1 Introduction

For more than a decade, blockchains have been a buzzword permeating the business press, where they are often presented as a ‘revolution’. Aside from this media attention, blockchains are now becoming a reality for an increasing number of organizations. Expanding beyond their roots in cryptocurrencies, blockchains have found their way into a broad range of industries, from retailing to insurance. Blockchains are starting to truly change the business world, and their impact on the global economy will likely only continue to grow over the coming decades. The number of blockchain-based projects has been rapidly increasing year by year. Deloitte’s global blockchain surveys in 2019 and 2020 show that the percentage of companies that have already employed blockchains has increased nearly twofold, growing from 23 per cent in 2019 to 39 per cent in 2020 (Deloitte, 2020, p. 7). This percentage is even higher among large enterprises (46 per cent in the ‘more than US$1 billion’ revenue sector). Based on the technology’s prospective usage across industries, a recent report by PwC shows that ‘blockchain technology has the potential to boost global gross domestic product (GDP) by US$1.76 trillion over the next decade’ (PwC, 2020, p. 4).

Blockchains have the potential to fundamentally disrupt the way in which business is conducted. They provide a new way of solving elemental business problems related to recording, tracking, verifying, and aggregating various types of information (Felin & Lakhani, 2018). Successful cases of blockchains abound in a variety of industries. The insurance industry benefits from blockchain-based fraud detection, record reconciliation, and risk prevention (CBInsights, 2019). In the energy sector, blockchains have been used to track and certify low-carbon energy and to enable direct transactions of energy between individuals, neighbourhoods, and even smart devices such as solar panels (Brink, 2021). Banks use blockchain technology to automate financial processes (e.g., transaction settlements and the issuance of credits and guarantees), create trustworthy auditable trails, and enhance the security of their systems (Garg et al., 2021). The auto industry has employed blockchains to trace parts across a vehicle’s life cycle (Zavolokina et al., 2020). In the used car market, blockchains help track and immutably record information about vehicles, such as service history, mileage, and age (Gaszcz, 2019). Pharmaceutical companies employ blockchains to authenticate pharmaceutical products and prevent counterfeits from entering the supply chain (Mattke et al., 2019). Healthcare providers use blockchains to streamline information management systems and improve the interoperability of healthcare databases (Tanwar et al., 2020). For media companies, blockchains provide an attractive solution to help fight fabricated information and ensure the authenticity of news releases (Lacity & van Hoek, 2021b).

Consider *DL Freight* as one example of a blockchain that facilitates more efficient supply chains (for more details about the case, see Lacity & van Hoek, 2021a). DL Freight was initiated by Walmart Canada and DLT Labs, a company developing enterprise blockchain solutions. The major purpose of DL Freight is to drastically reduce the need for reconciling inconsistent information across the supply chain. Before implementing the blockchain, Walmart Canada had to incur significant costs to verify carriers' charges and to address disputes with them, and carriers complained about lengthy waiting times before receiving payments. The DL Freight blockchain aims to eliminate costly reconciliation processes by providing a single version of the truth in a reliable manner. Instead of validating and recording freight invoices and payments ex post, the DL Freight blockchain enables validation, recording, and sharing in real time. It uses smart contracts (i.e., preprogrammed codes that execute once certain conditions are met) to automatically produce invoices, issue reimbursements for late shipments, and process payments. Such automated actions are taken based on information collected by digital devices, such as GPS trackers on the truck, to determine the location of the freight. Consequently, the relevant data are transparent to authorized users, who share a common understanding of information for which agreements have been reached. Following the implementation of DL Freight, disputes regarding invoices reportedly decreased from 70 per cent to less than 2 per cent, and relationship satisfaction among supply chain participants significantly improved (Lacity & van Hoek, 2021a).

The above real-life examples of contemporary blockchain applications show that the technology can add value to a broad range of business activities. However, what are blockchains, and what makes them so different from other technologies? What changes will blockchains truly bring about, especially with regard to the strategic management of organizations? In this Element, we provide a critical assessment of the status quo as well as identify potential challenges and opportunities associated with blockchains. We especially highlight how blockchains can address a range of organizational issues related to both cooperation and coordination. Our core thesis is that blockchains can help firms overcome these enduring organizational challenges in a new way that cannot be fully replicated by traditional solutions. We show that blockchains may significantly change the way we think about traditional contracting and trust issues while offering novel opportunities in terms of organizational design.

In the next section, we start by outlining the history of blockchains and the fundamental features that make them stand out as a digital innovation that is poised to impact an increasingly broad range of organizations. After explaining what blockchains are, we turn our attention to decentralization as the most salient property that makes them stand out from other technologies, along with some resulting properties (i.e., immutability, data integrity, transparency, and tokenization), and to smart contracts as a key value-adding complementary feature. In Section 3, we provide an overview of the existing knowledge of blockchains in the management literature, outlining the central research themes of different management disciplines and the major theoretical lenses and methodologies employed. In Section 4, we focus on discussing the implications of blockchains for three important strategic issues, namely, contracting, trust, and organizational design. Blockchains are, of course, not without limitations. In Section 5, we direct our attention to some potential problems associated with blockchains and elaborate on important technical, ethical, regulatory, and environmental challenges. In Section 6, we conclude this study with a discussion of the implications of blockchains for both managers and academics.

2 Blockchain Fundamentals and Features

2.1 A Brief History

Although 2008, when the Bitcoin whitepaper was released, is often seen as the starting point of blockchain technology, the idea of a cryptographically secured chain of blocks for storing information can be traced back to Haber and Stornetta in 1991. In fact, the blockchains we see today are essentially an innovative integration of many technologies that date years, and even decades, earlier (Narayanan & Clark, 2017). In 2008, Satoshi Nakamoto (a pseudonym) introduced Bitcoin, a cryptocurrency that can be securely traded among users without a trusted party coordinating the exchange. In the years that followed, blockchains were primarily developed to support different types of cryptocurrencies, with limited other functionalities. These blockchains are often called the first generation. Going beyond monetary systems, a second generation of blockchains started to emerge, of which the Ethereum blockchain was the leader. Ethereum uses a different programming language, which supports smart contracts and more complex decentralized applications. This feature represents an important advancement because it allows people to code complex tasks into blockchain systems. Blockchains have thus been implemented in different industries with a variety of functionalities, as illustrated by the multiple examples presented earlier. To date, developers have devoted their attention to improving earlier versions of blockchain technology by solving existing drawbacks, such as poor scalability and interoperability. These newer developments are also referred to as the third generation of blockchains, among which the Cardano blockchain emerged as a leader. Next, we will explain the technology in greater detail.

2.2 Definitions

Given the relative novelty of blockchains, no consensual definition has emerged thus far. Influenced by the interest and focus on blockchains, practitioners and academics have suggested a variety of conceptualizations. We list some of the prominent attempts at defining blockchains in Table 1.

Based on the commonalities among extant conceptualizations, we propose the following integrative definition: blockchains are cryptography-based decentralized and distributed systems consisting of an ongoing list of digital records that are shared within a peer-to-peer network. This definition aims to capture the most general and fundamental features of blockchains while striving for conciseness.

A blockchain network contains different types of participants called nodes. A node can be any type of device, such as a computer, laptop, or server, with the

Table 1 Different definitions of blockchains in the literature

Literature	**Definition of blockchains**
Babich & Hilary (2020, p. 224)	'A family of technologies used to develop and maintain distributed ledgers (i.e., databases that are massively replicated on all the "nodes" or machines in the system)'
Chod et al. (2020, p. 4379)	'Blockchains are cryptographically secure, distributed ledgers that can enable decentralized verifiability of digital-goods transactions'
Cole et al. (2019, p. 470)	'Blockchain is, essentially, a distributed database system that records transactional data or other information, secured by cryptography and governed by a consensus mechanism'
Du et al. (2019, p. 51)	'A blockchain is a chain of data blocks each of which is created to record a transaction'
Pazaitis et al. (2017, p. 109)	'A blockchain is a distributed ledger or database of transactions recorded in a distributed manner, by a network of computers'
Saberi et al. (2019, p. 2118)	'Blockchain technology is a distributed database of records or shared public/private ledgers of all digital events that have been executed and shared among blockchain participating agents'
Treiblmaier (2018, p. 547)	'The blockchain [is] a digital, decentralized and distributed ledger in which transactions are logged and added in chronological order with the goal of creating permanent and tamperproof records'

required hardware (e.g., internet access) and software to be connected with other nodes. Blockchains operate in peer-to-peer networks, which refer to the architecture where every node has equal privilege and can exchange data and resources directly with each other. This design is different from the traditional client–server architecture, where information needs to pass through servers to be transmitted. Blockchains involve a number of previous advancements in cryptography, such as public–private key encryption, hash encryption, and digital signatures, integrating them in an innovative way to ensure information security (see Narayanan & Clark, 2017 for a discussion of the technical details of blockchains).

From a process perspective, a blockchain works as follows (see Figure 1). A participant in the network requests a new transaction, which is broadcast to other nodes in the network. Based on a certain consensus mechanism (i.e., the protocol based on which the nodes agree with each other), some nodes collectively verify whether the received transaction request is legitimate. Once verified, the transaction is added to the blockchain, usually in the form of a block with several pieces of records aggregated together. New blocks will be attached to the existing blocks by using hashes (i.e., one-way mathematical functions that map data of any size to data of a fixed size). Finally, the updated chain of information is broadcast to the network, indicating the complete execution of the transaction request.

Beyond the general features discussed in this section, note that individual blockchains can differ markedly from one another in terms of design, data structure, and consensus mechanisms, among other features (Werbach, 2018). The most frequently used way to categorize blockchains is the distinction

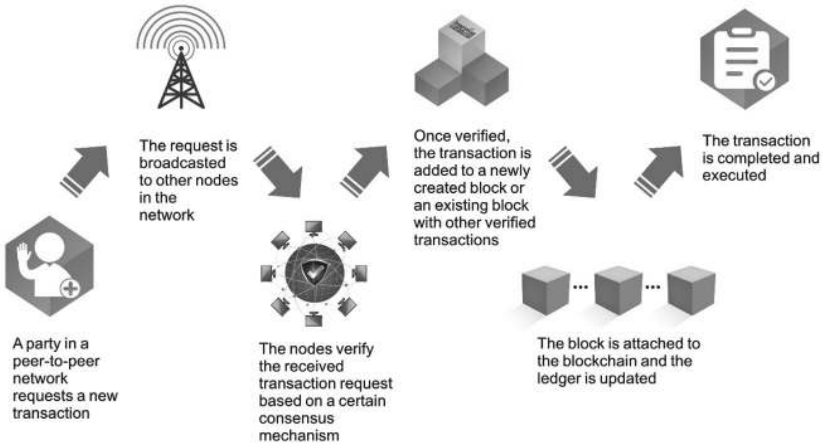

Figure 1 The functioning of blockchains (Lumineau et al., 2021a)

between public and private blockchains, sometimes also referred to as permissionless and permissioned blockchains. In public/permissionless blockchains, any node with access to the Internet can participate in viewing and verifying information. Bitcoin and Ethereum are examples of such blockchains. In private/permissioned blockchains, only participants with permissions can participate in viewing and verifying transactions. Many enterprise blockchains aiming to be integrated and utilized for enterprise usages take this form, such as IBM's Hyperledger and R3's Corda. Some scholars further clarify the nuances of the differences by disentangling the right to read and submit transactions (public vs. private) from the right to validate transactions (permissionless vs. permissioned) (e.g., Beck et al., 2018). In fact, while different blockchains resemble each other to certain degrees, they also differ in many aspects of both design and performance (see the discussion of different consensus mechanisms in the next section). The term 'blockchain' has to date been used as an umbrella term to refer to a number of distributed ledger technologies by different parties (Narayanan & Clark, 2017). In this Element, our definition aims to distil the central features that generalize across most types of blockchains, whereas our discussion of blockchain features addresses the diversity in blockchain solutions.

Just as the Internet supports the direct exchange of information, a key objective of blockchains is to support the direct exchanges of value between independent parties, which traditionally happen through intermediaries (Lacity, 2020). For example, when people need to wirelessly transfer money to one another, banks are required to keep the record and make sure that the sender no longer possesses the value (i.e., cannot use the money) after sending it – also known as the double-spending problem. Blockchains can solve such problems without intermediaries, supporting their role in facilitating the direct exchange of value. To understand why they have this capability, we need to examine the critical functionalities enabled by blockchains. We start by considering decentralization, which is the most fundamental feature of blockchains.

2.3 Decentralization

By recombining a variety of technologies, including digital signatures and encryption methods, the most salient feature enabled by blockchains is arguably the decentralization of exchange networks (Hanisch et al., 2022). Blockchains enable a dispersion of rights to access information and make decisions (Vergne, 2020), which were traditionally held by trusted intermediaries (e.g., governments, banks, platform owners) through hierarchical lines.

Centralization has been the dominant approach to organization for manifold reasons, among which information consistency is particularly relevant.

Maintaining a consensual understanding of the status quo is important for any kind of collaborative relationship. For example, for financial systems, it is critical to keep information identical across different subsystems to avoid people arbitrarily withdrawing money from some accounts.

Generally, maintaining consensus tends to be easier for a centralized system than for a decentralized system. The central trusted party is tasked with verifying and distributing information, while others merely receive the information. In contrast, in decentralized systems where no such trusted party acts as a central coordinator, anyone can alter the information, and consensus is difficult to achieve and maintain.

Blockchains enable decentralization while maintaining information consistency through built-in consensus mechanisms. Put simply, consensus mechanisms define the voting rule among nodes and determine how the decisions to verify and add information to the blockchain are made in a way that all nodes agree on. Relevant consensus mechanisms range from proof-of-work (PoW), proof-of-stake (PoS), and practical Byzantine fault tolerant (PBFT) to lesser-known variants, such as proof-of-elapsed-time and proof-of-burn. There are also many hybrid consensus mechanisms, including proof-of-activity (hybrid of PoW and PoS) and proof-of-authority (hybrid of PoS and Byzantine fault tolerant) (Wang et al., 2019).

Consensus mechanisms are at the core of blockchains and reflect distinct blockchain designs. Each consensus mechanism has certain pros and cons and thus involves trade-offs across relevant performance dimensions of blockchains, including Byzantine fault tolerance, energy consumption, scalability, and the transaction rate. *Byzantine fault tolerance* refers to the maximum voting power of malicious nodes that the system can tolerate, which relates to the relative security of the system. Some consensus mechanisms, such as PoW and proof-of-elapsed-time, depend on a considerable number of computation tasks to allocate voting rights, which creates significant *energy consumption*. *Scalability* refers to the capacity of the system to accommodate a large number of participants. PBFT (and its variants), which is usually used in permissioned blockchains, often faces difficulties in attracting more participants to scale up. On the flip side, PBFT-based blockchains can maintain a high *transaction rate*, which represents the speed of reaching consensus and adding blocks. A comparison of different consensus mechanisms is presented in Table 2 (based on Bodkhe et al., 2020 and Wang et al., 2019).

A common theme that underlies all consensus mechanisms is their attempt to deliberately make it costly for any single party to unilaterally change the information on the system without drawing attention (Vergne, 2020). Hence, in blockchains, no single authority has full discretion in terms of verifying and updating records. Decentralization is thus a major merit of blockchains, as it can

CAMBRIDGE

Cambridge University Press & Assessment
978-1-009-06073-8 — Blockchains
Wenqian Wang, Fabrice Lumineau, Oliver Schilke
Excerpt
More Information

Table 2 A comparison of different consensus mechanisms

	Proof-of-work	Proof-of-stake	Practical Byzantine fault tolerance	Proof-of-burn	Proof-of-elapsed-time
Basis of voting power	Based on the computational power to solve random puzzles	Based on the current monetary stake and random selection	Based on randomly selected orders	Based on the willingness to lose stake in the short term	Based on randomly assigned waiting ti
Byzantine fault tolerance	50 per cent	50 per cent	≤33 per cent	N/A	N/A
Level of decentralization	High	High	Medium	High	Medium
Energy consumption	High	Low	Low	Low	High
Scalability	High	High	Low	High	High
Transaction rate	Low	High	High	High	Medium

fundamentally alter the traditional paradigm of maintaining a consensual understanding of the status quo according to which members of the system have to rely on a centralized party as the sole entity aggregating and holding information and making decisions.

2.4 Immutability, Data Integrity, Transparency, and Tokenization

The unique ability of blockchains to decentralize both access to information and decision-making rights lends blockchains a number of characteristics that make them attractive candidates for organizing a variety of important tasks. Centralized systems with a single point of failure are vulnerable to external malicious hacks, unexpected errors in the centralized authority's server, or even deliberate cheating by the central party. In contrast, blockchains are designed with the objective that no single party can change the recorded data without other parties noticing. The addition of new information to the blockchain requires a consensus among the nodes whose major task is verification, and the specific consensus mechanism is part of the protocol of the blockchain infrastructure. The system is thus resistant to the failure of individual nodes to the extent that even the system does not know exactly whether there is a failed component (Babich & Hilary, 2020). As long as the network has a majority of honest nodes that perform their tasks correctly and do not attempt to modify the transactional history, participants can have confidence that their transaction records are not corrupted.

In addition, blockchains allow identical information to be stored across different physical addresses (i.e., computers). This feature differs from most traditional digital systems, which concentrate information on a central server. Hacking then becomes more difficult because there is no centralized target to break into. Consequently, the information stored in blockchains is considered *immutable* and *censor resistant*, which further reinforces confidence in the *integrity of data* stored on blockchains.

The architecture of blockchains also greatly improves the *transparency* and *traceability* of the associated information. The information stored on blockchains is timestamped and linked chronologically. Depending on the protocol and purpose of the blockchain, participants have access to the information that they are supposed to see. Due to the immutability of blockchains, participants can easily trace the origin of digital assets or the source of information stored on blockchains, which makes blockchains particularly useful for supply chain management (Saberi et al., 2019). Some examples include the Food Trust blockchain, which traces the logistical status of products across the actors of a food supply chain, and the Everledger blockchain, which traces and authenticates the origin of diamonds. The participants of these blockchains do not have to rely on cues and heuristics to judge potential value and risk along the supply chain but have a better understanding of the product due to the enhanced transparency and traceability supported by these blockchains (Montecchi et al., 2019).

The abovementioned properties of blockchains greatly enhance the value of *tokenization*, which refers to the process of converting assets, either physical or digital, into digital tokens on blockchains. Since digital artefacts (e.g., text, image, sound, numbers) can be easily copied and transmitted, it has been difficult to ensure that the original copy has been destroyed after being transferred to another party. Blockchains provide a decentralized solution that prevents the double-spending problem by ensuring that only one copy of the digital asset is valid. Such a design makes it possible to employ non-fungible tokens (NFTs) that are unique and cannot be replaced. For example, people may use an NFT to represent an artwork (Ennis, 2021). Since it is practically impossible to replicate the token, the NFT effectively provides authentication and certification of ownership of the artwork. Other examples of tokenization through blockchains include the trade of music ownership (Forde, 2021), the verification of data regarding carbon emission quotas (Kim & Huh, 2020), and the certification of land registry (Oprunenco & Akmeemana, 2018). The use of NFTs will change the way people portray their identities online (Segal, 2021).

2.5 Smart Contracts and Automation

Most blockchains rely on smart contracts to automatically execute transactions involving digital assets (Buterin, 2014). Smart contracts are lines of computer code that automatically execute whenever certain predefined conditions are met. Thus, smart contracts can greatly facilitate the automation of transactions. For example, a smart contract can be programmed to automate payments. To illustrate, as soon as a set of radio-frequency identification (RFID) chips reaches a dock, the smart contract automatically generates a receiving report and authorizes the payment (Yuthas et al., 2021).

The idea of smart contracts originated well before the invention of blockchains (Szabo, 1997). However, for the longest time, it failed to garner much popularity since it has always been possible to alter agreements unilaterally, leaving low-power parties vulnerable to changes. In contrast, blockchains have made it possible to make agreements immutable, a property that strongly complements smart contracts and ensures that the programs are intact and that the transaction conditions have not been tampered with (Narayanan & Clark, 2017).