The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions

Bahar Farahani, Farshad Firouzi, Markus Luecking

PII: S1084-8045(20)30394-5

DOI: https://doi.org/10.1016/j.jnca.2020.102936

Reference: YJNCA 102936

To appear in: *Journal of Network and Computer Applications*

Received Date: 30 June 2020

Revised Date: 11 September 2020

Accepted Date: 17 November 2020

Credit Author Statement

Bahar Farahani: Supervision, Administration, Conceptualization, Methodology, and Writing.
Farshad Firouzi: Conceptualization, Methodology, and Writing.
Markus Luecking*:* Software and Writing.

Bahar Farahani
Farshad Firouzi
Markus Luecking

The authors appreciate the reviewer's insightful comments and would like to thank their constructive discussions, which helped us to improve the readability, as well as to enhance our novel contributions. The concerns are addressed in our revised article in the way described below.

Q1: In the introduction section, the first three paragraphs are very short and authors are suggested to merge the second paragraph within paragraphs one and two.

A1: Thanks for your constructive note. We have merged the second paragraph with the third one.

Q2: In general, it is not recommended to cite references for a technology, concept, or particular terms. For example, in the first paragraph, one point is referred with 5 cites and another with 7, whereas no references are made in the introduction.

A2: As recommended by the reviewer, we have revised the manuscript, particularly the introduction section.

Q3: In Section 3, the subsection should not start directly, rather a little introduction about the topic should be given as in Section 2.

A3: We appreciate your valuable comment. Section 3 has been revised accordingly and a new paragraph has been added to introduce the topics covered in Section 3.

Q4- In Figure 2, the Blockchain stack is illustrated, however, it is not properly explained. Authors are advised to elaborated all parts of the diagram.

A4: We greatly thank you for your insightful comments. A new subsection has been added to Section III to discuss the DLT/Blockchain stack. Please see Page

13 (Section D. DLT Stack for IoT) and Page 14 (Section E. Blockchain and IoT Integration Schemes).

Q5- In Section 4, the reference architecture is demonstrated and is shown in Fig. 3. To have a clear picture of the reference architecture, authors are suggested to add 1-2 more paragraphs to better elaborate on it. I am sure, it will be interesting to the general audience.

A5. Several sentences have been added to Section 4 to address the comment.

The Convergence of IoT and Distributed Ledger Technologies (DLT): Opportunities, Challenges, and Solutions

Bahar Farahani[*], Farshad Firouzi[†], and Markus Luecking[‡]
[*]Cyberspace Research Institute, Shahid Beheshti University
[†]Department of Electrical, and Computer Engineering, Duke University
[‡]FZI Research Center for Information Technology

Abstract

Digital revolution is characterized by the convergence of technologies — from cloud computing to edge/fog computing, Artificial Intelligence (AI), big data, Intelligent Internet of Things (IoT), and Distributed Ledger Technology (DLT) — that is blurring the lines between physical and digital worlds. In this context, the IoT tsunami, the ubiquitous adoption of intelligent connected devices, and the public embracement of DLT, of which blockchain is a popular example, are increasingly becoming an integral feature of many modern systems, particularly, IoT-based smart and connected healthcare. Although the IoT and DLT/blockchain are two very different technologies and distinct from each other, the fusion of blockchain and IoT technologies is an unprecedented paradigm shift that is expected to disrupt both current and future systems in various fields. Blockchain has exactly what is needed to fix the weaknesses and vulnerabilities of IoT. It solves the security fault line among intelligent IoT where most of the IoT devices are connected to each other through the public trustless environment. Moreover, its distributed peer-to-peer nature can address the shortcomings of client/server models in Cloud-IoT solutions. Although the convergence of IoT and blockchain (Blockchain-IoT) can potentially tackle major shortcomings of today's solutions, its adoption is still in infancy, suffering from various issues and thus there is a necessity to address significant challenges including scalability, consensus algorithms, data privacy, efficiency, availability, storage, interoperability, and standardization, among others. In addition, there is no consensus towards any reference model or best practices that specify how blockchain should be utilized in IoT. This paper aims to present a holistic reference architecture as well as fundamentals, recent advancements, promises, and challenges in order to foster the investigations on cutting-edge research and allowing one to contribute to advancing the convergence of blockchain and IoT.

I. Introduction

The healthcare and technology industries have been highly interlinked for a long time. However, the smart and connected health tsunami is taking increasingly a big leap in almost all healthcare processes [1], [3]. To date, innovative technologies like cloud computing and big data have been utilized by the Internet of Things (IoT) bringing greater availability, accessibility, personalization, precision, and lower-cost delivery of healthcare services, and Distributed Ledger Technology (DLT) appears to be the likely next step to be converged with IoT and other smart and connected health technologies [6]. Traditionally, cloud solutions are able to provide secure data storage and interoperability for IoT solutions, however Cloud IoT paradigm suffers from several shortcomings, such as security. DLT technology — including blockchain and Directed Acyclic Graph (DAG) — is transforming the way information is disseminated [4]. Its ability to build trust through distributed networks without requiring a third party is an advancement that may alter multiple industries, particularly IoT-based Smart and Connected Health, by potentially tackling major shortcomings and addressing weaknesses and vulnerabilities of today's client/server cloud IoT models. For instance, cloud servers can be disabled by software bugs, cyber attacks, or other mechanical issues. In contrast, IoT systems that utilize blockchain technology are not vulnerable to a single point of failure because identical data is maintained on multiple devices and computers [7].

The combination of innovative technologies such as cloud computing and the IoT has proven priceless, and blockchain is expected to further revolutionize the IoT by establishing a trustworthy information sharing service that ensures data is immutable and tractable [8], [9]. Blockchain can also improve IoT security by making data sources identifiable at any point, and thus potentially can solve the security fault line in cloud IoT systems. This is especially vital when IoT data must be securely distributed among many participants. For example, protecting food safety in healthcare domain requires the ability to monitor edible products. This can require the participation of distributors, manufacturers, farmers, etc. A data leak occurring at any point, could create the opportunity for fraud, lengthen the infection source search process, endanger consumer lives, and wreak havoc on organizational, industry, and national economic interests. These examples demonstrate the way blockchain can augment the IoT, providing answers to issues such as IoT data reliability, scalability, and privacy [10]. The massive growth of the IoT must be facilitated by standardized protocols and mechanisms designed to reduce the heterogeneity that usually leads to the creation of vertical silos and slows IoT adoption. Along with improving integration and reducing heterogeneity, improving IoT data integrity is also important. People are likely to trust information provided by governmental agencies or financial institutions, but it is vital that users be sure that information provided by external entities and IoT devices has not been tampered with. This need is a difficult one to address using centralized architecture because dishonorable institutions can change data to meet their own needs, making it less reliable. This points to the need to confirm that data has not been altered [11]. Recently, cloud computing technology has given the IoT the ability to analyze data and translate information into real-time action and up-to-the-minute knowledge. This unparalleled IoT expansion has generated new means of sharing and accessing information, including a foundational open data model. However, one of the main vulnerabilities of these new methods of information sharing is a lack of confidence. While centralized architectures have contributed substantially to IoT growth, when it comes to data transparency, they are opaque and leave participants questioning how their data will be used [9].

Currently, IoT security is aimed at securing communication, leaving security gaps around data lifecycle security (i.e., data sharing and access control). Cloud-based models manage IoT device connectivity, identification, and verification. While this paradigm has been the primary focus of IoT systems, it may not be the most effective solution because it ignores data location and requires the integration of a trusted third party. Reimagining the way IoT data is handled, would empower users to rely on a decentralized, independent, and robust data management system that guarantees data ownership. Such a system would include [12]: i) Access Control: Access is managed using DLT/blockchain-based decentralized, auditable mechanism that ensures data ownership and encrypted information sharing; ii) Secure Data Storage: Data is maintained in such a way that it is verifiable, immutable, and trusted; iii) IoT Compatibility: Allows data to be appended by one writer and viewed by multiple readers. From the viewpoint of many, blockchain could widely benefit IoT functionality and drive further technological innovation, particularly from a security point of view. Many research issues and challenges remain to be explored so that blockchain and IoT can be effectively utilized together. Such research is just beginning, but it is expected that improved integration would provide decentralization, improved interoperability, higher privacy/security, lower operating costs, better fault tolerance, greater resilience, accelerated transaction speed, fair monetization, secure data sharing, and novel IoT e-business models. The interdisciplinary landscape healthcare domain, demands a large number of significant technological advancements in blockchain, cloud computing, and IoT communities to come together and to synergize their efforts. This paper focuses on presenting a holistic reference blockchain-IoT architecture for healthcare, identifying new perspectives and highlighting impending research issues and challenges for the integration of blockchain and IoT.

The rest of this paper is organized as follows. Section II presents the fundamentals of DLTs and blockchain. In Section III, we discuss how IoT could benefit the blockchain and what challenges and barriers have to be tackled to grow further. This section also describes the main techniques and models for the integration of IoT and blockchain. Section IV presents the most common use cases of blockchain-IoT. Section V demonstrates the convergence of DLT/blockchain and IoT-based smart and connected health. Section VI presents a holistic reference architecture for blockchain-IoT in healthcare and with the help of a case study evaluates its performance. Finally, Section VII concludes the paper.

II. Distributed Ledger Technologies (DLTs)

Distributed ledgers are a form of technology used to distribute, exchange, or store data among users via public or private networks. Basically, it is a database that is stored and located across many nodes situated at different geographic locations. Each computer in the network is known as a node. Distributed ledgers can also be thought of as communal datasheets maintained on several distributed nodes. This technology is centered on distributed systems. Distributed ledgers are categorized into one of three groups, including blockchain, Directed Acyclic Graph (DAG), and hybrid DLT, depending on how the technology is implemented [4], [6].

A. Types of DLT

1) Blockchain: The concept of blockchain was coined in 2008 with the publication of a paper titled ”Bitcoin: A Peer to Peer Electronic Cash System” that was likely written pseudonymously by a group known as Satoshi Nakamoto. Fundamentally, blockchain is a continuously growing list of records (known as blocks) that are connected to each other using cryptography. In other words, a blockchain is a shared, decentralized, and immutable database ledger that stores time-stamped series of record of transaction data in a series of blocks connected by hash. Note that blockchain is based on a peer-to-peer (P2P) topology and managed by participants (identified by a private-public key pair) in the network. The new data records (blocks) are added to the blockchain through a process called mining. Each block in blockchain consists of three important elements: i) the cryptographic hash of the previous block, ii) timestamp, and iii) transaction data which is generally represented by a Merkle tree. Note that once the transaction data is recorded in any block, it cannot be altered without modification of all previous blocks (See Fig. 1) [4], [6].

Blockchain’s core unit of record is a transaction. When a new transaction is created, it is sent to the whole blockchain network. The transaction is received by nodes, known as block miners, that authenticate it by confirming the attached signature. The authenticated transaction is then mined into securely encrypted blocks. For a block miner to generate a block, a consensus problem must be solved via distribution. Any miner that solves the consensus problem sends the newly generated block to the whole network. When the new block is received, the miners that have not yet solved the problem add the block to their local chains because the transaction has been authenticated and the block can provide the consensus problem answer. Each new block includes a link to the prior block in the chain through cryptography. All block miners are able to synchronize chains regularly, and particular terms are established to make sure that the distributed network's ledger only maintains the longest chain in the event of a chain discrepancy [4], [6].

Merkle trees are also very fundamental components of blockchain technology. These structures enable secure and timely confirmation of the consistency and content of large amounts of data. Merkle trees condense block transactions by creating a digital fingerprint that identifies the whole group, allowing users to confirm if a transaction is part of a block. These trees are created from the bottom up using transaction IDs or repetitive hash pairs of nodes until only one hash remains (i.e., Merkle Root or Root Hash). Every leaf node is comprised of a hash of transaction data, and non-leaf nodes are hashes of prior hashes. Because Merkle trees are binary in nature, they must have an even number of nodes. If an odd number of transactions exist, the final hash is duplicated to establish an even number. Fig. 1 illustrates four block transactions (i.e., A, B, C, and D). Each transaction is hashed and the hash is stored on a leaf node, which creates Hash A, B, C, and D. Sequential leaf node pairs are condensed on a parent node by hashing together. Hash A and B, subsequently creating Hash AB. Similarly, Hash C and D are combined to create Hash CD. The resulting Hash AB and Hash CD are hashed, resulting in the Root Hash (Merkle Root).

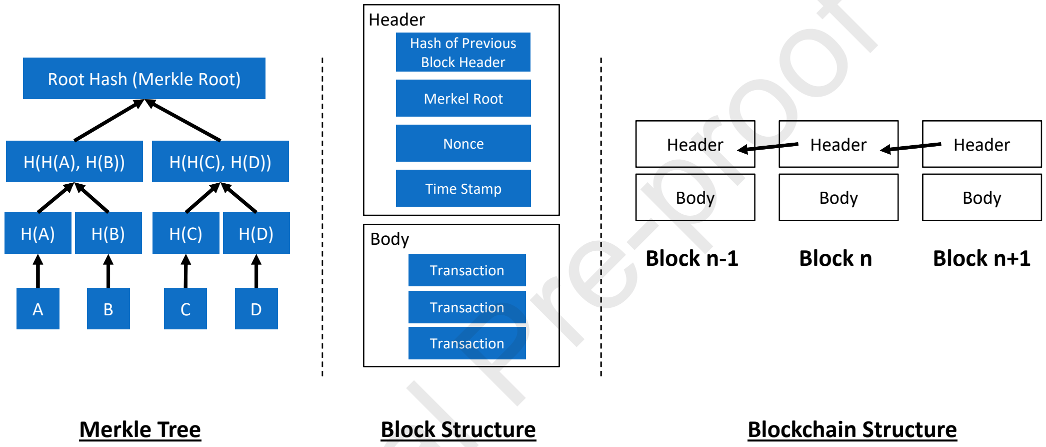


Fig. 1: Blockchain structure.

2) Directed Acyclic Graph (DAG): Like blockchain, DAG is able to store transactions. These data transactions are characterized by nodes linked to at least one, but possibly many other transactions. However, links are specifically directed – pointing from a prior transaction to a newer one in accordance with topological order. It should also be noted that DAGs do not permit loops because they are acyclic. From a Computer Science perspective, a DAG serves as a graph where transactions act as the nodes on the graph and the edges of the DAG have directions. In contract to blockchain, DAGs are not made up of blocks and no mining occurs. While transactions authenticate one another, a transaction is unable to validate itself. In addition, new transactions must authenticate at least one prior transaction when joining the DAG. Each new transaction must refer back to the parent transaction. The new transaction signs the parent transaction hashes and then incorporates those hashes in the new transaction [4], [6].

3) Hybrid DLTs: Hybrid DLTs combine DAGs and blockchain technologies, as evident e.g., in Bexam. Bexam is a hybrid DLT that utilizes pliable chains in conjunction with hierarchical nodes to provide the security benefits of blockchain and the speed capability of a DAG, generating approximately 40 million transactions each second. Bexam is easy to integrate into enterprise-level infrastructures and is highly scalable. In addition, the computing resource and power requirements are minimal. Bexam also utilizes token technology to create transactions [4], [6].

B. Permissioned vs. Permissionless

Blockchains can be permissionless or permissioned. Permissioned blockchains can be further classified to federated or private (See Table I) [4], [6].

- **Permissionless (Public)**: Also referred to as public blockchain, this type allows all transactions to be transparent to all nodes. Any node in the network is able to participate in blockchain consensus to authenticate a transaction. The node does not need permission and may not be known to the network. Within a permissionless network, such as Bitcoin, nodes support one another and work on a vast scale.
- **Permissioned**: These blockchain networks can be categorized as Federated or Private.

TABLE I: Public vs. Federated vs. Private Blockchain.

	Public	**Federated (Consortium)**	**Private**
Access	Anyone	Multiple selected organizaitons	Single organizaiton
Participants	Permissionless, anonymous	Permissioned, known identities	Permissioned, known identities
Decentralization	Decentralized	Partially decentralized	Centralized
Security & Consensus	Consensus mechanism, PoW or PoS	Pre-approved participants, voting/multi-party consensus, PBFT, PoET, PoA	Pre-approved participants, voting/multi-party consensus, Ripple
Immutability	Immutable	Partially immutable	Alterable
Transparency	Transparent	Partially transparent	Opaque
Transaction speed	Typically slow	Lighter and faster	Lighter and faster
Scalability and felixibility	Typically poor	Good	Supperior
Popular platforms	Bitcoin, Ethereum	Hyperledger	Multichain, GemOS

- **Federated (Consortium)**: These blockchains are run by a particular group of users and do not permit participants outside the group to verify transactions. The public may be allowed to read transactions but only members of a selected group can write transactions. Hyperledger Fabric is the most common and well established federated blockchain.
- **Private**: These blockchains are usually central to a single organization that holds the ability to authenticate transactions. The public or approved parties may be allowed to read transactions. An example of private blockchain includes Multichain.

C. Distributed Ledger Platforms

The most popular DLT/Blockchain platforms include:

- **Bitcoin**: The world's first and most valuable cryptocurrency; Bitcoin offers a secure, cost-effective, and efficient payment system. Bitcoin is primarily used for payment purposes. Although it is difficult to utilize Bitcoin with other IoT applications, the consensus algorithm and data structure provide reference points for many DLT-based IoT solution.
- **Ethereum**: Currently, Ethereum is the second-largest cryptocurrency platform. Ethereum provides a smart contract system based on Solidity programming language as well as a decentralized virtual machine, the Ethereum Virtual Machine (EVM), which is capable of executing scripts. With Ethereum, transaction fees are known as gas costs. Gas refers to the computing effort needed to complete an operation.
- **Hyperledger Fabric**: Hyperledger Fabric is the primary member of Hyperledger, an open-source blockchain model family hosted by the Linux Foundation. Hyperledger Fabric is a modular blockchain framework supporting smart contracts (knowns as chain code) that can be created in node.js or Go. This blockchain technology is specifically designed for use by commercial applications.
- **IOTA**: IoTA is a distributed ledger focused primarily on IoT and no-fee Machine to Machine (M2M) micropayments; In contrast to Ethereum and Bitcoin, IOTA's data structure is made up of a directed acyclic graph (i.e. tangle) rather than a blockchain. Instead of using miners to store transactions in blocks, each IOTA node acts as a miner and new transactions are required to approve two previous unverified transactions. This means network throughput scales in a linear fashion based on the number of transactions submitted. It is worth noting that IOTA includes no transaction fees or throughput limits, which is more attractive for IoT applications.
- **MultiChain**: MultiChain is a private blockchain that can be utilized either within or between organizations. MultiChain is an extended open source fork of Bitcoin offering a rich set of features including extensive configurability, rapid deployment, permissions management, native assets and data streams.
- **Hydrachain**: Its an extension of Ethereum platform to create private ledger.
- **IoT Chain**: A platform intended to supply a light system for meeting the scalability and security needs of IoT devices. IoT Chain integrates a directed acyclic graph with the PBFT consensus algorithm to provide lightning-fast speed.
- **HDAC**: A multichain platform that handles IoT contracts and M2M transactions. This platform's consensus algorithm is an energy-efficient version of PoW, known as ePoW.
- **Hedera Hashgraph**: A distributed ledger technology based on directed acyclic graphs for time-sequencing transactions with an asynchronous Byzantine Fault Tolerance consensus algorithm to secure the system against attacks.
- **Atonomi**: A platform designed to create secure, trustworthy IoT systems by supplying immutable, identity management services; Atonomi is constructed on the Ethereum structure.
- **OriginTrail**: A decentralized, blockchain-based platform based on Ethereum that is used to share supply chain data; This network is made up of three layers, including the data layer, network layer, and blockchain layer.
- **IoTeX**: A blockchain-in-blockchain platform designed for use with M2M transactions requiring privacy; The architecture is made up of a public rootchain and subchains. The rootchain manages subchains. Subchains are responsible for managing

groups of connected devices and are comprised of either private or public blockchain. Subchains communication among themselves by creating cross-blockchain transactions to the rootchain.

- **Streamr**: Streamr is an open source, off-chain network based on Ethereum; This platform is used to trade data in real-time. Streamr offers a global data marketplace where any user can buy or sell data.
- **Grid+**: An Ethereum-based platform designed for use with energy markets; Smart energy agents are used in real-time to pay electricity bills.

D. Validation Process

Blockchain verification, also known as mining, is generally completed using a consensus algorithm that institutes the rules that nodes must adhere to when authenticating blocks. Consensus requires that participating nodes receive a positive response from all other nodes by adhering to the prescribed transaction order. This allows the nodes to decide if the block will be added to the chain. While no centralized authority verifies chain transactions, all transactions are entirely secure and accurately verified due to consensus protocol, a key component of any blockchain. Consensus algorithms require all peers in the network to achieve mutual agreement regarding the distributed ledger's condition. This ensures blockchain reliability and builds trust among unknown participants in a distributed computing network. Basically, consensus algorithms make sure that each new block in the chain is the only authenticated version agreed upon by all nodes. Many consensus algorithms have been created for use in blockchain. Each one has unique strengths and weaknesses, making it suitable for specific uses [4], [6], [13], [14], [15], [8], [16], [17].

- **Proof-of-Work (PoW)**: PoW is the most widely known consensus algorithm. It is utilized to verify transactions and add newly authenticated blocks to the chain. Miners work to verify transactions, solve the problem, suggest candidate blocks, and collect rewards. The proof of work is based on a function (or a computational puzzle) which is hard to compute and solve, and costly and time-consuming to produce a piece of data, but easy to check and verify that the data is correct. The most common proof-of-work functions include Integer square root modulo a large prime, Weaken Fiat–Shamir signatures, Diffie–Hellman–based puzzle, Hash sequences, and Cuckoo Cycle. PoW is able to solve the Byzantine General problem and defend against Denial of Service (DoS) attacks because it takes massive computing power to mount a successful DoS attack. However, PoW blockchains are susceptible to what is known as a 51% attack. In such an instance, the attacker somehow has amassed 51% of the chain's mining power. In addition, PoW requires massive power use to support complex problem solving.
- **Proof-of-Stake (PoS)**: This algorithm was designed to combat PoW's weaknesses. In particular, recall that PoW requires a great deal of computing power to solve a computational puzzle. This protocol assumes that a node owning more of the blockchain will want the chain to succeed. So, if a node possesses 30% of the stakes in a blockchain, that node has a 30% chance of being selected as a miner and can theoretically mine only 30% of the blocks. In comparison to PoW, PoS does not require massive energy consumption or hugely powerful computing hardware. PoS blockchains are energy efficient and because they do not require mining, PoS chains can run much faster. While PoS design greatly reduces the chance of a 51% attack, it is not possible to achieve complete decentralization because a set number of nodes are tasked with creating new blocks.
- **Delegated Proof-of-Stake (DPoS)**: This well-known consensus algorithm was created by Daniel Larimer. There are three groups of entities in DPoS: delegates, stakeholders, and witnesses. Delegates and witnesses are chosen by the stakeholders. Delegates/witnesses are responsible for achieving consensus. Every stakeholder votes for one witness (by placing tokens on the name of candidates) with the witness receiving the greatest number of votes being elected. Stakeholders continue to vote raise the quantity of witnesses until at least 50% of the stakeholder group determines that the blockchain is appropriately decentralized.
- **Practical Byzantine Fault Tolerance (PBFT)**: This popular algorithm, designed to function with asynchronous systems, empowers blockchain to handle Byzantine faults. This algorithm requires low latency as well as low overhead time. All of a blockchain's nodes are organized by sequence with one node designated as leader. The other nodes are considered backup. When one node transmits a message, the remaining nodes exchange information to verify the message in the event that it is compromised while in transmission. Good nodes reach a majority agreement regarding the blockchain's status. PBFT's advantages include the ability to finalize blocks and transactions without confirmation. It also requires substantially less energy in comparison to PoW. On the other hand, PBFT works best for small blockchains because of the way it communicates among nodes and is vulnerable to Sybil attacks.
- **Proof-of-Burn (PoB)**: This algorithm does not require expensive hardware. Instead, coins are "burned" when validators irretrievably transmit them to an address. Validators obtain the ability to mine on the network by sending coins to the irretrievable address and then being randomly selected. While a short-term loss is sustained, burned coins provide validators with a long-term commitment.
- **Proof-of-Capacity (PoC)**: This consensus algorithm requires that validators use hard drive space rather than burning coins or buying expensive hardware. A validator with more hard drive space will have a greater chance of being chosen to mine

a subsequent block and earn a reward.

- **Proof-of-Elapsed Time (PoET)**: Known as one of the most equitable algorithms, PoET is commonly used in permissioned blockchain networks. Each validator has an equal opportunity to create a block. Every node waits for a random amount of time and then adds proof of waiting time to the block. Generated blocks are broadcasted across the network for review. The winning validator will have the lowest timer value in the proof part of the block. The winner's block is then added to the chain. Checks are built into the algorithm to make sure the same node does not win every election or create the lowest timer value.
- **Proof-of-Activity (PoA)**: This algorithm was suggested as a Bitcoin mining alternative. It was created to generate consensus by merging facets of PoW and PoS. The main focus is to reward active stakeholders. Similar to PoW, peers begin by mining and then utilize PoA to reach consensus. Computing requires finding PoW against the block header, absent block transactions. Next, random validators vote in order to verify the mined block header. Like PoS, a validator's chance of being chosen corresponds to network share. A block is verified if all validators agree. If validators are offline, the next block is chosen as well as another group of verifiers. Utilizing PoA requires high computing power and an uniformed implementation is at risk for "nothing at stake" attacks.
- **DAG-based Consensus**: Platforms, including IOTA, Byteball, Dagcoin, and Hashgraph, distribute ledgers as a DAG instead of chains. An IOTA tangle can illustrate how consensus is obtained using a DAG distributed ledger. In this platform, a node within the tangle is a transaction rather than a block. Issuing a transaction requires that a node arbitrarily approve two other un-verified transactions through light proof-of-work. A subset of transactions within the tangle is then confirmed either indirectly or directly through new transactions. As new transactions are added to the tangle, prior transactions are verified by several new transactions. The confidence level of a transaction is known as the fraction of the number of new transactions referencing a specific transaction in new transactions.

E. Benefits of DLTs and Blockchain

The manner in which blockchain is generated and maintained provides many benefits in comparison to traditional database options. Primary blockchain features including consensus and decentralization are inherent characteristics of blockchain that generate novel benefits [7], [8], [9], [10], [11].

- **Decentralization**: Unlike centralized network infrastructures, in blockchain-based infrastructures, two nodes can engage in transactions with each other without the need to place trust upon a central entity to maintain records or perform authorization. Within traditional systems, transactions are authenticated using a trusted agency such as a government or bank. Such centralization often results in greater costs, performance bottlenecks, and single-point failures by service providers. On the other hand, blockchain allows peers to authenticate transactions without intervention by a centralized agency which reduces service costs, alleviates performance bottleneck, and mitigates single-point failure risks [18].
- **No Third Party Required**: Because blockchain enables trustless participants to interact, no centralized agency is needed to verify transactions.
- **Reliable Data Storage**: Blockchain eliminates the need for third party interactions, lessening the risk of unsanctioned access or modification to stored data.
- **Pseudonymity**: While blockchain data is very transparent, privacy is protected because blockchain addresses are anonymous. However, blockchain only safeguards privacy to a specific level because addresses can be traced by inference, making it useful in detecting illegal transactions or fraud. This is why blockchain protects pseudonymity rather than complete privacy [9], [8], [19], [20].
- **Traceability**: All blockchain transactions are given a timestamp recorded when the transaction takes place. This makes it easy to confirm and trace the point of origin for historical data after reviewing the data with the appropriate timestamps.
- **Non-Repudiation**: A private key is used to attach a signature to each transaction, which can then be accessed and confirmed by others through the public key resulting in an encrypted transaction.
- **Immutability**: Because each new blockchain transaction must be approved by consensus, blockchain is highly resistant to censorship or tampering. In addition, any previous blockchain records are immutable; therefore, changing any prior record would require an attacker to take down the majority of a network's nodes.
- **Transparency**: For public blockchain systems such as Ethereum or Bitcoin, all users may interact and access the network equally. Each new transaction is authenticated and added to the blockchain, making it available to each and every user. This generates greater transparency and builds trust among users.
- **Permanence**: Blockchain transactions are permanently stored, making them available for audit or verification.
- **Availability**: Blockchain uses a large network of nodes that work peer-to-peer. Data is replicated and updated on each node. One inaccessible node does not cause a system malfunction; therefore, systems using blockchain are highly available.
- **Security**: Blockchain offers greater integrity and security than traditional databases because transactions are not recorded until all participants agree. Verified transactions are then encrypted and linked together in a chain. In combination with distributed copies, this makes it very difficult to hack blockchain.

- **Cost Savings**: Utilizing blockchain can reduce transaction cost because transactions can be completed directly peer-to-peer or business-to-business, eliminating the need for a bank or other third party. Costs around governance, overhead, auditing, etc. can be substantially lower.
- **Transaction Speed**: Blockchain saves time by removing lengthy authentication and clearance processes. All participating parties agree upon one version of data that is available in the blockchain ledger.
- **Smart Contracts**: Smart contracts implement agreements and handle digital asset transfers among participants under specific conditions in the blockchain. Smart contracts provide transparent execution, permanence, and decentralization while making sure program execution is secure.
- **Auditability**: Each participant has a copy of the blockchain and is able to access timestamped transactions, allowing for the verification of transactions that include specific addresses within the chain. These addresses do not correspond to real world identities and cannot be traced to the owner, but specific addresses can be audited and inferences generated about transactions undertaken by a specific blockchain address.

III. Blockchain IoT

In this section, the main challenges of IoT (e.g., security issues), the revolutionary advantages and challenges of combining IoT and DLT/Blockchain technologies, as well as the corresponding architectures and integration techniques will be discussed.

A. *Challenges of IoT*

The IoT is a natural outflow of humanity's endeavor to use computers to connect with others around the world. Next, as the digital world continues to expand, humans will work to connect the world's physical objects so that they may trade data and interact for the purpose of making life safer and more efficient. Currently, the IoT is made up of physical devices, gateways, fog/edge nodes, Cloud, and the Internet. The IoT allows physical devices or objects to transmit data via a gateway device so that fog nodes and Cloud servers can analyze and store data. It is also possible for these devices to accept commands to execute an action from one another via the Cloud. Commands may also come from a Cloud central manager. Standardized protocols and IoT stack work together to develop architecture layers that supply services for physical devices within the IoT system. Presently, the majority of IoT designs utilize centralized architecture, but this paradigm is plagued by many weaknesses, including [7], [8], [9], [10], [11]:

- **Heterogeneity**: IoT systems are characterized by heterogeneity when it comes to communication mechanisms, data types (i.e., unstructured, structured, semi-structured), and devices. This diversity also presents challenges for privacy, interoperability and security.
- **Inferior Scalability**: All data is transmitted from a device or object to the Cloud, where it is analyzed. Responses are then returned from the Cloud to the object, if appropriate. Scalability issues will only worsen as billions of future devices and objects join IoT systems.
- **Single Point of Failure**: Each physical object presents a point of vulnerability and may compromise security for the whole IoT network. If one object fails, it can bring down the network.
- **Maintenance Difficulty**: Updating IoT network software and the firmware of endpoint IoT devices is very difficult because updates have to be sent to a massive number of objects in a variety of physical locations.
- **Security**: This is known as the most challenging and important weakness to address. In general, today's IoT systems are vulnerable to attacks based on object identity, manipulation, services, or cryptanalysis. Outside of traditional web security, the IoT is vulnerable to additional factors that can increase threat potential. IoT objects are often isolated pieces of hardware that may be compromised in ways not foreseen by their creators. These devices are also often connected to one another, making it difficult to govern their interactions or guard against data manipulation attacks. In addition, these devices usually have a set amount of computing power that limits the implementation of complex security. When IoT objects are interconnected by the Internet, they create a complicated system that can be challenging to protect. Therefore, systems become increasingly vulnerable to web attacks such as traffic analysis, password attacks, eavesdropping, Sybil or DDS attacks, and message spoofing. Indeed, the alteration or spoofing of data can happen anywhere in the IoT network including within physical devices, through communication networks that transmit data, or during Cloud data processing or storage. The public has long been concerned about the security of data collected and stored in the Cloud. IoT devices (e.g., smart actuators) can be asked to execute a command from the Cloud or another IoT device. If a command is commandeered, the result could be devastating. An example of such a catastrophe would include opening a home's door to a thief. Inappropriate IoT device actions could also result in fires or the flooding of buildings. Unfortunately, a generalized security model is not easily administered. Appropriately addressing IoT security requires innovative security paradigms that anticipate the evolution of policies as well as the development of best practices that merge security-by-design with technology designed to work with a variety of stacks and processes that address IoT security holistically.
- **Privacy**: The massive amounts of data produced by devices can give extensive sensitive information e.g., about device owner habits or location. This information can be gathered without clear consent and revealed to outside parties by

IoT platforms, which strips users of personal data control. Moreover, data that is maintained on centralized cloud servers could be scrutinized to obtain personally identifiable information (e.g., health information) and unfortunately, system users typically have little say over who uses data and how. While policies exist to protect IoT data privacy, it is challenging to create solutions that safeguard privacy as part of the design.

- **Resource Constraints**: IoT systems, such as RFID tags, sensors, smart meters, and actuators, often rely on computing devices with limited resources, such as microcontrollers. These devices also do have limited storage capacity and computing power to handle complex algorithms that would help protect data making IoT devices susceptible to cyberattacks. .
- **Immutable Records**: Current IoT networks do not maintain permanent records of the interactions among physical devices, making it difficult to trace the root cause of an issue.
- **Single Data Copy**: Current architecture stores only one data copy within the Cloud. If that copy is manipulated, it is impossible to determine what was altered. It is also not possible to intercept and stop data tampering.
- **Server Failure**: If a centralized server fails, the whole infrastructure is at risk for failure. If a DoS attack is successful, it can turn a server into a single point of failure.
- **Inefficiency**: As the IoT grows, centralized servers will not be able to handle the communications needed for IoT automation, which can restrict system expansion.
- **Large-Scale Data Management**: IoT devices can produce massive amounts of data that can be challenging to manage when it comes to transmission, storage, and elaboration. Scalable models are needed to better manage high data volume.
- **Lack of Standardization & Interoperability**: Many open solutions, facilitated by international governing groups, alliances, or independent bodies (i.e., OMG, ITU-T, W3C, ETSI, IEEE, OneM2M, OASIS IEC, ETSI, etc.), are available. These governing groups cover a variety of IoT objects, systems, services, and architectures. Some of the standards adhere to neutral, cross-domain approaches, but other standards apply only to certain domains. The unregulated creation of standards and lack of universally accepted guidelines results in further separation and can further reduce IoT adoption as well as further integration across several domains.
- **Mobility vs. Stable Topology**: IoT application topology can change at various speeds. An example of an application with solid topology would include smart home technologies. Mobile topologies include vehicle networks (VANETs) used in transportation applications. Many smart home devices are situated within a stable network, while the rapid movement of vehicles requires time-variance topologies. The mobility of IoT devices can present difficulty around network connectivity and entity management.
- **Access Control Management (ACM)**: ACM are security protocols that control resource or service access within the system. Access control and identity go hand-in-hand. IoT identity systems are meant to facilitate communications and manage resource and device authorization. In short, identities outline access permissions between interacting parties and also control access within the system. When it comes to IoT technologies, many conventional access control mechanisms created to function with centralized architectures, including Role-based Access Control (RAC) and Access Control Lists (ACLs), are ineffectual because of the continuous expansion of policies and roles. In addition, an ever-growing number of factors and guidelines (i.e. location, time) must be considered in the development of access controls. Attribute-based Access Control (ABAC) models focus on this issue, but centralized identity providers within these models still have scalability problems. ABAC models still have issues that result from centralized identity providers or administrators. As a result, such control solutions are not a good fit for decentralized, scalable IoT systems. The Capability-based Access Control (CAC) paradigm can be attractive due to its adaptability, but CAC models still require service users to utilize third party authentication (i.e. certificate authorities, identity providers). This is incongruous with trustless IoT networks in which users can be provided without approval of third parties. CAC models are only suitable for trusting environments. Based on the access control information outlined above, the issues in creating IoT access control protocols include the following: i) Designing an access control protocol that effectively manages access to diverse IoT components (i.e., services, users, objects, etc.), even with fast growth in roles, policies, and users; ii) Building an access control mechanism for use in trustless environments.

The challenges mentioned above require that we reconsider IoT structure. At this time, blockchain appears to be one of the best technologies for facilitating a distributed system securely. However, in comparison to the IoT, blockchain's history is more recent and mysterious.

B. IoT Security Issues

The most common attacks on IoT networks include [11], [21], [22], [23], [24]:

- **End Device Attacks**: Adversaries can capture and control a physical node. Information such as certificates and keys maintained on the captured nodes is then visible to the attacker. The information obtained can be used to masquerade as a valid node and perpetuate further attacks such as a false data injection.
- **Communication Channel Attacks**: Attackers can eavesdrop and tamper with transmission channels. If radio signals are not encrypted, attackers can easily obtain information due to the broadcast nature of the signal. Encrypted signals can also

be analyzed to infer private information including information destinations or sources. It is also possible for adversaries to jam wireless channels with noise.

- **Network Protocol Attacks**: Attackers can utilize man-in-middle, wormhole, Sybil, and replay attacks against network protocol weak spots. During a Sybil attack, a device takes on multiple valid identities within an IoT system. These kinds of attacks affect the integrity and efficiency of routing protocols and voting methods.
- **Sensory Data Attacks**: Attackers communicate through ad hoc protocols where messages are sent to a destination hop-by-hop. During this process, adversaries manipulate existing data or include fake data. The messages are then forwarded to nodes in the chain. When fake data is accepted, an IoT application can send incorrect instructions or provide an erroneous service. This reduces the dependability of IoT networks. For example, traffic jams worsen if drivers receive incorrect driving assistant messages.
- **Denial of Service (DoS) Attacks**: These attacks deplete resources and clog IoT system services. Sleep deprivation attacks are a kind of DoS attack that compromises sleep routine programming to keep nodes or devices awake until the battery power is exhausted. Because IoT devices have a set limit to communication and network resources, a DoS attack can devastate network connectivity and network lifespan.
- **Software Attacks**: Adversaries use software backdoors using worms, viruses, or scripts to compromise software and take over operations. Protecting IoT data and devices (i.e. actuator commands, sensor data) is the foundation of safeguarding IoT networks. Effective Intrusion Detection Systems (IDS) must be implemented to guard the integrity, confidentiality, and verification of IoT communications and information. IoT devices must be correctly identified to ensure data is coming from the correct point of origin. Traditionally, this is confirmed by a trusted Identity Provider. Encryption and authentication algorithms safeguard data integrity. Once data is transmitted to the data storage location, the security of data is dependent on the storage service provider.

Securely deploying IoT requires that certain guidelines and mechanisms be considered:

- **Data Integrity, Confidentiality, and Privacy**: Appropriate encryption is needed as IoT data moves through network hops, ensuring confidentiality. Because many diverse devices, networks, and services are integrated together, the privacy of data maintained on devices can be vulnerable to IoT network nodes that have been compromised. Attackers can affect data integrity by causing vulnerable IoT devices to alter stored data for negative purposes.
- **Accounting, Authentication, and Authorization**: Authentication between communicating parties is required to protect IoT communications. IoT devices must also be authenticated in order to access privileged services. There is a wide array of IoT authentication protocols available because of the heterogeneous nature of IoT architectures and networks. These diverse environments can make it difficult standardize global IoT authentication mechanisms. In similar fashion, authorization protocols make sure that system or information access is granted only to authorized parties. Appropriately applied authentication and authorization protocols create a reliable environment that allows secure communication to take place. In addition, the accounting, auditing, and reporting of resource utilization generates a dependable means of protecting network management.
- **Service Availability**: IoT services can be impeded by Denial of Service (DoS) attacks. Malicious plans can include jamming, replay attacks, or sinkhole attacks, intent on manipulating IoT elements at differing layers to lower the Quality of Service (QoS) for users.
- **Resource Constraints and Energy Efficiency**: IoT devices possess limited resources and usually have minimal storage and power. IoT system attacks can elevate the energy used by inundating the network and depleting resources with repetitive or false service requests.
- **Single Points of Failure**: The constant expansion of IoT networks can reveal many single-points-of-failure that erode IoT services, necessitating the creation of impervious environment for many devices and generate different protocols for operation of a network that is more tolerant to faults.

C. Benefits of Merging IoT and Blockchain

IoT is an innovative technology with great potential, but current IoT systems utilize devices with limited resources that are vulnerable to cyberattacks. These networks are difficult to scale; maintenance is difficult; and they have not overcome single point of failure issues. In addition, IoT data is not permanent and data security and privacy remain key points of concern. Blockchain's decentralization, manner of creating and storing data, and consensus mechanism can address the weaknesses presented by centralized IoT (See Table II). A variety of use cases have demonstrated that blockchain is applicable to all parts of an IoT system. It can be utilized to authenticate and encrypt data in communication networks, manage and store device identifications, and securely hold Cloud data as well as information held by distributed objects or devices. Blockchain can also reduce potential risk by utilizing many nodes to exchange peer-to-peer data, making it nearly impossible to compromise data. The consensus required by blockchain technology also keeps a compromised node from joining an IoT network. Blockchain also refuses data from a compromised node, protecting data integrity. In summary, blockchain offers the following benefits to IoT [7], [8], [9], [10], [11]:

TABLE II: Comparison between IoT and Blockchain.

Characteristic	**IoT**	**Blockchain**
Structure	Centralized (Cloud IoT model)	Decentralized
Reliability	Single Point of Failure (e.g., DoS attack to cloud servers)	More reliable as it eliminates single points of failure
Resources	limited resources (IoT devices) with limited bandwidth and computational capabilities	Resource consuming and high bandwidth consumption
Scalability	Integrates billions of devices	Suffers from low throughput and low transaction speed
Automation	Typically needs human intervention	Autonomic interactions governed by smart contracts
Latency	Requires low latency	Mining is a time consuming task
Traceability	Low traceability	Tamper proof
Transparency	Low transparency	Trace any past transaction
Interoperability	Heterogeneous system with poor interoperability	Enhances interoperability because it can operate with diverse and fragmented networks with a universal internet access
Data Sharing	Data exchanging is a challenging task	Data sharing can achieved through a P2P blockchain layer with uniform access across different IoT systems.
Privacy	Suffers from privacy vulnerability as confidential IoT data are uploaded to the third-party cloud servers	Supports P2P data sharing among connected devices without requiring communication through a centralized network
Security	Prone to many security vulnerabilities and malicious attacks	More secure as all transactions are encrypted and digitally-signed by cryptographic keys. Blockchain can be used for automatically-updating IoT device firmwares
Integrity	Infrastructure (e.g., Cloud) provider can alter the IoT data	Guarantees data integrity

- **Decentralization**: Blockchain requires that a majority verify a transaction and approve it before it is added to the distributed ledger. No individual entity has the authority to verify a transaction or create rules for transaction acceptance. Trust is required in order for the majority of participants to achieve agreement and verify a transaction. Therefore, blockchain offers a secure platform for IoT objects or devices while removing centralized traffic and single point of failure vulnerabilities inherent to centralized architecture.
- **Scalability**: Moving from a centralized model to a distributed peer-to-peer architecture helps eliminate performance bottlenecks and single points of failure. It also works to keep a few large companies from monopolizing the storage or processing of data for large groups of people. Decentralized architectures also improve system and IoT scalability as well as fault tolerance while reducing IoT silos.
- **Improved Interoperability**: Blockchain can convert, process, and store a variety of IoT data in blocks. In addition, blockchain can operate with diverse, fragmented networks because blockchain is implemented over a peer-to-peer network that facilitates comprehensive access to data and permits data to be shared among various business entities (e.g., hospitals, patients, pharmacies, labs) in a secure and efficient way.
- **Adaptability**: The diversity of IoT devices and algorithms limits interoperability, but blockchain operates as a distributed database, free of semantics. Therefore, utilizing blockchain to manage IoT networks improves ecosystem adaptability. Blockchain has been proven to work across heterogeneous platforms and IoT infrastructures based on blockchain have the potential to adapt to diverse use cases and environments.
- **Coordination**: Blockchain provides quick transaction processing as well as coordination of billions of devices.
- **Transparency**: Blockchain allows authorized network users to trace any past transaction, providing a reliable means of pinpointing data leaks.
- **Traceability**: Tracing systems using blockchain have been developed to provide stakeholders and participants with tracing services so that data/product quality and origin can be verified. In addition, blockchain allows for the tracing of sensor data to ensure accountability. IoT blockchain data can be identified at any time, from any location, and all past transactions can be verified. The permanence of blockchain data also makes it almost impossible to manipulate stored transactions. Chain participants are able to authenticate data and confirm it has not been altered.
- **Autonomic Interactions**: Governed by smart contracts, blockchain allows IoT devices or subsystems to interact automatically without human intervention, in which there is no need for any traditional central role, such as governments.
- **Reduced Cost**: One of the most discussed benefits of blockchain for businesses is the potential for lowering operating costs. Blockchain enables peer-to-peer data transmission without the need for a central agency, which reduces expenses. Attempting to scale a reliable, centralized infrastructure would be very costly. Decentralization provides a less expensive means of scaling IoT while also addressing single point of failure concerns.
- **Streamlined Accounting**: Enterprise-level accounting departments would benefit from the transparency of blockchain by

being aware of who is sharing data or transmitting funds through a time-stamped chain. Even with the need to add a translation layer, an immutable data chain makes accounting and auditing simpler.

- **Accelerated Data Sharing**: Blockchain can enable direct information sharing between connected devices and partners in the IoT ecosystem instead of communication via a centralized network (e.g., cloud). However, blockchain currently limits the number of transactions completed per second. But, a permissioned blockchain can handle the massive amounts of data, large number of devices, and transaction speed required at the enterprise level. In addition, in blockchain we can reduce transaction verification time by using trusted nodes. This is vital for meeting the performance needs of IoT data exchange.
- **Contract Execution**: Smart contracts, a multiparty agreement stored using blockchain, enables stakeholders to execute contact arrangements when specific criteria are met. Smart contracts are able to automatically authorize payments when the contractual service requirements have been met.
- **Greater Reliability**: Blockchain improves IoT fault tolerance and eliminates single points of failure. It also removes the potential for bottlenecks created by reliance on centralized servers and prevents third parties from managing users' personal data. Indeed, every node in the chain includes a copy of the ledger that holds every network transaction, making blockchain resilient to attack. If a node is jeopardized, the chain continues to maintain all other nodes. Because each node contains the entire ledger, IoT data sharing is also improved.
- **Byzantine Fault Tolerance**: The IoT is made up of constantly available smart devices that gather data and utilize automated functions. Controlling IoT networks requires high availability, which is not always possible in architectures using centralized servers. Blockchain is immune to Byzantine Faults because of its ability to recognize failures using distributed consensus and recordkeeping mechanisms.
- **Trustless**: All participants and devices in an IoT network can build trust without depending on a centralized agency to store data or manage connectivity. This keeps potentially third parties from gathering private data and enables faster, automated payment for services.
- **Accelerated Transaction Speed**: Blockchain can expedite the development of IoT system services, reducing transaction time from days to nearly instantaneous.
- **Improved Security**: Blockchain can be useful for storing data (or hash of data) because transactions are encrypted and signed with digital cryptographic keys (i.e. elliptic curve digital signature algorithm). Blockchain supports peer-to-peer information sharing among connected devices rather than requiring communication through a centralized network, which reduces cyberattack vulnerability. It also utilizes pseudonymity for addresses and distributed consensus for record permanence. It is impossible to change data in a public blockchain because the chain is not located in a single place. In addition, the cost of new computational or monetary transactions prevents DDoS and flooding attacks. Blockchain and smart contracts can also increase system security by updating device firmware automatically in order to address vulnerabilities. In summary, blockchain improves data security and IoT stack security protocols as outlined below [8], [25], [26], [27], [28], [29], [30]:
  - **Highly Encrypted Transactions**: These transactions are the most secure due to the encryption power of hashing tags that are very difficult to hack.
  - **No Single Point of Failure**: Decentralization guards against cyberattacks that focus on a single point of entry to take a network down through DDoS or spoofing attacks.
  - **Cryptographic Signatures**: These signatures are not available in a single location so, man-in-the-middle attacks are unable to intercept a lone communication thread.
  - **Node Status Tracking**: The ability to track a node is helpful in anticipating and defending against attempts to hack IoT security.
  - **Data Integrity** When it comes to network and data security, this is the guarantee that data may only be altered by, or accessible to, authorized parties. Attacking a blockchain in order to modify data would require an attacker to alter blockchain transactions or create fake blocks that hold erroneous transactions. This is almost impossible in a public blockchain where immutable records are verified and stored through consensus mechanisms. These blockchain properties support decentralizing the IoT via blockchain in order to protect data integrity.
  - **Confidentiality**: Protecting sensitive information from access by unauthorized participants; Blockchain addresses confidentiality issues by using public/private key pairs. Blockchain applications include confidentiality and authorization components because every transaction is inscribed with the sender's private key.
  - **Availability**: Incorporating blockchain with IoT systems improves network availability through the decentralization characteristics of blockchain. Blockchain-based data storage solutions include availability features because it includes no central points of failure.
- **Improved Privacy**: Creating privacy-aware IoT solutions requires ensuring IoT data ownership so that users can control data access. Data privacy can be achieved typically using one of the following options [8], [31], [32], [28], [33], [34],

[35], [36], [37], [38]:

  - Token-based Access Model: Requests for encrypted data access can be sent as transactions to the owner of data. Note that the owner can store the data off-chain in distributed file systems (e.g., IPFS), distributed databases (e.g., BigchainDB) or cloud. This allows data owners to control every aspect of data sharing.
  - Associate Role-Based Model: IoT participants use smart contracts to grant role-based data access privileges to users in exchange for monetary compensation or services.
  - Attribute-based Encryption (ABE): ABE is a newer model that encrypts data according to an access policy containing specific characteristics. Data owners, users, and consumers can include a variety of attributes in decryption keys and access policies to encrypt ciphertexts.
  - Tiered Architecture: As a highly promising data sharing solution, this option utilizes tiered blockchain architecture. Several private blockchains are connected to a public blockchain or federated blockchain to create a network. Users of different blockchains can choose to send data to other blockchains based on access control policies enforced via smart contracts.

- **Improved Autonomy**: Decentralized peer-to-peer networks provide greater IoT device independence. In addition, communications aren't passed through a centralized server in order to perform automatic services. Participants can authenticate data received as well as the identification of the sender. The security of blockchain storage also allows for the deployment of software updates to IoT devices.
- **Improved Functionality**: Blockchain provides greater functionality through the programmable logic of smart contracts and the ability to handle interactions as transactions. Smart contracts also provide security functions around confidentiality, authentication, and access control to improve IoT security.
- **Peer-to-Peer Data Sharing**: Cloud technology is vital to processing, transmitting, and storing data. While it contributes to the evolution of IoT applications, today's cloud-based architecture has resulted in a multitude of separate data silos that hamper comprehensive IoT data analytics. In contrast, blockchain-based architecture facilitates peer-to-peer secure data sharing.
- **IoT e-Business Models**: Currently, IoT service providers require users to transmit data to a centralized server; however, data exchanged using public blockchain can enable users to participate in data marketplaces in order to monetize IoT data. Blockchain provides incentives for users to provide resources for others.
- **Monetization**: IoT ecosystems are made up of three-tiered architectures involve i) endpoint IoT devices responsible for creating data, ii) connecting IoT devices to gateways that transfer data to the highest architecture layer, and iii) cloud platforms that analyze and process data to generate valuable information. Monetizing IoT data is important within the IoT ecosystem when it comes to data sharing and ownership. IoT device data is generally context-rich and highly valuable. Traditional monetization requires users to give up data to third parties (e.g., cloud providers who collect and ingest data), but data shared with context information can expose sensitive personal data, especially in the case of smart health applications devices. In these scenarios, blockchain provides a means of monetization while removing dependence on third party service providers, like cloud platforms. Data brokers and data markets can utilize blockchain to allow peer-to-peer data sharing because it provides secure access control on top of a secure storage layer. This enables the blockchain to allow or disallow data access in exchange for cryptocurrency. Service providers, data customers, and data owners can interact directly through blockchain without requiring a central third party. The level of data shared is controlled by the data owner through smart contracts. These contracts clearly outline the nature of shareable data as well as the timeframe for sharing. The distributed ledger allows data owners to trace data movement through blockchain participants. In addition, cryptocurrencies also allows data monetization on the blockchain [8].
- **Managing IoT Quality of Service (QoS)**: Because of the rapid growth of the IoT, ensuring QoS can be difficult at the edge of networks or on the Cloud. Traditionally, QoS measurement mechanisms depend on a centralized party that utilizes specific agents to gather data and evaluate service performance. However, these traditional mechanisms are unable to handle the diverse, distributed nature of IoT services. To manage QoS in IoT, we should be able to gather, access, and update accurate quality data frequently. Blockchain's participant approach guarantees the trustworthiness of data needed to measure the quality of IoT services [39].
- **Identity Management**: Systems using blockchain-based access and identity management can be used to improve IoT security. These systems have been utilized to safely maintain information regarding digital rights, identity, credentials, and the origin of goods. If information is entered currently, blockchain's immutability is attainable. However, a primary challenge for some applications is the difficulty ensuring that individuals, physical assets, resources utilized, and other relevant information is stored securely. This can be achieved fairly simply for many IoT devices. For example, private blockchain may be utilized to maintain cryptographic hashes of specific firmware for devices. These systems generate immutable records of device status and configuration. Such records can be used to confirm that a specific device is authentic and that neither settings nor software have been modified. Only after authentication a device is permitted to

connect with other participating services or devices.

- **Access Management**: As the IoT evolves and becomes established as part of tomorrow's Internet, it faces the challenge of managing billions of devices all around the globe. The access management technology currently available for IoT utilizes centralized client/server paradigms with technical limitations when it comes to global management. These models were originally created to address conventional human-machine based Internet situations in which devices are part of a trusted domain. However, IoT scenarios are often more changeable because they are often mobile and are managed by different communities across their lifespan. IoT devices may be managed by multiple managers simultaneously. In addition, many IoT devices and managers have limited computing power, battery life, and resources to operate correctly within current access management systems, highlighting the need for innovative approaches. Some researchers are currently attempting to utilize blockchain to create access control systems for the IoT [40], [41], [28], [42], [43]. These scientists use blockchain transactions to approve or disallow IoT access requests by defining access with smart contracts, making use of blockchain's immutability and enabling transparent auditing of access control. However, blockchain is not the solution to every problem. Storage on blockchain platforms is minimal and expensive, making it unlikely that all IoT device access control policies are added to the blockchain. While private blockchain access control protocols could potentially address the need for storage, isolated blockchain could impede wider adoption due to interoperability concerns. For instance, the authors of [44], [41] proposed FOCUS architecture that makes use of three-dimensional social networks, including the relationships among things, relationships among owners, and the relationships between things and owners to create user-centered access control protocols that globally manage all access control policies. Without blockchain, privacy preserving is incomplete due to dependence on centralized identity providers where identity protection is still a problem. Both those providing services and those that access them must allow full trust to centralized identity providers. Therefore, centralized identity providers can view interactions between service providers and service customers, which weakens the privacy of identity information. On the other hand, blockchain's identity management is handing identity control back to users. Identity solution designs are affected by paradigm changes that allow users to determine who can access personal information. While users could have total control of personal information via blockchain identity management, public blockchain still has the potential to reveal some identity data. This means it is important to include privacy preserving tools (i.e., zero knowledge proofs, multi-party computation) to support the selective sharing of sensitive IoT data and refine identity privacy [40], [41], [28], [42], [43].
- **Data Management**: Current research challenges exist around storing and managing smart object data. Managing IoT data includes aggregating online data, event log provision, storage, and auditing for offline data analysis and processing of queries. IoT data management systems must be capable of abstracting complicated semantics for top-level IoT applications because unprocessed data is diverse and contains weak semantics. Additionally, some IoT application domains are time-sensitive, so promptly processing IoT data is vital when considering the restricted capability of IoT devices. Conventional centralized models are unable to simultaneously ensure trust and data integrity when managing heterogeneous data. Scalability and latency are still data storage issues in blockchain technology. However, using blockchain for IoT data management can ensure global data integrity and remove dependence on semantics for recording the creation of IoT data [8].

D. DLT Stack for IoT

Fig. 2 shows the different layers of the DLT/blockchain stack for IoT applications. In particular, the DLT stack consists of the following layers [45], [9]:

- **Device Layer**: This layer represents smart devices, sensors, actuators, controllers, and edge/fog node, which are connected by a diverse of wireless/wired communication protocols to form the Internet of Things.
- **Data Layer**: This layer gathers IoT data in the forms of transactions from the lower layer and wraps up encrypted data using digital signatures, asymmetric cryptographic algorithms, and hashes.
- **Network Layer**: This layer serves as a P2P network that overlays the communication layer. DLTs utilize a P2P architecture due to the core need for decentralization. Decentralization is only accomplished through a network architecture that enables peers to share resources without third-party intervention. While all P2P participants are able to serve equally as a requestor or service provider, they can be categorized according to support functions like database, routing, miner, and wallet.
- **Consensus Layer**: This layer handles distributed consensus required to confirm the trustworthiness of a block and ensures all peers have an accurate ledger copy. However, note that agents and nodes might end up having different views of system's status (i.e., forks) mainly due to network faults, communication latency, or malicious nodes. Therefore, one of the challenges of a consensus algorithm is to avoid such forks.
- **Contract Layer**: This layer is responsible for digital currency and creation and handling of smart contracts.
- **Application Layer**: This layer provides users with services for a variety of industrial areas such as supply chains, manufacturing, utilities, logistics, and healthcare.

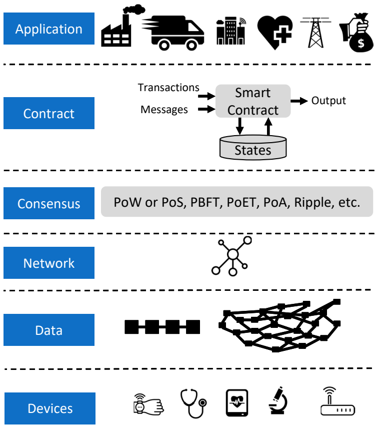


Fig. 2: DLT Stack.

E. Blockchain and IoT Integration Schemes

Blockchain and IoT can be integrated with each other in the following main ways (See Fig. 3) [7], [8], [46], [47]:

- **Tight Integration**: This integration scheme requires that all communications among participants take place through blockchain. In other words, all the IoT devices are considered as blockchain peers. In this approach, all IoT interactions are recorded in the blockchain to ensure accountability. This scheme allows tracing of all communication between a specific IoT service and device.
- **Loose Integration**: recording every IoT interaction increases blockchain storage and bandwidth needs which might be infeasible for some use cases. To address this issue, in this scheme, resource-rich IoT devices (e.g., gateways or fog nodes that also register IoT devices) can perform consensus and other power-hungry tasks, whereas resource constrained devices are not needed to hold a copy of the blockchain or process blockchain records. IoT devices can communicate with one another off the chain or interact with the blockchain via the gateways. This introduces discovery and routing protocol needs, but guarantees low latency among devices and provides a choice for recording blockchain interactions. In other words, not all transferred data must be kept on the blockchain. The blockchain acts as a control mechanism in which smart contracts serve as programmable logic when data is transferred using peer-to-peer technology. Users can choose either to utilize blockchain for interactions or they can rely on conventional cloud IoT protocols for interaction among IoT devices. This approach utilizes and combined the best of two worlds i.e., decentralized recordkeeping via blockchain as well as real-time IoT communication. This scheme is best applied to situations with high throughput, frequent interaction, reliable IoT data, and low latency. However, this scheme must optimize the separation between real-time interactions and those occurring through blockchain. In addition, the level of decentralization obtained through this approach is not as impenetrable as when devices send transactions directly to a blockchain.

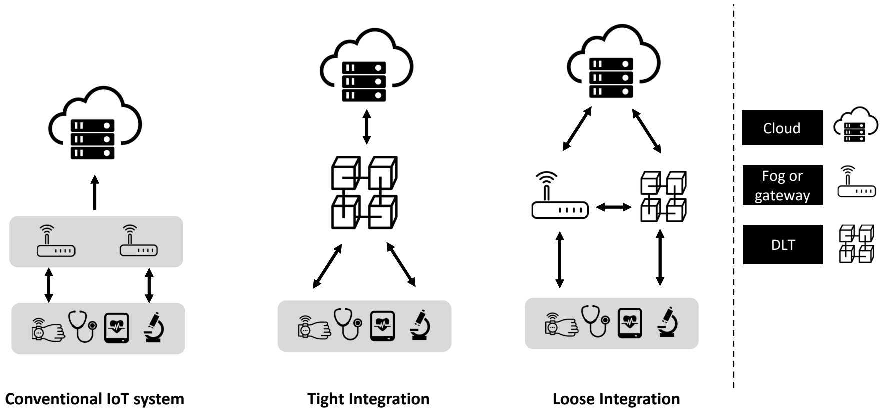


Fig. 3: Blockchain and IoT integration schemes.

Note that On-chain or Off-chain transactions can exist on blockchain IoT. On-chain transactions are accessible via the distributed ledger and viewable by every blockchain node. The validity of these transactions is confirmed when the chain mirrors the transactions on the public distributed ledger. An on-chain transaction must be authenticated by a set number of blockchain participants, which can take time due to the various steps before it is considered successful. In addition, the expense of a transaction can be unappealing to network participants. In contrast, off-chain transactions exchange data outside the blockchain. The benefits of off-chain transactions include: i) Lower-Cost: Transactions are generally free because they are not authenticated by participants; ii) More Efficient: Because no validation is needed, transactions are recorded instantaneously; and iii) Greater Privacy: Transactions cannot be viewed by public blockchain participants.

Understanding the advantages and disadvantages of using blockchain for data storage requires that we consider what kind of information is stored. Because blockchain is a distributed ledger, all nodes can view the ledger containing all confirmed transactions in a block. Transactions hold information concerning who sent information to another participant and under what parameters. Because all transactions are validated on each machine in the network, smaller or less efficient network devices must confirm and store block transactions as quickly as larger, faster participants, which elevates memory costs exponentially. Another issue is that only a specified amount of data fits in a block, thereby restricting the amount of data in a single transaction. Transactions containing a large amount of data slow network speed because subsequent transactions cannot occur within the block. Additionally, larger blockchains lead to centralization becuase smaller machines are able to handle only a set quantity of storage; therefore, a regular user may rethink using blockchain if it jams up the hard drive.

Lowering costs and reducing the clutter of blockchain can be accomplished by employing the off-chain technique of storing hashes of data rather than the raw data in blockchain. Blockchain serves to build trust among participants and provide transaction proof. Data is not needed to accomplish that purpose. However, certifying data security and privacy for some use cases requires that data be encrypted prior to hashing. Off-chain cases that need data for distribution may utilize the solutions indicated below:

- Distributed File systems: Allow file access in peer-to-peer networks; Currently Stori and IPFS are the two main solutions in this market.
- Distributed Databases: Because most use cases need to store data via databases, this solution must provide high throughput, low latency, high capacity, and robust query support. Many of these needs are not met by blockchain, but a distributed database like IPDB or BigchainDB can create a network managed by an alliance of nodes that verifies and stores requests in a database. BigchainDB can be utilized with a decentralized database and IPDB is creating a public database available to all.

F. Blockchain and IoT Adoption Considerations

As previously explored, security architecture is one of the primary issues for current IoT systems. Blockchain improves security through decentralization and consensus-based decision making. However, it is important to consider the challenges posed by creating an architecture that incorporates a distributed ledger [48], [7], [8], [9], [10], [11]:

- **Scalability**: IoT systems must include some means for handling large amounts of data gathered by networked sensors as well as latencies or reduced transaction processing speed. Outlining a clear data model in advance can prevent future problems and save time when moving the solution to production.
- **Network Privacy & Transaction Confidentiality**: It is difficult to share an IoT network's private transaction history in a shared ledger on a public blockchain because transaction pattern analysis can be used to infer the identity of users or devices protected by public keys. Entities need to fully comprehend privacy needs to determine if a private or hybrid blockchain best fits their requirements.
- **Privacy**: Complete privacy is not possible with blockchain due to data immutability. Any data change has to be confirmed by the majority of nodes in the network; therefore, blockchain thoroughly protects transactions but does not permit the removal of sensitive data.
- **Sensors**: IoT sensor reliability can be weakened by interfering with the measurement of criteria required for transaction execution. It is important to safeguard IoT device integrity by ensuring they cannot be compromised by third parties. This creates a protected environment for gathering data and completing transactions.
- **Processing Power**: Most IoT devices lack the processing power to handle the computations required to participate directly with blockchain.
- **Storage**: While blockchain does not need a centralized server for storage, the ledger must be stored on each node. The ledger will grow in size over time and based on the number of nodes added to the network.
- **Naming and Discovery**: Because blockchain was not originally designed for the IoT, nodes were not designed to locate one another. For example, the Bitcoin application embeds some sender IP addresses in the Bitcoin client. Nodes use these addresses to create the network topology. However, this model is not applicable to IoT because many devices move continuously, which alters topology.
- **Legal and Compliance Concerns**: IoT is an emerging arena without regulated compliance or legal precedent, which creates issues for IoT service providers or device manufacturers. It makes many businesses unsure of utilizing blockchain.

- **Skill Deficit**: Very few individuals truly understand how blockchain functions, especially in conjunction with IoT. This presents hiring challenges for blockchain projects.
- **Blockchain Security Vulnerabilities**: Blockchain is known for its tamper-resistant, decentralized networks. However, blockchain does have security vulnerabilities including [11]:
    - **Double Spending**: Malicious actors purposefully mislead participants by producing conflicting transactions, such as spending the same Bitcoin more than once. Adversaries can also pre-mine blocks to try to get conflicting transactions accepted by the chain.
    - **Consensus Protocol Attacks**: Adversaries can breach consensus protocols by owning a large portion of the network's computing power in order to control or reconstruct the blockchain (i.e. 51% attack). An attacker that possesses more than 50% of the hash power can force a blockchain to accept invalid blocks by solving the consensus problem more quickly than the remaining peers. In addition, 33% hash power has been shown to overpower PoW blockchains.
    - **Eclipse Attacks**: These attacks on peer-to-peer networks occur when adversaries control all valid node connections and keep nodes from connecting with legitimate peers. This form of attack was first attempted on Bitcoin, using a randomized protocol to force a Bitcoin node to connect with certain chosen peers in order to maintain peer-to-peer communication and blockchain functions. Ethereum was also reportedly exposed to eclipse attacks by the Kademlia peer-to-peer protocol.
    - **Smart Contract Vulnerability**: Smart contracts are vulnerable because of the immutability and openness of blockchain. Both adversaries and the public can identify possible fraud or bugs. It can be difficult to address bugs in an implemented smart contract because of blockchain immutability. An example of this includes the 2016 Decentralized Autonomous Organization (DAO) attack that culminated in a divided Ethereum blockchain.
    - **Programming Fraud**: Adversaries can use programming code fraud to pull out blockchain properties as evidenced by the 2018 piracy attack.
    - **Distributed Denial of Service (DDoS) Attacks**: Adversaries work to deplete blockchain resources by using the entire network's processing capability. This is done by initiating a coordinated attack. A 2016 attack occurred when attackers used underprice EVM instructions to slow block processing speed. The resulting large number of low balance accounts opened the door for a DDoS attack.
    - **Private Key Leaks**: Adversaries take over an account by stealing the account's private key through a physical node take over or through a traditional network attack.
- **Storage Capacity & Scalability**: Blockchain's storage capability and scalability are debatable, but when it comes to IoT applications, their innate scalability and capacity limits make the obstacles even larger. It may seem that blockchain is not suited to IoT applications but there are methods for diminishing or eliminating such limitations completely. IoT devices create gigabytes (GBs) of real-time data, which is a substantial obstacle to integrating blockchain. Some current blockchain platforms can handle only a few transactions each second, which would result in IoT device bottlenecks. In addition, blockchain was not designed to handle the massive amount of data produced. However, combining these technologies could resolve such issues. While a vast amount of IoT data is stored, only limited portions are utilized to obtain knowledge or drive actions. A variety of methods have been suggested in order to filter, compress, or normalize IoT data. Because the IoT includes target services (i.e. cloud, blockchain), communication, and embedded devices, saving data provided by the IoT is beneficial to many layers. Compressing data makes data processing, transmission, and storage of generated data lighter. Finally, blockchain's consensus protocol which creates bottlenecks could be transformed to widen bandwidth and reduce transaction latency, resulting in improved IoT transitions as evidenced by Bitcoin-NG.
- **Consensus Challenge**: The limited resources of IoT devices make them incongruous for participating directly with consensus protocols (i.e. PoW). There are many consensus mechanisms in development, but many are immature and have not been adequately tested. Resource requirements are based on the kind of consensus mechanism used in a particular blockchain. Generally, solutions send tasks to gateways or other unrestricted devices able to perform the function. Off-chain options that transmit data outside the chain to lessen latency may improve functionality. While there are initiatives aimed at including full blockchain nodes into IoT devices, mining is still a primary obstacle in the IoT because of its limitations. The IoT is primarily made up of devices with resource limitations, but on a global scale the IoT has massive computing power. It is expected that the IoT will grow to include 20 to 50 billion devices by 2020. Research in this area should continue in order to fully utilize the distributed paradigm and worldwide potential of the IoT to adapt consensus. For instance, Babelchain uses an innovative consensus mechanism known as Proof of Understanding (PoU) to adapt PoW for IoT applications. Requiring less energy resources, PoU translates from other protocols rather than employing miners to decipher hash puzzles. The effort is more focused on practical computation while also addressing key issues in IoT communication. Rather than agreeing on transaction status, network peers agree regarding the message's meaning (i.e. action, format, and content). In addition, blockchain data is able to generate information for learning.

IV. Main Applications of DLT and Blockchain

DLT/Blockchain-IoT is applicable to a variety of areas in everyday life, including the financial sector, energy domain, identity management, and supply chain management, healthcare, smart factory among others [4], [6], [7], [8], [9], [10], [11].

A. *Smart Manufacturing*

Blockchain is used in smart manufacturing in several ways, including [49]:

- Secure Firmware Updates: Blockchain can be used to enhance smart manufacturing security. Centralized IoT systems experience a significant bottleneck by restricting factory upgrades. For example, addressing breaches in security requires that firmware be regularly upgraded. But, the majority of firmware updates must be downloaded via centralized servers and manually installed on IoT devices. This can be an inefficient and expensive process when working with distributed IoT systems.
- Enhancing Tracking and Tracing: Blockchain can be used by organizations to more securely, precisely, and effortlessly exchange data in complicated IoT-assisted supply chains. Blockchain has the capability of creating immutable records of products, materials, or parts, promoting total transparency and creating a primary information source for all chain participants. This can be highly valuable when supply chains include diverse IT systems, some participants are not trusted by all participants, or require constant inclusion of new users.
- Monetizing and Protecting Vital Intellectual Property: It is very important that manufacturing companies protect intellectual property. Blockchain can be used to definitively prove intellectual property ownership in the event of a dispute. For example, Bernstein Technologies has created blockchain-based web service that enables the registration of intellectual property and creating a certificate that confirms intellectual property ownership.
- Protecting and Simplifying Quality Checks: Companies can use blockchain and IoT to facilitate quality control and improve customer value. Without blockchain, providing complete transparency and accurate documentation regarding product or process quality can be an expensive endeavor, requiring support from centralized third parties. Blockchain is able to monitor and trace parts throughout the supply chain and provide permanent documentation of the production process and quality assurance. Blockchain is able to tag products and record each transaction, quality confirmation, or change in the blockchain. Utilizing this blockchain application requires that production incorporates automated quality inspections that create and record information directly to the chain. This allows multiple participants to access data, which removes the need to perform inbound quality checks to confirm supplier quality checks. This application may also decrease the need for centralized party or original manufacturer quality audits because participants could use blockchain's certificate management ability to view all documentation and ensure authenticity.
- Advancing Machines as a Service: Blockchain multiplies the possibilities of utilizing a pay-per-use model for IoT-based manufacturing machinery, referred to as Machines as a Service (MaaS). This paradigm allows providers of equipment to charge users based on the output generated rather than directly selling the machinery itself. For example, a compressor supplier could sell compressed air according to volume rather than selling the compressor itself. Using a MaaS paradigm would enable manufacturers to circumvent expensive preliminary investments and more easily upgrade machinery in order to utilize the most innovative technology. When applied well, MaaS models empower manufacturers to expand production flexibility.
- Enabling Machine-Controlled Maintenance: Blockchain IoT model has the capability to facilitate innovative maintenance models and reduce time required for complete maintenance. Innovative manufacturing requires advancements in maintenance to keep pace with new, more complex machinery. Outsourcing maintenance requires users to provide installation information and service agreements to blockchain devices, providing a digital duplication (digital twin) of the device. Blockchain is then able to automatically execute and pay for machinery maintenance. If a piece of equipment needs maintenance, it can generate a service request as well as a smart contract for the maintenance. When completed, the payment is automatically processed and permanent documentation of the maintenance performed is added to the blockchain. These blockchain applications are currently in the development phase, but have the potential to increase equipment dependability, support equipment status monitoring, and develop auditable equipment health assessments. When maintenance is completed by in-house providers, blockchain can confirm that maintenance was completed in adherence to guarantee and warranty agreements. Permanent maintenance history documentation also supports sale of previously-owned machinery. Reduced product lifecycles and continuous changes in design will inspire manufacturers to upgrade equipment more often. Manufacturers selling used machinery can provide potential buyers with the blockchain records to confirm equipment has been appropriately maintained.

B. *Supply Chain Management*

Blockchain is also applicable to supply chain management. It can be useful for documenting the process of sending goods from producers to consumers. Blockchain can record and manage detailed information about warehouses, retail locations, grocery stores, delivery vehicles, movement of goods, and weather conditions with the help of IoT devices. It can also help managers trace issues, locate items in real-time, and plan more efficiently to achieve appropriately stock levels.

C. Food Industry

Blockchain IoT also has the capability of improving transparency when it comes to food product lifecycles. Accurately tracing consumable products is important to food safety, but it can be difficult for IoT to confirm food monitoring across an entire supply chain. Tracing require that raw materials information be digitized across all food manufacturing sectors. Blockchain technology guarantees traceability of food industry information collected by IoT devices.

D. Financial Services

Blockchain technology is most often utilized the financial sector because of its initial connection with Bitcoin. In contrast to more traditional financial services, blockchain supports peer-to-peer transactions (e.g., in IoT data marketplaces) without the need for third party intervention, removing the need for banks or other institutions that require expensive fees. Blockchain also provides immutable transaction records that facilitate transaction verification and helps prevent transaction disputes. Blockchain is also able to reduce transaction processing time to mere seconds, even for international transactions that would normally require several days to process. Financial services that utilize blockchain can also be utilized at any hour of the day. In addition, blockchain-based IoT market places enables customers to securely buy or sell IoT products/services/data instantaneously, and the proceeds are immediately available for reinvestment. Blockchain has the potential to change the way business is done. The insurance industry could also be made more efficient through blockchain by simplifying asset verification and reducing fraudulent claim activity. Blockchain could also be useful in making the ownership of copyrighted digital content more transparent and allowing content creators to obtain royalties quickly.

E. Energy

Blockchain IoT technology could be applicable to the oil and peer-to-peer and wholesale electrical grids. Blockchain IoT can connect customers directly to a wholesale electricity distribution grid, enabling users to trade energy on the grid without the need for retailers, which would reduce electrical costs. It is anticipated that linked electrical grids will be created to enable users to sell or buy renewable energy at much lower prices. Moreover, blockchain IoT can be utilized to improve data recording, tracing, and storage in electrical data systems that handle market pricing, fuel pricing, and other marginal expenses, permitting the public to see transaction prices. Oil and gas companies are also considering the use of blockchain IoT in data and supply monitoring as well as commodity trading. These companies value privacy and the protection of trade secrets, making them more likely to utilize consortium or private permissioned blockchain options that only allow data access by specific parties. This would reduce data management expenses, cut down on processing delays, and improve data security.

F. Digital Identity Management

Blockchain can be utilized to protect human, property, and IoT device identities. Blockchain allow for the creation of smart connected property such as homes, jewelry, appliances, or vehicles that are embedded with a digital identity at the point of manufacture. The property's identity is recorded along with the owner's identity on a blockchain that can also trace transfer of ownership. Blockchain is also applicable to managing non-physical property like stock shares or patents. Some suggest that blockchain could also be utilized to manage human identity and their interaction with IoT devices. Given an identity at birth, that human identity record could be used for education, employment, insurance, health, and governmental records. This would simplify the current use of independent record systems that are difficult to synchronize and vulnerable to fraud and errors. Current systems require users to provide personal data, but do not make clear how that data is used, where it is stored, or who has access. This creates problems both for data owners as well as database owners as online companies may sell or abuse users' personal information. In contrast, blockchain is able to build trust and protect privacy using encryption, giving data owners greater control over personal data (e.g., collected by IoT devices, such as smart health wristbands).

G. Additional Applications

Blockchain also has the potential to revolutionize elections and voting by securing electronic voting and ensuring record transparency and permanence, which reduces election costs. The real estate industry would benefit from using blockchain to store property titles and document transfer of property ownership. Educational records stored via blockchain would provide instantaneous access and ensure credential integrity. Driving records and licensing information maintained using blockchain would make the process of owning and operating a vehicle more efficient and error-free. Finally, blockchain could be utilized to backup data and safeguard against corruption.

V. Blockchain for Smart and Connected Health

A. *Challenges in Healthcare*

While healthcare providers and researchers regularly experience frustration around slow communications, workflow differences, and siloed data, they are often hesitant to share data. This is due to perceptions that personally identifiable information and health data regulations do not allow for data sharing and due to the liability and financial consequences of sharing data. In addition, incongruent health systems create communication gaps, making it difficult to provide coordinated, patient-centered care. One of the main issues in creating healthcare systems is the inability to generate secure links to connect separate systems and create an end-to-end network while simultaneously securing healthcare provider privacy. While standardizations such as FHIR and HL7 support rudimentary interoperability to facilitate data exchange among systems, the magnitude of interoperability is confined by applied standards and needs data mapping between systems in the majority of cases. It can be difficult to maintain these systems because a change in a single interface requires other system participants to adapt as well [4], [5].

B. *Main Applications of DLT/Blockchain in Healthcare*

It is widely speculated that blockchain could greatly impact the healthcare industry by managing data and connecting multiple heterogeneous systems to improve EHR accuracy. Blockchain has the capability to support medical supply chains, facilitate drug prescriptions, safeguard system access, maintain risk data, support data sharing, and generate an audit trail for healthcare activities. In addition, healthcare provider credentialing, medical billing, clinical trials, health record exchange, and industry contracts could benefit from blockchain as healthcare moves toward an IoT-based patient-centered model. Healthcare systems established using blockchain would also improve data dependability and security because records could be consolidated and patients would have ownership of health information.

Blockchain also reduces dependence on a centralized third party to verify data ownership or reliability and handle transactions or data exchange. Blockchain allows secure, pseudonymous transactions to take place directly between participants. Blockchain's capacity for transparency, immutability, and decentralization address widespread healthcare problems such as incorrect or incomplete records and barriers to accessing one's own health data. Effective healthcare systems depend on interoperability so that platforms and software applications can communicate securely and effortlessly to share and utilize data across a variety of healthcare institutions and application providers. Unfortunately, today's healthcare systems are generally siloed and have access to only partial data. Slow communication and diverse workflows further reduce interoperability, but blockchain can provide access to complete, tamper-proof, long-term medical records currently maintained in disparate systems [50], [51], [2], [1], [52], [53], [54], [55], [56], [57], [58], [59], [46], [47].

The main use cases and applications of DLT/blockchain in healthcare domain can be summarized as follows:

*1) **Healthcare Record Sharing**:* Generally, sharing health records is difficult because it contains personal patient information, but blockchain technology has the potential to improve this process. The security of and access to healthcare records is a common industry problem. Sharing records can be difficult because records are scattered across various systems. Neither patients nor medical providers can achieve a comprehensive picture of current medical status because it is impossible to obtain real-time data if records are spread across multiple healthcare systems. Linking records, even using a common identifier such as a Social Security Number, is difficult due to lack of interoperability. Sharing health data is an unproductive process for the reasons outlined below:

- **Slow Process Speed**: Health data copies have to be created and picked up. Current regulations give healthcare providers 30 days to provide patient records; however, many providers need only 5-10 business days to provide records.
- **Lack of Data Security**: Copies of patient data can be stolen or lost as patients take information from one place to another.
- **Incomplete Records**: Records may be incomplete as medical histories are fragmented across multiple systems. Because there is no universal data storage system, patients are required to monitor where and when medical care is received in order to obtain current records.
- **Lack of Data Context**: The current healthcare system is centered on care providers rather than patients, which makes it difficult for patients to take ownership of their healthcare records and control who accesses and uses it.

Blockchain helps to span the communication gap among providers, eliminating the need for a centralized third party and facilitating direct interactions among participants. On its own, blockchain cannot completely solve the issue of data sharing. It must be amalgamated into current separate health systems and data standards. Recently, a few architectures, such as MedRec Architecture and MedShare Architecture have been proposed to address data sharing in healthcare industry:

- MedRec Architecture: This architecture uses blockchain-based architecture to store health records by improving interoperability, data security, and data access. It uses permissioned peer-to-peer blockchain technology and smart contracts with the Ethereum framework to monitor and manage network status transitions.
- MedShare Architecture: This architecture is comprised of four layers. The user layer allows data access via a graphic interface. A data query layer is made up of structures that process system query requests. The database infrastructure layer is made of system databases accessible only by specified institutions. Finally, the data structuring and provenance

layer handles in-system processing using a blockchain network structure, smart contracts, consensus mechanism, and node authentication.

*2) **Healthcare System Log Management**:* Log management is vital because logs provide historical data needed to detect intruders and analyze errors. Appropriately managing logs also gives users more control over information access. However, traditional systems in use are susceptible to data manipulation. Blockchain can ensure that log records are immutable. For instance, the authors of [60] investigated the use of blockchain in healthcare system logs by using blockchain technology to manage information access logs. The method used also sought to standardize data and provide auditing capabilities through the implementation of permissioned blockchain. It is worth noting that the security audit logging can be complicated because the information gathered may be incomplete or useless [50].

*3) **Patient Monitoring**:* Remote Patient Monitoring (RPM) is used to gather medical data from bio sensors or IoT devices in order to monitor a patient's status outside a clinical setting. Patient monitoring is a vital component of treating patients within the healthcare system. The recent development of wearable healthcare devices and big data analytics can be utilized to generate new opportunities for remote healthcare services, reducing the strain on clinic or hospital resources. However, reviewing healthcare data presents both security and privacy issues. Blockchain technology offers a method for sharing, storing, and obtaining the gathered data. For instance, connected and smart IoT ehealth devices could be implanted in patients, and blockchain could serve to securely monitor and store the personally identifiable information gathered by the sensor or device. Such technology would need to comply with HIPPA, the GDPR, and any other regulation applicable to protecting personal data.

Over the past few years, several blockchain-based solutions have been proposed for RPM. Some researchers have demonstrated that smart contracts using Ethereum blockchain can facilitate real-time monitoring and secure automated interventions. Others propose utilization of a blockchain using a hyperledger-centered method of blockchain data gathering and exchange for mobile healthcare stakeholders. Blockchain has also been used to create SMEAD, a mobile monitoring device for diabetics. Mobile devices have also successfully sent data to blockchain applications on Hyperledger Fabric. Another researcher has created Patient Centric Agent (PCA) using blockchain to guarantee data privacy and security with a remote constant monitoring application.

*4) **Tracing**:* Blockchain is also capable of tracking contagious patients suffering from illnesses including COVID-19, Severe Acute Respiratory Syndrome (SARS), or Middle East Respiratory Syndrome (MERS). An infected individual or suspected carrier could wear an IoT device to track movement, enabling the deployment of more effective countermeasures while maintaining patient privacy.

*5) **Monetizing IoT eHealth Resources and Data**:* IoT eHealth service providers and data owners can interact transparently using blockchain without the need for an intercessor. The type and level of shared data is controlled by the owner through smart contracts, as is the timeframe. Using blockchain's distributed ledger, data owners can monitor the movement of data between entities. Cryptocurrencies also allow for the monetization of IoT eHealth data.

*6) **Drug & Pharmaceutical Supply Chains**:* Blockchain could also be useful in healthcare supply chain management and specifically in the area of drug and pharmaceutical supplies. If counterfeit or inferior drugs are delivered, this can have fatal consequences for a patient; however, this is not an uncommon issue. Blockchain has the capability to address such issues by recording all transactions that pertain to prescriptions on a blockchain that connects all key stakeholders such as physicians, manufacturers, patients, distributors, and pharmacists. This method alerts participants to any data tampering. There are also companies that allow the public to access immutable temperature documentation related to the IoT-based transportation of pharmaceutical products in order to confirm quality control compliance.

*7) **Health Insurance Claims**:* Insurers determine if claims should be paid, denied, or paid only in part. Generally, a claim is only partially paid if the insurer decides that a medical service was incorrectly billed or not medically necessary. This means it is vital that all insurance claims be correctly coded. Even a tiny error, such as the misspelling of a name, can result in claim denial. Most insurance claims are processed through an automated system, but claims that are more complicated are more vulnerable to fraud or errors, making the claims decision process more difficult. At this time, almost a quarter of insurance claims are rejected due to simple errors like incorrect demographic details. IoT and Smart contracts offer the capability to automate the decision process to a greater degree by using a distributed network that provides claim transparency to both healthcare providers and insurers. This means that fraud or errors can be caught and corrected more promptly. Smart contracts also guarantee that network participants have access to current information and are appropriately advised of policy or guideline changes.

Blockchain would allow insurance claim processing to benefit from increased data permanence, clearer audit trails, improved data transparency, and decentralization. Patients would not need to gather paperwork to submit claims for payment. The blockchain platform would automatically connect hospitals, healthcare providers, and insurers; therefore, insurers would be able to authenticate the claim and prevent fraud. Some research points to insurance claim processing as one of the most favorable sectors for applying blockchain; however, inaugural implementations have been limited to date. One example can be found in MIStore, a health insurance storage system that uses the Ethereum platform. Earlier this year Samsung SDS revealed a health insurance claim processing platform using Nexledger enterprise blockchain to tackle the hassle of filing claims and reduce fraud.

*8) **Fraud Detection**:* Blockchain can also assist with authenticating information to detect fraud or data tampering and discover malignant acts such as inserting incorrect reviews in online systems. Researchers are also interested in studying fraud detection as it relates to crowdfunding e.g., in healthcare, which is a method of obtaining investment from a large group of people or purchasing company stock to increase equity. Blockchain can be utilized by crowdfunding applications to simplify transactions and make the transfer of funds more efficient and secure. Blockchain could also be used as an economical platform to register shares or stocks of healthcare companies, enabling direct transactions among entrepreneurs and investors. In addition, blockchain could be used by healthcare company shareholders to create a voting system for governance or enable regulators to assess market status and guard against investment fraud.

*9) **Patient Digital Identity**:* Patient identity confirmation is a foundational piece of exchanging health data. A patient is located within a record database by a unique dataset. Enterprise Patient Master Index (EPMI) and Master Patient Index (MPI) were developed to manage the identities of patients within a trustworthy network or institution. Although development efforts have continued, matching patient identities is difficult. Failure to match identities has generated duplicate records as well as inaccurate or incomplete data. Because generally agreed upon standards for the collection of identifying information do not exist, the information required can vary between organizations. While demographic information such as a name, address, Social Security Number, and date of birth are commonly utilized to register patients, names can be stored in a variety of formats and multiple patients may have the same or similar names. In addition, dates of birth can be entered in different ways and addresses change if patients move. Some patients may not have or wish to provide their Social Security Number. Finally, demographic information manually entered can include errors. The more data an organization requires, the greater the capacity for errors. Even if an organization condenses patient information down to a unique identification number, the identifier usually does not work across multiple organizations.

*10) **Healthcare Interoperability**:* Interoperability in the healthcare industry refers to the ability of diverse software and IT systems (i.e. EHR) to share data, communicate, and use exchanged information. Greater interoperability within and among institutions improves the level of care provided to patients. This is especially apparent as providers are empowered to securely exchange records with others (as appropriate) at different locations regardless of relationship status. The primary barrier to interoperability is the implementation of centralized information storage in one database. Centralized storage options result in fragmented health records, reduced health data access, limited interoperability, and lack of high-quality data for research. Millions of health records are created each day and maintained using a centralized database at various hospitals. While centralized third parties are required to ensure information reliability in disparate networks, information that is dispersed among different hospitals is susceptible to being lost or inaccessible to patients.

C. Main Challenges of Utilizing Blockchain in Healthcare

The main challenges facing the integration of blockchain in the healthcare domain can be summarized as follows: many security vulnerabilities

- **Throughput**: High throughput is a necessity in healthcare systems because without immediate access, a lifesaving diagnosis may be delayed. Unfortunately, due to an ever-growing number of nodes in the network and network transactions, additional checks are needed, which can create bottlenecks in the network.
- **Latency**: Authenticating a block requires approximately 10 minutes, which can be harmful to security services if there is a successful cyberattack during that period. Healthcare systems must be agile and constantly accessible because any delay could impact exam analysis.
- **Security**: System security could be compromised, for example if 51% of the network's computational power is commandeered. A healthcare system that loses functionality also loses credibility.
- **Resource Use**: Blockchain technology also requires significant resources for the mining process. Healthcare systems would incur high energy and computing costs because multiple devices (e.g., wearables) are required to monitor patients.
- **Resource Constraints**: Many IoT healtcare devices (e.g., wearables) are constrained due to their power limitations, storage, memory, processing capabilities. Therefore, they cannot execute complex blockchain algorithms.
- **Usability**: Healthcare systems are very complex, making it necessary to develop an Application Programming Interface (API) that is user friendly and intuitive.
- **Centralization**: While blockchain is known as a decentralized architecture, some methods centralize miners, which lessens network reliability. The central node is vulnerable to cyberattacks.
- **Privacy**: It is commonly believed that blockchain can guarantee the privacy, but this has been disproven by some. Additional privacy strategies that comply with privacy laws and the GDPR are needed.

VI. Reference Architecture

Fig. 4 sketches the proposed reference architecture for the healthcare domain, including the roles, components, and the interactions taking place between them. The reference architecture consists of several private blockchains and one main federated blockchain network that interconnects healthcare institutions and orchestrate the data life cycle from data publication to data consumption. The reference architecture is designed to support healthcare stakeholders to share data in a faster, secure and trusted manner without losing important properties like traceability, accountability, and data privacy.

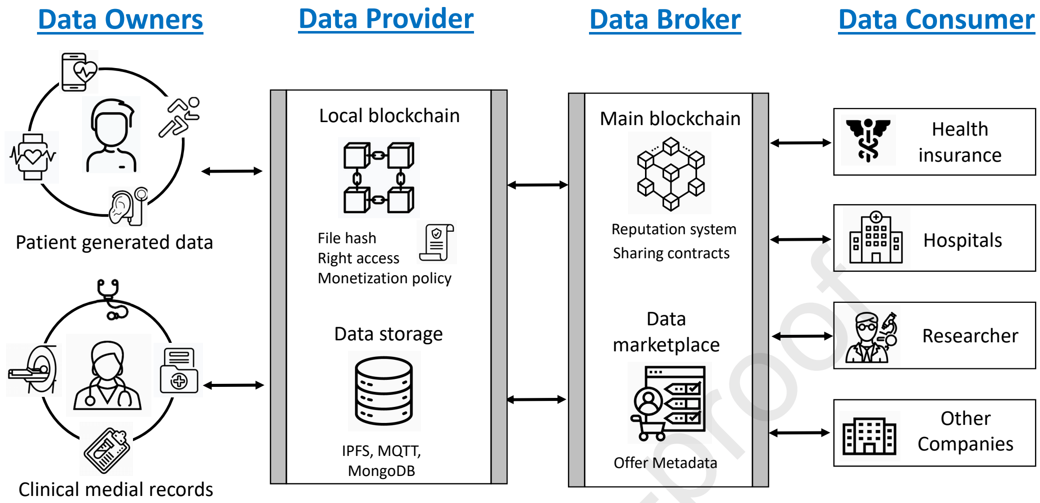


Fig. 4: Sketch of the reference architecture.

A. *Entities*

The reference architecture is composed of the following main entities, roles, and components:

- **Data Owner (DO)**: A person which owns data and allows other entities (e.g., Data Provider) to collect, process and share his own data with others. The data owner has the control over his data and defines his own data access policies.
- **Data Provider (DP)**: A legal entity that provides and maintains the local data infrastructure as well as data storage to collect and store a variety of different medical data (e.g., IoT data streams, x-ray images) of DOs. The DP is also responsible to publish metadata (i.e., description of dataset), usage constraints, billing information, etc. to data broker.
- **Data Consumer (DC)**: An entity that requests data access from the data marketplace (data broker).
- **Data Broker (DB)**: A legal entity that registers, stores, and displays information (metadata) about available datasets in the ecosystem enabling data customers to explore (e.g., using a query interface) and discover datasets and the corresponding DOs/DPs. The DB can also offer a complementary data marketplace solution for data monetization and settlement services for all financial and data exchange transactions as well as a reputation system. Note that the reputation system manages crowd-sourced reviews about the quality of datasets, data owners, providers, and customers. It should be noted that data broker is non-exclusive meaning that multiple brokers may be around at the same time.
- **Identity Providers**: This entity (e.g., Certification Authority of the federated blockchain) manages all participants of the ecosystem.

One of the most important entities in the reference architecture is data provider. Generally, blockchains have storage and data processing limitations. Storing large data on the blockchain leads to a downgrading performance [61]. Unprocessed files of raw genomic data, for instance, can be in excess of 1TB per genome [62]. In addition to large datasets, wearable IoT devices are generating data streams (e.g. heart rate monitoring) to improve the patient quality of care by remote patient monitoring. To efficiently address volume, variety, velocity, and veracity (The Four V's of Big Data), data providers need to exploit a holistic data processing architecture. The most well-known architectures for big data processing are Lambda architecture and Kappa architecture (See Fig. 5) [63]. Lambda architectures can be segregated into three layers; batch, speed and serving layer. The batch layer is termed as data lake and consists of traditional big data storage. This layer supports batch processing of incoming data and holds all the data that has got feed into it. For streaming real-time data the speed layer is used. The results of both layers are then forwarded to a third layer called serving layer, which uses data to cater the pending queries on ad-hoc basis. The Kappa architecture is a simpler alternative to the Lambda architecture as real-time stream and historical batch data are handled using the same technology stack [63]. In this architecture, the batch processing layer is removed and all incoming data are fed through the streaming system. It should be noted that raw medical data can vary in structures and formats that are difficult to analyses and integrate into other systems [64]. Thus, raw medical data are sorted and presented in simpler form through data standards to also address interoperability. Converting raw data to an unified data standard supports data analysis and management scheme [65]. For example, each time raw data is added to the data storage, the raw data can be automatically transformed into a Fast Healthcare Interoperability Resource (FHIR) standard dataset in order to provide a consistent and simple data structure [66]. Note that according to local regulations other standardized data formats (e.g., openEHR, HL7) can be applied as well.

Another important entity is the data broker, which consists of a federated blockchain and smart contracts to deal with the challenges of trading medical data among different data providers and consumers. The data broker is operated by various healthcare stakeholders who know each other but do not fully trust each other. In the proposed reference architecture, the data broker provides full transparency on individual data trades and reputation scores and ensures that data is not used for the wrong purpose or sold against the data owner's data trading policy.

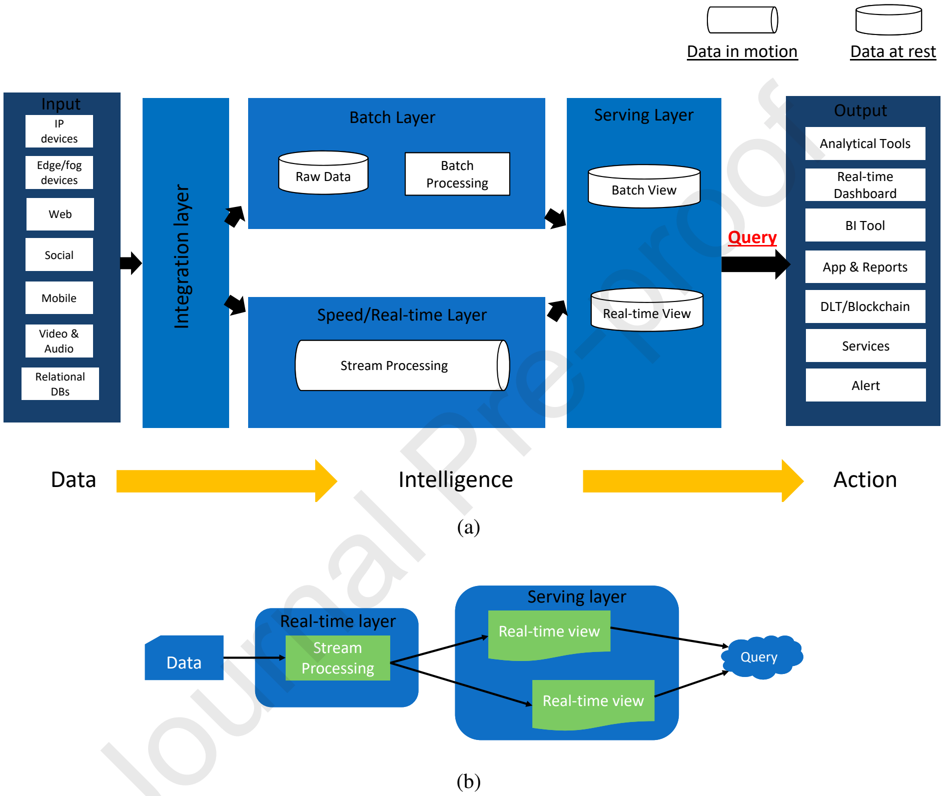


Fig. 5: (a) Lambda architecture. (b) Kappa architecture.

B. Process

Processes specify the interactions taking place between the different roles and components.

1) Data Owner (DO) & Data Provider (DP): Smart Contract Creation: If a DO (e.g., patient) agrees with a DP (e.g., hospital) to share or sell his medical data, both entities must agree first on a set of policies, including information about who is allowed to access the DO data, expiration date or monetization policy of data. Both entities digitally sign the agreement with their private keys and store their set of policies on the DO smart contract (SC) on the local private blockchain (LC) of the DP (See Fig. 6). In addition to the data policy and digital signature, the smart contract of the DO is used to log each data upload of new medical data and each data access. Assuming that the local blockchain allows all registered entities (e.g., DO, DP) to have the right to query and read the logs of the blockchain, the DO keeps control over his own medical data.

2) Data Owner (DO) & Data Provider (DP): Upload Personal Data: All personal medical data are stored securely off-chain on the local data storage system of the DP (e.g., based on Lambda or Kappa architectures) and only information required to be tamper-resistant and transparent are stored on-chain. To fulfill the General Data Protection Regulation (GDPR) compliance and to give DOs full control over their own data; sensitive medical data must be anonymized and trackable at any time [67]. Therefore, we combined local data storage with a local blockchain as shown in Fig. 7. The data upload starts with digital multi-signature of medical data and the corresponding attestation. Multi-signatures require multiple users, in our scenario the

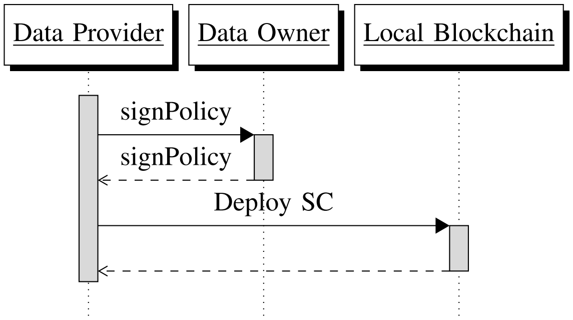


Fig. 6: Process of registering the DOs data policies on the local blockchain.

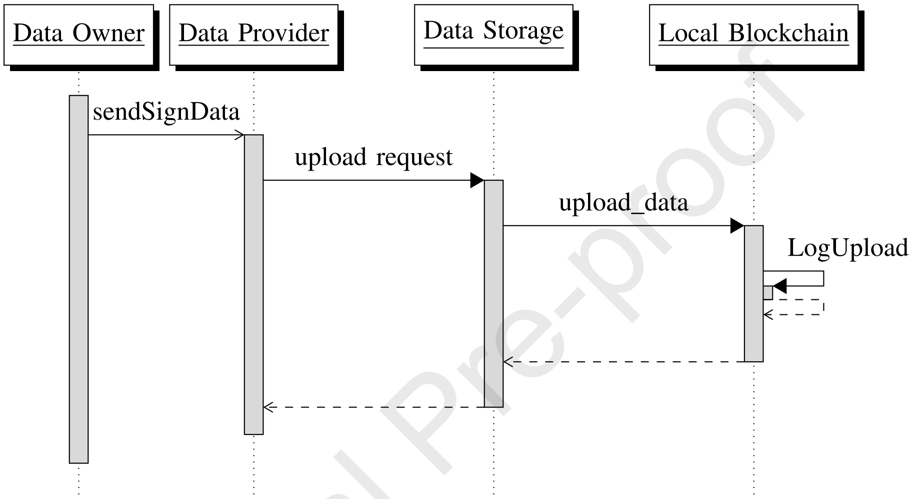


Fig. 7: Process of storing medical data of the DO on the local data storage and corresponding metadata on the local blockchain.

DO and DP, to both use their private keys to sign medical data and corresponding attestations (e.g., diagnose). The public and private key pair are generated using unique identifier (e.g. fingerprint) of the DO and are securely stored on the Certification Authority (CA) of the DP. Next, the DP forwards the signed data to the local data storage. Subsequently, metadata of each uploaded medical dataset is generated to group the medical data on the data marketplace (data broker) and thus simplify subsequent data analysis. The metadata data would include information such as the file hash of each medical data on the local data storage, data type, expiration date and short data description. There are several models available to store and manage metadata, such as CKAN [68] which can easily be harvested into different systems. File hashes are used to link off-chain stored data with on-chain available data information. Considering high frequent data streams, the data stored on a specific API or topic (e.g., MQTT topic) can be hashed and uploaded to the smart contract of the DO instead of hashing each single data entry. All metadata are stored transparently on the blockchain and do not contain any sensitive information about the DO. The data storage system queries the smart contract of the DO on the local blockchain to check the data policies and verify the digital signatures of the DO and DP. If both signatures are valid and the data to be uploaded complies with the predefined data policies of the DO, the upload is logged to the DO's smart contract.

Storing only metadata on a blockchain removes dependencies on storage systems and has the important benefit of verifiable data integrity. The corresponding cost for on-chain data storage of metadata is low compared to the storage of raw medical data because of its relatively small data size. Considerations on what information will be stored on-chain and off-chain is important to comply with the GDPR compliance, which should give DOs control over their personal data. For instance, it is difficult to delete sensitive data of a public permissionless blockchain which is immutable by nature. Thus, data usage policies might also define data access expiration or cancellation date in order to fulfill the so called *right to be forgotten* according to the GDPR compliance.

3) Data Provider (DP) & Data Broker (DB): Publish Metadata: The number of transactions for a large medical system can be around a few million per day [69]. Simulations show that none of the most popular DLT technologies (e.g., Ethereum) can handle such a large system [70]. To avoid potential performance bottlenecks we use a multi-chain network (tiered architecture). This network is based on a single *mainchain* (federated blockchain) for data sharing and multiple *local blockchains* for data

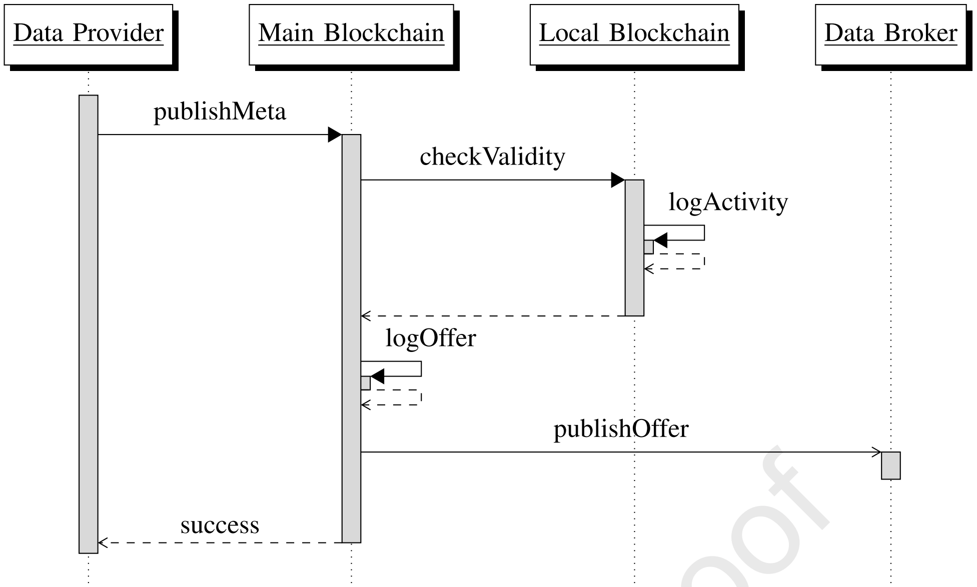


Fig. 8: Process of publishing metadata the main blockchain of the DB and sending data offers to the data marketplace.

collection and access management. The division into a single mainchain (MC) and multiple local blockchains allows for parallel processing of non-competing transactions and extends the entire networks functionality because different consensus mechanisms and smart contracts can be used for different blockchains. To start data sharing across different stakeholder, the DP can publish metadata to the data marketplace (data broker). For this purpose, a smart contract of the mainchain is executed by the DP to check the validity and data policy of the offered medical data. After successful validity checks, the events are logged on the local blockchain of the requesting DP. This way, the DO can follow data activities. Next, the smart contract of the mainchain publishes the data offer to the marketplace of the DB and logs the corresponding metadata on the mainchain. Fig. 8 summarizes the process of publishing metadata.

4) Data Consumer (DC) & Data Broker (DB): Explore Metadata & Purchase Dataset: To request metadata from the data marketplace, the DC first queries the listed metadata and access policies from the data marketplace. All DC are registered with their public key in CA of the system. After an initial registration, the DC can invoke smart contracts of the mainchain using a specific deposit (e.g., cryptocurrency). Next, the smart contract of the mainchain generates an access token and also triggers the corresponding local blockchain with the public key of the DC and the access token. If the DC is allowed to access the data (e.g., not black listed), the access token is sent to the DC. Simultaneously, the access token and the corresponding public key of the DC are logged in the local blockchain of the DP. Next, the DC sends his access token and his digital signature to the data storage system to request data access. The data storage system checks if the access token and signature are logged on the local blockchain before sending data back to the DC. Alternatively, the data storage system could also send a temporary single use download link to the DC to access the requested data instead of sending directly the entire dataset. The sequence diagram of the data transfer is shown in Fig. 9.

5) Data Consumer (DC): Reputation Flow (Dataset Evaluation): Distributed ledger technologies are not a panacea for data quality. Therefore, a reputation system is implemented on the mainchain. Reputation systems help DC to pre-evaluate the trustworthiness of potential dataset, increase the data quality and reduce risks associated with information fraud [71]. Aggregate reputations of individual entities across the entire marketplace enable DC to make trustworthy service selections, helping potential DC to check the quality, reliability and integrity of reviews. For instance, the DB asks the DC for a review after data access. Subsequently, the DC has the option to submit his reviews to help upcoming DC to check the quality of content before making a purchase. Therefore, the unique access token and the digital signature of the DC are required for the review submission on the mainchain. In return, a smart contract verifies the validity of the access token and digital signature before the review is stored. The submitted reputations of medical meta data should be accessible to all registered data marketplace participants. This way the DC can check first the existing reputations by previous DCs before requesting medical data. However, sometimes DCs might not want to give a review after accessing medical data from a specific DP and incentive mechanism are needed to encourage DCs to review the data and to be more cooperative. Incentive mechanisms may consist of a refund to DCs who submit valid reviews or a mutual evaluation between both parties (See Fig. 9).

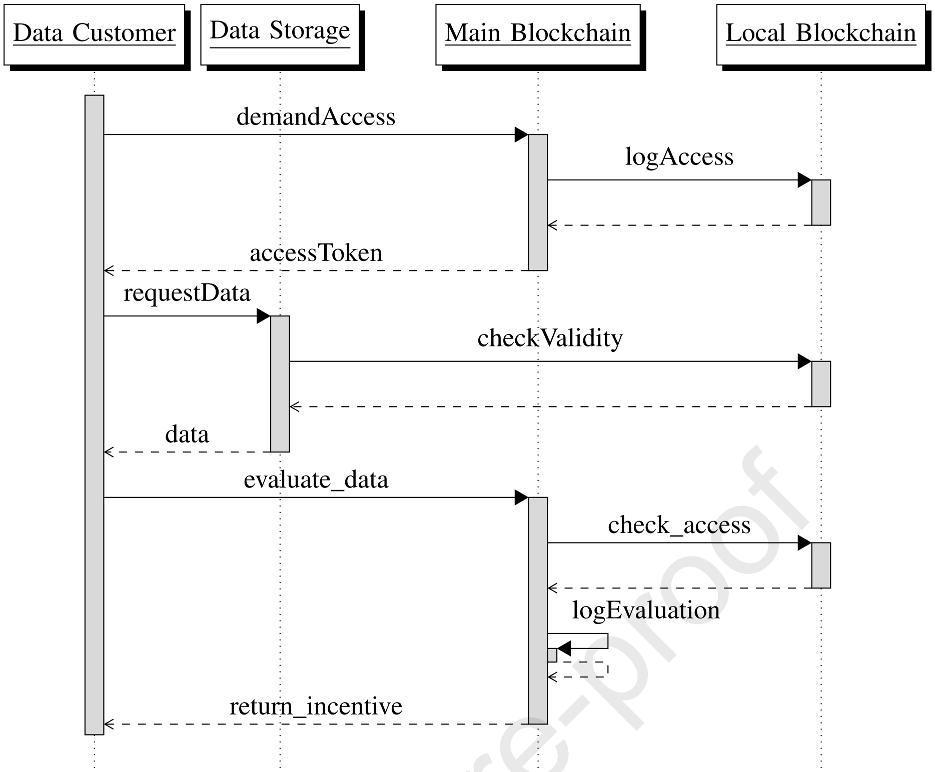
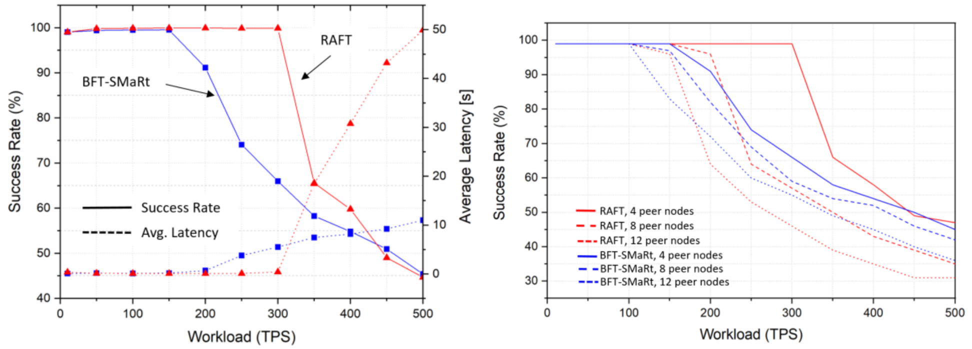


Fig. 9: Process of requesting and accessing data from the main blockchain.

C. *Performance Evaluation*

Medical systems are expected to serve a large number of different entities which might access data simultaneously [70]. Therefore, throughput and scalability test are carried out to highlight the feasibility of our use-case study. For the main and local blockchains we choose to use private blockchains. Unlike public blockchains (e.g., Ethereum), only entities which are granted permission (e.g. registered in the network) can participate in a private blockchain. Compared to the public permissionless blockchain, the limited number of participating entities allows a high transaction throughput (e.g., Bitcoin only achieves seven transactions per second). In addition, private blockchains do not employ a pricing scheme for the execution of smart contracts (e.g., gas in Ethereum), which reduces operational cost and enables business applications. For our evaluation tests we use the Hyperledger Framework (HLF) which is designed for the development of private blockchains and equipped with different consensus mechanisms and a membership identity service that manages user IDs and authenticates all participants on the network [72]. HLF incorporates three software components: clients, peer nodes, and orderer nodes. Clients form endpoints that enable applications to interact with the blockchain network (e.g., list of metadata offered on a centralized data marketplace). Peer nodes endorse transactions and maintain replications of the blockchain network. Orderer nodes generate new blocks, propagate them through the network and participate in the consensus mechanism. All these components collaborate through channels to share and manage identical copies of the network. In a HLF network, multiple channels for multiple blockchain (e.g., mainchain, local blockchain) with different consensus mechanisms and smart contracts can be connected to each other by peer nodes to enable a cross-chain communication (e.g. between different smart contracts). The performance and security level of a blockchain network is significantly affected by the chosen consensus mechanism [73]. Therefore, for all tests we use a crash fault-tolerant consensus (RAFT) and a byzantine fault tolerance consensus (BFT-SMaRt). Crash Fault Tolerance (CFT) networks can still reach consensus if single network components fail. Byzantine fault tolerance (BFT) networks are more complex and deals with systems that may have malicious actors. The threats that a consensus mechanism must be resilient against (e.g., network connections can be interrupted, malicious participants) might be different for each blockchain network and thus, different consensus mechanisms need to be taken into account. For instance, local blockchains might be operated by hospitals and require a lower trust level compared to the mainchain which might be operated by different healthcare stakeholder including insurance companies or different healthcare associations.

The performance of the blockchain network was tested by varying the workload from 10 to 500 submitted transactions per second (tps) for each network setting. The scalability test of the network was carried out by changing the number of nodes from four to twelve. It should be noted that all tests were carried out in Docker containers using the Hyperledger Caliper performance benchmark framework [74] and an Intel(R) Core(TM) i7-8700 server with a 3.20GHz CPU and 16GB memory.



(a)

(b)

Fig. 10: (a) Throughput tests using different consensus mechanisms in HLF based on four orderer and four peer nodes. (b) Scalability tests using different consensus mechanisms in HLF based on four orderer nodes and four to twelve peer nodes.

The results of the performance tests for two different consensus mechanisms are shown in Fig. 10(a). The valid success rate (more than 95%) of submitted write transactions can reach highest to 200 tps for the BFT-SMaRt and up to 300 tps for the RAFT consensus mechanism. Note that for a latency above 1 second not validated transactions are queued at the network nodes buffer waiting for being processed. Compared to the BFT-SMaRt, RAFT achieves a better throughput of successfully submitted transactions. The higher throughput of the crash fault-tolerant consensus is based on how blocks are generated. RAFT is using a leader based approach and has a low communication overhead, compared to BFT-SMaRt. According to University of Kentucky (UK) HealthCare the average number of computerized transactions for a medical system is approximately 10 million per day [69], which is equal to 116 tps. Thus, we consider the requirement of high throughput for both consensus mechanism to be fulfilled.

Scalability is considered as a critical parameter in blockchain frameworks [75]. As depicted in Fig. 10(b) the throughput significantly decreases when the blockchain network scales up (e.g., at twelve peer nodes the throughput decreases from 300 to 100 tps for the RAFT consensus mechanism). Surprisingly, the custom developed BFT-SMaRt consensus mechanism achieves a better scalability than RAFT consensus mechanism. This difference might be based on how blocks of the blockchain are stored. While in BFT-SMaRt blocks are stored in the Random Access Memory (RAM), blocks are stored on the hard drive storage in HLF supported consensus mechanisms [76]. The required level of decentralization of the blockchain network (e.g., by defining the number of peer nodes) is affecting the valid success rate (more than 95%) of submitted write transactions for both consensus mechanism.

VII. Conclusion

Although IoT and DLT/blockchain are two distinct technologies that have evolved independently, their elements are often complimentary of one another. As these two technologies are becoming more and more interconnected over time, a new paradigm, IoT-Blockchain, has been created to address some of the major challenges of IoT, such as security, data integrity, auditability, transparency, reliability, secure peer-to-peer data sharing, and data monetization. This also provides new opportunities for the development of new and creative applications and business models in vertical domains, e.g., from healthcare to supply chain, energy industry, and smart manufacturing. At the same time, various challenges are rising, particularly in terms of scalability and the integration of IoT-Blockchain with other technologies, such as artificial intelligence as well as cloud and edge computing. This paper comprehensively addressed all important aspects of Blockchain-IoT with a focus on IoT eHealth, presented opportunities, applications, solutions, and existing architectures as well as investigated main challenges for more holistic research in this fast-growing field. Furthermore, we presented and evaluated a holistic privacy-aware tamper-resistant tiered reference architecture that could be easily integrated into conventional IoT eHealth solutions enabling various parties (patients, hospitals, research institutes, etc.) to collect, share, and monetize IoT health data.

References

[1] F. Firouzi, B. Farahani, M. Ibrahim, and K. Chakrabarty, “Keynote paper: From eda to iot ehealth: Promise, challenges, and solutions,” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2018.
[2] F. Firouzi, A. M. Rahmani, K. Mankodiya, M. Badaroglu, G. V. Merrett, P. Wong, and B. Farahani, “Internet-of-things and big data for smarter healthcare: from device to architecture, applications and analytics,” 2018.
[3] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, “Towards fog-driven iot ehealth: Promises and challenges of iot in medicine and healthcare,” *Future Generation Computer Systems*, vol. 78, pp. 659–676, 2018.
[4] F. Firouzi, K. Chakrabarty, and S. Nassif, *Intelligent Internet of Things: From Device to Fog and Cloud.* Springer, 2020.

[5] B. Farahani, F. Firouzi, and K. Chakrabarty, "Healthcare iot," in *Intelligent Internet of Things*. Springer, 2020, pp. 515–545.

[6] X. Liu, B. Farahani, and F. Firouzi, "Distributed ledger technology," in *Intelligent Internet of Things*. Springer, 2020, pp. 393–431.

[7] Z. Xiong, Y. Zhang, N. C. Luong, D. Niyato, P. Wang, and N. Guizani, "The best of both worlds: A general architecture for data management in blockchain-enabled internet-of-things," *IEEE Network*, vol. 34, no. 1, pp. 166–173, 2020.

[8] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2018.

[9] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.

[10] W. Viriyasitavat, L. Da Xu, Z. Bi, and D. Hoonsopon, "Blockchain technology for applications in internet of things—mapping from system design perspective," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8155–8168, 2019.

[11] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for internet of things," *Computer Communications*, vol. 136, pp. 10–29, 2019.

[12] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of iot data," in *Proceedings of the 2017 on Cloud Computing Security Workshop*, 2017, pp. 45–50.

[13] Proof-of-Work Explained, available at https://cointelegraph.com/explained/proof-of-work-explained.

[14] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *self-published paper, August*, vol. 19, p. 1, 2012.

[15] M. Castro, B. Liskov *et al.*, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, no. 1999, 1999, pp. 173–186.

[16] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, 2008.

[17] I. B. C. L. A. Mizrahi and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake," 2014.

[18] E. Bellini, Y. Iraqi, and E. Damiani, "Blockchain-based distributed trust and reputation management systems: a survey," *IEEE Access*, vol. 8, pp. 21 127–21 151, 2020.

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

[20] S. S. Chawathe, "Clustering blockchain data," in *Clustering Methods for Big Data Analytics*. Springer, 2019, pp. 43–72.

[21] X. Zha, K. Zheng, and D. Zhang, "Anti-pollution source location privacy preserving scheme in wireless sensor networks," in *2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 2016, pp. 1–8.

[22] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372–383, 2014.

[23] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, 2016.

[24] E. Alsaadi and A. Tubaishat, "Internet of things: features, challenges, and vulnerabilities," *International Journal of Advanced Computer Science and Information Technology*, vol. 4, no. 1, pp. 1–13, 2015.

[25] L. Axon and M. Goldsmith, "Pb-pki: A privacy-aware blockchain-based pki," 2016.

[26] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, "World of empowered iot users," in *2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, 2016, pp. 13–24.

[27] J. H. Park and J. H. Park, "Blockchain security in cloud computing: Use cases, challenges, and solutions," *Symmetry*, vol. 9, no. 8, p. 164, 2017.

[28] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "Fairaccess: a new blockchain-based access control framework for the internet of things," *Security and Communication Networks*, vol. 9, no. 18, pp. 5943–5964, 2016.

[29] O. Alphand, M. Amoretti, T. Claeys, S. Dall'Asta, A. Duda, G. Ferrari, F. Rousseau, B. Tourancheau, L. Veltri, and F. Zanichelli, "Iotchain: A blockchain security architecture for the internet of things," in *2018 IEEE wireless communications and networking conference (WCNC)*. IEEE, 2018, pp. 1–6.

[30] A. Banafa, *Secure and Smart Internet of Things (IoT)*. River Publishers, 2018.

[31] Y. Zhang and J. Wen, "The iot electric business model: Using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 983–994, 2017.

[32] A. Ouaddah, A. Abou Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in iot," in *Europe and MENA cooperation advances in information and communication technologies*. Springer, 2017, pp. 523–533.

[33] G. Zyskind, O. Nathan, and A. Pentland, "Enigma: Decentralized computation platform with guaranteed privacy," *arXiv preprint arXiv:1506.03471*, 2015.

[34] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for iot," *Ieee Access*, vol. 6, pp. 115–124, 2017.

[35] T. Hardjono, N. Smith, and A. S. Pentland, "Anonymous identities for permissioned blockchains," 2014.

[36] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016, pp. 839–858.

[37] S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, "A blockchain connected gateway for ble-based devices in the internet of things," *IEEE Access*, vol. 6, pp. 24 639–24 649, 2018.

[38] M. S. Ali, K. Dolui, and F. Antonelli, "Iot data privacy via blockchains and ipfs," in *Proceedings of the seventh international conference on the internet of things*, 2017, pp. 1–7.

[39] W. Viriyasitavat, L. Da Xu, Z. Bi, D. Hoonsopon, and N. Charoenruk, "Managing qos of internet-of-things services using blockchain," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1357–1368, 2019.

[40] O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018.

[41] 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.

[42] A. Outchakoucht, E. Hamza, and J. P. Leroy, "Dynamic access control policy based on blockchain and machine learning for the internet of things," *Int. J. Adv. Comput. Sci. Appl*, vol. 8, no. 7, pp. 417–424, 2017.

[43] J. P. Dias, H. S. Ferreira, and Â. Martins, "A blockchain-based scheme for access control in e-health scenarios," in *International Conference on Soft Computing and Pattern Recognition*. Springer, 2018, pp. 238–247.

[44] X. Zhu and Y. Badr, "Fog computing security architecture for the internet of things using blockchain-based social networks," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018, pp. 1361–1366.

[45] Q. Zhu, S. W. Loke, R. Trujillo-Rasua, F. Jiang, and Y. Xiang, "Applications of distributed ledger technologies to the internet of things: A survey," *ACM Computing Surveys (CSUR)*, vol. 52, no. 6, pp. 1–34, 2019.

[46] M. Naz, F. A. Al-zahrani, R. Khalid, N. Javaid, A. M. Qamar, M. K. Afzal, and M. Shafiq, "A Secure Data Sharing Platform Using Blockchain and Interplanetary File System," *Sustainability (Switzerland)*, vol. 11, no. 24, pp. 1–24, 2019.

[47] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "GDPR-Compliant Personal Data Management: A Blockchain-Based Solution," *IEEE Transactions on Information Forensics and Security*, vol. 15, no. OCTOBER, pp. 1746–1761, 2020.

[48] Can blockchain accelerate Internet of Things (IoT) adoption?, available at https://www2.deloitte.com/ch/en/pages/innovation/articles/blockchain-accelerate-iot-adoption.html.

[49] S. Zhao, S. Li, and Y. Yao, “Blockchain enabled industrial internet of things technology,” *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1442–1453, 2019.

[50] E. J. De Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, “A survey of blockchain-based strategies for healthcare,” *ACM Computing Surveys (CSUR)*, vol. 53, no. 2, pp. 1–27, 2020.

[51] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, “Towards fog-driven iot ehealth: promises and challenges of iot in medicine and healthcare,” *Future Generation Computer Systems*, 2017.

[52] B. Yan and G. Huang, “Supply chain information transmission based on rfid and internet of things,” in *2009 ISECS International Colloquium on Computing, Communication, Control, and Management*, vol. 4. IEEE, 2009, pp. 166–169.

[53] B. Houtan, A. S. Hafid, and D. Makrakis, “A survey on blockchain-based self-sovereign patient identity in healthcare,” *IEEE Access*, vol. 8, pp. 90 478–90 494, 2020.

[54] A. Kumar, D. Kumar Sharma, A. Nayyar, S. Singh, and B. Yoon, “Lightweight proof of game (lpog): A proof of work (pow)’s extended lightweight consensus algorithm for wearable kidneys,” *Sensors*, vol. 20, no. 10, p. 2868, 2020.

[55] A. M. Rahmani, T. N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jiang, and P. Liljeberg, “Exploiting smart e-health gateways at the edge of healthcare internet-of-things: A fog computing approach,” *Future Generation Computer Systems*, vol. 78, pp. 641–658, 2018.

[56] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, “Continuous patient monitoring with a patient centric agent: A block architecture,” *IEEE Access*, vol. 6, pp. 32 700–32 726, 2018.

[57] V. Patel, “A framework for secure and decentralized sharing of medical imaging data via blockchain consensus,” *Health informatics journal*, vol. 25, no. 4, pp. 1398–1411, 2019.

[58] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, “Medshare: Trust-less medical data sharing among cloud service providers via blockchain,” *IEEE Access*, vol. 5, pp. 14 757–14 767, 2017.

[59] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, “Secure and trustable electronic medical records sharing using blockchain,” in *AMIA annual symposium proceedings*, vol. 2017. American Medical Informatics Association, 2017, p. 650.

[60] J. Anderson and S. Smith, “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.

[61] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, “Blochie: A blockchain-based platform for healthcare information exchange,” *Proceedings - 2018 IEEE International Conference on Smart Computing, SMARTCOMP 2018*, pp. 49–56, 2018.

[62] K. Y. He, D. Ge, and M. M. He, “Big data analytics for genomic medicine,” *International Journal of Molecular Sciences*, vol. 18, no. 2, pp. 1–18, 2017.

[63] F. Firouzi, K. Chakrabarty, and S. Nassif, *Intelligent Internet of Things: From Device to Fog and Cloud*, 2020.

[64] RACHEL L., “Data Standards in Clinical Research: Gaps, Overlaps, Challenges and Future Directions,” vol. 14, no. 6, pp. 687–696, 2007.

[65] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, “A Blockchain-Based Medical Data Sharing and Protection Scheme,” *IEEE Access*, vol. 7, pp. 118 943–118 953, 2019.

[66] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, “FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data,” *Computational and Structural Biotechnology Journal*, vol. 16, pp. 267–278, 2018. [Online]. Available: https://doi.org/10.1016/j.csbj.2018.07.004

[67] D. Hawig, C. Zhou, S. Fuhrhop, A. S. Fialho, and N. Ramachandran, “Designing a distributed ledger technology system for interoperable and general data protection regulationâ€“compliant health data exchange: A use case in blood glucose data,” *Journal of Medical Internet Research*, vol. 21, no. 6, pp. 1–13, 2019.

[68] CKAN, available at https://ckan.org/portfolio/metadata/.

[69] L. Dawahare, “UK HealthCare Exploring Ways Big Data Analytics Can Improve Patient Care.” [Online]. Available: https://med.uky.edu/news/uk-healthcare-exploring-ways-big-data-analytics-can-improve-patient-care

[70] A. Donawa, I. Orukari, and C. E. Baker, “Scaling Blockchains to Support Electronic Health Records for Hospital Systems,” *2019 IEEE 10th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2019*, pp. 0550–0556, 2019.

[71] Y. Cai and D. Zhu, “Fraud detections for online businesses: a perspective from blockchain technology,” *Financial Innovation*, vol. 2, no. 1, 2016.

[72] Hyperledger Foundation, “A Blockchain Platform for the Enterprise,” 2018. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.4/

[73] S. M. Hosseini Bamakan, A. Motavali, and A. Babaei, “A survey of blockchain consensus algorithms performance evaluation criteria,” *Expert Systems with Applications*, p. 113385, 2020.

[74] Hyperledger, “Hyperledger Blockchain Performance Metrics.” [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2018/10/HL_Whitepaper_Metrics_PDF_V1.01.pdf

[75] C. Stathakopoulou, “On Scalability and Performance of Permissioned Blockchain Systems,” 2018.

[76] “Byzantine Fault-Tolerant (BFT) State Machine Replication (SMaRt) v1.2.” [Online]. Available: https://github.com/bft-smart/library