TUTA/IOE/PCU

*Journal of the Institute of Engineering, 2017, **13(1):** 37-47*

Printed in Nepal

Clinical Process in Blockchain for Patient Security in Home Care

David Mendes[1], Hugo Galvão[1], Margarida Eiras[2], Manuel Lopes[3]
[1]DECSIS, SA, Direção de Inovação e Desenvolvimento, Évora, Portugal
[2]Escola Superior de Saúde Pública, Lisboa, Portugal
[3]Rede Nacional de Cuidados Continuados, Ministério da Saúde, Portugal
Corresponding author: *diverzulu@gmail.com*

Received: *Sep 20, 2017* ***Revised:*** *Nov 22, 2017* ***Accepted:*** *Dec 25, 2017*

Abstract: We explain how a solution for data privacy, and specifically for cognitive security, can be enforced and guaranteed using blockchain technology in SAAL (Smart Ambient Assisted Living) environments. Using our proposal the access to a patient's clinical process is secure for the adequate interested and authorized parties while resist tampering and ransomware attacks that have recently plagued the HIS (Hospital Information Systems) in various countries.

Key words: Healthcare process, blockchain, data privacy, interoperability

1. Introduction

In the realm of clinical information storage and maintenance one of the most hazardous situations that have been developing lately are the ransomware attacks and sensitive information breaches that are frightening the Hospital and National Health Information Services all around the world. Some new forms of data (actually information and knowledge) storage are in need that can circumvent this problem urgently for the adherence to health information processing that is emergent in these times of *Artificial Intelligence* and *Big Data Analytics* dawn. We suggest a decentralized structure that show characteristics that prevent, by design, all these problems and is not vulnerable to these kind of threats while promoting security in the edge-computing era [1, 5, 33].

2. Problem

We define an abstraction that we call **ICP** (Individual Care Process) a knowledge item that collects comprehensive information about an individual's health and care history. It is necessary for the comprehensive functioning of the **ICP**, to keep the information coming from many sources, which can change it without central control, but with the consistent need to keep an unchanging record of all state transitions, considering the registry of any care or health related event as a state transition. The type of sources of state change can be:

- Health care providers who maintain centralized registration as the EHRs of hospitals or health centers, but managed by the national health information systems services (like SPMS in Portugal);
- Informal care providers in the community such as family members or neighbors, which we call the basic family unit;
- Formal care providers such as PSSI (Private Social Solidarity Institutions) or Continuing

Care Support Teams (RNCCI home support teams in Portugal);
- The HNS (National Health Service) that maintains, through informed consent, the health record of each citizen;
- Data present in associations of users of morbidities (diabetics for example);
- Sensors of activity data (functionality) and clinical data in assisted living environments, concretely linked in **IoT** (Internet of Things);
- An NHS entity that may receive actionable suggestions from the Smart Environments and can implement them with obvious economic benefits.

All of these stakeholders may, in accordance with the fulfillment of the necessary authorizations for access to clinical data, consult and change this data.

The distributed technology that allows us to guarantee this type of access while maintaining the privacy and confidentiality of the data is *Blockchain*, in which the different actors maintain the ledger of all the transactions.

We can visualize the ICP as the ledger for all events related to the health / care process of a citizen. Blockchain technology ensures that only the owner of the private authentication key can authorize the manipulation of the sensitive data of your ICP. Access to data that a given health care provider can access is encapsulated in the ICP itself by prior informed consent and we can maintain a high level of granularity based on such consent.

For example, to be encapsulated that, according to the legislation in force and already prepared for the emergent application of the GDPR (General Data Protection Regulation) on 2018/5/18 and the regulation already in force eIDAS 910/2014, Privileged access to sensitive data can be encapsulated and defined at the individual provider level or the type of specific data results. A physician (or other clinical staff) bound by professional secrecy may have access to diagnostic data, therapy or medical history provided that they are authenticated under the eIDAS but may safeguard some specific diagnostic or outcome data as enforced by the upcoming GDPR.

3. Methods

3.1 Cognitive Security Impact Evaluation

It has become utterly important that data protection be not only concerned with data in isolated terms but with the cognitive power that systems can extract from data when taken aggregated. Nowadays data owners can infer cognitive relations when in possession of disparate data chunks. For instance, the suggestions that NETFLIX provides for their customers are not only based in their history of movie or TV series selections but also in information gathered through their internet browsing profiles. Individual profiling as well as Group profiling, are currently a major privacy concerns, and to avoid them a special attention has to be provided to Cognitive Security [22]. This kind of concern has lead in European Union to the enforcement of General Data Protection Regulation that will be effective in all EU countries in May 25 of 2018. In wireless networks like those present in AAL environments special concerns have to be taken has illustrated in [13] and particularly in Smart Environments [15, 32, 3, 2, 30] as already predicted by [11, 4, 12].

3.2 Blockchain Data Privacy and Protection

It is necessary for the operation of the comprehensive **ICP** (Individual Care Process) to keep the information coming from many sources that can change without central control, but with the need

to keep a record of all immutable state transitions. The distributed technology that allows us to ensure this type of access and data confidentiality is the Blockchain [14–18], in which the different actors maintain the ledger of every healthcare transaction [8, 24, 10, 21, 23].

We can visualize the ICP as the ledger of all events related to the process of health/care of a citizen. Blockchain technology ensures that only the owner of the private authentication key may authorize the handling of sensitive data from his/her CPAIP. Access to data, which a particular healthcare provider may have access to be encapsulated in the ICP itself by prior informed consent and it is possible to maintain a high level of granularity based on these consents. For example, be encapsulated in accordance to the legislation (regulation) in force and already prepared for the emerging application of GDPR (General Data Protection Regulation) in 18/5/2018 [29] and the regulations already in place eIDAS 910/2014 regarding digital signature and document certification [32, 20, 26].

Privileged access to sensitive data can be encapsulated and defined at the level of the individual provider or the type of data-specific results. A physician (or other clinical staff) with professional secrecy enforced may have access to diagnostic data, therapy or medical history when authenticated under eIDAS but ICP is able to restring some data results or specific diagnoses according to their prior consents.

It is important to note the use of DLA (Distributed Ledger Algorithms) algorithms that require only little computational power while maintaining an adequate level of Justice in the transactions order. These algorithms are deeply studied to support DLT (Distributed Ledger Technologies) and already available that we will use in our solution. Specifically it will be implemented the DLA that use BFT (Byzantine Fault Tolerance) [15] like Hashgraph and others based on the Hyperledger project of the Linux Foundation [18, 8].

With these algorithms, even the IoT gateways, based on smartphones, may act on the ledger while ensuring absolute authenticity and privacy of the ICP [19].

3.3 Personal Rights and Information Protection

ICP is a non repudiable, immutable transactional ledger it only maintains the acting proofs not the information about the act itself which is maintained distributed where it was originated or is legally stored. We do not intend to have an end-of-life policy for the ICP for it will evolve with backward semantic compatibility granted with the incorporation of more interested parties. These organizations that handle personal healthcare information like National Health Systems, Secondary, Primary, Emergency or Continued care providers, Diagnostic Complementary Exams Laboratories, Law Enforcement Agencies or others may have to define their own set of policies for data collection, storage, protection, retention, transfer, destruction or re-use and it accommodates because ICP only acknowledges the existence of those pieces of information.

A committee is put up in place that rules all the ethical, moral and legal aspects of any activity to be proposed and carried out along our works. This innovation and research project will comply with the ethical principles and applicable international, EU and national law (in particular, EU Directive 95/46/EC). It will ensure respect for people and for human dignity and fair distribution of the benefits and burden of research, and protect the values, rights and interests of the research participants.

In case of collecting personal data, we will obtain the necessary notifications and authorizations for collecting and processing the data (including specific authorizations and the necessary approvals, if applicable) and the free and fully informed consent of the research participants.

3.4 Informed Consent

The basic principles of Research Ethics include informed consent, understood as that individual's research subjects should be fully informed about all aspects of the research in which they are being asked to participate, including the future use of the data they might provide, the complete details and possible dangers they might face. For this reason, a written model informed consent forms for data collection is designed, in compliance with ethical principles and relevant national, European Union and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols.

Nevertheless, a remote consent could be appraised, with integrated support in the ResearchStack framework. It is defined as any consenting process with zero in-person steps, when a participant is able to join a study without ever seeing a member of the research team. We could benefit of a tool to handle the process of elicitation and recruiting of the participants of study while guaranteeing the adequate informed consents in accordance with the projects Ethics Committee and the international and European ruling GDPR.

Since the launch of ResearchStack on the Android platform in June 2016, many academic and commercial institutions around the world have adapted this framework to develop mobile app-based research studies in health [33]. These studies cover a wide variety of subject areas and particularly in healthcare. Additionally, these app-based studies target a wide variety of participant populations.

Using a mobile recruiting tool, not only the process is easier for the responsible institutions and professionals because the Patient Recruitment is simpler, but also their retention is increased.

ResearchStack could be used for researchers to inform and receive informed consent from patients, and to collect personal health data from participants in trials. ResearchStack has out-of-the box functionality for patient consent, surveys for Patient Reported Outcomes and collecting health data from sensors in the phone or devices connected in the **PAN**[1]. We shall not use it further since ResearchStack has no facilities to integrate data further upstream, for that purposes we use its own integration engine. One further interesting feature of ResearchStack is that it is compatible with Apple's ResearchKit and thus opens the possibility of easily porting to Apple iOS.

4. Blockchain

Blockchain is a shared, distributed ledger that facilitates the process of recording transactions and tracking assets in a business network. Transactions can be verified and recorded through the consensus of all parties involved. Today, many business transactions are inefficient, expensive and vulnerable.

With traditional methods for recording transactions and tracking assets, participants on a network keep their own ledgers and other records. If a central system is compromised, due to fraud, cyberattack, or a simple mistake, the entire business network is affected. A blockchain requires each individual participant – or node – to hold a copy of the record. Any potential changes to the

1 Personal Area Network

record must be compared against each and every node before being approved, which strengthens security and reduces the likelihood of unauthorized changes.

The blockchain architecture gives participants the ability to share a ledger that is updated, through peer-to-peer replication, every time a transaction occurs. Peer-to-peer replication means that each participant (node) in the network acts as both a publisher and a subscriber. Each node can receive or send transactions to other nodes, and the data is synchronized across the network as it is transferred.

The blockchain network is economical and efficient, because it eliminates duplication of effort and reduces the need for intermediaries. It's also less vulnerable because it uses consensus models to validate information. Transactions are secure, authenticated, and verifiable. The participants in both transaction systems are the same. What has changed is that the transaction record is now shared and available to all parties.

A blockchain network has the following key characteristics:

- **Consensus:** For a transaction to be valid, all participants must agree on its validity.
- **Provenance:** Participants know where the asset came from and how its ownership has changed over time.
- **Immutability:** No participant can tamper with a transaction after it's been recorded to the ledger. If a transaction is in error, a new transaction must be used to reverse the error, and both transactions are then visible.
- **Finality:** A single, shared ledger provides one place to go to determine the ownership of an asset or the completion of a transaction.

The blockchain can be permissioned and offer enhanced privacy. Through the use of IDs and permissions users can specify which transaction details they want other participants to be permitted to view. It is particularly valuable in increasing the level of trust among network participants. Because every transaction builds on every other transaction, any corruption is readily apparent, and everyone is made aware of it.

Permissions and cryptography prevent unauthorized access to the network and ensure that participants are who they claim to be. Because participants in a transaction have access to the same records, they can validate transactions and verify identities or ownership without the need for third-party intermediaries. The transactions are time-stamped and can be verified in near real time.

Electronic medical records are currently maintained in data centers (in a cloud-like environment), and access is limited to hospital and care provider networks. Most healthcare data is held in some type of centralized location: an EHR system, a data warehouse, or a repository run by a health information exchange. Each system may have been developed independently and might generate and store the data in its own particular format, leading to the data siloes and interoperability woes that frustrate providers, patients, researchers, and facilitators. Centralization of such information also makes it vulnerable to security breach and can be expensive [14].

Since multiple providers often hold their own versions of the patient record, none of which are validated against each other, a patient could visit five different providers and encounter five different errors in her record, all of which could cause a different sort of harm. The blockchain approach might just be the overhaul that healthcare is looking for. Blockchain can hold the complete medical history for each patient, with multiple granularities of control by the patient, doctors,

regulators, hospitals, insurers, and so on, providing a secure mechanism to record and maintain a comprehensive medical history for every patient.

Blockchain provides the validation that the healthcare industry needs, and it delivers that service in a way all parties can trust. No single entity is in charge of holding the data, yet all participants are responsible for ensuring data integrity and security. If no one can change the record without all stakeholders signaling approval of the edits, and no unauthorized party can access the health record without the participants giving collaborative permission, the healthcare industry can avoid two of its most dangerous big data risks at the same time.

Data stored on blockchains can be shared securely with a pre-approved and trusted group of individuals, patients can be sure that their data is being used properly, that it is all held in one single place - in one standardized format - and that there can be complete transparency, accuracy, and trust in the information across all of its users.

Patients would no longer have to coordinate the tedious and frustrating task of gathering their own records from five or ten providers to send to their new specialist. Instead, they would just add the specialist to the chain, whereupon he could access the same data as everyone else in the closed community [1].

According to an international survey conducted by IBM, 16% of Healthcare Stakeholders Plan to Use Blockchain by 2017 [22]. The blockchain is consensus-based and transactional. All relevant network participants must agree that a transaction is valid. This is achieved through the use of consensus algorithms.

In a business network where participants are known and trusted, transactions can be verified and committed to the ledger through various means of consensus (agreement), including the following:

- Proof of stake: To validate transactions, validators must hold a certain percentage of the network's total value. Proof-of-stake might provide increased protection from a malicious attack on the network by reducing incentives for attack and making it very expensive to execute attacks.
- Multi-signature: A majority of validators (for example, three out of five) must agree that a transaction is valid.
- Practical Byzantine Fault Tolerance (PBFT): An algorithm designed to settle disputes among computing nodes (network participants) when one node in a set of nodes generates different output from the others in the set [14].

Many of the most influential blockchain systems to emerge so far, including Bitcoin, have relied on proof of work (**PoW**). Under this model, anyone who wants to add to the blockchain must perform a work-intensive task using information from the existing blockchain in order to add new information.

This provides a practical protection against manipulation of the blockchain because, in order to undermine group consensus, a malicious party would need to invest a great deal of time producing sufficient PoW to exert a meaningful influence on the blockchain.

Requiring healthcare providers to expend large amounts of computing resources hashing data to produce PoW would be very inefficient. In industries like healthcare, it may make more sense to rely on node votes. Because participants in a blockchain in healthcare are more likely to be altruistic

and operate under real identities than are users of a highly anonymous, unregulated system like Bitcoin, the benefits of avoiding PoW may outweigh the risks associated with node voting as the solution to byzantine faults [27].

4.1 Distributed Ledger Algorithms

It is important to use Distributed Ledger Algorithms (**DLA**) algorithms that only require small computational power and maintain an adequate level of justice in the transaction order. These algorithms are deeply studied to support the technologies already available from **DLT** (Distributed Ledger Technologies) that we will use in our solution. Specifically, DLAs implementing "Byzantine Fault Tolerance" [15] such as Hashgraph and others based on the Linux Foundation's Hyperledger project [18, 8] are implemented.

With these algorithms, the implemented Smartphone-based **SAAL** (Smart Ambient Assisted Living) **IoT** gateways can act on the ledger while guaranteeing the authenticity and absolute privacy of the **ICP**, even in **IoT** [19].

4.2 Byzantine Fault Tolerance

To ensure the consensus of the transactions needed for building the Hyperledger blockchain is used an algorithm based in Byzantine Fault Tolerance system. This algorithm is mandatory to allow a transaction to be accepted as valid and being added to the ledger. This system is already used in practical cases, such as tolerate failures and avoid adulteration in the well-known bitcoin cryptocurrency but also in flight control systems of Boeing 777 and 787.

Byzantine Fault Tolerant systems are designed to tolerate a number **f** of Byzantine faulty nodes in a network. To ensure that a transaction is accepted as valid, 2f+1 valid signatures from distinct peers are needed. If some error occurs in a peer, due to an invalid message or timeout, then a transaction to the next peer in the chain is sent.

In non-failure cases, a client submits a transaction to a leader peer. That peer verifies the transaction and signs it. It then broadcasts to the remaining 2f+1 validating peers. The other peers receive the signed transaction and do their own signature. The broadcast is sequentially made until the last needed peer receives the required amount of valid signatures, including its own. All the signatures are validated and that transaction is then considered valid. Having met the consensus state, a final broadcast to all peers is done so that they can add the transaction, with all the signatures, to the ledger. The sequence that the peers send their transactions is based in a reputation system.

To detect failures, when a peer sends a transaction, is given a timeout for receiving an answer. If that timeout is reached then a new transaction is made for an additional peer in the chain. The process is repeated until reaching 2f+1 valid signatures. At that time the transaction is considered valid and a broadcast with that signed transaction is made to all peers [16].

4.3 Information Hiding through API

The REST APIs are specified according to the **OpenAPI** Specification (**OAS**) version 3.0 [35]. Producing and maintaining the specification in this neutral format opens up the possibility of distributing the implementation through the various clouds of serverless computing whose promoters are part of the initiative **Google**, **IBM**, **Microsoft** and **AWS**, among many others. **OpenAPI** tool support, essentially OSS, as well as community support is currently unparalleled.

Shared definitions are crucial to managing the change process to which most software processes are continually under scrutiny. Defining a single reference point for documentation, code generation, publishers, test automation, and change management allows us to keep track of and minimize the costs of developing and deploying distributed computing artifacts. An open specification is the guarantee of neutrality for the different suppliers and, if the main stakeholders in the industry are involved, the guarantee of widespread adoption and the implementation of a future de facto standard.

The key API will:

- Allow manipulation of the **ICP** (ledger) in a distributed way using Blockchain technology.
- Encapsulating the **ICP** as an object that contains the named authorizations for its manipulation.
  Authorizations allow the object itself to be viewed/changed by who (human or device) authenticates, according to **eIDAS 910/2014** [20, 26], with permissions to do so.
- The **ICP** does not contain information on the patient's personal identity and, as such, its manipulation does not compromise the subject's privacy and safety.
- If named authorizations in the **ICP** allow this, an authenticated user can reconstruct the identity in the public segment of AAL using a token generated for that purpose, but always in an ephemeral and non-transmissible environment to prevent personal re-identification according to the **GDPR**[2], **HIPPA**[3] and, for the case of intercontinental information transmission, the **Umbrella Protocol** [28].
- To enable the development, using **DL**[4] techniques, of the models that allow to guarantee the activation of the less differentiated caregiver.
  Allow the application of **DL** algorithms to reason about the **ICP** in order to suggest rules for automatic activation of care providers (human or devices). These algorithms developed automatically in a supervised learning phase and verified by reinforcement learning should be available as microservices in the Public Cloud for activation by a responsible body.

5. Solution

According to the several considerations introduced above, we developed our solution using a raw blockchain implementation [14] with the **Hyperledger Fabric DLA** [13] in order to attain **computable reasoning** over a highly secure and authentic home based ambient assisted living environment.

6. Discussion

Some other related proposals have been emerging recently as of mid-2017 like [17] and some important players in the Software industry are devoting attention to this possibility like Microsoft and Google as well as major industry conferences around the subject like the IEEE promoted Blockchain in Healthcare: A Rock Stars of Technology Event held in Feb. 22, 2017. Alternatively, the **US ONC**[5] "Blockchain in Healthcare" Code-A-Thon in mid-March at Georgetown University's McDonough School of Business. The competition was a follow- on effort to support ONC's widely publicized "Use of Blockchain in Health IT and Health-related Research Challenge", as well as

2 General Data Protection Regulation

3 Health Information Privacy and Protection Act

4 Deep Learning

5 Office of the National Coordinator of Health Information Technology

the ONC/NIST "Blockchain in Healthcare" Workshop where important scientific and technical knowledge was developed like the first prizewinner [34]. Valuable contributions arise from the initiatives that propel the interest and validity of the proposed approach.

7. Conclusions

We introduce the usage of Blockchain technology as a means to achieve unsurpassed security in health records bookkeeping. While completely tamper proof, we indicate the algorithms which usage can lead to a fair, democratic maintenance of the ledger while being low computational power consumers. This characteristic enables the usability by low computing power device like those present in the AAL environments. The level of safety perceived by monitored patients in these domiciled or institutionalized environments is very high while their health information is guaranteed to be at no risk.

References

[1] Ahmed A, Ahmed E (2016), *A survey on mobile edge computing*. 10th International Conference on Intelligent Systems and Control (ISCO), doi:10.1109/ISCO.2016.7727082: 1–8.

[2] Alirezaie M, Renoux J, Köckemann U, Kristoffersson A, Karlsson L and Blomqvist E et al. (2017), An Ontology-based Context-aware System for Smart Homes: E-care@home. Sensors, 17, doi:10.3390/s17071586.

[3] Asano S, Yashiro T, Sakamura K (2016), Device collaboration framework in IoT-aggregator for realizing smart environment. TRON Symposium (TRONSHOW), doi:10.1109/TRONSHOW.2016.7842886: 1–9.

[4] Attar A, Tang H, Vasilakos AV and Yu FR, Leung VCM (2012), A Survey of Security Challenges in Cognitive Radio Networks: Solutions and Future Research Directions. Proc. IEEE, doi:10.1109/JPROC.2012.2208211: 3172–3186.

[5] Beck MT, Werner M, Feld S, Schimper T (2014), *Mobile Edge Computing: A Taxonomy*. Citeseer, Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.670.9418.

[6] Bresnick J (2016), Is Blockchain the Answer to Healthcare's Big Data Problems?. In: HealthITAnalytics [Internet], 27 Apr 2016 [cited 29 Aug 2017], available: https://healthitanalytics.com/news/is-blockchain-the-answer-to-healthcares-big-data-problems.

[7] Bresnick J (2017), 16% of Healthcare Stakeholders Plan to Use Blockchain by 2017. In: HealthITAnalytics [Internet], 4 Jan 2017 [cited 29 Aug 2017], available: https://healthitanalytics.com/news/16-of-healthcare-stakeholders-plan-to-use-blockchain-by-2017.

[8] Cachin C (2016), Architecture of the Hyperledger blockchain fabric. Workshop on Distributed Cryptocurrencies and Consensus Ledgers, available: https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf.

[9] Castro M, Liskov B (2002), Practical Byzantine Fault Tolerance and Proactive Recovery. ACM Trans Comput Syst. New York, USA: ACM (20), doi:10.1145/571637.571640: 398–461.

[10] Christidis K, Devetsikiotis M (2016), Blockchains and Smart Contracts for the Internet of Things. IEEE Access, doi:10.1109/ACCESS.2016.2566339: 2292–2303.

[11] Clancy TC, Goergen N (2008) Security in Cognitive Radio Networks: Threats and Mitigation. 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008), doi:10.1109/CROWNCOM.2008.4562534:1–8.

[12] Fragkiadakis AG, Tragos EZ (2013), A survey on security threats and detection techniques in *cognitive radio networks*. *Surveys & Tutorials*, Available: http://ieeexplore.ieee.org/iel5/9739/5451756/06129369.pdf.

[13] Greenstadt R, Beal J (2008), *Cognitive Security for Personal Devices*. Proceedings of the 1st ACM Workshop on Workshop on AISec. New York, NY, USA, doi:10.1145/1456377.1456383 : 27–30.

[14] Gupta M (2017), *Blockchain for Dummies*. Burchfield CA, editor: www.wiley.com: John Wiley & Sons, Inc.

[15] Holler J, Tsiatsis V, Mulligan C, Avesand S, Karnouskos S and Boyle D (2014), *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*. Academic Press, Available: https://market.android.com/details?id=book-wtfEAgAAQBAJ

[16] Hyperledger/iroha (2017) , In: GitHub [Internet], [cited 29 Aug 2017], available: https://github.com/hyperledger/iroha.

[17] Ichikawa D, Kashiyama M and Ueno T (2017), Tamper-Resistant Mobile Health Using Blockchain Technology. JMIR mHealth and uHealth, (5), doi:10.2196/mhealth.7938.

[18] Jacobovitz O (2016), Blockchain for Identity Management. Available: https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf.

[19] Jain S, Kajal A (2015), Effective Analysis Of Risks And Vulnerabilities In Internet Of Things. *International Journal of Computing and Corporate Research* ijccr.com, available: http://www.ijccr.com/March2015/4.pdf.

[20] Jordan F, Pujol H and Ruana D (2014), Achieving the eIDAS Vision Through the Mobile, Social and Cloud Triad. ISSE 2014 *Securing Electronic Business Processes*, Springer Vieweg, Wiesbaden, doi:10.1007/978-3-658-06708-3_6: 81–93.

[21] Kakavand H, Kost De Sevres N and Chilton B (2017), The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies. papers.ssrn.com, available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251.

[22] Kinsner W (2012), *Towards cognitive security systems*. IEEE 11th International Conference on Cognitive Informatics and Cognitive Computing, doi:10.1109/ICCI-CC.2012.6311207: 539–539.

[23] Liang X, Shetty S, Tosh D, Kamhoua C, Kwiat K and Njilla L (2017), ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. International Symposium on Cluster, Cloud and Grid Computing, IEEE/ACM.

[24] Mainelli M, Smith M and Others (2015), Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology). *The Journal of Financial Perspectives*, the-blockchain.com, (3), Available: http://www.the-blockchain.com/docs/Journal%20of%20Financial%20Perspectives%20-%20Sharing%20Ledgers%20for%20Sharing%20Economies.pdf: 38–69.

[25] Morabito V (2017), *Blockchain Value System. Business Innovation through Blockchain*. Springer International Publishing, doi:10.1007/978-3-319-48478-5_2: 21–39.

[26] Morgner F, Bastian P and Fischlin M (2016), Securing Transactions with the eIDAS Protocols. Information Security Theory and Practice, Springer, doi:10.1007/978-3-319-45931-8_1: 3–18.

[27] NASDAQ (2017), Distributed. Byzantine Fault Tolerance: The Key for Blockchains. In: NASDAQ.com [Internet], NASDAQ, 29 Jun 2017 [cited 29 Aug 2017], available: http://www.nasdaq.com/article/byzantine-fault-tolerance-the-key-for-blockchains-cm810058.

[28] Ouaddah A, Mousannif H, Abou Elkalam A and Ait Ouahman A (2017), *Access control in the Internet of Things: Big challenges and new opportunities*. Computer Networks, (112), doi:10.1016/j.comnet.2016.11.007: 237–262.

[29] Parlamento E. and Conselho da UE (2016), GDPR - EUR-Lex - 32016R0679 - EN. Journal Oficial da União Europeia. (59), available: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.POR&toc=OJ:L:2016:119:TOC

[30] Pramanik MI, Lau RYK, Demirkan H and Azad MAK (2017), *Smart Health: Big Data Enabled Health Paradigm within Smart Cities*. Expert Syst Appl. Elsevier, Available: http://www.sciencedirect.com/science/article/pii/S095741741730444X.

[31] Ransing RS and Rajput M (2015), Smart home for elderly care, based on Wireless Sensor Network. International Conference on Nascent Technologies in the Engineering Field (ICNTE), doi:10.1109/ICNTE.2015.7029932: 1–5.

[32] Regulation EU No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation) (2014), European Union: 44–59.

[33] Shi W, Cao J, Zhang Q and Li Y and Xu L (2016), *Edge Computing: Vision and Challenges*. IEEE Internet of Things Journal, doi:10.1109/JIOT.2016.2579198: 637–646.

[34] Shrier AA, Chang A, Landa F, Mayo J, van Riezen R and Hardjono T (2016), Blockchain and Health IT: Algorithms, Privacy, and Data. Office of the National Coordinator for Health Information Technology, available: https://www.healthit.gov/sites/default/files/1-78-blockchainandhealthitalgorithmsprivacydata_whitepaper.pdf.

[35] Sneps-Sneppe M and Namiot D (2012), M2M applications and open API: What could be next?. *Internet of Things, Smart Spaces, and Next Generation Networking*, Springer, available: http://link.springer.com/content/pdf/10.1007/978-3-642-32686-8.pdf#page=444: 429–439.

[36] Zyskind G, Nathan O and Pentland A (2015), Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Security and Privacy Workshops, doi:10.1109/SPW, **27**: 180–184.