. Retrieved from https://blog.ethereum.org/2016/07/20/hard-fork-completed/

Buy Bitcoin Worldwide. (2017). *Bitcoin volatility index – charts vs dollar & more*. Retrieved from https://www.buybitcoinworldwide.com/volatility-index/

Casey, M. (2016). *Could the blockchain empower the poor and unlock global growth?* Retrieved from http://techonomy.com/2016/03/blockchain-global-growth/

Castor, A. (2017). *Why quantum computing's threat to Bitcoin and blockchain is a long way off*. Retrieved from https://www.forbes.com/sites/amycastor/2017/08/25/why-quantum-computings-threat-to-bitcoin-and-blockchain-is-a-long-way-off/#1b1a22022882

Cohen, D., Schwartz, D., & Britto, A. (2017). *The XRP ledger consensus process*. Retrieved from https://ripple.com/build/xrp-ledger-consensus-process/

Coindesk. (2014). *What are Bitcoin mining pools?* Retrieved from https://www.coindesk.com/information/get-started-mining-pools/

Coindesk. (2017a). *How will Ethereum scale?* Retrieved from https://www.coindesk.com/information/will-ethereum-scale/

Coindesk. (2017b). *Bitcoin price index – real-time Bitcoin price charts*. Retrieved from https://www.coindesk.com/price/

Coinmarketcap. (2017). *Cryptocurrency market capitalizations*. Retrieved from https://coinmarketcap.com/

Committee on Payment and Settlement Systems & World Bank. (2007). *General principles for international remittance services*. Retrieved from https://www.bis.org/cpmi/publ/d76.pdf

Cyberblock. (2017). *Top 9 market cap blockchains ranked in order by transaction speed. Let's see where Steem fits in*. Retrieved from https://steemit.com/cryptocurrency/@cyberblock/top-9-market-cap-blockchains-ranked-in-order-by-transaction-speed-lets-see-where-steem-fits-in

Daly, N. (2010). *International remittance service providers: An overview of mobile international remittance service provider service offerings.* Retrieved from https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/03/gsmaremittanceserviceproviderwhitepaper182.pdf

Deininger, K., & Feder, G. (2009). Land registration, governance, and development: Evidence and implications for policy. *The World Bank Research Observer, 24*(2), 233-266. http://dx.doi.org/10.1093/wbro/lkp007

Del Castillo, D. (2016). *Alternative Ethereum blockchain gains support as price declines*. Retrieved from https://www.coindesk.com/ethereum-classic-price-services-alterative-blockchain/

Demeester, T. (2017). *Critique of Buterin's "A proof of stake design philosophy"*. Retrieved from https://medium.com/@tuurdemeester/critique-of-buterins-a-proof-of-stake-design-philosophy-49fc9ebb36c6

Demirguc-Kunt, A., Klapper, L., Singer, D., & Van Oudheusden, P. (2015). *The global Findex Database 2014: Measuring financial inclusion around the world* (Policy Research Working Paper: Vol. 7255). Washington, DC: World Bank. Retrieved from http://documents.worldbank.org/curated/en/187761468179367706/pdf/WPS7255.pdf

Derousseau, R. (2017). *Bitcoin for beginners: 3 things to know before you invest.* Retrieved from http://fortune.com/2017/11/24/bitcoin-cryptocurrency-investing/

De Soto, H. (2000). *The mystery of capital: Why capitalism triumphs in the West and fails everywhere else*. London: Bantam Press.

Digiconomist. (2017a). *Bitcoin energy consumption index*. Retrieved from https://digiconomist.net/bitcoin-energy-consumption

Digiconomist. (2017b). Ethereum energy consumption index (beta). *Digiconomist*. Retrieved from https://digiconomist.net/ethereum-energy-consumption

Down, K., & Hutchinson, M. (2015). Bitcoin will bite the dust. *Cato Journal, 35*(2), 357-382.

Edwards, D. (2017). *Formal technical and economic whitepaper for Casper is available for review*. Retrieved from https://steemit.com/ethereum/@dana-edwards/formal-technical-and-whitepaper-for-casper-is-available-for-review

Ether World. (2017). *Inspire: Peer to peer lending on blockchain*. Retrieved from https://medium.com/@ether_world/inspire-peer-to-peer-lending-on-blockchain-590023743bde

Falls, A. (2017). *Ether Review #69 – IOTA & the post-blockchain era*. Retrieved from https://soundcloud.com/arthurfalls/ether-review-69-iota-the-post-blockchain-era

ForkLog. (2016). *The brief history of Bitcoin mining: How it all started*. Retrieved from http://forklog.net/bitcoin-mining-past-present-and-future/

Galland, D., Mack, C., & Clark, J. (2011). *The average life expectancy for a Fiat currency is 27 years ... Every 30 to 40 years the reigning monetary system fails and has to be retooled*. Retrieved from http://georgewashington2.blogspot.de/2011/08/average-life-expectancy-for-fiat.html

Github. (2017). *White paper*. Retrieved from https://github.com/Ethereum/wiki/wiki/White-Paper

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C., & Siering, M. (2014). *Bitcoin – asset or currency? Revealing users' hidden intentions*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425247

Gridcoin. (2017). *Gridcoin – rewarding scientific distributed computing*. Retrieved from http://www.gridcoin.us/

GSMA. (2016). *Driving a price revolution: Mobile money in international remittances*. Retrieved from https://www.gsmaintelligence.com/research/?file=8F31B31705C20A63A41DB9711BF84C25&download

Hearn, M. (2015). *Double spending in Bitcoin*. Retrieved from https://medium.com/@octskyward/double-spending-in-bitcoin-be0f1d1e8008

IBM. (2016). *Fast forward: Rethinking enterprises, ecosystems and economies with blockchains*. Retrieved from https://www-935.ibm.com/services/us/gbs/thoughtleadership/blockchain/

IOTA Foundation. (2017). *What are the main use cases of IOTA?* Retrieved from https://learn.iota.org/faq/what-are-the-main-use-cases-of-iota

Kalan, G. R., & Aykut, D. (2005). *Assessment of remittance fee pricing*. Retrieved from http://siteresources.worldbank.org/INTPROSPECTS/Resources/AssessmentofRemittanceFeePricing.pdf

Kempe, M. (2017). *The land registry in the blockchain – testbed*. Retrieved from https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

Kerekes, C. B., & Williamson, C. (2010). Propertyless in Peru, even with a government land title. *The American Journal of Economics and Sociology, 69*(3), 1011-1033.

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017). *Ouroboros: A provably secure proof-of-stake blockchain protocol*. Retrieved from https://eprint.iacr.org/2016/889.pdf

Landesman, M. (2017). *What is a keylogger trojan? Some viruses can monitor all your keystrokes*. Retrieved from https://www.lifewire.com/what-is-a-keylogger-trojan-153623

Lee, P. (2017). *Blockchain set to transform loan trading and collateral markets.* Retrieved from https://www.euromoney.com/article/b14djmk97srdh5/blockchain-set-to-transform-loan-trading-and-collateral-markets

Light, J. (2017). *Abra tellers are now available in over 170 cities around the world*. Retrieved from https://www.abra.com/blog/abra-tellers-available-in-over-170-cities/

Lightning Network. (s.a.). *The Bitcoin Lighting Network*. Retrieved from https://lightning.network/lightning-network-summary.pdf

Lorenz, J.-T., Münstermann, B., Higginson, M., Oleson, P. B., Bohlken, N., & Ricciardi, V. (2016). *Blockchain in insurance – opportunity or threat*. Retrieved from https://www.mckinsey.com/industries/financial-services/our-insights/blockchain-in-insurance-opportunity-or-threat

Madeira, A. (2017). *What is the block size limit*. Retrieved from https://www.cryptocompare.com/coins/guides/what-is-the-block-size-limit/

Mastermined. (2017). Dash evolution: Masternodes. *Dash Force News*. Retrieved from https://www.dashforcenews.com/dash-evolution-masternodes/

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of Bitcoins: Characterizing payments among men with no names. *;login:, 38*(6), 10-14.

Mizrahi, A. (s.a.). *A blockchain-based property ownership recording system*. Retrieved from https://chromaway.com/papers/A-blockchain-based-property-registry.pdf

Monaco, V. (2015). *Identifying Bitcoin users by transaction behavior*. Retrieved from https://www.researchgate.net/publication/277248535_Identifying_Bitcoin_users_by_transaction_behavior

Monero. (2017). *How does Monero's privacy work?* Retrieved from https://www.monero.how/how-does-monero-privacy-work

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from https://bitcoin.org/bitcoin.pdf

NEM. (2015). *NEM technical reference*. Retrieved from https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf

NEM. (2016). *NEM update 0.6.82: Lower fees and new API*. Retrieved from https://blog.nem.io/nem-updated-0-6-82/

NEO. (2017a). *Consensus*. Retrieved from http://docs.neo.org/en-us/node/consensus.html

NEO. (2017b). *System fees*. Retrieved from http://docs.neo.org/en-us/sc/systemfees.html

NEO. (2017c). *NEO white paper: A distributed network for the smart economy*. Retrieved from http://docs.neo.org/en-us/

Neville, S., & Allaire, J. (2016). *Circle's new capital, China and Euro expansion*. Retrieved from https://blog.circle.com/2017/06/14/free-cross-border-payments-european-growth-product-features-and-new-services/

Neville, S., & Allaire, J. (2017). *Free cross border payments, European growth, product features and new services*. Retrieved from http://blog.circle.com/2017/06/14/free-cross-border-payments-european-growth-product-features-and-new-services/

Organisation for Economic Co-operation and Development. (2017). *Final official development assistance figures in 2015*. Retrieved from http://www.oecd.org/dac/financing-sustainable-development/development-finance-data/final-oda-2015.htm

Peck, M. E. (2015). *Bitcoin: The Cryptoanarchists' answer to cash: How Bitcoin brought privacy to electronic transactions*. Retrieved from https://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash/0

Popov, S. (2017). *The Tangle*. Retrieved from https://iota.org/IOTA_Whitepaper.pdf

Primecoin. (2014). *About Primecoin*. Retrieved from http://primecoin.io/about.php#value-xpm

R3 and Norton Rose Fulbright. (2016). *An R3 and Norton Rose Fulbright white paper. Can smart contracts be legally binding contracts?* Retrieved from http://www.nortonrosefulbright.com/knowledge/publications/144559/can-smart-contracts-be-legally-binding-contracts

Ripplewiki. (2014). *Payments*. Retrieved from https://wiki.ripple.com/Payments#Trust_lines

Rizzo, P. (2015). *Blockchain land title project "stalls" in Honduras*. Retrieved from https://www.coindesk.com/debate-factom-land-title-honduras/

Safaricom. (2017). *Safaricom Twaweza*. Retrieved from https://www.safaricom.co.ke/

Schiener. (2017). *A primer on IOTA (with presentation)*. Retrieved from https://blog.iota.org/a-primer-on-iota-with-presentation-e0a6eb2cc621

Schwartz, D., Youngs, N., & Britto, A. (2014). *The ripple protocol consensus algorithm*. Retrieved from https://ripple.com/files/ripple_consensus_whitepaper.pdf

Scott, J. (2017). *IOTA consensus masterclass*. Retrieved from https://forum.iota.org/t/iota-consensus-masterclass/1193

Smerkis. (2017). *Georgia records 100,000 land titles on Bitcoin blockchain: BitFury*. Retrieved from https://cointelegraph.com/news/georgia-records-100000-land-titles-on-bitcoin-blockchain-bitfury

Smith, J. (2016). *Clinton Global Initiative, 2016*. Retrieved from https://medium.com/@BitFuryGroup/the-bitfury-group-leadership-to-present-at-clinton-global-initiative-f2d0c195f6f6

Steemhoops99. (2017). *Transaction speed – Bitcoin, VISA, IOTA, PayPal*. Retrieved from https://steemit.com/cryptocurrency/@steemhoops99/transaction-speed-bitcoin-visa-iota-paypal

Stellar Development Foundation. (2017). *Ready for faster, cheaper transactions? Get started with the basics of the Stellar network*. Retrieved from https://www.stellar.org/how-it-works/stellar-basics/

Suri, T., & Jack, W. (2016). The long-run poverty and gender impacts of mobile money. *Science, 354*(6317), 1288-1292.

Swiss Re. (2017). *Hackathon challenge: Blockchain-based agricultural microinsurance*. Retrieved from https://www.ears.nl/static/consensus-2017/SR_hackathon_factsheet.PDF

Szabo, N. (1997). Smart contracts: Formalizing and securing relationships on public networks. *First Monday, 2*(9).

Szabo, N. (2001). *Proplets – devices for controlling property*. Retrieved from http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/proplets.html

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind Bitcoin is changing money, business and the world*. New York, NY: Portfolio Penguin.

Tether. (2017). *Fiat currencies on the Bitcoin blockchain*. Retrieved from https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf

The Economist. (2013). *The Bitcoin bubble*. Retrieved from https://www.economist.com/news/leaders/21590901-it-looks-overvalued-even-if-digital-currency-crashes-others-will-follow-bitcoin

The Economist. (2015). *The trust machine*. Retrieved from https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

The Economist. (2017a). *Bitcoin divides to rule: The crypto-currency's split into two versions may be followed by others*. Retrieved from https://www.economist.com/news/business-and-finance/21725747-crypto-currencys-split-two-versions-may-be-followed-others-bitcoin

The Economist. (2017b). *If blockchains ran the world – disrupting the trust business.* Retrieved from https://www.economist.com/news/world-if/21724906-trust-business-little-noticed-huge-startups-deploying-blockchain-technology-threaten

United Nations. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development*. Retrieved from https://sustainabledevelopment.un.org/post2015/transformingourworld

Valkenburgh, V. (2017). *What is "Blockchain" anyway?* Retrieved from https://coincenter.org/entry/what-is-blockchain-anyway

Wieczner, J. (2017). *Hacking coinbase: The great Bitcoin bank robbery*. Retrieved from http://fortune.com/2017/08/22/Bitcoin-coinbase-hack/

Wikipedia. (2017). *Cryptographic hash function – Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/Cryptographic_hash_function#Illustration

Williamson, C. R. (2010). *The two sides of de Soto: Property rights, land titling, and development*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1940201

World Bank. (2016). *Doing business 2016: Measuring regulatory quality and efficiency*. Retrieved from http://www.doingbusiness.org/reports/global-reports/doing-business-2016

World Bank. (2017a). *Remittance prices worldwide: An analysis of trends in cost of remittance services*. Retrieved from https://remittanceprices.worldbank.org/sites/default/files/rpw_report_march_2017.pdf

World Bank. (2017b). *Financial inclusion*. Retrieved from http://www.worldbank.org/en/topic/financialinclusion/overview

World Bank. (2017c). *Migration and remittances – recent developments and outlook* (Migration and Development Brief 27). Washington, DC: Author. http://dx.doi.org/10.1596/ 978-1-4648-0913-2

# Publications of the German Development Institute/ Deutsches Institut für Entwicklungspolitik (DIE)

## Studies

98 Duguma, Mesay K., Michael Brüntrup, & Daniel Tsegai. (2017). *Policy options for improving drought resilience and its implication for food security: The cases of Ethiopia and Kenya* (87 pp.). ISBN 978-3-96021-048-1.

97 Reeg, Caroline. (2017). *Spatial development initiatives – potentials, challenges and policy lesson: With a specific outlook for inclusive agrocorridors in Sub-Sahara Africa* (176 pp.). ISBN 978-3-96021-048-1.

96 Hein, Jonas, & Britta Horstmann. (2017). *Aligning climate change mitigation and sustainable development under the UNFCCC: A critical assessment of the Clean Development Mechanism, the Green Climate Fund and REDD+* (131 pp.). ISBN 978-3-96021-043-6.

[Price: EUR 10.00; publications may be ordered from the DIE or through bookshops.]

## Discussion Papers

1/2018 Ali, Murad. Monitoring and evaluation in South-South Cooperation: The case of CPEC in Pakistan (35 pp.). ISBN: 978-3-96021-058-0. DOI: 10.23661/dp1.2018.

30/2017 Martin-Shields, Charles. *State fragility as a cause of forced displacement: Identifying theoretical channels for empirical research* (21 pp.). ISBN 978-3-96021-055-9.

29/2017 Lundsgaarde, Erik. *The European Fund for Sustainable Development: Changing the game?* (33 pp.). ISBN 978-3-96021-054-2.

28/2017 Castillejo, Clare. *The EU Migration Partnership Framework: time for a rethink?* (40 pp.). ISBN 978-3-96021-053-5.

27/2017 Hahn, Tina, & Georgeta Vidican-Auktor. *The effectiveness of Morocco's industrial policy in promoting a national automotive industry* (45 pp.). ISBN 978-3-96021-052-8.

26/2017 Stepping, Katharina M. K., & Lilli Banholzer. *Autocratic angels? Democratic demons? The impact of regime type, state capacity and economic development on reaching environmental targets* (33 pp.). ISBN 978-3-96021-050-4.

25/2017 Bracho, Gerardo. *The troubled relationship of the emerging powers and the effective development cooperation agenda: History, challenges and opportunities* (49 pp.). ISBN 978-3-96021-051-1.

24/2017 Matias, Denise. *Slow onset climate change impacts: Global trends and the role of science-policy partnerships* (11 pp.). ISBN 978-3-96021-049-8.

23/2017 Altenburg, Tilman. *Arbeitsplatzoffensive für Afrika* (27 pp.). ISBN 978-3-96021-047-4.

22/2017 Brandi, Clara. *Handel und Umweltschutz – Chancen und Risiken* (38 pp.). ISBN 978-3-96021-046-7.

21/2017 Sommer, Christoph. *Drivers and constraints for adopting sustainability standards in small and medium-sized enterprises (SMEs)* (66 pp.). ISBN 978-3-96021-045-0.

[Price: EUR 6.00; publications may be ordered from the DIE or through bookshops.]

For a complete list of DIE publications:
**www.die-gdi.de**