Ethik in der Medizin
https://doi.org/10.1007/s00481-024-00805-w

ORIGINAL ARTICLE

Ethical implications of blockchain technology in biomedical research

Giovanni Rubeis

Received: 5 December 2023 / Accepted: 14 February 2024

Abstract

Definition of the problem Biomedical research based on big data offers immense benefits. Large multisite research that integrates large amounts of personal health data, especially genomic and genetic data, might contribute to a more personalized medicine. This type of research requires the transfer and storage of highly sensitive data, which raises the question of how to protect data subjects against data harm, such as privacy breach, disempowerment, disenfranchisement, and exploitation. As a result, there is a trade-off between reaping the benefits of big-data-based biomedical research and protecting data subjects' right to informational privacy.

Arguments Blockchain technologies are often discussed as a technical fix for the abovementioned trade-off due to their specific features, namely data provenance, decentralization, immutability, and access and governance system. However, implementing blockchain technologies in biomedical research also raises questions regarding consent, legal frameworks, and workflow integration. Hence, accompanying measures, which I call enablers, are necessary to unleash the potential of blockchain technologies. These enablers are innovative models of consent, data ownership models, and regulatory models.

Conclusion Blockchain technologies as a technical fix alone is insufficient to resolve the aforementioned trade-off. Combining this technical fix with the enablers outlined above might be the best way to perform biomedical research based on big data and at the same time protect the informational privacy of data subjects.

✉ Univ.-Prof. Dr. phil. habil. Giovanni Rubeis
Department of General Health Studies, Division Biomedical and Public Health Ethics, Karl Landsteiner University of Health Sciences, Dr.-Karl-Dorrek-Straße 30, 3500 Krems, Austria
E-Mail: giovanni.rubeis@kl.ac.at

Published online: 28 March 2024

Keywords Artificial Intelligence · Big data · Informational privacy · Data security · Personalized Medicine

Ethische Aspekte von Blockchain-Technologien in der biomedizinischen Forschung

Zusammenfassung
Problemhintergrund Biomedizinische Forschung auf Grundlage von Big Data bietet immense Vorteile. Groß angelegte multizentrische Forschung, die große Mengen persönlicher Gesundheitsdaten einbezieht, v. a. genetische und genomische Daten, könnte zu einer stärker personalisierten Medizin beitragen. Dieser Typ Forschung erfordert den Transfer und die Speicherung hochsensibler Daten, wodurch sich die Frage ergibt, wie Datensubjekte vor „data harm" geschützt werden können, etwa vor Verletzungen der Privatsphäre, Disempowerment, Verlust von Rechten und Ausbeutung. Hier ergibt sich das Dilemma, wie die Vorteile der auf Big Data basierenden biomedizinischen Forschung zu nutzen sind und zugleich das Recht von Datensubjekten auf informationelle Selbstbestimmung zu schützen ist.
Argumentation Blockchain-Technologien werden aufgrund ihrer Features häufig als technische Lösung des genannten Dilemmas diskutiert. Dazu gehören die Herkunftsbestimmung von Daten, Dezentralisierung, Unveränderbarkeit sowie Zugang und das Governance-System. Allerdings wirft die Implementierung von Blockchain-Technologien in der biomedizinischen Forschung auch Fragen auf, besonders hinsichtlich Consent, rechtlicher Rahmenbedingungen und Integration in den Workflow. Somit bedarf es begleitender Maßnahmen, die ich als *„enabler"* bezeichne, um das Potenzial von Blockchain-Technologien aktualisieren zu können. Zu diesen gehören innovative Consent-Modelle, Modelle zum Datenbesitzrecht und regulatorische Modelle.
Schlussfolgerung Blockchain-Technologien als bloß technische Lösung sind unzureichend hinsichtlich des beschriebenen Dilemmas. Die Kombination aus dieser technischen Lösung und den genannten *„enablers"* könnte der richtige Weg sein, um auf Big Data fußende biomedizinische Forschung zu ermöglichen und zugleich die informationelle Selbstbestimmung von Datensubjekten zu schützen.

Schlüsselwörter Künstliche Intelligenz · Big Data · Informationelle Selbstbestimmung · Datensicherheit · Personalisierte Medizin

Introduction

Scientific and technical advances within the last two decades have transformed biomedical research. Especially whole genome sequencing, cloud computing and increasingly cheaper storage space as well as sophisticated machine learning algorithms enable the collection and processing of data on a larger scale. Hence, contemporary biomedical research depends on integrating large amounts of multivariate data, i.e., data that stems from various different sources. We are witnessing

a shift from small-scale single-site studies towards the "new normal" of large multisite research (Dove et al. 2014). One important aspect in this regard is scaling up studies by using large amounts of health data, including genetic and genomic data in order to define genetic markers for diseases (Racine 2021). This means that biomedical research increasingly depends on the exchange of large data sets between projects, institutions, and platforms (Dove et al. 2014). The main goal of this focus on integrating multivariate data is to achieve personalized medicine and patient-centered therapies (Racine 2021).

One example in this regard is cancer research (Jiang et al. 2022). This type of research requires the integration of various different data types such as molecular omics data, perturbation phenotypic data, molecular interaction data, imaging data, and textual data. Hence, data repositories play a significant role in providing success to data and enabling data exchange between actors (Jiang et al. 2022). One can identify three types of repositories: (1) repositories of original data generated in individual research projects, (2) repositories containing processed data from projects, (3) web applications or platforms that integrate data across projects and studies (Jiang et al. 2022). This means that not only is the required data numerous and complex, it often travels between institutions and researchers as well as between sectors, e.g., from the clinic to a research facility.

Another example for the big data approach in current biomedical research is drug development (Cremin et al. 2022). The conventional approach in drug development would be to start with cell models and then progress to the animal model before conducting clinical trials. However, this approach often fails because results from animal trials do not apply to humans. Big data in genomics research is an alternative that allows identification of disease pathways and also, due to the sheer amount of data available, genetic variants and their impact on disease. Hence, drugs could be personalized to an individual's genetic setup by using this approach. An important aspect here is data integration across different "omics" branches. Therefore, platforms for storing and exchanging complex multivariate datatypes data are also crucial in drug development (Cremin et al. 2022).

The big data approach especially in genomic research and biobanks generates one crucial ethical challenge. How can we protect an individual's right to informational privacy while at the same time generating benefits of big data-type research (Racine 2021; Ploug 2020; Porsdam Mann et al. 2020)? In a big data setting, several *data harms* threaten the informational privacy of users (Ballantyne 2020): unauthorized actors may access personal health data and use them for various, often mischievous purposes. Such a *privacy breach* may have serious consequences for an individual, since personal health data has to be considered as highly sensitive. It could be used to associate an individual with certain groups and sort them into risk categories, which may lead to social disadvantages like stigmatization or marginalization. Another potential data harm is *disempowerment*, which occurs when an individual loses or is not able to exercise control over their own health data. *Disenfranchisement* is another harm that is linked to a lack of transparency and occurs when an individual does not have to possibility to decide about data use. *Exploitation* signifies a data harm whereby for-profit agents use personal health data for their own interests without any benefit for the individual.

The risk of data harms in biomedical research is exacerbated by a fundamental power asymmetry. In a big data setting, we usually distinguish between different stakeholder roles (Zwitter 2014). *Data subjects* are individuals who provide their personal health data, either in a clinical or a research setting. *Big data collectors* are natural persons, clinical or research institutions, or for-profit agents that control and direct data collection as well as storage. *Big data utilizers* are agents that define and control the purpose or goals of data use. A big data divide exists between data subjects, who provide data, and big data collectors as well as utilizers who possess and control the means of data collection, storage, and analysis and decide upon data use (Mittelstadt and Floridi 2016). Hence, data subjects face a power asymmetry that often deprives them of control over their own health and makes them even more vulnerable to potential data harms.

An area where this question is particularly relevant is secondary research, i.e., research on biospecimens that have been obtained in a clinical setting for a specific purpose for which informed consent has been given. One particular issue here is how to obtain informed consent for the secondary use of health data in research (Mikkelsen et al. 2019). Since this research is mostly multicentric and involves big data collectors and utilizers from different nations, conflicts may arise between single-site ethical reviews and different local as well as national privacy regulations and policies (McLennan et al. 2019). In some legislations, such as the Europeans Union's General Data Protection Regulation (GDPR), secondary research does not require explicit consent and is covered by models of broad consent (Racine 2021). However, the question remains whether this is an ethically acceptable way of dealing with data and protecting an individual's right to informational self-determination. Hence, a solution is needed that not only passively protects individuals against fraud or other mischievous actions, but also gives them active control over their own data.

One such solution by a technical means could be blockchain technology. A blockchain is a distributed ledger that exists within a peer-to-peer network and enables users to exchange data in a decentralized and safe manner (Benchoufi and Ravaud 2017; Xie et al. 2021). This relatively new approach is best known from the finance sector, where it forms the technical base for cryptocurrencies. Other uses are tracking goods in supply chains, making economic transfers without intermediaries (e.g., notaries), or voting services (Leible et al. 2019). Due its properties, many commentators regard blockchain technology as the ideal solution for the often-discussed trade-off between informational privacy and the benefits of large-scale biomedical research.

In the following, I discuss the ethical aspects of blockchain technology in biomedical research. I focus on the question of whether blockchain technology can resolve the problem of protecting individuals' right to informational privacy in contemporary, big data-based biomedical research. In a first step, I outline the technical aspects as well as the advantages of blockchain technology for biomedical research. In a second step, I discuss the ethical implications with a focus on the main question detailed above. In a final step, I conclude how blockchain could be used in a proficient way.

Blockchain: technical aspects

In a blockchain, data is organized in linked blocks (Leible et al. 2019). Each block contains a data set and a timestamp, which allows to pinpoint the exact time this block has been added to the blockchain. In addition, cryptographic data hashing is used to ensure the chronological order and identifiability, which means that each block contains a small bit or hash of information of the previous block. The blocks also contain individual user identifiers that indicate data provenance and ownership (Lu 2019). Blocks are closed and allow reading and appending data only, which makes the data immutable (Leible et al. 2019). So-called nodes facilitate data transactions between users in a decentralized network. Each user can access the transaction information of each block, which allows them to retrace every data transfer and identify the users who transferred it (Lu 2019). The data exchange is thus transparent, retraceable, and at the same time immutable. Since all users of the network verify data transfers between parties and fraud or tempering with information is almost technically impossible, no central authority is needed to control the exchange (Leible et al. 2019). Users can also exchange additional data files via peer-to-peer platforms or a cloud, which is called off-chain or secondary solutions (Leible et al. 2019). The main features of blockchain technology are therefore decentralization of data exchange, immutability of data within the blockchain, and transparency of transfer (Casino et al. 2019; Leible et al. 2019; Xie et al. 2021).

One crucial feature of blockchain technology is the possibility to integrate so-called smart contracts (Gaynor et al. 2020). This signifies programs within the blockchain that store and verify contractually agreed-upon conditions for data use and access. A smart contract can be seen as an automated way for verifying whether a user is allowed to access or transfer a particular data set. When the program finds that a user fulfills the conditions that were defined by the data owner, it grants access. That allows data owners to decide which data they want to share to what extent and with whom.

One can distinguish three types of blockchain (Casino et al. 2019): A *public blockchain* allows anybody to join the network and grants every user the opportunity to make transactions or contracts. Most cryptocurrencies are examples. One also speaks of *permissionless blockchains*. A *private blockchain* only allows whitelisted users to join and defines permissions in regard to operations within the network. It uses extended consensus protocols that define the characteristics of users, which requires a centralized administration. A *consortium* or *federated blockchain* combines aspects from both other types by defining a set of nodes as leader nodes that grant access or permissions and is therefore partially decentralized. Private and consortium or federated blockchains are referred to as *permission blockchains*.

Advantages for biomedical research

Most of the essential features of blockchain technology offer great advantages in biomedical research. The most relevant features are data provenance, decentraliza-

tion, immutability (append-only), and access and governance system (Leible et al. 2019).

Data provenance signifies the ability to retrace the origin, processing, and movement of data (Johns et al. 2023). Blockchain provides consensus algorithms and cryptographic methods for maintaining a single list of blocks, each containing provenance information. The involved parties agree on a predecessor and successor for each block in the chain. The provenance information can be captured in a smart contract. In biomedical research, these features may be applied for transparency in terms of data validity. Cryptographic hashing and timestamping can be used to make data easily traceable and identifiable and prohibit any tampering. Furthermore, the traceable lineage of data within the blockchain allows researchers to meet regulatory requirements such as providing audit trails. Thus, blockchain technology could improve the trust in research processes (Elangovan et al. 2022).

Decentralization enables building ecosystems for research data and hence open science that allows participation, collaboration, and contribution by everyone. Therefore, blockchain technology could become an enabler of open science approaches that focus on free collaboration between researchers and data subjects (Leible et al. 2019). As a vision for a new way of organizing knowledge creation and distribution, open science depends on sharing, reusing, and redistributing research data as well as processes and methods. Since blockchain technology allows a decentralized and secure data transfer, it may help to overcome issues such as trustability or restricted access and enable easy collaboration (Leible et al. 2019). Stakeholders in a research process can exchange data directly without the need for a central data manger (Kuo et al. 2017). This could also enable citizen science and thus level access barriers and ensure diversity and representation of all members of the community (Leible et al. 2019). Since no single actor (person, institution, or company) owns the blockchain, the commercial re-use of data by for-profit agents is not a risk, which prevents power asymmetries between stakeholders (Elangovan et al. 2022). The decentralized data architecture powered by blockchain technology could therefore be interpreted as a facilitator of democratization in biomedical research.

The *immutability* or append-only feature of blockchain technology implies that data blocks cannot be altered. Together with the viewable record of all transactions, the immutability guarantees transparency and renders tempering with the data almost impossible (Kuo et al. 2017; Johns et al. 2023). In biomedical research, blockchain technologies could thus be used to ensure data validity and to fulfill regulatory requirements (Johns et al. 2023).

Regarding *access and governance system*, blockchain technology allows open or private access and combines this with individual governance models that empower data subjects to control the purpose of data use (Leible et al. 2019). Depending on the consensus mechanism and type of smart contract, data subjects could manage and control access to their health data. Usually, a smart contract defines decision pathways for the types of contract, the nature and scale of health data tracking, and details on data processing and storage (Gaynor et al. 2020). Data subjects may thus define the conditions of the contract and decide what information they want to share with whom for what purpose and which other conditions. Via health data tracking, data subjects may track enrollment for research studies and manage the

utilization of their health data for research purposes. Data subjects can also define different levels of access to stored information, meaning that they can grant other users, e.g., researchers, access to some but not all health data. In addition, the data provenance feature allows data subjects to trace access and data transfer, giving them the opportunity to control their data after they have given permission for data use by researchers (Ng et al. 2021). Another important aspect is the possibility of reconsent (Porsdam Mann et al. 2020). In the research process, research objectives might shift. When data subjects have agreed to a data use for a specific purpose within a research project, it can be complicated to obtain reconsent when objectives change. Smart contracts could automatize this process and thus facilitate an easy reconsent.

Ethical implications

Blockchain technology could offer the means to overcome the trade-off between the protection of the right to individual privacy and the access to personal health data on a large scale. One can demonstrate this by looking at the potential of blockchain technology for preventing data harms as outlined above.

One crucial ethical implication of blockchain technology is the level of data security and privacy protection it provides. Health data is encrypted and shared within a network of known users where each data access and transfer can be traced. The immutability of data blocks prevents nefarious actions like tampering with the data or data theft. Hence, blockchain technology is an ideal tool to prevent *privacy breach*.

Besides passively protecting data subjects, blockchain technology also gives data subjects active control over their own health data (Porsdam Mann et al. 2020). Through smart contracts, data subjects can define the level of access and authorize different users to varying extents. This could also be done in the form of an opt-out model where default settings grant access to certain users, which could be modified by data subjects (Porsdam Mann et al. 2020). The aforementioned possibility for data subjects to actively track data in terms of access and transfer and, thus, ensure that data is used only in agreed-upon ways is another aspect of control. It can also be seen as a potential empowerment of data subjects within the research process, thus, preventing *disempowerment* and *exploitation*.

Data security, privacy protection, and empowerment might also increase trustability, which is an essential requirement for participation in biomedical research. When data subjects can trust researchers and the research process as a whole due to high levels of security and control provided by blockchain technology, this might increase their willingness to participate in research and share data. Some speak of blockchain as "trustless" in the sense that trust is already encoded in the protocol, given the technical means of privacy protection, data security, and transparency (Benchoufi and Ravaud 2017). Trustability might be particularly relevant from the perspective of an open science approach that aims to include hitherto underrepresented groups. It is a well-known issue in biomedical research that some social or ethnic groups are less willing to participate in research projects, mostly due to historical and political

factors. Examples like the Tuskegee Syphilis Study come to mind (Yearby 2016). As a consequence, minority groups are underrepresented in research cohorts, which leads to bias in research results that in turn can cause or exacerbate health disparities in clinical practice. Blockchain technology as a driver of an open science approach could enable better representation of minority groups through higher trustability and the possibility to actively participate in the research process as an empowered data subject. Thus, blockchain technology might be a fitting approach to prevent *disenfranchisement*.

Further benefits of blockchain technology are not directly related to data subjects, but may improve research quality as such. As some authors argue, the immutability and transparency of blockchain, especially the feature of data provenance, might improve reproducibility of research results. There has been a debate on the issue of reproducibility for years, if not decades. Some even speak of a reproducibility crisis in biomedical research (Begley and Ioannidis 2015). Since blockchain technology makes tampering with data enclosed in blocks virtually impossible and offers full transparency in terms of data provenance, it could be an important facilitator of increasing reproducibility.

Other advantages for biomedical science besides preventing data harms include intellectual property protection through immutability and data provenance, making peer review transparent and creating better metrics for impact in science publishing, and open access repositories (Leible et al. 2019).

Challenges

Access

Although some commentators view blockchain technology as an enabler of open science and inclusive research, it has to be said that equal and open access is only granted in permissionless blockchains, i.e., public blockchains, not in the permissioned types (private and federated or consortium blockchain). Doing research based on a permissioned network would require a democratically elected committee, which would in turn imply to separate users into regular users and committee users (Leible et al. 2019). This would complicate the research process and potentially also undermine open access for all users. Depending on the nature of decision processes within the network, inequalities could arise (Leible et al. 2019). For example, committee users could democratically decide to exclude certain individuals from ethnic groups as users. In permissionless networks that imply equality of all users, system abuse could become a problem (Leible et al. 2019). For-profit actors could infiltrate such a permissionless network and re-use data for financial instead of research purposes.

Although some authors recommend public blockchain networks as the best solution (Porsdam Mann et al. 2020), evidence shows that consortium or federated blockchain networks are the most common in the medical sector (Xie et al. 2021). This is no surprise, given the fact such a network type allows control of access and user characteristics. However, this implies that open science in the fullest sense and complete decentralization cannot be achieved when two user types, regular and com-

mission, exist and access is only open to whitelisted users. On the other hand, this might be the highest level of open science achievable when it comes to biomedical research. Since trustability and privacy protection are of the utmost importance, data subjects may prefer a permissioned network over a permissionless one. The question then arises how to guarantee that whitelisting protects data subjects' interests and is not an instrument to exclude certain groups.

Consent

Blockchain technology does not resolve the consent issue in biomedical research. Consent does not become obsolete because of blockchain technology; on the contrary, it challenges us to redefine conventional concepts of informed consent. Smart contracts, an essential feature and advantage of blockchain technology, works on a consent basis. It requires the consent of data subjects in order to authorize certain users, types and level of access as well as purposes of data use. Hence, methods of consent have to be developed that fit with the specific requirements of smart contracts or existing methods have to be adapted accordingly.

This poses some challenges in itself. First, ensuring data subjects understanding of information. In a conventional research setting, data subjects either give consent during treatment in the clinic or as participants in a specific research project. This requires informing the data subject about the research methods and purposes. It can be challenging to provide information in a way that does not overwhelm data subjects, while at the same time gives them an adequate basis for making an informed decision. In a blockchain setting, smart contracts may pose an additional challenge. Researchers would have to inform data subjects about the workings of blockchain technology and the nature of smart contracts as well. This is not an impossible task, but it adds another layer of complexity to the process of obtaining consent that has to be thought of in advance. Explainability could become an issue here, which requires some level of digital literacy on behalf of researchers.

Second, digital literacy is also required from data subjects. As some commentators argue, handling blockchain technology and smart contracts requires a basic understanding of technical aspects and in some cases even coding skills (Leible et al. 2019; Porsdam Mann et al. 2020). This might set the bar too high for many data subjects and thus undermine the advantage of accessing and controlling one's own data. Therefore, the level of required digital literacy might negatively affect usability and acceptability and prevent data subjects from sharing their data in a blockchain setting.

Workflow integration

As with every healthcare technology, integration into the workflow is a crucial requirement for reaping the benefits of blockchain technology in biomedical research. Several factors have to be considered before implementing this technology. Choosing the right type of blockchain network architecture is crucial in this regard (Porsdam Mann et al. 2020). The network type not only affects factors such as data security and privacy protection as well as access, but also cost and scalability (Casino et al.

2019; Kiania et al. 2023). Public networks usually have a higher throughput, i.e., transactions per unit time, which makes consensus mechanisms costly (Casino et al. 2019). This might make it difficult for smaller institutions or research facilities to use such networks due to the lack of financial resources. Larger actors would be in a privileged position, which undermines the idea of broad data sharing and open science. One strategy to reduce these costs is distributing the ledger in smaller clusters (Kiania et al. 2023). This is sometimes referred to as sharding, meaning to subdivide the ledger into single units called shards, whereby each shard contains only part of the overall data and transaction history (Casino et al. 2019). This allows a higher throughput, since only part of the overall transaction data is included in the process. But this also implies security issues, since reduced overall transaction means reduced hashpower, which in turn makes infiltrating or overtaking a single shard easier than the ledger as a whole. Furthermore, the throughput might be negatively affected by the potential difficulties of cross-shard communication (Hashim et al. 2022). This shows that security, decentralization, and scalability form a trilemma, whereby optimizing one aspect necessarily decreases the others (Hashim et al. 2022).

Another crucial challenge for implementing blockchain into the workflow is lack of standardization and protocols (Leible et al. 2019). This is mainly due to the diversity of existing blockchain solutions (Casino et al. 2019). As a result, interoperability between blockchain networks is often difficult (Xie et al. 2021). Similar issues arise in the communication between blockchain networks and external systems like web services, platforms, or external sensors (Leible et al. 2019). Enabling inoperability with external systems requires so-called application programming interfaces (APIs). Hence, a sustainable technical ecosystem is necessary, which may be costly and require effort as well as manpower.

Finally, legal and governance challenges arise, especially concerning smart contracts (Leible et al. 2019). As of yet, the legal status of smart contracts is unclear, which is a major issue in terms of accountability as well as validity. For example, it is unclear who is responsible when data is lost or inaccessible due to programming errors or whether a timestamp on a data block has any validity as proof in court. Furthermore, smart contracts raise the question of data ownership. In addition, health data transfer via blockchain has to be conform with existing laws and regulations, such as the Europeans Union's GDPR or the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the USA (Arbabi et al. 2023). On the one hand, smart contracts could simplify compliance with regulations such as the accessibility of data to data subjects. On the other hand, regulations such as the restrictions of data transfer to non-European countries might be challenging for multicentric international research projects.

Enablers

The aforementioned challenges make it clear that although blockchain technology has tremendous advantages, it should not be seen a "silver bullet" (Leible et al. 2019) that resolves the trade-off between reaping the benefits of biomedical research and protecting the right to informational privacy. A technical fix alone is insufficient

here. Several additional, nontechnical measures are required to enable a beneficial use of blockchain technology in biomedical research, which I refer to as *enablers*.

The first enabler is innovative models of informed consent that are needed for smart contracts (Rubeis 2024). The main types of informed consent hitherto discussed in biomedical research are *specific consent* and *blanket consent*. Specific consent is the common type used in research projects, whereby data subjects consent to data use in a specific research project with clearly defined objectives and an end date. This works best when data use and transfer is limited to a small number of participants. It is difficult to sustain in larger research projects or where secondary use is involved, since not all possible data uses can be foreseen at the time consent is given. Blanket consent implies to acknowledge this fact and to inform data subjects that due to the dynamics of research projects and shifting objectives, their data might be used for purposes that are impossible to define yet. Data subjects can then decide whether they want to provide their data anyway. The right to informational privacy is thus protected by making the uncertainty in terms of possible data uses transparent. Blanket consent only works when closely monitored by ethics boards and enabled by reliable data security measures (Thompson and McNamee 2017), which would be too costly and extensive in large-scale projects.

Broad consent is similar to blanket consent in that it is not limited to a specific research project, but to data use in a biobank or data repository (Wiertz and Boldt 2022). It delineates the broad objectives and purposes of research that uses data from the biobank or repository. Data subjects consent to the overall objectives and purposes of researchers, but not to each single project. This type is more suitable to larger projects, but still lacks the granularity for data subjects to set their individual preferences. A better candidate is *tiered consent*, which combines specific and broad consent by giving data subjects the opportunity to define their preferences in term of data use. Data subjects give broad consent but can specify which forms of data use and research projects they authorize. It can be seen as a fine-tuning of broad consent that gives a data subject a higher level of control over their own data. When tiered consent uses means of *dynamic consent*, i.e., communication interfaces and an information and communications technology (ICT) architecture, one speaks of *meta consent* (Wiertz and Boldt 2022). This type enables data subjects to update their preferences in a dynamic way by using various communication and encryption technologies. Hence, technical solutions simplify the immense effort of informing and updating data subjects about new objectives and data uses and obtaining their consent. This is obviously the most suitable type of consent as an enabler for blockchain technologies. Meta consent could be achieved in blockchain networks using smart contracts and possibly off-chain solutions.

The second enabler is *data ownership*, which can be divided into private and public ownership models (Rubeis 2024). *Private ownership models* grant data subjects the right to control their data through propretization, which means that data subjects may monetarize them (Hummel et al. 2021). This way, data subjects would own their data as property and would be protected by property rights. This would allow them a higher level of control and protect them especially against the interests of for-profit organizations, thus, mitigating the big data divide. *Public ownership models* define personal health data as a common good due to the benefits of biomedical

research based on this data for the public (Piasecki and Cheah 2022). Following this approach, deidentified or anonymized health should be openly accessible in nonprofit platforms or data repositories.

I cannot discuss all benefits and risks or legal implications of ownership models here (see Ballantyne 2020 and Liddell et al. 2021 for a detailed analysis). An important aspect is that blockchain technologies could be used in both models as an enabler of protecting ownership rights through data provenance and defining them through smart contracts. In turn, data ownership could be an enabler for blockchain technologies in research since it helps to clarify some of the legal challenges discussed above.

The third enabler is *regulatory models* like policies and laws (Rubeis 2024). Legal uncertainties around blockchain technology could be clarified by defining their legal status and acknowledging them as an enabler of data security and privacy protection. An important aspect would be to define standards of compatibility for blockchain technologies with existing regulations like the GDPR or the HIPAA (Liddell et al. 2021). Again, enabling could work both ways since blockchain technologies could be the technical means to implement privacy and data security policies.

Conclusion

Blockchain technologies offer a wide variety of advantages for biomedical research. They could become an important tool for resolving the trade-off between reaping the benefits of biomedical research and protecting the right to personal privacy. Blockchain technologies have the potential to mitigate data harms such as privacy breach, disempowerment, disenfranchisement and exploitation due to their features of data provenance, decentralization, immutability, and access and governance system. However, in order to unleash this potential, several nontechnical enablers need to be implemented as accompanying measures. These enablers are mainly innovative models of informed consent, first and foremost meta consent, data ownership models, and regulatory models. A mix of blockchain technologies, tailored to specific research purposes and infrastructures, and fitting enablers might be the best way to do biomedical research in the big data era in a manner that protects informational privacy of data subjects.

Funding Open access funding provided by Karl Landsteiner University.

Declarations

Conflict of interest G. Rubeis declares that he has no competing interests.

Ethical standards For this article no studies with human participants or animals were performed by any of the authors. All studies mentioned were in accordance with the ethical standards indicated in each case.

References

Arbabi MS, Lal C, Veeraragavan NR, Marijan D, Nygård JF, Vitenberg R (2023) A survey on blockchain for healthcare: challenges, benefits, and future directions. IEEE Commun Surv Tutorials 25:386–424
Ballantyne A (2020) How should we think about clinical data ownership? J Med Ethics 46:289–294
Begley CG, Ioannidis JPA (2015) Reproducibility in science. Circ Res 116:116–126
Benchoufi M, Ravaud P (2017) Blockchain technology for improving clinical research quality. Trials 18:335
Casino F, Dasaklis TK, Patsakis C (2019) A systematic literature review of blockchain-based applications: current status, classification and open issues. Telemat Inform 36:55–81
Cremin CJ, Dash S, Huang X (2022) Big data: historic advances and emerging trends in biomedical research. Curr Res Biotechnol 4:138–151
Dove ES, Knoppers BM, Zawati MNH (2014) Towards an ethics safe harbor for global biomedical research. J Law Biosci 1:3–51
Elangovan D, Long CS, Bakrin FS et al (2022) The use of blockchain technology in the health care sector: systematic review. JMIR Med Inform 10:e17278
Gaynor M, Tuttle-Newhall J, Parker J, Patel A, Tang C (2020) Adoption of blockchain in health care. J Med Internet Res 22:e17423
Hashim F, Shuaib K, Zaki N (2022) Sharding for scalable blockchain networks. SN Comput Sci 4:2
Hummel P, Braun M, Dabrock P (2021) Own data? Ethical reflections on data ownership. Philos Technol 34:545–572
Jiang P, Sinha S, Aldape K, Hannenhalli S, Sahinalp C, Ruppin E (2022) Big data in basic and translational cancer research. Nat Rev Cancer 22:625–639
Johns M, Meurers T, Wirth FN et al (2023) Data provenance in biomedical research: Scoping review. J Med Internet Res 25:e42289
Kiania K, Jameii SM, Rahmani AM (2023) Blockchain-based privacy and security preserving in electronic health: a systematic review. Multimed Tools Appl 82:28493–28519
Kuo TT, Kim HE, Ohno-Machado L (2017) Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc 24:1211–1220
Leible S, Schlager S, Schubotz M, Gipp B (2019) A review on blockchain technology and blockchain projects fostering open science. F Bloc: 2
Liddell K, Simon DA, Lucassen A (2021) Patient data ownership: who owns your health? J Law Biosci 8:lsab23
Lu Y (2019) The blockchain: State-of-the-art and research challenges. J Ind Inf Integr 15:80–90
Mclennan S, Shaw D, Celi LA (2019) The challenge of local consent requirements for global critical care databases. Intensive Care Med 45:246–248
Mikkelsen RB, Gjerris M, Waldemar G, Sandøe P (2019) Broad consent for biobanks is best—provided it is also deep. BMC Med Ethics 20:71
Mittelstadt BD, Floridi L (2016) The ethics of big data: current and foreseeable issues in biomedical contexts. Sci Eng Ethics 22:303–341
Ng WY, Tan TE, Movva PVH, Fang AHS, Yeo KK, Ho D et al (2021) Blockchain applications in health care for COVID-19 and beyond: a systematic review. Lancet Digit Health 3:e819–e829
Piasecki J, Cheah PY (2022) Ownership of individual-level health data, data sharing, and data governance. BMC Med Ethics 23:104
Ploug T (2020) In defence of informed consent for health record research—why arguments from 'easy rescue', 'no harm' and 'consent bias' fail. BMC Med Ethics 21:75
Porsdam Mann S, Savulescu J, Ravaud P, Benchoufi M (2020) Blockchain, consent and prosent for medical research. J Med Ethics 47:244–250
Racine V (2021) Can blockchain solve the dilemma in the ethics of genomic biobanks? Sci Eng Ethics 27(3):35. https://doi.org/10.1007/s11948-021-00311-y
Rubeis G (2024) Ethics of medical AI. The International Library of Ethics, Law and Technology, 24. Springer Nature, Cham. https://doi.org/10.1007/978-3-031-55744-6

Thompson R, Mcnamee MJ (2017) Consent, ethics and genetic biobanks: the case of the Athlome project. BMC Genomics 18:830
Wiertz S, Boldt J (2022) Evaluating models of consent in changing health research environments. Med Health Care Philos 25:269–280
Xie Y, Zhang J, Wang H, Liu P, Liu S, Huo T et al (2021) Applications of blockchain in the medical field: Narrative review. J Med Internet Res 23:e28613
Yearby R (2016) Exploitation in medical research: the enduring legacy of the Tuskegee syphilis study. Case W Rsrv L Rev 1171:
Zwitter A (2014) Big data ethics. Big Data Soc 1:2053951714559253