Building Blocks of Negotiating Agents for Healthcare Data

Svetlana Boudko
Norsk Regnesentral
Oslo, Norway
svetlana.boudko@nr.no

Wolfgang Leister
Norsk Regnesentral
Oslo, Norway
wolfgang.leister@nr.no

ABSTRACT

The healthcare market demands advanced, flexible, and secure solutions for personal health data sharing. In our paper, we present preliminary work that proposes a distributed infrastructure of negotiating agents for the healthcare domain. This infrastructure will support healthcare stakeholders to share and access patient health data in a secure way, thus providing benefits for patients and their treatment. Distributed ledger technologies and smart contracts can be considered as a basis for negotiations between distributed agents that carry health-related data. We present an overview of related work and outline the research methodology.

CCS CONCEPTS

• **Security and privacy** → *Pseudonymity, anonymity and untraceability*; *Privacy-preserving protocols*; • **Computer systems organization** → *Distributed architectures*; *Distributed architectures*; • **Information systems** → *Web applications*; • **Networks**; • **Computing methodologies** → *Modeling and simulation*;

KEYWORDS

Smart contracts, Distributed ledger, Blockchain, Ethereum, IOTA, Tangle, Multiagents, Distributed Systems

ACM Reference Format:
Svetlana Boudko and Wolfgang Leister. 2019. Building Blocks of Negotiating Agents for Healthcare Data. In *The 21st International Conference on Information Integration and Web-based Applications & Services (iiWAS2019), December 2–4, 2019, Munich, Germany*. ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3366030.3366108

1 INTRODUCTION

Personal health data has significant value for various healthcare stakeholders including healthcare institutions, researchers, pharmaceutical companies, insurance companies, etc. Accurate and comprehensive data can help healthcare stakeholders to develop better patient-tailored treatments and medications and improve treatment routines [22]. Therefore, sharing personal health data can provide valuable benefits for patients and their treatment. However, unauthorised access to these data can lead to misuse and cause damage if attacked by ransomware, exploited by black market dealers, or accessed by other cybercriminals.

To provide availability and secure exchange of medical data, we need a secure distributed infrastructure for the healthcare domain, where software agents can negotiate decisions about data sharing. Such infrastructure shall be developed in compliance with regulations on privacy, healthcare, and other areas. For instance, the General Data Protection Regulation (GDPR) [12] requires that when processing and exchanging personal data between agents, the design of an infrastructure needs to address properties, such as data protection by design and by default, accountability, pseudonymisation, the right of access, and the right to erasure.

To implement negotiation routines without the involvement of external third parties, smart contracts [33] can be considered as the basis for negotiations between the agents. Smart contracts are digital agreements or software programs that can be implemented using distributed ledger technologies, such as the Ethereum blockchain [41] or IOTA [19].

In this paper, we present a preliminary work regarding a distributed multi-agent healthcare infrastructure where negotiating agents can operate and negotiate solutions for the benefit of patients. The work proposed in this paper includes the following contributions: 1) we have studied the related work and scientific background for software agent-based right negotiations related to health data; and 2) we have outlined main building blocks for the negotiating agents.

This infrastructure relies upon a multiagent system, and we discuss multiagent systems in Section 2. Smart contracts are presented in Section 3. We introduce and study the work related to distributed ledger applications in the healthcare domain in Section 4. Further, we outline the system requirements in Section 5, and conclude with future work in Section 6.

2 MULTIAGENT SYSTEMS

Multiagent Systems (MAS) are referred to as systems of multiple interacting intelligent agents [35, 42] that are autonomous entities such as software programs or robots. The complexity of tasks and problems that can be solved by MAS is significantly higher than the complexity of tasks that agents can solve on their own. Such agents may own different information and may have common or conflicting interests. These agents can be cooperative and work together to achieve a common goal, or they can be selfish. Intelligent agents can respond adaptively to changing contexts and situations. To cooperate and to achieve mutually beneficial agreements, negotiation mechanisms, rules and protocols must be implemented and be available for all agents. The agents must operate in compliance with suitable negotiation protocols. Further, decision-making models and strategies need to be deployed.

iiWAS2019, December 2–4, 2019, Munich, Germany

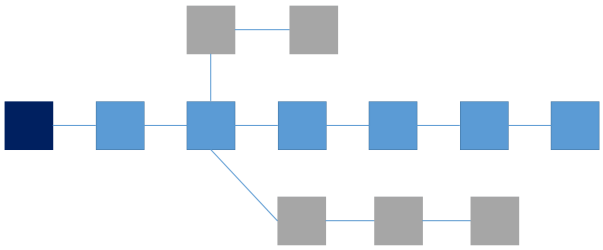

Figure 1: Example of a blockchain. The dark blue square represents the genesis block. The blue squares represent the blocks of the main chain. The grey squares belong to side branches and are discarded.

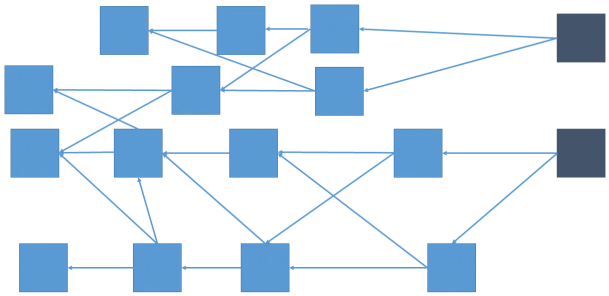

Figure 2: Example of a IOTA tangle showing incoming transaction flow. Blue squares show verified sites. Gray squares show tips.

Negotiation mechanisms and approaches have been widely studies [14, 21, 29], including multi-issue negotiations, concurrent negotiations, strategy-proof mechanisms, rational argumentation, auctions, and voting. Examples of negotiations may include resolving conflicts over the usage of joint resources, task assignments, and other examples from the literature [23].

Further, the agents need to authenticate each other and be accountable for their decisions and actions. As it is important to provide the properties of accountability, verifiability and trusted interactions, smart contracts and ledger technologies are candidates for consideration. These are presented in the upcoming section.

3 SMART CONTRACTS AND DISTRIBUTED LEDGER TECHNOLOGIES

Smart contracts [37–39] are software-based self-executing contracts able to ensuring trust between parties without the need for intermediaries. A smart contract is defined as "a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other. If and when the pre-defined rules are met, the agreement is automatically enforced. The smart contract code facilitates, verifies, and enforces the negotiation or performance of an agreement or transaction. It is the simplest form of decentralised automation" [2]. The terms of the contract are transparent to the involved parties, written in programming code. To implement smart contracts, distributed ledger technologies can be used, including a variety of blockchains and IOTA tangles. In addition, we consider Rights Expression Languages that can be used alone or in combination with other technologies.

3.1 Blockchain

First introduced in 2008, the blockchain technology was applied to implement the cryptocurrency Bitcoin [31]. The blockchain is a sequence of blocks of data that are linked using hash functions, as depicted in Figure 1. Each block consists of transaction data and a hash of the previous block. These blocks are created by some computers and sent to other computers for further validation. The computers that validate new transactions and record them on the blockchain are called miners.

Currently, blockchain technology is implemented in decentralised, second-generation blockchain networks like Ethereum [11, 41], to assure the transactions between the parts according to specific terms. Ethereum builds on the blockchain concept. It runs on a computer network and ensures that smart contracts are executed on all the computers on the network, without a central coordinator. Blockchain data are blocks of data which include transactions and smart contracts.

The Ethereum blockchain consists of four layers: 1) the application layer, 2) the data layer, 3) the consensus layer, and 4) the network layer. In this framework, the blockchain data structures define the data layer, while smart contracts are executed in the application layer. The consensus layer verifies transactions in a blockchain system and assures a consistent state of the blockchain. The blockchain network is implemented as a peer-to-peer network, and the network layer is used to define and formulate the network structure.

Drawbacks related to blockchain and Ethereum are reflected in several studies. Scalability is a known issue due to the agreement upon the longest chain, the average time for confirming transaction was 9.47 minutes in June 2019 [36]. Security problems and cyberattack vulnerability are presented by Chen et al. [6].

Mining requires significant computing power due to the consensus algorithm used. There are efforts to replace the proof-of-work method currently used in cryptocurrencies including Ethereum [8], there are plans to use algorithms that are less energy-intensive [13], such as the proof-of-stake. While Ethereum plans to cut its energy consumption [13], it is still running on proof-of-work completely [8]. However, for our application, other solutions such as corporate blockchains [43] could be employed.

3.2 Tangle IOTA

Differently from blockchain technology, IOTA was designed as an open source protocol for the IoT to secure the communication between IoT devices in a lightweight manner [19]. IOTA does not use the concept of blocks. Instead, its structure is built on directed

acyclic graphs (DAGs) called tangles. An example of such a graph is depicted in Figure 2. Contrary to the blockchain technology where the longest chain is always chosen, and side branches are discarded, the tangle uses different branches of the DAG, which improves both the overall throughput and scalability. If a transaction needs to be added to the tangle, it must be validated by at least two transactions on the ledger. An unconfirmed transaction is called a tip. IOTA uses a tip selection algorithm (TSA) that is based on a biased randomwalk to determine the tips to approve [34].

In addition, IOTA introduces an extension called Masked Authenticated Messaging (MAM). A second layer data communication protocol encrypts messages (masking), confirms source origin (authentication), and creates a continuous message stream on the Tangle until the source stops publishing it (messaging). In a MAM stream, each message holds the data, a reference to the address of the next message only flowing in one direction (forward), and a signature that proves that the publisher created that message. Unique IDs are created for each channel known as root. Therefore, only authorised parties can read and reconstruct the entire message stream [20]. A consensus protocol is used to provide integrity and assure privacy.

3.3 Rights Expression Languages

Rights management systems can play an important role in the context of digital assets rights protection and management. To support the protection of the data, the rights associated with these data need to be described and protected, for instance using a rights expression language (REL), which is a machine-processable language used to express intellectual property rights and other terms and conditions for use over content. There is a variety of RELs available, such as MPEG-21 Part 5, ccREL (for the Creative Commons), W3C Open Digital Rights Language (ODRL), XrML, or METSRights. Note that RELs are related to how the data are licensed [24].

There are examples where digital rights management has been implemented using blockchain technology [7, 26]. Leister et al. [25] propose to use the MPEG-21 standard [4, 18] in medical applications including data collection in wireless patient monitoring systems. The ISO standard MPEG-21 attempts to define a complete infrastructure for delivery and consumption of content, including the protection of rights. The basic unit for data in MPEG-21 is the digital item (DI), which is a generic item that can contain components, resources, or other containers. These structures can either refer to other structures, included data, or reference another item by a universal resource identifier (URI). To enforce digital rights, Parts 4, 5, and 6 of the standard define the rights in the Rights Data Dictionary (RDD), the Rights Expression Language (REL), and how to enforce rights using Intellectual Property Management and Protection (IPMP), respectively.

4 RELATED WORK

Initially introduced for the financial domain [31], distributed ledger technologies soon became popular among others, and are starting to be studied in areas like IoT, supply chain, banking, digital identity, and authorship and IPR, including healthcare services where data privacy and security are of particular concern. This technology has been considered for different parts of the healthcare domain to ensure data availability, interoperability, verifiability, and accountability [30]; as well as to address various healthcare issues including medical data management and security, drug development, and clinical trials [27].

Blockchain technology was used in several studies. A framework on managing and sharing EMR data is proposed by Dubovitskaya et al. [9], where blockchain technology for data management and EMR data sharing was applied. A patient-centric healthcare data management system [1] uses blockchain technology to protect privacy. Griggs et al. [15] proposed the integration of Wireless Body Area Networks and smart contracts. A consortium-managed blockchain is used for distributed data processing and transaction management. For the IoT in healthcare, the study by Dwivedi et al. [10] proposed a framework based on modified blockchain models for secure management and analysis of healthcare big data. Modified blockchain models are suitable for IoT devices and rely on distributed nature and additional privacy and security properties of the network. In a survey, Zhu and Badr [45] outlined the requirements for IoT identity management systems and investigated identity and privacy concerns in the context of IoT and blockchain solutions. Mamoshina et al. [28] presented a blockchain-enabled decentralised personal health data ecosystem for drug discovery, biomarker development, and preventative healthcare. Blockchain and deep learning technologies are used to assess the value of the various types of data, combinations of the various data types, time value of one data type and time value of a combination of data types.

With an emphasis on the IoT in healthcare and wearable technologies, Zheng et al. [44] studied the application of distributed ledger technology in the healthcare domain. IOTA distributed ledger Tangle was used for data sharing and transaction management. The authors developed a system that converged IoT, IOTA Tangle and the Masked Authenticated Messaging (MAM) protocols and propose to use it for sharing health-related data. An application framework and its prototype are supported by distributed ledger technologies and IoT technologies.

Brogan et al. [3] studied how the MAM extension module of the IOTA protocol can be used to securely share, store, and retrieve information from healthcare big data. The case study targets health activity data generated by wearable devices.

A proof-of-concept system for General Data Protection Regulation (GDPR) compliant exchange of blood glucose data-based on IOTA protocol was presented [16]. The authors evaluated a design based on the public IOTA distributed ledger and a design combining the public IOTA ledger with a private InterPlanetary File System (IPFS) cluster. The authors claim that their approach is GDPR-compliant, however, the paper contains no analysis that supports this assertion.

5 SYSTEM REQUIREMENTS

The requirements of the multiagent infrastructure are tailored for the healthcare domain where negotiating agents can operate and negotiate decisions. The requirements will be developed in compliance with the GDPR and healthcare regulations. When processing and exchanging personal data between agents, the design of the infrastructure will address such key requirements of the GDPR as data

protection by design and by default, accountability, pseudonymisation, right of access and right to erasure.

From the network view, the infrastructure is a middleware between the transport layer and the application layer. Negotiations within the infrastructure will evaluate and select appropriate types of negotiation mechanisms that can include one-to-one, one-to-many, and many-to-many mechanisms. The mechanisms will allow the agents to interact and to make decisions based on these interactions. The negotiation agents will be based on rights descriptions extended to healthcare applications and on negotiation types as distributive or integrative negotiation. Further, stages in the negotiation process, trust, tactics, strategies, conflict style and negotiation style will be part of the design. Taking into account the number and possible heterogeneity of the agents, the scalability will be carefully considered and addressed.

Heterogeneity of agents and data. The patient-related data originates from different sources. The system has to be able to access and process different data formats and negotiated if preprocessing of these data is needed before further rendering. Heterogeneity of agents and their information should be taken into account.

Negotiation mechanisms. Negotiation time, efficiency, simplicity, and stability needed to be defined.

Interoperability. Distributed ledger technologies are undergoing rapid development, and we foresee that new algorithms and technologies may soon become available. Various distributed ledger technologies may be deployed. Further, the design of the infrastructure needs to support a strict separation of concerns, as well as interchangeably of algorithms.

Privacy and security. We need to address privacy and trust by design. Authentication, authorisation, data availability and integrity must be addressed. We need to carefully consider the conformity with the privacy requirements, specifically the GDPR [5, 17, 32, 40]. Some properties of a blockchain in their original form oppose certain requirements from the GDPR, such as the right to be removed and to be forgotten. Originally, the content of the blockchain is visible to everybody, and the content of the blockchain cannot be erased nor changed. There are some attempts to solve this, such as encrypting content or using only references to the content. However, there could be unwanted side-effects, such as smart contracts being restricted or the content behind the links being unavailable.

Scalability The infrastructure may accommodate a large number of various heterogeneous agents that are involved in numerous transactions. Therefore, scalability will be carefully considered and addressed.

6 CONCLUSION AND FUTURE WORK

In this paper, we have outlined building components of the negotiating multiagent system for sharing healthcare data. Distributed ledger technologies, including blockchains and tangles, have been considered as the basis for implementing negotiation mechanisms. At this stage, our work is in a concept phase. There is no proof yet which of these technologies is most suitable, as each of them has advantages and disadvantages. Therefore, we plan to implement prototypes that use different technologies and compare them regarding system complexity, processing time, stability, security requirements, etc. Further, verification tools and routines for GDPR compliance will be considered, and agent prototypes will be developed for proof-of-concept.

ACKNOWLEDGEMENT

This work has been carried out in the context of the research project Health Democratization, funded by the Research Council of Norway in the IKTPLUSS programme, grant number 288856.

REFERENCES

[1] Abdullah Al Omar, Mohammad Shahriar Rahman, Anirban Basu, and Shinsaku Kiyomoto. 2017. MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data. In *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, Guojun Wang, Mohammed Atiquzzaman, Zheng Yan, and Kim-Kwang Raymond Choo (Eds.). Springer International Publishing, Cham, 534–543.

[2] Blockchainhub. 2019. Smart Contracts. interactive web site. https://blockchainhub.net/smart-contracts accessed: 7 August, 2019.

[3] James Brogan, Immanuel Baskaran, and Navin Ramachandran. 2018. Authenticating Health Activity Data Using Distributed Ledger Technologies. *Computational and Structural Biotechnology Journal* 16 (2018), 257 – 266. https://doi.org/10.1016/j.csbj.2018.06.004

[4] Ian S. Burnett, Fernando Pereira, Rik Van de Walle, and Rob Koenen (Eds.). 2006. *The MPEG-21 Book.* John Wiley & Sons, Hoboken, NJ, USA. ISBN 0-47001011-8.

[5] Clemens Cap. 2019. Grenzen der Blockchain (Limits of the Blockchain). *Informatik Spektrum* 42, 3 (05 2019), 191–196. https://doi.org/10.1007/s00287-019-01179-w in German.

[6] Huashan Chen, Marcus Pendleton, Laurent Njilla, and Shouhuai Xu. 2019. A Survey on Ethereum Systems Security:Vulnerabilities, Attacks and Defenses. (2019). https://arxiv.org/pdf/1908.04507.pdf submitted.

[7] More Crypto and Less Noise. 2019. Digital Rights Management - Why Steam Needs Blockchain. interactive web site. https://www.statista.com/statistics/793539/bitcoin-transaction-confirmation-time/ accessed: 04 September, 2019.

[8] Digiconomist. 2019. Ethereum Energy Consumption Index (beta). interactive web site. https://digiconomist.net/ethereum-energy-consumption

[9] Alevtina Dubovitskaya, Zhigang Xu, Samuel Ryu, Michael Schumacher, and Fusheng Wang. 2017. Secure and Trustable Electronic Medical Records Sharing using Blockchain. *AMIA ... Annual Symposium proceedings. AMIA Symposium* 2017 (2017), 650–659.

[10] Ashutosh Dwivedi, Gautam Srivastava, Shalini Dhar, and Rajani Singh. 2019. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors* 19, 2 (Jan 2019), 326. https://doi.org/10.3390/s19020326

[11] Ethereum. 2019. Ethereum. interactive web site. https://www.ethereum.org/ accessed: 7 August, 2019.

[12] European Parliament and Council of the European Union. 2016. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[13] Peter Fairley. 2019. Ethereum Plans to Cut Its Absurd Energy Consumption by 99 Percent. https://spectrum.ieee.org/computing/networks/ethereum-plans-to-cut-its-absurd-energy-consumption-by-99-percent

[14] Naoki Fukuta, Takayuki Ito, Minjie Zhang, Katsuhide Fujita, and Valentin Robu. 2016. *Recent Advances in Agent-based Complex Automated Negotiation* (1st ed.). Springer, Switzerland.

[15] Kristen N. Griggs, Olya Ossipova, Christopher P. Kohlios, Alessandro N. Baccarini, Emily A. Howson, and Thaier Hayajneh. 2018. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *Journal of Medical Systems* 42, 7 (06 Jun 2018), 130. https://doi.org/10.1007/s10916-018-0982-x

[16] David Hawig, Chao Zhou, Sebastian Fuhrhop, Andre S Fialho, and Navin Ramachandran. 2019. Designing a Distributed Ledger Technology System for Interoperable and General Data Protection Regulation–Compliant Health Data Exchange: A Use Case in Blood Glucose Data. *J Med Internet Res* 21, 6 (14 Jun 2019), e13665. https://doi.org/10.2196/13665

[17] Luis-Daniel Ibanez, Kieron O'Hara, and Elena Simperl. 2018. *On Blockchains and the General Data Protection Regulation.* Project Report. EU Blockchain Forum and Observatory. https://eprints.soton.ac.uk/422879/

[18] International Standards Organisation. 2004. *Information technology—Multimedia framework (MPEG-21)—Part 1: Vision, Technologies and Strategy.* Technical Report ISO/IEC TR 21000-1. ISO.

[19] IOTA Foundation. 2019. IOTA: The next generation of distributed ledger technology. interactive web pages. https://www.iota.org/ accessed: 26 August, 2019.

[20] IOTA Tutorial. 2019. Masked Authenticated Messaging. interactive web pages. https://iota-news.com/iota-tutorial-19-masked-authenticated-messaging/ accessed: 06 September, 2019.

[21] T. Ito, H. Hattori, M. Zhang, and T. Matsuo (Eds.). 2008. *Rational, Robust, and Secure Negotiations in Multi-Agent Systems.* Studies in Computational Intelligence, Vol. 89. Springer, Berlin, Heidelberg.

[22] Patty Kostkova, Helen Brewer, Simon de Lusignan, Edward Fottrell, Ben Goldacre, Graham Hart, Phil Koczan, Peter Knight, Corinne Marsolier, Rachel A McKendry, Emma Ross, Angela Sasse, Ralph Sullivan, Sarah Chaytor, Olivia Stevenson, Raquel Velho, and John Tooke. 2016. Who Owns the Data? Open Data for Healthcare. *Front Public Health* 21, 6 (17 02 2016), e13583. https://doi.org/10.3389/fpubh.2016.00007

[23] Sarit Kraus. 2001. Automated Negotiation and Decision Making in Multiagent Environments. In *Selected Tutorial Papers from the 9th ECCAI Advanced Course ACAI 2001 and Agent Link's 3rd European Agent Systems Summer School on Multi-Agent Systems and Applications (EASSS '01).* Springer-Verlag, Berlin, Heidelberg, 150–172. http://dl.acm.org/citation.cfm?id=646141.680955

[24] Wolfgang Leister. 2015. Open Licensing. In *INF5780: Open Source, Open Collaboration and Innovation*, Wolfgang Leister and Nils Damm Christophersen (Eds.). Number DART/03/2015 in NR Notat. Norsk Regnesentral, Oslo, Norway, Chapter 5, 107–136.

[25] Wolfgang Leister, Trenton Schulz, Arne Lie, Knut Grythe, and Ilangko Balasingham. 2011. Quality of Service, Adaptation, and Security Provisioning in Wireless Patient Monitoring Systems. In *Biomedical Engineer ing, Trends in Electronics, Communications and Software*, Anthony N. Laskovski (Ed.). Intech, Rijeka, Croatia, Chapter 36, 711–736.

[26] Zhaofeng Ma, Ming Jiang, Hongmin Gao, and Zhen Wang. 2018. Blockchain for digital rights management. *Future Generation Computer Systems* 89 (2018), 746–764.

[27] Tim K Mackey, Tsung-Ting Kuo, Basker Gummadi, Kevin A Clauson, George Church, Dennis Grishin, Kamal Obbad, Robert Barkovich, and Maria Palombini. 2019. 'Fit-for-purpose?' - challenges and opportunities for applications of blockchain technology in the future of healthcare. *BMC medicine* 17, 1 (March 2019), 68. https://doi.org/10.1186/s12916-019-1296-7

[28] Polina Mamoshina, Lucy Ojomoko, Yury Yanovich, Alex Ostrovski, Alex Botezatu, Pavel V. Prikhodko, Eugene A Izumchenko, Alexander Aliper, Konstantin Romantsov, Alexander Zhebrak, Iraneus Obioma Ogu, and Alex Zhavoronkov. 2018. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget* 9, 5 (2018), 5665–5690.

[29] I. Marsa-Maestre, M.A. Lopez-Carmona, T. Ito, M. Zhang, Q. Bai, and K. Fujita (Eds.). 2014. *Novel Insights in Agent-based Complex Automated Negotiation* (1. ed.). Studies in Computational Intelligence, Vol. 535. Springer, Tokyo.

[30] M. Mettler. 2016. Blockchain technology in healthcare: The revolution starts here. In *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom).* IEEE, Munich, Germany, 1–3. https://doi.org/10.1109/HealthCom.2016.7749510

[31] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. http://www.bitcoin.org/bitcoin.pdf

[32] Osborne Clarke. 2019. Blockchain and GDPR: beyond the right to be forgotten. interactive web site. https://www.statista.com/statistics/793539/bitcoin-transaction-confirmation-time/ accessed: 05 September, 2019.

[33] Terry Parker. 2016. *Smart Contracts: The Ultimate Guide To Blockchain Smart Contracts - Learn How To Use Smart Contracts For Cryptocurrency Exchange!* CreateSpace Independent Publishing Platform, USA.

[34] Serguei Petrov. 2018. The tangle. interactive web site. https://static.blockchain.wtf/wp-content/uploads/IOTA_Whitepaper.pdf accessed: 28 August, 2019.

[35] Yoav Shoham and Kevin Leyton-Brown. 2008. *Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations.* Cambridge University Press, New York, NY, USA.

[36] Statista. 2019. Average confirmation time of Bitcoin transactions from June 2017 to June 2018 (in minutes). interactive web site. https://www.statista.com/statistics/793539/bitcoin-transaction-confirmation-time/ accessed: 26 August, 2019.

[37] Melanie Swan. 2015. *Blockchain : blueprint for a new economy.* O'Reilly Media, Sebastopol, Calif.

[38] Nick Szabo. 1997. The Idea of Smart Contracts. Perma.cc record. https://perma.cc/V6AZ-7V8W

[39] Nick Szabo. 1998. Secure Property Titles with Owner Authority. reprint, Satoshi Nakamoto Institute. https://nakamotoinstitute.org/secure-property-titles/

[40] Christian Wirth and Michael Kolain. 2018. Privacy by BlockChain Design: A BlockChain-enabled GDPR-compliant Approach for Handling Personal Data. In *Proceedings of 1st ERCIM Blockchain Workshop 2018 (Reports of the European Society for Society Embedded Technologies)*, W. Printz and P. Hoschka (Eds.). European Society for Socially Embedded Technologies (EUSSET), Amsterdam, The Netherlands, 7. https://doi.org/10.18420/blockchain2018_03

[41] Gavin Wood. 2014. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Yellow Paper, EIP-150 REVISION. http://www.cryptopapers.net/papers/ethereum-yellowpaper.pdf

[42] Michael Wooldridge. 2009. *An Introduction to MultiAgent Systems* (2nd ed.). Wiley Publishing, Hoboken, NJ, USA.

[43] Ariel Zetlin-Jones and Bryan Routledge. 2019. What is a corporate blockchain. IBM Blockchain Blog, Blockchain education. https://www.ibm.com/blogs/blockchain/2019/01/what-is-a-corporate-blockchain/

[44] Xiaochen Zheng, Shengjing Sun, Raghava Rao Mukkamala, Ravi Vatrapu, and Joaquín Ordieres-Meré. 2019. Accelerating Health Data Sharing: A Solution Based on the Internet of Things and Distributed Ledger Technologies. *J Med Internet Res* 21, 6 (06 Jun 2019), e13583. https://doi.org/10.2196/13583

[45] Xiaoyang Zhu and Youakim Badr. 2018. Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions. *Sensors* 18, 12 (Dec. 2018), 4215. https://hal.archives-ouvertes.fr/hal-01945947