# Towards digitalisation of healthcare policies: case for smart legal contracts?

Zoran Milosevic [1,2]
[1]Deontik, Australia
[2]Institute for Integrated and Intelligent Systems, Griffith University, Australia

*Abstract* — **We present an approach for the digitalisation of healthcare policies based on our work on the formalisation and implementation of digital contracts. An abstract policy language is proposed leveraging the semantics of the RM-ODP enterprise language standard and augmented with the latest research in deontic logic. Several digital contract languages, considered as ledger agnostic smart legal contract languages, are identified as candidates to implement this policy language. We use healthcare consent policies included in the HL7 FHIR consent resource to test our approach.**

***Keywords – digital health policy; smart legal contracts; distributed ledger; blockchain; RM-ODP; FHIR.***

## I. Introduction

Healthcare policies describe constraints associated with clinical and administrative activities in healthcare, as well as constraints on the collection, exchange and use of healthcare data for different purposes. This paper presents an approach to the problem of digitalisation of healthcare policies, covering their translation from natural language to a digital format and then using this format to integrate policy expressions across systems and stakeholders involved in digital health. This approach leverages our experience in analysing healthcare policies and developing their computable expressions in the context of national and international e-health interoperability frameworks, most of which follow architecture guidelines of the Reference Model for Open Distributed Processing (RM-ODP)[1]. We propose an *abstract policy language* that makes use of RM-ODP and our earlier research related to the specification of digital contracts[3][5][7].

We investigate the applicability of some *digital contract languages* as candidates to implement the abstract policy language. Specifically, we focus on digital contract languages developed with distributed system principles in mind[3][28] because they could be treated as *smart legal contracts* to be deployed on different distributed ledger (DL) platforms, if required. Smart legal contracts are a new area of inquiry[6][16] aimed at extending DL-based smart contracts with legal constraints. Note that smart contracts [12][13] are computerized transaction protocols that either control workflow to ensure contract compliance or monitor contract conditions to detect and address breaches. They are not contracts in the legal sense.

A concrete policy language can then be used to express computable healthcare policies and these policies can be evaluated in a smart contract platform. This evaluation could apply DL technologies to provide an immutable audit trial of actions. The ultimate goal is to support policy enforcement either on a discretionary basis, where humans audit and follow-up potential policy violation flags or notifications, or non-discretionary, for example through controls on actions in a workflow engine.

We use the abstract language to capture policies that reflect consent specified using the HL7 Fast Health Interoperability Resource (FHIR) standard, namely the FHIR consent resource specification [2], which permits description of different healthcare consent policies including their legal aspects.

The following section provides motivation for this work, highlighting the increasing concerns of consumers and regulators about privacy and consent for digital health information. Section III provides examples of use of DLs in healthcare. Section IV introduces several healthcare consent policies from the FHIR consent resource used to test our approach. Section V presents key modelling concepts we use to describe policy. Section VI presents our approach to expressing these concepts in an abstract policy language and identifies candidate digital contract solutions to implement this language. Section VII discusses architectural options for using distributed ledger technologies. Section VIII describes related work. Section IX outlines future work.

## II. Motivation

This paper is motivated by the need to provide an increasing level of automation of healthcare policy monitoring, enforcement and integration with digital health platforms. This topic is traditionally addressed in the context of information security [3] but is increasingly considered in higher-level policies that are associated with healthcare delivery, such as informed consent. This is a process for getting permission before conducting a healthcare intervention on a person, or for disclosing personal information [30][31]. The latter policy is often referred to as *privacy consent*, i.e. defining how Individually Identifiable Health Information is to be collected, accessed, used and disclosed.

The clear expression of policies is also needed to increase trust among consumers and carers, where the question of access to information can be delegated based on various rules and regulations, including in acute and community care contexts.

Healthcare policies are described in a style similar to a legal contract, specifying obligations of providers or carers in the delivery of healthcare to individuals, as well as their permissions, authorisations or prohibitions. These policies reflect regulatory, legislative or organisational contexts. Our approach to capturing legal semantics for the abstract policy language is by leveraging the formalism of the recent Enterprise Language standard [9] from the RM-ODP family of standards [10], which makes use of formalisms from deontic logic and normative systems, while providing explicit support for distributed and federated infrastructures. Further, we consider use of domain specific languages for digital contracts as concrete languages to realise the abstract policy language. This in turn motivates us to consider smart legal contracts, serving as a link with DLs, and explore the use of smart legal contracts for digital health applications.

Some digital contract languages considered inherently support legal semantics, e.g. Business Contract Language (BCL) [3][5][7][28] and logic-based Formal Contract Language (FCL) [5][7], while others can be extended with legal support, e.g. Contract Specification Language (CSL) [14]. These languages can be mapped to different DLs and that they are declarative, as opposed to smart contracts which are typically imperative languages [8].

## III. Distributed ledgers and smart contracts in healthcare

### A. Current use cases and early solutions

Primary use cases identified in early surveys on the topic are managing clinical trial records, regulatory compliance, and managing medical/health records [18]. Additional use cases include tracking and tracing pharmaceuticals, such as for the so called "cold chain break". This refers to the problem of vaccine degradation due to them being stored in temperatures that are too hot, too cold, or exposed to ultraviolet light [19]. DLs can provide increased trust through consensus, provenance and supply chain immutability across the players involved, i.e. manufactures, public health authorities, central purchasers and auditing organisations.

Three further use cases were identified in [21]. The first is legal assurance on audit trails, to ensure that an audit trail has not been tampered with. Examples are compliance with GPDR removal-of-data requests, keeping records around infection control, and about cases of sexual abuse or other criminal behaviour. Note that the existing trust environment does not require voting/contest activities for creating new blocks. The second use case is a need for legally established trust, where DLs can be used to support the establishment of a legal agreement so that all parties involved are given confidence that true sharing of information would occur without the agreement giving advantage to any of the players involved. The subsequent information sharing as specified in the agreement does not need to involve a DL. The third use case is Clinical Credential Tracking, in particular in the USA.

There are an increasing number of open source blockchain initiatives in healthcare, as captured in the corresponding landscape map [22]. Some efforts propose the development of *utility tokens* as a way of supporting economic transactions on the web [29].

There are interesting recent use cases related to the opportunities arising from integration between blockchain and AI [33] with relevance for healthcare. For example, blockchain can be used to help in addressing AI explainability problems based on audit trails, and to support new ways of patients sharing of information for research purposes, some of which may involve monetization of patient data.

There have been interesting experiments with the use of blockchain in the context of the Australian MyHealthRecord (MyHR) [24]. The experiments were aimed to allow researchers to access medical information contained within MyHR, but uncertainty around current Australian legislation for the secondary use of data [25], suggests that these developments require a stable legal/regulatory framework before further investment.

In relation to smart contracts, there is limited published work regarding their use in healthcare. One notable exception is the use of Etherium smart contracts to facilitate secure analysis and management of remote medical sensors, arising from the Internet Of Things and other patient remote monitoring systems, as reported in [20]. In this system the sensors communicate with a smart device that calls smart contracts and writes records of all events on the blockchain. The solution supports patient monitoring and medical interventions by sending notifications to patients and medical professionals, while also maintaining a secure record of who has initiated these activities. The aim is to address many security vulnerabilities associated with remote patient monitoring and automate the delivery of notifications to all involved parties in a HIPAA-compliant manner [20].

### B. Considerations for use

The above examples are mostly research or experimental projects, and it can be said that DLs and smart contracts are not yet widely used in healthcare despite a certain level of hype surrounding the technology. Perhaps we will see some small changes in short term and bigger changes in longer term, as per Amara's law: "We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run" [27].

In order to help make optimal decisions about the use of these technologies in healthcare, it would be useful to have a framework for managers, architects and developers to identify circumstances under which the value of these technologies outweighs costs. A valuable source of information is the recently published NIST guide, which includes high-level guidelines for determining whether a DL might be valuable for a development initiative [23], as opposed to database solutions. Many of these guidelines would be useful for healthcare but with relaxed constraints related to trust. This is because in healthcare there are trusted institutions like hospitals or national bodies who can be relied on to verify the integrity of ledgers. This would mitigate the cost of the establishment and maintenance of trusted blockchain infrastructure, including some of the wastefulness of blockchain consensus mechanisms such as proof-of-work mining. We note that the recently established DeepMind verifiable Data Audit project [26], is aimed in further improving trust, and they are developing its own ledger for the data audit purpose.

Much of the NIST guidelines are used in the context of supporting immutable and tamper-proof storage of data. We believe that there is a value in additional guidelines for the use of smart contracts and potential support for automation of certain processes in healthcare. For example, the existing efforts to map traditional process languages onto smart contracts can be a useful starting point here [17]. This is of relevance for those healthcare processes that can be standardised, yet supporting variability for personalisation purposes. Early candidates are financial and supply chain processes, followed by referrals, discharge and care plan. In doing so however, one needs to carefully consider the impact of non-digital transactions as they prevail in healthcare. If the transactions are not digital, smart contracts have limitations in executing the transactions. Rather, they can capture a trusted, immutable record of execution. This applies to human-initiated actions, but even for a sensor reading, for example: the reading has already occurred and the ledger is just recording the occurrence afterwards. A real-time monitoring system cannot wait for consensus before delivering an alert. In fact, there are many situations where traditional smart contracts paradigm might not be necessary and can be replaced with the usual process definitions.

In many cases however, there is a value in considering how legal contracts can be translated into compliant processes [7]. This is because current process languages do not support expression of legal constraints over the activities in a process. Our earlier work provides many contributions in this respect [28].

## IV. Example: Consent policies

An important healthcare policy relevant to many healthcare episodes is that of a *consent*. Several definitions related to consent are listed below, as given in [2]. These introduce the key policy concepts to be discussed in more detail in the reminder of the paper. Consent is defined as:

*The record of a healthcare consumer's policy choices, which permits or denies identified recipient(s) or recipient role(s) to perform one or more actions within a given policy context, for specific purposes and periods of time.*

Note the generic nature of this definition, because actions can apply to both actions associated with information management and healthcare.

Further, the policy choices are typically captured in an agreement referred to as a Consent Directive, defined as:

*The legal record of a healthcare consumer's agreement with a party responsible for enforcing the consumer's choices, which permits or denies identified actors or roles to perform actions affecting the consumer within a given context for specific purposes and periods of time*

Next, various consent related options are typically specified in Consent Form, defined as:

*Human readable consent content describing one or more actions impacting the grantor for which the grantee would be authorized or prohibited from performing. It includes the terms, rules, and conditions pertaining to the authorization or restrictions, such as effective time, applicability or scope, purposes of use, obligations and prohibitions to which the grantee must comply. Once a Consent Form is "executed" by means required by policy, such as verbal agreement, wet signature, or electronic/digital signature, it becomes a legally binding Consent Directive.*

There are different types of consent directives in [2]

- Privacy Consent Directive: Agreement to collect, access, use or disclose (share) information.
- Medical Treatment Consent Directive: Consent to undergo a specific treatment or record of refusal to consent.
- Research Consent Directive: Consent to participate in a research protocol and its information sharing.
- Advance Care Directives: Instructions for potentially needed medical treatment, e.g. do-not-resuscitate.

The consent directives above include a set of conditions that, when considered together, constitute elements of a legally binding contract. Thus we suggest the use of contract language formalisms developed elsewhere to model this consent policy.

Note several concepts common to the above definitions and typically used in many policy specifications, namely:

- *Roles* to which policies apply when participating in actions, e.g. grantor and grantee
- *Policy constraints*, e.g. authorisation, prohibition, permission, obligation
- *Policy context* surrounding roles, actions and policy constraints, e.g. purpose of the consent and the legal jurisdiction defining the conditions for legally binding status.

The following section provides a precise description of these policy concepts based on the modelling languages specified in the RM-ODP [9][10].

## V. Policy concepts formalisation

The following is a list of key policy modelling concepts from RM-ODP enterprise language [9], selected to illustrate their use in modelling consent policies.

### A. Policy context

The central part in defining many policies is the specification of *constraints* on the actions of the *parties* who participate in interactions defined by some normative context. This context specifies rules of interactions and can be modelled through the use of the RM-ODP concept of *community*, describing the organisational or social environment for the participants involved.

A community defines how a set of participants should behave in order to achieve an objective. To make the rules reusable, a community is defined in terms of interactions between *roles* in the community, and policy constraints that apply to the roles [10]. A community role can be played by a *party*, which models a natural person or legal entity (see V.C). A role in a community can also be played by another community, making it possible to model hierarchical policy contexts.

RM-ODP supports the expression of more complex, cross-organisational interactions, and the associated policy constraints, through the concept of *federation*. Formally, <X> federation is defined as a community of <X> domains, *formed to meet a shared objective*, where a domain is a set of objects related by a characterising relationship to a controlling object. Note that in enterprise terms, policies can be administered by the controlling object over the domain. The capability to express federation is critical for healthcare in view of the need to manage the combined actions of private and public stakeholders within health sector and across other sectors.

### B. Deontic constraints

There are three fundamental types of constraints that reflect rules of any normative system, namely *obligations*, *prohibitions* and *permissions*. Their formal expression is the subject of deontic logic and these are often referred to as *deontic constraints*.

An *obligation* is a prescription that a particular behaviour is required. An obligation is fulfilled by the occurrence of the prescribed behaviour.

A *permission* is a prescription that a particular behaviour is allowed to occur. A permission is equivalent to there being no obligation for the behaviour not to occur.

A *prohibition* is a prescription that a particular behaviour must not occur. A prohibition is equivalent to there being an obligation for the behaviour not to occur.

These constraints provide a foundation for expressing more complex policies such as accountability concepts [9], a subset of which, relevant for this paper, is described next.

### C. Accountability concepts

A *party* is an enterprise object which models a natural person or any other entity considered to have some of the rights, powers and duties of natural person, e.g. company.

An *authorization* is an action indicating that a particular behaviour shall not be prevented. Unlike a permission, an authorisation is an empowerment, representing a permission provided by another party (e.g. a principal) to the party being authorised (e.g. an agent).

A *delegation* is an action that assigns something such as an authorization, responsibility or provision of a service to another object.

### D. Implications for smart contracts – legal extensions

The deontic constraints provide the foundation for expressing many legal aspects that characterise various legal instruments, including organisational, regulative or legislative policies. These constraints and policy context need to be superimposed on the specification of basic behaviour such as business interactions and processes [28].

Considering that current smart contract proposals are a form of a basic behaviour, e.g. a finite state machine, specifying a sequence of events or state changes that reflect agreements between parties [12][13], deontic constraints can be superimposed on smart contracts. We refer to such smart contracts as *smart legal contracts*.

Smart legal contracts require an appropriate policy language to provide constraints over smart contract events.

## VI. Policy language

This section shows how policy concepts described can form part of an abstract policy language. It then illustrates its use with several consent policy examples and identifies several concrete smart legal contract languages that could be used to implement this abstract policy language.

### A. Abstract policy language

The first element of our policy language is the concept of policy *context* as defined by the ODP concept of *community* as introduced in section V.A. The second element is further refinement of the deontic constraints [3], in terms of the behavioural modelling concepts listed next:

- triggering conditions which signify that normative policies are in force, i.e. a policy activation trigger; these can be temporal events or other events, such as violation of other policies; this provides support for dynamic activation of policies triggered by various conditions such as timeouts or violations of other policies, that activate the policy in question (e.g. contrary to duty deontic logic constraint),
- a role to which modality and behavioural constraints apply (defined by the community context), thus defining deontic constraints for the role,
- deontic modality that applies to the party fulfilling a community role, e.g. an obligation, permission or prohibition; a deontic modality can explicitly identify a target role referenced by the subject role in a modality expression,
- constraints on behaviour, typically expressed in terms event patterns [11]; the event pattern describes the expected behaviour of the party in question in terms of their actions and other occurrences such as expiration of deadlines, or actions of other parties; detailed descriptions of different types of event patterns is beyond scope of this paper, and can be found in [3],
- violation conditions specifying other policies that can be triggered in response to a violation of the primary deontic modality; this allows linking of the primary policies and those activated when violations occur.

Consequently, a high-level expression of a general policy constraint is of the following form:

*<communityContext><policyActivation><role><modality>*
*<event_pattern><target_role><violation>*

### B. Example1: privacy consent policy

Privacy consent policy, would thus look like:

*<ConsentContext><consentCreation>*
*<grantor><permission><accessPatentInfo>*
*<grantee>*
*<violation>*

In the above, *accessPatentInfo* specifies an event pattern, such as the period for which the consent was given and its purpose, e.g. access to a specific IT or physical resource (not included in the policy expression for simplicity).

This general consent statement can be instantiated for a specific consent policy instance. Consider a simple example, related to a personally controlled EHR:

"A consumer Bob grants permissions to an emergency clinician to access his EHR record, in case of emergency."

*<EDcare><emergencyPresentation><Bob><permission>*
*<accessEHRRecord><accreditedEmergencyClinician><>*

This policy is activated by *emergencyPresentation* event, which can be selected from a set of possible triggering events, that can be defined at an organisational, state or national level, possibly as part of a personal health record. The policy assumes the existence of patient identifier framework, e.g. Individual Health Identifier in Australia.

### C. Example 2: Advance care directive

Another example is advance care directive policy that authorises a substitute decision-maker, i.e. a person permitted under the law to make decisions on behalf of someone who does not have capacity, namely:

*<AdvancedCareContext><AdvancedCareDirectiveCreation>*
*<Grantor><authorise><MedicalDecision>*
*<SubstituteDecisionMaker>*

*<Legislation><obligation>*
*<actResponsibly><Grantee>*
*<violationConditions>*

The example illustrates the use of a care policy, and include authorisation for the Grantee to make a medical decision for the Grantor. The example also illustrates one obligation that applies to the Grantor, as defined by the other community referred to as Legislation, as well as a number of violation conditions, that may either activate some other policies, or generate alarms that may involve human decision makers, with potential escalations actions.

### D. *Example 3: Research consent directive*

This example is applicable in cases where an individual wishes to give permission to a research organisation to access their data, typically de-identified, for specific research purposes.

```
<ReserachConsentContext>
        <ResearchConsentDirectiveCreation>
                <Patient><authorise>
                <usePatientData><ResearchOrg>

                <ResearchOrg><obligation>
                <payForDataAccess><Patient>
        <violationConditions>
```

For simplicity, we do not specify the purpose element of the policy expression but we note that audit trails can be used to infer the purpose based on the trace of events. Delegation will be described in a longer publication.

### E. *Smart legal contract options*

This abstract policy language can be implemented using concrete domain specific languages that support deontic constraints in specification of business contracts (Fig1). Potential candidates are BCL [3] and FCL [5].

BCL uses event patterns to specify triggering, behavioural and violation conditions for the policy language, and adopts event and policy semantics from the RM-ODP enterprise language semantics [9]. Note that a similar event pattern language was successfully used in supporting real-time analytics solutions [11]. In our earlier work we showed how it is possible to add BCL constraints to a choreography language and engine, supporting implementation of processes without centralised control. The details of this solution are beyond the scope of this paper, but suffice to say, that proposal allows embedding legal-style of expression within many distributed infrastructures [28]. Although this research was performed prior to the emergence of DL technologies, much of the solution elements are applicable to distributed ledgers.

FCL is formal, defeasible deontic logic-based language that can be used to support contract reasoning. FCL also has a well-developed mapping to BCL [5].

Another candidate is Contract Specification Language (CSL) [14], a functional based language, based on event trace semantics. CSL requires certain extensions to support deontic constraints, as per our analysis carried out with Deon Digital, a Swiss company further developing CSL, as a contract language agnostic of any distributed ledger.

Full evaluation of the use of these languages is beyond the scope of this paper, but the snippet below shows the use of BCL for implementing policy in VI.B:

```
CommunityTemplate: EDCare
  ActivationSpecification: EmergencyPresentation
   Policy: PrivacyConsent
     Role: Patient
     Modality: Permission
     TargetRole: accreditedEmergencyClinician
     Condition:
          On EDPhysicianRequestEvent
                accessEHRRecord
```

Once policies are expressed in BCL or FCL, the policy rules can guide the translation into compliant processes, but this is not trivial as there are many possible sequences of activities to realise a contract, as discussed in [7].

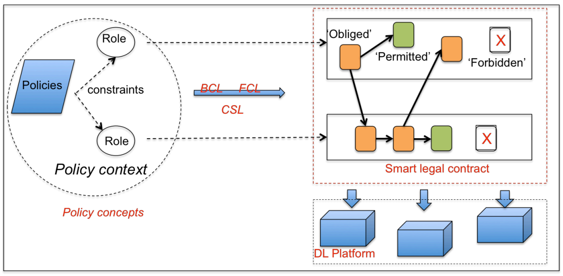

**Figure 1: From policy modelling concepts to smart legal contracts**

## VII. Distributed Ledger options

In many digital health systems it is valuable to use digital policy expressions to facilitate out-of band *monitoring* of activities of the parties against policy rules. This provides many benefits, such as faster reaction to important events that might signify occurrence of medical conditions requiring action, or detecting potential breaches of policies. This is typically done by a trusted third party, which can take the role of a monitor. Once the monitor detects a contract breach it can invoke various discretionary or non-discretionary enforcement options. This can but does not have to involve smart contracts, and depending on trust one may use public or private ledgers.

In some situations it is also possible to consider the use of DL technologies as a platform for supporting *execution* of processes governed by smart legal contracts. This execution can also embed monitoring and enforcement functionality, also discussed in [28].

While such contracts offer limited advantages for the examples presented, they could be used in activities such as procurement, where the automation of supply chain activities is likely to bring significant savings, or in in support of audit trails, as discussed in III.A. There is value in combining distributed ledgers and off-chain solutions. An interesting example is the use of FHIR servers, which contain patient information, with blockchain platform, which enforces legal rules of research consent directive, between the patient and research organisation [15].

## VIII. Related Work

To the best of our knowledge there are no specific policy formalisms that are focus on healthcare policies and the use of existing general policy formalisms from other standards. RM-ODP, as used in this paper, or OMG's SBVR [32] are good starting points.

There are several proposals for providing higher level, business process expression of agreements between parties and mapping them onto specific smart contract solutions, such as the proposal in [17]. These however, do not consider adding legal constraints to process descriptions.

In terms of smart legal contracts, there are preliminary discussions from the finance industry [16] and recent broader industry proposals in Australia [6]. Our own earlier work provides solutions in this regard [28]. These are only preliminary suggestions and much remains to be developed to raise the level of abstraction to accommodate the expression of legal constraints over business processes and thus support the expression of smart legal contracts.

## IX. Conclusions and Future Work

This paper provides our early thoughts about digitalisation of healthcare policies and using smart legal contracts to support policy implementation over processes in healthcare. The availability of such smart legal contracts would facilitate better collaboration among patients and clinicians, in a policy compliant manner.

In the future, we plan to engage clinical and health policy experts in detailed consultations about the form and usability of the policy language, and leverage the latest design thinking practice as a vehicle to deliver rapid and stakeholder relevant policy language solutions.

We intend to develop a detailed mapping from our abstract policy language to BCL, FCL and CSL languages, and general purpose smart contract languages, e.g. Solidity [12] and Hyperledger Fabric [13]. Further, we will investigate applicability of our earlier work on extending choreography with business contracts constraints [28] in the distributed ledger context.

We also plan to explore other uses of smart legal contracts as part of decentralised and federated health system, and the suitability of off-chain or hybrid solutions. For example, there might be value in specifying smart legal contracts purely for cross-organisational interactions (i.e. BPMN public processes) but leave the internal processes (i.e. BPMN private processes) performed off chain. We also intend to look into specific deployment scenarios, where smart legal contracts can be used to support reliable transfer of responsibility across providers within soft and hard time limits while ensuring provenance of data exchanged, e.g. in referrals. Another scenario is to support research consent contracts for analytics and AI purposes, the terms of which can change over time to reflect changing patient circumstances.

We note that there is no standard reference architecture model for analysing, designing and implementing DL and smart contracts. We plan to investigate the value of the RM-ODP standards for this purpose [9][10], as they provide a solid basis for describing and building widely distributed and federated systems systematically [10].

Finally, we are interested in applying this general policy framework to newly proposed approaches within the FHIR community for the specification of workflow patterns and as well as FHIR contract resource.

## Acknowledgment

I would like to thank Dr Andrew Berry (Deontik) for his input to the earlier version of this paper, to Dr Florian Herzog (Deon Digital) for fruitful discussions about the importance of legal semantics to smart contracts, and an anonymous reviewer who suggested adding information about using blockchain for handling healthcare data. I would also like to thank Grahame Grieve (Health Intersections), for his insights regarding the FHIR consent resource and use of blockchain in healthcare, and for his outstanding technical contribution, vision and efforts in driving the FHIR agenda.

## References

[1] Z. Milosevic, A.Bond, *Digital health Interoperability frameworks: use of RM-ODP standards*, IEEE EDOC SoE4EE workshop, 2016.

[2] FHIR Consent Resource, https://www.hl7.org/fhir/consent.html

[3] PF Linington, Z Milosevic, J Cole, S Gibson, S Kulkarni, S Neal, *A unified behavioural model and a contract language for extended enterprise*, Data & Knowledge Engineering 51 (1), 5-29

[4] Z. Milosevic, D. Arnold, L. O'Connor, *Inter-enterprise contract architecture for open distributed systems: Security requirements*, WETICE 1996

[5] G. Governatori, Z. Milosevic, Dealing with contract violations: formalism and domain specific language, IEEE EDOC2015.

[6] New blockchain-based smart legal contracts for Australian businesses, Data61, https://www.csiro.au/en/News/News-releases/2018/New-blockchain-based-smart-legal-contracts

[7] Z. Milosevic, S. Sadiq, M. Orlowska: *Translating business contract into compliant business processes*, IEEE EDOC2006 Con.

[8] G. Governatori, F Idelberger, Z Milosevic, R Riveret, G Sartor, X Xu, *On legal contracts, imperative and declarative smart contracts, and blockchain systems*, AI and Law, 1-33, 2018

[9] ISO/IEC 15414, Information technology: Open distributed processing, Reference model – Enterprise Language, 3rd ed, 2015.

[10] P.F. Linington, Z. Milosevic, A. Tanaka and A. Vallecillo, *Building Enterprise Systems with ODP, An Introduction to Open Distributed Processing*, Chapman & Hall/CRC Press, 2011.

[11] A.Berry, Z. Milosevic, *Real-time analytics for legacy data streams in health: monitoring health data quality*, EDOC2013

[12] Solidity smart contracts, Etherium, https://www.ethereum.org

[13] Hyperledger, Architecture, Smart contracts, hyperledger.org

[14] J. Andersen, E. Elsborg, F. Henglein, J.G. Simonsen, C. Stefansen, Compositional specification of commercial contracts, Int. J. Softw. Tools Technol Transfere (2006) 485–516.

[15] healthcaresecprivacy.blogspot.com/2018/08/blockchain-for-patient-to-sell-their.htm

[16] ISDA Linklaters Whitepaper, Smart Contracts and Distributed Ledger – A Legal Perspective, Aug 2017

[17] O. López-Pintado, L. García-Bañuelos, M. Dumas, I. Weber, A. Ponomarev, *CATERPILLAR: A Business Process Execution Engine on the Ethereum Blockchain*, arXiv:1808.03517, 2018/7/10

[18] IBM Institute for Business Value, *Healthcare rallies for blockchains: Keeping patients at the center*, 2016.

[19] I. Fish, M. Barnard, *Saving money and lives with blockchain for coldchain breaks*, May 7, 2018

[20] Griggs, K.N., Ossipova, O., Kohlios, C.P. et al., *Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring* , J Med Syst (2018) 42: 130.

[21] Blockchain in Heathcare – are standards needed?, http://www.healthintersections.com.au/?p=2778

[22] *An interactive landscape map and open-source registry of biomedical blockchains*, https://github.com/acoravos/healthcare-blockchains, accessed Oct 2018.

[23] D. Yaga, P. Mell, N. Roby, K. Scarfone , Blockchain Technology Overview, NIST, Oct 2018, https://doi.org/10.6028/NIST.IR.8202

[24] HealtcareIT News, May18, *Federal Government successfully trials blockchain for researcher access to Australian patient records*, https://www.healthcareit.com.au/article/federal-government-successfully-trials-blockchain-researcher-access-australian-patient,

[25] The Department of Health, *Implementing the Framework to guide the secondary use of My Health Record system data*, http://www.health.gov.au/internet/main/publishing.nsf/Content/eHealth-framework

[26] DeepMind, *Trust, confidence and Verifiable Data Audit*, https://deepmind.com/blog/trust-confidence-verifiable-data-audit/

[27] R. Amara, *Amara's Law*, https://en.wikipedia.org/wiki/Roy_Amara

[28] A Berry, Z Milosevic, *Extending choreography with business contract constraints,* International Journal of Cooperative Information Systems 14 (02n03), 131-179

[29] MedicoHealth, https://medicohealth.io.

[30] researchkit.org/docs/docs/InformedConsent/InformedConsent.html

[31] https://en.wikipedia.org/wiki/Informed_consent

[32] https://www.omg.org/spec/SBVR/About-SBVR/

[33] T. N. Dinh, My T. Thai, AI and Blockchain: A Disruptive Integration, IEEE Computer, vol. 51 no. 9, Sept 2018.