Blockchain technology: principles and applications

Chapter · September 2016

DOI: 10.4337/9781784717766.00019

1 author:

Marc Pilkington
Université Bourgogne Europe

Blockchain Technology: Principles and Applications

Marc Pilkington[1]

[1] Marc Pilkington is Associate Professor of economics at the University of Burgundy, France.

Blockchain Technology: Principles and Applications

ABSTRACT

This chapter expounds the main principles behind blockchain technology and some of its cutting-edge applications. We first present the core concepts of the blockchain. Secondly, we discuss a definition put forward by Vitalik Buterin; we sketch out the shift toward hybrid solutions, and we sum up the main features of decentralized public ledger platforms. Thirdly, we show why the blockchain is a disruptive and foundational technology, but we expose the potential risks and drawbacks of public distributed ledgers that account for the shift toward hybrid solutions. Finally, we present a non-exhaustive list of important applications, bearing in mind the most recent developments.

Blockchain Technology: Principles and Applications

Long before the advent of the blockchain, digital cash had been conceptualized in a setting with a central server trusted to prevent double-spending (Chaum, 1983)[1]. In spite of major cryptographic advances, failure to ensure compatibility between centralization, anonymity, and double-spending prevention, eventually put the viability of this new form of money into question. Three decades later, Bitcoin has acquired notoriety on the global marketplace, by replacing the central server's signature with a consensus mechanism based on proof of work (Back et al, 2014, p.3). The novelty and improvement over Chaum's thought-experiment are the decentralized nature of the payment system allowed by blockchain technology, thereby ushering in a new era that extends beyond global payments, to corporate governance, social institutions, democratic participation and the functioning of capital markets (Wright and De Filippi, 2015, p.3). In this chapter, we present the main principles behind this revolutionary technology as well as some cutting-edge applications.

In a first part, we present the core concepts. Secondly, we discuss a definition by Vitalik Buterin, the distinction between public and private blockchains, and the features of public ledgers. Thirdly, after restating the foundational and disruptive nature of this technology, we present the risks and drawbacks of public distributed ledgers, and show why the latter explain the shift toward hybrid solutions. Finally, we sketch out a list of important applications, bearing in mind the most recent developments.

A PRIMER ON BLOCKCHAIN TECHNOLOGY

The Crypto-economy

Cryptographic techniques draw on the science of cryptography, and allow for the protection of sensitive information (organizational, institutional or personal), either in storage or in communication. Initially devised for information security systems (Saper, 2013, p. 673), they are now moving into other use spaces.

The crypto-economy is an "economic system, which is not defined by geographic location, political structure, or legal system, but which uses cryptographic techniques to constrain behaviour in place of using trusted third parties" (Babitt and Dietz, 2014). A new subset of economics is hence emerging with the rise of crypto-economics, which may be defined as "a formal discipline that studies protocols that govern the production, distribution and consumption of goods and services in a decentralized digital economy. Cryptoeconomics is a practical science that focuses on the design and characterization of these protocols" (Zamfi, 2015).

In the final section, a typology of crypto-economy instruments is provided.

The Blockchain

Blockchain technology ensures the elimination of the double-spend problem, with the help of public-key cryptography, whereby each agent is assigned a private key (kept secret like a password) and a public key shared with all other agents. A transaction is initiated when the future owner of the coins (or digital tokens) sends his/her public key to the original owner. The coins are transferred by the digital signature of a hash. Public keys are cryptographically generated addresses stored in the blockchain. Every coin is associated with an address, and a transaction in the crypto-economy is simply a trade of coins from one address to another. The striking feature of the blockchain is that public keys are never tied to a real-world identity. Transactions, although traceable, are enabled without disclosing one's identity; this is a major difference with transactions in fiat currencies that, with the exception of (non-traceable) cash transactions, are related to specific economic agents endowed with legal personality (whether physical or juridical). Figure 1, below, offers a succinct chronology of the main turning points in the development and deployment of blockchain technologies.

With the formal release of Bitcoin XT 0.11C in August 2015, the Bitcoin world was shaken by a technical and near-ontological debate in inner circles of core developers about the possibility of forking the blockchain, so as to enhance the timing, execution and scalability of the cryptocurrency (Cotillard, 2015).

[Figure 1 here]

Payment Finality

Payment finality is "the discharge of an obligation by a transfer of funds and a transfer of securities that have become irrevocable and unconditional" (Committee on Payment and

Settlement Systems, 2003, p. 496). In a world of fiat money, payment finality is conceptualized in relation to bank money within a triangular payment structure involving a payer, a payee, and a bank acting as a ‘gobetween’ (Rossi, 2004, p.3). This ‘gobetween’ is in fact the trusted third party required in all payments until the advent of crypto-currencies. Yet, the latter are trustless protocols that dispense with the trusted third party. The meaning conferred to payment finality in a crypto-economy differs from the traditional banking system: a transaction is final once it is included in the blockchain, thereby becoming simultaneously verifiable by many sources (Dwyer, 2014, p.4).

Miners and Computational Problem Solving

The blockchain is a chain of transactional records that a subset of network participants (also known as ‘miners’) enriches by solving difficult computational problems. Miners fiercely (and anonymously) compete on the network to solve the mathematical problem in the most efficient way, thereby adding the next block to the blockchain. The block reward (i.e. newly minted coins) is sent to the miner’s public address. If the miner wants to spend these coins, (s)he must sign with the corresponding private key. When system-wide mining power increases, so does the difficulty of the computational problems required to mine a new block (Böhme et al, 2015, p. 218). This difficulty level is adjusted to keep the block-generation pace constant, roughly ten minutes (Dwyer, 2014, p. 5).

In the early days, mining was primarily done by individuals on home computers through central (or graphics) processing units. With rising complexity, algorithms have required more powerful mining techniques taken over by application-specific integrated circuits (ASIC), cloud mining and mining pools. 21 Inc, the self-proclaimed first Bitcoin computer, aims to revolutionize both the mining and the semiconductor industries, with its embedded mining innovation (Srinivasan, 2015). BitShare, a mining chip, potentially embedded into millions of Internet devices, works collectively to mine new currency. These new streams of crypto-currency both solve the problem of bearing the cost of micropayments, and bring to the fore a new crypto-business model by helping finance the chips themselves (Niccolai, 2015). The technical details remain unclear, but if the latter innovation were to be replicated and widely adopted, it would be a game changer for the whole crypto-economy.

Hashes and Hash Functions

The essence of the blockchain is informational before being economic or monetary, conducive to many emerging and increasingly popular token-free blockchains. It relies extensively on hashes and hash functions. A hash (output) is the result of a transformation of the original information (input). A hash function is a mathematical algorithm that takes an input and transforms it into an output. A cryptographic hash function is characterized by its extreme difficulty to revert, in other words, to recreate the input data from its hash value alone. This is called the collision resistance.

Proof-of-work and Proof-of-stake

The hashcash proof-of-work function is at the heart of block generation in the Bitcoin protocol. Cryptographic proofs-of-work are required for new blocks to be accepted. For verifying transactions, and calculating proof-of-work, Bitcoin relies on a cryptographic hash function, called the double SHA256 hashing algorithm, wherein the target is a 256-bit (i.e. extremely large) number[2] that all Bitcoin clients share. The lower the target, the more difficult (and processing time consuming) it is to generate a new block. For a block to be valid, it must hash to a value less than the current target. Each newly produced block acknowledges that work has been done generating it.

Proof-of-stake is a proposed alternative to proof-of-work already implemented for certain altcoins (other than Bitcoin), whereas others rely on a hybrid protocol (Graydon, 2014). Instead of splitting blocks across proportionally to the relative hash rates of miners (i.e. their mining power), proof-of-stake protocols split stake blocks proportionally to the current wealth of miners. Buterin (2014b) argues that proof-of-stake has a number of distinct advantages over proof-of-work (non-wasteful protocol, decreased likelihood of a 51% attack, potentially faster blockchains, etc).

A HOLISTIC VIEW OF BLOCKCHAIN TECHNOLOGY

Vitalik Buterin's Definition of the Blockchain

We have previously exposed the core concepts of the blockchain, and alluded to Bitcoin, which is today one blockchain-based platform amongst others, although it still is the most famous worldwide. For Vitalik Buterin (2015a), the blockchain is

> a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible, and which carries a

> very strong cryptoeconomically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies.

The definition arguably lacks scientific rigor ('a magic computer' is a debatable term). It is nevertheless useful to discuss, and highlight the features it omits. By not referring to oft-heard terms 'ledger', 'money' or 'transactions', Buterin makes the point that the essence of the blockchain is informational and processual, and does not relate directly to the monetary sphere. In this sense, blockchains may exist *without* an underlying token. In the same vein,

> If we modify our "database" schema so that each row can represent multiple assets, rather than the blockchain's native currency, then we can rid ourselves of that currency entirely. This leaves us with a blockchain as a way to achieve consensus and security in a peer-to-peer financial application for *any class of asset* (Greenspan, 2015, emphasis in the original).

By and large, this conception is not shared by all crypto-experts: "the coin is an integral part of the network's incentive mechanism to maintain its security; the two have an existential symbiotic relationship" (Swanson, 2015, p.8). Likewise, for technology entrepreneur Jeremy Allaire (2015; cited by Byrne, 2015, emphasis added),

> [It is often heard that] the blockchain's interesting but the "currency" or the store of value's not very interesting. That's just a fallacy. They're not possible separately. *There has to be an underlying value to the token that's used to move value*, and there has to be an incentive system for the creation of that token and the exchange of that token. That is the only way these systems work… that's a thing I think a lot of people fail to understand.

Likewise, this question is critically discussed by Gideon Greenspan (2015).

Buterin does not link the conceptual definition to any particular consensus algorithm, or technical properties of the blockchain. The Bitcoin algorithm is not a definitional feature of the blockchain, but a mere application thereof. Blockchains are the visible (albeit intangible) consequence of the actions taken by the users of a network. The blockchain is structured around a network, which is evolutionary in essence (Pilkington, 2016, forthcoming). This evolutionary process may be mapped by a state transition function, describing what state to move to, on receiving a given input in a given state. Again, Buterin rightly refrains from specifying any state transition function.

We find Buterin's definition useful in the sense that amongst the previously discussed core concepts, 'crypto-economy' and 'payments finality' are not definitional features *per se*, but rather fundamental characteristics of major blockchain applications, extended to the monetary and economic sphere.

Private, Public and Hybrid Blockchains

Public decentralized ledgers are accessible to every Internet user. The public nature stems from the free and unconditional participation of everyone in the process of determining what blocks are added to the chain, and what its current state is (Buterin, 2015b). These fully decentralized blockchains rest on a consensus mechanism of proof-of-work (or proof-of-stake) for validation purposes: "in the case of Bitcoin, the "longest chain – the chain with the most proof-of-work – is considered to be the valid ledger" (Swanson, 2015, p.4).

In a fully private ledger, write-permissions are monitored by a central locus of decision-making. Read-permissions are either public or restricted (Buterin, 2015b). A private blockchain amounts to a permissioned ledger, whereby an organizational process of Know-Your-Business (KYB) and Know-Your-Customer (KYC) enables the white listing (or blacklisting) of user identity. The difference between public and private blockchains is the extent to which they are decentralized, or ensure anonymity. Between the two extremes, there exists a continuum (Brown, 2015, Allison, 2015) of "partially decentralized" blockchains (Buterin, 2015b), rather than a strict public/private dichotomy. Partially decentralized, also called "consortium blockchains" (Buterin, 2015b), constitute a hybrid between the low-trust (i.e. public blockchains) and the single highly-trusted entity model (i.e. private blockchains).

Features of Decentralized Public Ledger Platforms

Bitcoin was the first decentralized public ledger, and has acquired a global status since 2013-2014. Although we are still far away from mass adoption, the success of Bitcoin is to be credited to the underlying innovation called the blockchain. What is the blockchain? It is simply a secure public ledger platform shared by all parties through the Internet or an alternative distributed network of computers. With the notable exception of token-free applications, the tour de force of the blockchain is to remove the need for a trusted third party to guarantee a transaction. Hereafter, we list five important features of public ledgers.

Protocol for Sending, Receiving and Recording Value

When extended to the (crypto) monetary sphere, the blockchain is nothing less than the continuation of the value transfer system, a technological innovation patented in the USA in 1998 (Jones et. al, 1998). Early value transfer systems embodied the concepts of value storage, encryption, and cryptographic public/private key pairing, at the heart of modern crypto-currencies. The main difference between blockchain technology and these crude predecessors is the level of decentralization of the network. As defined by Benkler (2006, p.62), "'[d]ecentralization' describes conditions under which the actions of many agents cohere, and are effective despite the fact that they do not rely on reducing the number of people whose will counts to direct effective action". Most payment platforms, such as Visa, rely on private secure communication networks, although "VISANet connects to both wired, wireless and also the Internet for processing". The fact that Visa owns its physical and virtual nodes (Khan, 2012) confers a centralized nature to its network. Although the emergence of major players in the mining industry is conducive to novel centralization trends (Sams, 2014, Böhme et al. 2015, 219-220), Bitcoin was initially designed as a decentralized network (Nakamoto, 2008, p.4). Hence, the blockchain is purely Internet-based, and the Bitcoin's blockchain is decentralized. The level of decentralization is far greater in the blockchain than in the first value transfer systems, thanks to the immense network effect of the Internet. However, the current level of decentralization is increasingly questioned by the emergence and adoption of private blockchains by organizations (see infra).

Internet-based Value Containers: Coins or Tokens

Blockchain Technology: Principles and Applications

The “crypto-currency” blockchain set (Byrne, 2015), which does not encompass all the “distributed application/ledger” blockchain set (ibid.), is a modern value transfer system, namely a protocol for sending, receiving and recording value on a public ledger. No transmission of value would ever be possible without the existence of a value container. This is what economists, who emphasize the unit of account function, call money (Schmitt, 1984, Keynes, 1930, Innes, 1913).

> *The use of money does not necessarily imply the physical presence of a metallic currency, nor even the existence of a metallic standard of value*. We are so accustomed to a system in which the dollar or the sovereign of a definite weight of gold corresponds to a dollar or a pound of money that we cannot easily believe that there could exist a pound without a sovereign or a dollar without a gold or silver dollar of a definite known weight (Innes, 1913, p.377).

Drawing on the narrative developed by Milton Friedman (1992), Barnes (2015) provides an insightful historical comparison between the blockchain principle and the stone coins called rai, up to 3.6 metres in diameter, used as a monetary instrument on the Pacific island of Yap. The stones, although huge, were in fact immaterial. What mattered was the continuous record of ownership and transactions that would help determine with precision, at a given moment in time, who the legitimate owner of the coin was. Today’s blockchain model works the same way: the public ledger or database is simply a more modern way to map out the actual transfer and ownership crypto-currency. The value container is called a coin, a terminology reminiscent of the currency lexical field, and in fact the primary purpose of a coin (whether tangible or virtual) is precisely to carry value between members of a community of payments. However, the value container may contain instead a fiat currency unit or a financial instrument, which would undermine its full-fledged virtual currency status. Strictly speaking, value containers (or tokens) and currencies are thus not synonymous.

Incentives for Collaborative Effort

The Bitcoin ecosystem analyzed through the lenses of complexity theory departs from mainstream postulates, such as rationality, equilibrium, and self-interest:

> Miners are self-interested in the sense that they hope to derive a future gain from their mining endeavor. Yet, the viability of the crypto-currency implies *a sense of altruism* amongst miners, ensured when individual and systemic incentives are aligned. Notwithstanding the existence of personal motives, *there might exist a cooperative behavioral dimension* in sharp contrast with a neoclassical economic arena dominated by Darwinian principles (Pilkington, 2016, forthcoming, emphasis added).

The alignment of individual and systemic incentives amounts to a groundbreaking scheme "for eliciting effort and the contribution of resources from people to conduct various record-keeping and verification activities for the public ledger" (Evans, 2014, p.3). In the Bitcoin ecosystem, decentralized public ledgers are intensive in labour and computer processing time, thereby reflecting how miners are rewarded (ibid., p.4).

Open Source Licenses and Governance Mechanisms

A central feature emphasized by Buterin (2015a) is the licensing model for enabling changes to the software of either the public ledger currency platform, or a token-free blockchain application. Standard open-source licenses are paramount so that users can modify the platform in a collaborative fashion (Evans, 2014, p.4).

Open source is a development method enabling software to harness the power of distributed peer review and processual transparency. It comes hand in hand with increased reliability, flexibility and reduced costs. (Open source initiative, 2015). The term open development method (ODM), or community-led development, has been coined to describe this new collaborative mode of governance, wherein the emphasis is primarily on collaboration and the community of users.

Immutability of the System

Immutability is a characteristic of blockchain technology (Coletti, 2015). Derose (2015b) argues that immutability, or resistance to tampering, is what confers its intrinsic value to crypto-currencies, thanks to a revolutionary feature, namely “the ability to declare a truth, globally and without a centre of authority, regardless of what anyone else does to change this truth”.

Certain features of the blockchain concept might be relaxed (see infra), but not immutability, which remains crucial: “a blockchain does not need to be a shared ledger, nor does it need to have a distributed consensus. It can be completely centralized as long as its data/state is externally verifiable and all data is immutable” (anonymous reviewer cited by Swanson, 2015, p.59). So if immutability is what ultimately makes a crypto-currency intrinsically worth trading, this must be the most essential feature of all. Hasn’t the Bitcoin’s blockchain ever experienced failure since its inception? On March 11, 2013, the network proved dysfunctional, with the appearance of a fork resulting in two concurrent Bitcoin networks with two distinct blockchains running in parallel, before one of them was eventually abandoned by the community of miners a few hours later (Buterin, 2013). Buterin (ibid.) describes a more serious bug that shook the network in August 2010, yet without any serious consequence. He explains the technical details of the incident akin to an integer overflow bug[3] that required the Bitcoin software to be republished resulting in a fork of the blockchain with a new valid chain overtaking the old one. Notwithstanding these two incidents, the Bitcoin distributed ledger remains immutable to date.

PUBLIC LEDGERS UNDER CRITICISM: TOWARD HYBRID SOLUTIONS?

Broadly available technology has always afforded a way of transferring power from central authorities to the masses (Buterin, ibid.). The same way the determination and communication of time, by means of large and expensive clock towers, was a testimony to the concentration of power in the hands of a minority, the tracking of time by individuals was enabled by early engineering innovations a few centuries ago (ibid.). The blockchain runs counter to the underlying principles behind traditional banking. A banker has a tendency to centralize all information related to payments, transactions and loans, to store and record the corresponding data in a computer system. This is what the business of the banker is about: storing money and information about money. Blockchain technology might yet prove extremely useful to the banking industry as a whole. We will review potential applications that could improve the efficiency and reduce the costs of financial institutions (see infra).

Derose (2015a) is full of praise for the remarkable capabilities of the blockchain that not only removes the need for trusted third-parties in money value transfers, but also reduces transaction costs to nearly zero, and enables fast transactions. Is Derose's optimism warranted? Although transaction costs have undoubtedly been reduced by crypto-technology, it remains true that "proof-of-work based consensus protocols are also slow, requiring up to an hour to reasonably confirm a payment to prevent double-spending" (Kwon, 2014, p.1). Maxwell (2015), a Bitcoin's system developer and current Blockstream's CTO, reminds us that traditional money systems are fundamentally based on trust, which is costly to maintain, and unpredictably violated. Agents must trust banks, the parties moving the funds, and the central bank that conducts monetary policy. Blockchain technology replaces a system based on trust by one of mathematically defined and mechanically enforceable rules (ibid.). In the global payments industry, a plethora of contingent services are provided by auditors, legal specialists, payment processors, brokers etc. Against the odds, blockchain technology disintermediates third-party transaction verifiers, thereby pushing the disintermediation process into unchartered territory in the modern era.

Swanson (2015, p.12) asks whether there is "a way of using distributed consensus mechanisms to transmit value transparently and securely without expensive proof-of-work methods?" A fully decentralized distributed ledger functions with anonymous validators (proof-of-work methods), to create a truthful record. Contrariwise, what would be the performance of a distributed consensus ledger with *known* validators endowed with the power to punish those who do not follow protocol? Using the example of two fictitious agents Bob and Alice, Swanson (ibid.) shows that the second scenario minimizes the need for interpersonal trust even more than the first one.

Buterin (2015b) has identified several weaknesses intrinsic to immutable public ledgers. Firstly, in some cases, such as land registries, reversibility is a desirable property of the blockchain, as government-uncontrollable registries risk not being recognized at all. Buterin (ibid.) admits that a public ledger with a smart contract allowing the government to enter the game, nuances this conclusion, without undermining it (ibid.). Secondly, the concept of an anonymous 51% attack arising from a collusion of miners taking control of a public decentralized network is widely documented in crypto-economics. The pitfall is eliminated in the event of *known* validators. Thirdly, transaction costs processed by public ledgers are higher, whereas private blockchains, with their reduced number of high-processing nodes, enable cost-effective transactions. Buterin (ibid.), however, notes that, thanks to scalable blockchain technology, there is an asymptotic trend bringing long-term costs of public ledgers in line with efficient private ones. Fourthly, the connectivity between nodes in public blockchains is lesser than in private ones, which increases the laps of time for total transaction finality. All things being equal, private blockchains are faster. Lastly, regarding the issue of privacy options, public ledgers can hardly compete with private blockchains and their restrictions of read-permissions (ibid.).

For Waldman (2015), the distinction between permissioned and permissionless blockchains is one between discretionary, wherein nodes represent identifiable members, and anonymous antidiscretionary blockchains (e.g Ethereum and Bitcoin). The latter “prioritize values of predictability and authority” whilst the former “prioritize participation, representation, and flexibility” (ibid.); they are simply different tools that serve different purposes:

> Fundamentally, an antidiscretionary blockchain is a technique for deploying a long-running, predictable software application on top of a community of people whose role is merely to verify. A discretionary blockchain is a technique for reifying and composing the everchanging will of a community in the form of a distributed software application (ibid.).

The fact that nodes do not represent identifiable members poses a number of ethical issues with regard to antidiscretionary blockchains. In Ethereum, “everything is dictated by the code,”, yet “anything that is completely computer-operated is a potentially oppressive system.” (De Filippi cited by Schneider, 2014). This sense of caution is reinforced by a comment of Buterin (2014a) on an article written by Schneider (2014):

> Lately I have become much more comfortable with the idea of computer-controlled systems for one simple reason: our world is already computer controlled. The computer in question is the universe with its laws of physics and humans provide the inputs to this great multisig by manipulating their body parts. At the "base layer", *no semblance of compassion really exists: the*

> *person who wins is the one who can wield the most violence*. This is true even in anarchies; when it comes down to it, it's the guy with the guns who has the final say. And yet humans have managed to take this base layer and build all sorts of other structures on top. The world of programmatic smart contracts is exactly the same; it's just a set of cryptographic "laws of physics" that you can build stuff on, except it's designed to be both much more efficient and at the same time voluntarist at the core - unlike in the "real world".

Buterin’s optimism regarding the infallibility of unbreakable machine-generated contracts is questioned by Palley (2014) who puts the human condition center stage: “why is the notion of an unbreakable contract problematic? It assumes that software can create perfect understanding between people, and that all terms in a contract can be described in code (which is language, still)”. For Guerrini (2015), the intersection between blockchain technology and artificial intelligence is likely to reshape future management practices in human organizations.

Blockchains are cutting-edge informational devices answering different needs and objectives. The resulting “way of blockchaining” (Buterin, 2015b) is contingent on a number of organisational and strategic parameters. The public vs private blockchain debate comes down to a bifurcation between permisionned and permissionless validators (Swanson, 2015, p.25). Yet, “the bifurcationists are not saying one approach is better than the other, rather, they each solve different problems” (ibid.). The blockchain world is an abstract space between the public ledger database and the purely private blockchain: “the defining characteristic of this space is the idea of decentralization. But don't think decentralization versus centralization. Think in terms of a continuum” (Brown, 2014).

The Bank of England (cited by Allison, 2015) is currently reflecting on ways to implement "hybrid systems" involving distributed ledger technology, also bearing in mind the idea of a continuum, and raising the issue of remuneration, incentives, and honest participation, so as to ensure socially efficient outcomes. This initiative might come as a surprise following the critical report (Ali et al., 2014, p. 6) issued a few months earlier expressing the institution's scepticism as regards the claimed ability of crypto-currencies to sustain high levels of decentralization.

> A significant risk to digital currencies' sustained use as payment systems is therefore that they will not be able to compete on cost without degenerating - in the limiting case - to a monopoly miner, thereby defeating their original design goals and exposing them to risk of system-wide fraud (ibid, 2014, p.6).

Finally, another source of pessimism in the long run is the game-theoretic parallel drawn with the Tragedy of Commons (Hardin, 1968; Graydon, 2014).

SOME BLOCKCHAIN APPLICATIONS

In this section, we review some significant applications of blockchain technology (Brokaw, 2014, Hayes, 2015). More broadly still, table 1 proposes two complementary typologies of crypto-economic instruments.

[Table 1 here]

Sidechain Technology and Smart Contracts

A sidechain functions as a separately managed ledger, with its own software code, that is "pegged" to the main blockchain ledger so as to allow transfers of key information from one chain to the other. It goes hand in hand with the idea of smart contracts (Maxwell, 2015), which are specific programs used by a user of the main blockchain, in order to decide whether a specific operation, say a given payment, should be permitted or not. The sidechain ledger indirectly taps the underlying authenticating power of the main blockchain, while simultaneously taking advantage of a more flexible software platform. The sidechain helps gain both agility and freedom of using multiple networks, without having to create new crypto-currencies (i.e altcoins), which would weaken the network effect (ibid.), and impede their mass adoption. Because of the value attached to crypto-currency holdings, there is a natural resistance to embrace untested changes. The sidechain and smart contracts offer a way out of this deadlock. Importantly enough, a widespread adoption of sidechains would nevertheless necessitate slight changes to the Bitcoin protocol (Bradbury, 2014).

A programme called Elements is currently under investigation by Blockstream cryptography experts working on the Alpha sidechain (Maxwell, 2015). We briefly review hereafter two developments of Elements:

Firstly, 'Confidential Transactions' is a new feature of the sidechain that ensures, through the introduction of a confidential address, that the amounts of cryptocurrency transferred are visible on the blockchain only to participants in the transaction (and/or those they designate). This goes beyond the privacy on Bitcoin's blockchain, which relies purely on pseudonymous, albeit public, identities. Financial privacy is in great demand from the cryptocurrency community in transactions for commercial and personal purposes.

Secondly, 'Segregated Witness' ensures that the specification of a transaction's effects on the ledger is separated from the data necessary to prove its validity, thereby eliminating all possibility of transaction malleability, and strengthening the overall security of the blockchain.

Ethereum

Ethereum is an innovative blockchain-based virtual machine and Cloud 2.0 platform, featuring stateful user-created digital contracts. The developers are working on a system allowing the exchange of complex contracts. More sophisticated interaction between users will allow the conclusion of digital contracts according to a distributed ledger model. Ethereum amounts to an extension of the crypto-economy, beyond virtual monetary exchanges, toward the establishment of a nexus of digital contracts pertaining to all areas of life (e.g. wage payment or marriage) with a solid technological and legal basis. According to one of Ethereum's founders:

> We have a blockchain that is featureless in a sense and it has embedded within it a programming language that allows people to create all sorts of things that run on top of the blockchain architecture. The building block for Ethereum is a smart contract; it is like a virtual machine or autonomous programme that is maintained by everyone in the network. Inside the contract you can

> specify what its purpose is. The contracts are the foundations for a new generation of applications on the internet (Alisie cited in Barnes, 2015).

Gridcoin

Drawing on the Bitcoin protocol and an open source middleware system for volunteer and grid computing, the Berkeley Open Infrastructure Network Computing Grid or BOINC (http://boinc.berkeley.edu/), the blockchain finds an unexpected application with GridCoin, a peer-to-peer internet-based cryptocurrency that aims to provide real benefits to humanity by compensating miners for participating in BOINC projects, leading to advances in medicine, biology, climatology, and astrophysics by redirecting the computational power towards BOINC research. The blockchain's most famous application generates unnecessary heat and wasted power for the proof-of-work algorithms. A media release (Long Future Foundation, 2015) presents a modelling tool, the Bitcurrency calculator, showing that Bitcoin could one day consume up to 60% of global electricity production, 13,000 terawatt hours, equal to powering 1.5 billion homes[4].

> Bitcoins are created in air-conditioned warehouses full of energy-hungry computers using a process known as bitcoin 'mining'. Bitcoin mining 'farms' are popping up all over the world right now and devouring vast amounts of electricity. There are even new plans to embed bitcoin mining chips into everyday objects like DVD players and refrigerators (Long Future Foundation, 2015).

The white paper (Halford, 2014) explains the rationale: “Gridcoin is the first cryptocurrency that successfully diverts wasted energy towards useful scientific research, operating as a distributed peer to peer network with no central authority, and provides greater efficiency using normal consumer grade hardware”.

Ripple Labs

As in (Jones & Higgins, 1998) (1998), the real potential for cryptocurrencies may be the streamlining of the transfer of value (World Economic Forum, 2015, p.14). Ripple laps, with its Ripple technology, has become since 2012 a major player in the payments revolution with an ambition to build a global payment protocol (Cawrey, 2014). Surprisingly enough, in our technology-driven globalized world, “it remains unrelentingly difficult to move money around the globe (ibid.). A harmonized protocol is needed to act at the interface between financial institutions worldwide: “as an open protocol, Ripple enables a peer-to-peer server architecture to facilitate the movement of value among financial institutions. This allows financial services companies to make payments directly to each other, whether across different networks, geographic borders or currencies" (Aranda & Zagone, 2015).

> By establishing a universal financial protocol, Ripple stands to break down the walls between financial institutions. Instead of each institution being a silo that works within the confines of its own rules and regulations, the RTXP serves to create a universal set of rules that each institution can abide by (Gehring, 2015).

The elaboration of a single protocol between the building blocks of the financial system is reminiscent of the invention of the Simple Mail Transfer Protocol (SMTP) in the early days of emails (ibid.). Schwartz et al. (2014, p.2) show that the Ripple Protocol achieves consensus at each ledger-close. It consists of a real-time gross settlement system, the Ripple Transaction Protocol (RTXP), securing instant and nearly free payments, currency exchange and remittance, regardless of size. Ripple allows the fast and secure transfer of tokens, whether in fiat, cryptocurrency, commodity or any other unit of value. The Ripple technology echoes our previous discussion of the centralization/decentralization continuum, and the emergence of hybrid solutions. It is a smart blend of permissioned and permissionless architecture (Kelleher, 2015). While everyone is allowed to enter the game, every participant can select the transaction validators, on the basis of trust, of a contract, or a customized evaluation (ibid.). Ripple's algorithm creates a decentralized market inside its protocol; in a sense, it is closer to a ledgerchain than a blockchain, with its decentralized meta-layer of control (ibid.).

Blockchain-based Digital Identity Providers

The problem of online digital identity comprises two interrelated issues, namely access control and personally identifiable information (Daily Fintech, 2015). The centralisation of digital identity-related information is of utmost political, legal, societal (and arguably philosophical) relevance. A pioneer in the field is the Government of India, currently running the world's largest national digital identity scheme, the Unique Identification Authority of India (UIDAI), with each resident being assigned a 12-digit unique number called Aadhaar (The Times of India, 2015).

Blockchain Technology: Principles and Applications

Blockchain technology confers to digital identity a novel and potentially revolutionary decentralization character in the digital age. An innovative company in the booming field of digital authentification is OneName, a “passcard identity company building access control on the blockchain”. OneName provides a trustless and decentralized service so that one’s digital identity cannot be controlled by a central institution or company.

Blockchain-based Voting Systems

In February 2015, the Bitcoin Foundation (2015) unveiled a new project revolving around a blockchain-based voting system, which “provides even greater transparency into the voting process, with every vote being recorded on the blockchain”. Building upon the immutability, transparency and consensus inherent in blockchain technology, voting systems -wherein every vote is recorded under a secure, cryptographic hash- appear as a major technological breakthrough. At the junction between e-democracy and blockchain technology, this type of voting system was first implemented by a Danish political party for internal elections purposes (Millet, 2014).

Blockchain Technology for the Banking/Finance Industry

Our section on Ripple emphasized the potential of Blockchain technology for the harmonisation of payment protocols in the global financial system. Yet, other important applications exist in the banking and finance industry. Although suspicion initially surrounded Bitcoin, reaching its climax with the Mt Gox scandal in 2014, it is now morphing into deep embrace with blockchain technology being touted as the main potential driver of financial services in the twenty-first century (Shubber, 2015). Likewise, for Accenture (2015), a digital revolution is on its way in the banking industry, although the consequences on major players are very uncertain. Banks are likely to be reshaped, following a period of turmoil, to better address the needs of individuals and institutions, by providing them with enhanced services.

On 24 March 2015, Nasdaq, the leading provider of trading, clearing, exchange technology, listing, information and public company services, signed a deal with the New York-based startup Noble Markets. The latter will provide Nasdaq with core trading technology to help them build a new market for cryptocurrencies (Casey, 2015). On 11 May 2015, Nasdaq announced its plans to leverage Blockchain technology, through the Open Assets Protocol, a colored coin innovation. Nasdaq will apply blockchain technology, in order to expand the equity management capabilities of ExactEquity™, its Nasdaq Private Market platform, resulting in enhanced integrity, audit ability, governance and transfer of ownership capabilities (Nasdaq.com, 2015). For Bob Greifeld, the Nasdaq CEO (ibid.), blockchain technology is not only relevant to the management of physical securities, but increasingly to immaterial assets, and should widely benefit global capital markets.

Enhancing the Transparency of Supply / Global Commodity Chains

In a globalized world, every commodity we consume corresponds to “a journey of people, places and materials” (Steiner, 2015). Yet, the underlying supply chains are often opaque to the end consumer. How do we recreate transparency and new relationships with consumer goods, so as to enable active participation (Williams, 2015), to verify product authenticity and ethical standards? Blockchain technology provides a groundbreaking solution. A shared, consensus-based and immutable ledger helps track the origin and the transformations undergone in the supply chain. The blockchain will create a formal registry enabling the identification and the tracking of possession of a good throughout the supply chain. One could also resort to connected objects installed in fishing boats, shipping trucks and storage coolers that will keep track of the environmental conditions, such as temperature or location, ensuring that a product was safely handled, complying with health and safety norms. Finally, because the blockchain ensures anonymity; promotions and discounts could be sent to users, without disclosing their personal information.

Social Inclusion in the Developing World

One of the most exciting and unforeseen applications pertains to social inclusion in the developing world, most notably, of the unbanked population, that is, all the adults in the world who do not hold an account at a bank, another financial institution or a mobile money service provider. "From 2011 to 2014, 700 million people became account holders at banks, other financial institutions, or mobile money service providers, and the number of "unbanked individuals dropped 20 percent to 2 billion adults" (World Bank, 2015a). Thus, the World Bank has set an ambitious goal: universal financial access by 2020 (World Bank, 2015b).

The largest potential for social progress in the developing world is mobile inclusion that will enable millions of underprivileged people to make and receive micropayments through a mobile device. For the CIO of the Commonwealth Bank of Australia, “in this economy and through Africa, with a population of about 1.2 billion in the continent, mobile inclusion is greater than 100 percent. There are more mobile devices than there are people in the population” (Wheteing, cited in Ngo, 2015). IHB, (I Have Bitcoins) is a privately held media and data services company, which relies extensively on blockchain technology, which it considers to be a disruptive force. IHB helps artisans in rural India to benefit from the purchasing power potential in the developed world, and sell their paintings on a global market platform, with no commission (unlike exporters, who mark up prices through opaque distribution channels, before the artwork is made available to the end-consumers in the developed world).

> The Indian handicraft industry is cottage based and mostly decentralized. Spread all over the country, mainly in rural and urban areas, it is a major source of income for rural communities. Employing over six million artisans, including a large number of women and those who belong to weaker sections of the society, the handicraft industry could benefit enormously from bitcoin (Nirgunarthy, 2015).

A partnership with Mozilla enables the distribution of smartphones to rural artisans, who set up small businesses connected to the global marketplace (Rabe, 2015).

Central and Eastern Europe (hereafter CEE) is one of the biggest remittance growth areas in the world. In the Republic of Moldova, a post-soviet republic with a large

Diaspora population, annual remittances account for a staggering 45.57% of per capita GDP (Stanley, 2015). Without a bank account allowing for international wire transfers, most people use companies like Western Union, to send money home. World Bank data showed that in 2013, over 700,000 Moldovans were working abroad whether permanently or temporarily. About 89% of the remittances were made by international transfer systems, and 11% by bank transfer.With persistently high remittance fees, new cost-effective ways of transferring money are expected to emerge: “one in seven sends money home [in CEE] using mobile phones” (ibid.).

CONCLUSION

We have exposed the core concepts at the heart of blockchain technology as well as some of the most significant features of public decentralized ledger platforms. After showing why the blockchain is a foundational and disruptive technology, with the potential to revolutionize the nature of the interface between economic agents, we have presented a non-exhaustive list of existing applications of blockchain technology. These applications range from Blockstream sidechains and Ethereum to digital identity providers and blockchain-based voting systems, as well as Ripple. And we have highlighted the societal relevance of these wide-ranging technological evolutions, which could effectively contribute to social inclusion in the developing world.

Blockchain enthusiasts, surfing on a wave of euphoria set in motion by scores of innovative start-ups (Shubarth, 2015) currently seem to outnumber the sceptics.

However, the present intellectual landscape still covers a wide spectrum of opinions, ranging from utter fervour (Masters, 2015) to ingrained pessimism (Kaminska, 2014).

The fundamental blockchain question is ultimately that of trust. Yet, as Seabright (cited by Harford 2010), “[f]actors which increase trust in society are not necessarily a good thing, because they can increase the bonds between gang members, whose main economic success comes from extorting or coercing other people”. This opinion is corroborated by Kaminska (2014), who thinks that blockchain technology has been mired in paradox from the onset. Without an inbuilt payoff mechanism, the cost of participation is dissuasive, and leaves aside all agents who do not have a direct interest in the projected consensus. Contrariwise, a payoff mechanism favours the most cost-efficient players and concentration of power; token-free blockchains are no exceptions. Finally, incentives to corrupt the system increase with the value of assets contingent on the eventual outcome of the consensus.

In spite of these important reservations, we believe that more blockchain applications will emerge in the near future in areas as diverse as art, tourism and sports. While still in their infancy, one should not underestimate the promising socio-economic benefits of these extraordinary technological changes.

REFERENCES

Accenture (2015). The Future of Fintech and Banking: Digitally disrupted or reimagined?, Fintech innovation lab London. Retrieved from http://www.fintechinnovationlablondon.net/media/730274/Accenture-The-Future-of-Fintech-and-Banking-digitallydisrupted-or-reima-.pdf

Ali, R., Barrdear J., Clews, R. & Southgate, J. (2014). The economics of digital currencies. *Bank of England. Quarterly Bulletin*, Q3. Retrieved from http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin2.pdf

Allaire, J. (2015). Bitcoin and the Future of Payments Technology. Panel Discussion, Museum of American Finance. Lecture/Symposia Series. February 11. Retrieved from https://www.youtube.com/watch?v=a-ZTSao8HPk&feature=youtu.be&t=661

Allison, I. (2015). Bank of England: Central banks looking at 'hybrid systems' using Bitcoin's blockchain technology. *International Business Time*. July 16. Retrieved from http://www.ibtimes.co.uk/bank-england-central-banks-looking-hybrid-systems-using-bitcoins-blockchain-technology-1511195

Aranda, D., & Zagone, R. (2015). The ‘Ripple’ Effect: Why an Open Payments Infrastructure Matters. *Consultative Group to Assist the Poor*, 01 May. Retrieved from http://www.cgap.org/blog/%E2%80%98ripple%E2%80%99-effect-why-open-payments-infrastructure-matters

Aura, T. (2005). Cryptographically Generated Addresses (CGA). Microsoft Research. March. Retrieved from https://tools.ietf.org/html/rfc3972

Babbitt, D.& Dietz, J. (2014). Crypto-economic Design: A Proposed Agent-Based Modelling Effort. Swarm Fest 2014: 18th Annual Meeting on Agent-Based Modelling & Simulation. University of Notre Dame . USA. June 29 – July 1. Retrieved from http://www3.nd.edu/~swarm06/SwarmFest2014/Babbitt.pdf

Back, A, Corallo, M., Dashjr, L., Friedenback, M., Maxwell, G., Miller, A., Poelstra, A., Timon, J., &.Wuille, P. (2014). Enabling Blockchain Innovations with Pegged Sidechains. Retrieved from http://www.blockstream.com/sidechains.pdf

Barnes, D. (2015). Blockchain manoeuvres: applying Bitcoin's technology to banking. *The Banker*, 14 May

Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms* Markets and Freedom, New Haven, CT: Yale University Press.

Bitcoin Foundation (2015). *Voting on the Blockchain - Version 1.0*. 25 February. Retrieved from https://blog.bitcoinfoundation.org/voting-on-the-blockchain-version-1-0/

Böhme, R., Christin, N., Edelman, B, & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, 29(2): 213-38, DOI: 10.1257/jep.29.2.213

Bradbury, D. (2015). Bitcoin Core Developers Weigh in on Side Chain Proposal. *CoinDesk*. 10 April. Retrieved from http://www.coindesk.com/bitcoin-core-developers-bitcoin-side-chains/

Brokaw, A. (2014). Crypto 2.0 Roundup: Bitcoin's Revolution Moves Beyond Currency. *CoinDesk*, 23 August. Retrieved from http://www.coindesk.com/crypto-2-0-roundup-bitcoins-revolution-moves-beyond-currency/

Brown, R.G. (2014). The unbundling of trust, how to identify good cryptocurrency opportunities? personal blog. Thoughts on the Future of Finance. 14 November, Retrieved from http://gendal.me/2014/11/14/the-unbundling-of-trust-how-to-identify-good-cryptocurrency-opportunities/

Buterin, V. (2013). Bitcoin Network Shaken by Blockchain Fork. *Bitcoin Magazine*, 13 March. Retrieved from https://bitcoinmagazine.com/3668/bitcoin-network-shaken-by-blockchain-fork/

Buterin, V. (2014a). Comment posted on Schneider (2014). Code your own utopia: Meet Ethereum, bitcoin's most ambitious successor. *Aljazeera America*. April 7. Retrieved from https://www.reddit.com/r/ethereum/comments/22av9m/code_your_own_utopia/

Buterin, V. (2014). *On Stake*. Ethereum Blog, 5 July. Retrieved from https://blog.ethereum.org/2014/07/05/stake/

Buterin, V. (2015a). *Visions, Part 1: The Value of Blockchain Technology*. Ethereum Blog. 23 April. Retrieved from https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/

Buterin, V. (2015b). On Public and Private Blockchains, Ethereum Blog, 7 August. Retrieved from https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Byrne, P. (2015). Blockchain without Bitcoin is now a thing. personal blog. April 8. Retrieved from http://prestonbyrne.com/2015/04/08/blockchain-without-bitcoin-is-now-a-thing/

Casey, M. (2015). Nasdaq to Provide Trading Technology for Bitcoin Market place. *The Wall Street Journal*, 23 March. Retrieved from http://www.wsj.com/articles/nasdaq-to-provide-trading-technology-for-bitcoin-marketplace-1427140006

Cawrey, D. (2014). Ripple Labs' Grand Plan to Build a Global Payment Protocol. CoinDesk. April 11. Retrieved from http://www.coindesk.com/ripple-labs-grand-plan-build-global-payment-protocol/

Chaum, D. (1983). Blind signatures for untraceable payments. In Chaum, D., Rivest, R.L, & Sherman, A.T. (eds), *Advances in Cryptology*. (pp.199-203). New York: Springer,

Committee on Payment and Settlement Systems (2003). Payment and Settlement Systems in Selected Countries. Basle: Bank for International Settlements.

Coletti, P. (2015). Bitcoin's baby: Blockchain's 'tamper-proof' revolution. *BBC News.* 20 May. Retrieved from http://www.bbc.com/news/technology-32781244

Cotillard, M. (2015). Bitcoin's Block Size Debate Tests Its Community Governance. *Brave New Coin*. 18 August. Retrieved from http://bravenewcoin.com/news/bitcoins-block-size-debate-tests-its-community-governance/

Crosman, P. (2015). Why Banks Are Testing Bitcoin's Blockchain (Without Bitcoin). *American Banker*. 1 June. Retrieved from http://www.americanbanker.com/news/bank-technology/why-banks-are-testing-bitcoins-blockchain-without-bitcoin-1074622-1.html

Daily Fintech (2015). Blockchain based Digital Identity will disrupt commerce and government. 22 May. Retrieved from http://dailyfintech.com/2015/05/22/blockchain-based-digital-identity-will-disrupt-commerce-and-government/

Derose, C. (2015a). Get Ready for the Rise of the Blockchain. *American Banker*. April 20. Retrieved from http://www.americanbanker.com/bankthink/get-ready-for-the-rise-of-the-blockchain-1073843-1.html

Derose, C. (2015b). Blockchain for Beginners -Behind the Ingenious Security Feature that Powers the Blockchain. *American Banker*. 21 May. Retrieved from http://www.americanbanker.com/bankthink/behind-the-ingenious-security-feature-that-powers-the-blockchain-1074442-1.htm

Dwyer, G. (2014). The Economics of Bitcoin and Similar Private Digital Currencies. July 8. dx.doi.org/10.2139/ssrn.2434628

Evans, D. (2014). Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms. April 15. Coase-Sandor Institute for Law & Economics. Research Paper No. 685.   http://dx.doi.org/10.2139/ssrn.2424516

Friedman, M. (1992). *Money mischief: episodes in monetary history*. New York: Harcourt Brace Jovanovich

Gehring, B. (2015). What is the Ripple Protocol? 19 February. Retrieved from https://ripple.com/knowledge_center/what-is-a-protocol-how-does-ripple-fit-in-2/

Graydon, C. (2014). Bitcoin's future: proof-of-stake vs proof-of-work. *Cryptocoinnews*. 30 August. Retrieved from https://www.cryptocoinsnews.com/bitcoins-future-proof-of-stake-vs-proof-of-work/

Greenspan, G. (2015). Ending the bitcoin vs blockchain debate - Is there any value in a blockchain without a cryptocurrency? MultiChain blog. July. Retrieved from http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/

Guerrini, F. (2015). How Artificial Intelligence Could Eliminate (Or Reduce) The Need For Managers. *Forbes / Tech*. August 3. Retrieved from http://www.forbes.com/sites/federicoguerrini/2015/08/03/managers-beware-from-smart-contracts-to-the-autonomous-ceo-ai-is-coming-for-your-job-as-well/

Halford, R. (2014). Gridcoin - Crypto-Currency using Berkeley Open Infrastructure Network Computing Grid as a Proof Of Work. White Paper. May 23rd. Retrieved from http://www.gridcoin.us/images/gridcoin-white-paper.pdf

Hardin, G (1968). The Tragedy of the Commons. *Science* 162 (3859): 1243–1248.

Harford, T. (2014). The Economics of Trust. *Forbes*. 21 July. Retrieved from http://www.forbes.com/2006/09/22/trust-economy-markets-tech_cx_th_06trust_0925harford.html

Hayes, A. (2015). How Will Bitcoin 2.0 Change The World? *Investopedia*. 13 April. Retrieved from http://www.investopedia.com/articles/investing/041315/how-will-bitcoin-20-change-world.asp

Innes, A. (1913). What is money? *The Banking Law Journal*, May, 378-408

Jones, T.L., & Higgins, G.R. (1998). Patent Number 5 778 067, July 7. Retrieved from https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US5778067.pdf

Kaminska, I. (2015). A new raison d'être for cryptocurrency, but an age-old problem. *FT Alphaville. The Blog, News and Commentary*. 20 October. Retrieved from http://ftalphaville.ft.com/2014/10/20/2012052/a-new-raison-detre-for-cryptocurrency-but-an-age-old-problem/?

Kelleher, T.S. (2015). Ripple's Overlooked Path to Decentralization. *American Banker*. July 23. Retrieved from http://www.americanbanker.com/bankthink/ripples-overlooked-path-to-decentralization-1075603-1.html?pg=2

Keynes, J.M (1971 [1930]). *A Treatise on Money*. London: Macmillan

Khan, F. (2012). Do Visa and MasterCard own their private network for processing payments? If so, is it very bad idea not to use the Internet instead? forum answer. updated 13 December. https://www.quora.com/Do-Visa-and-MasterCard-own-their-private-network-for-processing-payments-If-so-is-it-very-bad-idea-not-to-use-the-Internet-instead

Kwon, J. (2014).Tendermint: Consensus without Mining. White paper. Retrieved from http://tendermint.com/docs/tendermint.pdf

LearnCryptography.com (2014), 51% Attack. Retrieved from http://learncryptography.com/51-attack/

Long Future Foundation (2015). Loud wake up call over new internet money's power demand. Media Release. Brisbane. Australia. May 27. Retrieved from http://longfuture.org/wp-content/uploads/2015/05/bitcurrent-release.pdf

Masters, B. (2015). Blockchain: The Financial Challenge of our Time. Presentation made on June 2 at the Exponential Finance conference. New York City. Retrieved from https://www.youtube.com/watch?v=O1Yo8bt8JAU

Maxwell, G. (2015). Bringing New Elements to Bitcoin with Sidechains. SF Bitcoin Devs Meetup. Conference Paper. June 8. Retrieved from https://people.xiph.org/~greg/blockstream.gmaxwell.elements.talk.060815.pdf

Millet, J. (2014). Danish Political Party May Be First to Use Block Chain For Internal Voting. *NewsBTC*. 22 April. Retrieved from http://www.newsbtc.com/2014/04/22/danish-political-party-may-first-use-block-chain-internal-voting/

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

Nasdaq.com (2015). Nasdaq Launches Enterprise-Wide Blockchain Technology Initiative. *GlobeNewsWire*. 11 May. Retrieved from http://www.nasdaq.com/press-release/nasdaq-launches-enterprisewide-blockchain-technology-initiative-20150511-00485#ixzz3fkl5TZUa

Ngo. D. (2015). Commonwealth Bank of Australia to Integrate Ripple for Instant Settlements. Cointelegraph. 29 May. Retrieved from http://cointelegraph.com/news/114419/commonwealth-bank-of-australia-to-integrate-ripple-for-instant-settlements

Niccolai, J. (2015). This well-funded startup could turn Bitcoin mining - and the chip industry - on its head. *PCWorld*. May 18. Retrieved from http://www.pcworld.com/article/2923812/this-wellfunded-startup-could-turn-bitcoin-mining-and-the-chip-industry-on-its-head.html

Nirgunarthy, A. (2015). Bitcoin art from India**.** IHB. January 6th. Retrieved from https://ihb.io/2015-01-06/news/bitcoin-art-india-help-artisans-go-global-14956

Open Source Initiative (2015). http://opensource.org/about

Palley, S. (2014). Contracts, Computers and Cucumbers. Linkedin Pulse. 1 May. Retrieved from https://www.linkedin.com/pulse/20140501211427-112013610-byzantium-etherium-contracts-cucumbers

Pilkington, M. (2016). Bitcoin through the Lenses of Complexity Theory: Some Non-Orthodox Implications for Economic Theorizing. *Handbook of the Geographies of Money and Finance*. Martin, R.; Pollard.J. (eds). Edward Elgar: Cheltenham, forthcoming

Prisco, G. (2014) Mine For Citizen Science. *Cryptocoinsnews*. 24 November. Retrieved from https://www.cryptocoinsnews.com/mine-citizen-science/

Rabe, A. (2015). 3 ways Bitcoin can change development. *Alternatives in Development*. ICT. Technology. 4 March. Retrieved from http://www.whydev.org/3-ways-bitcoin-can-change-development/

Rossi, S. (2004). Central bank money and payment finality. *Quaderni di ricerca*. Lugano: Laboratoire de recherche en économie monétaire du Centre d'études bancaires, n° 11, February. Retrieved from http://www.csbancari.ch/pubblicazioni/RMElab/q11.pdf

Sams, R. (2014). Some Crypto Quibbles with Threadneedle Street. September 16. Retrieved from http://cryptonomics.org/2014/09/16/some-crypto-quibbles-with-threadneedle-street/

Saper, N. (2013). International Cryptography Regulation and the Global Information Economy. *Northwestern Journal of Technology and Intellectual Property*. Fall. 11(7), 673-88. Retrieved from http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss7/5/

Schmidt, E., & Cohen, J. (2013). *The new digital age: reshaping the future of people, nations and business*. John Murray: London, UK

Schmitt, B. (1984). *Inflation, chômage et malformations du* capital. Economica. Castella: Albeuve, Switzerland.

Schneider, N. (2014). Code your own utopia: Meet Ethereum, bitcoin's most ambitious successor. *Aljazeera America*. April 7. Retrieved from http://america.aljazeera.com/articles/2014/4/7/code-your-own-utopiameetethereumbitcoinasmostambitioussuccessor.html

Scubarth, C. (2015). Bitcoin startup funding soars as value dives: Here are the top deals so far this year. *Silicon Valley Business Journal. Techflash.* blogpost.7 August. Retrieved from http://www.bizjournals.com/sanjose/blog/techflash/2015/08/bitcoin-startup-funding-soars-as-value-dives-here.html

Schwartz, D., Youngs, N.,& Britto, A. (2014). The Ripple Protocol Consensus Algorithm. White Paper. Ripple Labs Inc. Retrieved from https://ripple.com/files/ripple_consensus_whitepaper.pdf

Shubber, K. (2015). Banks put aside suspicion and explore shared database that drives bitcoin. *Financial Times*. 14 October. Retrieved from http://www.ft.com/intl/cms/s/0/51c07a78-61cb-11e5-9846-de406ccb37f2.html

Srinivisan, B.S. (2015). A bitcoin miner in every device and in every hand. blog post, May 18. Retrieved from https://medium.com/@21dotco/a-bitcoin-miner-in-every-device-and-in-every-hand-e315b40f2821

Stanley, A. (2015). Money movers wake up to working migrants. *Financial Times*. June 29. Retrieved from http://www.ft.com/cms/s/3/71227fda-18ea-11e5-8201-cbdb03d71480.html#axzz3fqfFjlIL

Steiner, J. (2015). Blockchain Can Bring Transparency to Supply Chains. *The Business of Fashion*. 11 May. Retrieved from http://www.businessoffashion.com/articles/opinion/op-ed-blockchain-can-bring-transparency-to-supply-chains

Swanson, T. (2015). Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. Working paper. 6 April. Retrieved from http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf

The Times of India (2015). Aadhaar world's largest biometric ID system. 27 April, http://timesofindia.indiatimes.com/india/Aadhaar-worlds-largest-biometric-ID-system/articleshow/47063516.cms

Waldman, S.R. (2015). Soylent Blockchains. www.interfluidity.com. February. Retrieved from http://www.interfluidity.com/uploads/2015/02/soylent-blockchains-to-share.pdf

Waters, R. (2014). Bitcoin 2.0 gives the dreamers focus - but only without the hype. *Financial Times*. 4 December. Retrieved from http://www.ft.com/intl/cms/s/0/f53524de-7bca-11e4-b6ab-00144feabdc0.html#axzz3oSjgBwUx

Williams, R. (2015). How Bitcoin's Technology Could Make Supply Chains More Transparent. *CoinDesk*. 31 May. Retrieved from http://www.coindesk.com/how-bitcoins-technology-could-make-supply-chains-more-transparent/

Wright, A. & De Filippi, P., (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. March 10. Retrieved from http://ssrn.com/abstract=2580664

World Bank (2015a). Massive Drop in Number of Unbanked, says New Report. PressRelease. 15 April. Retrieved from http://www.worldbank.org/en/news/press-release/2015/04/15/massive-drop-in-number-of-unbanked-says-new-report

World Bank (2015b). Achieving Universal Financial Access by 2020 (Overview). 22 April. Retrieved from http://www.worldbank.org/en/topic/financialinclusion/brief/achieving-universal-financial-access-by-2020.print

World Economic Forum (2015). The Future of Financial Services - How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed. An Industry Project of the Financial Services Community. June. Retrieved from http://www3.weforum.org/docs/WEF_The_future__of_financial_services.pdf

Zamfir, V. (2015). *What is Cryptoeconomics*?. CryptoEconomicon 2015. Crypto Technology Conference. Mountain View, CA, USA. January 26-29. Retrieved from https://www.youtube.com/watch?v=9lw3s7iGUXQ

NOTES

[1] Chaum is credited with the first conceptualization framework for digital currencies; some of his ideas have been endorsed in the Cypherpunk's Manifesto.

[2] A 256-bit number or 2^{256} is an extremely large number, about 10^{168}.

[3] An integer overflow bug is generally caused by an arithmetic operation that attempts to create a numerical value which is too large to be represented within the available storage space.

[4] Longfuture Foundation spokesman, Guy Lane, previously released his Bitcarbon method in December 2013, based on the assumption that the amount of money a Bitcoin miner will spend on electricity is 90 percent of the value of the Bitcoin that they mine.