IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 22, 2020, accepted May 3, 2020, date of publication May 12, 2020, date of current version May 26, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2994090

A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare

BAHAR HOUTAN[1], ABDELHAKIM SENHAJI HAFID[2], AND DIMITRIOS MAKRAKIS[3]
[1]Department of Computer Science and Engineering, Islamic Azad University, Science and Research Branch, Tehran 1477893855, Iran
[2]Network Research Laboratory, Université de Montréal, Montreal, QC H3C 3J7, Canada
[3]School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON K1N 6N5, Canada

Corresponding author: Abdelhakim Senhaji Hafid (ahafid@iro.umontreal.ca)

This work was supported by the Natural Sciences and Engineering Research Council of Canada.

ABSTRACT Convergence of physical and digital identity and integration of various individual records, such as patient data, into a united repository remains a serious challenge. On one hand, collecting relevant data can help clinicians, specialists and healthcare service providers to facilitate care for patients. On the other hand, Self-Sovereign identity and the right to control personal data comes into question, because patients do not handle their data explicitly. Distributed Ledger Technology (DLT) is a novel method which would allow to securely record time-stamped data and enable patient-driven health and identity records. In this paper, we review the state-of-the-art in Blockchain (BC)-based self-sovereignty and patient data records in healthcare. Our motivation is to investigate the potential of BC technology for use in the patient data and identity management. As a distributed decentralized technology, BC can be very beneficial, giving patients control over their own data and self-sovereign identity. To the extent of our knowledge, there is no literature covering the same concerns. More specifically, the focus is on solutions that aim the realization of holistic BC-based Electronic Health Records (EHR) and Patient Health Records (PHR). EHR and PHR are used to record patient data, such as the doctor's notes upon a visit and radiology images. Hence, they include critical information regarding patient's privacy and identity. Therefore, development of pure decentralized Healthcare Information Systems (HIS) is a great challenge in terms of architectural and technical structure of the systems. Designing robust and reliable EHR and PHR, which represent the foundation of many other healthcare services, relies on carefully finding the balance in a trade-off between many factors, such as level of decentralization, privacy, scalability and data throughput. In this paper, we review the state-of-the-art and provide an analysis on the design trade-offs.

INDEX TERMS Blockchain, healthcare, privacy, self-sovereignty.

I. INTRODUCTION

Blockchain (BC) Technology defines a decentralized trustless security model. In this model, users in the edge of the network engage in the verification of the network transactions. Users form a decentralized network, in which end to end trustful transactions between anonymous parties are achievable. Transactions are stored in an open ledger visible to network participants; hence fraudulent transactions can be detected. Therefore, the security of data is assured in a decentralized manner, and without intervention of any intermediaries. The first applications of the distributed ledger paradigm are the open source public BCs, that implement cryptocurrencies like Bitcoin and alternative coins (altcoins) like Litecoin. Bitcoin utilizes the Distributed Ledger Technology (DLT) for a decentralized payment system and solves double-spend vulnerability by proposing the Proof of Work (PoW) mechanism [1], [2]. PoW employs game theory to incentivize network nodes to dedicate their computational resources to the network verification procedure. The participating nodes in this process are called miners in Bitcoin network. Moreover, the introduction of the smart contracts by Ethereum BC created the second generation of the technology that enabled development of decentralized applications (Dapps) on BC.

Smart contracts seem similar to the Cloud-based Software as a Service (SaaS) model. In this model, customers get services through a web program and don't need software services installed on their PCs or servers [3]; this is because the Cloud provider runs the software on its data center and enables clients to have access to data. Dapps make DLT

The associate editor coordinating the review of this manuscript and approving it for publication was Petros Nicopolitidis.

an alternative solution to SaaS Cloud for some crowd-based business models, in which services are based on shifting key activities of service provider to users. BC can be used in these models to incentivize the participation of the crowd in return for gaining reward and reputation. Besides, the evolution of Dapps during recent years enables the materialization of low cost inter- and intra- organizational business processes, since unnecessary middle steps are eliminated. This does not only attract start-ups and the open-source community to cultivate the potential of the technology, but also large companies [4]. Hence, permissioned and consortium BCs like Hyperledger Fabric [5], R3 Corda [6] and Stellar [7], are some of the customized versions for the enterprise use. This type of BCs is semi-decentralized; this means the service provider can decide the distribution of permission, access and control of network resources among the network nodes.

The motivation to apply BC solutions compared to the client-server network services is that BC promises security, reliability, timeliness and efficiency due to being decentralized and also eliminating many intermediaries in the formal procedures. But, according to the authors of [8], the third generation of BC must define a new software engineering paradigm and Cloud architecture design in order to enhance existing Cloud solutions with decentralized/distributed features. On existing BC implementations, data storage and computation are still expensive and limited, mainly because the technology is new and there are still many open security challenges. Limited features ensure controllability of early developed solutions. Therefore, authors in [8] recommend combining DLT and Cloud solutions to capture the advantages of both. Other challenges that stand on the way of wide acceptance of BC by businesses are performance, user-friendliness, openness, administration and cost-effectiveness [9].

Healthcare Big Data comes in many forms. There are various health data sources, constantly generating data. In addition to the data registered when a patient undergoes healthcare related procedures or visits a physician, new data sources have emerged [10]. All sources of clinical data are integrated in data silos, where data gathered from various sources are combined and unified; this facilitates information exchange between institutions. Thus, experts can make efficient diagnosis and care for patients based on comprehensive structured data that data silos offer to them. New e-health solutions, like wearable health monitoring gadgets, that provide services based on patient's lifestyle data, will improve patient care. This is because they enable clinicians view hidden health related data of patient's daily life. However, in this case, privacy and data ownership become increasingly critical, because collected data contain private and personal information, of which security and safety must be assured by service providers.

Healthcare is one of the sectors that has taken the initiative to develop BC-based solutions to address existing challenges. The healthcare ecosystem consists of many stakeholders, such as medical institutions, specialists, hospitals, health insurance companies and patients. Up to now, it has been convenient for health organizations to have full control over patient's information. In traditional models, patient's medical data, along with inter- and intra-organizational data is kept in large repositories stored in secured data centers. However, due to wide use of digitization, healthcare Big Data and the number of health data generating sources and services are growing exponentially.

Currently, clinicians, hospitals and medical institutions use Health Information Systems (HIS) to record, exchange and analyze health data. As sources, such as wearables and handheld devices, have emerged, merging this patient data with the digital identity brings up challenging issues. These issues include standardized governance, exchange and analysis of large mass of health data efficiently and securely.

There are many technical challenges that remain unanswered by the literature, which require thorough investigation. Among these challenges is the lack of a standardized implementation method to facilitate comparison and evaluation of existing solutions. BC development frameworks are still under development, because the technology continues to have some privacy and security related weaknesses; therefore, most of existing solutions are not ready for use in real-world applications. Developers have to balance many factors, including the level of decentralization, privacy, scalability and data throughput, when designing a BC-based system.

There exist a few related surveys in the open literature [11]–[16]. McGhin *et al.* [11] categorise healthcare BC applications according to: (1) System security; (2) Interoperability; (3) Data sharing; and (4) Mobility. McGhin *et al.* have selected related works targeting mobile health, wireless, IoT, research and trial analysis. Our work takes a different approach; it focuses on the use of such technologies and applications by BC-based EHR and PHR at ecosystem level. Kuperberg [12] presents a systematic review of identity and access management systems (IAM). He defines essential aspects for the realization of BC-based identity management systems, such as user-friendliness, compliance and liability, regulations, standardization and integration. However, it does not cover healthcare related works, in which patients, doctors, researchers, medical and health research institutions, and insurance companies are the role players in the ecosystem. The transactions in healthcare systems, in addition to identity data exchanges, include exchanges of patient data between the participants, such as the doctor's notes upon a visit or radiology images. Zhu and Badr [13] study the challenges that are related to the creation of identity management systems for Internet of Things (IoT), concerning access control, privacy and performance. They compare existing identity management systems in terms of decentralized authentication, domain name service (DNS), BC infrastructure, privacy preservation mechanism, etc. However, they do not cover the challenges in creating Electronic Health Records (EHR) and Patient Health Records (PHR), which represent the foundation of Internet of Healthcare Things (IoHT). Dimitrov [14] addresses challenges in developing healthcare

management systems. However, the scope of the survey [14] is limited to the organizational management scope. In our paper, we have covered a wider range of applications and development aspects, such as architectural and technical issues, and the trade-off between the level of decentralization and privacy protection in these systems. Hau *et al.* [15] have conducted a questionnaire-based survey among medical doctors and patients regarding their interests on the use of BC technology in the management and distribution of medical information. Their findings show that patients are more favorable in using BC than medical experts. The survey [15] does not cover technical aspects of medical information management systems; it studies the problem from the user's perspective. Our perspective of the problem is technical and architectural. Hathaliya and Tanwar [16] have conducted a comprehensive study on the security and privacy in distributed health-care information systems (Healthcare 4.0); they did consider different technologies for data exchange, such as Cloud Computing, Fog Computing, IoT and telehealthcare technologies. The survey provided in [16] also investigates BC as one of the essential solutions for provision of security and privacy. It provides a comprehensive view of the challenges of future healthcare systems and a classification of various solutions. Our paper focuses on BC-based solutions; thus, it covers in depth the challenges and technical details of these solutions. It provides findings and insight that are not covered in [16].

More specifically, we survey the state of the art of BC technology for self-sovereignty in healthcare. We particularly focus on the challenges facing the realization of BC-based patient data exchange, self-sovereign identity and data governance. The contributions of this paper can be summarized as follows:

1. The first thorough review in open literature addressing the application of BC to self-sovereign patient's medical data storage, access, processing and sharing. In particular, we review and classify existing contributions into five groups: (1) data control and protection; (2) digital identity; (3) social data governance; (4) healthcare and patient data; (5) Social insurance, etc.
2. A review of: (a) applications that have been implemented as proof of concept; (b) published works, which have not produced an implementation yet; and (c) established standards. Our work also identifies the potential benefits of combining DLTs with traditional approaches of medical data sharing, such as EHR and PHR.
3. A thorough investigation of the trade-off between the level of decentralization and privacy in BC-based HIS and Identity Management Systems (IdMSs).

The organization of the paper is as follows. Section II presents BC related advantages and limitations. In section III, we provide the description of self-sovereignty based on BC and categorize existing approaches. Section IV presents the concept of distributed patient data management. Section V presents different approaches and challenges in the realization of distributed HIS. Section VI provides an analysis of existing BC-based patient identity and data management systems. Section VII summarizes and provides critical analysis of existing research in the area. Finally, Section VIII concludes the paper and presents future research directions.

II. TECHNOLOGICAL ADVANTAGES AND LIMITATIONS OF BC

A. DISTRIBUTED LEDGER TECHNOLOGY (DLT)

BC is a decentralized peer-to-peer asymmetric encrypted network. In asymmetric encrypted networks, each peer in the network acquires a public and a private key. Public key (or rather the hash of public key) represents the identification address of the peer and the private key is to decrypt the transactions corresponding to the public key. Furthermore, DLT is an immutable time-stamped record of all transactions between peers in a decentralized network. DLT can be implemented based on various decentralized mechanisms like BC, IOTA [17] and Hashgraph [18]. In this paper, we focus on implementation of DLTs based on BCs such as Bitcoin, Ethereum and Hyperledger. In these systems, a set of new transactions is collected in a block and added to DLT after the block has been verified via a consensus mechanism, such as PoW and Proof of Stake (PoS) [19]. Blocks are linked together (i.e., block n includes the hash of block n−1) and ordered based on their confirmation time; thus, transactions associated with blocks produced earlier are the most reliable and consequently most acceptable by the network peers. It is harder to remove or tamper transactions in older blocks. This is because a hacker, to tamper/remove transactions in block n, would need to change block n as well as those blocks linked to it (block n+1, block n+2…) to avoid detection. Moreover, decentralized architecture promises security, because redundant copies of DLT are stored throughout the network nodes. Hence, DLT is recoverable even if the network loses some of data storage nodes. Every node can execute PoW as part of the network's security mechanism, and in return, they are rewarded with tokens. In contrast, PoS considers the significance for a node to protect the integrity of BC (based on the size of damage the node might suffer if BC becomes compromised) as the criterion of measuring trustworthiness. Therefore, miners are chosen among the nodes that have the highest stake in maintaining the BC's integrity, since they are more likely to stay loyal to the network.

Current implementations of BC have a number of limitations. In particular, PoW-based implementations involve complex cryptography computations to verify and insert a new block to BC. Additionally, as the network size and the number of transactions grow, PoW becomes even more complex in terms of processing time and power consumption. There are still challenges in designing an optimal consensus mechanism. Wang *et al.* [20] provide a comprehensive survey of BC consensus mechanisms. Lack of scalability in existing DLTs hinders achieving pure decentralized recoverable

data records. Many applications still require using hybrid approaches, where centralized storage is used [21].

B. SMART CONTRACTS

The concept of smart contracts was introduced, before any BC was even in existence, by Nick Szabo in 1994. It defines the rules and penalties around an agreement in the same way that a traditional contract does, but also automatically enforces those obligations. A smart contract is a piece of code and data that is deployed to a BC; the first smart contract, with BC, was deployed on Ethereum in 2015. A smart contract can perform calculations, store information, and automatically send funds to other accounts. Several languages can be used to write the code for smart contracts; these include Solidity, Chain Code and Vyper. More specifically, a smart contract provides a number of functions/primitives (e.g., transfer token, store document and buy token) that can be called by users.

Smart contracts are designed to be executed on the BC nodes in a decentralized manner. Different BCs may have different implementation methods to run code on the peer-to-peer network. For example, Hyperledger Fabric introduces an equivalent concept to smart contracts, that is called Chain Code. Chain Code can be either internally controlled and executed by a network peer (User Chain Code), or be kept in an external Docker container (System Chain Code). Docker is a lightweight technology that enables running distributed software. Docker container allows specific users to communicate with the System Chain Code by ''GetState'' and ''PutState'' interfaces [22]. Chain Codes are designed to implement business logic; therefore, this mechanism ensures that only users can access the processes implemented in a Chain Code.

Dapps (i.e., smart contracts) are applications on a blockchain platform, such as Ethereum, visible to all participating nodes. On Ethereum, they are created with a standardized language (e.g., Solidity) and can run autonomously on the Ethereum Virtual Machine (EVM) [23]. Ethereum foundation proposes EVM as a mid-layer between BC nodes and Dapps in Ethereum public BC. Smart contracts acquire their computational resources from the network peers. Dapps are autonomous executable code that run on the peers of the network via EVM and can be activated by another smart contract or an actual user by receiving a transaction. Currently, smart contracts are limited in terms of operational commands, i.e. iterations, to prevent fraudulent attacks. Also smart contract developers must be aware of the computational and storage demands while writing the code, because Dapps need to pay/reward the peers to obtain their required processing or storage resources. In general, there are two approaches in the deployment of smart contracts; state-less and state-full [8]. State-less smart contracts have no storage. They run a simple piece of code without any loops or variables and need to communicate with an off-chain back-end to perform their tasks. State-full smart contracts can implement more complex applications like state machines. In the case of Ethereum, a smart contract might use the EVM's built-in storage or might also communicate with a database or Cloud.

Currently, smart contracts have a number of limitations. For example, Ethereum smart contract operational codes are limited, e.g. limited number of iterations, so that the contract cannot stall (e.g., infinite loop) and runs out of gas. Additionally, all variables in a smart contract's code are visible to public after the smart contract is deployed on BC. This makes it hard for developers to include unpredictable random functions in the code. To guarantee security and trust, some types of function calls (references) cannot be performed in Solidity to avoid information leakage or malicious acts via autonomous contracts. According to the Solidity's documentation, the contracts must always be small and easily understandable and include fail-safe mode [24]. Atzei *et al.* [25] describe a list of common attacks on smart contracts. The cost of deployment and execution of Dapps, based on incentive mechanisms, is also another limitation preventing from running more sophisticated computations on BC, such as Artificial Intelligence (AI) analytics. Another downside of Ethereum Dapp development is that once the Dapp is deployed, it cannot be debugged or changed. Therefore, developers must be able to proof-check their code before deployment, e.g., using Satisfiability Module Theorem-based verification tools [26]. Yet, at the initial stages of development, developers can deploy and test their applications free of charge by connecting to parallel free Ethereum networks (e.g., TestRPC, Ropsten and Kovan). These networks work with free tokens, which can be retrieved either, by mining or be obtained from Ethereum faucets. After the deployment of the smart contract on parallel test networks, miners are payed with free Ethereum tokens. The testing of the Dapp is done by network peers. At this stage, users might deal with the potential errors of the Dapp that may lead to the common known Dapp development bugs [25]. Developers need to rewrite and deploy the Dapp again on the ledger each time they improve it. Finally, the tested and final Dapp can be deployed on the main Ethereum network (Mainnet).

C. BC SCENARIOS

BC solutions can be implemented based on various approaches in terms of permission and access control. BC schemes are classified as public, private or hybrid BCs.

1) PUBLIC BC

Most of BC identity and healthcare solutions use public BCs like Ethereum and smart contracts as their underlying BC technology. Public BCs, although called trust-less, govern trust because they are controlled by the consensus of the entire network and do not belong to a single entity or a group. Public BCs enable patients to have full control over their identity and information. However, the data stored on the public distributed ledgers are open to be tracked and reviewed by everyone. Storing patient's critical identity information on public BCs instead of consortium or private BCs, violates patient's privacy and the right to have some content removed.

In Ethereum, deployment of smart contracts and data storage are based on the gas fee specified for the contract. Gas fee is the reward to be paid to miners for dedicating their storage and computing resources to the contract. This reward provides incentive to miners to remain loyal to the network. Therefore, cost efficiency of smart contracts is a challenge for public BC Dapps developers.

2) PRIVATE BC

In this paper, private BCs are defined as non-public BCs. They include BCs run by a single organization or several organizations (most common case); in this case, they are called consortium BCs. Private BCs and consortium BCs are used interchangeably in the rest of the paper. Recent studies recommend the use of consortium BCs instead of public Ethereum-based Dapps for implementation of an organizational decentralized infrastructure. BCs of this type overcome performance, energy consumption and scalability issues that public BCs have. Also, they offer more control and confidentiality when managing sensitive data than public BCs. Private BCs implement semi-decentralized DLT, in which access and ownership of data is programmable; they are more flexible for use by the enterprise and organizational applications. The applications in this category are usually developed in an organization and the identity and trustworthiness of network participants are known. This makes the consensus and verification mechanism simpler when compared to public BCs.

3) HYBRID BC

Cloud Computing has been extensively used for storing, sharing, analyzing and gaining insights from healthcare Big Data. Combination of Cloud Storage and Cloud Computing with BC technology is deemed beneficial to the management of decentralized data stored on DLTs; however, realizing this combination is very challenging. BC is more reliable because of employing decentralized topology and promises lower costs for data security and access control than Cloud Computing. Cloud is less expensive than BC in terms of data storage and less complex for privacy preservation.

The integration of BC solutions with the Cloud enables large-scale interoperability and the ability to serve more sophisticated BC applications. BCs combined with off-chain storage, while more complex, ensure privacy and trust between the stakeholders by using public-private key and consensus mechanisms. As an example, Ethereum is too expensive to be purely used as Cloud Storage, as shown in [27], therefore this method benefits from the advantages of centralized and decentralized storage methods. Table 1 compares centralized and decentralized approaches.

III. TOWARDS SELF-SOVEREIGN IDENTITY

HIS contain highly personal details of individuals [28]. Self-sovereign identity represents the individuals' ability to have control over their identity and existence. Nowadays, physical and digital worlds have become tightly connected, making

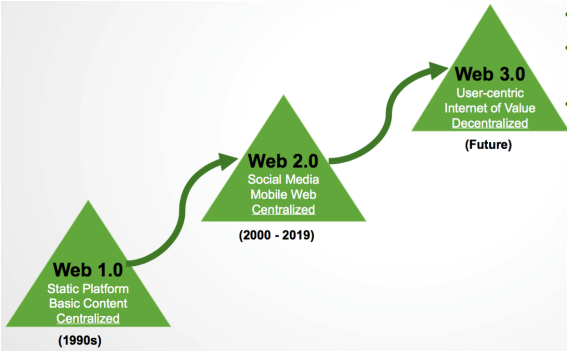


FIGURE 1. Evolution of web.

self-sovereignty of digital identity as critical as protecting physical identity.

A new challenge is answering the question: how to process a patient's digital data, while still protecting the privacy and security of patients? In conventional centralized models, preservation of patients' privacy is the responsibility of the patient's healthcare service provider. Hence, gaining access to services requires the patient's trust in his/her service provider. Conventional centralized models suffer from a number of limitations including SPoF. Therefore, patient data can be lost because of hardware or system malfunctions. Also, if data is hacked or tampered, patients will not be able to trace or recover the changes of their data. Also, moving data from one center to another requires implicit involvement of the service providers. In this regard, decentralized trust-less peer-to-peer transactions based on BC can be beneficial for patients by enabling them to take control over their own data.

The characteristics of BC technology are suitable for implementing the functionalities that must be put in place for the realization of a standardized interoperable healthcare ecosystem that supports self-sovereign identity. Regardless of the source of health data, patients are at the center of the ecosystem, since patients govern the process of sharing their health data with other players of the healthcare ecosystem.

However, some unmet challenges remain related to the use of BC in data management [29]. They are related to development of effective technology capable of fortifying data management services with the required levels of security and privacy of patient data and prevention of information leakage. This should be achieved without hampering the ability to materialize large-scale integration and powerful analytics of healthcare Big Data.

In this survey, published works are included and discussed if they cover one or more of the following topics: (1) digital identity records management; (2) self-sovereignty of patient-data; and (3) Decentralized applications for autonomous clinical operations and patient-data records. Table 2 shows a list of the existing solutions we did cover. They have been developed using various systems, such as Bitcoin, Ethereum and Hyperledger. Under "Other Systems" we include projects that are built upon NEO, Ocean, Blockstack,

TABLE 1. Comparison between centralized and decentralized approaches.

CENTRALIZED: CLOUD STORAGE AND COMPUTING	DECENTRALIZED: BLOCKCHAIN (BC)
Single Point of Failure (SPoF)	Redundant copies of records assures security
Centralized control and administration	Consent algorithms (Proof of Work (PoW)/ Proof of Stake (PoS) etc.) using incentives to encourage users to participate in network governance
Powerful processors and high capacity storage	Expensive processing and limited storage capacity
Expensive infrastructure for the service provider	Processing power and storage is dedicated to the network by the users
Maintenance and protection of data is the responsibility of the Cloud service providers	Trust-less network in which data and privacy protection is the user's responsibility
Far smaller electricity consumption	High electricity consumption especially for BCs using PoW (e.g., Bitcoin currently consumes more energy than Switzerland)
Less latency	Public BCs using PoW have long transaction confirmation times
More scalable	More scalable
Faster response time	slow response time (a.k.a. confirmation time); e.g., at least 10 minutes for bitcoin.

GEM and some application specific BCs. According to Table 2, it is perceivable that the modern web is moving towards value-creation based on personal data. Basic BC solutions target the challenges encountered in Web 2.0, namely governance, control and protection of personal or organizational data.

The category of data control and protection can be grouped into two types of solutions. The first type of solutions corresponds to solutions that introduce an anonymous decentralized alternative for the internet. For example, ZeroNet [30] promises uncensored open internet using various existing peer-to-peer anonymity solutions, such as Bitcoin's cryptography, TOR onion hidden network [31] and BitTorrent's file-sharing [32]. Offline access to websites, blogging and email services are made possible by ZeroNet network [33]; online services are hosted and distributed through the peer-to-peer network (i.e., users that have accessed the services previously. For example, one can view a website by downloading its content from previous visitors).

The second type of solutions introduces decentralized schemes to the integration and convergence of data generated by numerous sources of digital information. For example, Factom [34] provides BC-based data integrity solutions for enterprise platforms. Factom introduces the Proof of Existence (PoE) data verification mechanism for Bitcoin BC [35]; it is based on a different concept than verifying financial transactions using Bitcoin's PoW. Factom's goal is to prove that enterprise data has been collected at a point in time and the changes on the collected data have been time-stamped in BC. Therefore, the progress of data during time is trackable. Data can be logs of security cameras' feeds, account balances, etc.

As we move forward, the solutions become more sophisticated covering digitization of personal identity, social data, patient's data and their use in business applications and services, such as insurance. One major application of BC in the area of digital identity is to build a decentralized Identity as a Service (dIaaS). For example, a comprehensive approach to digital identity is presented in the Sovrin project [36] that uses Hyperledger Indy [37], a specialized tool for digital identity. Sovrin integrates and converges different aspects of digital identity, ranging from physical addresses and identity cards to login credentials. In the proposed model, the data is stored either in organizational data silos or BCs and DLTs. Sovrin converges data into one decentralized identity solution. In cooperation with organizations, Sovrin formed a decentralized trust ecosystem called Stewards [38]. Other similar solutions for dIaaS include Remme [39], NodalBlock [40], Nuggets [41], SecureKey [42], NameCoin [43] and Procivis [44]. The major motivations to build dIaaS include: (1) standardizing machine-readable digital identity; (2) solving the problem of having to keep multiple credentials for identification by different digital entities using asymmetric encrypted keys; and (3) elimination of the ''hidden man'' from the credentials verification.

The next level, after integration of different aspects of identity, is the adoption of dIaaS in the official authentication and verification processes, also known as Know Your Customer (KYC). For example, IdentityMind [45] proposes electronic DNA (eDNA), a multi-layered KYC approach, to solve the challenge of authentication when physical and digital identities are combined. The proposed KYC model employs artificial intelligence (AI); it can verify information, such as name, address, phone and government issued ID, and link it to the corresponding digital identity. Other solutions that target BC-based KYC include Bridge [46], Civic [47], Evernym [48], NodalBlock [40] and uPort [49].

With BC-based digital identities, physical and digital identities are combined. This led to the introduction of innovative biometrics recording solutions based on BC. For example, Biometrids [50] employs machine learning for identification of individuals by face recognition. Digital information regarding the three-dimensional (3D) facial characteristics is encrypted and considered as unique credentials for an individual like fingerprint. However, this method is vulnerable to attacks where hackers are able to imitate a 3D model of their victim's face.

Hajialikhani *et al.* [51] introduce the Proof of Unique Human mechanism. In this system, biometrics data, like finger prints, DNA, iris and face scan of individuals, are

TABLE 2. Self-sovereignty solutions classification.

CLASS	SCENARIOS	BITCOIN	ETHEREUM	HYPERLEDGER	OTHER SYSTEMS
Data Control & Protection	Blockstack [61]	-	-	-	✓
	Dock.io [62]	-	✓	-	-
	ZeroNet [30]	-	-	-	✓
	Ocean protocol [63]	✓	-	-	-
	Jolocom [64]	-	✓	-	-
	Pickiochain [65]	-	-	-	✓
	Yourblock [66]	-	✓	-	-
	Persona [67]	-	-	-	✓
	Synapse AI [68]	-	✓	-	-
	Essentia.one [69]	-	-	-	✓
	Factom [34]	-	-	-	✓
Digital Identity	Biometrids [50]	-	✓	-	-
	BlockchainHelix [70]	-	-	-	✓
	Bridge [46]	-	-	-	✓
	Civic [47]	-	-	-	✓
	evernym [48]	-	-	✓	-
	Identitymind [45]	-	-	-	✓
	Remme [39]	-	-	✓	-
	NodalBlock [40]	-	✓	-	-
	Nuggets [41]	-	✓	-	-
	Procivs [44] and Vetri [71]	-	✓	-	-
	Secure Identity Ledger [72]	-	-	-	✓
	Secure key [42]	-	-	✓	-
	Uniqueid [51]	-	✓	-	-
	Uport [49]	-	✓	-	-
	Sovrin [36]	-	-	✓	-
	Namecoin [43]	✓	-	-	-
Social Data Governance	Aragon [73]	-	✓	-	-
	Bitnation [54]	-	✓	-	-
	BoardRoom [56]	-	✓	-	-
	Colony [57]	-	✓	-	-
	Coin governance system [58]	-	✓	-	-
	DemocracyEarth [59], [60]	-	-	-	✓
Healthcare & Patient Data	MEDIBLOC [74], [75]	-	-	-	✓
	AMBROSUS [76]	-	✓	-	-
	ScriptDrop [77], [78]	-	✓	✓	-
	HealthWizz [79]	-	✓	-	-
	ProofWork [80]	-	-	✓	-
	Dentacoin [81]	-	✓	-	-
	MedRec [82]	-	✓	-	-
	Gem [83]	-	-	-	✓
	SimplyVital Health [84]	-	✓	-	-
Social Insurance	Bandboo [85]	-	-	-	✓
	Etherisc [86]	-	✓	-	-
	Timbrella [87]	✓	✓	-	-

measured by certified entities, called ''verifiers''. For each individual, a unique identification is generated and the measured data is added to BC. The consensus mechanism makes the assumption that elites, which are entities well trusted in the society, such as university professors and public figures, can be employed in the verification mechanism of the network, since they have less incentive to sabotage the system. Each transaction needs to be verified by at least three verifiers. Also transparency and Completely Automated Public Turing test, to tell Computers and Humans Apart (CAPTCHA) [52], are other security mechanisms that are used in the proposed system.

The social data governance's focus is on the role of self-sovereignty in the social engagements. Accordingly, social engagement refers to social activities that include participation, interaction and transaction of individuals in a community [53]. BC promises end-to-end solutions for social interactions, which in comparison to conventional methods, are smoother and friction-less because these solutions remove the role of multiple public notaries in the bureaucracy

and jurisdiction of such interactions. According to a timeline presented in the BitNation's whitepaper [54], BC is a medium that facilitates the evolution of existing governance schemes towards Holacracy. According to [55], Holacracy is a scheme for decentralized organizational management, governance and decision-making. Holacracy is not confined to hierarchies and consists of many self-organizing entities.

Decentralized digital identities on BC and autonomous smart contracts enable border-less universal encrypted IDs on BC. Every entity that has access to BC, regardless of his/her geographical location, can engage in social activities, join communities and even create border-less organizations. Various social and governmental interactions can be redesigned and implemented using end-to-end approach by smart contracts, i.e. voting, marriage and inheritance. The consequence is that decentralized global organizations, companies, communities and governments are implementable by BC, also known as Distributed Autonomous Organsizations (DAO). Table 2 shows that almost all of the social data solutions have been implemented using Ethereum smart contracts; this is because the major enabler of this class of self-sovereignty solutions is the autonomous code that runs on top of identity data recorded on DLT. Existing social data governance solutions include Aragon [55], BitNation [54], BoardRoom [56], Colony [57], Coin Governance System [58], and DemocracyEarth [59], [60].

Programmable digital identity on DLT is the backbone for various social services dealing with identity and personal data. The last two classes of self-sovereignty in Table 2, namely ''healthcare and patient data'' and ''social insurance'', represent the applications of BC in the patient data management, BC-based data-driven healthcare and insurance services. In section IV, the classes of ''patient data'' and ''social insurance'' will be discussed in detail.

The list in Table 2 presents research contributions from academia and BC-based startups that have set their goal on providing social and healthcare data-driven solutions. Most of the solutions in Table 2 have been developed on the Ethereum platform, with most having produced initial versions, and working towards the development of new improved ones. Ethereum is the favourite choice to start developing Dapps. At current time, the number of those Dapps under development, having reached the proof-of-concept stage, is not large.

IV. PATIENT DATA MANAGEMENT

Fig. 2 shows the classification of BC health care applications and the advantages BC technology provides to each one of them. The characteristics (see Fig. 2) are based on the contributions of the papers and applications studied in preparation of this survey. The significant features of BC in these applications include timestamped immutable data history, autonomous smart contracts, decentralized verification, interoperability, transparency, gamification and decentralized value transfer.

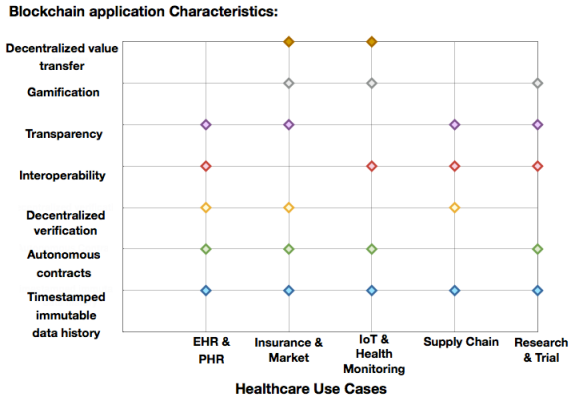


FIGURE 2. BC characteristics in healthcare use cases.

Binding digital identity with health data, keeping a holistic standard electronic record of patient's health data and creating an interoperable health ecosystem are key challenges in healthcare that can be addressed by BC.

A. PATIENT DATA

Various types of health data can be stored on BC. Two categories have been identified [88]–[90]: (1) self-reported data that is recorded by third party lifestyle applications, such as wearables, monitoring devices and mobile pedometers, social networks, Body Area Sensor Networks (BASN) and smart home services; and (2) health and medical data currently placed in the existing HIS databases, i.e. medical records, lab results, diagnosis history, as well as data that the user adds to her/his HIS upon request, i.e. reporting health status to the family doctor periodically. Other static data include date of birth and description of physical appearance or social records. The collection of aforementioned data represents the personal attributes and digital identity of an individual for HIS. Since, there are various sources of data, the size of data may also increase as the number of information sources increase. Each of these data sources can be subject to breaches; therefore, each source is responsible for the handling and management of the data they produce [91]. Also, the sources need to understand each other's data.

European Union General Data Protection Regulation (EU GDPR) is the latest important change that strengthens the protection of user privacy. Accordingly, these rules reduce the control of European companies across all sectors on their client data and enable clients to access data and be informed of the possible attacks on their data. Clients are also able to request the company to erase their data or move them to another controller [92]. However, self-sovereign identity is the next level of privacy, in which people directly control the transactions made on their health data [89].

B. DECENTRALIZED IDENTITY MANAGEMENT SYSTEMS (IDMS)

IdMSs are enterprise systems developed to manage individual data and control actions, such as authentication, authorization

and access. These systems can be used for cross company data management. In this regard, BC can be an alternative implementation model to achieve decentralized IdMS. This model shifts the ownership of health data to patients, completely or partially. Examples of BC-based IdMS are covered in Table 2 under the Digital Identity class. Via decentralized IdMS, patients don't have to trust and consent to third parties to obtain services for registering, updating, revoking and looking-up their own digital identities [93]; indeed, they can independently perform such tasks using their public and private keys.

V. HEALTHCARE INFORMATION SYSTEMS (HIS)

HIS is a system for collection, storage, management and exchange of healthcare data. These systems are designed both for patients' medical care and to facilitate clinician operational processes. Esposito *et al.* in [94] define three types of HIS; Electronic Medical Records (EMR), EHR and PHR. EMR is a digital history of clinical and medical diagnoses recorded at a single practice or by a particular clinician or nurse. EMR cannot be connected to other sources of data. In comparison to EMR, EHR cover more sources of information, i.e. EHR may contain a practitioner's diagnosis and prescriptions, lab results in the form of images/data and/or emergency room records. EHR also support data exchange standards and patient portability between different entities. On the other hand, in PHR, patients are involved in the collection and monitoring of their data. New sources of information, e.g. smart phones or wearable devices or other entities, require the patient's consent to be able to record the history. Furthermore, the patient has to approve if he/she wishes to make the data accessible to a certain entity.

A. ELECTRONIC HEALTH RECORDS (EHR)

EHR systems are used extensively in hospitals; they are systems that gather all the medical information of patients in a computer readable format. In comparison to the conventional paper-based systems, they enable smoother and faster communication and data sharing among clinicians. Furthermore, EHR converge data of various silos; therefore, data in EHR can be utilized to achieve more concise interpretations [95]. Data management is one of the challenges facing EHR. Connecting and integrating multiple EHR is another challenge, because each might follow different data coding schemes [96]–[98]. Therefore, having a standardized scheme is essential to achieving interoperability of EHR, which would lead to an integrated healthcare ecosystem.

According to the authors of [99], healthcare interoperability solutions come in two forms: institution-driven and patient-driven. Institution-driven schemes involve various healthcare entities in order to integrate and exchange healthcare data located in EHR. EHR is intended to be used by institutions to manage patient's data; therefore, the implementation of EHR is part of institution-driven solutions. To form a network of EHR they need to be standardized in terms of interoperability, safety/security, quality/reliability, efficiency/effectiveness, and communication [100]. Data exchange needs to be accurate, effective, consistent and reusable by the systems in order to ensure they produce meaningful information [101].

The International Organization for Standardization (ISO) defines two types of interoperability [100], namely functional and semantic. If the EHR facilitates human-readable data exchange between multiple HIS, it is classified in the functional EHR category. Semantic interoperability means data exchange is performed in a format that data can be further analysed and processed by the receiving HIS. In another perspective, interoperability can be classified in three groups; foundational, structural and semantic [102]. Foundational standards only support data exchange from one system to another. Data can be interpreted by human operators but not by HIS. In structural standards, exchanged data fields can be interpreted; this means that data types and fields are recognizable by all participating HIS. The highest level of interoperability is achieved by semantically interoperable systems, in which meaningful conclusions can be reached from EHR by performing computerized analysis on the structured health data. Furthermore, Gupta *et al.* [103] propose two categories for EHR interoperability; syntactical and semantic interoperability. Syntactical interoperability refers to standardizing the health data structure, syntax and HIS' communication protocols. In addition to simplifying data exchange between multiple organizations, semantic interoperability ensures that meaningful interpretations can be produced by computer analysis tools. Semantic interoperability has been a common concept in all of the above mentioned classifications. Through semantic interoperability, health organizations will not need to follow a standard EHR grammar or syntax in order to be able to cooperate; however, they can integrate together semantically [104].

There exist important EHR interoperability standards; these include OpenEHR [105], ISO EN13606 [106], Digital Imaging and Communications in Medicine (DICOM) [107], Direct Trust [108], and Health Level 7 [109]. Most significantly, HL 7 defines a set of standard messaging grammar and communication protocols for data exchange within and outside healthcare systems [100]. Some EHR standards by Health Level 7 (HL 7) include: HL 7 v2.0, HL 7 v3.0 Clinical Document Architecture (CDA) and HL 7 v4.0 Fast Healthcare Interoperability Resources (FHIR). More details about EHR standards can be found in [103], [110]. According to [110], HL 7 v4.0 FHIR is stronger than the two older versions in terms of encryption. All three versions of HL 7 support Secure Socket Layer (SSL), which is used to create an encrypted link between EHR and safeguard sensitive patient data. This ensures that data can only be read or modified by authorised users of the communicating EHR. In general, SSL communications can be secured both with Pre-Shared Key (PSK) or Public Key Infrastructure (PKI); this means that HL 7 v4.0 FHIR provides support for symmetric and asymmetric encryption. In communications between HL 7 v4.0 FHIR compatible EHR, Transport Layer

Security (TLS), a more secure version of SSL, can also be utilized [111].

It should be pointed out that the integration of different versions of HL 7 is not an easy task. Since HL 7 v2.0 EHR are only compatible with EHR built on the same standard, HL 7 v3.0 does not support communication with HL 7 v2.0; furthermore, HL 7 v4.0 FHIR has only limited compatibility with v2.0.

The newest HL 7 standard, HL 7 v4.0 FHIR, is based on the HyperText Transfer Protocol (HTTP)-based REpresentational State Transfer (RESTful) architecture. As RESTful defines an API architecture for web services, FHIR is considered as an internet-based EHR standard. Therefore, data elements or resources are addressed with identifiers similar to URLs of web pages.

According to [112], in HL 7 standard releases, consent to the exchange of user data has been defined. These definitions are as follows: HL 7 V3.0 Domain Analysis Model (DAM), HL 7 V3.0 CDA1 (consent), HL 7 V4.0 FHIR (consent) and HL 7 V2.0 (consent segments). The consent mechanism in the aforementioned standards are explicit and patients depend on external servers [113], as HL 7 mainly employs Security Assertion Markup Language (SAML) and eXtensible Access Control Markup Language (XACML) to allow users influence their data exchange. However, one cannot achieve self-sovereignty via existing standards. To address this limitation, there have been some research contributions (e.g., [114] and [115]) targeting the development of a decentralized interoperability approach, by combining BC mechanisms with HL 7 standards. Furthermore, in a 2016 study by IBM, DLT has been predicted to be an effective secure interoperable solution for implementing EHR [116].

B. PATIENT HEALTH RECORDS (PHR)

Patient-driven data management follows the same concept as EHR; however, in this case, patients have ownership controls and on-demand access to their health and medical data. Therefore, data exchange between the healthcare entities require consent from the patients. Patient-driven interoperability approach is called PHR.

DLT features are applicable to realize this approach [117]. Indeed, DLT as a decentralized infrastructure, is used to encrypt and store unified data, as well as ensure security and privacy of users besides interoperability. In DLT, patients' data can be accessible by any peer in the network. Public BCs employ transparent DLT approach, in which transactions are visible to any network node. However, other approaches for organizational DLTs use different data access controls; they can also be used to implement interoperable healthcare applications.

With the DLT-based patient-driven EHR, new applications are made possible. For example, insurance companies can seamlessly access the stream of health and medical records of patients. Based on this data stream, health insurance companies can define healthy lifestyle incentive models, and design customer-specific bonus packages [118]. Examples of these packages include: (a) rewarding discounts to healthy clients that are active in sports based on data they consent to be gathered from their wearables or mobile phones; (b) developing a reputation based insurance program, in which clients compete with each other in keeping healthy habits and earn tokens in return; (c) encouraging patients to share their activity data in return for tokens; and (d) enabling patients to pay for side services, such as extra insurance coverage, using tokens.

VI. BC-BASED PATIENT IDENTITY AND DATA MANAGEMENT SYSTEMS

Table 3 compares the characteristics of healthcare BC solutions. The comparison factors are: incentive, data market, enabling PHR, decentralized asset tracking, Web/Mobile Application, IoT, EHR compatibility/interoperability and proof-of-concept implementation.

The incentive factor in Table 3 indicates whether the solution has employed BC to design an application that incentives participants, e.g., the crowed-sourcing applications that reward participants based on their engagement with the application. Data market factor indicates whether the solution enables (a) users/clients to earn money by enabling access to their data; or (b) service providers to create value based on data they request from their clients. The enabling PHR field is checked if the application has a patient-driven approach. If the application enables registration and auditing/inspection of information/physical objects on the DLT, then it has the decentralized asset tracking feature. Some applications have developed Web/Mobile applications for their use cases and realize Web 3.0. Service providers that have developed application-specific embedded device(s), have IoT field checked in Table 3. Because they have developed an application-specific embedded device for their services. Furthermore, EHR compatibility/interoperability has been checked for applications that aimed at standardization and integration of EHR to improve the interoperability between health organizations. Finally, proof-of-concept implementation indicates that the solution is already developed and its source code is available.

The solutions shown in Table 3, aim to realize EHR and PHR to some extent. The main target in most solutions is distributed identity and health record-keeping; patient-driven healthcare; and peer-to-peer interoperability of patients with experts and experts with experts. We classify the architectures used by existing solutions for identity data management and interoperability between the healthcare ecosystems into three classes: decentralized, hybrid and pseudo-BC architectures.

1) DECENTRALIZED ARCHITECTURES

This class uses only BC technology for patient data management. For example, Simply Vital Health [84] is implemented entirely on Ethereum BC and smart contracts. According to Health Nexus system's proposed architecture, the BC mechanisms are paired with distributed storage mechanisms based on Maymounkov and Mazieres [119] and Storj [120] to avoid keeping health data in centralized storage systems. Kademlia

TABLE 3. BC healthcare application specification comparison.

BC-based PHR	Disributed Ledger Technology	Data management and Privacy	Feature Comparison							
			Incentive	Data market	Enabling PHR	Asset Tracking	Web/Mobile App	IoT	Interoperable	Proof of Concept
OmniPHR [135]	Multi-BC (Private BC + openEHR + ISO 13606)	Apache (Kafka + Zookeeper + Storm + Spark) + OpenLink Virtuoso	X	X	✓	X	✓	✓	✓	✓
MEDIBLOC [74], [75]	Delegated PoS + QRC20 token	Merkle Tree root as key + key-value DB	X	✓	✓	X	✓	X	✓	✓
ScriptDrop (Pharmacies and deliverers only) [77], [78]	PoS (Eth) + ERC20 token	Permissioned Hyperledger Fabric	✓	X	X	✓	X	NA	NA	NA
HealthWizz [79], [115]	PoS + ERC20 token	Local storage or Cloud Services	X	✓	✓	X	✓	✓	✓	NA
Dentacoin (Specialized for Dental care) [81]	PoS + ERC20 token Ethereum ledger	On public ledger	✓	X	✓	X	✓	X	✓	NA
MedRec [82], [146]	PoS	SQLite or any similar DB	X	✓	✓	X	✓	X	✓	✓
Gem [83]	GemOS specialized platform for healthcare	Compatible with multiple storage methods	X	X	✓	✓	✓	X	✓	NA
Simply Vital Health (Health Nexus) [84]	Consortium BC (Modified Ethereum)	Data storage contracts	X	✓	✓	✓	✓	X	✓	✓
Zhang et al. [114], [147]	PoS	Fire-walled database	X	X	✓	✓	✓	X	✓	✓
Thwin et al. [126]	Private/Consortium	Cloud (encrypted data) + Gateway Server (metadata/access log)	X	X	✓	✓	✓	X	X	NA
Gou et al. [144]	Proposes attribute-based signature	Cloud	NA	NA	✓	NA	NA	NA	✓	NA
Dubovitskaya et l.. [125]	Hyperledger	Cloud + local storage + BC	NA	NA	NA	NA	NA	NA	✓	NA
Auditchain [121]	Hyperledger	Obfuscated hashed text on BC	NA	NA	✓	✓	✓	NA	✓	✓

is a Distributed Hash Table (DHT) used for fault-tolerant data exchange and routing in distributed networks. Moreover, Storj is a distributed storage platform that enables users to rent their storage system in a peer-to-peer network. The Health Nexus architecture is also compatible to communicate with off-chain storage systems. Health Nexus' token is called Health Cash.

Anderson, in [121], proposes Auditchain, which is implemented using Hyperledger. Auditchain is concerned with implementing EHR based on permissioned BC, to contain data in one single BC for simplifying logging, auditing logs and data analysis. The first layer of Auditchains architecture stack is the Hyperledger Fabric BC. The peers of the permissioned BC are the hospitals, clinics or doctor's offices. These peers require certificate to join the network to prevent malicious insertion of data to the log. Next layer consists of Hyperledger Chain Codes, running on the peers that are responsible for unifying the log data format, returning the response to client queries and inserting new entries to the ledger. In addition to the overhead data, that includes author ID, data type and ID., data is stored in obfuscated text form which is generated by either encryption or hashing. The third layer is the application layer where a NodeJS back-end communicates with BC via Hyperledger Fabric APIs. On top of the stack, API endpoint creates an interface between users and Auditchain that accesses the back-end to fetch user's queries.

2) HYBRID ARCHITECTURES

This architecture is used in the case of complex applications that deal with large amounts of data and need to follow

healthcare standards. For example, Medibloc team [74] has designed a new interoperable BC-based healthcare data system, called Personal Health Record. Medibloc's system design consists of three layers: (1) core; (2) service; (3) applciation. The core layer uses Qtum BC [122], and is responsible for secure data exchange and transparent record keeping. Healthcare data, like images, may be very large; thus, patient data is stored in centralized key-value data storage systems, like LevelDB [123] and RocksDB [124]. Additionally, Merkle tree is employed to manage data storage and control the accessibility of peers to certain parts of the data. Indeed, data is converted to a hash using the Merkle tree. Thus, only the root of the tree is stored in BC, as the key to the data that is stored whether in the user's devices or some centralized storage systems. The key is generated by encrypting the data and can be only de-crypted by the owner of the data who has the private key (asymmetric encryption). Since Qtum BC uses EVM for implementing smart contracts, in the second layer, fundamental services are developed based on smart contracts running on EVM. The second layer retrieves data from the core layer and provides data to the off-chain entities in the application layer. Application layer utilizes healthcare information it receives from the lower layers to implement off-chain services that are accessible through web or mobile platforms. There are three types of storage in this architecture: BC, User's devices and Data centers. Medibloc also targets data marketing by introducing two types of tokens; internal token, called Medi Point, and external token, called Medi token. Internal tokens can only be exchanged within the platform, while external tokens are tradable like every cryptocurrency. Medi point is tied to the amount of patient data generated by medical practitioners and participation of entities inside the platform. Medi token allows socio-economic interactions both within Medibloc users and Medibloc users with other BCs.

Dubovitskaya *et al.* [125] propose a hyperledger-based platform that covers three scenarios: patient care, medical research and connected health. The platform uses a hybrid architecture. It is designed for hospital interoperability, in which each hospital is considered as a node of BC; it also makes use of an off-chain local database, that stores patient data, on-premise. Each hospital can register users on BC; nodes are connected to an off-chain membership service that authenticates and verifies the identity of patients. Moreover, all nodes need to be connected to the national practitioner's data bank to certify doctors and prevent fraudulent attacks. Users register to BC only after having been checked by these two entities. Additionally, all hospitals are connected to a Cloud server to store and categorize patient data. On every node, a Hyperledger Chain Code acts as an additional validation mechanism to the aforementioned centralized services.

In the model proposed by Thwin and Vasupongayya [126], users encrypt their data through a set of proposed steps, and then send the encrypted data to a gateway. Subsequently, the gateway receives data and stores the encrypted data on the Cloud Storage. The gateway maps data to a certain ID and then stores this ID both on a local server and a private BC. User can access data by sending a query in a predefined format to the gateway. The gateway is also responsible for authentication and validation of the user's data access queries, retrieving and re-encryption of data from the Cloud Storage.

Zhang *et al.* [114] propose the FHIRChain architecture for health resource exchange and interoperabiliy by addressing the requirements of the two existing interoperability standards; (1) Office of the National Coordinator for Health Information Technology (ONC) Health IT Certification Program [127]; and (2) HL 7 v4.0 FHIR standards [128]. In the proposed architecture, pointers to various types of FHIR compatible databases are registered in BC. The authors have developed a number of Dapps using Javascript and Solidity on a private test network for Ethereum BC. The architecture gathers data, in a common standard signature format, from multiple sources and facilitates access to data for Medical professionals.

In [115], the developers of HealthWizz propose a HL7 FHIR compatible architecture. FHIR compatible database stores data and a key to the data is encrypted and recorded on the Ethereum BC. Users add data to BC by submitting the data to a front-end application, that is developed using the web tools, such as ECMA6, HTML5, AngularJS and React JS. The front-end application verifies the user credentials, stores the main data on a centralized Cloud service, such as Google Drive, Microsoft OneDrive and Dropbox etc. Then, it hashes the data and sends the hash to a smart contract. The contract verifies the user and the hash, and records the hash in BC. When, someone needs to retrieve data from the healthcare information system, he/she has to send a request to the front-end application. In this stage, the data owner is asked if he/she approves the data seeker. If the response is yes, the application will provide the seeker with an access key by triggering a data sharing smart contract for the seeker. The access key enables the seeker to access the database and retrieve data, if verified by the FHIR Cloud server. The FHIR server runs OAuth 2.0 for privacy [129].

By combining BC and off-chain storage, Zyskind *et al.* [130] propose a BC-based data management system that can be used for a trusted data storage and computing platform. In this system, data is kept off-chain, in a centralized key-value database; it is a combination of Maymounkov and Mazieres [119] DHT and LevelDB [123] key-value storage. The distributed ledger holds the key to the data. DLT allows two types of transactions: (1) access management for authentication; and (2) data storage/retrieval queries.

OmniPHR [131], which builds on [131]–[136], evaluates various BC systems, such as Hyperledger Fabric and Ethereum, and proposes an application specific BC. This work [131] specifically focuses on private BCs, based on Hyperledger Platform; it combines these via a middleware, called OmniPHR, with various tools from Apache organization for data exchange, processing and management, such as Kafka [137], Zookeeper [138], Storm [139] and

Spark [140]. The healthcare data is stored in OpenLink Virtuoso database [141]. To the extent of our knowledge OmniPHR is the only work among the literature that uses OverSim [142], a p2p network simulation tool built on a common network simulator like OMNeT++ [143], to evaluate the performance of their proposed private multi-BC architecture, in terms of behavior of the network participants and scalability of the network. The measurements include the effects of network size and load on various parameters such as routing, hop count and latency.

3) PSEUDO BC ARCHITECTURES

These solutions employ some BC features, such as Byzantine Fault Tolerance (BFT), time-stamped data aggregation and assymmetric authentication, to answer some open research problems of healthcare. Although these solutions are not decentralized, they have taken advantage of BC features to overcome some bottlenecks in EHR and PHR. In the solution proposed by Gou *et al.* [144], every patient has a chain of blocks. A new block is added to the patient's chain of blocks at each visit to a clinic, doctor or hospital. Hence, a history of all visits and health records can be viewed by referring to each patient's chain of blocks. There is a verifier (miner) role in this architecture. As the patient adds his/her health data to his/her chain of blocks, miners access data and verify its correctness. Although the chains of blocks are stored in centralized Cloud Storage, the authors state that they have used BC's signature mechanism in their centralized solution. The authors propose the Multiple Authorities Attribute-based Signature (MA-ABS) scheme, which is a filtering mechanism that is based on signature, to control access of multiple entities to patient data.

Bauer *et al.* in [145], identifies a key limitation in existing PHR. It is the lack of a mechanism to enable health providers to securely control the records they add to PHR. This means, they need to be able to select parts of data, they consider confidential, which should not be released. Also, another challenge is to enable patients to share their data by filtering them, for example based on the source of the data. Adding this mechanism to PHR will improve patient privacy and also confidentiality of patient care data. The proposed scheme is not using BC. However, it proposes a cryptographic credential system with three roles; (1) prover: an entity that owns cryptographic records signed by a certifier; (2) verifier: an entity that views data received from the prover and needs to authenticate if data has not been tampered since recorded (certification check); and (3) certifier: any entity that generates data, medical institutes, doctors and patients, who need to sign their records.

VII. SUMMARY AND CRITICAL ANALYSIS

A. SUMMARY

In this paper, we studied the state-of-the-art in data management and self-sovereignty in healthcare. This study uses the following inclusion criteria to select related works: (1) digital identity records management; (2) self-sovereignty of patient-data; and (3) decentralized applications for autonomous clinical operations and patient-data records. There have been many contributions that have set as their goal to implement self-sovereign IdMS using BC. The focus of these contributions can be classified into five groups, namely data control and protection, digital identity, social governance, healthcare and patient data, and social insurance. More specifically, there have been significant contributions in the area of healthcare and patient data management in terms of implementing both institution-driven and patient-driven, namely EHR and PHR, subsequently. EHR and PHR models are the representation of the evolution towards semantic web (i.e., Web 3.0). In the semantic web, patient data needs to be collected, restructured and processed to obtain improvement in healthcare services. Hence, the importance of keeping self-sovereignty of patient's data must be taken into account. DLT based on BC is a promising method to implement patient-data management and self-sovereignty. Indeed, BC offers many features, such as transparency, immutable decentralized record keeping and interoperability.

In order to enable healthcare BC services, it is essential to implement decentralized patient data and digital identity records. Fig. 3 illustrates that EHR and PHR are at the core of BC applications for healthcare. Successful patient data and digital identity management leads to the development of more advanced applications, such as (1) IoT: medical devices/sensors generate healthcare related data; (2) research and trial using patient's data; (3) supply chain for healthcare related services; and (4) healthcare insurance: can use patient's data for more adequate services. EHR and PHR will provide a foundation to seamlessly timestamp, record and associate data gathered from various services to patients' digital identity on BC. For example: (1) recording healthcare IoT devices used by patients; (2) using data, from various sources recorded on BC-based PHR, medical researchers and practitioners can retrieve insights and/or make predictions; (3) the production history of medicines/drugs can be tracked from the manufacturing process to the pharmacy's customers; and (4) insurance companies can have access to the whole or partial history of patients' health records and offer consumer specific services.

There have been many attempts for realizing interoperability of healthcare organizations utilizing various approaches to implement BC: (1) fully BC-based architectures: They use BC for data management, access control, verification and storage; and (2) partially BC-based architectures: they use BC for storage of hashed/encrypted keys of data and centralized storage systems (e.g., Cloud servers or local data centers) to store data.

B. CRITICAL ANALYSIS

There are still unsolved challenges in developing a BC-based HIS.

Firstly, as Table 3 shows there is still lack of a standardized implementation method for BC-based EHR and PHR.

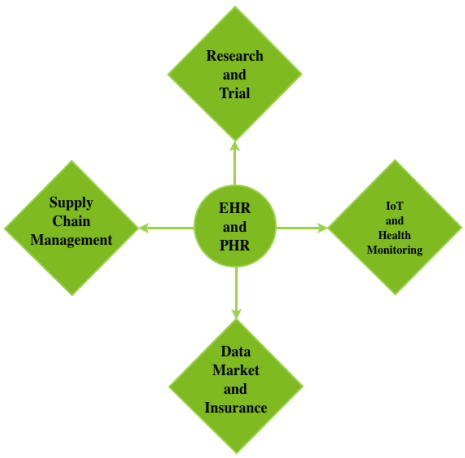


FIGURE 3. EHR and PHR as the driver for BC healthcare application classes.

Existing solutions have chosen different storage approaches, BC consensus algorithms, encryption and permission scenarios. Accordingly, comparison and evaluation of the existing solutions becomes hard due to lack of a standardized implementation method. However, as Table 3 shows, most existing solutions use hybrid architecture (BC and centralized systems) to achieve the benefits of both centralized and decentralized HIS implementation methods.

Secondly, the existing solutions are mostly in beta or test stages. Dapps cannot be debugged and tested after deployment on BC. Early stages of Dapps on BC are error prone; therefore they are not trustworthy. As a result, most existing solutions are not ready to be used in real-world applications. Additionally, BC development frameworks are still under development and not complete. Indeed, the technology still has some open privacy and security issues to be investigated such as quantum-resistance.

Thirdly, after reviewing the literature, it is perceivable that existing EHR and PHR deal with the trade-off between various parameters. More specifically, designers/developers should carefully consider the trade-off between decentralization, privacy/security and throughput when designing BC based healthcare systems.

VIII. CONCLUSIONS AND THE FUTURE RESEARCH CHALLENGES

In conclusion, most of the discussed use-cases in this paper were developed using the first and second generation of BCs. The majority of the currently developed use-cases focus on cryptocurrency (BC 1.0) and smart contracts/Dapps (BC 2.0). The third generation, BC 3.0, connects Dapps to form DAO. In more complex scenarios, connecting DAO form Decentralized Autonomous Societies (DAS). This study did show that BC-based EHR and PHR are essential to realize a distributed autonomous healthcare ecosystem. Such an ecosystem includes; (1) IoT; (2) research and trial;(3) supply chain; and (4) healthcare insurance. Akande [148] reported that most existing solutions did investigate the capabilities of the technology; however, the overall impact of the technology on the healthcare ecosystem and the entire value chain are still to be studied.

The initial objective fueling the design of pure BC solutions is the elimination of intermediaries and decentralization to achieve distributed trust. The patient's privacy protection and the right to be forgotten are possible but not completely met in the hybrid BC architectures which are the most reliable existing solutions. All existing solutions have addressed this problem but none has presented a firm answer or proof of concept for that.

To conclude, we enumerate five Research Challenges (RC) that need to be investigated to realize the envisioned DAO and DAS (BC 3.0) particularly for healthcare systems:

- **RC1:** Trade-off between decentralization and privacy in hybrid BCs.
- **RC2:** Realization of the highest possible benefits of decentralization for hybrid BCs use-cases.
- **RC3:** Integration of centralized storage systems and BC-based decentralized EHR and PHR.
- **RC4:** Implementation of DAO and DAS to form a decentralized autonomous healthcare ecosystem.
- **RC5:** Implementation of a proof of concept for EHR and PHR while taking into account RC1, RC2 RC3 and RC4.

REFERENCES

[1] Bitcoin. *Bitcoin—Open Source P2P Money*. Accessed: Dec. 22, 2019. [Online]. Available: https://bitcoin.org/en/

[2] *Proof of Work (POW)*. Accessed: Apr. 14, 2020. [Online]. Available: https://en.bitcoin.it/wiki/Proof_of_work

[3] M. Vaishnnave, K. S. Devi, and P. Srinivasan, "A survey on cloud computing and hybrid cloud," *Int. J. Appl. Eng. Res.*, vol. 14, no. 2, pp. 429–434, 2019.

[4] R. Beck and C. Müller-Bloch, "Blockchain as radical innovation: A framework for engaging with distributed ledgers as incumbent organization," in *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, 2017, pp. 1–10. [Online]. Available: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1684context=hicss-50

[5] *Hyperledger Fabric*. Accessed: Dec. 22, 2019. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.4/

[6] *R3 Corda*. Accessed: Dec. 22, 2019. [Online]. Available: https://www.r3.com/corda-platform/

[7] Stellar. *Stellar—An Open Network for Money*. Accessed: Dec. 22, 2019. [Online]. Available: https://www.stellar.org

[8] M. Westerlund and N. Kratzke, "Towards distributed clouds: A review about the evolution of centralized cloud computing, distributed ledger technologies, and a foresight on unifying opportunities and security implications," in *Proc. Int. Conf. High Perform. Comput. Simulation (HPCS)*, Orleans, France, Jul. 2018, pp. 655–663.

[9] D. Höfelmann and P. Sandner. *Entscheidungshilfe Für den Einsatz von Blockchain-Technologien in Unternehmen: Vier Frameworks im Vergleich*. Accessed: Apr. 10, 2019. [Online]. Available: https://medium.com/@philippsandner/entscheidungshilfe-für-den-einsatz-von-blockchain-technologien-in-unternehmen-vier-frameworks-im-fa7b5a9a0bc5

[10] M. Z. A. Bhuiyan, A. Zaman, T. Wang, G. Wang, H. Tao, and M. M. Hassan, "Blockchain and big data to transform the healthcare," in *Proc. Int. Conf. Data Process. Appl. (ICDPA)*, 2018, pp. 62–68.

[11] T. McGhin, K.-K.-R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, Jun. 2019.

[12] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Trans. Eng. Manag.*, early access, Aug. 8, 2019, doi: 10.1109/TEM.2019.2926471.

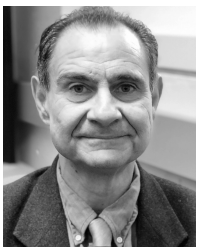
[13] X. Zhu and Y. Badr, "A survey on blockchain-based identity management systems for the Internet of Things," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1568–1573.
[14] D. V. Dimitrov, "Blockchain applications for healthcare data management," *Healthcare Informat. Res.*, vol. 25, no. 1, p. 51, 2019.
[15] Y. S. Hau, J. M. Lee, J. Park, and M. C. Chang, "Attitudes toward blockchain technology in managing medical information: Survey study," *J. Med. Internet Res.*, vol. 21, no. 12, 2019, Art. no. e15870.
[16] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in healthcare 4.0," *Comput. Commun.*, vol. 153, pp. 311–335, Mar. 2020.
[17] S. Popov. *The Tangle*. Accessed: Mar. 18, 2018. [Online]. Available: https://tinyurl.com/y55h5w2n
[18] L. Baird, M. Harmon, and P. Madsen. "Hedera: A public hashgraph network & governing council," Hedera Hashgraph, LLC, White Paper v.1.5, Feb. 2019, vol. 1. [Online]. Available: https://www.hedera.com/hh-whitepaper-v1.5-190219.pdf
[19] *Proof of Stake (POS)*. Accessed on Apr. 14, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Proof_of_stake
[20] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019.
[21] M. N. K. Boulos, J. T. Wilson, and K. A. Clauson, "Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare," *Int. J. Health Geographics*, vol. 17, p. 25, Jul. 2018. [Online]. Available: https://ij-healthgeographics.biomedcentral.com/articles/10.1186/s12942-018-0144-x
[22] *Hyper Ledger Fabric Archive*. Accessed: Dec. 15, 2019. [Online]. Available: https://github.com/hyperledger-archives/fabric/wiki/System-Chaincode-Specification
[23] *Ethereum*. Accessed: Dec. 22, 2019. [Online]. Available: https://www.ethereum.org
[24] *Solidity Security Considerations*. Accessed: Apr. 21, 2020. [Online]. Available: https://solidity.readthedocs.io/en/v0.6.0/security-considerations.html
[25] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (sok)," in *Proc. Int. Conf. Princ. Secur. Trust*. Uppsala, Sweden: Springer, 2017, pp. 164–186.
[26] L. Alt and C. Reitwießner, "Smt-based verification of solidity smart contracts," in *Proc. Int. Symp. Leveraging Appl. Formal Methods*. Limassol, Cyprus: Springer, 2018, pp. 376–388.
[27] *Example Gas Costs*. Accessed: Dec. 22, 2019. [Online]. Available: https://tinyurl.com/yyzvfuc6
[28] A. Meri, M. Hasan, M. Danaee, M. Jaber, M. Jarrar, N. Safei, M. Dauwed, S. K. Abd, and M. Al-bsheish, "Modelling the utilization of cloud health information systems in the Iraqi public healthcare sector," *Telematics Informat.*, vol. 36, pp. 132–146, Mar. 2019.
[29] H. T. Vo, A. Kundu, and M. Mohania, "Research directions in blockchain data management and analytics," in *Proc. 21st Int. Conf. Extending Database Technol.*, 2018, pp. 445–448.
[30] *Zeronet Decentralized Web Platform Using Bitcoin Cryptography and Bittorrent Network*. Accessed: Sep. 3, 2017. [Online]. Available: https://zeronet.io/files/ZeroNet_Presentation.pdf
[31] Tor. *Tor Project—Anonymity Online*. Accessed: Dec. 15, 2019. [Online]. Available: https://www.torproject.org
[32] Bittorreent. *BitTorrent—The World's Most Popular Torrent Client*. Accessed: Dec. 15, 2019. [Online]. Available: https://www.bittorrent.com
[33] *Zeronet Github*. Accessed: Dec. 15, 2019. [Online]. Available: https://github.com/HelloZeroNet/ZeroNet
[34] P. Snow, B. Deery, J. Lu, D. Johnston, and P. Kirby, "Factom," Factom, Austin, TX, USA, White Paper version 1.2, Apr. 2018. [Online]. Available: https://www.factom.com/assets/docs/Factom_Whitepaper_v1.2.pdf
[35] *Factom Project Github*. Accessed: Dec. 15, 2019. [Online]. Available: https://github.com/FactomProject/FactomDocs
[36] "Sovrin: A protocol and token for self-sovereign identity and decentralized trust, v1.0," Sovrin Found., Provo, UT, USA, Whitepaper version 1.0, Dec. 2018. [Online]. Available: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf
[37] *Hyperledger Indy*. Accessed: Dec. 15, 2019. [Online]. Available: https://wiki.hyperledger.org/display/indy/Hyperledger+Indy
[38] *Sovrin Operated by Stewards*. Accessed: Dec. 15, 2019. [Online]. Available: https://sovrin.org/stewards/
[39] *Remme*. Accessed: Nov. 19, 2018. [Online]. Available: https://remme.io/use-cases
[40] Nodalblock. *Nodalblock: Your Access to Blockchain*. Accessed: Nov. 19, 2018. [Online]. Available: http://rednodaldeabogados.com/en/
[41] *Nuggets White Paper v16*. Accessed: Oct. 15, 2017. [Online]. Available: https://nuggets.life/images/Nuggets-White-Paper.pdf
[42] Secure Key. *SecureKey: Building Trusted Identity Networks*. Accessed: Nov. 19, 2018. [Online]. Available: https://securekey.com
[43] *Namecoin*. Accessed: Nov. 19, 2018. [Online]. Available: https://namecoin.org
[44] *Procivis*. Accessed: Nov. 19, 2018. [Online]. Available: https://procivis.ch/about-us/
[45] *Identity Mind*. Accessed: Nov. 19, 2018. [Online]. Available: https://identitymindglobal.com
[46] *Bridge Protocol*. Accessed: Nov. 20, 2018. [Online]. Available: https://www.bridgeprotocol.io
[47] Civic. *Civic Wallet—Digital Wallet for Money and Cryptocurrency*. Accessed: Nov. 19, 2018. [Online]. Available: https://www.civic.com/developers/
[48] Evernym. *The Solution: Self-Sovereign Identity—Evernym*. Accessed: Nov. 19, 2018. [Online]. Available: https://www.evernym.com/solution/
[49] Uport. *uPort—Tools for Decentralized Identity and Trusted Data*. Accessed: Nov. 19, 2018. [Online]. Available: https://www.uport.me/#community
[50] *Biometrids: Decentralised and Anonymous id by Facial Recognition on the Blockchain*. Accessed: Dec. 15, 2017. [Online]. Available: https://tinyurl.com/tz36fzl
[51] M. Hajialikhani and M. Jahanara, "UniqueID: Decentralized proof-of-unique-human," 2018, *arXiv:1806.07583*. [Online]. Available: http://arxiv.org/abs/1806.07583
[52] *Completely Automated Public Turing Test To Tell Computers and Humans Apart (Captcha)*. Accessed: Jan. 25, 2020. [Online]. Available: https://en.wikipedia.org/wiki/CAPTCHA
[53] Wikipedia. *Social Engagement*. Accessed: Dec. 15, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Social_engagement
[54] S. T. Tempelhof, E. Teissonniere, J. F. Tempelhof, and D. Edwards, *Bitnation. Pangea Jurisdiction and Pangea Arbitration Token (PAT): The Internet of Sovereignty*. Planet Earth: Bitnation, 2017. [Online]. Available: https://github.com/Bit-Nation/Pangea-Docs/raw/master/BITNATION%20Pangea%20Whitepaper%202018.pdf
[55] *Aragon Blockchain*. Accessed: Dec. 15, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Holacracy
[56] Boardroom. *BoardRoom—Blockchain Governance Suite*. Accessed: Nov. 19, 2018. [Online]. Available: http://boardroom.to/#About
[57] A. Rea, A. Fischer, and J. du Rose. *Colony Technical Whitepaper*. Accessed: Nov. 19, 2018. [Online]. Available: https://colony.io/whitepaper.pdf
[58] *Coin Governance System*. Accessed: Nov. 19, 2018. [Online]. Available: https://cgs.vote
[59] *The Social Smart Contract—An Open Source Whitepaper v0.2*. Accessed: Dec. 15, 2018. [Online]. Available: https://tinyurl.com/spsbxxz
[60] Democracy.Earth. *Democracy Earth—Borderless Governance*. Accessed: Nov. 19, 2018. [Online]. Available: https://www.democracy.earth
[61] M. Ali, R. Shea, J. Nelson, and M. J. Freedman. *Blockstack Technical Whitepaper*. Accessed: Dec. 19, 2017. [Online]. Available: https://blockstack.org/whitepaper.pdf
[62] Dock.io Whitepaper. *Decentralized Professional Data Exhchange Powered by Ethereum*. Accessed: Dec. 15, 2018. [Online]. Available: https://crushcrypto.com/wp-content/uploads/2018/01/DOCK-Whitepaper.pdf
[63] *Ocean Protocol: A Decentralized Substrate for AI Data & Services-Technical Whitepaper*. Accessed: Dec. 3, 2018. [Online]. Available: https://oceanprotocol.com/tech-whitepaper.pdf
[64] C. Fei, J. Lohkamp, E. Rusu, K. Szawan, K. Wagner, and N. Wittenberg, "Jolocom: Self-sovereign and decentralised identity by design," Jolocom GmbH, Berlin, Germany, Tech. Rep., 2018. [Online]. Available: https://tinyurl.com/v2ly5zx
[65] *Pickiochain—A Secure Personal Data Chain*. Accessed: Dec. 29, 2018. [Online]. Available: http://www.hodlerxl.com/pikciochain/pikciochain-secure-personal-data-chain/

[66] *Yourblock—-Blockchain Based Comparison and Incentivized Personal Data Storage Platform*. Accessed: Dec. 29, 2018. [Online]. Available: https://tinyurl.com/stjqx35
[67] I. Frincu, D. Cearnau, and S. Neagu. *Persona Whitepaper*. Accessed: Dec. 29, 2017. [Online]. Available: https://icosbull.com/whitepapers/522/Persona_whitepaper.pdf
[68] *Whitepaper—AI Economies on the Blockchain*. Accessed: Dec. 29, 2017. [Online]. Available: https://consensus.ai/whitepaper.pdf
[69] *Essentia*. Accessed: Nov. 19, 2018. [Online]. Available: https://essentia.one
[70] Blockchain Helix. *Blockchain HELIX: Creating Trusted Digital Identity*. Accessed: Nov. 19, 2018. [Online]. Available: https://blockchain-helix.com/
[71] Vetri Team, "Value your data," VETRI, Procivis AG, Zürich, Switzerland, Tech. Rep., 2017. Accessed: May 12, 2020. [Online]. Available: https://vetri.global/static/WP-VETRI.pdf
[72] Secure Identity Ledger. Accessed: Nov. 19, 2018. [Online]. Available: https://secureidentityledger.com
[73] *Aragon Blockchain*. Accessed: Nov. 19, 2018. [Online]. Available: https://github.com/aragon/whitepaper
[74] *Medibloc Whitepaper*. Accessed: Nov. 19, 2018. [Online]. Available: https://tinyurl.com/yyanlmzz
[75] *Medibloc*. Accessed: Nov. 19, 2018. [Online]. Available: https://medibloc.org/en/
[76] *Ambrosus*. Accessed: Nov. 19, 2018. [Online]. Available: https://ambrosus.com/solutions/#medicine
[77] *Blockchain Healthcare Review: How Scriptdrop Is Using Blockchain Technology For RX Med Adherence*. Accessed: Oct. 25, 2017. [Online]. Available: https://blockchainhealthcarereview.com/how-scriptdrop-is-using-blockchain-technology-for-rx-med-adherence/
[78] *Ancapetre: Blockchains and Pharmacies: A New Way of Leveraging Medication Adherence*. Accessed: Oct. 25, 2017. [Online]. Available: http://www.ancapetre.com/blockchains-pharmacies-new-way-leveraging-medication-adherence
[79] Healthwizz. *Health Wizz—Mobile Application*. Accessed: Nov. 28, 2018. [Online]. Available: https://www.healthwizz.com
[80] Proof.Work. *Proof.Work—HealthCare Blockchain*. Accessed: Oct. 28, 2018. [Online]. Available: https://proof.work/ourvision/
[81] *Dentacoin: The Blockchain Solution for the Global Dental Industry (Whitepaper v. 2.2)*. Accessed: Oct. 28, 2018. [Online]. Available: https://dentacoin.com/assets/uploads/whitepaper.pdf
[82] *Medrec*. Accessed: Oct. 28, 2018. [Online]. Available: https://medrec.media.mit.edu
[83] Gem. *Health—Gem*. Accessed: Oct. 28, 2018. [Online]. Available: https://enterprise.gem.co/health/
[84] L. Hendren and K. Kuzmeskas. *Health Nexus—White Paper Version 1.0*. Accessed: Oct. 28, 2018. [Online]. Available: https://crushcrypto.com/wp-content/uploads/2018/03/HLTH-Whitepaper.pdf
[85] *Bandboo: Insurance Powered by Communities*. Accessed: Dec. 22, 2019. [Online]. Available: https://www.bandboo.co
[86] *Whitepaper—Etherisc Decentralized Insurance*. Accessed: Nov. 22, 2018. [Online]. Available: https://etherisc.com/files/what_is_etherisc_1.0_en.pdf
[87] A. Paperno, V. Kravchuk, and E. Porubaev. *Teambrella: A Peer-To-Peer Insurance System*. Accessed: Dec. 22, 2018. [Online]. Available: https://teambrella.com/WhitePaper.pdf
[88] E. Scheuer and P. Rieger. *Health Information Traceability Foundation*. Accessed: Mar. 22, 2020. [Online]. Available: https://tinyurl.com/qplzzek
[89] D. Baars, "Towards self-sovereign identity using blockchain technology," MSc Thesis, Fac. Elect. Eng., Math. Comput. Sci., Univ. Twente, Enschede, The Netherlands, 2016.
[90] X. Liang, S. Shetty, J. Zhao, D. Bowden, D. Li, and J. Liu, "Towards decentralized accountability and self-sovereignty in healthcare systems," in *Proc. Int. Conf. Inf. Commun. Secur.* Beijing, China: Springer, 2017, pp. 387–398.
[91] M. Chernyshev, S. Zeadally, and Z. Baig, "Healthcare data breaches: Implications for digital forensic readiness," *J. Med. Syst.*, vol. 43, no. 1, p. 7, Jan. 2019.
[92] Eu GDPR. Accessed: Oct. 19, 2019. [Online]. Available: https://eugdpr.org
[93] X. Zhu and Y. Badr, "Identity management systems for the Internet of Things: A survey towards blockchain solutions," *Sensors*, vol. 18, no. 12, p. 4215, 2018.
[94] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K.-R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan. 2018.
[95] M. Quinn, J. Forman, M. Harrod, S. Winter, K. E. Fowler, S. L. Krein, A. Gupta, S. Saint, H. Singh, and V. Chopra, "Electronic health records, communication, and data sharing: Challenges and opportunities for improving the diagnostic process," *Diagnosis*, vol. 6, no. 3, pp. 241–248, Aug. 2019.
[96] G. Jetley and H. Zhang, "Electronic health records in IS research: Quality issues, essential thresholds and remedial actions," *Decis. Support Syst.*, vol. 126, Nov. 2019, Art. no. 113137.
[97] C. Rathert, T. H. Porter, J. N. Mittler, and M. Fleig-Palmer, "Seven years after meaningful use: Physicians' and nurses' experiences with electronic health records," *Health Care Manage. Rev.*, vol. 44, no. 1, pp. 30–40, 2019.
[98] L. Otero Varela, N. Wiebe, D. J. Niven, P. E. Ronksley, N. Iragorri, H. L. Robertson, and H. Quan, "Evaluation of interventions to improve electronic health record documentation within the inpatient setting: A protocol for a systematic review," *Systematic Rev.*, vol. 8, no. 1, p. 54, Dec. 2019.
[99] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 224–230, Jan. 2018.
[100] A. Begoyan, "An overview of interoperability standards for electronic health records," *USA, Soc. Des. Process Sci.*, Jun. 2007. [Online]. Available: https://tinyurl.com/ve6rmy9
[101] S. V. B. Jardim, "The electronic health record and its contribution to healthcare information systems interoperability," *Procedia Technol.*, vol. 9, pp. 940–948, Jan. 2013.
[102] M. Reisman, "EHRs: The challenge of making electronic data usable and interoperable," *Pharmacy Therapeutics*, vol. 42, no. 9, p. 572, 2017.
[103] N. Gupta and B. Gupta, "Big data interoperability in e-Health systems," in *Proc. 9th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, Jan. 2019, pp. 217–222.
[104] I. Berges, J. Bermudez, and A. Illarramendi, "Toward semantic interoperability of electronic health records," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 3, pp. 424–431, May 2012.
[105] OpenEHR. *OpenEHR—Wikipedia*. Accessed: Jan. 25, 2020. [Online]. Available: https://en.wikipedia.org/wiki/OpenEHR
[106] *En13606*. Accessed: Jan. 25, 2020. [Online]. Available: http://www.en13606.org
[107] *Digital Imaging and Communications in Medicine (DICOM)*. Accessed: Jan. 25, 2020. [Online]. Available: https://www.dicomstandard.org
[108] *Direct Trust*. Accessed: Jan. 25, 2020. [Online]. Available: https://www.directtrust.org
[109] *Health Level Seven International*. Accessed: Jan. 25, 2020. [Online]. Available: https://www.hl7.org
[110] B. Abraham, "Comparative study of healthcare messaging standards for interoperability in ehealth systems," M.S. thesis, Dept. Comput., Data Math. Sci., Western Sydney Univ., Penrith, WA, Australia, 2017.
[111] *Hl7 FHIR Security*. Accessed: Jan. 25, 2020. [Online]. Available: https://www.hl7.org/fhir/security.html
[112] A. Mense and B. Blobel, "HL7 standards and components to support implementation of the European general data protection regulation (GDPR)," *Eur. J. Biomed. Inform. (EJBI)*, vol. 13, no. 1, pp. 27–33, 2017. [Online]. Available: https://tinyurl.com/szujw2d
[113] *Blockchain vs FHIR: A Showdown for Healthcare Integration?* Accessed: Jan. 25, 2020. [Online]. Available: https://www.ibm.com/blogs/insights-on-business/healthcare/blockchain-vs-fhir-showdown-healthcare-integration/
[114] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying blockchain to securely and scalably share clinical data," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278, 2018.
[115] *Health Wizz Whitepaper*. Accessed: Mar. 18, 2018. [Online]. Available: https://tinyurl.com/tsr67fu
[116] A. Deshpande, K. Stewart, L. Lepetit, and S. Gunashekar, "Distributed ledger technologies/blockchain: Challenges, opportunities and the prospects for standards," *Overview Rep. Brit. Standards Inst. (BSI)*, pp. 1–34, May 2017.
[117] D. Ivan, "Moving toward a blockchain-based method for the secure storage of patient records," in *Proc. ONC/NIST Use Blockchain Healthcare Res. Workshop*, Gaithersburg, MD, USA: ONC/NIST, 2016, pp. 1–11.
[118] C. Jaffe, C. Mata, and S. Kamvar, "Motivating urban cycling through a blockchain-based financial incentives system," in *Proc. ACM Int. Joint Conf. Pervas. Ubiquitous Comput. Proc. ACM Int. Symp. Wearable Comput.*, Sep. 2017, pp. 81–84.

[119] P. Maymounkov and D. Mazieres, "Kademlia: A peer-to-peer information system based on the XOR metric," in *Proc. Int. Workshop Peer-to-Peer Syst.* Cambridge, MA, USA: Springer, 2002, pp. 53–65.
[120] *Storj*. Accessed: Dec. 15, 2019. [Online]. Available: https://documentation.storj.io/
[121] J. Anderson, "Securing, standardizing, and simplifying electronic health record audit logs through permissioned blockchain technology (technical report)," Senior Honors Thesis, Dept. Comput. Sci., Dartmouth College, Hanover, NH, USA, 2018.
[122] P. Dai, N. Mahi, J. Earls, and A. Norta. (2007). *Smart-Contract Value-Transfer Protocols On A Distributed Mobile Application Platform*. [Online]. Available: https://qtum.org/uploads/files/cf6d69348ca50dd985b60425ccf282f3.pdf
[123] Leveldb. *GitHub—Google/LevelDB: LevelDB is a Fast Key-Value Storage Library Written at Google That Provides an Ordered Mapping From String Keys to String Values*. Accessed: Dec. 15, 2019. [Online]. Available: https://github.com/google/leveldb
[124] Rocksdb. *RocksDB—A Persistent Key-Value Store*. Accessed: Dec. 15, 2019. [Online]. Available: https://rocksdb.org/
[125] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in *Proc. AMIA Annu. Symp.* Bethesda, MD, USA: American Medical Informatics Association, 2017, p. 650.
[126] T. T. Thwin and S. Vasupongayya, "Blockchain based secret-data sharing model for personal health record system," in *Proc. 5th Int. Conf. Adv. Inform., Concept Theory Appl. (ICAICTA)*, Aug. 2018, pp. 196–201.
[127] *ONC Program*. Accessed: Dec. 15, 2019. [Online]. Available: https://www.healthit.gov/topic/certification-ehrs/about-onc-health-it-certification-program
[128] *Hl7 Standards*. Accessed: Dec. 15, 2019. [Online]. Available: https://www.hl7.org/implement/standards/
[129] OAuth 2.0. Accessed: Dec. 15, 2019. [Online]. Available: https://oauth.net/2/
[130] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, May 2015, pp. 180–184.
[131] A. Roehrs, "Omniphr: A blockchain based interoperable architecture for personal health records," Ph.D. dissertation, Dept. Appl. Comput., Universidade do Vale do Rio dos Sinos, São Leopoldo, Brazil, 2019.
[132] A. Roehrs, C. A. da Costa, R. da Rosa Righi, V. F. da Silva, J. R. Goldim, and D. C. Schmidt, "Analyzing the performance of a blockchain-based personal health record implementation," *J. Biomed. Informat.*, vol. 92, Apr. 2019, Art. no. 103140.
[133] T. Quaini, A. Roehrs, C. A. da Costa, and R. da Rosa Righi, "A model for blockchain-based distributed electronic health records," *IADIS Int. J. WWW/Internet*, vol. 16, no. 2, pp. 66–79, 2018.
[134] A. Roehrs, C. A. da Costa, R. da Rosa Righi, S. J. Rigo, and M. H. Wichman, "Toward a model for personal health record interoperability," *IEEE J. Biomed. Health Informat.*, vol. 23, no. 2, pp. 867–873, Mar. 2019.
[135] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, "OmniPHR: A distributed architecture model to integrate personal health records," *J. Biomed. Informat.*, vol. 71, pp. 70–81, Jul. 2017.
[136] A. Roehrs, C. A. da Costa, R. D. R. Righi, and K. S. F. de Oliveira, "Personal health records: A systematic literature review," *J. Med. Internet Res.*, vol. 19, no. 1, p. e13, 2017.
[137] Apache Kafka. *Apache Kafka—A Distributed Streaming Platform*. Accessed: Apr. 9, 2020. [Online]. Available: https://kafka.apache.org/
[138] *Apache Zookeeper*. Accessed: Apr. 9, 2020. [Online]. Available: https://zookeeper.apache.org/
[139] *Apache Storm*. Accessed: Apr. 9, 2020. [Online]. Available: http://storm.apache.org/
[140] Apache Spark. *Apache Spark—Unified Analytics Engine for Big Data*. Accessed: Apr. 9, 2020. [Online]. Available: https://spark.apache.org/
[141] *Openlink Virtuoso*. Accessed: Apr. 9, 2020. [Online]. Available: https://virtuoso.openlinksw.com/
[142] *The Oversim p2p Simulator*. Accessed: Apr. 9, 2020. [Online]. Available: http://www.oversim.org/
[143] *Omnet++ Discrete Event Simulator*. Accessed: Apr. 9, 2020. [Online]. Available: https://omnetpp.org/
[144] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.
[145] D. Bauer, D. M. Blough, and A. Mohan, "Redactable signatures on data with dependencies and their application to personal health records," in *Proc. 8th ACM Workshop Privacy Electron. Soc. (WPES)*, 2009, pp. 91–100.
[146] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.
[147] P. Zhang, D. C. Schmidt, J. White, and G. Lenz, "Blockchain technology use cases in healthcare," in *Advances in Computers*, vol. 111. Amsterdam, The Netherlands: Elsevier, 2018, pp. 1–41.
[148] A. Akande, "Disruptive power of blockchain on the insurance industry," MSc Thesis, Inst. Comput. Sci. Softw. Eng. Curriculum and Univ. Tartu, Tartu, Estonia, 2018.

BAHAR HOUTAN received the bachelor's degree in hardware engineering from Islamic Azad University (IAU), South Tehran Branch, Tehran, Iran, in 2014, and the M.Sc. degree in computer architecture from IAU, Science and Research, Tehran, in 2017. She is currently pursuing the Ph.D. degree in computer science with Mälardalen University, Västerås, Sweden. Her research interests include the IoT, blockchain technology, and networked real-time embedded systems.

ABDELHAKIM SENHAJI HAFID spent several years as the Senior Research Scientist with Bell Communications Research (Bellcore), NJ, USA, working in the context of major research projects on the management of next generation networks. He was also an Assistant Professor with Western University (WU), Canada, the Research Director of Advance Communication Engineering Center (venture established by WU, Bell Canada, and Bay Networks), Canada, a Researcher with CRIM, Canada, the Visiting Scientist with GMD-Fokus, Germany, and a Visiting Professor with the University of Evry, France. He is currently a Full Professor with the University of Montreal. He is also the Founding Director of the Network Research Laboratory and Montreal Blockchain Laboratory. He is a Research Fellow with CIRRELT, Montreal, Canada. He has extensive academic and industrial research experience in the area of the management and design of next generation networks. His current research interests include the IoT, fog/edge computing, blockchain, and intelligent transport systems.



DIMITRIOS MAKRAKIS is a member of the Montreal BlockChain Laboratory. Prior to joining the Academia, he worked as the Research Scientist with the Communication Research Centre (CRC) of the Canadian Government and at Telesat Canada. He started his academic career as a Faculty Member with the Department of Electrical Engineering of Lakehead University. He then joined the Department of Electrical and Computer Engineering, Western University. During his tenure at Western University, he founded and was the Executive Director of the Advanced Communications Engineering Center (ACEC); an advanced telecommunications research facility, established by the joint support of Western University, Bell Canada and Bay Networks (absorbed later by Nortel Networks). He is currently with the School of Electrical Engineering and Computer Science (EECS), University of Ottawa, and the Founding Director of the Broadband and Wireless Research Laboratory (BroadWIRLab) and the Bio-Communication and Nano-Networks Research Laboratory (Bio-CommNetLab). He has published many research articles in highly reputed journals and conferences, holds patents and has contributed to ITU's standardization initiatives. His current research evolves around the subjects of cyber-security and applications, nano-networks, bio-networks, the internet and nano-Internet of Things, wireless networks, application of artificial intelligence.