CAMBRIDGE

Cambridge University Press
978-1-108-83487-2 — Searching for Trust
Victoria L. Lemieux
Excerpt
More Information

PART I

Introduction

CAMBRIDGE

Cambridge University Press
978-1-108-83487-2 — Searching for Trust
Victoria L. Lemieux
Excerpt
More Information

1
What Good Is Blockchain?

The phone rang in my office. It was late summer 2017. I answered and was greeted on the other end of the line by the voice of one my colleagues in the Computer Science Department asking, “Is blockchain really a *thing*?” I have been asked this question any number of times since then, though each time it takes a slightly different form. James Mickens, a Harvard computer scientist, produced a video in 2018 entitled *Blockchains Are a Bad Idea* that is a variation on the same theme. In the video, Mickens points out that many of the features of blockchains can be provided by existing technologies. To many, blockchain technology seemingly offers nothing new, since, by and large, it presents an assemblage of preexisting theories, algorithms, and mathematics, as I will discuss in Section 1.3, and a computationally inefficient one at that (see, e.g., Truby, 2018; Li et al., 2019)![1]

Observed from a purely computational or technical (in the sense of information and communications technology) perspective, it is not easy to see what all the fuss is about when it comes to blockchains, nor why there should be such interest in them. As Mickens argues in his video, blockchain systems, such as Bitcoin, have features and capabilities that can be provided by existing systems: tamper resistance can be provided by digital signatures (discussed in

[1] Bitcoin mining consumes an enormous amount of electricity. According to the Bitcoin Energy Consumption Index (see, e.g., Digiconomist, 2021), a single Bitcoin transaction consumes the equivalent of the carbon footprint of 664,375 Visa transactions (299.76 $kgCO_2$) and the same amount of power as the average United States household usage over 21.63 days (631.08 kWh). De Vries (2018, p. 801) states that “The Bitcoin network can be estimated to consume at least 2.55 gigawatts of electricity currently, and potentially 7.67 gigawatts in the future,” making it comparable with countries such as Ireland (3.1 gigawatts) and Austria (8.2 gigawatts) in energy consumption based on 2018 data. On this point, see also Das and Dutta (2020). Owing to the amount of energy needed to mine Bitcoin and cool the mining equipment, miners tend to gravitate their operations to places where they can obtain electricity relatively cheaply and where it is easier to keep their equipment cool (Bjarnason, 2019; Baydakova, 2021). Unscrupulous miners have also been known to steal the electricity they need (Nadeau, 2020).

Cambridge University Press
978-1-108-83487-2 — Searching for Trust
Victoria L. Lemieux
Excerpt
More Information

Section 1.3) with or without blockchain, as can the ability to prove a claim or to achieve non-repudiability of a transaction (ISO, 2018a, s. 3.48); message ordering can be achieved through the use of hash pointing (discussed in Section 1.3) without resorting to blockchain; and highly available storage needs can be handled by commercial cloud storage (Mickens, 2018). Yet, as an archival scientist – someone who studies the theory of recordkeeping and the long-term preservation of authentic records – blockchain makes sense to me. Even if I doubt some of the claims I hear about it, I see it as a response to a perceived erosion of society's "fact infrastructure" in an age of disinformation and disorders of social trust. It is this perspective on blockchain technology that I will explore in this volume.

1.1 Blockchain Is Meaningless

My colleague's question about blockchain came, not unreasonably, at the peak of what has been described as the blockchain "initial coin offering hype cycle," which was ramping up to its late 2017, early 2018 crescendo. At the time, many were touting blockchain (and their own initial coin offerings, the cryptocurrency community's equivalent to initial public offerings) as a solution to all the world's problems. To illustrate the zeitgeist of the time, technology writer Alex Hern (2016) wrote a (tongue-in-cheek) piece for *The Guardian* in 2016 entitled, "Blockchain: The Answer to Life, the Universe and Everything?" that appropriately began with the sentence, "Have you heard the good news? The blockchain is here – and it's going to save everything."

Don and Alex Tapscott's 2016 book, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*, set out a vision of how blockchain could be used to transform and change the world for the better by tracking the provenance of digital and real-world assets, banking the unbanked, and unleashing new businesses. Given the lack of real-world evidence at the time, many were (and remain) skeptical, as outlined in, for example, David Gerard's critical 2015 book *Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum & Smart Contracts.* At the same time, few really understood what the term blockchain meant. Adrianne Jeffries (2018), writing for *The Verge* in early 2018, described a blockchain Tower of Babel in which everyone was speaking their own incomprehensible blockchain language, concluding that "'Blockchain' is meaningless."

How is it that blockchains are meaningless to some, while others see their potential to transform the world? The old parable of the blind men and the elephant suggests an explanation. In this story, a group of men come across a creature they have never seen before: an elephant. Each man grabs hold of a different part of the elephant and describes it based on their own limited perception and experience. None of the men has the knowledge needed to understand the parts holistically to determine that what they are encountering is an elephant. Our attempts to make sense of blockchains are analogous when we try to provide an explanation of them without taking a holistic view.

It is for this reason that I argue we need to approach understanding blockchains not from a singular disciplinary perspective but holistically. In this volume, I will draw upon Lemieux and Feng's (2021) multidisciplinary "three-layer" model, which conceives of blockchains and distributed ledgers as *socio-informational-technical systems*. The model was "born of the need to develop an appropriate framework for the problem-centered design of blockchains, in which the problems are themselves 'wicked,' multidimensional, and multidisciplinary" (Palmer et al., 2021, pp. 591–592). It is well known that "systems designed from a single point of view have often proved to have 'blind' spots which can render them ineffective, or even dangerous. With this in mind, we aimed to design a framework which encourages holistic problem analysis and affords a common language, underpinned by a reasonably shared ontology and epistemic worldview" (Palmer et al., 2021, p. 592).

The original model was simplistic, recognizing that blockchains had social, informational (or more accurately, as I will discuss in Chapter 6, evidential), and technical dimensions. In 2019, a diverse group of blockchain scholars came together to discuss the original three-layer model, especially the interactions among the three layers. With further theoretical refinements arising from these discussions, the most recent version of the model represents blockchains as complex, dynamic systems with four interrelated sub-systems – the original three layers (the social, the informational, and the technical) and a governance sub-system – which work together to achieve trust among social actors (Lemieux and Feng, 2021).

The technical sub-system is reasonably well understood, even as there remain novel technical challenges to be overcome, being those technical components that implement blockchain and distributed ledger systems. The social sub-system – which encompasses social, political, and economic implications of these tools and platforms – though arguably less well understood, has at least been recognized as an important aspect of blockchain systems. Indeed, common use of the term blockchain "ecosystem," rather than "system," draws attention to the fact that blockchains comprise communities that are often "contentious and non-homogeneous, in which unpredictable agents can disrupt the planned flow of ecosystem participation" and in which, therefore, governance is needed (Palmer et al., 2021, p. 591). The final sub-system, the informational, focuses on the ledger itself. Paradoxically, given that a defining feature of blockchain technology is the production of an "immutable" distributed ledger that features heavily in "archival imaginaries" (Woodall and Ringel, 2020) that posit blockchain and distributed ledger technology as a cure-all for our current epistemic ailments, it is this aspect of the technology that has received the least scholarly and research attention.

Scholars who have addressed the question of the immutability of blockchain and distributed ledgers have noted that "'immutability' of blockchain records is a matter of debate, as high-profile events in the blockchain space have shown that blockchain records are changeable at will by the people who govern the blockchain system, and it currently is unclear which variations of blockchain technology actually create a record that even approaches immutability" (Walch, 2017b, p. 1). This observation highlights an important insight that is only possible from a holistic vantage point on blockchain and distributed ledger technologies – one that takes into consideration the social, informational (or evidential), and technical dimensions of the technology in equal measure. From this vantage point, blockchain immutability is best viewed not as a property of blockchain-based ledgers but as a sustained commitment that a group of individuals holds onto because they believe that the attribute is desirable, even necessary. In the remainder of this chapter, I will explore this idea more deeply.

1.2 The Social Construction of Meaning

Recognizing that it would be difficult to advance scientific discussions about blockchain technology without a stable definition of the term, in 2017, global blockchain experts became involved in an international project to develop a standard blockchain and distributed ledger vocabulary under the auspices of the International Organization for Standardization (ISO) Technical Committee on Blockchain and Distributed Ledger Technologies (TC307). This work, which involved the input of over 300 international experts from 50 countries over the span of almost three years, resulted in what has become the first ISO standard on blockchain and distributed ledger technologies, ISO 22739:2020 *Blockchain and Distributed Ledger Technologies – Vocabulary* (ISO, 2020a; Oclarino, 2020). The working group that developed the vocabulary converged on a set of interlocking definitions that capture a shared understanding of what a blockchain is and, equally importantly, what it is not.

After many months of deliberation, the ISO experts arrived at a definition of blockchain as a "distributed ledger with confirmed blocks organized in an append-only sequential chain using cryptographic links" (ISO, 2020a, s. 3.6), with a distributed ledger being defined as a "ledger that is shared across a set of [distributed ledger technology (DLT)] nodes and synchronized between the DLT nodes using a consensus mechanism" (ISO, 2020a, s. 3.22). Thus, in this volume, when I use the term distributed ledger, it encompasses the concept of a blockchain because blockchains are a type of distributed ledger. The ISO defined a ledger as an "information store that keeps records that are intended to be final, definitive and immutable" (ISO, 2020a, s. 3.43).

The idea that blockchains are a type of distributed ledger was not an uncontroversial position among ISO experts, since some held the view that the unique features of the blockchain's chained block data structure and consensus mechanism made blockchains categorically different from distributed ledgers. Despite the consensus reached by the ISO community about the meaning of blockchain, it remains true, as I have previously observed, that "different epistemic communities have formed their own ideas about what blockchain is, some with very strong political and social views around open source, sharing, and autonomy" (as quoted in Jeffries, 2018). It also remains true that legal definitions of blockchain technology continue to proliferate (see, e.g., Walch, 2017a, 2017b). As a result, it is doubtful that everyone will accept and adopt the ISO definitions. Nevertheless, these definitions can at least provide a stable foundation for discussion of blockchain and distributed ledgers for the purposes of this volume, even if they do not end the debate about the meaning of blockchain and related concepts.

It is significant that the ISO experts did not define blockchains strictly in terms of technical components, such as the networked databases that communicate and interact with one another over a network in order to implement a blockchain. ISO 22739 instead refers to these technical components as instantiating blockchain or distributed ledger technology *systems* (ISO, 2020a, s. 3.33). To attempt to understand blockchain purely in terms of the computational technologies, experts understood, is to miss the mark by focusing on the wrong abstraction layer, to use a concept from computing. In software engineering and computing, abstraction involves thinking about and representing a thing, for example, a system, at different levels of granularity or detail. Abstractions, like models, are representations that help simplify a complex world and focus the mind on important details (Butterfield et al., 2016).

In contrast to focusing on the technical system view in its definition of the term blockchain, ISO TC307 chose to focus on a *higher* level of abstraction. In ISO 22739, by recognizing blockchains as a distributed type of ledger, ISO experts connected blockchain with a long tradition of *recordkeeping*. This, in turn, connects blockchains to the theories, principles, and methods of *archival science*[2], which is the science underpinning recordkeeping. Archival science, as Thomassen (2015, p. 84) explains,

> is an academic and applied discipline that involves the scientific study of process bound information, both as product and as agent of human thoughts, emotions, and activities, in its various contexts. Its field of study encompasses personal documents, records, and archives of communities, government agencies, and other formal organizations, and archival materials in general, whether kept by archival institutions, units, or programs. It covers both the records themselves and their contexts of creation, management, and use, and their sociocultural context. Its central questions are why, how, and under what circumstances human beings create, keep, change, preserve, or destroy records, and what meanings they may individually or jointly attribute to records and to their recordkeeping and archival operations.

Thomassen (2015, p. 85) goes on to explain that archival science focuses on more than just records or archival documents to think about records or archival documents *in context*, that is, "the context of the data within a record and the contexts of creation, management, and use, as well as the socio-political, cultural, and economic contexts underlying these contexts." Although it has existed for centuries as a practical field, archival science as an academic discipline is considered relatively new, even if it has disciplinary forerunners that extend back centuries (Duranti, 1989; Thomassen, 2015). The more practical orientation of most archivists and the relative newness of contemporary archival science might account in large part for the comparative absence of archivists and archival science from discourse on blockchains.

Why should it be so important to recognize blockchains as recordkeeping systems and connect them to archival concepts? For one thing, defining blockchains in this way makes it possible to treat them as a single category. No matter how many different types of blockchains and distributed ledgers there are now in the world, or there might be in the future, they all will have one thing in common – a ledger.

Another reason is that recordkeeping and archival theories, principles, methods, practices, and professionals have been long associated with the preservation of "information created or received and maintained as evidence and as an asset by an organization in pursuit of legal obligations or in the course

[2] The "archive" and archives and recordkeeping research has received a great deal of attention within the academy in the past two decades. This research encompasses a diverse range of disciplinary perspectives on the "archive" and the study of archives and archivists. Such studies can be distinguished from archival science, which has its own discipline and its own unique body of theory and practices. At the same time, the cognate field of archival studies encompasses a "multiverse" of perspectives, including those from archival science and archival studies (on this point, see Duranti and Michetti, 2016; Gilliland et al., 2016).

of conducting business," that is, with records (ISO, 2020b, s.3.2.10). Evidence is here not limited to the legal sense of the term but rather is "information that could be used either by itself or in conjunction with other information, to establish *proof about an event or action* [emphasis added]" (ISO, 2020b, s. 3.2.6). In order to offer proof of an event or action, evidence must be shown to be inviolate and complete (ISO, 2020b, s. 3.26). Thus records, in order to offer evidence, must, among other things, possess the characteristics of authenticity (actually be what they purport to be),[3] reliability (complete, accurate, and able to stand for the events or actions they represent),[4] and integrity (complete and unaltered) (ISO, 2016, s. 5.2.2). It follows, then, that if we want to design blockchain and distributed ledger systems capable of creating, capturing, and preserving sources of evidence, then recordkeeping and archival theories, principles, methods, practices, and professionals offer knowledge and experience that can provide valuable guidance.

It is the promise – if not yet the reality – of being capable of producing inviolate and complete evidence – or, as expressed in the definition of a ledger in the international standard on blockchain and distributed ledger vocabulary, of being designed to produce final, definitive, and immutable records (ISO, 2020a, s. 3.43) – that sets blockchains (and other distributed ledgers) apart from other types of information systems, such as the commonly used transaction processing systems, management information systems, or office automation systems.

Indeed, in a datafied world, the capability of producing and preserving immutable evidence, as blockchains are designed to do, is a rare one. As paper records and recordkeeping have gradually fallen away to be replaced by digital records and recordkeeping, greater value has been placed on ensuring that the information created by an organization in the conduct of its business can be reassembled into new information assets that might be mined to advance organizational strategy, more often than not profit-driven, or sold to other organizations for similar purposes. As the now well-worn expression goes, "data is the new oil."[5] New business models have arisen based upon exploiting

[3] ISO 30300: 2020, s. 3.2.2, which reads in full "quality of a record (3.2.10) that can be proven to be what it purports to be, to have been created or sent by the agent (3.1.3) purported to have created or sent it, and to have been created or sent when purported" (ISO, 2020a).

[4] ISO 15489:2016, s. 5.2.2 describes reliable records as ones "whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest" and "which can be depended upon in the course of subsequent transactions or activities." The standard goes on to note that reliable records are usually created "at the time of the event to which they relate, or by systems routinely used to conduct the transactions" (ISO, 2016). In other texts, this notion is similarly captured in the phrase "made in the usual and ordinary course of business."

[5] Clive Humby is attributed with coining the phrase "data is the new oil," but the phrase came into popular usage following a 2017 article in the *Economist* (Economist, 2017).

information as assets. To enable these new business models, what once would have been created as records in fixed form is now created and kept in a malleable and manipulable form. Datafication and the creation and storage of vast troves of information have given rise to the so-called era of Big Data and an entirely new field of endeavor – data science, the art of data manipulation and exploitation. While the ability to manipulate records by transforming them into novel forms of data has led to great innovation and scientific advances, it has also undermined the basis of societal proof about past events and actions and, in so doing, contributed to the emergence of an age of disinformation (a topic that will be discussed more fully in Chapter 4). Blockchain, a unique type of ledger, promises to restore society's evidence base. To understand how and, more importantly, why, it is helpful to reflect upon the genesis of blockchain technology.

1.3 Genesis of Blockchain

The blockchain origin story, like all good origin stories, remains somewhat shrouded in mystery. In October 2008, Satoshi Nakamoto – a pseudonym for a person or persons unknown to the present day[6] – proposed a combined digital asset, bitcoin (I will use "bitcoin" with a lower case "b" whenever I am referring to bitcoin the cryptocurrency and with an upper case "B" whenever I am referring to Bitcoin the network), and peer-to-peer payment system (the Bitcoin blockchain network) in a modest nine-page paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, 2008a). Against the backdrop of a global financial crisis, the genesis block of the Bitcoin network was mined on January 3, 2009 and the first block thereafter was created on January 8, 2009.[7] Nakamoto (2009b) announced the release of the Bitcoin protocol software as open source the day after the first block was mined.

[6] Many theories exist about the real identity of Satoshi Nakamoto (see, e.g., O'Neal, 2019). Some argue that Nakamoto is the American computer scientist, legal scholar, and inventor of the concept of smart contracts Nick Szabo; others that Nakamoto was the late Hal Finney, a cypherpunk and one of the early contributors to Bitcoin's codebase; and still others posit that Nakamoto is British cryptographer Adam Back, CEO of Blockstream. Yet another possibility is Craig Wright – who has actually claimed to be Satoshi Nakamoto – an Anglo-Australian computer scientist and businessman. Rather interestingly, Wright was granted the United States copyright registrations for the original Bitcoin whitepaper and code, which he still holds (Bitcoin SV, 2019).

[7] The original block hash at Block 0 is 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f and the hash of Block 1 is 00000000b873e79784647a6c82962c70d228557d24a747ea4d1b8bbe878e1206. As Bitcoin is a shared and transparent ledger, readers can see this for themselves at www.blockchain.com/btc/block/000.