Leveraging blockchain to enable smart-health applications

Angelo Capossele*, Mauro Conti†, Andrea Gaglione*, Riccardo Lazzeretti‡, Paolo Missier§ and Michele Nati*
*Digital Catapult Centre, London, UK, Email: {angelo.capossele,andrea.gaglione,michele.nati}@digicatapult.org.uk
†University of Padua, Padua, IT, Email: conti@math.unipd.it
‡Sapienza University of Rome, Rome, IT, Email: lazzeretti@diag.uniroma1.it
§Newcastle University, Newcastle, UK, Email: paolo.missier@newcastle.ac.uk

***Abstract*—Smart health (s-health) is an emerging paradigm that brings together a whole new range of digital data, both personal and non-personal, in order to deliver a holistic approach to health that overcomes the boundaries of the traditional patient caring system. By including non-personal smart city data, mobile s-health applications can improve prediction, prevention, and prescriptive care, while generating feedback that make cities smarter when accounting for and adapting to individual needs. As a result, the constantly ongoing societal challenge of improving individual life will receive additional support. As an example of such life improvement, cities might reduce pollution by promoting mobile applications that incentivize people lacking of adequate physical activity to use alternative transport means.**

Despite of the envisioned benefits, the diverse nature and jurisdiction of infrastructures and data required to develop s-health applications open up a number of challenges that need to be addressed. In this position paper, we first present a sustainable model for fostering the creation of s-health applications, then identify and discuss the existing challenges, and finally explore the role of blockchain in overcoming some of them.

I. Introduction

Healthcare will be no more limited only to the collection, storage and analysis of biomedical data. Electronic health (e-health) and mobile health (m-health) are going to become limiting concepts in a short while. Thanks to emerging networking technologies, such as 5G and low-power wide-area networks (LPWANs), and wearables technologies, traditional and institutional e-health and m-health data can be combined with the Internet of Things (IoT) and smart cities infrastructures. This helps to establish a large availability of information about individuals' health and their social context.

While the use of such information will continue to improve prediction and prevention of medical conditions, as well as prescription of treatments and medical research, completely novel scenarios can also be envisioned under the smart health (s-health) [1] paradigm. According to [1], s-health is: *"the provision of health services by using the context-aware network and sensing infrastructure of smart cities"*. As a result, more context-awareness and personalization of services will be achieved. For instance, s-health can achieve the dual benefit of enriching citizens' health data with context information of the area they live or usually attend, while creating more informed recommendations for city authorities on how to organize city services according to different citizens' needs: a dual dimension currently excluded by traditional healthcare solutions.

Outdoor air pollution is one of the first causes of death for many citizens affected by respiratory diseases. Holistically developed s-health applications can indeed guarantee availability of personalized pollution-free route recommendations for citizens suffering from chronic obstructive pulmonary disease (COPD) or other respiratory problems [2], [3], as well as incentivize less polluting alternative transport modes for those citizens lacking of adequate daily physical activity [3]. On the other hand, authorized s-health applications can generate feedback to help cities to intelligently reconfigure, e.g., dynamically adapting congestion charge zones or activating public irrigation water spray to reduce polluting agents. By delivering s-health applications (apps), cities will turn into more citizens- and patients-friendly environments, thus increasing municipalities revenues when quality of life improves.

Figure 1 illustrates a platform model that enables the development of s-health apps to collect, combine and analyze a variety of data provided by citizens and patients, social feeds and urban sensors. Such a model goes beyond the current existing e-health or m-health solutions [4], [5], [6], which focus on the collection and analysis of only health data. It should provide interfaces for accessing assets, data, and infrastructure, connected through existing architectures such as: i) e-health and m-health for what concern EHR (electronic health record) and PHR (personal health record) data, as well as social networks and wearables for citizens' habits and preferences; ii) IoT and 5G for what concern access

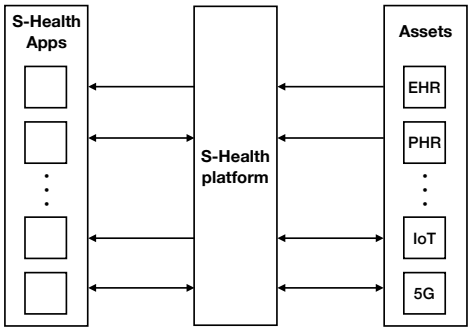

Fig. 1: S-Health vision schema.

978-1-5386-6282-3/18/$31.00 ©2018 IEEE

to smart cities data and infrastructure for delivering feedback to individuals and reconfiguring smart cities.

Despite the benefits promised by this envisioned scenario, there are several challenges to address. Combined data belongs to different stakeholders and jurisdictions, and liability in accessing it needs to be clearly identified and managed. The envisioned platform cannot be limited to only provide devices connectivity and data access. In fact, it should also guarantee contracts compliance and certain level of security when accessing them, thus maintaining trust among the involved stakeholders. In particular, the access to medical data is strictly regulated, and new limitations and compliance requirements for accessing these and other personal data are emerging, especially in the EU, due to the enforcement of the new general data protection regulation (GDPR - 2016/679, effective from May 25, 2018) [7]. There is a lack of understanding from individuals on how their data could be accessed and mistrust to guarantee third party access, whereas there is demonstrated citizens interest to contribute to social development. Moreover, smart cities assets are owned by different stakeholders (e.g., hospital, city councils) who have limited trust in sharing them if no clear contracts are in place to regulate how they might be used and leveraged by different third parties. In addition to that, the lack of adequate incentives to reuse and re-purpose existing assets often lead to the creation of standalone, ad-hoc solutions.

Therefore, we envision that a s-health platform must provide a middleware on top of different architectures, to grant infrastructure and data access for s-health apps while maintaining trust and incentives across a variety of stakeholders. We believe blockchain [8] and distributed ledger technology (DLT) can be instrumental to overcome these issues and to realize this vision, by permitting federation and governance decentralization. Opportunities and benefits of blockchain for remote healthcare have been already outlined in several health related projects such as Pointnurse, aimed to facilitate and disintermediate tele-nursing and nursing recruiting [9], MedRec, a decentralized record management system to handle EHRs [10], and Medicalchain, a telemedicine platform allowing patients to communicate with doctors and share their own medical records with them [11]. However, all these solutions fail to deliver the vision of a platform for s-health application development that leverages infrastructure and data sharing between different stakeholders.

The contribution of our position paper is threefold, in particular:

- We describe in detail the ecosystem of stakeholders (asset providers, app developers, policy makers and regulators, use case providers, and users) and their interaction model that makes s-health apps and service developments practical;
- We discuss the main technical, commercial and legal challenges for s-health apps;
- We explain how blockchain provides a contract layer to solve the identified challenges and incentivizes the availability of assets needed to build novel s-health apps.

II. Related Work

S-health is still a concept, however, several e-health and m-health architectures have been proposed. In the following, we review a set of architectures for health data as well as some blockchain based health solutions.

A. Architectures for health data

Service oriented architectures (SOAs) [12], [13] have played an important role in the development of healthcare systems, by helping to exchange information between applications. By using SOAs and external web services, interoperability issues can be resolved, but many others still remain. SOAs are often focused on specific applications [13], [14] and not taking advantage of a common architecture for several purposes. Continua [4] is a non-profit, open industry consortium of e-health and technology companies. It facilitates interoperability among connected health technologies such as sensors, smart devices, and back-end services. Through shared standards and reusable components, open mHealth [5] guarantees authoring, integration, and evaluation of personal data for hospitals, accountable care organizations, and public health practitioners. GSMA m-health [6] mainly provides an architecture for remote monitoring of patients using mobile network with added value of embedded security, although not currently suitable for emergency solutions (which might better rely on future 5G networks).

M-health and e-health mainly focus on supporting remote health monitoring (anywhere, anyhow, at any time), while the proposed s-health practical vision aims to support both enhanced remote health monitoring and city sustainability. More specifically, an s-health platform can interconnect with these existing e- and m-health reference architectures through the use of B2B Medical Data Exchange (or alternatively with the Conversion & Storage Medical Data modules) while supporting the possibility for patients and clinicians to set up rules (reflected in the B2B Administration module; providing also auditing capabilities) for data access. Such integration should follow standard interface like the Continua HRN interface.

S-health vision is therefore to extend such architectures by creating a platform for sharing existing medical data, under user control, with app developers and allow seamless integration with smart cities data. This first objective could be achieved by leveraging existing the GSMA m-health architecture and creating additional roles, other than the existing ones (Patient, Subscriber, Clinician, Observer) to allow access to the medical data through the Web Portal and the Provisioning and Assurance module. The Accounting Service Devices database should also be replicated and not owned by third parties, in order to increase trust. However, this will still not solve the challenges related to the integration of such medical data with other data, therefore a need for a dedicated s-health platform is still pressing.

Smart city and personal devices must be interconnected as well in order to fulfill the s-health vision. Medical-grade devices should comply to healthcare messaging standard, e.g., IEEE 11073, IHE PCD-01, or DICO (Continua WAN

Interface). To facilitate such integration, 5G can provide access to the infrastructure through given infrastructure control and (virtual) network functions, and can allow the connection of multiple IoT devices. 5G can then support well the s-health need to connect new and more data from a higher number of connected devices as well as deliver feedback with small latencies and high reliability.

However, healthcare technologies on 5G are still in their infancy. Dealing with healthcare data, privacy, security and safety as well governance is still the main challenge 5G will have to focus on. Other barriers are interoperability and incentives to infrastructure owner to share resources. Nevertheless, 5G network can definitely be the communication infrastructure for s-health apps and accessed via standard interfaces (Application and Business Service Plane). However, s-health platform will have to add a new level of accountability, monitoring, compliance on who is accessing what and for what purpose (in our view using blockchain) thus increasing trust and transparency while allowing to identify liability.

B. Blockchain and health

Blockchain [8], [15] is essentially a distributed ledger of information (e.g., a transaction from A to B in the bitcoin world), a copy of which cannot be arbitrarily altered without the alteration being spotted, and for which consistency of each information can be achieved in a decentralized and distributed way, without requiring trust in any third party. These properties–which in the bitcoin world provide a very strong business case (e.g., removing transaction costs associated to clearinghouse functionalities when transferring money)–can also provide a trust case for exchanging access to different assets, without requiring trust among parties.

Bitcoin [16] was the first application built on top of the blockchain technology. It is a digital and interoperable currency using the blockchain infrastructure. It achieves low transaction fees and prevents the double-spending problem, that is the possibility to spend a given amount twice, without requiring to trust in any third party to police this risk. Bitcoin and other alt-coin (i.e., bitcoin plus metadata) seem to provide an interoperable and open cross-domain incentives platform for redistributing the value created from assets sharing, transparently covering the interests of all the involved parties. Blockchain is later evolved to manage Smart Contracts, small pieces of software that encode a set of conditions and actions that a machine can interpret and execute. Smart contracts can be managed by the blockchain infrastructure without third party involvement or supervision. These functionalities appear to be interesting when it comes to give permission to decentralized applications (DApps) to access different assets (data sets and devices) only for specific purposes. Such assets and services are provided by different sources and controlled by more than one entity (in contrast to the traditional centralized client/server web). S-health apps can be seen as a particular type of DApps.

Recently, there is a great attention on the development of healthcare architectures based on blockchain. For example, a partnership of companies that includes Gem[1], Philips, and Capital One [17], [18], is proposing a blockchain-based enterprise architecture allowing healthcare companies to build on their *collective intelligence* or Data IQ, to create the patient-centric care model of the future. Similarly, Hyperledger has announced the formation of the Hyperledger Healthcare Working Group aiming at improving the process for accessing and updating healthcare provider data. Blockchain-enabled health IT systems can provide technological solutions to health data interoperability, integrity and security, portable user-owned data and other areas. Some examples:

1) data exchange systems that are cryptographically secured and irrevocable, enabling seamless access to historic and real-time patient data, while eliminating the burden and cost of data reconciliation;
2) estimated 5-10% of healthcare costs are fraudulent, resulting from excessive billing, or billing for unperformed services. Blockchain-based systems can provide realistic solutions for minimizing these medical billing-related frauds by automating the majority of claim adjudication and payment processing activities thus, eliminating the need for intermediaries and reduce the administrative costs and time for providers and payer;
3) ensure a chain-of-custody log, tracking each step of the supply chain at the individual drug/product level. Private keys and smart contracts could help build in proof of ownership of the drug source at any point in the supply chain and manage the contracts between different parties (iSolve LCC is working with multiple pharma/biopharma companies to implement its Advanced DLT blockchain solutions to help manage drug supply chain integrity);

It is clear how blockchain and distributed ledger technologies have been so far used in the health sector to solve issues involving the many jurisdiction participating to creation and sharing of medical data. S-health vision goes beyond this, adding the additional complexity coming from adding other source of data and responsible authorities. Blockchain can hence be the core of the middleware placed on the top of these diverse set of assets and apps, while guaranteeing accountability, monitoring, compliance, trust, transparency and liability across a variety of stakeholders.

III. S-HEALTH ECOSYSTEM

In this section we describe the stakeholders required to make s-health apps development practical [1], [2], [3], the benefits they might gain from being part of the s-health ecosystem, and the barriers they face.

Asset providers (AP) use the common s-health platform to share existing infrastructures (e.g., from smart transport, home and building infrastructures), non-personal data (e.g., transport and traffic data, environmental data, streetlights usage) as well as to allow consented access and exchange of personal information (e.g., from medical and behavioural records, social networks, user devices, smartphone and wearables). Being

[1]https://enterprise.gem.co/health/

able to re-permission existing assets, asset providers will save additional capital investment (CAPEX) in required infrastructures, while eventually reducing operational costs (OPEX) of existing ones;

App developers (AD) create applications for Users, using assets (devices and data) provided by AP. Entrepreneurial App developers, with little capital and pressing time-to-market, can now access different required assets and create new advanced apps, without any large required capital investment in infrastructure and data. Apps usage creates incentives for AP to guarantee further trusted assets access for the larger benefit of various Users;

Users (AU) are those consuming s-health apps for a given perceived benefit and include but are not limited to: i) Individuals/Patients receiving better management of their health and lifestyle while deciding how their data can be accessed and shared with third parties; ii) Clinicians having continuous access to all the data related to their patients, including not only data collected in hospitals or results of analysis carried out by colleagues, but being able to augment them with data about patients' habits and the places they live in (e.g., air quality). S-health apps empower them to offer better assistance to their patients and reduce visit time; iii) Researchers obtaining, under participating subjects consent, aggregated and anonymized datasets, and performing large-scale medical research studies on the relationships between citizens and city life;

Use case providers (UP) are those providing use cases and business cases and incentives for new apps to be developed (e.g., city councils, governments, hospitals). Among them: i) Insurers could commission the development of wellness apps to access information to better estimate risks, provide more personalized policies to their customers while incentivizing them to live a healthier lifestyle; ii) City councils could commission development of personalized smart transport app, taking into account citizen needs, their health and lifestyle, while reducing pollution and its associated costs (e.g., fines payment);

Policy makers and regulators (PR) can leverage the transparency embedded in the s-health platform contract layer to assess compliance. They are not directly involved to the value creation and sharing of the s-health ecosystem, but involved in its promotion and validation. The latter recall for the main role of the s-health platform, which beyond connectivity, should provide mutual trust, privacy, integrity and ownership of the shared data and infrastructure.

To better highlight the value created by the s-health apps ecosystem to different stakeholders, we have mapped them according to the model illustrated in Figure 2. The model represents the interaction flow among the s-health stakeholders in terms of action provided and incentives and benefits received. To evaluate the described model, we interviewed several stakeholders within the scope of the European project

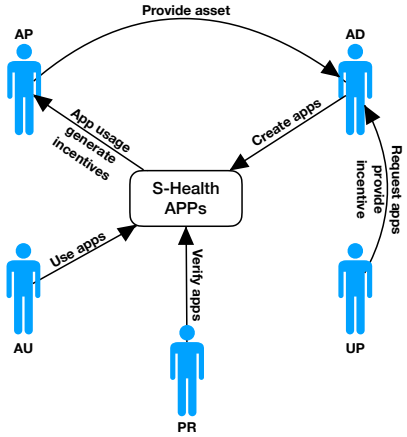

Fig. 2: Stakeholders interaction flow.

SynchroniCity[2] (2017-2020). We tested the vision of s-health, by interviewing 8 city councils (Antwerp, Carouge, Eindhoven, Helsinki, Manchester, Milan, Porto and Santander) covering the role of both AP and UP, and SMEs, covering the role of AD. Aim of these interviews was to validate the benefits of a platform to enable s-health apps, while helping to identify the concrete barriers hindering the different stakeholders categories from making available and exploiting the required assets. 75% of respondents agree with the identified benefits, while 87% recognize data ownership, how to measure and track quality of data and transparency on governing data access as the main barriers. Moreover, 62% of respondents identify data licensing and track of data usage issues as well.

IV. Opportunities and Challenges

From a technical point of view, due the advancements in wearable technology, IoT and smart cities infrastructures, the amount of data generated daily constantly increases [19]. Data owners should keep the control over their data, which have to be effectively stored, while granting the access only to authorized apps. Similarly, access to smart cities services requires strong authentication to protect citizens safety. Therefore, finding the right balance among the value, risks, and liability in exploiting the capabilities of s-health applications and infrastructures will be crucial for their development and mainstream adoption.

Despite the clear benefits for the stakeholders, the realization of s-health apps faces many legal, technical and commercial barriers that need to be addressed before their benefits can be unleashed. Tables I-III provide a list of the main challenges in the s-health ecosystem, which arise from the interactions among the stakeholders identified above. Also, for each of the challenges, the tables report and analyze approaches and tools leveraging blockchain technology that can be potentially applied to tackle them.

[2]A large scale pilot initiative aiming to deliver a digital single market for IoT-enabled urban services in Europe and beyond: http://synchronicity-iot.eu/about/ (Accessed on Apr 29, 2018)

TABLE I. S-health technical challenges.

Challenge	Blockchain opportunities and future open research
T1. *Trusted and transparent assets accountability*: S-health applications require access to assets from a variety of domains and owned by different AP with limited trust on how their assets will be used and by whom.	Tracking the accesses to assets such as transactions on public ledgers increases transparency, trust and control [15], [20]. Researchers should define privacy-preserving models for digitization/tokenization of assets and their tracking. Efficient search for assets on a blockchain requires User Experience (UX) research to develop human-friendly tools.
T2. *Assets provenance, accuracy and quality*: Heterogeneity of assets and AP make it difficult to track quality and identify responsibilities.	Tracking data sources provenance and quality scores (e.g., by measuring usage) on distributed ledgers simplifies the identification of responsibilities, stimulates the production of good quality data sources [21], [22], and provides a baseline for their pricing [23], [24]. Efficient, scalable and sustainable blockchain systems are needed to manage the high volume of transactions. Research is required to protect the privacy of AP.
T3. *Context-aware privacy and access control*: Personal assets allow to understand individual lifestyle and context. It is necessary to guarantee a trusted, fine-grained control when sensitive medical data is accessed, while taking the associated burden away from AU.	Smart contracts can act as trusted personal agents implementing and enforcing personalized compliant privacy rules defined according to PR guidelines to grant contextual access for secondary use of AU personal data and to track given consent and permission [21]. Creation of interfaces that simplify individual definition of personalized and legally valid rules and translate this into smart contracts represent a multidisciplinary challenge.

TABLE II. S-health legal challenges.

Challenge	Blockchain opportunities and future open research
L1. *IP Management (asset ownership)*: While the ownership of assets should be guaranteed to AP, the access to assets (in particular, data) might lead app developers to derive new Intellectual Properties (IPs), the ownership of which should be identified and protected.	S-health apps should be created by AD using distributed repositories (e.g., Git); required assets can be tracked using blockchain in an independent, transparent, and trusted log of app development contributions, in order to share and distribute the created value among AP and s-health AD [20]. Open issues are related to the definition and enforcement of seamless license agreements and to the resolution of disputes when some assets are removed from a given app.
L2. *Ethical use of big data analytics*: Related to the previous challenge and the growing use of machine learning in s-health apps development, there is the need to increase algorithm transparency to show how assets, in particular personal data, are ethically used thus gaining public trust.	Blockchain can be leveraged to create an immutable and non-repudiable ledger of output returned by algorithms embedded into any s-health app when given input data is provided, thus allowing the verification of algorithm integrity by AP, AU, and PR. Development of tools, certification and labels for inspecting and visualizing algorithms' ethics, while preventing reverse engineering, still require multi-disciplinary research.
L3. *Compliance (including that of secondary or cross-jurisdictional use) for assets access*: Repurposing and reusing existing assets, in particular personal data, might create compliance issues and request to re-permissioning data access for secondary purposes. In addition, PR demand for transparency on how assets, in particular personal data, are accessed, used, and eventually shared with third parties. A number of individual rights for AP and UC, such as data erasure and portability, also need to be guaranteed according the GDPR [7] and ACA [25].	By using blockchain as an immutable record of consent log, AD can demonstrate that consent is properly gathered for each new request of assets (in particular personal data), without the need of a trusted third party. If the consent transactions created only point to assets stored off-chain, data assets can be erased by revoking the access of the parties. Standardized interoperable consent formats need to be identified and stored as part of a blockchain transaction, carefully identifying the metadata to provide AU and AP privacy [20], [21]. Research needs to develop privacy-preserving tools to inspect consistency of the created ledger as well as create automated procedures to avoid the burden of having individuals frequently involved in the re-permissioning process.

TABLE III. S-health commercial challenges.

Challenge	Blockchain opportunities and future open research
C1. *Risk management and liability costs*: Developing decentralized s-health apps might reduce the control on the quality of the used assets and increase the risks and costs for AD and AP, thus hampering the adoption adopt such model.	Blockchain allows to distribute liability, while providing an immutable record to capture proper assets maintenance (e.g., SW and security updates). Autonomous smart contract can be developed and deployed to collect caution fees for assets provisioning and usage, identify liabilities and automatically charge responsible AP [20]. This model forces AP to maintain the quality of their assets high. On the other hand, new insurance models to protect AP are needed as well.
C2. *New business models*: S-health app model can increase the availability of assets for s-health AD, by increasing the reuse of data and infrastructures, incetivizing UP, and lowering the required OPEX and CAPEX costs, respectively. New business models need to be explored to guarantee sustainability costs of the system, incentivize AP, and cover risk and management costs.	Decentralized autonomous organizations (DAOs) could be leveraged to help UP in identifying business and use cases for s-health applications. Saved money can be used to issue DAO participation tokens to AP to vote use cases, receive incentives, and cover management costs. Research is required to provide testing and certifying methodologies for smart contracts safety [26] and entrust of the needed PR. Research needs to reduce costs associated to consensus protocols by investigating new hybrid proof-of-work/proof-of-stake algorithms.
C3. *Reputation of assets providers and s-health app developers*: While commoditizing assets provisioning and use, to maintain fairness of access from both AD and AP, it is important to develop a transparent, interoperable, asymmetric, and unbiased reputation scheme.	Reputation assignment is a bilateral process. Blockchain can be used to transparently store interoperable reputation transactions, by independently collect bilateral scores (implemented as smart contracts) for the parties involved in each transaction and without requiring third party mediation. However, research is still required to define the trustworthiness metrics (e.g., adherence to SLAs) to be used for assets and app developers, and the tools to measure them.

V. Conclusion

This position paper extends the s-health vision by Solanas et al. [1] by describing a sustainable model for fostering the creation of s-health applications. We hope this vision will open a dialogue among the envisioned stakeholders (in particular, assets providers and regulators) and motivate them to create s-health compliant sandboxes where this model and assumptions can be tested, further enhanced by solving open research challenges, and finally largely adopted.

As next steps, we aim to first design a detailed architecture to allow compliant and sustainable s-health apps development and to identify existing technology providers able to contribute to the realization of the architecture. We will analyze trade-off of adopting permissioned- versus unpermissioned-based blockchain solutios with respect to different dimensions such as privacy, scalability, efficiency, and incentives. To achieve that, we need to understand the requirements with respect to the above dimensions from the stakeholders' ecosystem, and will leverage the large opportunities for stakeholders engagement offered by the EU SynchroniCity project.

VI. Acknowledgments

This work has been partially supported by the H2020 project SynchroniCity (agreement No 732240), EU TagItSmart! Project (agreement H2020-ICT30-2015-688061), the grant n. 2017-166478 (3696) from Cisco University Research Program Fund and Silicon Valley Community Foundation, and the Security and Privacy of Biometrics for Mobile Authentication (SPoB-MA) project (grant n. RM11715C7878B045 of Sapienza University of Rome Bando Ricerca 2017).

References

[1] A. Solanas, C. Patsakis, M. Conti, I. S. Vlachos, V. Ramos, F. Falcone, O. Postolache, P. A. Pérez-Martínez, R. Di Pietro, D. N. Perrea *et al.*, "Smart health: a context-aware health paradigm within smart cities," *IEEE Communications Magazine*, vol. 52, no. 8, pp. 74–81, 2014.

[2] D. Ding, M. Conti, and A. Solanas, "A smart health application and its related privacy issues," in *Smart City Security and Privacy Workshop (SCSP-W), 2016*. IEEE, 2016, pp. 1–5.

[3] C. Patsakis, R. Venanzio, P. Bellavista, A. Solanas, and M. Bouroche, "Personalized medical services using smart cities' infrastructures," in *Medical Measurements and Applications (MeMeA), 2014 IEEE International Symposium on*. IEEE, 2014, pp. 1–5.

[4] R. Carroll, R. Cnossen, M. Schnell, and D. Simons, "Continua: An interoperable personal healthcare ecosystem," *IEEE Pervasive Computing*, vol. 6, no. 4, 2007.

[5] D. Estrin and I. Sim, "Open mhealth architecture: an engine for health care innovation," *Science*, vol. 330, no. 6005, pp. 759–760, 2010.

[9] "Pointnurse project." [Online]. Available: https://pointnurse.wordpress.com/

[6] GSMA, "Connected mobile health devices: A reference architecture," *White paper, version 1*, 2011, https://www.gsma.com/iot/wp-content/uploads/2012/03/connectedmobilehealthdevicesareferencearchitecture.pdf.

[7] "Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation)," *Official Journal L. 2016;119(1)*.

[8] V. Buterin, "Daos, dacs, das and more: An incomplete terminology guide," *Ethereum Blog*, vol. 6, p. 2014, 2014.

[10] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *Open and Big Data (OBD), International Conference on*. IEEE, 2016, pp. 25–30.

[11] "Medicalchain project." [Online]. Available: https://medicalchain.com/en/

[12] A. Shaikh, M. Memon, N. Memon, and M. Misbahuddin, "The role of service oriented architecture in telemedicine healthcare system," in *Complex, Intelligent and Software Intensive Systems, 2009. CISIS'09. International Conference on*. IEEE, 2009, pp. 208–214.

[13] C. De Capua, A. Meduri, and R. Morello, "A smart ecg measurement system based on web-service-oriented architecture for telemedicine applications," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 10, pp. 2530–2538, 2010.

[14] E. M. Monteiro, C. Costa, J. L. Oliveira *et al.*, "A cloud architecture for teleradiology-as-a-service," *Methods of information in medicine*, vol. 55, no. 3, pp. 203–214, 2016.

[15] S. Underwood, "Blockchain beyond bitcoin," *Communications of the ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[16] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[17] "Better off abroad? blockchain health firms gain ground outside the us." [Online]. Available: https://www.coindesk.com/better-off-abroad-blockchain-health-firms-are-gaining-ground-outside-the-us/

[18] "With monsoons of data, healthcare's salvation just may be blockchain." [Online]. Available: https://www.forbes.com/sites/jillrichmond/2017/03/10/with-monsoons-of-data-healthcares-salvation-just-may-be-blockchain/#e6767e35a19e

[19] "Ericsson mobility report." [Online]. Available: https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf

[20] P. Boucher, *How Blockchain Technology Could Change Our Lives: In-depth Analysis*. European Parliament, 2017.

[21] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *Security and Privacy Workshops (SPW), 2015 IEEE*. IEEE, 2015, pp. 180–184.

[22] "Provenance project." [Online]. Available: https://www.provenance.org/

[23] P. Missier, S. Bajoudah, A. Capossele, A. Gaglione, and M. Nati, "Mind my value: a decentralized infrastructure for fair and trusted iot data trading," in *Proceedings of the Seventh International Conference on the Internet of Things*. ACM, 2017, p. 15.

[24] "Everledger project." [Online]. Available: https://www.everledger.io/

[25] "Affordable Care Act (ACA)." [Online]. Available: https://www.healthcare.gov/glossary/affordable-care-act/

[26] F. Idelberger, G. Governatori, R. Riveret, and G. Sartor, "Evaluation of logic-based smart contracts for blockchain systems," in *International Symposium on Rules and Rule Markup Languages for the Semantic Web*. Springer, 2016, pp. 167–183.