BLOCKCHAIN™ IN HEALTHCARE TODAY

NARRATIVE/SYSTEMATIC REVIEWS/META-ANALYSIS

HEALTH DATASETS AS ASSETS: BLOCKCHAIN-BASED VALUATION AND TRANSACTION METHODS

Wendy M. Charles* and Brooke M. Delgado

BurstIQ, Inc., Denver, CO, USA

Abstract

There is increasing recognition about health-oriented datasets that could be regarded as intangible assets: distinct assets with future economic benefits but without physical properties. While health-oriented datasets – particularly health records – are ascribed monetary value on the black market, there are few established methods for assessing the value for legitimate research and business purposes. The emergence of blockchain has created new commercial opportunities for transferring assets without intermediaries. Therefore, blockchain is proposed as a medium by which research datasets could be transacted to provide future value. For authorized individuals to verify their transactions, blockchain methodologies offer security, auditability, and transparency. The authors share data valuation methodologies consistent with accounting principles and include discussions of black market valuation of health data. Furthermore, this article describes blockchain-based methods of managing real-time payment/micropayment strategies.

Keywords: *Blockchain*; *data valuation*; *intangible assets*; *data sales*; *health records*

Received: 10 November 2021; Revised: 19 December 2021; Accepted: 21 December 2021; Published: 21 January 2022

Individually identifiable information is collected about patients in nearly every health and wellness-oriented app, wearable device, and healthcare setting (1). This information is used to identify treatment opportunities within the healthcare facilities where the patients are treated. However, data are also regularly shared and sold to other technology or life sciences organizations to design innovations in health care, identify new healthcare markets, create business opportunities, and uncover revenue collection opportunities (2).

Life sciences research organizations have a tremendous need to acquire health information from real-world sources, referred to as 'real-world data', as part of a United States (US) Food and Drug Administration (FDA) Real-World Evidence Framework initiative (3). With careful planning, the FDA notes that 'a non-interventional study has the potential to meet FDA's regulatory standards for an adequate and well-controlled clinical study' (4). Among sources of real-world data, life sciences organizations seek information on the effectiveness of pharmaceutical compounds when used in typical care conditions – rather than the stringent environment of a clinical research setting – to learn how physicians are utilizing these drugs and which patient groups may experience unexpected benefits or adverse events (5). As a recent example, the drug Blincyto (blinatumomab) received accelerated FDA approval to treat acute lymphoblastic leukemia using a single-arm trial. The experimental group was compared with a historical control group using electronic health records from 694 patients in the European Union and US (6). Electronic health records also created the control group for a new FDA-approved indication for Prograf (tacrolimus) to help prevent organ rejection (7). Overall, acquiring and using existing health information allow research organizations to achieve faster, lower cost research that demonstrates treatment effectiveness within real-world care conditions. Therefore, there is a tremendous need to acquire health information.

Many organizations have uncertainty regarding the best technologies to manage health information exchange and monetization securely. While some companies utilize traditional database technologies, blockchain technologies have emerged to allow for more capabilities. X. Wang et al. (8) pointed out that blockchain is already used to exchange contracts, capital, and digital assets, so that this technology would inevitably be used to exchange data. In addition, buying and selling assets previously required an intermediary, such as a financial institution

*Correspondence: Wendy M. Charles. Email: wendy.charles@cuanschutz.edu

or marketplace. However, blockchain technologies can simplify the data transaction process by allowing organizations to transfer assets without intermediaries (9). The transfer is completed, validated, and recorded on the blockchain in near-real-time (10).

Nature of health information

While health information can be collected from many places, such as patient wellness apps, patient repositories, and research studies, most health information used for sharing and sale originates from organizations that deliver or support health care (1). In the US, these organizations are referred to as covered entities, involving '1) a health plan, 2) a healthcare clearinghouse or 3) a healthcare provider, who transmits any health information in electronic form in connection with a transaction' (45 CFR 160.103).

The nature of health information that can be shared and sold depends on the degree to which information is considered to constitute 'protected health information' and whether the issuing organization is a covered entity. While each country imposes privacy regulations to protect health information, a review of privacy requirements is outside the scope of this article. Therefore, this section addressed only the health information privacy requirements of the US The Health Insurance Portability and Accountability Act (HIPAA) defines protected health information as individually identifiable health information transmitted or maintained in any other form or medium (45 CFR 160.103), and a covered entity.

Authorized methods of distributing protected health information include:

1 **Unidentified information**. A covered entity can use and share unidentified health information without restriction when the healthcare organization first removes all 18 components that could identify an individual (45 CFR 164.514(a)). It is also permissible for a statistician to determine there is a minimal risk that the intended recipient could use the information – alone or in combination with other reasonably available information – to identify individuals included in the dataset (45 CFR 164.514(b)).

2 **Limited data set**. A covered entity may disclose a dataset that removes direct identifiers of the individual (or of relatives, employers, or household members of the individual) and enters into a data use agreement with the recipient (45 CFR 164.514(e)). A limited dataset may include elements of dates related to an individual and geographic identifiers, such as town/city and zip code, provided that this information – either alone or in combination with other information – is unlikely to identify the individuals represented in the dataset (45 CFR 164.514(e)).

3 **Identifiable data set**. A covered entity must obtain authorization for any disclosure of protected health information that is a sale of health information as defined in 45 CFR 164.501 and 45 CFR 164.508(a)(4). Specifically, covered entities may 'not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list' (11).

The HIPAA regulations do not apply to information generated or provided by a patient or healthcare consumer who is not maintained by a covered entity.

Nature of health data acquisition

There are several methods by which organizations can obtain health information.

Direct sales from patients

Several startups have been formed to compensate patients for sharing their health information. For example, EncrypGen enables individuals to upload their DNA profiles to a marketplace and set a price to sell their profiles (12).

Healthcare organization purchases

Pharmaceutical company Roche AG purchased Flatiron Health, acquiring 260 community cancer clinics to obtain cancer treatment information to support regulatory decisions (13). Roche's purchase price of $1.9B averages $1,000 per medical record for 2 million oncology patients (14).

Business associate agreements

A covered entity may share health information with a member of its workforce or a business associate for providing professional services, provided that the covered entity represents that the health information includes the minimal necessity to achieve the stated purpose (45 CFR 514(d)(iii)). For example, Ascension Health and the Mayo Clinic distribute health information to Google under Business Association Agreements to design artificial intelligence algorithms to identify opportunities for treatment and revenue (15, 16).

Academic or government data warehouses

More than 10,000 unidentified health-related datasets are publically available on Data.gov (https://www.data.gov/). PubMed (https://pubmed.ncbi.nlm.nih.gov/) allows authors to upload their health datasets with their publications (2). In addition, some universities offer publicly accessible data warehouses for researchers to query and download unidentified data. As of October 2021, the University of Michigan's Inter-university Consortium for Political and Social Research program offers datasets from over 16,000 studies represented in nearly 100,000 publications (https://www.icpsr.umich.edu/web/pages/ICPSR/).

Citation: Blockchain in Healthcare Today 2022, **5**: 185 - http://dx.doi.org/10.30953/bhty.v5.185

Data marketplaces

Data sellers have created a $100B market with companies buying, selling, and trading unidentified information (14). In fact, 14 US health systems started a new company, Truveta, to aggregate and sell their unidentified patient data (17).

This article focuses on data marketplaces and blockchain-based technologies' role in managing pricing, access, and monetization.

Financial value of health information

The data allow decision-makers to make calculated, insightful, and profitable decisions, adding value to data mining alone (18). Health information derived from electronic health record systems creates value for life sciences research because of the complex demographics, health history, and other health-oriented behaviors. Because life sciences organizations seek data to develop new revenue-generating opportunities, they are willing to pay for this health information – ascribing value to the data. This section explores factors for determining data value.

Health datasets as assets

Because a dataset provides value and offers potential financial benefits, a dataset could be considered an asset (19, 20). According to the Financial Accounting Standards Board (21), recognized by the US Securities and Exchange Commission, an asset has three characteristics:

1. A probable future benefit that contributes to net cash inflows
2. An entity obtains and controls others access to it
3 The transaction to control or benefit from the asset has already taken place (22).

Data are classified as intangible assets when they have no physical properties. As shown in Fig. 1, examples of intangible assets include patents, trademarks, copyright, and intellectual property (23). Intangible assets are generally not accounted for on an organization's balance sheet (24) but add to the organization's value in the marketplace. Similar to most intangible assets, the potential data value is challenging to measure (8).

Data valuation

Data value is determined by various factors such as data complexity, number of records in the dataset, number of variables, and quality of the data (25). Furthermore, unidentified health records are less valuable because researchers need dates and geocodes to contextualize disease progression and comorbidities (26). In addition, data valuation is influenced by data perishability, which involves devaluation over time, and time dependency, a measure of the time since data collection (27). The use of blockchain also offers features that may increase data value (28).

Organizations use both subjective and objective methods to determine the dataset value. The following strategies are not comprehensive but describe the most common methods used to value intangible assets: the cost, income, and market approaches.

Cost approach

With a cost approach, datasets are valued based on the estimated historical costs to create the dataset (29) or the anticipated costs incurred to replace the dataset (30). This approach is aligned with the HIPAA requirement to limit data sales for research to cost-based fees to cover the cost of preparing health information (45 CFR 164.502(a)(5)(3)(ii)). When using historical cost as the basis, organizations should consider likely inflation and other infrastructure costs necessary for replacing the dataset (31). Organizations may benefit

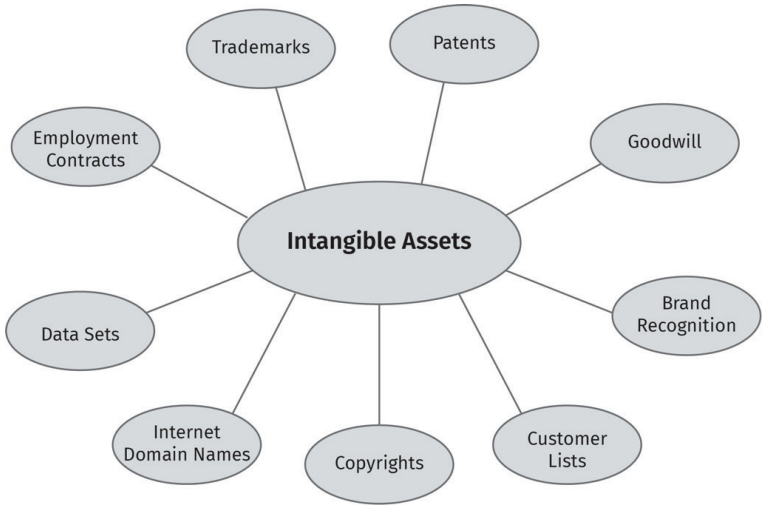

Fig. 1. Representative types of intangible assets.

from blockchain-based transparency in price histories and formulas (32).

The use of blockchain technology for preparing or replacing the data could potentially increase or decrease the replacement costs. Data valuation could increase when the technologies are novel and there is no competition with the methodology (26). However, blockchain technology also introduces data redundancies and audit trails to significantly reduce replacement costs (33). Future valuations using the cost approach should consider emerging economic and technological developments.

Income approach

The income approach considered the estimated increased revenue generated by the dataset (31). For example, suppose a pharmaceutical company acquires health datasets as real-world evidence that could support a regulatory decision for a new indication. In this case, the datasets could be valued with the projected new drug revenue stream. Blockchain-based data exchanges facilitate data sharing about data uses and related metadata that can be used to determine trends and future needs (32). However, future revenue forecasts are also influenced by market share and adoption rates, requiring several assumptions that could change (29).

Market approach

The market approach appraises data based on the price of comparable data traded or sold. Pricing may be set by guidelines posted within the marketplaces or by analyzing similar sales data (34). Blockchain-based audit trails are currently used to track the history of data values (35), allowing for more convenient access to historical sales information.

Similarly, the market may bear higher values for datasets involving more records, identifiable data, and quality (29). Zozus and Bonner (35) notes that blockchain-based metadata have been used to facilitate evaluations of data quality and other attributes that may influence valuation. These authors describe how data value-level metadata are used to calculate data age and potential discrepancies. Accordingly, blockchain-based data provenance and integrity may increase perceptions of data value (28), resulting in higher market-driven pricing.

The market approach can also be used to consider supply and demand. Specifically, data buyers consider the availability of other datasets within the market to determine the relative value of any particular dataset (9). Concepts of supply and demand drive pricing of illegal data sales on the black market or dark web (36). Stack (36) notes that social security numbers sell for around $1 on the dark web, and credit cards sell for $5–110 [with the median ranging from $25 to 40, (37)]. Medical records sell for $1–1,000, depending on information completeness (38, 39). Specifically, electronic health records are more valuable for illicit sales when they include e-commerce transactions and credit card information (40). Data are typically sold using blockchain technology on the dark web in exchange for cryptocurrency – and data are held for ransom requesting cryptocurrency – because of the pseudonymous nature of transactions (40).

These data valuation methods can only provide estimates, and organizations are encouraged to use multiple data valuation approaches (29). Birch et al. (41) encouraged organizations to use advanced technological solutions for these approaches because data access can be tracked and measured more efficiently. As described in the following section, blockchain-based systems are often used to track and record user engagement with datasets, allowing for better value measurements. However, because data values are in constant flux, data valuations should be reviewed and recorded at least annually to ensure accuracy (29).

Health data marketplaces

Marketplaces provide digital platforms for buyers and sellers to exchange data. As shown in Fig. 2, the volume of data bought and sold on data marketplaces – of all types – is expected to increase 25% from 2020 to 2022 (42).

Types of blockchain-based marketplaces

There are three primary characteristics of blockchain-based marketplaces: private, consortium, and independent data marketplaces. Platform architecture is either

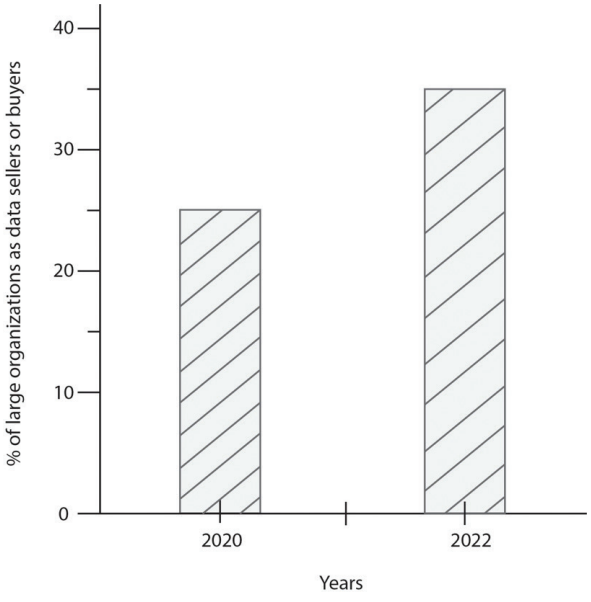

Fig. 2. Percentage of large organizations as sellers or buyers of data via online data marketplaces.

Citation: Blockchain in Healthcare Today 2022, **5**: 185 - http://dx.doi.org/10.30953/bhty.v5.185

centralized or decentralized (43). In this section, the benefits and drawbacks of each characteristic are described.

Private marketplaces are controlled by a single vendor or organization that controls access and governance (44). A private marketplace owner can use the marketplace to its advantage – such as having access and insight to all data exchanges, and the owner can both sell data and charge subscription fees (34). However, private marketplaces can introduce bias on the platform (44), and the platform operator is responsible for protecting the data and ensuring that all data privacy laws are met (23).

Consortium marketplaces have a group of owners who cooperate to support platform operations and decision-making (44). Consortia benefit from sharing costs and resources to maintain the reliability of the network (45). These organizations often utilize pooled data to create larger health datasets and collaborate on research. A drawback pertains to the trust required of the other collaborators to protect and manage data appropriately (46), as well as questions about ownership (23).

Independent health marketplaces allow individual patients/consumers to provide and sell their own data on a platform, where the buyers, sellers, and marketplaces are independent entities (44). Each entity has independent control – and often independent monetization – over their data and how data are used. As a downside, it is difficult to gain enough market size to individually source and sell data without the buying power of a consortium or large private organization (44).

Centralized versus decentralized architecture

The infrastructure and architecture of a platform refer to locations of data storage, access, and technical governance. A centralized blockchain marketplace collects and stores data where a single (or few) organization(s) provide access controls, regular maintenance, and oversight (47). As an example for health data, centralized marketplaces can negotiate health data purchases directly from healthcare organizations and payers, as well as negotiate large-scale sales to life sciences organizations. Centralized marketplaces can offer additional layers of encryption and smart contracts (47). However, there are potential vulnerabilities for hacking and less operational transparency (48).

A benefit to a decentralized marketplace is quality (47). As data are secured by smart contracts and accessed directly from the data provider, higher quality can be assumed. A drawback of decentralized marketplaces is that it creates more difficult transactions (49). Each transaction must be facilitated through a distributed ledger. An example of a decentralized marketplace is where unidentified data are aggregated using software, but data never leave the source location, and each organization cannot access data from others.

A decentralized location allows the data to stay with the data provider (47). Blockchain-based data exchange platforms exist today as decentralized ecosystems that enable individuals or organizations to source and share data (47). Rather than centralized management where there are potential points of vulnerability (48), blockchain-based data exchanges allow for distributed data stewardship and communication (50).

Blockchain technologies offer data management methods for sales and transactions in ways that traditional databases typically cannot provide. Among examples, blockchain can support transaction visibility to ensure that the data exchange and payment process are fair and consistent with payment terms (51). Furthermore, because malicious data buyers or sellers may refuse to pay for data (48), smart contracts automate payments and revenue distributions (52). This capability also ensures efficiencies for data exchanges and resource allocations (53). Furthermore, smart contracts ensure that only authorized individuals can contribute or access specific data in a very granular manner (54).

Examples of blockchain-based health data marketplaces

Blockchain not only offers a new technology to manage data sharing and tracking but also facilitates new economic models. Considering that blockchain first received wide recognition for the transparent exchange of cryptocurrency, the same reasoning is applied to the exchange of other assets. As noted by Lee (55), blockchain-based marketplaces offer trusted data while transparently tracking both transactions and payments.

While many blockchain-based data sales and exchange platforms are still early in development, several have achieved stable platforms and market awareness. Several companies also attempt to utilize blockchain-based decentralization with incentive schemes to reward both providers and patients for participation.

Three primary players are involved in blockchain-based data marketplaces: providers, buyers, and digital platform owners (47). Providers list their data in exchange for monetary value, buyers purchase data to add value to their organizations, and marketplace owners/controllers provide a place where data can be stored and sold (47). While open data marketplaces are available to download/exchange data at no charge (47), the authors focus on profit-generating marketplaces. Profit-generating data marketplace participation varies from business-to-business (B2B), consumer-to-consumer (C2C), business-to-consumer (B2C), business-to-business-to-consumer (B2B2C), and business-to-consumer-to-business (B2C2B) (56). The following companies offer blockchain-based data marketplaces for data exchange or monetization of health information. This list is intended to be representative but not necessarily comprehensive.

BurstIQ, Inc. (https://www.burstiq.com/): Colorado-based B2B2C technology company, BurstIQ, promotes itself as the first blockchain-based data management platform to process large volumes of health information on chain while meeting health information and regulatory privacy requirements (57). The on-chain capabilities allow organizations to connect patients' longitudinal, multidimensional health profiles, called LifeGraphs®, using artificial intelligence and machine learning (58). BurstIQ also developed health marketplaces where patients could loan, sell, and license their health information based on automated matchmaking. BurstIQ expanded the collaboration space for research and development, now called 'The Foundry', to share data and leverage crowd intelligence (59). The use of blockchain provides data governance, granular consent capabilities, data provenance, and data security.

Ciitizen, located in Palo Alto, California (https://www.ciitizen.com) and recently acquired by Invitae (60), is designed as a B2C2B personal health record platform where patients can aggregate health information from all healthcare providers and share information for research. While the website does not specify the use of blockchain, Ciitizen's blockchain technologies have been listed among blockchain-based health platforms (e.g. 61). The platform is free for patients; however, researchers pay a fee to access health records when patients agree to share their health information for research. Of particular note, Citizen shares these fees with the individuals who agree to provide their health information for research (62). Among the Research FAQs, the website specifies, 'Should a patient's information be included in a study, Ciitizen is committed to returning a portion of the value gained from this study with users to the extent permitted by law (e.g. in the form of direct payment, services, discounts, donations, or other value) or to donate this value to an advocacy or research non-profit as directed by the patient' (62).

Operating in France and Russia, Datapace.io offers a B2C2B blockchain-based data marketplace for IoT sensor data (https://datapace.io/) but can be used to buy or sell any data (63). The marketplace uses Hyperledger Fabric to build the platform and modules using a high-performance practical Byzantine Fault Tolerance consensus mechanism. Individuals receive tokens native to the platform for contributing data and managing the Proof-of-Stake consensus mechanism (63).

Datum platform (https://datum.org) was founded in 2017 and is headquartered in Zug, Switzerland. The B2C2B Datum network allows anyone (outside the US, China, or South Korea) to own and manage his or her data using the DigiArt Token (DAT) smart token for buying and selling data (64). While data agnostic, the Datum network founders specify that the blockchain platform is intended for buying and selling individuals' health information for research. The platform is compared with a decentralized version of the Apple HealthKit that respects data owners' terms and conditions for data usage (64). The Datum network enhances data research capabilities by capturing and linking data from IoT devices, specifying that the network could capture information from digital health devices and provide research data to scientific or medical institutions (64).

Founded in 2015, Dawex (https://www.dawex.com) markets itself as an advanced blockchain-based B2B data-exchange environment where organizations can share and commercialize data. The company notes that the blockchain platform provides data transaction security and traceability (65). As of 2020, Fernandez et al. (66) commented that Dawex created a successful sharing platform but had yet to determine how to address data integration and pricing. Specifically, buyers were required to offer a price without being permitted to evaluate the value of the dataset (66).

Embleema (https://www.embleema.com/), based in Metuchen, NJ, is designed to collect electronic health records and share them as real-world data for research. Embleema uses a private HIPAA- and General Data Protection Regulation (GDPR)- compliant blockchain to manage granular patient consent and securely store patient information (67). The B2C2B blockchain is also designed for transparency of recruitment opportunities, study progress, and results. Patient participants log in with blockchain-based public and private key pairs instead of user names and passwords (68). When individuals share their health information or participate in virtual studies such as surveys, participants receive points that can be exchanged for unspecified 'rewards' (69). However, the Patient Advocacy page specifies that users receive compensation for using their data (68).

EncrypGen (https://encrypgen.com/), located in Miami, FL, is a B2C2B blockchain-based DNA marketplace that allows individuals to provide their Genome in return for '$DNA', a utility token that can be used to buy and sell DNA profiles. The EncrypGen platform facilitates storing, sharing, searching, buying, and selling user-provided profiles (70). The blockchain 'gene-chain' backbone is used to manage the privacy and security of genetic data as well as facilitate the data-exchange process. EncrypGen makes data available to third parties, such as research scientists, willing to pay for genetic information (50).

Enigma (https://www.enigma.co), a San Francisco and Tel Aviv-based B2B and B2C2B company, offers an open-source blockchain protocol for data sharing. The main-net blockchain, the Secret Network, allows decentralized applications to perform computations on encrypted data. Because of the persistent encryption, the data remain private to the nodes – even on a public blockchain (71). Enigma is designed to be blockchain agnostic and data agnostic, but the company promotes

Citation: Blockchain in Healthcare Today 2022, **5**: 185 - http://dx.doi.org/10.30953/bhty.v5.185

its ability to facilitate research on health information. Further, the platform offers a data marketplace that allows data monetization (71).

Hu-manity.co (https://hu-manity.co/) was founded in 2018 and is based in Sparta, NJ. In this B2C2B platform, individuals can upload all, part, or none of their healthcare records to the data marketplace and specify how their healthcare data can be accessed and used (72). Hu-manity.co allows patients to specify how their health information could be used with the prospect that pharmaceutical companies would pay each user for access to their data (73). Of interest, the company allows individuals to 'claim title' to their data and recognize their health information as 'personal property' (72). The IBM blockchain is used to allow granular consent of data and securely track the uses of data. The website notes that the company has not yet received a critical mass of people using the app, but once enough data are available, data participants will receive utility tokens – the 'Hu' token – that could be exchanged for internal offers and incentives with the plan for offering fiat currency in the future (72).

LunaDNA (https://www.lunadna.com/), a San Diego-based B2C2B company, was formed in 2017 as a member-owned platform to help individuals manage the scientific and monetary value of their DNA. Individuals are encouraged to upload genetic files with the option of completing additional surveys and adding electronic health records to receive shares in the company (74). A portion of LunaDNA's proceeds from research is shared with members as (fiat) dividends per the company's filing with the US Securities and Exchange Commission (74).

In May 2021, the Finnish company Nokia launched a B2B blockchain-based data marketplace for sharing and monetizing data (https://www.nokia.com/networks/services/nokia-data-marketplace/). While this data marketplace is not designed exclusively for health data, Nokia specified that health data are a use case for federated learning and monetization within its marketplace (75). Nokia specifies that a private, permissioned blockchain creates trusted and secure data transactions with transaction automation and federated intelligence (75). The nature of monetization to users (i.e. fiat currency or cryptocurrency) is not specified.

PhrOS (https://phros.io/services/health_data_market) was founded in 2016 in Taipei, Taiwan as a B2C2B data-exchange network with a dedicated health data market. Patients can sign consent to share healthcare data with the network to be used for research. Patients and researchers exchange 'health points' for health-related data (76). A blockchain is used to manage the fine-grained consent options to use patients' health information, create a token-based exchange network, and offer wallet services to control users' keys and tokens (76). The website specifies that it can automatically gather and update participants' health record data and push alerts to healthcare providers or hospitals if patients need immediate care.

Data tokenization

Blockchain technologies have spawned innovation for sophisticated methods for managing data. Because cryptocurrency is a digital asset represented on blockchains, the same approach has been applied to representing physical and digital assets for proof of ownership (77). Referred to as 'tokenization', classes of blockchain-based tokens are divided into two categories of fungible tokens and non-fungible tokens (NFTs). Fungible tokens are designed to be divided into fractions where each fraction is equal to others in value, allowing them to be interchangeable (78). In contrast, NFTs are unique assets that cannot be divided and are not interchangeable, such as a photo or physical object (78). The tokenization of digital assets has created new investment opportunities and new methods of establishing asset ownership (77).

Health records are also now being classified as NFTs as unique assets with the original value (79). Hapiffah et al. (80) created a proof of concept for a medical record system where patients' medical record data are registered as NFTs to establish proof of evidence and ownership. Sandner et al. (79) recognized that datasets can be classified as NFTs for blockchain-based token exchanges where a dataset's value is identified with the value of the NFT. The blockchain also then provides transparency and auditability to ensure honest data transactions (79).

Considerations

Complications impacting data valuation and sale can be economical, social, or ethical. If blockchain organizations wish to engage in data valuation and sale, these values drive considerations of monetization and privacy (1).

Patient monetization

While healthcare or life sciences organizations may benefit from the sale and use of patients' health information, will any of that money be given to the patients represented in the datasets? Klugman (81) argues that 'it is only "just" that [patients] benefit from the sale' (approx. p. 2). He adds that if the healthcare organizations are acting in the best interests of patients, then they should share data profit with the patients. Tlacuilo Fuentes (82) notes that patients regularly receive benefits from retail organizations in exchange for using their data, such as discounts or free uses apps/services. Klugman (81) adds that it is well within a healthcare organization's authority to offer additional services or reductions to copays and deductibles when healthcare organizations profit from patient health information.

While it is an admirable goal to provide compensation to patients who knowingly or unknowingly provide their

information in a data marketplace, the marketplaces must determine methods of allocating compensation to these individuals. There are various reward programs granted for the use of data; however, this section focuses exclusively on sharing payments for individuals represented in health datasets purchased and used for research.

Query pricing

Data are often accessed during queries where researchers may simply be attempting to determine study feasibility or compare and contrast datasets (51). In this case, the researcher needs to access an individual's data to determine whether the data are sufficient without committing to a dataset. Should individuals be compensated when datasets are merely sampled?

Research and development pricing

Biocuration may only be a tiny part of research and development where a profitable product may not result for many years, if at all (83). Many research studies do not have initial funding – much the less profit (26). How should the original data subjects be recognized if a patient provides an early and relatively insignificant contribution to a later project?

Horizontal value split

This challenge reflects the many parties that contribute to the healthcare data chain (51). Parties involve the healthcare provider who enters the data, the healthcare organization that stores and maintains the electronic health record system or data warehouse, the data broker, or even the data marketplace. Because each party provides data or infrastructure to support data, how should values be divided among these parties?

Vertical value split

This challenge describes dividing the value among the individual patients represented in a dataset where the data of different people contribute to the dataset (51). Should patients with more healthcare visits, therefore contributing more data, be compensated more than those with fewer healthcare visits? Or should patients with higher health data quality receive more compensation than those with less quality?

Cost sharing split

As there are many costs for storing and curating data, should the profits be distributed in the same proportion as the costs (26)? Should the costs for resources and capital investments first be declared and quantified before determining how best to distribute the profits? A form of cost-sharing split is to grant free services in exchange for selling the data. For example, PicnicHealth provides a free personal health record app to patients/consumers if these individuals allow their health information to be sold for future research (84). Otherwise, patients/consumers must pay $299 for processing the past medical records and $39 per month.

When individuals receive monetization for participating in a data marketplace, it is also necessary to consider the financial ramifications of withdrawal. Should a company allow an individual to remove their data before costs are recovered if the transaction was in exchange for free genetic sequencing (50)? LunaDNA, a blockchain-based DNA marketplace, allows individuals to withdraw consent for subsequent use of their data; however, the individual will lose all ownership shares previously granted (85). This arrangement could coerce individuals to allow their data to be used instead of missing out on potential financial benefits.

While some blockchain designers have proposed cryptocurrency-based payments based on decentralized anonymous research networks (86), it may be impractical for research payments in the US to remain anonymous. Payments for participating in research are considered taxable income, and Internal Revenue Service (IRS) Form 1099 must be issued to the participant if payments equal or exceed $600 in a calendar year (87). It is unlikely that monetization payments could reach that amount, but organizations would have to track the identities of the individuals to comply with IRS regulations (88).

Even if patient compensation were feasible, Hank Greely, Director of Stanford University's Center for Law and the Biosciences (14) wrote, 'as to compensation, figuring out a royalty kind of system seems very hard to me because of the difficulty of assigning cause/contribution to any particular person's data … and any flat compensation would likely not be very much' (approx. p. 2). When the monetization to individuals is very small, the administrative costs would likely exceed the financial benefit to consumers. Even when using blockchain-based automation, there are costs for data transfers, creating a business model that would be difficult to sustain.

Privacy and security

Blockchain-based technologies can offer new methods to protect the privacy of patient-level information.

Zero-knowledge proofs

Zero-knowledge proofs are blockchain-based strategies that allow one party to prove that some statement is true to another party without revealing anything but the truth of the statement (52, 89). This technology is particularly effective for performing quality assurance without needing to access patient-level information.

Citation: Blockchain in Healthcare Today 2022, **5**: 185 - http://dx.doi.org/10.30953/bhty.v5.185

Homomorphic encryption

Homomorphic encryption involves encryption methods that allow one to perform calculations on encrypted data that does not allow visibility into raw data. When decrypted, the calculated output is the same as if the operations had been performed on the unencrypted data (90). While promising, homomorphic encryption has not yet achieved widespread adoption.

Federated learning systems

Federated learning systems share machine learning algorithms or edge training plans without sharing the raw data (91). Organizations can bring analytic tools to the data while protecting individuals' privacy (92).

Creation of synthetic data

Some blockchain technologies allow the creation of synthetic data that mask individually identifiable data within a dataset (93).

Even when using blockchains to manage health data, no technology is impervious to vulnerabilities. Unidentified strategies using encryption may be vulnerable to future computing advances (92). Furthermore, blockchains and smart contracts have been hacked or breached (50) – even the sizeable public blockchain networks should not be described as entirely immutable (94). Therefore, organizations should remain cautious about data protection for data sharing and sales because there could be considerable unintended consequences for the patients represented in the datasets.

Data quality

While health data acquisition is often thought to be relatively straightforward – especially when using a data service or marketplace – there are often misconceptions about health data quality. The reality is that health information is not designed for research purposes and can be notoriously inaccurate and incomplete (95). Vezyridis and Timmons (26) described that within the National Health Services electronic health record systems, the billing codes used to record the same disease could vary widely between healthcare practices. In addition, the massive volume of electronic health datasets also affects quality because it is challenging to implement data standards and ranges (25).

Health data inaccuracies may require researchers to spend valuable time identifying and eliminating health information that may be of poor quality (83). Worse, researchers may inadvertently use inaccurate health information in research that is not reproducible or may lead to spending limited research funds on projects that are ultimately dead ends (92). Finally, the use of unidentified datasets further complicates data quality because a researcher cannot examine the original sources to confirm or correct data values (92). While some may encourage the use of blockchain to address health data accuracy (96), the use of blockchain for inaccurate health information exemplifies the 'zero state problem' described by LaPointe and Fishbane (97). The authors note that organizations have not achieved 'trusted data' by adding inaccurate information to a blockchain.

Discussion

Mandl and Perakslis (92) point out that it is sadly ironic that patients and healthcare organizations are often unable to obtain health information necessary for treatment; however, the same patients may be included in massive datasets that are shared and sold without appropriate monitoring or oversight. For many health data marketplaces, neither patients nor healthcare organizations are given visibility or control of health information sold in data marketplaces.

This article describes how blockchain technologies are increasingly used to manage the transparency and control of health data in data marketplaces. This technology can advance individual patients' control over their information, monitor access to their data, and control permissions (32), including the ability to revoke permissions (82).

Limitations

As there is a growing interest in managing health datasets as assets, blockchain technologies can improve data valuation and asset management (8). However, there are no uniform approaches to valuation (26) or assetization of health information (25). Thus far, most research conducted on data value has focused on the factors that can influence perceived data value (25). However, there is a need to draft effective algorithms that consider data valuation methods, industry sectors, and data. Furthermore, it is unclear how Fair Market Value limitations required for some datasets may influence or educate these algorithms.

In addition, the scope of research on data marketplaces is not well developed (23), and the research on blockchain-based data valuation and sales is scant. These areas would benefit from an additional study to advance concrete methods of data valuation and responsible development of blockchain-based data marketplaces.

Future work

Blockchain-based data marketplaces are emerging to provide data management and automate monetization practices. However, minimal research has been conducted involving heavily regulated data, such as health information or data intended for submission to the FDA. There is a great need for determining appropriate blockchain platforms and best practices for data management to create sustainable marketplaces for this emerging area.

While the legal, ethical, and regulatory considerations of health data ownership are beyond the scope of this study, additional research on data ownership may advance understanding about authority to control and value health information (81).

Similarly, there is an additional need for understanding whether blockchain-based NFTs can establish datasets as assets and whether NFTs can enhance concepts of data ownership, data control, and value. Specifically, could NFTs demonstrate the value of intangible data assets and/or exclusivity of these data assets?

Conclusion

The sales and exchange of health information grow significantly more extensive and diverse as data can be collected from electronic health record systems and patient-generated data from wearables and wellness apps. The need for sales and exchange is bolstered by the need for real-world data within life sciences organizations. The combination of health data volumes and needs creates a new data economy (82) and opportunities to better assess the data value for these economic opportunities.

Health data assets have been managed by complex and outdated methods where patients are unaware of control and uses of their health information. However, as patients are increasingly empowered with greater electronic access to their health information – and privacy regulations have enabled individuals to have more information and control over data uses – blockchain-based data management systems will serve as an enabling technology. This technology allows patients opportunities for granular consent and greater visibility into the uses of their health information. While mechanisms of data monetization and assetization are still being developed, blockchain technology is a critical tool for maximizing the potential for the emerging health data economy.

Acknowledgements

The authors gratefully acknowledge the thoughtful review, editing, and graphic support provided by Leanne Johnson and Hayley Miller.

Conflicts of interest and funding

The authors work for a company that designs blockchain platforms used for healthcare information. However, this article was intended to provide broad educational information on data marketplaces and data valuation. Several blockchain platforms are described in a neutral and objective manner. The authors did not receive any funding or financial source of support to write this manuscript.

Authors' contributions

Both authors contributed to the conception, design, writing, and editing of this article.

References

1. Demuro P, Petersen C, Turner P. Health "big data" value, benefit, and control: the patient ehealth equity gap. Stud Health Technol Inform 2020; 270: 1123–7. doi: 10.3233/SHTI200337
2. Tang C, Plasek JM, Bates DW. Rethinking data sharing at the dawn of a health data economy: a viewpoint. J Med Internet Res 2018; 20(11): e11519. doi: 10.2196/11519
3. Food and Drug Administration. Framework for FDA's real-world evidence program. Silver Spring, MD; 2018. Available from: https://www.fda.gov/media/120060/download [cited 12 September 2021].
4. Food and Drug Administration. Role of RWE in regulatory decision-making. Silver Spring, MD; 2021. Available from: https://www.fda.gov/drugs/news-events-human-drugs/fda-approval-demonstrates-role-real-world-evidence-regulatory-decision-making-drug-effectiveness [cited 12 September 2021].
5. Food and Drug Administration. Real-world evidence. Silver Spring, MD; 2021. Available from: https://www.fda.gov/science-research/science-and-research-special-topics/real-world-evidence [cited 12 September 2021].
6. Przepiorka D, Ko C-W, Deisseroth A, Yancey CL, Candau-Chacon R, Chiu H-J, et al. FDA approval: blinatumomab. Clin Cancer Res 2015; 21(18): 4035–9. doi: 10.1158/1078-0432.CCR-15-0612
7. Food and Drug Administration, Center for Drug Evaluation. FDA approves new use of transplant drug based on real-world evidence. Silver Spring, MD; 2021. Available from: https://www.fda.gov/drugs/news-events-human-drugs/fda-approves-new-use-transplant-drug-based-real-world-evidence [cited 7 October 2021].
8. Wang X, Feng Q, Chai J. The research of consortium blockchain dynamic consensus based on data transaction evaluation. In: Proceedings of 2018 11th International Symposium on Computational Intelligence and Design (ISCID). Piscataway, NJ: IEEE; 2018, pp. 214–17. doi: 10.1109/ISCID.2018.10150
9. Agarwal A, Dahleh M, Sarkar T. A marketplace for data: an algorithmic solution. In: EC '19: Proceedings of the 2019 ACM Conference on Economics and Computation. New York: Association for Computing Machinery; 2019, pp. 701–26. doi: 10.1145/3328526.3329589
10. Moro Visconti R. Blockchain valuation: Internet of value and smart transactions. In: Moro Visconti R, ed. The valuation of digital intangibles. Cham: Palgrave Macmillan; 2020, pp. 401–22. doi: 10.1007/978-3-030-36918-7_16
11. Office for Civil Rights. Marketing: health information privacy. Washington, DC: US Department of Health and Human Services; 2009. Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html [cited 19 September 2021].
12. DNA Token. Pompano Beach, FL: EncrypGen; 2021. Available from: https://encrypgen.com/dna-token/ [cited 19 September 2021].
13. Elvidge S. Roche buys cancer data company Flatiron Health for $1.9B. Washington, DC: Biopharma Dive; 2018. Available from: https://www.biopharmadive.com/news/roche-buys-cancer-data-company-flatiron-health-for-19b/517285/ [cited 19 September 2021].
14. Cutler JE. How can patients make money off their medical data? Arlington, VA: Bloomberg Law; 2019. Available from: https://news.bloomberglaw.com/pharma-and-life-sciences/how-can-patients-make-money-off-their-medical-data [cited 19 September 2021].

Citation: Blockchain in Healthcare Today 2022, **5**: 185 - http://dx.doi.org/10.30953/bhty.v5.185

15. Fisher M. Google-ascension: why is HIPAA probably not being violated? Atlanta, GA: Health IT Consultant; 2019. Available from: https://hitconsultant.net/2019/11/13/google-ascension-why-is-hipaa-probably-not-being-violated/ [cited 19 September 2021].
16. HIPAA Journal. Google confirms it has legitimate access to millions of Ascension patients' health records. Sherman Oaks, CA; 2019. Available from: https://www.hipaajournal.com/google-confirms-it-has-legitimate-access-to-millions-of-ascension-patients-health-records/ [cited 19 September 2021].
17. Ross C. Backed by hospitals, Truveta wades into the business of selling health data. Boston, MA: STAT; 2021. Available from: https://www.statnews.com/2021/02/17/truveta-patient-data-terry-myerson/ [cited 19 September 2021].
18. Wang D, Liu W, Liang Y, Wei S. Decision optimization in service supply chain: the impact of demand and supply-driven data value and altruistic behavior. Ann Oper Res 2021. doi: 10.1007/s10479-021-04018-y
19. Li H, Li H, Wen Z, Mo J, Wu J. Distributed heterogeneous storage based on data value. In: Proceedings of 2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). Piscataway, NJ: IEEE; 2017, pp. 264–71. doi: 10.1109/itnec.2017.8284985
20. Nolin JM. Data as oil, infrastructure or asset? Three metaphors of data as economic value. J Inform Commun Ethics Soc 2019;18(1):28–43. doi: 10.1108/JICES-04-2019-0044
21. Financial Accounting Standards Board. Statement of financial accounting concepts No 2. 2008. Report No.: CON2. Available from: https://www.fasb.org/jsp/FASB/Document_C/DocumentPage?cid=1218220132599&acceptedDisclaimer=true [cited 26 September 2021].
22. Financial Accounting Standards Board. Statement of financial accounting concepts No. 6. 2008. Report No.: CON6. Available from: https://www.fasb.org/jsp/FASB/Document_C/DocumentPage?cid=1218220132831&acceptedDisclaimer=true [cited 8 October 2021].
23. Banterle F. Data ownership in the data economy: a European dilemma. Rochester, New York, USA: SSRN; 2018. No.: 3277330. doi: 10.2139/ssrn.3277330
24. Suarez SG, le Roux CL, Saxunová D, Li Y. Intangible assets as invisible value in the global business environment. In: Nováčková D, Saxunová D, Delaneuville F, eds. European Union and its new challenges in the digitalized age. Prague: Wolters Kluwer; 2020, pp. 140–50. Available from: https://www.fm.uniba.sk/fileadmin/fm/Veda/projekty/Jean_Monnet_project/Book_of_Chapters_-70-Schuman-170x240__5_.pdf [cited 8 October 2021].
25. Bendechache M, Limaye N, Brennan R. Towards an automatic data value analysis method for relational databases. In: Filipe J, Smialek M, Brodsky A, Hammoudi S, eds. Proceedings of the 22nd International Conference on Enterprise Information Systems. Setúbal, Portugal: SciTePress, Science and Technology Publications, Lda; 2020, pp. 833–40. doi: 10.5220/0009575508330840
26. Vezyridis P, Timmons S. E-Infrastructures and the divergent assetization of public health data: expectations, uncertainties, and asymmetries. Soc Stud Sci 2021;51(4):606–27. doi: 10.1177/0306312721989818
27. Valavi E, Hestness J, Ardalani N, Iansiti M. Time and the value of data. Harvard Business School; 2020. Report No.: 21-016. Available from: https://www.hbs.edu/ris/Publication%20Files/WP21-016_277b3482-f84f-4a6c-8dbc-00e6826bf1a2.pdf [cited 19 September 2021].
28. Nasonov D, Visheratin AA, Boukhanovsky A. Blockchain-based transaction integrity in distributed big data marketplace. In: Shi Y, Fu H, Tian Y, Krzhizhanovskaya VV, Lees MH, Dongarra J, et al., eds. Computational science – ICCS 2018. Cham: Springer; 2018, pp. 569–77. doi: 10.1007/978-3-319-93698-7_43
29. Schwartz R, Platten D, Nadell D. How much is your data worth? Duff & Phelps; 2020. Available from: https://www.duffandphelps.com/-/media/assets/pdfs/webcasts/how-much-is-your-data-worth.pdf [cited 28 September 2021].
30. Firica O, Manaicu A. How to appraise the data assets of a company. Qual Access Success 2018; 19(S3): 41–9. Available from: https://www.srac.ro/calitatea/en/arhiva/supliment/2018/Q-as-Contents_Vol.19_S3_October-2018.pdf [cited 9 October 2021].
31. Hitchner JR. Financial valuation workbook: step-by-step exercises and tests to help you master financial valuation. Hoboken, NJ: John Wiley & Sons; 2017, 480 p. Available from: https://play.google.com/store/books/details?id=kArGDgAAQBAJ [cited 9 October 2021].
32. Mamoshina P, Ojomoko L, Yanovich Y, Ostrovski A, Botezatu A, Prikhodko P, et al. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. Oncotarget 2018; 9(5): 5665–90. doi: 10.18632/oncotarget.22345
33. Lawrenz S, Andreas SPR. Blockchain technology as an approach for data marketplaces. In: ICBCT 2019: Proceedings of the 2019 International Conference on Blockchain Technology. New York: Association for Computing Machinery; 2019, pp. 52–9. doi: 10.1145/3320154.3320165
34. Yao L, Jia Y, Zhang H, Long K, Pan M, Yu S. A decentralized private data transaction pricing and quality control method. In: ICC 2019 – 2019 IEEE International Conference on Communications (ICC). Piscataway, NJ: IEEE; 2019. doi: 10.1109/icc.2019.8761577
35. Zozus MN, Bonner J. Towards data value-level metadata for clinical studies. In: Lau F, Bartle-Clar J, Bliss G, Borycki E, Courtney K, Kuo A, eds. Building capacity for health informatics in the future. Amsterdam: IOS Press; 2017, pp. 418–23. doi: 10.3233/978-1-61499-742-9-418
36. Stack B. Here's how much your personal information is selling for on the dark web. Dublin, Ireland: Experian; 2017. Available from: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ [cited 21 September 2021].
37. Robinson SC. What's your anonymity worth? Establishing a marketplace for the valuation and control of individuals' anonymity and personal data. Digit Policy Regul Gov 2017; 39: 88. doi: 10.1108/DPRG-05-2017-0018
38. Chernyshev M, Zeadally S, Baig Z. Healthcare data breaches: implications for digital forensic readiness. J Med Syst 2018; 43(1): 7. doi: 10.1007/s10916-018-1123-2
39. Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, et al. Healthcare data breaches: insights and implications. Healthcare (Basel) 2020; 8(2): 133. doi: 10.3390/healthcare8020133
40. Trustwave global security report. Greenwood Village, CO: Trustwave; 2019. Available from: https://www.trustwave.com/en-us/resources/library/documents/2019-trustwave-global-security-report/ [cited 21 September 2021].
41. Birch K, Chiappetta M, Artyushina A. The problem of innovation in technoscientific capitalism: data rentership and the policy implications of turning personal digital data into a private asset. Policy Stud 2020; 41(5): 468–87. doi: 10.1080/01442872.2020.1748264

42. Goasduff L. Gartner top 10 trends in data and analytics for 2020. Stamford, CT; 2020. Available from: https://www.gartner.com/smarterwithgartner/gartner-top-10-trends-in-data-and-analytics-for-2020 [cited 22 September 2021].
43. van de Ven M, Abbas AE, Roosenboom-Kwee Z, de Reuver M. Creating a taxonomy of business models for data marketplaces. In: Pucihar A, Kljajić Borštnar M, Bons R, Cripps H, Vidmar D, Perša J, eds. 34th Bled eConference Digital Support from Crisis to Progressive Change Conference Proceedings. Maribor: University Maribor Press; 2021, pp. 313–25. doi: 10.18690/978-961-286-485-9
44. Stahl F, Schomm F, Vossen G, Vomfell L. A classification framework for data marketplaces. Vietnam J Comput Sci 2016; 3(3): 137–43. doi: 10.1007/s40595-016-0064-2
45. Hayashi T, Ohsawa Y. TEEDA: an interactive platform for matching data providers and users in the data marketplace. Information 2020; 11(4): 218. doi: 10.3390/info11040218
46. Gray K. Consortia, buying groups and trends in demand aggregation. Cleveland, OH; 2003. Available from: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.584.5281&rep=rep1&type=pdf [cited 27 September 2021].
47. Fruhwirth M, Rachinger M, Prlja E. Discovering business models of data marketplaces. In: Bui TX, ed. Proceedings of the 53rd Hawaii International Conference on System Sciences. Honolulu, HI: University of Hawai'i; 2020, pp. 5738–47. doi: 10.24251/HICSS.2020.704
48. Dai W, Dai C, Choo K-KR, Cui C, Zou D, Jin H. SDTE: a secure blockchain-based data trading ecosystem. IEEE Trans Inform Forensics Secur 2020; 15: 725–37. doi: 10.1109/TIFS.2019.2928256
49. Spiekermann M. Data marketplaces: trends and monetisation of data goods. Intereconomics 2019; 54(4): 208–16. doi: 10.1007/s10272-019-0826-z
50. Ahmed E, Shabani M. DNA data marketplace: an analysis of the ethical concerns regarding the participation of the individuals. Front Genet 2019; 10: 1107. doi: 10.3389/fgene.2019.01107
51. Laoutaris N. Why online services should pay you for your data? The arguments for a human-centric data economy. IEEE Internet Comput 2019; 23(5): 29–35. doi: 10.1109/MIC.2019.2953764
52. Zhu L, Dong H, Shen M, Gai K. An incentive mechanism using Shapley value for blockchain-based medical data sharing. In: 2019 IEEE 5th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS). Piscataway, NJ: IEEE; 2019, pp. 113–18. doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00030
53. Wang Z, Zheng Z, Jiang W, Tang S. Blockchain-enabled data sharing in supply chains: model, operationalization, and tutorial. Prod Oper Manag 2021; 30(7): 1965–85. doi: 10.1111/poms.13356
54. Grabis J, Stankovski V, Zariņš R. Blockchain enabled distributed storage and sharing of personal data assets. In: Proceedings of the 2020 IEEE 36th International Conference on Data Engineering Workshops (ICDEW). Piscataway, NJ: IEEE; 2020, pp. 11–17. doi: 10.1109/ICDEW49219.2020.00-13
55. Lee CK. Blockchain application with health token in medical & health industrials. In: Zhao S, ed. Proceedings of the 2nd International Conference on Social Science, Public Health and Education (SSPHE 2018). Paris, France: Atlantis Press; 2019, pp. 233–6. doi: 10.2991/ssphe-18.2019.55
56. Täuscher K, Laudien SM. Understanding platform business models: a mixed methods study of marketplaces. Eur Manag J 2018; 36(3): 319–29. doi: 10.1016/j.emj.2017.06.005
57. Brennan B. BurstIQ – Blockchain platform for securing, analyzing and monetizing all of your PHI. Park City, UT: Blockchain Healthcare Review; 2017. Available from: https://blockchainhealthcarereview.com/burstiq-blockchain-platform-for-securing-analyzing-and-monetizing-all-of-your-phi/ [cited 22 September 2021].
58. BurstIQ Technology. Denver, CO; 2020. Available from: https://www.burstiq.com/technology/ [cited 22 September 2021].
59. BurstIQ Foundry. Denver, CO; 2021. Available from: https://www.burstiq.com/foundry/ [cited 22 September 2021].
60. Raths D. Invitae to purchase patient-centric medical records company Citizen. Jacksonville, FL: Healthcare Innovation; 2021. Available from: https://www.hcinnovationgroup.com/finance-revenue-cycle/mergers-acquisitions/news/21237543/invitae-to-purchase-patientcentric-medical-records-company-ciitizen [cited 22 September 2021].
61. Campbell J. Why one startup turned away from medical record portability. San Francisco, CA: Medium; 2018. Available from: https://medium.com/@cmpbl/why-one-startup-turned-away-from-medical-record-portability-9a8cacf49794 [cited 22 September 2021].
62. Ciitizen – FAQ. Tokyo, Japan; 2020. Available from: https://www.ciitizen.com/faq/ [cited 22 September 2021].
63. Draskovic D, Saleh G. Datapace: decentralized data marketplace based on blockchain. Villarceaux, France: Datapace.io; 2017. Available from: https://datapace.io/datapace_whitepaper.pdf [cited 19 September 2021].
64. Haenni R. Datum network: the decentralized data marketplace. Zug, Switzerland: Datum; 2017. Available from: https://datum.org/assets/Datum-WhitePaper.pdf [cited 23 September 2021].
65. Data exchange platform. Lyon, France: Dawex Systems; 2021. Available from: https://www.dawex.com/en/data-exchange-platform/ [cited 21 September 2021].
66. Fernandez RC, Subramaniam P, Franklin MJ. Data market platforms: trading data assets to solve data problems. In: Balazinska M, Zhou X, eds. Proceedings of the VLDB Endowment. New York, NJ: Association for Computing Machinery; 2020, pp. 1933–47. doi: 10.14778/3407790.3407800
67. Embleema – Home. Metuchen, NJ; 2019. Available from: https://embleema.com/ [cited 22 September 2021].
68. Embleema – Patient advocacy groups. Metuchen, NJ; 2020. Available from: https://embleema.com/solutions/patient-advocacy-groups/ [cited 22 September 2021].
69. Embleema – Virtual studies. Metuchen, NJ; 2020. Available from: https://embleema.com/virtual-studies/ [cited 22 September 2021].
70. Vahdati M, Gholizadeh HamlAbadi K, Saghiri AM. IoT-Based healthcare monitoring using blockchain. In: Namasudra S, Deka GC, eds. Applications of blockchain in healthcare. Singapore: Springer; 2021, pp. 141–70. doi: 10.1007/978-981-15-9547-9_6
71. Enigma – Securing the decentralized web. San Francisco, CA; 2020. Available from: https://www.enigma.co/about/ [cited 23 September 2021].
72. Hu-manity – Frequently asked questions. Sparta, NJ: Hu-manity.co; 2021. Available from: https://hu-manity.co/faqs/ [cited 23 September 2021].
73. Harris R. If your medical information becomes a moneymaker, could you get a cut? Washington, DC: NPR; 2018. Available from: https://www.npr.org/sections/health-shots/2018/10/15/657493767/if-your-medical-information-becomes-a-moneymaker-could-you-could-get-a-cut [cited 19 September 2021].

Citation: Blockchain in Healthcare Today 2022, **5**: 185 - http://dx.doi.org/10.30953/bhty.v5.185

74. LunaPBC. Luna Public Benefit Company. San Diego, CA; 2021. Available from: https://www.lunadna.com/lunapbc/ [cited 09 October 2021].
75. Nokia Data Marketplace. Espoo, Finland; 2021. Available from: https://www.nokia.com/networks/services/nokia-data-marketplace/ [cited 22 September 2021].
76. Healthcare blockchain operating system. Portland, OR: Digital Treasury Corporation; 2021. Available from: https://phros.io/services/health_data_market [cited 23 September 2021].
77. Stein Smith S. Data as an asset. In: Stein Smith S, ed. Blockchain, artificial intelligence and financial services. Cham: Springer; 2020, pp. 213–39. doi: 10.1007/978-3-030-29761-9_17
78. Ante L. The non-fungible token (NFT) market and its relationship with Bitcoin and Ethereum. Rochester, New York, USA: SSRN; 2021. No.: 3861106. doi: 10.2139/ssrn.3861106
79. Sandner P, Tóth D, Siadat A, Weber N. Data tokenization: morphing the most valuable good of our time into a democratized asset. Jersey City, NJ: Forbes; 2021. Available from: https://www.forbes.com/sites/philippsandner/2021/07/06/data-tokenization-morphing-the-most-valuable-good-of-our-time-into-a-democratized-asset/ [cited 23 September 2021].
80. Hapiffah S, Sinaga A. Analysis of blockchain technology recommendations to be applied to medical record data storage applications in Indonesia. Int J Inform Eng Electron Bus 2020; 12(6): 13–27. doi: 10.5815/ijieeb.2020.06.02
81. Klugman C. Hospitals selling patient records to data brokers: a violation of patient trust and autonomy. Stanford, CA: Bioethics.net; 2018. Available from: https://www.bioethics.net/2018/12/hospitals-selling-patient-records-to-data-brokers-a-violation-of-patient-trust-and-autonomy/ [cited 19 September 2021].
82. Tlacuilo Fuentes I. Legal recognition of the digital trade in personal data. Mex Law Rev 2020; 12(2): 87–117. doi: 10.22201/iij.24485306e.2020.2.14173
83. International Society for Biocuration. Biocuration: distilling data into knowledge. PLoS Biol 2018; 16(4): e2002846. doi: 10.1371/journal.pbio.2002846
84. Be part of something bigger. San Francisco, CA: PicnicHealth; 2021. Available from: https://picnichealth.com/research [cited 19 September 2021].
85. LunaPBC. Can I lose shares in LunaDNA? LunaDNA Help Center. San Diego, CA; 2018. Available from: https://support.lunadna.com/support/solutions/articles/43000037181-can-i-lose-shares-in-lunadna- [cited 9 October 2021].
86. Zhao H, Bai X, Zheng S, Wang L. RZcoin: Ethereum-based decentralized payment with optional privacy service. Entropy 2020; 22(7): 712. doi: 10.3390/e22070712
87. Internal Revenue Service. 2019 Instructions for Form 1099-MISC. Washington, DC: U.S. Department of the Treasury; 2018. Available from: https://www.irs.gov/pub/irs-prior/i1099msc--2019.pdf [cited 26 September 2021].
88. Charles W, Marler N, Long L, Manion S. Blockchain compliance by design: regulatory considerations for blockchain in clinical research. Front Blockchain 2019; 2: 00018. doi: 10.3389/fbloc.2019.00018
89. Tomaz AEB, Nascimento JCD, Hafid AS, De Souza JN. Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain. IEEE Access 2020; 8: 204441–58. doi: 10.1109/ACCESS.2020.3036811
90. Zhou L, Wang L, Ai T, Sun Y. BeeKeeper 2.0: confidential blockchain-enabled IoT system with fully homomorphic computation. Sensors (Basel) 2018; 18(11): 3785. doi: 10.3390/s18113785
91. Rahman MA, Hossain MS, Islam MS, Alrajeh NA, Muhammad G. Secure and provenance enhanced internet of health things framework: a blockchain managed federated learning approach. IEEE Access 2020; 8: 205071–87. doi: 10.1109/ACCESS.2020.3037474
92. Mandl KD, Perakslis ED. HIPAA and the leak of "deidentified" EHR data. N Engl J Med 2021; 384(23): 2171–3. doi: 10.1056/NEJMp2102616
93. Wang T, Wu X, He T. Trustable and automated machine learning running with blockchain and its applications. SAS Institute, Inc.; 2019. Available from: http://arxiv.org/abs/1908.05725 [cited 28 September 2021].
94. Yaga DJ, Mell PM, Roby N, Scarfone K. Blockchain technology overview. Gaithersburg, MD: National Institute of Standards and Technology; 2018. Report No.: 8202. doi: https://doi.org/10.6028/NIST.IR.8202
95. Hripcsak G, Knirsch C, Zhou L, Wilcox A, Melton G. Bias associated with mining electronic health records. J Biomed Discov Collab 2011; 6: 48–52. doi: 10.5210/disco.v6i0.3581
96. Wu H-T, Tsai C-W. Toward blockchains for health-care systems: applying the bilinear pairing technology to ensure privacy protection and accuracy in data sharing. IEEE Consum Electron Mag 2018; 7(4): 65–71. doi: 10.1109/MCE.2018.2816306
97. LaPointe C, Fishbane L. The blockchain ethical design framework. Washington, DC: Georgetown University; 2019. Available from: https://beeckcenter.georgetown.edu/wp-content/uploads/2018/06/The-Blockchain-Ethical-Design-Framework.pdf [cited 26 September 2021].