Blockchain Technology

Riccardo Esclapon

Whitepaper on Blockchain Technology

Main Stakeholders

- Blockchain innovators
- Venture Capitalists
- Banks and financial services
- Coders and developers
- Academics and scholars
- Government and non-government organizations
- Every person, depending on how widely adopted the blockchain becomes long term

WHAT IS A BLOCKCHAIN?

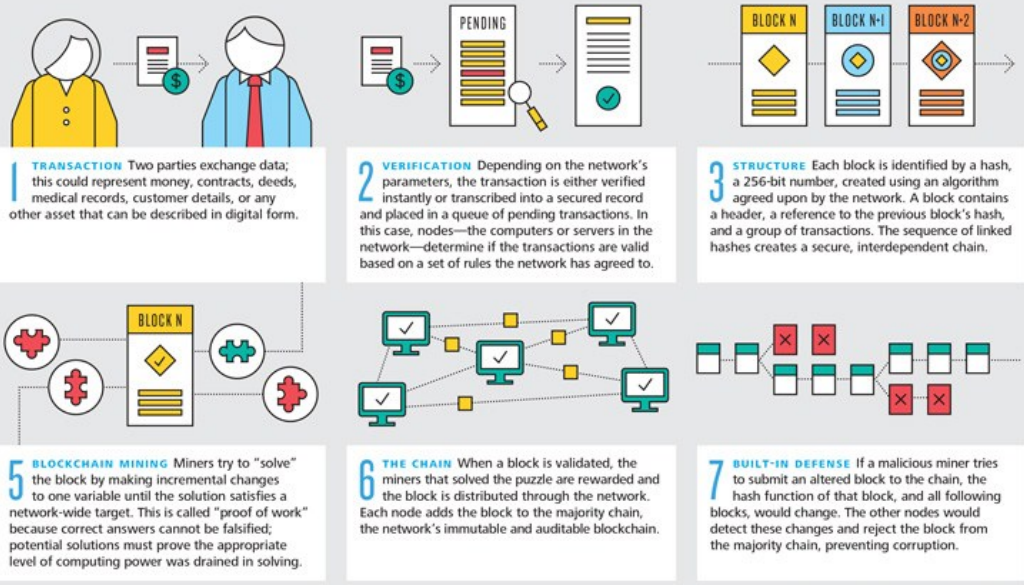
A blockchain is a system of storing data which makes it possible to leverage a global peer-to-peer network to allow secure transactions without a central authority. This is the underlying technology of *Cryptocurrencies*. A cryptocurrency is essentially "virtual" currency that is encrypted and allows for transactions between participants. Bitcoin is a cryptocurrency and is the most famous application of block chain technology, but it is just one of the vast potential applications of the technology. The goal of this white paper is to scratch the surface on what those applications are both today and for the future, and to give a rudimentary but holistic understanding of structural societal problems that will be revolutionized by the blockchain.

BITCOIN

Bitcoin, being by far the most advertised and heard about form of blockchain technology, is the obvious place to start looking at for answers on what makes it so exciting. Although most of us hear talking about Bitcoin when criminal activity is involved or when someone made (or lost) a fortune investing in the "volatile" currency, there are actual practical applications that can have a positive impact on a lot of people and fix some very fundamental problems we face as a society today. Without going into technical detail about the actual mechanics of it or every step (refer to *Figure 1* below for more information), Bitcoin uses cryptography to secure transactions. In order to interact with the blockchain, a user must use a public key and a private key. Your public key is your bitcoin address; this is the combination of letters and numbers that refer to your "virtual safety deposit box" through which other users can send you bitcoin. Your private key, on the other hand, is a secret combination that can be used to access and transfer the currency to a Bitcoin address and should be physically secured by the owner of the ledger (which is the equivalent of a bank account for cryptocurrencies). Using -

Figure 1. Blockchain: How it works

Blockchain allows for the secure management of a shared ledger, where transactions are verified and stored on a network without a governing central authority. Blockchains can come in different configurations, ranging from public, open-source networks to private blockchains that require explicit permission to read or write. Computer science and advanced mathematics (in the form of cryptographic hash functions) are what make blockchains tick, not just enabling transactions but also protecting a blockchain's integrity and anonymity.



1 TRANSACTION Two parties exchange data; this could represent money, contracts, deeds, medical records, customer details, or any other asset that can be described in digital form.

2 VERIFICATION Depending on the network's parameters, the transaction is either verified instantly or transcribed into a secured record and placed in a queue of pending transactions. In this case, nodes—the computers or servers in the network—determine if the transactions are valid based on a set of rules the network has agreed to.

3 STRUCTURE Each block is identified by a hash, a 256-bit number, created using an algorithm agreed upon by the network. A block contains a header, a reference to the previous block's hash, and a group of transactions. The sequence of linked hashes creates a secure, interdependent chain.

4 VALIDATION Blocks must first be validated to be added to the blockchain. The most accepted form of validation for open-source blockchains is proof of work—the solution to a mathematical puzzle derived from the block's header.

5 BLOCKCHAIN MINING Miners try to "solve" the block by making incremental changes to one variable until the solution satisfies a network-wide target. This is called "proof of work" because correct answers cannot be falsified; potential solutions must prove the appropriate level of computing power was drained in solving.

6 THE CHAIN When a block is validated, the miners that solved the puzzle are rewarded and the block is distributed through the network. Each node adds the block to the majority chain, the network's immutable and auditable blockchain.

7 BUILT-IN DEFENSE If a malicious miner tries to submit an altered block to the chain, the hash function of that block, and all following blocks, would change. The other nodes would detect these changes and reject the block from the majority chain, preventing corruption.

Graphic: Deloitte University Press | DUPress.com

Cryptocurrency Benefits

- Transparency. An immutable record of all activity exists
- Network security
- No double transactions
- Low transaction fees
- Nearly instant transactions
- Financial access for everyone
- Protection of financial information

Cryptocurrency Weaknesses

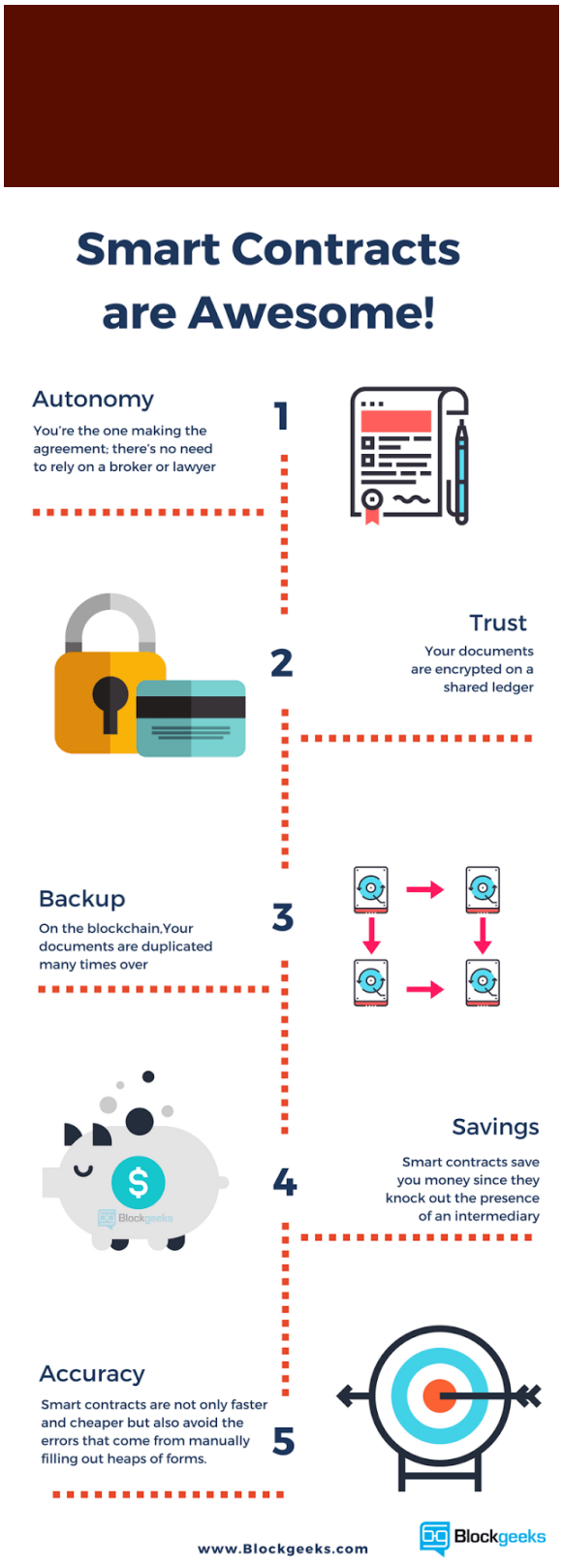
- Difficulty to use, in some cases more than others
- Private key needs to be properly secured
- Not widely accepted
- No protection against mistakes, there is no reversing of a transaction

Cryptocurrency Applications

- A company or government cannot freeze or take your assets. This can drastically improve the life of people in some developing countries by taking their wealth out of someone else's control. This is a potential way out of poverty for some people
- Fraud and identity theft protection
- Immediate settlement on processes that normally involve third parties, like a notary or a lawyer
- Many more

the private key, the user "signs" the transaction (to verify that it was actually them who initiated it) containing the amount and address to be sent to. This information is then sent out to the wider bitcoin network, where it gets *verified* by miners. This process takes information in the block and applies a *one way mathematical function* to create what we call a "hash". To understand the nonsense that you just read, let's look at an example: $N = p * q$. If we pick p=5 and q=6, we can very easily calculate N to be 30. On the other hand, if we know that N = 30 but nothing else, it is a lot more difficult to reverse engineer the values for p and q. You have to figure out all the possible combinations and determine the right one, which takes infinitely more computing power than simply multiplying those two numbers. On a very basic level, the Bitcoin miners are putting tremendous computing power towards solving very hard one-way functions, which are increasingly difficult to solve as the blockchain grows in size, but as we saw from the other example, incredibly harder to reverse. This makes the Bitcoin blockchain unhackable. In order to fully understand how un-hackable it is, realize that the current estimated annual electricity consumption as of November 14th, 2017 in TWh of Bitcoin mining is 27.28* and is constantly on the rise. That is enough electricity to power an estimated 2,526,122 U.S. households. That is so much energy, that it is becoming a very legitimate environmental issue. A single Bitcoin transaction could power 8.77 U.S. households for an entire day. Bitcoin is currently using 0.13% of all electricity in the world, and although that is an issue that the community is currently in the process of resolving (Bitcoin's code and functionality can be modified if there is consensus in the community), that also means that it would take a completely unrealistic amount of computing power to reverse the one way functions that miners use all that electricity on. What all of this really means, is that the information on the blockchain is "controlled" by an independent computer algorithm that no single party can influence (which is usually a government, good or bad). The way the blockchain works and the way our institutions operate, make Bitcoin an incredible use case for this technology (as well as being a tremendous investment opportunity, giving it lots of attention), but what other applications derived from blockchain technology could there be that might not be as obvious or talked about that are likely to change our daily lives? Let's take a look at "Smart Contracts" to try and understand what some of those applications could be.

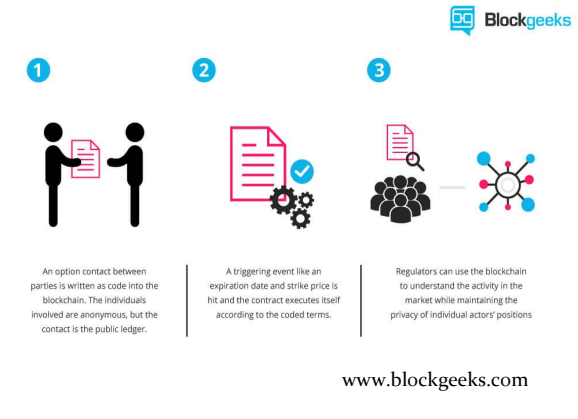
*estimates are from www.bitcoinenergyconsumption.com



SMART CONTRACTS

Smart contracts are self-executing contracts made possible by the blockchain, and are used with the Ethereum blockchain (discussed in the next section). At its very essence, a transaction is a contract between the seller and the buyer. That is typically not enough however: often, you need some form of third party to ensure the enforcement of any given contract. Let's take a look at an example where that is **not** the case to see what problems arise: Let's say someone wants to buy drugs on Craigslist. Both the buyer and the seller want to have a transaction, but without a third party to ensure both sides are getting properly compensated, there is a profound lack of trust that inevitably affects that transaction. It is therefore natural for services of legal activities to step in to fix the problem. If we look at Airbnb, for example, one party rents out their home or part of their home to a stranger, while the other one sleeps in a stranger's home. If Airbnb did not exist, people would be pretty reluctant to do either of those things. Smart contracts are able to effectively fix the same issues that a third party like Airbnb does, but they provide a more flexible, cost effective and efficient solution to most problems, some of which might not be fixed otherwise; if there is no financial motive to fix that problem for example, no third party would step in and do so, but with smart contracts we can easily implement solutions to those problems. As William Mougayar, a blockchain expert and entrepreneur puts it, traditional financial transactions are similar to how you would share a word document before Google Docs. You would have to send someone the document probably via e-mail and have them open it, review it and send it back to you with their comments and revisions. The blockchain, is like Google Docs, where "both parties have access to the same document at the same time, and the single version of that document is always visible to both of them. It is like a shared ledger, but it is a shared document". This might not seem consequential, but the implications are large. It means that you no longer need a third party ensuring that the transaction goes smoothly for both the buyer and the seller, because the system in place is able to provide the same or superior level of trust as any human (and therefore flawed) third party.

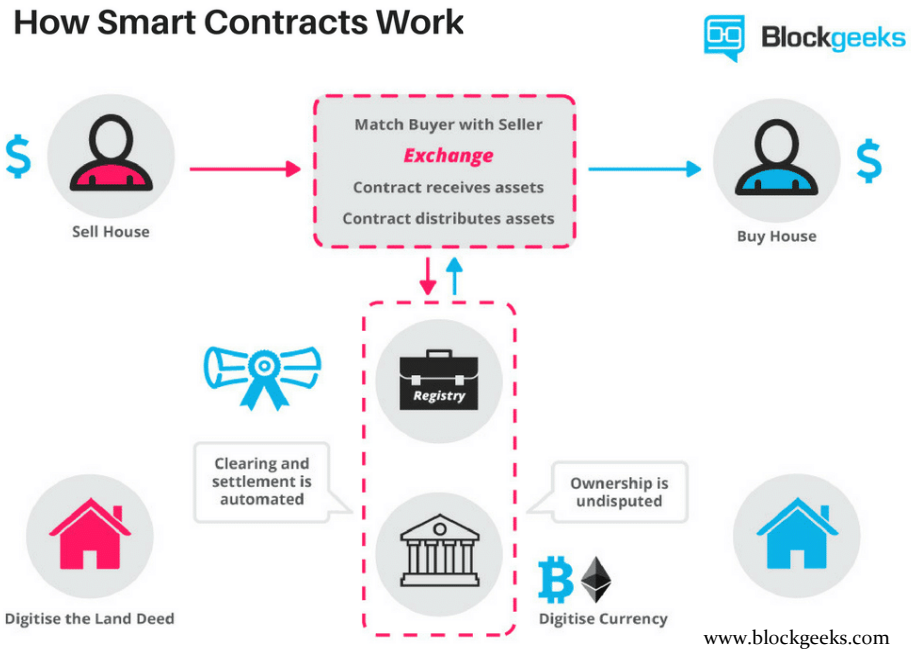
Let's look at an example: you want to buy tickets for a basketball game off of an online website. Traditionally, the basketball team would go to a third party that specializes in ticket sales, to whom they give up a portion of their profits or pay a large monthly sum. They might do this because they do not know how to deal with billing customers and do not have the

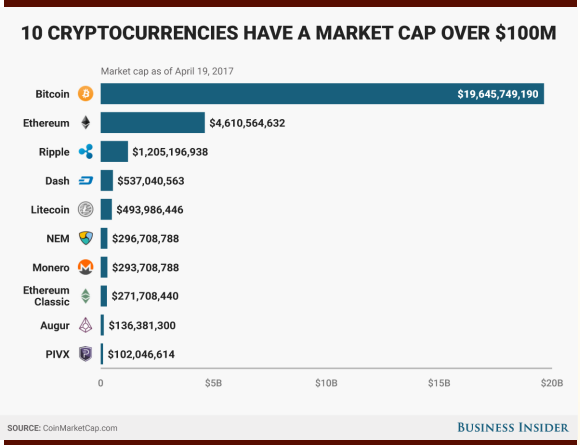


Examples of Potential Smart Contract Applications

- Cars. Insurance companies could issue smart contracts that charge rates that depend on the conditions of the driving. A smart contract might even be able to determine who was at fault in case of a crash and distribute the right amounts automatically without getting anyone else involved
- Hospitals or any institution or business that might handle sensitive data. The blockchain would be the safest way to safely store social security numbers, and medical histories, which could be programmed to allow anyone with access to view the medical history; they would also be able to gain access immediately instead of waiting for paperwork and bureaucratic steps to finish.
- Purchasing property or expensive items that typically require a handsomely paid middleman could be streamlined and cost-effective
- Improved gambling

appropriate infrastructure to safely handle sensitive customer data. The customer, respectively, would go directly to the third party website and deal with them directly for the transaction. The third party can then hold what each side was promised and give them respectively once both contracts have been honored. If a smart contract were used, the process would be streamlined and be more cost effective and efficient for both parties. Here is what it would look like: the basketball team wants to sell you a ticket. They issue you a smart contract, which acts as an intermediary. The smart contract would be connected to your public address for your ledger, and once both the money and the ticket are successfully transferred and received, the smart contract distributes them safely. The implications of this technology go beyond buying tickets to a basketball game. As the IoT (Internet of Things) becomes more and more the reality that we live in, the capabilities and potential of these smart contracts will improve. Let's take a look at what this would mean for the most common type of contract in the world for example; a contract to lease an apartment. You want to rent an apartment, and pay in cryptocurrency. You get a receipt recorded within the smart contract. You are given some form of access to the apartment, probably through a code to unlock the door. If you do not receive the code in time, the smart contract issues you a refund. If the landlord issues the code to unlock the door ahead of time, the smart contract still waits for the proper date, on which it will release both the code and the cryptocurrency funds (the monthly rent). This would never really happen (hopefully), but in theory, if the tenant did not pay his rent on time and had a grace period before he/she is kicked out, the smart contract could disable access to the washing machine, or make the water in the shower be limited in temperature to only get lukewarm, or whatever else was possible through connected devices one day in the future.

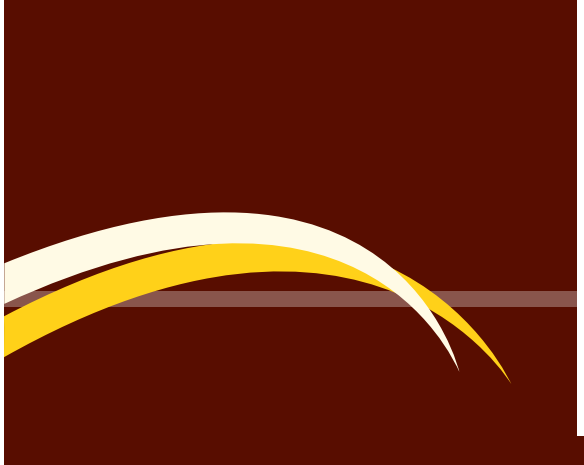




THE BLOCKCHAIN LANDSCAPE

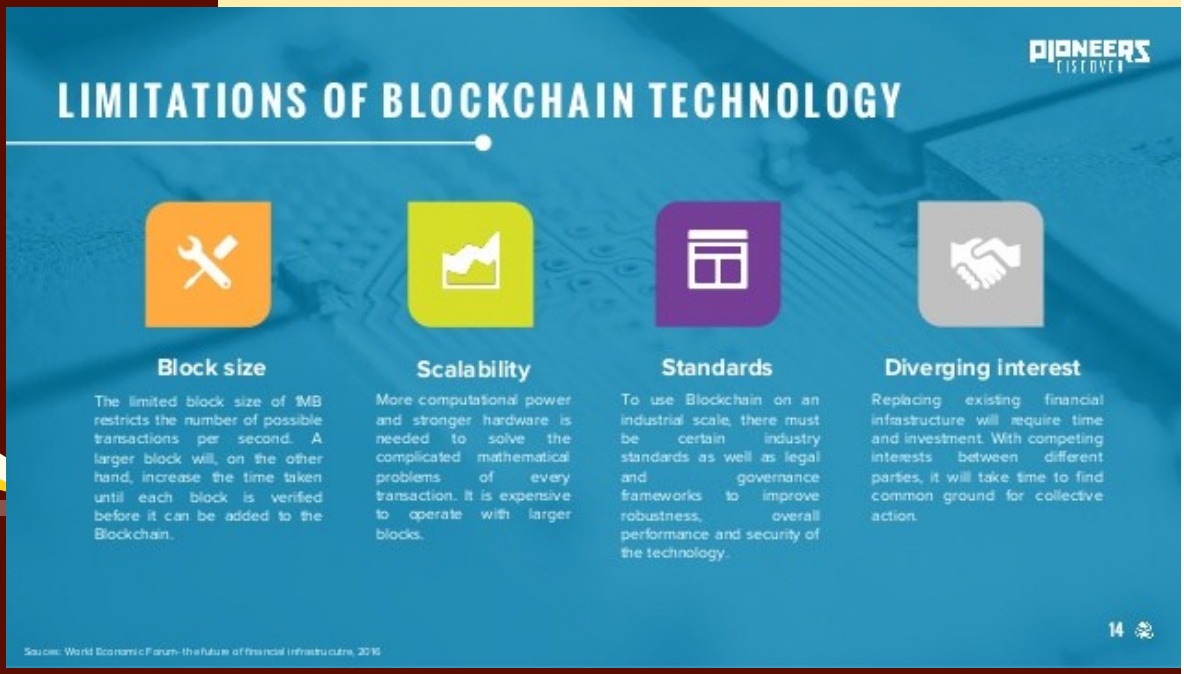
Bitcoin was the first cryptocurrency to introduce the idea of the blockchain, but today there are more than 500 that leverage this technology. Some cryptocurrencies have better applications than others. The smart contracts we discussed in the previous section are what the Ethereum blockchain uses, and which many people consider to be superior to the more limited applications of Bitcoin. Ethereum is the second most popular cryptocurrency that currently exists, and it could not be more different from Bitcoin. While Bitcoin leverages privacy and tangible value (and predictable growth of that value) to facilitate transactions, Ethereum focuses on compatibility, applications and working with governments and organizations to deliver solutions through smart contracts, instead of fighting against them like Bitcoin famously does. In fact, Bitcoin is considered to be the first version of cryptocurrencies, and Ethereum the "2.0 version" and evolution of it. Again, the smart contracts previously discussed are an innovation that only Ethereum brought about. The main difference between Bitcoin and Ethereum, is that in addition to having a series of transactions, the Ethereum blockchain also contains smart contracts. Once a smart contract is created on the blockchain, users of the platform can interact with it. For example, the state of Colorado could issue a smart contract for tenants and landlords to utilize. The parties would enter into the smart contract and the Ethereum blockchain then creates a permanent record of the inputs for the transaction, the code for the smart contract, and the output from when the smart contract is executed. The blockchain is very flexible with the type of smart contracts you can create, and in fact you could even have smart contracts that create other smart contracts.

Ethereum is not necessarily a "better" solution, but in my opinion it is a more realistic and possible to implement alternative to Bitcoin (mostly because it plays nice by companies and governments), and will play a particularly pivotal role in driving innovation in blockchain technology and applications.



BLOCKCHAIN LIMITATIONS

Both Bitcoin and Ethereum are blockchain “experiments” in their own merit, and are currently both resolving issues of their own that arose from their success and widespread adoption. Ethereum, for example, has a massive scaling problem and can currently only handle 30 transactions per second, while Bitcoin keeps slowing down as the blockchain keeps getting longer and can currently handle about 7 transactions per second. Neither one can compete with the average 2,000 transactions a second by Visa and a maximum capacity of 56,000 per second. As this first round of proof of concept blockchain technology runs into problems, it will be interesting to see the extent to which the technical solutions and infrastructure will keep up (or in most cases probably not keep up). The solutions are possible, but what seems like a bigger challenge is getting the community to agree on those solutions. The code for Bitcoin, for example, is available for everybody to look at (open source) and even modify. Anybody can change it, but the changes need to be accepted by the majority of the community, and making sure the majority’s interests are furthered can be easier said than done. This has led to much controversy and even lead to a “fork”, where the community was undecided and it lead to the creation of new cryptocurrency called “Bitcoin Cash”; the main reason it came about, was that the interests of the miners differed from the interests of other parties involved, thus leading to disagreement. All the protocols and politics going on behind the scenes are much too complicated to delve into, but the really important idea here is that the future of cryptocurrencies and blockchain technology and the applications of it, depends in great part on circumstances and decisions by governments or powerful individuals. Therefore, making any definite conclusions on what the landscape for this technology is going to look like in the future is close to impossible, which very well might be its biggest limitation.



BIBLIOGRAPHY

- Nir Kshetri (2017) Will blockchain emerge as a tool to break the poverty chain in the Global South?, Third World Quarterly, 38:8, 1710-1732, DOI: 10.1080/01436597.2017.1298438
- Scott B, Loonam J, Kumar V. Exploring the rise of blockchain technology: Towards distributed collaborative organizations. Strategic Change. 2017;26:423–428. https://doi-org.colorado.idm.oclc.org/10.1002/jsc.2142.
- Kirkland, Rik and Don Tapscott. "How Blockchains Could Change the World." *Mckinsey Quarterly, no. 3, July 2016, pp. 110-113. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=bth&AN=118459144&login.asp&site=ehost-live&scope=site.*
- *Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin.org, bitcoin.org/bitcoin.pdf.*
- *Tapscott, Don, and Alex Tapscott. "Realizing the Potential of Blockchain A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies." World Economic Forum, July 2017.*
- *Biella, Matteo, and Vittorio Zinetti. "Blockchain Technology and Applications from a Financial Perspective." Unicredit Techincal Report, 26 Feb. 2016.*
- *@dmitry-buterin, Dmitry Buterin, et al. "What Are Smart Contracts? A Beginner's Guide to Smart Contracts." Blockgeeks, blockgeeks.com/guides/smart-contracts/.*
- *"The Social Benefits of the Blockchain – Seeds – Medium." Medium, Medium, 21 July 2017, medium.com/@SeedsInc/the-social-benefits-of-the-blockchain-b09eea682f42.*
- *Taylor, Simon. "Blockchain: Understanding the Potential." Barclays, July 2015.*