Smart Contracts in Healthcare

Michael Schnitzbauer

1 Introduction

In a digitally transformed world, the whole ecosystem including business, economy, legal, and political systems can be managed by digital ledger technology (DLT) with smart contracts (Mohanty 2018).

Contracts need approval from authorities and a successful transaction can be prevented by inefficiencies caused by individuals, groups, businesses, or laws. In comparison smart contracts are executed on the digital ledger without the need of a middleman for authorization. "A smart contract is a computerized transaction protocol that executes the terms of a contract" on the blockchain (Szabo 1994). A vending machine is an example in the real world how smart contracts work. The insertion of money into the machine enforces a contract to sell a good at a given price without a shop clerk (Yano et al. 2020). The automation of all these smart contracts can be done on a blockchain/DLT. The DLT framework provides the currency to fuel the execution of smart contracts.

The blockchain/DLT was invented by Satoshi Nakamoto for the first cryptocurrency Bitcoin (Nakamoto 2009). Data can be stored on the digital ledger transparent, immutable, and with a consensus mechanism to allow secure, non-anonymous or anonymous transactions. DLT with smart contracts could lead to a fully automated digital world in the future. Smart contracts are coded and stored in the digital ledger, being transparent, can be shared, and are protected from deletion, tampering, and revision.

The lawyer, broker, or banker as middleman will no longer be needed (Yano et al. 2020). The smart contracts are self-executing coded contracts which are coded, for example, on the Ethereum blockchain with Solidity, Vyper, and LLL. "The terms of the contract between the buyer and seller [are] directly written into the lines of

M. Schnitzbauer (✉)
metaxyp®, Berlin, Germany

P. Glauner et al. (eds.), *Digitalization in Healthcare*, Future of Business and Finance,
https://doi.org/10.1007/978-3-030-65896-0_19

code. Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for central authority, legal system, or external enforcement mechanism. They render transactions traceable, transparent, and irreversible" (Mohanty 2018). Smart contracts can be developed and run on the DLT as decentralized Apps (DApps). They interact with the DLT and facilitate on-chain storage (Johnston et al. 2014). Antonopoulos and Wood provide a detailed description of smart contracts development with solidity on the Ethereum blockchain (Antonopoulos and Wood 2019). The number of DApps is increasing and DApp.com gives as a cross-chain platform an overview about current and future developments (DApp.com 2020).

2 Decentralized Digital Ledger Technology with Smart Contracts: A Chance for Healthcare

Digitalization could help to transform the current centralized healthcare ecosystems via a partly centralized and decentralized system to a fully interoperable decentralized system. In the transformation process centralized IT systems should coexist with decentralized IT systems. The operability of the healthcare system could be ensured in the transformation phase. Profits could be directly invested in the transformation process.

Decentralized IT systems could leverage patient-centered care on a national and global scale. The patients own their health data in these systems and decide who can access the data, powered by smart contracts.

To start the transformation process towards a more efficient and effective decentralized infrastructure a change in IT strategy in Germany is necessary. It is a major problem that in Germany IT strategy is not aligned with business strategies or IT strategy does not even exist. The IT investment budget can be very low and in around 66% of hospitals in Germany, supported by a study from Deloitte, chief information officers (CIO) reported that the IT budget is only 3% of the total budget. The other 33% have an IT budget of around 6%. New technologies are not sufficiently supported and therefore IT departments lack a lot of funding (Deloitte 2018). The law for the future of hospitals in Germany (Krankenhauszukunftgesetz) will support the healthcare ecosystem to build up a digital infrastructure with 3 billion euros and this could also help to establish decentralized technologies in the future healthcare system in Germany (German Health Ministry 2020a).

A decentralized integrated DLT with smart contracts provides the technologies to carry out authorizations and identifications. Therefore it could help to achieve the transformation of patients' health data to electronic health records (EHR). Many countries started their own initiatives to digitalize their health care ecosystems on a national level. Estonia is very successful in this transformation and they even implemented a system with a full blockchain environment to manage EHR (Estonia Health Ministry 2020).

The German "elektronische Gesundheitsakte" will be introduced in 2021 and insurance companies for healthcare in the public and private sector have to offer

an EHR to their customers by law which will lead again to many solutions without interoperability (German Health Ministry 2020b). The USA started its initiative in 2009 and still has not succeeded to introduce a complete national EHR system and a high number of data breaches happened in the EHR system since 2009 (ARRA 2009; Liu et al. 2015).

In Germany a EHR with interoperability will not be introduced in the near future, but the investment of 3 billion euros could help to start the transformation and implementation of higher IT budgets. The IT strategy decisions in the next 5 years will show whether Germany will transform its healthcare system to an interoperable system with a decentralized infrastructure powered by smart contracts. There are many prerequisites to do before this transformation can successfully happen. The following sections should give an idea which key tasks need to be accomplished to switch in the direction of decentralization and the potent role of smart contracts could play in this scenario.

3 Privacy Laws to Secure the Patients' Data: HIPAA and GDPR

Two privacy data laws shall provide the example how privacy laws guarantee the secure transaction of health data within the healthcare ecosystem.

In the USA the Health Insurance Portability and Accountability Act (HIPAA) was introduced to manage patients' privacy. HIPAA privacy regulations ensure that health information of the identifiable individual is managed confidential and the individual person is protected when healthcare data is transferred, received, handled, or shared by healthcare stakeholders, for example, organizations and healthcare professionals. It guarantees that only the minimum necessary health information is used or shared when operating a business. A prerequisite for digital health apps and other systems used in healthcare is that they must be HIPAA compliant when they share personally identifiable information (PII) (HIPAA 2020).

In Germany the General Data Protection Regulation (GDPR) protects health data as special categories of personal data. Sector-specific provisions need to be observed, i.e. provisions of the social code, the German E-health Act, federal state laws on hospitals, or the professional codes of ethics for physicians and pharmacists. Additionally, medical secrecy has to be protected under the data protection regulations. Efficient data protection concepts have to be implemented in all entities processing health data (GDPR 2020).

These regulations require law advice when you want to develop a DApp as an entrepreneur for the European or American market and they have to be followed to publish the DApp on those markets.

In case of the US system any PII to be accessed by a DApp or which is written on a digital ledger when it is public must be encrypted and the interaction parties have to manage the secure interaction with the DApp and any other software solution or system created to collect and add data to an EHR (Zhang et al. 2017).

4 What Is Interoperability in Healthcare?

In an interoperable healthcare system, clinics can exchange their healthcare information without any boundaries and they also can optimize their healthcare processes (Geraci et al. 1991).

There are three types of interoperability:

1. Foundational interoperability: data exchange between multiple healthcare institutions. Data interpretation is not required by the responder.

2. Structural interoperability: data exchange mediated by structured data formats. Data interpretation guaranteed by the usage of these standardized data formats.

3. Semantic interoperability: data interpretation enabled at the level of semantics which allows the interpretation of data meaning.

The three interoperability types allow different IT architectures and integrated data acquisition devices, i.e. mobile devices for blood sugar acquisition or mobile health tracking devices for blood pressure, pulse, etc. to deliver their structured data with quality, security, and in a cost-effective way. Foundational and structural interoperability are prerequisites for the achievement of semantic interoperability which is high in demand for quality of care and the future implementation of new technologies like decentralized DLT frameworks with smart contracts and future technology integration of artificial intelligence (Zhang et al. 2017).

Additionally, chief medical officers are needed to communicate clinical domain knowledge to data scientists and more sophisticated data standards are necessary for the preparation of unstructured acquired data into the EHR, i.e. acquisition of mobile health data by tracking devices for preventive or personalized medicine.

Key in the future will be to integrate clinical domain knowledge and integrated standards who communicate this knowledge, because the myriad sources of health care information cannot be easily interpreted with information systems (Zhang et al. 2017).

Health Level Seven International developed the fast healthcare interoperability resources (FHIR) as an interoperability standard to facilitate the transfer of healthcare information between healthcare stakeholders, like patients, caregivers, healthcare providers, payers, researches, etc. FHIR can directly share specific and well-structured data in comparison to a document-centric approach like PDF-file storage which stores a wide-range of unstructured data with a high security risk. A modern healthcare app like DApps should support data standards like HL7 FHIR which is the blueprint for a standard application programming interface (API) and also is a step towards semantic interoperability (HL7 2020).

5 The Step Towards Patient-Centered Care as a Modern Healthcare Model

Patient-centered care gives back autonomy to patients and gives them full access, decision, and control to their health care data. This prevents data fragmentation, communication inaccuracy, and transmission delays (Oates et al. 2000; Reynolds 2009; Ash et al. 2004; Zhang et al. 2017). In patient-centered care three components are critical to the process: health promotion, communication, and partnership (Constand et al. 2014). We owe the patient a fourth component in a decentralized world: health data sovereignty (see Fig. 1).

DApps should allow data view in real time and patients should be notified when new data is added to the EHR, e.g. in a COVID-19 test, when results are directly transmitted to the EHR. Current health systems have limitations that prevent and further refine a fully patient-centered model:

Patients have a lack of data access control in the conventional system.

In the conventional health system patients cannot easily change or cancel a health provider's access to their data. Providers own the patient´s data permanently after they get access. Patients move between many providers during their life when they have medical issues or just visit their general practitioner for a recipe. In their life time many providers get access to their data. The more parties have stored your patient's data, the higher the risk of data theft due to the increasing probability of data security breaches. In the conventional health care system the access to stored health care data from a specific patient is a challenge. Patients cannot cancel access to their data by the providers, nor can they share data with other providers. The lack of interoperability between providers prevents secure patient-centered health data management. Patients have to register at every provider with communicating their health data and they have to fill out registration forms every time they seek medical treatment at a hospital, clinic, etc. Their data is stored in centralized silo databases at every provider in their own data processing center (Zhang et al. 2017).

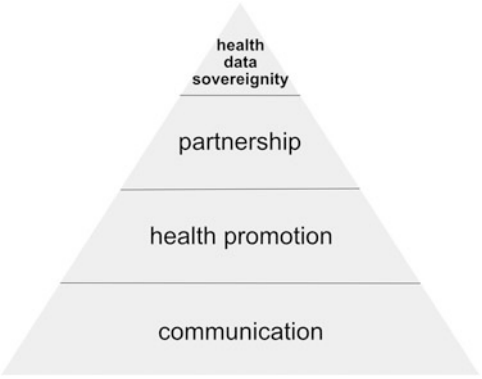

Fig. 1 Patient-centered care builds on the three critical components: communication, health promotion, and partnership. For a decentralized world we have to add a fourth one: data sovereignty. Source: Author

6 The Whole DApp Workflow Must Be GDPR or HIPAA Compliant

The protection of PII against confidentiality breach is a main proposition of HIPAA compliance. A healthcare app data processing workflow from accessing to processing and then distributing the data necessitates HIPAA compliance. In centralized healthcare systems data servers are encrypted and data is protected behind firewalls. In a DLT environment data is publicly available and it is complicated to securely store and manage sensitive health information on the digital ledger (Zhang et al. 2017). In GDPR the patient must give explicit consent that his sensitive personal data can be processed (GDPR 2020).

Currently, DLT cannot be used to store encrypted health data on the ledger. The storage costs and operation expenses would be high to manage the data. Another problem of a public ledger is that the stored sensitive health data would be publicly accessible as long as the ledger is running. Private blockchains could revolutionize this challenge in the future when storage gets cheaper and faster access technology is broadly available, i.e. 5G.

The encryption mechanism of the DLT/blockchain used to protect stored data is critical. It could lead to large data loss when the algorithm is corrupted. New algorithms could damage the algorithm and higher computing power, for example, by quantum computing could solve the cryptographic puzzle and make the stored data vulnerable for hackers. Technology in DLT/blockchain can be updated by hard forks and also if the encryption algorithms are updated frequently maximum protection can only be guaranteed if any temporary breach is prevented (Zhang et al. 2017). Healthcare DApps should be designed well and the storage of encrypted sensitive information should be avoided on the DLT/blockchain. In the future new promising technologies will allow to store data in decentralized cloud systems.

A current approach to connect the DLT/blockchain to patients' health data is to store and point at non-identifiable or encrypted metadata. The metadata refers to the actual patient's health data. Another possibility is to store a small data package which is necessary to transfer sensitive data via a trusted channel, like Chainlink that allows a smart contract on the DLT to search and call a data source off-chain. "[Chainlinks'] smart Contracts provide the ability to execute tamper-proof digital agreements, which are considered highly secure and highly reliable. In order to maintain a contract's overall reliability, the inputs and outputs that the contract relies on also need to be secure. Chainlinks provide a reliable connection to external data that is provably secure end-to-end" (Chainlink 2020).

7 Future Decentralized DLT Frameworks Should Support Turing-Completeness

Bitcoin was the first cryptocurrency and it was designed to buy and sell commodities on a crypto exchange securely and pseudo-anonymously (Nakamoto 2009). Cryptocurrencies are not designed to mediate the transfer of healthcare data models.

Health care systems with interoperability should mediate both the transfer of sensitive patients' data and communications between different stakeholders in the system. In this scenario DApps with decentralized DLT/blockchain as a backbone should be Turing-complete and have implemented programming features which can solve any computation problem. Ethereum as an open-source blockchain platform with smart contracts is ready for Turing-complete DApp development (Ethereum 2020; Zhang et al. 2017).

8 User Identification and Authentication Is a Key Support Prerequisite of DApps

Two stakeholders in healthcare need identification and authentication: patients and healthcare professionals, i.e. physicians, pharmacists, administrators of clinics and insurance companies. Generally, to forget or misplace PII is more prevalent among patients which is the bigger group compared to healthcare professionals. Exposition to healthcare information and continuing education material is higher with healthcare professionals. DApps have to support user identifiability and authentication in addition to strategies to mitigate lost PII (Zhang et al. 2017).

9 DApps Need to Have Structural Interoperability Integration

Vendor-specific data models are used in conventional health systems and apps and those models need to be upgraded and organized to a common standard which is a complex task. DApps need to provide at least structural interoperability and in ideal circumstances semantic interoperability which allows the interexchange of clinical information and the interpretation of received data when similar data models have been implemented. For standardization popular healthcare standards, e.g. HL7 FHIR, DICOM, etc. should be used (Zhang et al. 2017).

10 DApps and Its DLT Framework Must Have High Scalability to Manage a High Number of Patients in the National/Global Healthcare System

Healthcare is a ubiquitous good everybody needs sooner or later. The healthcare systems worldwide have many customers and DApps need to provide their services to millions of users and have to comply with scalablity. It is important to assess a DApp's feasibility by analyzing how it manages high amounts of traffic on the DLT/blockchain, e.g. How much information can be stored on the ledger of the blockchain until the blockchain platform terminates operation from the app to prevent it from being a malicious attack. Another example is how a DApp will track and route operations to the right party within a high number of users? In

that case interoperability of the blockchain should be enabled by the DApp and the same service quality should be provided when users or components of the DApp scale up (Zhang et al. 2017). Scalability for a blockchain environment is still a concern, because when there is a high number of participants in the DLT the system also has an increase in the need for computational power for the whole blockchain ecosystem (Roehrs et al. 2017; McGhin et al. 2019). Sensors or smart devices make the challenge of scaling even greater, because the computer power of the devices is smaller than that of the average computer, to circumvent this problem resources can be offloaded to edge devices of the cloud (Hou 2017; McGhin et al. 2019).

11 How Can Decentralized Systems with Smart Contracts Be Cost-Effective in Comparison to Centralized Existing Approaches?

In the DLT/blockchain network the network nodes who are managed by operators are rewarded cryptocurrency as an incentive for their contribution to sustain the decentralized system with the necessary data integrity and agreement mediated by the fault-tolerant consensus mechanism. DLT/blockchain users have to pay the price for the operator's incentive with respect to storing data and performing computations.

How high will be the costs to pay for the services provided by the decentralized ledger for a healthcare DApp? Can those costs compete with existing centralized systems?

This cost estimation gets important when the services of a DApp are provided to a high number of patients/health provider populations.

Is a healthcare system with DLT and improved interoperability with a patient-centered model more cost-effective that current centralized solutions? What will be the costs for network maintenance and for upgrades to new technology implementations and new versions of the system?

What impact will the implemented DLT/blockchain have when operational costs are directly related to the native cryptocurrency of the employed blockchain? Will fluctuations in price affect cost estimations? Will special tokens be tailored to fit these needs with a token economy approach (Zhang et al. 2017)?

12 Support of Patient-Centered Care Model

The on-going acceptance of a patient-centered care model could help to switch from a centralized healthcare system to a decentralized DLT-based healthcare system where the patients get health care data access, health care data control, and can share their health care data for treatment, for research, in patient support groups, in training groups, etc.

The change from centralized health care systems to decentralized health care systems allows many questions to be asked:

How do we efficiently change the centralized system to a patient-centered decentralized system? Do we need to bridge the introduction of decentralized systems with a centralized/decentralized solution? How can we store health care information on the cloud securely with the help of new decentralized cloud technologies?

In the end we have to decide whether DApps with smart contracts on the digital ledger can overcome the conventional centralized systems with the introduction of patient-oriented features (Zhang et al. 2017).

13 Potential Benefits and Examples of DLT with Smart Contracts in Health Care Ecosystems

In a patient-centric health care system all stakeholders, like patients, doctors, researchers, insurers, clinics will benefit from a DLT system with smart contracts (Carson et al. 2018; Kuo et al. 2017; Khatoon 2020; Skiba 2017).

The decentralization of health data would enable full interoperability: First between health stakeholders at a national level and later at a global level. Borders between different healthcare systems could become blurred and payment between different systems could be leveraged by standardization of payment methods and the use of smart contracts.

Health data exchange could be possible worldwide and security will be provided by the DLT. To solve the problem of scalability faster telecommunications, i.e. the 5G standard which will be introduced soon could provide the necessary coverage around the world and speeds up to 10 gigabits per second will be possible. As a consequence a faster deployment of decentralized networks could happen (Li 2019).

The storage of data in decentralized cloud systems could move centralized data silos to the cloud. The distribution of data and the way data is stored in those systems have to be adapted. Current decentralized cloud technologies divide data in small data chunks which is called sharding. In the next step these chunks are distributed over the decentralized network which is called swarming. This allows to store data in a decentralized "torrent" architecture. A problem which has to be solved is that health data cannot be openly distributed in a public blockchain. A partly decentralized and partly centralized approach could solve the step towards decentralization in the beginning: Encrypted meta data could be stored in the DLT and the health data itself in centralized data silos until better solutions are developed (Siacoin et al. 2020).

DLT would benefit research, preventive medicine, personalized medicine, and artificial intelligence, because the health data would be stored structured in a decentralized health data ecosystem and could easily be analyzed. Personalized data could be tracked in real time and patients would give the permission to access their data (Randall et al. 2017).

The access of health data from a decentralized health data network where patients have to give their permission by smart contracts as a starter could change research.

It could be advertised by multi-center-studies by generating a smart contract for the specific study. The EHR could recommend potential studies from the study trial register and list them for suitable patients in their health record. The patient could give his authorization by simply signing the smart contract of the study. The researchers then get access to the clinical data, radiological data, etc. A foundational change could happen for study population acquisition, because a global decentralized health data ecosystem also would include patients from small- and middle-income countries. Non-university hospitals would also be able to have an incentive to participate in multicenter studies nationally and globally, because a decentralized EHR provides the infrastructure. The smart contract system manages all study relevant management tasks predetermined by the study protocol.

Studies could be adapted to race, religion, and society requirements (Brennan 2017; Radanovic and Likic 2018).

The management of studies by smart contracts could also lead to new ways of research funding. Participating centers could be given study tailored research grants by the appropriate multi-center-study backed by a research foundation with their own side chain, like the German Research Foundation, the NIH, etc. Research money spending could be reduced, because smart contracts do not need any third parties. A more open policy in research could lead to critical voices around study protocols.

Another application in healthcare is pharmacovigilance for the pharmaceutic industry. Smart contracts can write the different produced medication batches into a blockchain. Medications of patients can be identified via the connected side chain from the pharmaceutic company to the EHR and all batches are personalized to the treated patients which is mediated by a smart contract. When the batch cannot be verified in the pharmacovigilance blockchain, then it is sure that a fraud batch was sold to the drugstore and must be stopped from distribution. A fraud solving smart contract could help to solve this problem by informing the patient and the logistics distributor. All are connected by a DLT sidechain and communication is mediated by the appropriate smart contract. The logistics partner could then be stopped automatically to distribute the batch of this fraud medication. The patient is informed that he has a wrong batch, asked to dispose it and the smart contract also orders a new batch of the medication.

Patients could also directly report side effects of a medication by their HER in a patient reported outcome. All pharmaceutical companies must be connected by side chains to the health care DLT framework. Then a special smart contract could report of side-effect to the vendor, producer, and the scientists and improve drug surveillance.

Global health data exchange could accelerate the future of healthcare and personalized medicine. This allows the treatment of patients based on their personal imprinting influenced by their own genetics, epigenetic, life habits and environment. (Kshetri 2018).

The decentralization of data will prevent patient's data loss, because everything is written in the same archive and a chronological life time record is generated (Dimitrov 2019). The decentralization of data management for patient records will

offer accessible infrastructure which allows low- and middle-income countries to connect without having to establish a cost intensive own infrastructure. A lot of data of this under-served and often underestimated group is just waiting to be added (Boulos et al. 2018).

Interoperable structures could also allow doctors to fill out more flexible roles from home by telemedicine or from different locations around the world, because a decentralized system can establish new opportunities which still have to be developed further by experience and try out scenarios. The increasing connectivity and standardization in healthcare could lead to new economic possibilities which can easily be managed by smart contracts and integrated into the decentralized ecosystem by side chains. Another important integration is the direct connection of wearable data to the patient's record which are already collected by step counters and devices for blood glucose management and blood pressure management.

The future will create a new type of smart health care stakeholder powered by a smart contract blockchain environment which will thrive new possibilities to work together interdisciplinary and puts aside grudge.

Currently we are not prepared to go the step beyond our current system. I am curious to follow the next step and some examples I depicted are chosen to be provocative, but I just try to encourage people to start thinking over one's horizon. Hierarchies prevent our system from thriving beyond the point where we only try to tailor our research after grant proposals (Kuo and Oncho-Machado 2018; Greenberger 2019). A patient-centric approach could even more strengthen the patient's position and further will give the doctor the opportunity to build up cooperative relationships, provide extensive information about diagnosis and treatment (Stawicki et al. 2018).

14 Conclusion

Decentralized future DLT frameworks with high transparency, immutability, implemented DLT side chains, and smart contracts could provide the structural IT backbone for a future global health ecosystem and be the key requirement for the realization of healthcare interoperability. Future developments will implement additional layers to the ledgers that allow data storage on decentralized cloud solutions directly connected to the DLT framework with given privacy and security.

Future technology with decentralized cloud solutions, better cryptography tailored by quantum computing, and the 5G communication protocol could start the future health care economy by providing scalability for DApps.

Currently the number of DLT and smart contract developers is rising, because decentralized ledger technology is implemented in every industry besides healthcare. More books are published by pioneer programmers to guide interested programmers towards DApp development on the blockchain and also about smart contract development.

New micro- and macroeconomic solutions could arise by integrating DLT with current healthcare protocols and the usage of smart contracts as a support could

solve healthcare's interoperability problem, get a decentralized EHR which can be used from all stakeholders and future smart contracts could automate healthcare payments, enhance patient admission with home preparation of the hospital stay, automated quality management on structured EHR data, data structuring in a decentralized EHR, national and global comparison of hospitals, structured data in the EHR for artificial intelligence analysis, and the support of clinical-decision-support-systems, multi-center-studies with tailored, automated patient acquisition through the blockchain.

References

American Recovery and Reinvestment Act of 2009 (ARRA). (2009). Retrieved September 25, 2020, from https://www.govinfo.gov/content/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf

Antonopoulos, A. M., & Wood, G. (2019). *Mastering Ethereum: Building Smart Contracts and DApps*. O'Reilly Media.

Ash, J. S., Berg, M., & Coiera, E. (2004). Some unintended consequences of information technology in health care: The nature of patient care information system-related errors. *Journal of the American Medical Informatics Association, 11*(2), 104–112.

Boulos, M. N. K., Wilson, J. T., & Clauson, K. A. (2018). Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare. *International Journal of Health Geographics, 17*, 25.

Brennan, B. (2017). Blockchain HIE overview: A framework for healthcare interoperability. *Telehealth and Medicine Today, 2*, 3.

Carson, B., Romanelli, G., Walsh, P., & Zhumaev, A. (2018). *Blockchain beyond the hype: What is the strategic business value*. McKinsey & Company. Retrieved September 30, 2020, from https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value

Chainlink. (2020). Retrieved September 29, 2020, from https://chain.link/

Constand, M. K., MacDermid, J. C., Dal Bello-Haas, V., & Law, M. (2014). Scoping review of patient-centered care approaches in healthcare. *BMC Health Services Research, 14*, 271.

DApp.com. (2020). Retrieved September 25, 2020, from http://www.dApp.com

Deloitte. (2018). *IT im Krankenhaus – Zwischen neuen Herausforderungen und Chancen*. o.O. Deloitte.

Dimitrov, D. V. (2019). Blockchain applications for healthcare data management. *Healthcare Informatics Research, 25*, 51–56.

Estonia Health Ministry. (2020). Retrieved September 25, 2020, from https://e-estonia.com/solutions/healthcare/

Ethereum. (2020). Retrieved September 29, 2020, from https://ethereum.org/en/

GDPR. (2020). Retrieved September 25, 2020, from https://gdpr.eu/

Geraci, A., Katki, F., McMonegal, L., Meyer, B., Lane, J., Wilson, P., Radatz, J., Yee, M., Porteous, H., & Springsteel, F. (1991). *IEEE standard computer dictionary: Compilation of IEEE standard computer glossaries*. IEEE Press.

German Health Ministry. (2020a). Retrieved September 25, 2020, from https://www.bundesgesundheitsministerium.de/krankenhauszukunftsgesetz.html

German Health Ministry. (2020b). Retrieved September 25, 2020, from https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/e/elektronische-patientenakte.html

Greenberger, M. (2019). Block what? The unrealized potential of blockchain in healthcare. *Nursing Management, 50*, 9–12.

HIPAA. (2020). Retrieved September 25, 2020, from https://www.hhs.gov/hipaa/index.html

HL7. (2020). Retrieved September 29, 2020, from https://www.hl7.org/
Hou, H. (2017). The application of blockchain technology in E-government in China. In *Computer Communication and Networks (ICCCN), 26th International Conference on IEEE*.
Johnston, D., Yilmaz, S. O., Kandah, J., Bentenitis, N., Hashemi, F., Gross, R., Wilkinson, S., & Mason, S. (2014). *The general theory of decentralized applications, dApps* (Vol. 9). GitHub, June.
Khatoon, A. (2020). A blockchain-based smart contract system for healthcare management. *Electronics, 9*, 94.
Kshetri, N. (2018). Blockchain and electronic healthcare records. *Computer, 51*, 59–63.
Kuo, T. T., Kim, H., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association, 24*, 1211–1220.
Kuo, T. T., & Ohno-Machado, L. (2018). Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. *arXiv.*
Li, D. (2019). 5G and intelligence medicine-how the next generation of wireless technology will reconstruct healthcare? *Precision Clinical Medicine, 2*(4), 205–208.
Liu, V., Musen, M. A., & Chou, T. (2015). Data breaches of protected health information in the United States. *JAMA, 313*(14), 1471–1473.
McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications, 135*, 62–75.
Mohanty, D. (2018). *Ethereum for architects and developers: With case studies and code samples in solidity* (pp. 40–41). Apress.
Nakamoto, S. (2009). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved September 24, 2020, from http://www.bitcoin.org/bitcoin.pdf
Oates, J., Weston, W. W., & Jordan, J. (2000). The impact of patient-centered care on outcomes. *Family Practice, 49*, 796–804.
Radanovic, I., & Likic, R. (2018). Opportunities for use of blockchain technology in medicine. *Applied Health Economics and Health Policy, 16*, 583–590.
Randall, D., Goel, P., & Abujamra, R. (2017). Blockchain applications and use cases in health information technology. *Journal of Health and Medical Informatics, 8*, 2.
Reynolds, A. (2009). Patient-centered care. *Radiologic Technology, 81*(2), 133–147.
Roehrs, A., da Costa, C.A., & da Rosa Righi, R. (2017). OmniPHR: A distributed architecture model to integrate personal health records. *Journal of Biomedical Informatics*.
SiaCoin, Swarm, & Ethereum. (2020). Retrieved September 30, 2020, from https://sia.tech; https://swarm-guide.readthedocs.io/en/latest/index.html;https://swarm-guide.readthedocs.io/en/latest/architecture.html;https://github.com/ethereum/wiki/wiki/Sharding-FAQ
Skiba, D. J. (2017). The potential of blockchain in education and health care. *Nursing Education Perspectives, 38*, 220–221.
Stawicki, S. P., Firstenberg, M. S., & Papadimos, T. J. (2018). What's new in academic medicine? Blockchain technology in health-care: Bigger, better, fairer, faster, and leaner. *International Journal of Academic Medicine, 4*(1), 11.
Szabo, N. (1994). *Smart contracts*. Retrieved September 24, 2020, from http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html
Yano, M., Dai, C., Maduda, K., & Kishimoto, Y. (2020). *Blockchain and crypt currency* (pp. 77–94). Springer.
Zhang, P., Walker, M., White, J., & Schmidt, D. C. (2017). *Metrics for assessing blockchain-based healthcare decentralized apps* (pp. 1–4). IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom).