Introduction to Blockchain

Wendy M. Charles

Abstract As life sciences research organizations explore methods to facilitate patient-centered and innovative technologies, they are increasingly exploring distributed ledger technologies ("blockchain") to address many of these needs. Blockchain is demonstrating the potential to transform life sciences research, allowing more data capabilities and innovation. Blockchain-based applications vary from audit trails for provenance to integrating remote devices to managing data for decentralized trials. As blockchain is emerging in life sciences, there are questions about the benefits and drawbacks of these technologies. This chapter introduces basic information about the common characteristics of blockchain technologies and the features they add to life sciences research. This chapter also addresses some of the uses of blockchain and lays the groundwork for the real-world applications, benefits, and drawbacks described in future chapters.

Keywords Blockchain · Distributed ledger technologies · Privacy · Trust · Audit trails · Performance

1 Introduction

Life sciences organizations use computerized systems to perform many aspects of research. Computerized systems can include laboratory processing equipment, as well as software for electronic consent, electronic signatures, electronic data capture, clinical trials management system, trial master files, statistical analysis software, image graphics, and electronic transmissions to data coordinating centers and to the regulatory agencies [1].

While life sciences research involves greater volumes of data, current electronic data management and collection methods may not be flexible enough to meet modern technological needs [2]. For example, there are increasing calls for patient-centered technologies, such as offering "dynamic consent," which involves methods to honor

W. M. Charles (✉)
Life Sciences Division, BurstIQ, Denver, CO, USA
e-mail: wendy.charles@cuanschutz.edu

W. Charles (ed.), *Blockchain in Life Sciences*, Blockchain Technologies,
https://doi.org/10.1007/978-981-19-2976-2_1

specific terms of individuals' consent and data access for research participants [3]. Further, few efficient or cost-effective ways exist to combine data from many sources or silos [4]. Therefore, distributed ledger technologies (collectively described as "blockchain" throughout) feature characteristics and capabilities that could address data challenges in life sciences research [5]. Most notably, blockchain offers opportunities to accelerate research innovation in ways not possible with current data technologies [6].

There is increasing interest and development of blockchain technologies in life sciences research [7]. In fact, "nearly 70% of all life sciences executives surveyed specified that they planned to implement one or more blockchain projects in 2020" ([8], p. 2). Therefore, it is necessary for stakeholders in life sciences organizations to become familiar with the nature of blockchain features that can be used to advance life sciences research.

2 Blockchain Core Characteristics

Blockchain is not technically a new technology but a set of methods that bring together standard techniques for recordkeeping. The concepts have evolved from a trusted process for time-stamping digital documents in 1991 [9] to the exchange of digital currency without intermediaries in 2008 [10]. Public interest and participation in blockchain rose with the development of Bitcoin as a "cryptocurrency," a digital currency secured by cryptography that can be exchanged by individuals ("peers") in a peer-to-peer manner without financial institutions [11].

Since 2008, the sophistication of blockchain technologies has evolved beyond the original blockchain technologies [12]. Andrianov and Kaganov [13] offer that blockchain is similar to a cloud-based service not tied to a data center, utilizing common cryptography characteristics, distributed data management, and synchronized data flows [14]. With the development of different methods and platforms, it is most accurate to consider blockchain as a set of tools and technologies rather than any single technology. As a result, there are no consistent or standard definitions of blockchain [15], including ongoing debates on whether private and/or centralized networks can constitute blockchains [16, 17].

The following are common features of most types of blockchains.

2.1 Ledgers

The first characteristic of blockchain methodology involves using "ledgers" instead of data tables or relational databases [18]. Like an audit log, an ever-growing ledger records each instance where data are created, and previous records generally cannot be modified or deleted. Modified data are instead appended to the ledger to show that the value has changed, but the original value remains for historical data purposes

[18]. With the ability to use a ledger instead of prescribed data fields, a blockchain can import and track structured or unstructured data from diverse electronic sources, depending on the data mapping and configurations [19].

When a prescribed number of entries are added to the ledger, the entries are assembled in a "block" with time stamps, validation methods, historical structure, and other selected metadata [13, 18]. When a block is formed, the entries contained in the block cannot be modified.

2.2 *Cryptography*

Blockchains also utilize "cryptography," a method of using codes and algorithms to secure information and communication [20]. As shown in Fig. 1, when entries of any type are added, they are represented with digital signatures comprised of unique strings of alphanumeric characters referred to as "hashes" [18]. These one-way hashes are created by complex algorithms that cannot be reversed to reveal the input [19].

Hashes are not only used to record entries onto the ledger, but also to create a digital summary of the entries in the block. As shown in Fig. 2, a block's hash is also the mechanism used to link blocks in sequential order. As a block is added to the chain, it contains the hash of the previous block.

If it were possible to modify data within a block, the modification would change the hash of that block (Fig. 3). Because blocks are linked with hashes, a change in a block's hash would change the hash in the next block, and so on in subsequent blocks—a task that is exceptionally computationally challenging [21].

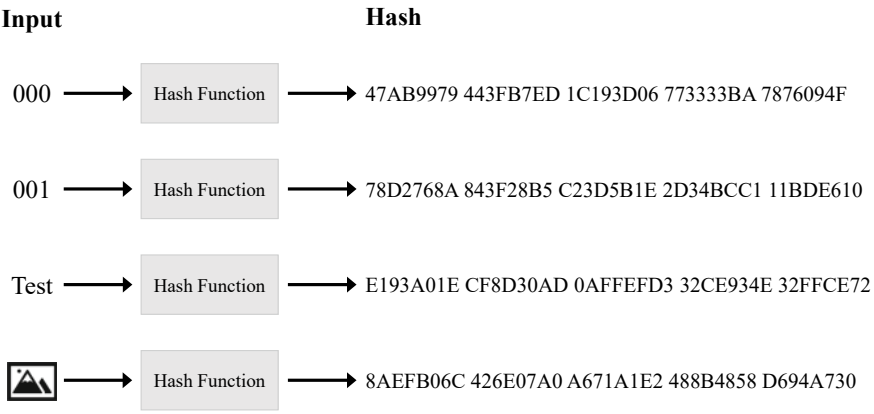

Fig. 1 Fictional examples of hashes. Regardless of input type, the alphanumeric hashes are unique and sophisticated so that the hashes cannot be reversed to reveal the input

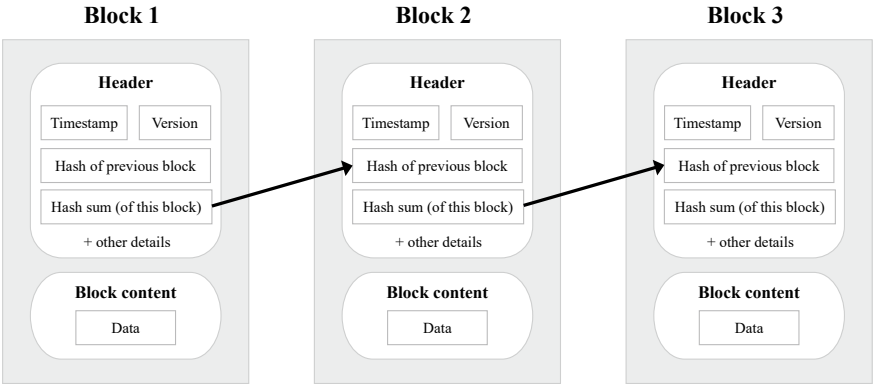

Fig. 2 Simplified depiction of block design and mechanisms of linking blocks using hashes

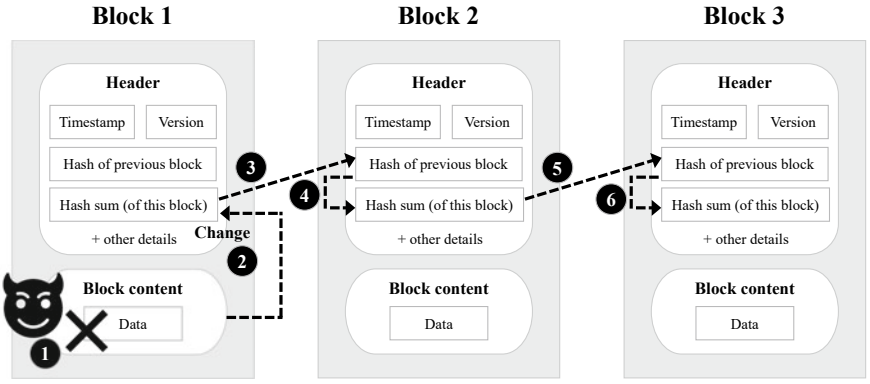

Fig. 3 Simplified depiction of how a data change in one block of an existing chain would require changing the hashes in subsequent blocks. This would be an exceptionally challenging task

2.3 Immutability (Tamper Evidence and Tamper Resistance)

While blockchain is sometimes referred to as "immutable," this book takes the position offered by the U.S. National Institutes of Standards and Technology (NIST):

> Most publications on blockchain technology describe blockchain ledgers as being immutable. However, this is not strictly true. They are tamper evident and tamper resistant, which is a reason they are trusted for financial transactions. They cannot be considered completely immutable because there are situations in which the blockchain can be modified. ([18], p. 34)

Rather than immutable, NIST encourages using the terms "tamper resistant and tamper evident" ([18], p. 34) to denote a blockchain's strong, but not absolute, security. A blockchain provides evidence that data existed at a specific time and that

data were not altered [13]. This data integrity feature is particularly pertinent for life sciences research systems that do not otherwise provide a complete chain of custody or data security from data creation to data analyses.

2.4 Distribution

The last primary characteristic of blockchains involves the distribution or decentralization of storage. Instead of central servers or centralized data centers, blockchain utilizes storage distributed over many servers, referred to as "nodes" [18]. This network structure, involving peer-to-peer/organization-to-organization connections, typically creates multiple, identical copies of the ledger across the participating servers in the network. The distributed storage allows data transfer without an intermediary or risk of interference [22], preserves data integrity and availability [19], and provides data redundancy to reduce vulnerabilities to viruses, ransomware, or downtime [23]. Distributed nodes in life sciences organizations are optimally advantageous for decentralized clinical trials where data collection and management are distributed throughout the network [13]. Further data monitoring can occur from a wider variety of locations.

For the nodes to agree on which data entries are the most current and to ensure consistency across the network, blockchains use "consensus mechanisms" to reach an agreement [24]. A thorough discussion of consensus mechanisms is beyond the scope of this chapter, but the reader is encouraged to read some published overviews (e.g., [15, 25, 26]).

3 Blockchain Features

This section introduces blockchain features that may be selected for life sciences research. This section aims not to provide a comprehensive list of blockchain features but to compare and contrast standard features. This section focuses on the differences between permissioning, on- and off-chain storage designs, and smart contracts.

3.1 Permissionless Versus Permissioned

"Permissioning" involves access controls to specify which individuals, roles, or organizations are allowed to participate in a blockchain project. When blockchain permissioning was first introduced, blockchains were described as public/permissionless and private/permissioned. However, this distinction has since become more nuanced as permissioning is now available on some public blockchains [6]. For example, Enterprise Ethereum and Ethereum Private use the public Ethereum open-source

code but offer private zones [27, 28]. While there are a few different ways that permissioning features could be described, this chapter characterizes approaches as "permissionless," "permissioned," and "hybrid," with a brief discussion of "consortium" blockchains.

3.2 Permissionless

The first types of blockchain platforms used for cryptocurrency were designed to offer a transparent environment for currency exchange [29]. Platforms such as Bitcoin and Ethereum permitted anyone from the public to join, review, and approve transactions [30]. These platforms use hundreds to thousands of nodes to strengthen network integrity and security [31], making it practically infeasible to corrupt a network of that size [32]. Popular permissionless blockchains are Bitcoin, Ethereum, Dash, and Monero [33].

To provide incentives for public nodes to process transactions, permissionless blockchains typically utilize consensus mechanisms where the submitter pays a transaction fee in digital currency for the nodes to process the data [34]. These transactions often use a consensus mechanism referred to as proof of work, where nodes compete against each other to complete complex computational puzzles to win the right to validate the transaction and form the block [35]. This computationally intensive process is called "mining" and is sometimes criticized for relatively slow transaction speeds, high electricity use, and pollution [36].

While large, permissionless networks are lauded for their transparency and broad decentralization, the management of patient-level information would create major privacy concerns [31]. In addition, due to the need for centralized project coordination and compliance, a completely permissionless infrastructure does not allow for the oversight required of regulated research [37]. Furthermore, permissionless networks that use slow, computationally intensive processing would not meet the requirements for high-speed processing needed for research collection and analyses [6]. Last, the costs for processing large volumes of data would likely be high and cost-prohibitive [16, 38]. Therefore, most life sciences organizations pursuing blockchain projects are starting with permissioned blockchains.

3.2.1 Permissioned

Permissioned blockchains involve a governance structure that requires individuals or organizations to receive permissions to join the network. For life sciences organizations, activities must be associated with an established, named identity for accountability [6]. Permissioned networks involve distributed and synchronized ledgers but may be restricted to nodes within a single organization or a group of organizations that invest in the governance and maintenance of the network, such as academic

institutions or commercial sponsors [39]. Because these organizations provide financial support to the network, data activities do not typically require transaction fees customary of permissionless blockchains [40].

Permissioned open-source blockchains include Hyperledger Fabric, Corda, Ethereum Private, and MultiChain [33]. Permissioned blockchain companies designed for health information or life sciences research include BurstIQ's BurstChain®, Carechain, Hashed Health, and Patientory, among others [39].

Permissioned blockchains offer many advantages for privacy and flexibility but can manifest vulnerability to the limitations in protecting data integrity. Dai et al. [32] point out that there is a risk of collusion among limited nodes that may lead to excluding certain transactions or even rolling the chain back to an earlier recorded state. Along these lines, permissioned blockchains may have a controlling authority that can corrupt nodes or allow vulnerabilities that could be exploited by attackers [13].

3.2.2 Hybrid Permissioning

"Hybrid" blockchains contain features of both permissionless and permissioned blockchains. For example, a private network may manage confidential information and permissions for access and data posting but stores metadata and pursues periodic backup to a permissionless blockchain for additional data integrity [41, 42]. A hybrid blockchain design may offer a distributed network with flexibility and usability of permissioned features [41].

To ensure that permissioned blockchain research data remained trustworthy, ConsenSys adds a Hyperledger Besu module to manage a private network while connecting to the Ethereum network [43]. Similarly, Dai et al. [32] connect a private clinical trials blockchain to the Ethereum network. A snapshot of the permissioned chain is captured at periodic intervals (e.g., once per day, once per week) as a transaction on the permissionless ledger.

3.2.3 Consortium

A "consortium" blockchain involves the cooperation of separate legal entities that provide governance and support for blockchain operations [25]. A consortium is considered a semi-decentralized infrastructure with control over operations, maintenance, and regulatory compliance [13].

3.3 Off-Chain Versus On-Chain Storage

With consideration that life sciences research requires volumes of data across large networks of users, it is necessary to create data management strategies that can

effectively manage data processing needs. Data can be stored in secure organizational storage with only the metadata on the ledger ("off chain"), or data could be stored together with metadata on the ledger ("on chain") [44]. These storage strategies are compared and contrasted as follows:

3.3.1 Off-Chain Storage

The first permissioned blockchains were designed to maintain traditional storage mechanisms in servers, while the blockchain was designed to record when data were added or appended. This data storage strategy is also designed to manage files, such as digital images and genomic information, too large for ledger storage [45]. This strategy could also demonstrate data integrity when the hash is unaltered [41] with time stamping by the blockchain [22].

As life sciences organizations have implemented blockchain projects, their concern for protecting intellectual property and data confidentiality has initially resulted in decisions to maintain storage off chain [38]. Such off-chain storage technology may use an InterPlanetary File System to track where each file is stored among the distributed storage [46].

However, off-chain storage may not protect the actual data or files stored off chain. Košťál et al. [47] point out that there may be a hash on the blockchain to indicate that data were deleted or altered, but the hash does not protect or restore the data in the server. As an additional consideration, the extra copies of the ledger can be expensive [22, 31].

3.3.2 On-Chain Storage

As an alternate strategy, data can be stored on the ledger with metadata and time stamping. Raw data points can be stored with tags that allow data to be mapped for grouping and aggregation. Some blockchains also allow small files to be stored on chain [6]. While there is concern that on-chain storage could reduce scalability, a measure of speed and performance, organizations using on-chain storage to create an infrastructure of separate chains and mapping [6]. For example, BurstIQ created a platform that stores data on chain with high-speed flexible mapping and access permissions [48]. This blockchain is also capable of addressing the Health Information Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) to accommodate regulated health information and individually identifiable information on the chain [49].

3.3.3 Hybrid Storage

As a hybrid storage strategy, organizations have been exploring storing non-private data on chain, such as demographic information, but storing sensitive data in off-chain servers [13]. A hybrid approach is also desirable for organizations who wish to store most data on chain, but need to manage large files off chain in data lakes [31]. This strategy offers a combination of privacy and scalability, allowing ledger length to remain more manageable [6].

Overall, blockchain-based data storage requires careful planning to ensure consistent performance for the project's duration [45].

3.4 Smart Contracts

Smart contracts are small computer programs or short code segments that execute automatically when specific conditions or rules are met [50]. Because smart contracts are designed to run automatically, smart contracts can increase efficiency and accuracy by eliminating human involvement [51]. From a computational standpoint, smart contract code can only be executed or canceled [13]. This computational strategy provides security and failover because smart contracts can be run and restarted if there is a disruption [13].

4 Blockchain Benefits for Life Sciences

Considering the unique needs of life sciences research, blockchains provide the following features-often exceeding what could be offered in a traditional data system [39]. This section recognizes that life sciences organizations already utilize many electronic systems that offer some of the features attributed to blockchain earlier in this chapter. Blockchain offers many features included in traditional commercial off-the-shelf clinical trial management systems or electronic data capture software required by U.S. Food and Drug Administration (FDA) regulations since 1997 (21 CFR Part 11). These "Part 11" systems already offer access controls, error checking, prevention of data alterations, data backups, and end-to-end audit trails of all activities.

To determine where blockchain capabilities could exceed the capabilities of conventional electronic data systems, NIST published a flowchart (initially created by the Department of Homeland Security) [18]. Common decision points pertain to (1) whether data need to be shared, (2) more than one organization is involved with creating and managing data, (3) there are high requirements for data integrity, and (4) there may not be trust among all parties. Some of these characteristics are slightly outdated and do not necessarily reflect newer blockchain platform capabilities. Life

sciences organizations recognize that newer technologies, such as blockchain, are needed to enhance trust and security.

4.1 Trust

Beckstrom [52] points out that "trust is the foundational principle in clinical trials" (p. 111). The issue of trust has been a longstanding concern of patients and communities toward research institutions due to historical abuses, such as enrolling participants in research studies without their full knowledge. In the more modern era, individuals' data have been used and distributed for research purposes without their awareness or consent [53]. Unfortunately, even when individuals willingly participate in research projects, most current electronic data capture systems are designed to restrict individuals' access to the data collection or discoveries [54]. Both Benchoufi et al. [54] and Beckstrom [52] suggest that individuals would not only like to contribute to scientific advances, but would also like to gain visibility into the uses of their data to verify that the terms of their preferences are honored. Benchoufi et al. [41] argue that cases of research fraud and dubious research findings have created a growing mistrust of research institutions, stating that they can no longer be considered "trustable by default" (p. 1).

Blockchain has been introduced into the life sciences sector precisely because of the desire for more trust in data integrity, research outcomes, and collaborations among organizations that may not completely trust each other. Beckstrom [52] suggests that blockchain is a valuable addition to research collaborations where the cooperation in the blockchain network enforces honest behavior, and the transparent nature of the blockchain (within permissions) allows for better accountability [55].

Trust requires not only technology, but also coherent governance [41]. Specifically, "blockchain technologies offer a way to design governance systems: public, permissioned or private Blockchains; open- or closed-source software and smart contracts; fixed or evaluative governance rules" ([41], pp. 4–5).

4.2 Audit Trails—Provenance

The FDA defines an audit trail as "a secure, computer-generated, time-stamped electronic record that allows for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record" ([56], p. 4). Audit trails contain previous entries and metadata to associate activities with a time stamp, the person associated with the change, and the previous and new entries. This feature inherent in blockchain proves proof of existence [54].

While the FDA has required audit trails for electronic record systems since 1997, some traditional systems have been designed with insufficient ability to trace data back to original data sources—one of the top data system problems identified during

FDA inspections [37]. Benchoufi and Ravaud [57] point out that a blockchain allows additional metadata and end-to-end data provenance. This complex, enduring audit trail allows researchers, quality assurance personnel, and/or regulatory authorities to verify the authenticity of data entries [55] and is convenient for remote auditing [57].

4.3 Data Transparency Versus Privacy

With consideration that blockchains were initially designed for transparency as a method to promote trust, blockchains designed for life sciences have had to find a careful balance between transparency and privacy.

Life sciences research is structured to be a collaborative endeavor where scientists share ideas and data. Scientists who receive research funding from government agencies, such as the NIH, are required to create a Data Sharing Plan and make their data available upon request [58]. However, individuals and academic institutions are hesitant to share research datasets when there are desires to maintain a research edge in a competitive funding climate and concerns that data may be misrepresented from the context in which it was collected [59]. There are also often high costs for data administration and disputes about ownership [60].

Additionally, there is a tradeoff between the desire to provide transparency and trust among research participants [17], healthcare providers [22], and study sponsors [61]. This section describes different perspectives on the tradeoff between transparency and privacy.

4.3.1 Need for Data Privacy

Within life sciences research, the privacy of individual participation is a regulatory requirement [62]. Therefore, some life sciences organizations exposed to permissionless blockchains may be hesitant to use blockchain to process sensitive or confidential research information [63]. The emergence of private blockchains designed with permissioning capabilities has created new opportunities to utilize the features of blockchain while protecting the confidentiality of information.

As discussed earlier, some life sciences organizations utilize off-chain storage to protect private information. Benchoufi et al. [41] further advocate that data queries be designed to limit private information that recipients can receive. Angeletti et al. [63] offer the prospect that individual participants' data could even be stored in their personal computers, allowing individuals more control over how their information is used.

Blockchain also offers technological strategies to promote privacy. Differential privacy is a cryptographic method for publicly sharing a research dataset where only aggregate data are provided without allowing visibility of individual-level data. This approach is based on the premise that aggregate data do not change much if an

individual is added or excluded from the data, reducing the likelihood that individual participants could be identified [63].

Organizations are also exploring opportunities to use blockchain and artificial intelligence (AI) to create synthetic data. Sometimes referred to as "decentralization intelligence" [64], data remain private within individual organizations' storage. However, the data can be modeled across organizations to create representative data sets to be analyzed and used without compromising the privacy or confidentiality of actual data.

Another privacy-preserving blockchain strategy involves "zero-knowledge proofs." Zero-knowledge proofs are cryptographic protocols that "enable one party, called prover, to prove that some statement is true to another party, called verifier, but without revealing anything but the truth of the statement" ([65], p. 204448). While promising, the technology for zero-knowledge proof capabilities is new and has not achieved wide adoption yet.

Other privacy-preserving strategies for blockchain involve edge computing for near real-time applications to manage privacy constraints associated with computing in a cloud environment [66]. Another strategy involves homomorphic encryption, where data are processed while encrypted, and the encrypted output can only be decrypted later by authorized parties [67]. It is important to note that privacy-preserving strategies continue to develop as more organizations are testing novel advances in programming.

4.3.2 Need for More Transparency

Over the past several years, there have been many investigations and media reports about research misconduct, unscientific research practices, and outright fraud within life sciences organizations [59]. In a high-profile example, a former Duke University pulmonary biology lab technician was accused of doctoring "nearly every experiment or project in which she participated" ([68], p. 978). An investigation conducted by the Office of Research Integrity found that this technician "engaged in research misconduct by knowingly and intentionally falsifying and fabricating research data included in one hundred and seventeen (117) figures and two (2) tables in thirty-nine (39) published papers, three (3) manuscripts, and two (2) research records" ([69], p. 60097). This investigation resulted in a settlement where Duke University agreed to pay the government $112.5 million for submitting falsified data to receive federal grants that may not have otherwise been awarded [70]. Sivagnanam et al. [59] noted that most questionable research findings do not involve deliberate fraud but are difficult to replicate because the data and code are not available to the research community.

Therefore, there has also been a call for more transparency of life sciences research data due to concerns about fraud and misconduct in organizations that manage data internally. While electronic data systems are designed to meet specific regulatory requirements for the submission of new drugs or devices with protections against data modifications, there is concern that other research systems could allow users

or administrators to modify the primary data files, resulting in undetectable—and unrecoverable—alterations [17, 32]. Blockchain-based electronic systems provide transparency of research components critical for a study's integrity, such as data, programming code, research protocols, and statistical analysis plans [41].

Even though identifiable research participant information must be protected, blockchain technologies offer privacy-preserving strategies that allow replicating findings or sharing data without compromising research participants' identities or organizations' intellectual property. Further, projects have demonstrated that granular data sharing can be enabled that also protects intellectual property [71, 72].

4.4 Security

When blockchain technologies are used to store life sciences research data, the data must be securely maintained to protect data integrity (21 CFR Part 11), the privacy of research participants' sensitive information (21 CFR 56.111(a)(7)), and intellectual property [73]. Blockchain technologies offer several features that enhance the security of information. While these features are likely to be implemented differently, the following examples are recognized as common features. First, blockchains use cryptographic hash functions extensively that provide platform operations security and consistency [74]. Because the hash output has been created from a sophisticated algorithm, it is practically impossible to reverse engineer this information to determine the input [18]. This concept, called "collision resistance," specifies that it should be difficult for two raw text inputs to create the same output [74].

Within life sciences research, there is a frequent need to correct or update data. This capability is achieved in a blockchain with "append-only" programming where a correction/update is added as a new entry without overwriting the old entry [37]. When data are corrected or updated, many blockchain platforms design query programming that recognizes only the most current entries for the data queried, even though the ledger contains all historical changes to data [75].

In addition, the distribution of ledgers across nodes in the network creates information redundancy, preventing a single point of failure [63, 76]. Even when a node goes offline, the ledgers replicated among other nodes remain available for continued processing. Hirano et al. [77] confirmed blockchain network availability during an unplanned AWS cloud server outage in Tokyo when a node became unavailable during network testing. Because the blockchain maintained nodes in multiple locations, the redundant ledgers allowed for stable operation during the outage, and the AWS autoscaling service updated the data without errors.

Last, the nature of decentralized blockchain architecture (for some blockchain types) creates a network in which all individuals or organizations who maintain nodes must agree to follow the same protocols to prevent any entity from interfering or controlling blockchain operations [76]. This peer-to-peer environment creates a system where the nodes provide group support and oversight to ensure consistent functioning.

4.5 Performance

With consideration of the blockchain features that appear promising for adding benefit to life sciences research, the following are features that enhance capabilities for efficiencies and flexibility.

4.5.1 Automation

Smart contracts may be used to automate quality controls and safety alerts [21]. These automation can extend to enrolling patients and automating study-related visits, supplies, investigational products, and payments [13].

When clinical studies involve informed consent documents that grant or withdraw permissions, smart contracts are used to execute individuals' preferences about future uses of their data or specimens or access to private health information [13]. These smart contracts can execute granular permissions ranging from specific health values to an entire medical record and for specified periods [13, 40].

To facilitate data sharing among researchers, smart contracts are used to automate data sharing permissions among authorized parties. Specifically, smart contracts are designed to verify researchers' access to certain information and automate information transfers depending on the specified terms [6, 40].

For a sponsor or Contract Research Organization, smart contracts are not contracts, but are used to codify validation logic within legal contracts to validate transactions and rules, reducing the need for arbiters [13, 40]. Further, smart contracts can execute the terms of contracts, such as claims adjudication and billing to reduce reliance on paid staff [13]. Smart contract automation further enhances efficiencies of calculating outcomes and reports, including managing database closure [13].

4.5.2 Flexibility

Blockchain also offers electronic data system capabilities beyond the commercial off-the-shelf software available for life sciences research. Rather than purchase all-in-one commercial software, blockchain is used to create more functionality in existing software, data systems, and Internet of Things devices by using application programming interfaces to combine data streams for near real-time aggregation [6, 78].

4.5.3 Scalability

The performance of a blockchain can be measured in transactions per second, computing power, or consensus response time [79]. While cryptocurrency blockchains were designed to generate blocks slowly—an average of 10 min for Bitcoin [80]—to instill trust among the nodes, this performance is too slow for most

applications [81]. Because life sciences research blockchains require high-speed read and write access, life sciences organizations utilize several features to improve speed. These may include using a consensus mechanism aligned with the governance structure of a private network, such as Proof of Authority or Proof of Stake [82], breaking files into chunks referred to as shards [83], and/or utilizing side chains [84]. Therefore, speeds for private blockchain networks have increased between 2000–20,000 transactions per second [85, 86], allowing for acceptable speed and performance for most life sciences tasks.

5 Conclusions

Blockchain is emerging to create more sophisticated and holistic data systems for life sciences research [78]. Progressing far beyond the original features of blockchain for cryptocurrency, the development of blockchain within life sciences research organizations includes many types of platforms, variations of consensus mechanisms, combinations of storage, and more capabilities for smart contracts. Electronic data systems need not be replaced by blockchain, but could be enhanced by adding these capabilities. The goal is to move the life sciences industry toward a more collaborative network with more data integrity and sharing among authorized parties while providing checks and balances among partners [87].

The following chapters of this book introduce the complexity of how blockchain is currently being used for many areas within life sciences research, with discussions of the benefits and challenges of each of these applications. While blockchain promises to create efficiencies and advancements in life sciences research, we are reminded that blockchain is software—not magic. This technology cannot solve all—or even most—problems inherent in life sciences research, but has been shown to enhance trust in life sciences data.

6 Key Terminology and Definitions

Blockchain: "A distributed digital ledger of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules." ([18], p. 49)

Consensus mechanism: A fault-tolerant mechanism used in blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed nodes or multi-agent systems [24].

Dynamic consent: Dynamic consent describe personalized, online consent and communication "designed to achieve two objectives: (1) facilitate the consent process and (2) facilitate two-way, ongoing communication between researchers and research participants" ([3], p. 3).

Hash: A unique output (also called a hash digest) for an input of nearly any size (a file, text, image, etc.) by applying a cryptographic hash function to the input data ([18], p. 52).

Homomorphic encryption: A form of encryption allowing one to perform calculations on encrypted data without decrypting it first. The result of the computation is in an encrypted form. When decrypted, the output is the same as if the operations had been performed on the unencrypted data [67].

Scalability: The ability of a blockchain platform to manage increasing volumes of transactions and increase the number of nodes in the network [79].

Smart contract: A segment of code or a small computer program deployed designed to execute automatically when certain conditions are met. Nodes execute the smart contract within the blockchain network; all nodes must derive the same results for the execution, and the execution results are recorded on the blockchain [88].

Zero-knowledge proofs: "A protocol that enables one party, called prover, to prove that some statement is true to another party, called verifier, but without revealing anything but the truth of the statement" ([65], p. 204448).

Acknowledgements The author gratefully acknowledges the review and thoughtful feedback from Brooke Delgado, Leanne Johnson, and Hayley Miller.

References

1. U.S. Food and Drug Administration (2017, April 19) Program 7348.810: chapter 48—bioresearch monitoring program. Sponsors, contract research organizations and monitors. https://www.fda.gov/media/75916/download. Accessed 4 Feb 2020
2. Efanov D, Roschin P (2018) The all-pervasiveness of the blockchain technology. Elsevier Ltd., Amsterdam. http://www.sciencedirect.com/science/article/pii/S1877050918300206
3. Budin-Ljøsne I, Teare HJA, Kaye J, Beck S, Bentzen HB, Caenazzo L, Collett C, D'Abramo F, Felzmann H, Finlay T, Javaid MK, Jones E, Katić V, Simpson A, Mascalzoni D (2017) Dynamic consent: a potential solution to some of the challenges of modern biomedical research. BMC Med Ethics 18(1):4. https://doi.org/10.1186/s12910-016-0162-9
4. Angeletti F, Chatzigiannakis I, Vitaletti A (2017b) The role of blockchain and iot in recruiting participants for digital clinical trials. IEEE Communications Society, New York. https://ieeexplore.ieee.org/abstract/document/8115590
5. Hughes L, Dwivedi YK, Misra SK, Rana NP, Raghavan V, Akella V (2019) Blockchain research, practice and policy: applications, benefits, limitations, emerging research themes and research agenda. Int J Inf Manag 49:114–129. https://doi.org/10.1016/j.ijinfomgt.2019.02.005
6. Charles WM (2021a) Accelerating life sciences research with blockchain. In: Namasudra S, Deka GC (eds) Applications of blockchain in healthcare, vol 83. Springer Nature, Berlin, pp 221–252. https://doi.org/10.1007/978-981-15-9547-9_9

7. Agbo CC, Mahmoud QH, Eklund JM (2019) Blockchain technology in healthcare: a systematic review. Healthcare (Basel) 7(2):56. https://doi.org/10.3390/healthcare7020056
8. Treshock M, Fraser H, Pureswaran V (2018) Team medicine: how life sciences can win with blockchain (03013903USEN-00). https://www.ibm.com/downloads/cas/RYD0QA7G
9. Haber S, Stornetta WS (1991) How to time-stamp a digital document. J Cryptol 3:99–111. https://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=1954002DCD3DC6DB6C052994F8EF24CE?doi=10.1.1.46.8740&rep=rep1&type=pdf
10. Nakamoto S (2008, March 24) Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. Accessed 11 Oct 2020
11. Fulton F (2016) In: Collins C (ed) Bitcoin for dummies. Wiley, New York. https://www.academia.edu/30046580/Bitcoin_For_Dummies_-_1st_Edition_2016_
12. Conte de Leon D, Stalick AQ, Jillepalli AA, Haney MA, Sheldon FT (2017) Blockchain: properties and misconceptions. Asia Pac J Innov Entrep 11(3):286–300. https://doi.org/10.1108/APJIE-12-2017-034
13. Andrianov A, Kaganov B (2018) Blockchain in clinical trials: the ultimate notary. Appl Clin Trials 27(7/8):16–19. http://images2.advanstar.com/pixelmags/applied-clinical-trials/pdf/2018-08.pdf#page=16
14. Lin I-C, Liao T-C (2017) A survey of blockchain security issues and challenges. Int J Netw Secur 19(5):653–659. https://doi.org/10.6633/IJNS.201709.19(5).01
15. Zheng Z, Xie S, Dai H-N, Chen X, Wang H (2017) An overview of blockchain technology: architecture, consensus, and future trends. IEEE, Piscataway. https://ieeexplore.ieee.org/document/8029379/
16. Lopez PG, Montresor A, Datta A (2019) Please, do not decentralize the internet with (permissionless) blockchains! (11) [Preprint]. https://arxiv.org/abs/1904.13093
17. Zhuang Y, Sheets LR, Shae Z, Tsai JJP, Shyu C-R (2018) Applying blockchain technology for health information exchange and persistent monitoring for clinical trials. AMIA Annu Symp Proc 1167–1175. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6371378/
18. Yaga D, Mell P, Roby N, Scarfone K (2018) Blockchain technology overview (NISTIR 8202). NIST Interagency/Internal Report, Issue. https://www.nist.gov/publications/blockchain-technology-overview
19. Charles WM (2021b) Blockchain will transform clinical research. J Clin Res Best Pract 17(2). https://www.magiworld.org/resources/journal/2_Blockchain.pdf
20. Zhao B, Huang X (2020) Encrypted monument: the birth of crypto place on the blockchain. Geoforum 116:149–152. https://doi.org/10.1016/j.geoforum.2020.08.011
21. Engelhardt MA (2017) Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector. Technol Innov Manag Rev 7(10):22–34. https://doi.org/10.22215/timreview/1111
22. Omar IA, Jayaraman R, Salah K, Yaqoob I, Ellahham S (2021) Applications of blockchain technology in clinical trials: review and open challenges. Arab J Sci Eng 46(4):3001–3015. https://doi.org/10.1007/s13369-020-04989-3
23. Li H, Zhu L, Shen M, Gao F, Tao X, Liu S (2018) Blockchain-based data preservation system for medical data. J Med Syst 42(8):141. https://doi.org/10.1007/s10916-018-0997-3
24. Tosh DK, Shetty SS, Liang X, Kamhoua CA, Njilla LL (2017) Consensus protocols for blockchain-based data provenance: challenges and opportunities. IEEE, Piscataway. https://ieeexplore.ieee.org/abstract/document/8249088
25. Ray PP, Dash D, Salah K, Kumar N (2020) Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases. IEEE Syst J 15(1):85–94. https://doi.org/10.1109/JSYST.2020.2963840
26. Shahaab A, Lidgey B, Hewage C, Khan I (2019) Applicability and appropriateness of distributed ledgers consensus protocols in public and private sectors: a systematic review. IEEE Access 7:43622–43636. https://doi.org/10.1109/ACCESS.2019.2904181
27. About Enterprise Ethereum Alliance (2020) Enterprise ethereum alliance. https://entethalliance.org/about/. Accessed 31 July 2020

28. Private Ethereum Networks (2019) Go Ethereum. https://geth.ethereum.org/docs/interface/private-network. Accessed 31 July 2020
29. Calvaresi D, Calbimonte J-P, Dubovitskaya A, Mattioli V, Piguet J-G, Schumacher M (2019) The good, the bad, and the ethical implications of bridging blockchain and multi-agent systems. Information (Basel) 10(12):363. https://doi.org/10.3390/info10120363
30. Labazova O (2019) Towards a framework for evaluation of blockchain implementations. Bepress/Elsevier, Inc., Amsterdam. https://aisel.aisnet.org/icis2019/blockchain_fintech/blockchain_fintech/18/
31. Jung HH, Pfister FMJ (2020) Blockchain-enabled clinical study consent management. Technol Innov Manag Rev 10(2):14–24. https://doi.org/10.22215/timreview/1325
32. Dai H, Young HP, Durant TJS, Gong G, Kang M, Krumholz HM, Schulz WL, Jiang L (2018) TrialChain: a blockchain-based platform to validate data integrity in large, biomedical research studies (1807.03662) [Preprint]. National Center for Cardiovascular Disease. https://arxiv.org/abs/1807.03662
33. Kumar Sharma T (2019) Permissioned and permissionless blockchains: a comprehensive guide. Blockchain Council. https://www.blockchain-council.org/blockchain/permissioned-and-permissionless-blockchains-a-comprehensive-guide/. Accessed 25 July 2021
34. Wang Y, Wang H (2020) Using networks and partial differential equations to forecast bitcoin price movement. Chaos 30(7):073127. https://doi.org/10.1063/5.0002759
35. McGinn D, McIlwraith D, Guo Y (2018) Towards open data blockchain analytics: a Bitcoin perspective. R Soc Open Sci 5(8):180298. https://doi.org/10.1098/rsos.180298
36. Köhler S, Pizzol M (2019) Life cycle assessment of bitcoin mining. Environ Sci Technol 53(23):13598–13606. https://doi.org/10.1021/acs.est.9b05687
37. Wong DR, Bhattacharya S, Butte AJ (2019) Prototype of running clinical trials in an untrustworthy environment using blockchain. Nat Commun 10(1):917. https://doi.org/10.1038/s41467-019-08874-y
38. Steinwandter V, Herwig C (2019) Provable data integrity in the pharmaceutical industry based on version control systems and the blockchain. PDA J Pharm Sci Technol 73(4):373–390. https://doi.org/10.5731/pdajpst.2018.009407
39. Essén A, Ekholm A (2020) Centralization vs. decentralization on the blockchain in a health information exchange context. In: Larsson A, Teigland R (eds) Digital transformation and public services: societal impacts in sweden and beyond. Routledge, London, pp 58–82. https://doi.org/10.4324/9780429319297
40. Choudhury O, Sylla I, Fairoza N, Das AK (2019) A blockchain framework for ensuring data quality in multi-organizational clinical trials. IEEE, Piscataway. https://ieeexplore.ieee.org/document/8904634
41. Benchoufi M, Altman DG, Ravaud P (2019) From clinical trials to highly trustable clinical trials: blockchain in clinical trials, a game changer for improving transparency? Front Blockchain 2(23). https://doi.org/10.3389/fbloc.2019.00023
42. Sato T, Himura Y (2018) Smart-contract based system operations for permissioned blockchain. Curran Associates, Inc. https://ieeexplore.ieee.org/document/8328745
43. ConsenSys (2020) Enterprise Ethereum: 5 reasons why Enterprise Ethereum is so much more than a distributed ledger technology. ConsenSys. https://consensys.net/enterprise-ethereum/best-blockchain-for-business/5-reasons-why-enterprise-ethereum-is-so-much-more-than-a-distributed-ledger-technology/. Accessed 31 July 2020
44. Joshi P, Gokhale P (2021) Electronic health record using blockchain and off chain storage: a systematic review. IT Ind 9(1):247–253. http://www.it-in-industry.org/index.php/itii/article/view/125
45. Zhang P, Schmidt DC, White J, Lenz G (2018) Blockchain technology use cases in healthcare. In: Raj P, Deka GC (eds) Advances in computers Blockchain technology: platforms, tools and use cases, vol 111. Academic Press, Cambridge, pp 1–41. https://doi.org/10.1016/bs.adcom.2018.03.006
46. Sun J, Yao X, Wang S, Wu Y (2020) Blockchain-based secure storage and access scheme for electronic medical records in IPFS. IEEE Access 8:59389–59401. https://doi.org/10.1109/access.2020.2982964

47. Košťál K, Helebrandt P, Belluš M, Ries M, Kotuliak I (2019) Management and monitoring of IoT devices using blockchain (dagger). Sensors (Basel) 19(4):856. https://doi.org/10.3390/s19040856
48. Pennec F (2018, February 23) Healthcare blockchain startup BurstIQ secures $5M investment. HIT Consultant Media. https://hitconsultant.net/2018/02/23/healthcare-blockchain-startup-burstiq-secures-5m/. Accessed 26 July 2020
49. Srivastava G, Parizi RM, Dehghantanha A, Choo K-KR (2019) Data sharing and privacy for patient IoT devices using blockchain. Springer, Berlin. https://doi.org/10.1007/978-981-15-1301-5_27
50. Chamber of digital commerce (2018) "Smart contracts" legal primer. https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-Legal-Primer-02.01.2018.pdf
51. McKinney SA, Landy R, Wilka R (2018) Smart contracts, blockchain, and the next frontier of transactional law. Wash J Law Technol Arts 13(3):313–347. http://hdl.handle.net/1773.1/1818
52. Beckstrom K (2019) Utilizing blockchain to improve clinical trials. In: Metcalf D, Bass J, Hooper M, Cahana A, Dhillon V (eds) Blockchain in healthcare: innovations that empower patients, connect professionals and improve care. CRC Press, Taylor & Francis Group, pp 109–121. https://www.routledge.com/Blockchain-in-Healthcare-Innovations-that-Empower-Patients-Connect-Professionals/Dhillon-Bass-Hooper-Metcalf-Cahana/p/book/9780367031084
53. The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (1979) The Belmont report: ethical principles and guidelines for the protection of human subjects of research. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/
54. Benchoufi M, Porcher R, Ravaud P (2018) Blockchain protocols in clinical trials: transparency and traceability of consent. F1000Res 6. https://doi.org/10.12688/f1000research.10531.5
55. Albanese G, Calbimonte J-P, Schumacher M, Calvaresi D (2020) Dynamic consent management for clinical trials via private blockchain technology. J Ambient Intell HumanIz Comput. https://doi.org/10.1007/s12652-020-01761-1
56. U.S. Food and Drug Administration (2018, December 7) Data integrity and compliance with drug CGMP: questions and answers guidance for industry. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/data-integrity-and-compliance-drug-cgmp-questions-and-answers-guidance-industry. Accessed 19 Jun 2021
57. Benchoufi M, Ravaud P (2017) Blockchain technology for improving clinical research quality. Trials 18:335. https://doi.org/10.1186/s13063-017-2035-z
58. National Institutes of Health (2003) Final NIH statement on sharing research data. https://grants.nih.gov/grants/guide/notice-files/NOT-OD-03-032.html
59. Sivagnanam S, Nandigam V, Lin K (2019) Introducing the open science chain. Association for Computing Machinery, New York. https://doi.org/10.1145/3332186.3332203
60. Glicksberg BS, Burns S, Currie R, Griffin A, Wang ZJ, Haussler D, Goldstein T, Collisson E (2020) Blockchain-authenticated sharing of genomic and clinical outcomes data of patients with cancer: a prospective cohort study. J Med Internet Res 22(3):e16810. https://doi.org/10.2196/16810
61. Kumari M, Gupta M, Ved C (2021) Blockchain in Pharmaceutical Sector. In: Namasudra S, Deka GC (eds) Applications of blockchain in healthcare, vol 83. Springer Nature, Berlin, pp 199–220. https://doi.org/10.1007/978-981-15-9547-9_8
62. Charles WM, Marler N, Long L, Manion ST (2019) Blockchain compliance by design: regulatory considerations for blockchain in clinical research. Front Blockchain 2(18). https://doi.org/10.3389/fbloc.2019.00018
63. Angeletti F, Chatzigiannakis I, Vitaletti A (2017a) Privacy preserving data management in recruiting participants for digital clinical trials. ACM, New York. https://dl.acm.org/citation.cfm?id=3144733
64. Singh SK, Rathore S, Park JH (2020) Block IoT intelligence: a blockchain-enabled intelligent IoT architecture with artificial intelligence. Futur Gener Comput Syst 110:721–743. https://doi.org/10.1016/j.future.2019.09.002

65. Tomaz AEB, Nascimento JCD, Hafid AS, De Souza JN (2020) Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain. IEEE Access 8:204441–204458. https://doi.org/10.1109/ACCESS.2020.3036811
66. Jayasinghe U, Lee GM, MacDermott Á, Rhee WS (2019) TrustChain: a privacy preserving blockchain with edge computing. Wirel Commun Mob Comput 2019:2014697. https://doi.org/10.1155/2019/2014697
67. Zhou L, Wang L, Ai T, Sun Y (2018) BeeKeeper 2.0: confidential blockchain-enabled IoT system with fully homomorphic computation. Sensors (Basel) 18(11):3785. https://doi.org/10.3390/s18113785
68. McCook A (2016) Duke fraud case highlights financial risks for universities. Science 353(6303):977–978. https://doi.org/10.1126/science.353.6303.977
69. U.S. Department of Health and Human Services (2019) Findings of research misconduct. Fed Regist 84(219):60097–60098. https://ori.hhs.gov/sites/default/files/2019-11/2019-24291.pdf
70. Office of Public Affairs (2019) Duke University agrees to pay U.S. $112.5 million to settle false claims act allegations related to scientific research misconduct. U.S. Department of Justice. https://www.justice.gov/opa/pr/duke-university-agrees-pay-us-1125-million-settle-false-claims-act-allegations-related. Accessed 23 Aug 2021
71. Burki TK (2019) Pharma blockchains AI for drug development. Lancet 393(10189):2382. https://doi.org/10.1016/S0140-6736(19)31401-1
72. Warr WA (2021) National Institutes of Health (NIH) workshop on reaction informatics. https://chemrxiv.org/engage/api-gateway/chemrxiv/assets/orp/resource/item/611cf1a6ac8b499b36458d19/original/national-institutes-of-health-nih-workshop-on-reaction-informatics.pdf
73. Wang J, Wang S, Guo J, Du Y, Cheng S, Li X (2019) A summary of research on blockchain in the field of intellectual property. Elsevier, Amsterdam. http://www.sciencedirect.com/science/article/pii/S187705091930239X
74. Dasgupta D, Shrein JM, Gupta KD (2019) A survey of blockchain from security perspective. J Bank Financ Technol 3:1–17. https://doi.org/10.1007/s42786-018-00002-6
75. Banga R, Juneja M (2018) Clinical trials on blockchain. PhUSE, Broadstairs. https://www.lexjansen.com/phuse/2018/tt/TT11.pdf
76. Wang Y, Li J, Yan Y, Chen X, Yu F, Zhao S, Yu T, Feng K (2021) A semi-centralized blockchain system with multi-chain for auditing communications of wide area protection system. PLoS ONE 16(1):e0245560. https://doi.org/10.1371/journal.pone.0245560
77. Hirano T, Motohashi T, Okumura K, Takajo K, Kuroki T, Ichikawa D, Matsuoka Y, Ochi E, Ueno T (2020) Data validation and verification using blockchain in a clinical trial for breast cancer. J Med Internet Res 22(6):e18938. https://doi.org/10.2196/18938
78. Learney R (2019) Blockchain in clinical trials. In: Metcalf D, Bass J, Hooper M, Cahana A, Dhillon V (eds) Blockchain in healthcare: innovations that empower patients, connect professionals and improve care. CRC Press, Taylor & Francis Group, pp 87–108. https://www.routledge.com/Blockchain-in-Healthcare-Innovations-that-Empower-Patients-Connect-Professionals/Dhillon-Bass-Hooper-Metcalf-Cahana/p/book/9780367031084
79. Eklund PW, Beck R (2019) Factors that impact blockchain scalability. Association for Computing Machinery, New York. https://doi.org/10.1145/3297662.3365818
80. Rathore H, Mohamed A, Guizani M (2020) A survey of blockchain enabled cyber-physical systems. Sensors (Basel) 20(1):282. https://doi.org/10.3390/s20010282
81. Burchert C, Decker C, Wattenhofer R (2018) Scalable funding of bitcoin micropayment channel networks. R Soc Open Sci 5(8):180089. https://doi.org/10.1098/rsos.180089
82. Lee H-A, Kung H-H, Udayasankaran JG, Kijsanayotin B, Marcelo AB, Chao LR, Hsu C-Y (2020) An architecture and management platform for blockchain-based personal health record exchange: development and usability study. J Med Internet Res 22(6):e16748. https://doi.org/10.2196/16748
83. Ricotta F, Jackson B, Henry T (2019) Secure adaptive data storage platform. United States Patent No. US 2019/0012466 A1. https://patentimages.storage.googleapis.com/74/97/75/8d9604b1b85a5d/US20190012466A1.pdf

84. Merena S, Thangadurai E, Shankar M (2021) Electronic health care record using blockchain technology. Int J Eng Res Appl 11(1):10–13. https://doi.org/10.9790/9622-1101031013
85. Gorenflo C, Lee S, Golab L, Keshav S (2020) FastFabric: scaling hyperledger fabric to 20 000 transactions per second. Int J Network Manage 30(5):e2099. https://doi.org/10.1002/nem.2099
86. Nakaike T, Zhang Q, Ueda Y, Inagaki T, Ohara M (2020) Hyperledger fabric performance characterization and optimization using GoLevelDB benchmark. IEEE, Piscataway. https://ieeexplore.ieee.org/document/9169454
87. Meyyan P (2018, January 16) Decrypting the utility of blockchain in clinical data management. VertMarkets. https://www.clinicalleader.com/doc/decrypting-the-utility-of-blockchain-in-clinical-data-management-0001. Accessed 23 Oct 2018
88. Alharby M, Aldweesh A, van Moorsel A (2018) Blockchain-based smart contracts: a systematic mapping study of academic research. IEEE, Piscataway. https://ieeexplore.ieee.org/document/8756390

Dr. Wendy Charles has been involved in clinical trials from every perspective for 30 years, with a strong background in operations and regulatory compliance. She currently serves as Chief Scientific Officer for BurstIQ, a healthcare information technology company specializing in blockchain and AI. She is also a lecturer faculty member in the Health Administration program at the University of Colorado, Denver. Dr. Charles augments her blockchain healthcare experience by serving on the EU Blockchain Observatory and Forum Expert Panel, HIMSS Blockchain Task Force, Government Blockchain Association healthcare group, and IEEE Blockchain working groups. She is also involved as an assistant editor and reviewer for academic journals. Dr. Charles obtained her PhD in Clinical Science with a specialty in Health Information Technology from the University of Colorado, Anschutz Medical Campus. She is certified as an IRB Professional, Clinical Research Professional, and Blockchain Professional.