Blockchain-based Electronic Patient Records for Regulated Circular Healthcare Jurisdictions

Sofia Alexaki
Ecole des Ponts Business School
Paris, France
s.alexaki@pontsbschool.com

George Alexandris, Vasilis Katos
Dept. of Computing and Informatics
Bournemouth University
Bournemouth, United Kingdom
galexandris@bournemouth.ac.uk,
vkatos@bournemouth.ac.uk

Nikolaos E. Petroulakis
Institute of Computer Science
Foundation for Research and Technology–Hellas (FORTH)
Heraklion, Crete, Greece
npetro@ics.forth.gr

Abstract— Circular, data-driven healthcare is increasingly being considered as an effective model to provide efficient, cost-effective and sustainable healthcare services in the future. Central to this model is the service-dominant "building-block"-type provision of care services to patients, paired with the collaboration of healthcare providers through a common infrastructure. This combination enables the forming of a decentralized, holistic care cycle. Sharing of patient medical information is pivotal towards reaching this goal; however, preserving medical record integrity and privacy, while at the same time allowing provider interoperability are often conflicting requirements. Blockchains and Smart Contracts can provide the underlying technology to support the decentralized care cycle by addressing patient privacy and medical record integrity, while simultaneously offering efficient interoperability between providers. To demonstrate how this could be achieved, a conceptual medical record access and sharing mechanism is presented which is suitable for a system operating within a regulated healthcare jurisdiction.

Keywords—Circular Economy, Blockchain; Smart Contracts; Healthcare.

I. INTRODUCTION

In recent years, the concept of 'Circular Economy', an economy restorative and regenerative by design [1], has evolved from a niche idea to an ambitious undertaking, shaping policies locally, nationally and internationally. This novel economic thinking is about introducing the notion of circularity, aiming to keep products, materials and components at their highest utility and value at all times. It is conceived as a continuous positive development cycle, reforming the current economy model of 'take-make-dispose', by preserving and enhancing natural capital, optimising resource yields and minimising system risks by managing efficiently finite stocks and renewable flows [2], [3]. In the context of healthcare, the target of achieving sustainability is particularly challenging, given the rising demand for healthcare services by a growing, and increasingly ageing population [5]. Simultaneously, healthcare expenditures are ballooning; the United States spent $10.348 per person in 2016, while the projected increase of expenditures for the average OECD country may be up to 40% by 2030 compared to 2012 [6] and as high as 72% for emerging economies like China [7]. The rising costs have already resulted in cuts in service capacity, and overcrowding [8]. To tackle this situation while adhering to the principles of a circular economy, researchers and analysts propose a profound change to existing healthcare business models [9], [10], moving from vertical siloed organizations to integrated, horizontal service-oriented cross-functional structures which can support modular "building block"-type of solutions [11]. The emphasis is on creating a platform which integrates various products and services to provide a full care cycle for patient conditions [9], enabling also further opportunities (e.g. in personalized healthcare [12], ambient assisted living [13] or sensor-based tele-health [14]), while simultaneously addressing environmental sustainability [15]. Crucial towards this direction is the necessity of an underlying IT infrastructure which facilitates sharing of information and promotes collaboration between multiple medical stakeholders such as patients, healthcare providers, regulators or insurance companies [16], [17]. In a user-centric system, data sharing should begin with the patient data itself; nevertheless, when it comes to documenting patient healthcare data, in most cases each provider keeps track of their own activities (e.g. diagnoses, prescriptions, clinical notes, etc.) on a proprietary patient healthcare record. At the same time, surveys have shown that quality of care improves considerably if providers and medical stakeholders share access to a patient's healthcare record [18]. However, despite recent advances in data standards for medical interoperability (e.g. FHIR [19]), sharing of records between providers is mostly uncommon for a variety of reasons, with the most frequent ones being:

- Business logic: Each provider has their own workflows regarding reading, editing and updating of healthcare records
- Trust: Providers need to trust each other to preserve an authoritative and up-to-date view records
- Privacy: What data can be shared with whom, and how medical conditions deemed sensitive by the patient (e.g. addictions) can be handled

Another, increasingly important downside of non-sharing of data is that the medical data repository becomes a single point of failure and can be targeted by attacker leading to ransomware attacks [20] or denial of services [21].

From the patient angle, what is commonly witnessed is that patient history is fragmented between many providers, forcing patients to piece together various information patches from disparate medical activities in order to create a continuous and consolidated view of their medical record [22]. This requires

effort on behalf of the patient, and the difficulties are compounded by real-world situations such as

- Complex medical cases spanning multiple and diverse activities
- Concurrent visits or treatments to different providers
- Medical history exceeding operational lifetime of provider
- Information exchange between international providers

Except from the logistical complexities described previously, patients cannot be fully assured that privacy provisions are in place. Specifically, there is no reliable way of knowing who has viewed their data and how their data is used. Taking this notion a step further, the patient is unable to actively manage permissions in a granular fashion in order to protect sensitive parts of her medical data. Consequently, in the current medical record management systems no trusted feedback exists as to who has accessed the data and which parts have been viewed. To summarize, it becomes clear that collaboration in the healthcare domain in order to achieve higher efficiencies and, ultimately, circularity, is not trivial, given the difficulties of sharing medical data while ensuring data integrity and protecting patient privacy. At the same time, we witness a paradox where patients, although central to the care process, have virtually no control over their data.

II. Application Description

A blockchain-based application can form the backbone of a decentralized healthcare platform shared by both patients and providers, acting (at least) as an interface to the patient's health record. Some of the benefits that it can offer are:

- All transactions (read/write) are immutably recorded
- No single authority has custody over the patient's record
- Increased resilience to failures or security incidents which can affect access to a patient's record
- Near real-time, common view of the state of a patient's health care record, accessible by all participating providers. This is especially important for critical health data
- "Smart Contracts" residing on the blockchain and owned by the patient can be used to control who is authorized to perform what

A. Working Context

Despite all benefits, due to inherent technological limitations stemming from a decentralized architecture, blockchains cannot effectively address every possible business case. Within the scope of this work, the problem space will be constrained to the requirements of regulated healthcare jurisdictions accountable to governmental authorities (i.e. public health and social insurance organizations), who, at the most fundamental level, maintain a jurisdiction-wide registry of enrolled beneficiaries and providers with the purpose of compensating providers for health services offered to beneficiaries. We examine the increasingly more common scenario where these authorities mainly act as regulators of health care services rather than providing health services directly to beneficiaries. This is a crucial point, as it allows authorities to move away from being the sole custodian of medical records. Instead, they can assume a role in overseeing the proper exchange and recording of medical services between beneficiaries and providers for all intents and purposes, not merely by compliance auditing "after the fact", but through active participation in the actual healthcare platform. With this in mind, we use the upcoming overhaul of National Health Insurance System of the Republic of Cyprus to comply with European Commission reforms [23], as a blueprint for operational requirements with respect to electronic healthcare record management.

Specifically, the medical records should contain (at least):

- Metadata of a patient-provider encounter (i.e. visit date/time, location, etc.)
- Codified symptoms / diagnoses in ICD-10 ("International Classification of Diseases") or ICPC-2 ("International Classification of Primary Care, Second Edition") for each encounter
- Codified undertaken activities (custom codification) for each encounter
- Prescriptions, lab orders and referrals to other providers
- Clinical notes for each encounter

With regards to medical records access management, the following rules apply:

- Beneficiaries should have complete access to their medical record
- Beneficiaries should be able to hide all or parts of the medical record
- Beneficiaries should be notified when a healthcare provider (e.g. a doctor) wishes to access their record
- Healthcare providers accessing a beneficiary's record should indicate a reason for access
- Beneficiaries should be able to view a complete history of who has accessed their record

It should be noted that the above requirements were postulated with the underlying assumption that the governmental authority acts as a gatekeeper and a repository to all medical records in a centralized fashion. As discussed in the previous section, this violates the principle of decentralization which is crucial to ensuring that patients retain control of their medical data and also for avoiding single failure points. In this light, a blockchain can help satisfy these requirements without resorting to a centralized architecture.

B. Participation Considerations

One of the main questions when designing a blockchain system is whether it should be public or permissioned. For the case of governmental health authorities, identification of all participants is mandatory. Therefore, it makes sense to opt for a permissioned blockchain, in order to benefit from a potential higher throughput as mentioned by Christidis et al in [24], given that identification of beneficiaries and providers needs to occur anyway in order to oversee health services and compensate for them. In

addition to identifying the blockchain participants, the authority can decide who can run blockchain nodes and validate transactions. In our opinion, blockchain transactions could be validated by a miner network formed by the authority itself, healthcare providers, authorized medical stakeholders (e.g. insurance companies) and other regulatory bodies. All the aforementioned participants have an interest in viewing the current state of beneficiary data, thus they are incentivized to maintain the decentralized network. Further participants can include consumer rights organizations, privacy watchdogs and other Non Governmental Organisations (NGOs). With regards to achieving privacy, opting for a permissioned platform facilitates the mandatory use of a trusted execution environment hardware for the computing nodes such as Intel SGX [25] and the use of lightweight cryptography and password hashing to provide confidentiality of user credentials in clients [26], [27]. Finally, an additional benefit of using a permissioned blockchain would be that the authority retains a degree of control over source code and blockchain governance.

C. *Smart Contracts*

The main building blocks of the application are implemented using Smart Contracts, a common term to describe stored programs on the blockchain which can be run by triggering a transaction to them. Smart contracts are uniquely addressable, can preserve state and execute in a prescribed manner within the virtual machine of the blockchain. The most prominent example of Smart Contract support is the Ethereum blockchain [28], which offers a Turing-complete programming language for programming complex logic in smart contracts. Smart Contracts can evolve in decentralized autonomous organizations (DAOs), a term describing contracts calling other contracts and depending on the outcome, are able to change their behaviour based on already encoded rules [29]. Within this work, Smart Contracts are implemented based on the Ethereum blockchain (or Quorum [30], its permissioned sibling) using the Solidity programming language [31]. The groundwork of the application is based on the following smart contracts which extend:

Identity Registry: A contract which contains the addresses (i.e. the public key) of all platform participants and maps them to a real-life identity. This includes beneficiaries, providers and other medical stakeholders (e.g. insurance companies). This contract is owned and managed by the regulating authority, in this case a governmental entity.

Patient Record: A contract which holds the actual medical data of the beneficiary. Every user with a beneficiary role has a patient record which is managed by herself. The patient record also covers cases where other providers are involved, e.g. purchasing prescribed drugs or taking lab tests. The contract is owned by the beneficiary.

Electronic Patient Record (EPR) Access Agreement: This is a contract – also in the literal sense – between a healthcare provider and a beneficiary, which determines in a granular fashion which parts of the patient record the provider can access. The access scope and the access conditions (e.g. time window) are described in this agreement. Further, the contract allows viewing of prescribed activities which should be performed by other providers. For example, this enables a clinical lab scientist to view what lab exams (e.g. coded in the "Logical Observation Identifiers Names and Codes" (LOINC) standard) have been ordered by a doctor in order to execute them. The contract is created and owned by the beneficiary, although it can be envisaged that another party creates this contract in case of an emergency treatment where the beneficiary is unable to perform this action.

Agreement List: A contract which can be either owned by the beneficiary or by the provider, and contains a mapping of all the owner's EPR access agreement addresses with other parties.

D. *Data Model*

A high-level depiction of the data model resulting from the smart contracts described above is depicted in Figure 1. The data rows are implemented in the Solidity programming language using the *mapping* construct for key-value pairs. Contracts can reference each other's location using the address type. In the example shown below, the Identity Registry references many Agreement-

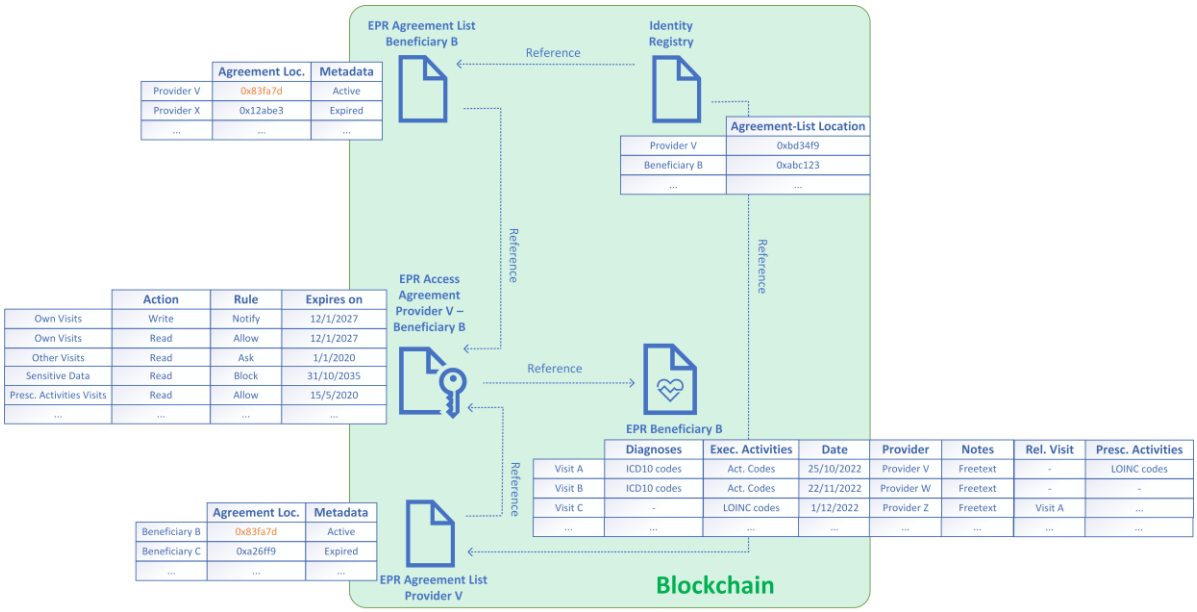

Figure 1: Data Model

Lists, which in turn reference many EPR Access Agreements. Finally, each EPR Access Agreement references a single Patient Record.

Agreements can be augmented with metadata denoting the validity of the agreement. The validity of the agreements is usually managed by the beneficiary and be cancelled, renewed or set to expire automatically after a certain period, thus capturing various business cases where a beneficiary terminates her association with the provider. Further to the validity of an agreement, functions can be added, as in the case of the EPR Access Agreement to fine-tune permissions, and notification patterns. These functions themselves can also be subject to validity constraints, which can be embedded into the function call using the Solidity *modifier* type, which can be used to turn functions "on" and "off", resembling contract "termination by right" [32].

The actual medical data is kept in the Patient Record contract using codifications for diagnoses, executed activities and prescribed activities. In our design, the patient-provider encounter (i.e. a visit) acts as the primary key for identifying and ordering a logical set of medical data, although other approaches are possible. Within a visit, two types of activities can exist: Executed Activities which denote actions undertaken during the visit, e.g. a Cardiac Stress Test, and Prescribed Activities which specify the actions proposed to be conducted by the beneficiary as a result of the visit, e.g. purchase of drugs, performing of lab exams. As mentioned previously, activities need to be codified for minimizing storage requirements (which is important for optimal blockchain operation), but also to be universally interpretable given that this is a shared record between medical stakeholders. Codification standards such as LOINC (for lab exams) or the European Union's "European Patient Smart Open Service" (epSOS) (for drug prescriptions) can be considered. Another aspect of prescribed activities is that at least two providers are involved; a prescribing provider (e.g. a doctor) and an executing provider (e.g. a clinical lab scientist), who need to exchange information about what actions need to be performed (e.g. blood tests) and the outcome of these actions (e.g. blood test results). The data model caters for this by having a different permissions category which allows an executing provider to view visits with activities available for execution. The executing provider can then add a new visit to the patient record which relates to a previous visit, and enter the results of the activities prescribed during that visit. The prescribing provider can then view the results of this new visit, since it relates to a visit which was recorded by herself.

E. Operative Cases

The proposed mode of operation of the system is illustrated using two common use cases which are detailed in this section.

1) Creating a Beneficiary-Provider Agreement for EPR Access

This use case is a prerequisite for all subsequent medical care actions by a specific provider. It also mirrors the concept of a "Personal Doctor" (or "Family Doctor"), where the beneficiary must be allocated to a doctor of first resort (Pediatrician, General Practitioner or Geriatrician depending on age of the beneficiary) due to jurisdictional requirements. Through the concept of a different EPR Access Agreement contract per provider described previously, the system supports that the Personal Doctor of the beneficiary can have increased access privileges to the medical record, as opposed to other providers.

The EPR Access Agreement contract is created by the provider, but is owned and controlled by the beneficiary. In order to create the agreement, the provider needs to look up the beneficiary's agreement list via the Identity Registry

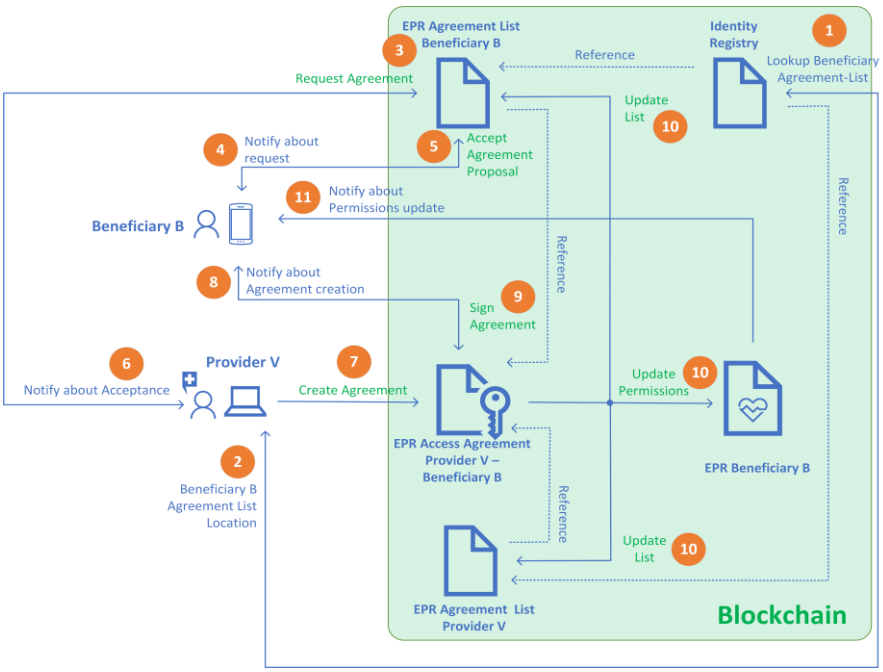

Figure 2: Provider requesting an EPR Access Agreement

contract and request to be added to it by calling an appropriate function in the Agreement List contract. This function, when called, notifies the beneficiary, who can accept or decline this request using an off-chain application. If the beneficiary accepts the request, the provider creates a new EPR Access Agreement contract and requests from the beneficiary to sign it. In signing the contract, the beneficiary also updates the permissions of her own Patient Record contract, granting the newly created EPR Access Agreement contract full or partial access to it. At the same time, both the beneficiary's and the provider's Agreement List contracts will be updated to reflect the new access permissions. The flow of the operation is illustrated in Figure 2.

Although there are several interactions depicted, only the ones in green will alter the state of the contracts and will be recorded on the blockchain. The other transactions can be logged by off-chain applications, depending on the preferences of the users.

2) Allowing a Provider to access an EPR

A provider may access a patient's EPR for various reasons, and depending on the provider's intent, the agreement contract can enforce rules for allowing or prohibiting access. The access rules of the contract can be managed directly by the beneficiary via an off-chain application. The same application can be notified by the agreement contract when access to the EPR is requested.

Access to a beneficiary's Patient Record contract by a provider occurs only via the EPR Access Agreement contract. Consequently, whenever a provider wishes to access the Patient Record contract she should first locate the EPR Access Agreement contract for this beneficiary in her own Agreement List contract. Once the contract is located, the provider calls a function in the EPR Access Agreement contract which performs the sought action with respect to the patient's medical record (e.g. retrieve data about a previous visit). After successfully validating the permissions of the caller, the function emits an event to notify the beneficiary about the EPR access and calls the appropriate function in the Patient Record contract, which returns the requested data. Figure 3 shows in more detail the sequence of actions which need to be performed in order to access the medical record.

Similar to the previous flow in Figure 2, only the transactions in green will alter the state of the contracts and will be recorded on the blockchain.

3) Further Additions

Besides the underlying structure for regulating access to a beneficiary's medical record, additional off-chain modules need to be implemented in order to offer the required functionality to all blockchain participants (Beneficiaries, Providers, Regulators) in a user-friendly manner. Specifically, client applications are needed which will:

- Retrieve the beneficiary medical history from the Patient Record contract and present it in a meaningful way
- Allow the beneficiary to manage existing Patient Record contract permissions
- Allow providers to view and update Patient Record information
- Allow the beneficiaries and providers to create, manage and view EPR Access Agreements with each other
- Allow regulators to manage the beneficiary and provider identities in the Identity Registry

These applications can be web-based and should follow the "Distributed Application" (or "DApp") paradigm [33], and communicate with the contracts via blockchain-specific libraries (e.g. web3.js for the Ethereum blockchain [34])

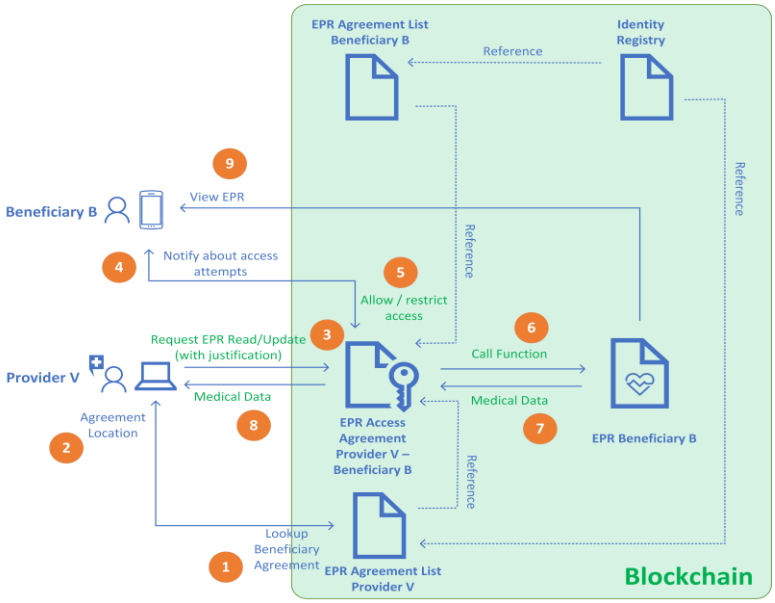

Figure 3: Provider accessing an EPR

III. Conclusion

Blockchains are a powerful technology which introduces new levels of data sharing, transparency and control. Specifically in the domain of digitized health data, blockchains can act as an enabler for a new breed of

circular, decentralized systems and applications. Governmental health authorities by virtue of their role as a regulator, can leverage the benefits of blockchains while retaining a sufficient degree of control over the blockchain application. This makes a common view of patient data accessible by all providers possible, while at the same time, ensures that patients retain complete control of their medical record. For the latter part, Smart Contracts play a pivotal role towards offering granular and dynamic control of a patient's record. We have shown that the combination of Blockchains and Smart Contracts are flexible enough to satisfy the main requirements for implementing, accessing and sharing patient records. As such, they represent an attractive and arguably more efficient alternative to centralized systems for health regulators for creating a platform to offer modular, and interoperable healthcare services, thus providing the necessary collaborating mechanism to enable circularity.

REFERENCES

[1] K.Hobson. Closing the loop or squaring the circle? Locating generative spaces for the circular economy. Progress in Human Geography Vol 40, Issue 1, 2015. pp. 88 - 104

[2] World Economic Forum. The Fourth Industrial Revolution 'is already here – and it is a matter of survival' (Press release, 26 October 2015)

[3] Ellen MacArthur Foundation. Towards the Circular Economy: Economic and Business Rationale for an Accelerated Transition (2015)

[4] A. Tukker. Product services for a resource-efficient and circular economy - A review. Journal for Cleaner Production Vol. 97, 2015, pp 76-91

[5] World industry outlook: Healthcare and pharmaceuticals, The Economist Intelligence Unit, May 2014

[6] http://www.oecd.org/els/health-systems/health-data.htm

[7] L. Lorenzoni et al. Public Expenditure Projections for Health and Long-Term Care for China Until 2030. OECD Health Working Papers, No. 84, OECD Publishing, Paris. 2015

[8] K. Xing, M. Rapaccini, F. Visintin. PSS in Healthcare: an under-explored field. Procedia CIRP. 64. 241-246. 10.1016/j.procir.2017.03.068.

[9] E. Porter, Michael & Lee, Thomas. The Strategy That Will Fix Health Care. Harvard Business Review. 91. 2013

[10] Deloitte. Global health care outlook Common goals, competing Priorities. 2015

[11] J. Marceau, E. Basri. Translation of innovation systems into industrial policy: the healthcare sector in Australia. Industry and Innovation Vol. 8, no. 3 2001, pp. 291-308;

[12] M. H. Yip, R. Phaal and D. R. Probert, "Stakeholder engagement in early stage product-service system development for healthcare informatics," 2013 Proceedings of PICMET '13: Technology Management in the IT-Driven Services (PICMET), San Jose, CA, 2013, pp. 2564-2574.

[13] V. Moumtzi and C. Wills, "Utilizing living labs approach for the validation of services for the assisting living of elderly people," 2009 3rd IEEE International Conference on Digital Ecosystems and Technologies, Istanbul, 2009, pp. 552-557.

[14] P. Flores-Vaquero, A. Tiwari, J. Alcock, W. Hutabarat, C. Turner. A product-service system approach to telehealth application design. Health Informatics Journal 2016; 22(2):321-332.

[15] J. Moultrie, L. Sutcliffe, A. Maier. Exploratory study of the state of environmentally conscious design in the medical device industry. Journal of Cleaner Production Vol. 108 Part A, 2015 pp 363-376.

[16] P.A. Tilmann, P. Tzortzopoulos, C.T. Formoso. Redefining healthcare infrastructure: moving toward integrated solutions. Health Environment Research & Design Journal 2010; 3(2):84-96

[17] R. Breitschwerdt, S, Robert, O. Thomas. Mobile Application Systems for Home Care: Requirements Analysis & Usage Potentials. AMCIS 2011 Proceedings - All Submissions. 152.

[18] Jan Walker, Michael Meltsner, Tom Delbanco. 2015. US experience with doctors and patients sharing clinical notes. British Medical Journal, BMJ 2015;350:g7785 https://doi.org/10.1136/bmj.g7785

[19] HL7 International. Fast Healthcare Interoperability Resources. https://www.hl7.org/fhir/

[20] Ransomware attack breaches 128,000 patient records at Arkansas provider. http://www.healthcareitnews.com/news/ransomware-attack-breaches-128000-patient-records-arkansas-provider.

[21] DDoS attack hits Latvia's national 'e-health' system. https://eng.lsm.lv/article/society/health/ddos-attack-hits-latvias-national-e-health-system.a264478/

[22] Kim M. Nazi et al. 2015. VA Open Notes: exploring the experiences of early patient adopters with access to clinical notes. Journal of the American Medical Informatics Association, Volume 22, Issue 2, 1 March 2015 https://doi.org/10.1136/amiajnl-2014-003144

[23] Christos Koutsampelas, Panos Pasharedes. 2017. A bold step towards reforming healthcare in Cyprus. European Commission, ESPN Flash Report ec.europa.eu/social/BlobServlet?docId=17892&langId=en

[24] Konstantinos Christidis, Michael Devetsikiotis. 2016. Blockchains and Smart Contracts for the Internet of Things. IEEE Access, Vol. 4 2016

[25] V. Costan, S. Devadas. Intel SGX Explained. Computer Science and Artificial Intelligence Laboratory Massachusetts Institute of Technology

[26] H. Manifavas, G. Hatzivasilis, K. Fysarakis, K. Rantos. Lightweight Cryptography for Embedded Systems – A Comparative Analysis. SETOP 2013, Springer, LNCS, vol. 8247, pp. 333-349

[27] G. Hatzivasilis. Password-Hashing Status. Cryptography, vol. 1, no. 2, p. 10, Jun. 2017

[28] Vitalik Buterin. A next-generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/White-Paper

[29] Ethereum Foundation. Decentralized Autonomous Organization. https://ethereum.org/dao

[30] JP Morgan Chase. Quorum, a permissioned implantation of Ethereum supporting data privacy. https://github.com/jpmorganchase/quorum

[31] Solidity. A contract-oriented high-level language for implementing smart contracts. http://solidity.readthedocs.io/en/v0.4.21/

[32] Bill Marino, Ari Juels. 2016. Setting Standards for Altering and Undoing Smart Contracts. International Symposium on Rules and Rule Markup Languages for the Semantic Web RuleML 2016

[33] ConsenSys. Dapp Architecture Designs. https://github.com/ConsenSys/Ethereum-Development-Best-Practices/wiki/Dapp-Architecture-Designs

[34] web3.js Ethereum JavaScript API. https://web3js.readthedocs.io/en/1.0/