Journal of
Sensor and Actuator Networks

MDPI

Article

Blockchain and IoMT against Physical Abuse: Bullying in Schools as a Case Study

Nikolaos Ersotelos [1], Mirko Bottarelli [1], Haider Al-Khateeb [1,*], Gregory Epiphaniou [2], Zhraa Alhaboby [1], Prashant Pillai [1] and Amar Aggoun [1]

[1] Wolverhampton Cyber Research Institute (WCRI), School of Mathematics and Computer Science, University of Wolverhampton, West Midlands WV1 1LY, UK; N.Ersotelos@wlv.ac.uk (N.E.); M.Bottarelli@wlv.ac.uk (M.B.); Z.Alhaboby@wlv.ac.uk (Z.A.); P.Pillai@wlv.ac.uk (P.P.); A.Aggoun@wlv.ac.uk (A.A.)
[2] Warwick Manufacturing Group (WMG), University of Warwick, International Manufacturing Centre, Coventry CV4 7AL, UK; gregory.epiphaniou@warwick.ac.uk
* Correspondence: H.Al-Khateeb@wlv.ac.uk

Abstract: By law, schools are required to protect the well-being of students against problems such as on-campus bullying and physical abuse. In the UK, a report by the Office for Education (OfE) showed 17% of young people had been bullied during 2017–2018. This problem continues to prevail with consequences including depression, anxiety, suicidal thoughts, and eating disorders. Additionally, recent evidence suggests this type of victimisation could intensify existing health complications. This study investigates the opportunities provided by Internet of Medical Things (IoMT) data towards next-generation safeguarding. A new model is developed based on blockchain technology to enable real-time intervention triggered by IoMT data that can be used to detect stressful events, e.g., when bullying takes place. The model utilises private permissioned blockchain to manage IoMT data to achieve quicker and better decision-making while revolutionising aspects related to compliance, double-entry, confidentiality, and privacy. The feasibility of the model and the interaction between the sensors and the blockchain was simulated. To facilitate a close approximation of an actual IoMT environment, we clustered and decomposed existing medical sensors to their attributes, including their function, for a variety of scenarios. Then, we demonstrated the performance and capabilities of the emulator under different loads of sensor-generated data. We argue to the suitability of this emulator for schools and medical centres to conduct feasibility studies to address sensor data with disruptive data processing and management technologies.

Keywords: blockchain; smart contracts; medical sensors; academy; bullying; students; chronic conditions; vulnerable groups

Citation: Ersotelos, N.; Bottarelli, M.; Al-Khateeb, H.; Epiphaniou, G.; Alhaboby, Z.; Pillai, P.; Aggoun, A. Blockchain and IoMT against Physical Abuse: Bullying in Schools as a Case Study. *J. Sens. Actuator Netw.* **2021**, *10*, 1. https://doi.org/10.3390/jsan10010001

Received: 1 December 2020
Accepted: 25 December 2020
Published: 29 December 2020

1. Introduction

Primary and secondary education students spend about a third of their life attending school, which suggests that the school environment impacts significantly on their lives. Therefore, schools are expected to be places of promoting emotional well-being, and where early signs of changes to students' behaviour and of mental distress can be spotted [1]. Schools are well placed to perform an essential role to safeguard children. For example, they are expected to develop robust practices to identify and act on signs of abuse (and neglect), have a good vetting process in place for adults working with children, and train members of staff to keep their knowledge up to date on regulations and safeguarding policy. Another aspect is to establish trust with children to feel confident to seek advice and report to members of the team should they have a worry.

In relation to children and young people, the promotion of welfare in schools is regularly inspected. For instance, the Office for Standards in Education (Ofsted) in the UK publishes safeguarding and inspectors' responsibilities including essential requirements such as enforcing the Department for Education (DfE) statuary guidance for schools [2]. It also makes references to other guidelines, including "keeping children safe in education," "working together to safeguard children," and "prevent duty guidance for England and Wales" [2]. Consequences from regular inspections affect schools' ratings at a national level and trigger follow-up processes to promote compliance and adequate safeguarding.

Safeguarding action plans aim to protect young people from problems ranging from neglect to abuse (sexual, emotional, physical). In this study, we focus on bullying and physical abuse targeting young people with disabilities and chronic conditions. Recent studies show that the impact of bullying can be severe, with health implications on these vulnerable groups [3,4]. Moreover, there is evidence suggesting they were victimised due to their visible signs of disabilities, as discussed in refs. [5,6]. Bullying is a fixated behaviour targeting a victim; it is defined as an aggressive act carried out by an individual or by a group repeatedly. It includes threats and abuse to intimidate or dominate the victims. This dangerous behaviour has an essential characteristic around the perception of power imbalance, which can either be physical or social [7]. Bullying can have a devastating impact on victims' psychological well-being and psychosocial functioning. It can be persistent and include a stalking behaviour, which is an abnormal behaviour characterised by persistence, fixated threats and intrusions by the "offender" towards the "victim" resulting in fear and distress.

Current intervention mechanisms are still problematic with an area for improvement. Despite increased awareness of the impact of bullying, recent studies report a high prevalence in schools. A systematic review [8] and meta-analysis to estimate prevalence among Australian children reported the 12-month prevalence of physical bullying victimisation at 15.17% with a lifetime prevalence of 25.27%. The content of 463 student surveys representing middle schools across the Southern United States shows 37% of students were bullied either physically or online [9]. In China, the incidents of bullying reported were 26.10% [10]. In the UK, a survey by the Organisation for Economic Co-operation and Development (OECD) (Teachers and School Leaders 2018 survey) covering around 250,000 teachers from 48 industrialised countries showed that in 2018 [2] 29% of English secondary schools received reports of bullying, 29.4% in Finland, 27.0% in Sweden, 27.2% in France, and 25.6% in Bulgaria.

In this study we offer a two-fold contribution. Firstly, we design a new layer of protection for medically vulnerable students by exploiting the characteristics of Internet of Medical Things (IoMT) data from medical sensors and wearable devices already attached to students due to chronic conditions to add a new layer of protection. IoMT data can be used to detect stress and incidents of victimisation. In this regard, we propose and discuss how a private permission blockchain deployment in established IoMT infrastructures can support safeguarding with timely reporting of incidents (near real time) while regulating data sharing between stakeholders (e.g., schools and medical centres). The role of blockchain is inevitable to keep a track record of changes that is also trusted (e.g., complies with the rules of digital evidence). We argue that this novel approach to supporting the well-being of vulnerable victims of bullying and physical abuse is a key enabled to support fundamental safeguarding principles, namely, empowerment, prevention, proportionality, protection, partnership, and accountability.

Secondly, we appreciate that stakeholders with no existing infrastructure require feasibility studies. Therefore, the second contribution is manifested through the development of an emulator to demonstrate the performance and capabilities of the proposed architecture given different loads of sensor-generated data. We argue to the suitability of this emulator for schools to conduct feasibility studies to address sensor data with disruptive data processing and management technologies. The emulator takes under consideration organisational and functional characteristics of the IoMT sensors, network-related metrics, and data attributes to better visualise inhibitors to the successful integration of these environments with disruptive technologies such as blockchain. The emulator acts as a standalone tool that can be utilised to test and verify the scalability and interoperability of sensors with distributed data management and processing structures.

In the remaining part of this paper, we cover background and related work in Section 2 and propose a blockchain-based safeguarding model for schools in Section 3. The integration of blockchain with IoMT data for the model is fully investigated in Section 4, including challenges and consensus mechanisms. In Section 5, we present the design requirements of our experiments and emulator. We also test different consensus mechanisms to investigate the efficacy of a private permissioned blockchain in the management and processing of data generated by medical sensors. Section 5 discusses the main results and analysis from our experiments, and Section 6 concludes our work.

2. Background and Related Work

2.1. Bullying and Its Impact on People with Disabilities and Chronic Conditions

Bullying is an aggressive intentional act that is verbally, physically, or socially hurtful and is repeated over time directly or indirectly [11–13]. In bullying experiences, there is a perceived power imbalance between the bully and the victim, thus, it can also be described as using power to control others and cause distress [13]. Bullying is a local and international issue that is consistently associated with a negative impact on the victims [3,14,15]. In Sweden, a study of 5248 schoolchildren reported that 14% experienced bullying in the past two months. The reported impact was severe, such as poor general health, physical health problems (headache, migraine, stomach ache, tinnitus, musculoskeletal pain), mental health problems (insomnia, anxiety, worry, depression), and self-injurious behaviour [13].

The impact of bullying is potentially more severe on vulnerable groups such as people with disabilities and chronic conditions [3,4]. In Canada, individuals who have epilepsy were victimised compared to their peers in schools. Likewise, young people with chronic kidney disease were victimised [5]. Sentenac et al. [6] studied 12,048 cases of victimization targeting students aged between 11 and 14 years old in France and Ireland. Findings showed that young people living with diabetes, arthritis, cerebral palsy, and allergies were frequently targeted by other children. The prevalence in Ireland was 20.6% and 16.6% in France [6]. Other documented targeted conditions include attention deficit hyperactivity disorder (ADHD) [16], autism [17], hearing impairment or deafness [18], and chronic tic disorders [19]. The underlying causes were "being different" [20,21] or having a different lifestyle as part of the self-management in conditions such as diabetes and asthma [22]. Nonetheless, the impact of such conditions is potentially devastating and has immediate and long-term medical manifestation [3].

Furthermore, cyberbullying is a form of bullying that occurs when such experiences take place partially or fully in cyberspace, such as bullying through email, instant messaging, chatrooms, or webpages, or by receiving digital images or messages to a phone [3,11]. Cyberbullying could take the form of offensive messages sent to a target (harassment), an online fight between two people, posting personal data of the target online without permission, blocking a person from a social list, impersonation, stalking, or sexting (sending nude pictures of the target without their knowledge or consent) [23]. Cyberbullying is increasingly reported with a reported prevalence of up to 41% among children with long-term conditions [24]. It causes no less impact compared to its offline counterpart, such as subjective health complaints [24], which include a group of general symptoms indicating health status, including headache, feeling low, being irritable, nervousness, sleep, or dizziness. These symptoms were significantly higher in cases of online harassment, especially among female victims [24,25]. Other impacts include post-traumatic stress symptoms [26], depression and anxiety [27], and suicidality and self-harm [28]. Hence, often cyberbullying and bullying are researched together [13].

2.2. IoMT Applications

The Internet of Medical Things (IoMT) has infiltrated almost every field of modern healthcare that seamlessly integrates with large-scale automation systems and parallel computation platforms. Sensors and actuators in these environments have naturally evolved into highly distributed applications that computerise processes in e-health services offered and general supply-chain management. At the same time, they proved to better link physical properties with digital controls [29]. They are provided with unique identifiers and the ability to sense, process, and make decisions based on a data stream externally or internally processed. This decision-making capability is often underpinned by the complete absence of human interference or interaction. Mohammed et al. [30] suggested a smart healthcare monitoring system (SW-SHMS) to collect data through wearable sensors, which are collected and stored in the cloud for further analysis. In this way, phycological disorders may be spotted and transmitted to a user's doctor. Zualkernan et al. [31] proposed the use of a mobile phone keyboard to monitor emotions and moods. This is done by testing users' typing styles, texting speeds, the time lapses between presses, and even their physical shaking; it is then measured using an accelerometer and a multi-response linear regression machine learning algorithm. Lane et al. [32] and Hicks et al. [33] developed applications called "BeWell" and "AndWellness" for use in android smartphones to promote better health by tracking social and mental activities, including the quality of sleep and social interactions and by providing intelligent feedback.

The main objectives of the referred applications are to sense, acquire, and analyse (process) data, which can be used to detect in time the students who need further support. Then the main issue that arises is the secured storage of the sensitive collected health data. The answers to the above questions are (i) the IoMT, which allows smartphones or other devices to use and manage the connection to the Internet; (ii) the cloud services that provide an efficient and effective framework for storing and processing big amounts of data, providing Infrastructure as a Service; and (iii) blockchain technology, which allows the security hardening of sensitive and heavy volumes of data. Applying blockchain technologies to protect data from healthcare applications is getting increasing research focus.

2.3. *Blockchain Technology for Healthcare Information*

Specific properties of blockchain technology have already been used to address, efficiently and with interoperability, healthcare information and product transactions [34]. These areas include pharmaceuticals, e-health, and clinical research. For instance, pharmaceutical companies can track drug journeys more swiftly and securely, and medical equipment supply chains can be more streamlined, enabling buyers to acquire them more efficiently and securely. In addition, patients, doctors, clinical researchers, and healthcare providers can share electronic health records both quickly and with significant advantages in privacy, security, safety, transparency, and data integrity. Thus, in contrast to conventional data-management technologies, where the patients' data are placed under direct control by a central server, a blockchain decentralised system firmly establishes patient ownership by putting them "in the driving seat" for managing and controlling their own data (see Figure 1). This "smart" and "citizen-based" interoperability approach for health records enables health data exchange among health information systems and patients. It also offers inherent provenance and integrity of the data, as well as great traceability and support for seamless data sharing that can eliminate duplication, errors, and inconsistencies compared to traditional centralised data storage.

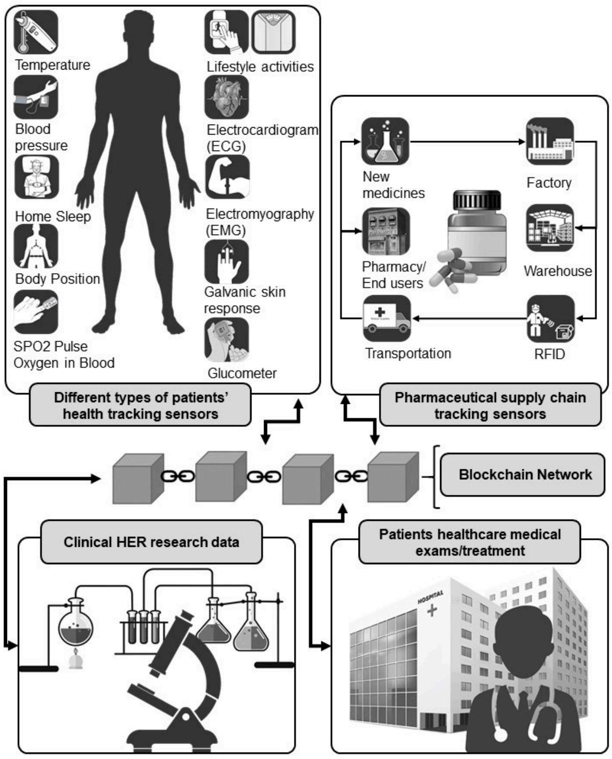

Figure 1. Blockchain use cases in Internet of Medical Things (IoMT).

2.4. Blockchain for Sharing Electronic Health Records (EHR)

Electronic health records (EHR), which are created and maintained throughout a patient's lifetime by all providers, are vital sources of intelligence, the sharing of which is essential for operating a quality service [35]. However, in their current, fragmentary form, they are not easily accessed by patients. Blockchain, on the other hand, based on a combination of telemedicine and precision medicine, would make collaborative decision-making between professionals and patients possible. Using a private blockchain Ethereum platform with a Practical Byzantine Fault Tolerance (PBFT) consensus mechanism, ref. [36] created a system where patients can store their lifestyle data derived from their mobile sensors as new events in the database. This Health Insurance Portability and Accountability Act (HIPAA)—compliant system records and monitors real-time interventions, notifies patients and professionals, and identifies initiators. The authors believe this resolves many remote monitoring security vulnerabilities. In contrast, ref. [37] proposed a public blockchain network based on Proof-of-Importance (PoI) protocol to ensure that medical records exist and have not been tampered with and that an off-chain cloud storage-based framework exists to manage, share, and record patients' data, which is subject to a hashing algorithm to ensure integrity. Thereafter, the data is available to the patient and cannot be accessed by unauthorised parties. Ref. [38] also developed a public blockchain platform named BlockChain platform for Healthcare Information Exchange (BloCHIE) that supports two Proof of Work (PoW) algorithms—the first incorporates an electronic medical record from the relevant institution signed by both institution and patient, and the second consists of personal data derived from the patient's sensors. To meet both authenticity and privacy requirements, the authors reinforced the platform with on-chain and off-chain verification procedures.

2.5. Blockchain Applications in Healthcare

Other examples of blockchain applications in healthcare include clinical research and pharmaceuticals. Blockchain offers the pharmaceutical supply chain the ability to preserve the authenticity and condition of drugs and mitigate against counterfeiting by tracing and tracking pharmaceutical products throughout their life cycle [39]. Information such as temperature and humidity conditions of the medicines are also monitored and stored on the blockchain platform. Ref. [40] also proposed a pharmaceutical turnover control system for monitoring the transportation of the drugs based on a private blockchain network administered by a state-controlled agency. As it is a Hyperledger Fabric-based network, all nodes have different roles in the system. Not all "endorser peers" nodes, though, are directly involved in the execution of smart contracts. While the end-user "client peers" place their orders, "Endorser peers" validate and execute them; however, special "nodes-guarantors" are required to execute the code of smart contracts. Credibility risks in collecting clinical trial data can be eliminated with the use of blockchain technology. It thus ensures that its analysis of clinical research complies with the pre-specified plans. Furthermore, threats to privacy, integrity, sharing, record keeping, and patient enrolment can be avoided [41].

Ref. [42] developed a pubic blockchain using a Proof of Capacity (PoC) web-based interface named BlockTrial, which allows users to run trial-related "smart contracts." The patients grant access to their health data collected from the sensors, and researchers may request data stored off-chain, while a durable and transparent log of all transactions is created in the form of a distributable ledger. BlockTrial is beneficial as it both allows patients better access and control over their data and encourages researchers to adhere to reporting requirements.

Similarly, ref. [43] developed SCoDES, a Hyperledger blockchain framework based on PoC to improve the procedures for managing patient consent, with confidentiality, to share their health data with clinicians. The collected data from the sensors is shared between medical platforms using appropriate software (e.g., React, REpresentational State Transfer (REST) Server, and Research Electronic Data Capture (REDCap)).

3. Proposed Architecture and Emulator Environment

A high-level demonstration of the solution is shown in Figure 2 and the emulator's architecture is shared in Figure 3. The proposal was designed to establish collaboration between the IoMT service provider (e.g., hospital, medical centre) and a participating school attended by the patient. In our case study, the scenario focuses on bullying at schools due to the size of the problem, as evidenced by published studies. Figure 2 illustrates how students with long-term conditions (which can be a disability, chronic disease, or both) are supported by disease management programmes (DMPs) to support the stability of their day-to-day lives. However, several factors could introduce risk through instability. Bullying and physical abuse are one of the key reasons a life's routine can be affected. Furthermore, a bullying experience, in this case, can be life-threatening and require urgent intervention (e.g., by security officers on campus).

The IoMT data is typically shared with the medical service provider without the added value of blockchain immunity and data management. We propose an access control module responsible for permitting the required access to IoMT data to trigger the required intervention. Several principles govern the model. These are:

- Segregation of duties between stakeholders;
- Principle of least privilege; and
- Forensic readiness enabled by an automated process where the chain of custody is blockchain-based and updated in real time.

To evaluate the performance of the blockchain-based model in a hypothetical IoMT scenario, Figure 3 presents the architectural components of our IoMT–blockchain emulator, namely, the main design requirements and the reference architecture. It consists of several virtual machines, each containing different elements encapsulated and isolated in containers. These containers communicate with the rest of the system via a Docker Swarm network, which orchestrates local docker installations. The use of containers is justified by their substantial lightness, portability, and a corresponding reduction in management overhead since they share the same operating system. The use of virtual machines has not been completely excluded but considered to logically group components that are geographically located remotely in a production scenario, such as organisations and storage.

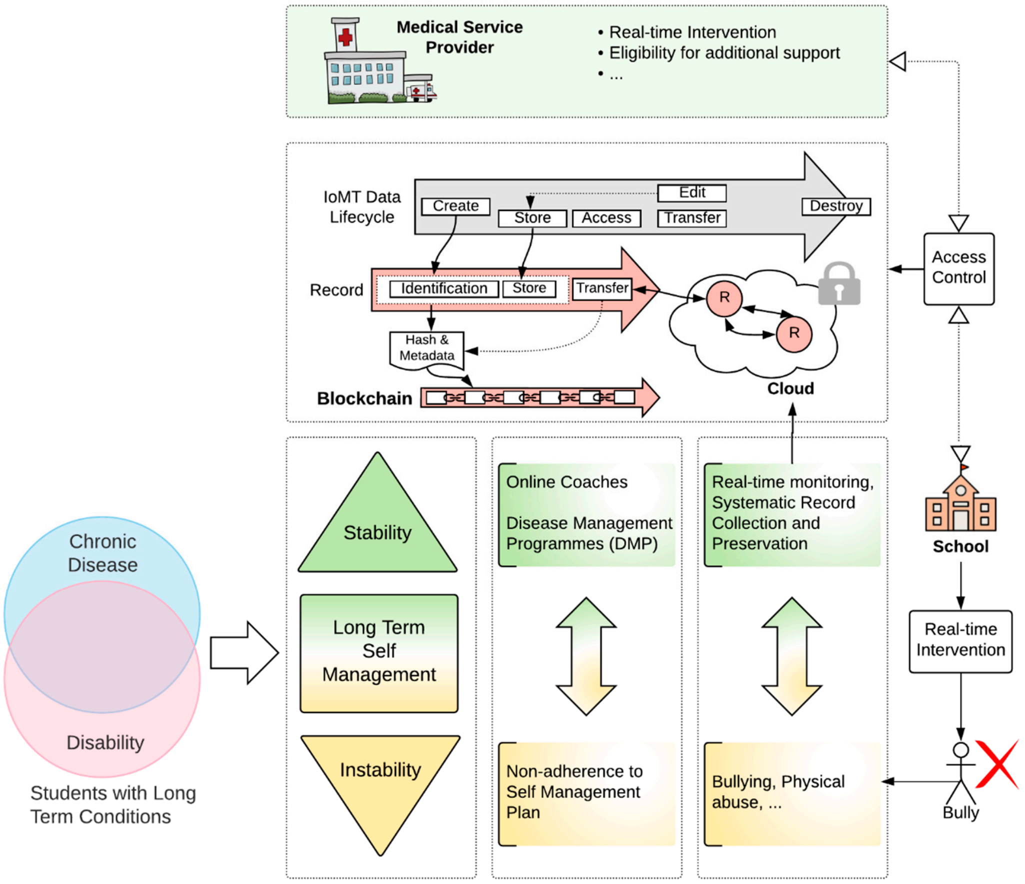

Figure 2. Real-time analysis of IoMT data to monitor the well-being of patients is extended to facilitate on-campus intervention by schools against physical abuse. The model can be generalised to other stakeholders if they joined the private permissioned blockchain.

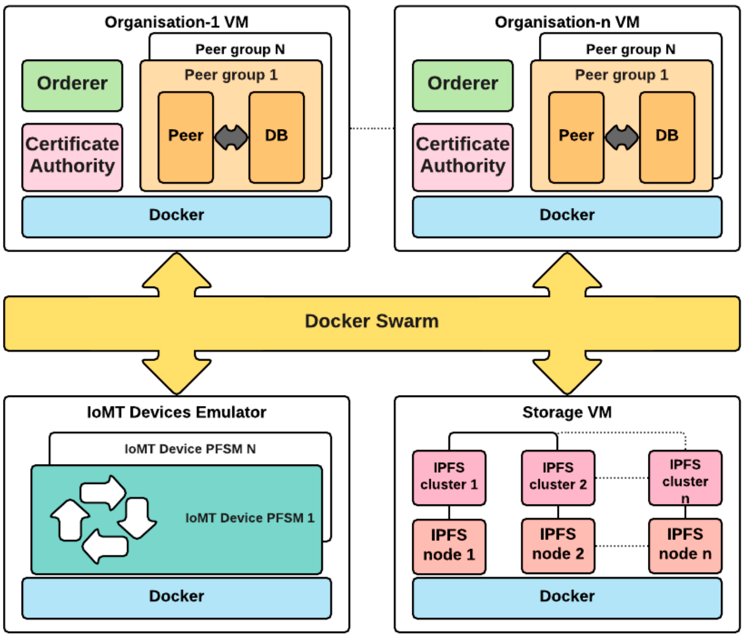

Figure 3. The architecture of the IoMT emulator.

The description starts with the introduction of an abstract model of IoMT sensors based on the elementary interactions performed on the blockchain platform and modelled through a probabilistic finite-state machine (PFSM). This model provides the opportunity to define a test environment as close as possible to a real scenario without the need to introduce unnecessary complexities, which are not relevant in the performance evaluation of the platform itself. In the corresponding virtual machine (VM), the emulator spawns several entities that access the blockchain platform, each of which can have independent and unique behaviour according to its status and functionalities. At the same time, the impact on the platform is continuously monitored to discover and measure possible constraints and bottlenecks of the system.

One or more VMs contain the organisations that participate in the blockchain. Each organisation includes a CA (certificate authority) server that manages the certificates and credentials regulating the access to the blockchain. The peers have distributed replicas of the ledger, being the sources and the destinations of all transactions. The choice of the number of peers is influenced by many factors, including the need to provide high availability and data distribution to reduce access latency. It is not unusual for an organisation to have multiple peers distributed across different geographic areas. Each peer is associated with a support database, which contains the last value for each key entered and updated by the transactions, hence the name "world state database." Its presence is crucial for the performance of the system: Access to the last state of an asset (for example, the last version of the patient's health record) becomes immediate without having to traverse all the blocks of the chain. Finally, each organisation also contains an orderer node that participates in a Raft cluster. Orderers are the key players in the consensus mechanism, as they reach an agreement on validating the new block of transactions added to the ledger.

Although it is possible to save patients' information directly in the transaction payload, this possibility must be evaluated by considering the data size and rate. All the data stored in the transactions will be replicated on each peer and cannot be removed, directly resulting from the immutability property of the blockchain. To tackle this scalability issue, we considered the solution of storing data off-chain in additional VM storage, which contains a network of nodes implementing an InterPlanetary File System (IPFS). IPFS is a protocol very often associated with the blockchain, as it shares its distributed nature. Furthermore, in IPFS the address of a document coincides with the hash of its content, avoiding unnecessary storage of future identical files and at the same time, reducing the space required in the case of files with common sub-parts. Such a hash is then stored in a blockchain transaction, inheriting its properties of immutability and integrity. In our approach, the storage is composed of a configurable number of IPFS nodes, each one connected to a cluster service to provide a fail-safe environment by guaranteeing a minimum number of replicas. Access to IPFS functionalities is implemented via RESTful Application Programming Interfaces (APIs), which are exported by the nodes themselves.

4. Integration of Blockchain Types and Associated Consensus Mechanisms in IoMT

Blockchains consist of multiple blocks containing transactions records strung together. The four requirements for adding a block are (i) it must be a transaction, (ii) it must be verified, (iii) it must be stored, and (iv) it must receive a hash. For a more detailed classification, a blockchain requires a distributed ledger, a consensus mechanism, and associated cryptographic means [44].

A distributed ledger is a consensually shared database synchronised across multiple nodes that allows transactions to have public witnesses [45]. To that aspect, all nodes are permitted to retrieve and store a copy of the recorded transactions. Once added to the ledger, data cannot be removed or edited. To achieve a consensus regarding a transaction's legitimacy, the nodes must adhere to a predefined mechanism protocol. Without consensus, all stored transaction blocks are at risk of various attacks known as Byzantine manners [46].

Public or permissionless blockchains, such as those used for Bitcoin [47] and Ethereum [48] algorithms, hold the transactions' information in the public domain and can be read and contributed to without requiring permission. They are decentralised, immutable, accessible to all, and no individual participant can control the network. In such a system, medical data, including treatment and institutional costs, once validated, could be inserted by professionals and patients, making them transparent. In an open public blockchain, the more popular the network is, the more time a transaction will require to be validated. As new transactions entries would require a consensus from all the nodes' multiple transactions would clog the network. Lastly, consensus mechanisms running on public open blockchain networks such as Proof-of-Work (PoW), Proof-of-Authority (PoAu), ByzCoin, Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), Leased Proof-of-Stake (LPoS), Casper, Proof-of-Burn (PoB), Elastico, and OmniLedger consume considerable amounts of electricity. Such drawbacks mean that open public blockchains in their current state cannot compete with traditional systems [49].

Alternatively, in a private or permissioned blockchain, based on Practical Byzantine Fault Tolerance (PBFT), Delegated Practical Byzantine Fault Tolerance (DPBFT), Proof-of-Elapsed-Time (PoET), RSCoin, Tendermint, Pore, or Raft consensus protocols, membership is by invitation only. A single entity and the participants governing it require permission to read, contribute to, or audit its multiple layers of often confidential information, some of which requires higher levels of security and privacy that can only be accessed by authorised parties. They are also highly scalable, and since only a few nodes are capable of managing data, the network can process more transactions more quickly than a public blockchain. These characteristics of private blockchain platforms make them optimal for an IoMT network [49]. Due to the sensitivity and the size of data, privacy, trust, speed, and scalability are key criteria that are better met by the private blockchain [50]. However, its disadvantages are that (i) being private makes it centralised, (ii) trust becomes an important issue since transactions cannot be independently validated, and (iii) its security is compromised since its fewer nodes make it easier to exploit. The right selection of consensus mechanisms addresses these disadvantages. Both public and private blockchains are competitors. However, there is plenty of room for them both to be developed, as they each have their individual advantages. Indeed, creating a hybrid network based on either Ripple or Aergo consensus protocols could be a viable solution for a decentralised structure with centralised elements. There are numerous benefits of using a hybrid blockchain as it combines a private blockchain speed of generating the transactions' hash combined with the verification security procedure benefits provided by the public blockchain [51].

The consensus mechanisms define the verification process, validation time, processing cost, and thus, the security and efficiency of the network [52]. Four main categories of consensus mechanisms can be discriminated based on their characteristics, i.e., (i) PoW, (ii) PoS, (iii) a hybrid that is a combination of both PoW and PoS, and (iv) Byzantine Fault Tolerance. Table 1 presents a comparison of the consensus mechanisms, evaluating specific performance parameters.

The Proof-of-Work (PoW) is the most popular resource-intensive consensus protocol and requires great computation power and advanced hardware for the fastest node to solve complex computational algorithms and be selected to validate and generate a new block (mining process) [53]. Similar to the PoW mechanism is the Proof-of-Capacity (PoC), which allows nodes to use the available hard drive space instead of the device's computing processing power. The disadvantages, though, include lower adoption rates and possible malware, which may affect the mining process. Both PoW and PoC protocols are susceptible to scalability issues [54].

Table 1. Comparison of consensus mechanisms [46,54–56].

Consensus Mechanisms	Network Type	Decentralisation	Scalability	Throughput	Latency	Tolerance	Power Consumption	Network Resources	Storage Resources	Consensus Type
PoW	Public	High	High	Low	High	Low	High	Low	High	Competitive
PoC	Public	High	High	Low	High	N/A	Low	Low	Very High	Collaborative
PoET	Both	Med	High	High	Low	N/A	Low	Low	High	Competitive
PoS	Both	High	High	Low	Med	High	Med	Low	High	Competitive
DPoS	Public	Med	High	High	Med	High	Med	N/A	High	Collaborative
DPoW	Public	High	High	Low	High	High	Med	N/A	High	Collaborative
PoR	Private	High	High	N/A	High	High	Low	Low	Low	Collaborative
LPoS	Public	High	High	Low	Med	High	Med	Low	High	Competitive
PoI	Public	High	High	High	Med	High	Low	Low	High	N/A
PoA	Public	High	High	Low	Med	High	High	Low	High	Collaborative
Casper	Public	High	High	Med	Med	High	Med	Low	High	N/A
PoB	Public	High	High	Low	High	Low	Med	Low	High	N/A
PBFT	Private	Med	Low	High	Low	Med	Low	High	High	N/A
DPBFT	Private	Med	High	High	Med	Med	Low	High	High	N/A
Stellar	Public	High	High	High	Med	Variable	Low	Med	High	N/A
Ripple	Public	High	High	High	Med	Low	Low	Med	High	N/A
Tendermint	Private	Med	High	High	Low	Med	Low	High	High	N/A
ByzCoin	Public	High	High	High	Med	Med	High	Med	High	N/A
Algorand	Public	High	High	Med	Med	Med	Low	High	High	N/A
Dfinity	Both	High	High	N/A	Med	N/A	Low	N/A	N/A	N/A
RSCoin	Private	Low	High	High	Low	N/A	Low	Med	High	N/A
Elastico	Public	High	High	Low	High	Low	Med	High	High	N/A
OmniLedger	Public	High	High	High	Med	Low	Med	Med	Low	N/A
RapidChain	Public	High	High	High	Med	Med	Med	Low	Low	N/A
Raft	Private	Med	High	High	Low	High	Low	N/A	High	N/A
Tangle	Public	Med	High	High	Low	Med	Low	Low	Low	N/A
Pore	Private	Low	High	N/A	Low	N/A	N/A	N/A	N/A	Collaborative

As a solution, PoS is more environmentally friendly and does not require computational power as it chooses a node to be the validator based on a pseudo-random selection process. However, to commit to the process, nodes must stake their own coins [57]. In addition, although it eliminates the excessive PoW computational requirement, the blockchain becomes centralised because of its dependence on nodes with the highest amount of stake. The DPoS protocol is more efficient, faster, and democratic than PoS, as the generation and validation of new blocks is based on a voting system among a team of elected delegates. The voting power of each node increases based on the number of coins it holds, which makes it more centralised but also more scalable as it can process more transactions per second (Tps) than PoW and PoS. More variations of the PoS that partially solve the centralisation problem are the LPoS and the Proof-of-Importance (PoI). LPoS allows wealthy nodes to lease funds to low balance nodes, thereby increasing their selection chances to verify transactions [54]. In the PoI the node's reputation is also taken into account in the selection process.

The PBFT protocol, based on a voting consensus approach for validating transactions, assumes nodes are authenticated, thereby improving robustness and performance. However, it is beneficial only for small consensus groups since the scale of transactions is large and outcomes are few. PBFT has been used in IoMT for sharing clinical data between healthcare providers [58] because it can provide integrity and value of the collected data from the vital sensors and monitors, and assurance and transparency of the data management [59].

The consensus mechanism that was selected to achieve the necessary agreement among the distributed processes was the Raft. It was chosen because it has PBFT characteristics, is designed for a private blockchain network, has been proven to be safe, and is a modern, reliable, and relatively less complicated distributed consensus algorithm. The nodes fall into three categories: (i) leader, (ii) follower, and (iii) candidate (see Figure 4). The "leader" is responsible for validating transactions, monitoring and controlling the log replications on the cluster's servers, deciding on new entries' placements, and assuring data flow between all servers without needing to consult any of them. If a malfunction is spotted on the leader's activities, then a new leader is elected. The "follower" servers, whose responsibilities up to that moment are to sync up their copies of data with the leader's data at regular time intervals [60], become candidates if they cannot establish communication with the leader for a specific period—called an election timeout. A leader election then begins. The candidate server increases the term counter by voting for itself to become a new leader. It will also send a message to all other servers canvassing their votes; it must be stated that any node in the cluster can become a leader. The candidate gets defeated when it receives a message with a term number equal to or bigger than its current term. In that case, it becomes a follower. The candidate receiving the most votes becomes the leader. If there is a split vote, a new term must start, and a new election takes place. The democratic voting system for electing a new leader and the operational sustainability can remain operational even if a minority of servers, i.e., two out of five, fail. The high performance and the low latency characteristics were also considered for selecting this consensus mechanism protocol to run our IoMT dedicated emulator.

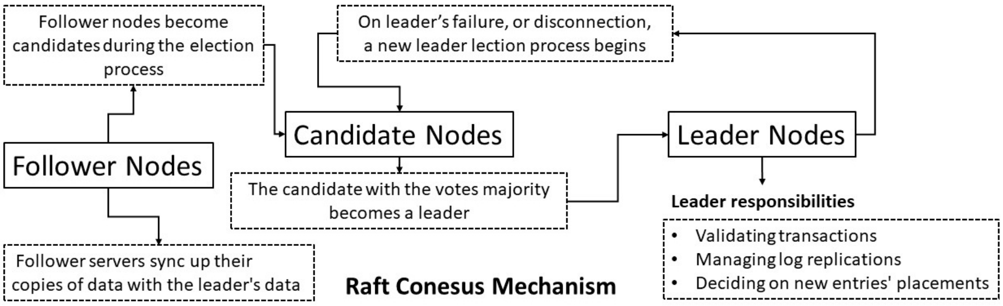
Follower nodes become candidates during the election process
On leader's failure, or disconnection, a new leader lection process begins
Candidate Nodes
Leader Nodes
Follower Nodes
The candidate with the votes majority becomes a leader
Leader responsibilities
• Validating transactions
• Managing log replications
• Deciding on new entries' placements
Follower servers sync up their copies of data with the leader's data
Raft Conesus Mechanism

Figure 4. Structure of the Raft consensus mechanism.

5. Experiments

An extensive series of experiments was conducted to analyse the feasibility and performance of the proposed architecture. The choice of the specific blockchain implementation was made according to the maturity and modularity levels of the solution. Hyperledger Fabric [61] was demonstrated to be the best option, considering the expressiveness of its smart contracts, created with GOLang and Javascript programming languages, and the availability of ready-made and tested side projects that significantly extend its functionalities.

The evaluation metrics that were used during the tests were the transaction latency, Central Processing Unit (CPU) utilisation, memory consumption, and disk throughput. These metrics were analysed based on three different directions: the rate at which transactions were accessed, the size of the corresponding payloads, and finally, the specific type of access. To monitor these Key Performance Indicators (KPIs), we introduced a separate virtual machine hosting a tool called Hyperledger Explorer. The latter provided a web frontend and a layer of APIs to consult the blockchain platform. More specifically, these APIs were used to monitor the status of the system and the system's nodes, to inspect the transactions' contents, and to provide coarse indicators, as the number of transactions and blocks per hour. More accurate data was provided by a second tool, named Hyperledger Caliper, which was used to monitor all containers deployed in our testbed. During its execution, Hyperledger Caliper spawned a predefined number of client components, written in Javascript, which connected to the blockchain platform, invoking the smart contracts through a callback mechanism.

5.1. Archetypes of Data-Aware Smart Contracts and PFSM Composition

In its standard implementation, Hyperledger Caliper is only able to invoke a single smart contract in each test. Although this procedure is simple and effective, it is not sufficient for the evaluation of real scenarios, where the interaction between an IoMT sensor and the blockchain involves the invocation of multiple smart contracts. To obtain results that can be generalised to different contexts, we first categorised the fundamental read–write interactions between IoMT sensors and the blockchain platform, and we developed them in the form of smart contracts:

- The smart contracts *writeOnchainData* and *readOnchainData* store and retrieve data directly to and from the transactions saved in the blockchain. The data size must be limited as these payloads can never be removed and are automatically replicated in all peers. Possible examples are sensors that store the acquired values with low frequency and small payloads, such as humidity sensors.
- The smart contracts *writeOnchainBatch* and *readOnchainBatch* manage batch data, directly saved inside a single blockchain's transaction. Typical examples are time series. Batch operations avoid the generation of various transactions and the corresponding number of consensus agreements.
- The smart contracts *writeOffchainData* and *readOffchainData* store and retrieve files and big data to and from off-chain storage. The writing process starts with the upload to the IPFS endpoint and the creation of a blockchain transaction that includes the obtained hash value and eventual metadata. On the other hand, the reading process begins by reading the blockchain hash, which is used as the file path for the download by the storage service.

To properly model the complex interaction between IoMT devices and the blockchain's smart contracts, we extensively used PFSMs. The latter was composed of a set of transitions, each one starting from and ending with a state with a specific probability of occurring. Each transition was bound to a smart contract that was executed at the same time the transition was fired. The probability of making a transition allowed the closer approximation of devices' logic, distinguishing between standard and special operations. Furthermore, smart contracts' parameters, such as the size of the payload or the batch length, could be configured independently in each step of the machine, aiming for even more accurate modelling. Figure 5. A possible representation of IoMT device iStress using a PFSM presents a possible representation of the stress-detection device named iStress proposed in ref. [62] using a PFSM: The operation of the device was considered as the continuous iteration of the diagram shown. In the start node, it was very likely (p = 0.90) that the data from the three primary sensors were read, namely the accelerometer, the humidity, and the temperature sensors. Each of these reads invocated the *writeOnchainData* smart contract, which saved the values in the blockchain. Furthermore, it was possible to execute an empty transaction (with probability p = 0.10) that simulated the unavailability of new data from those sensors. In the "Stress Analysis and Detection Unit" node, data analysis took place, which included a variable number of readings (smart contract *readOnchainBatch* with p = 0.45) and the following choice of one of the three possible outcomes: "Low Stress," "Normal Stress," or "High Stress." Each of these was written on the blockchain via the *writeOnchainData* smart contract. We deliberately assigned a low incidence to the "High Stress" outcome (p = 0.05), however, due to its severity, it was likely to generate an event outside the system, for example to the healthcare facility, which was simulated through the *writeOffchainData* smart contract.

Our testbed allowed for the definition of multiple PFSMs, each one representing a device or a class of sensors interacting with the blockchain platform. In doing so, an architect could recreate various scenarios, thus evaluating and predicting the impact of IoMT sensors on the blockchain even before the availability of physical devices. The emulation process led to a two-fold benefit: Firstly, by knowing the characteristics of an existing blockchain infrastructure, it was possible to estimate the number of devices that could be connected while maintaining the minimum quality of service, as in the case of maximum transaction latency. Secondly, by knowing the amount and type of devices and the expected number of patients, it was possible to predict the computational resources that should be acquired, either on-premises or in the cloud, as a part of a feasibility analysis and the estimation of the implementation costs.

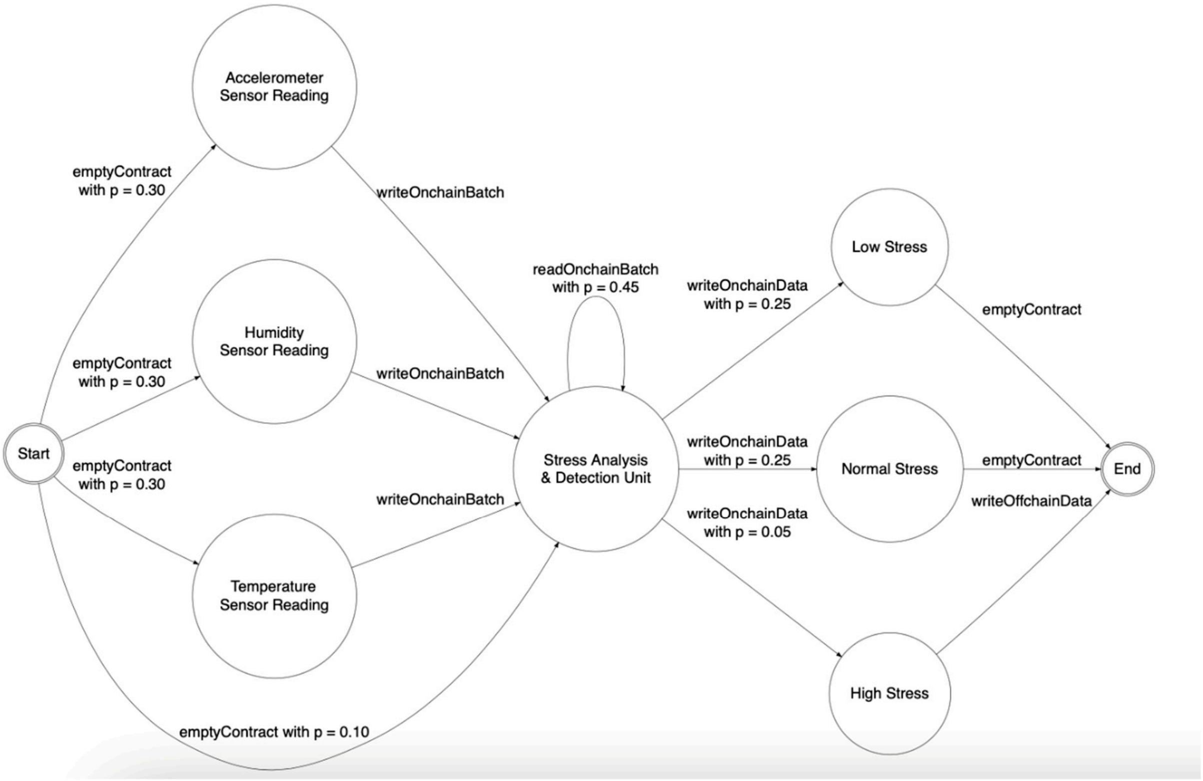
Accelerometer Sensor Reading
emptyContract with p = 0.30
writeOnchainBatch
Humidity Sensor Reading
emptyContract with p = 0.30
writeOnchainBatch
Start
emptyContract with p = 0.30
writeOnchainBatch
Temperature Sensor Reading
emptyContract with p = 0.10
readOnchainBatch with p = 0.45
Stress Analysis & Detection Unit
writeOnchainData with p = 0.25
writeOnchainData with p = 0.25
writeOnchainData with p = 0.05
Low Stress
Normal Stress
High Stress
emptyContract
emptyContract
writeOffchainData
End

Figure 5. A possible representation of IoMT device iStress using a Probabilistic Finite Sate Machines (PFSM).

5.2. Experiment Procedure

Figure 6 shows the flow chart representing the procedure used during the experiments. For each smart contract archetype, an independent testbed environment was allocated, each one having the same hardware characteristics and computational resources. In this environment, the Hyperledger Explorer and Hyperledger Caliper tools were used to monitor the KPIs. Furthermore, in each test, Hyperledger Caliper was associated with a bespoke callback module for interacting with the specific contract in the blockchain.

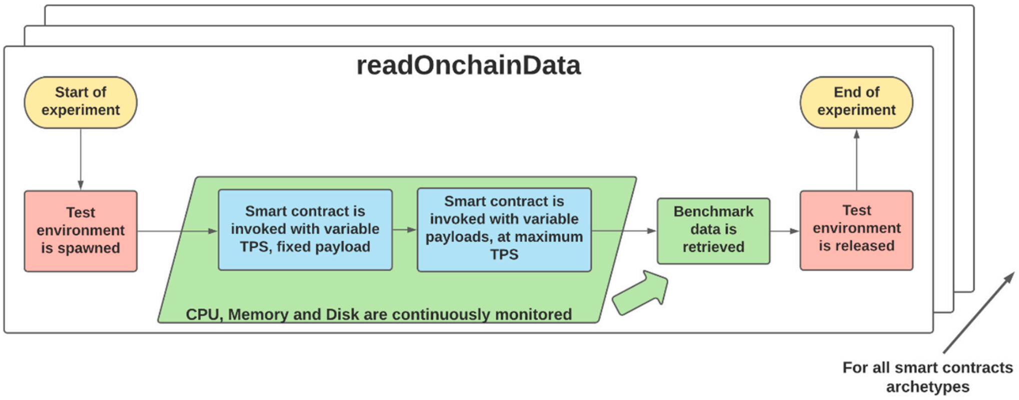
readOnchainData
Start of experiment
Test environment is spawned
Smart contract is invoked with variable TPS, fixed payload
Smart contract is invoked with variable payloads, at maximum TPS
CPU, Memory and Disk are continuously monitored
Benchmark data is retrieved
Test environment is released
End of experiment
For all smart contracts archetypes

Figure 6. The procedure used during the experiments, executed for each smart contract archetype.

In the first phase of the experiments, a smart contract at increasing frequencies (Transaction per second or Tps) was invoked with a fixed payload in order to analyse the latency. The latency measurement included the time needed for the transfer of the payload between the various nodes of the network, the duration of the chosen consensus method, and the creation time of a new block that would contain the transaction itself. The reciprocal of the minimum latency was the maximum frequency with which transactions could be created in the system and determined an upper bound of the rate of interactions between the IoMT sensors and the blockchain. In the second phase, the same smart contract was invoked under different payload sizes to investigate the corresponding maximum achievable frequency of invocation. These sizes were powers of two, from 256 to 32,768 bytes for on-chain operations and above that limit for the off-chain storage. The maximum Tps was determined by a fixed-length backlog-based technique, where the smart contract was invoked only if the backlog had a free slot. When the smart contract was fired, the call was inserted in the backlog and removed as soon as the transaction was completed. If the backlog was full, no new smart contract was executed until an ongoing one was completed. In this way, the emulated device could dynamically adapt its data rate to the instantaneous workload of the blockchain.

For the entire duration of the experiment, the environment was continuously monitored in order to collect detailed information regarding CPU utilisation, memory consumption, and disk throughput. This information was retrieved directly from each component of the architecture, namely, the peers (Pe), the databases (Db), the orderers (Or), the off-chain storage (St), and the certificate authority (CA). By doing so, the components and the subsystems more likely to limit the scalability of our proposed solution get identified.

6. Results and Discussion

The results in this section emerged from a case study including two organisations. The testbed included virtual machines hosted in Amazon AWS EC2 (Amazon, Seattle, WA, USA), each equipped with 2 vCPU, 8 Gb of RAM, and 30 Gb of Solid-State Drive (SSD) storage. Tests lasted 120 s, during which the performance of system components was monitored.

The maximum rate of transaction creation (transactions per second, or Tps), although dependant on payload's size, was 120, which constituted the upper limit in rate-related tests. Figure 7 shows the results of the test for writeOnchainData as an example. Moreover, since the absolute performances were correlated to the specific hardware infrastructure, we opted for the normalisation of the worst-condition results (i.e., 32,768-byte payload and 120 Tps) with the ones corresponding to the most favourable conditions (i.e., 256-byte payload and 10 Tps). Figure 8 illustrates which resources were more influenced and could become potential bottlenecks of the system. Similar plots were produced for all other smart contracts as well.

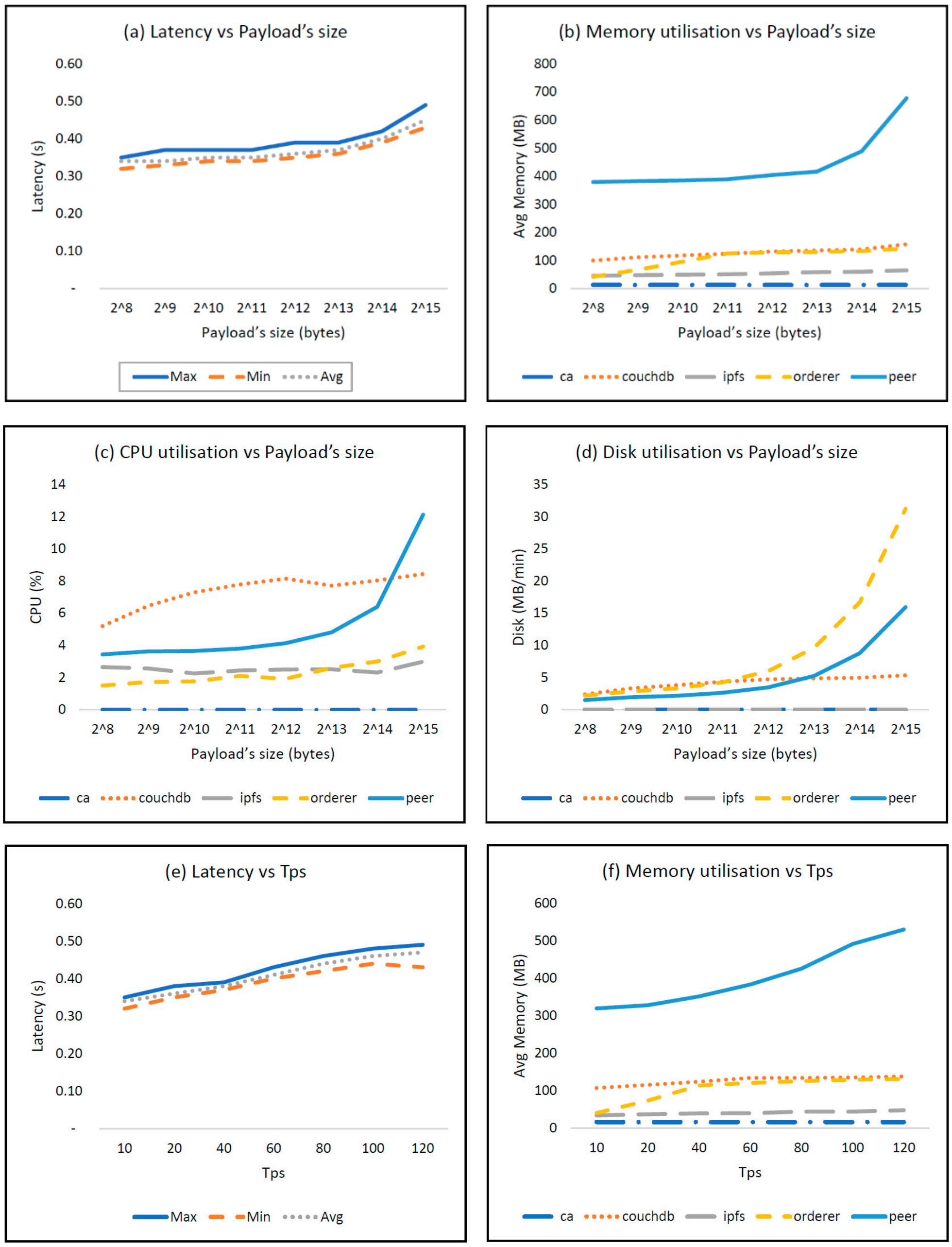

Figure 7. *Cont.*

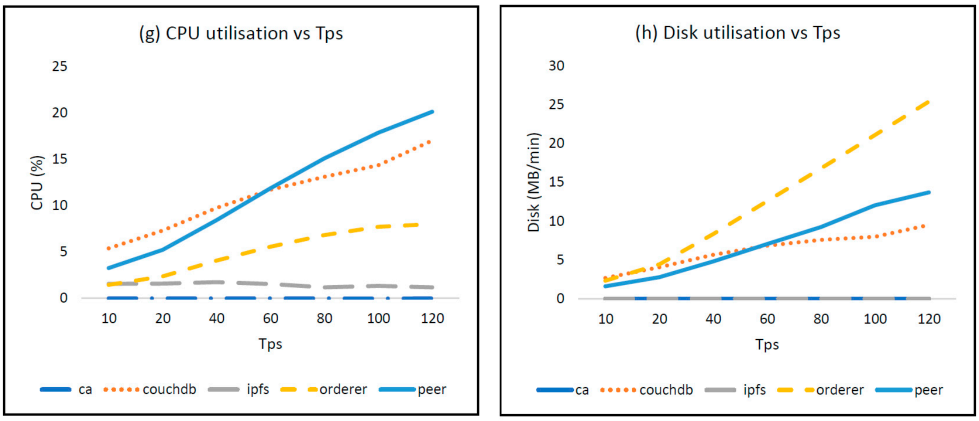

Figure 7. Analysis of *writeOnchainData* with different payload sizes and transactions/sec. (**a**) Latency vs. Payload's size; (**b**) Memory utilisation vs. Payload's size; (**c**) CPU utilisation vs. Payload's size; (**d**) Disk utilisation vs. Payload's size; (**e**) Latency vs. Tps; (**f**) Memory utilisation vs. Tps; (**g**) CPU utilisation vs. Tps; (**h**) Disk utilisation vs. Tps.

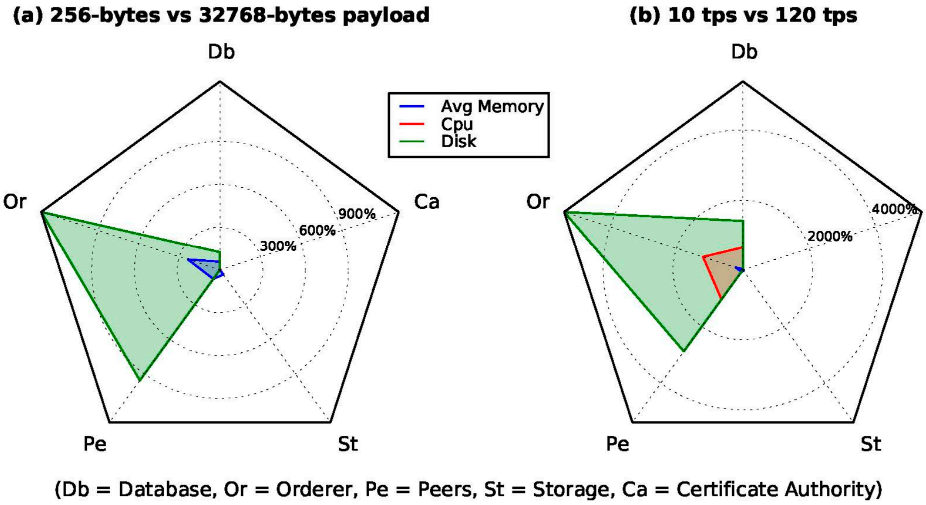

Figure 8. Impact of the smart contract *writeOnchainData* with bigger payload (**a**) and higher Tps (**b**).

According to Figure 7a,e, the time required for the transaction's creation grew slightly with larger data sizes and faster invocations but always remained under 1 s. Considering that the payload doubled in each test, the apparent exponential behaviour of peers' memory, CPU, and disk utilisation increased linearly. An interesting observation arises by comparing peers with the underlying world state databases (CouchDB). At first sight, they should have been subjected to the same load, since the increasing payloads were equally stored in both components. Nonetheless, memory and disk utilisations were lower in databases, as a consequence of the inner compression method applied by the latter, which was also confirmed by the CPU usage. By disabling compression or by providing high-entropy payloads that can be hardly compressed, peers and databases showed similar resource usage. Orderer disk utilisation was also significant, as illustrated in Figure 8a,b, where the disk subsystems emerged as the components most directly affected by the increase in both data size and data rate.

The tests carried out on the *readOnchainData* smart contract showed that the average latency was stable at 0.01 s for all the payload's sizes and Tps. Nonetheless, as the payload's size increased, more orderer memory was used, concurrent with a slight increase in database CPU utilisation, plausibly due to data decompression. On the other hand, by increasing Tps, only peer CPU utilisation was affected, due to the higher number of smart contract invocations. Reading the data from the transactions was therefore a very efficient action because the consensus was avoided by querying the peer directly. Furthermore, it was possible to force the execution of the consensus method, giving the possibility to isolate the delay introduced by the consensus. The results in Table 2. Latency of readOnchainData with *consensus* enabled suggest that the Raft-based consensus's overhead was approximately 0.30 s.

Table 2. Latency of *readOnchainData* with consensus enabled.

Tps	Max Latency (s)	Min Latency (s)	Avg Latency (s)
10	0.33	0.30	0.32
20	0.33	0.31	0.32
40	0.34	0.32	0.33
60	0.35	0.33	0.34
80	0.37	0.35	0.36
100	0.38	0.35	0.37

The *writeOnchainBatch* smart contract was tested to assess its limits. Considering a batch of fixed length equal to 10 elements, the maximum size of each element was 8192 bytes, for a total payload of 80 kbytes. Beyond this size, transactions were not completed fast enough to sustain the desired 10 Tps. The most utilised component was the orderer for both memories used and disk access, followed by CPU usage of the peers. Considering a fixed batch of 10 elements of 256 bytes each, the maximum invocation frequency was 53 Tps, which emerged from the use of the backlog. Finally, considering a 256-byte payload, a maximum batch length of 75 was reached before the resulting latency prevented a stable rate of 10 Tps. This limitation was imposed by the orderer's memory and disk usage. However, this approach allowed the writing of 750 items per second, well above the 114 maximum achievable with *writeOnchainData*. The smart contract *readOnchainBatch* proved to be efficient and fast in all configurations at the expense of a slight increase in memory and CPU usage due to the larger transactions executed.

In the last part of our experiments, we analysed the impact of the off-chain storage, namely, the smart contracts *writeOffchainData* and *readOffchainData*, with increasing file-size (from 256 kb to 10 mb). During the writing phase, the file was transmitted to the IPFS service directly; then its hash was stored in a transaction using *writeOnchainData*. On the contrary, the reading phase included the invocation of *readOnchainData* in order to retrieve the hash used as a file anchor in the off-chain file download. In both cases, the latency was almost linear with the file size, with a maximum rate of 100 files per second in the smallest configuration. Access to the blockchain has proven to be much faster than the corresponding access to IPFS storage, whose performances were closely linked to the slowness of the disk subsystem.

7. Conclusions

Bullying among school children is not a new phenomenon. Recent statistics have proven that there is a growth rate year by year, impacting mainly the most vulnerable students, especially those with chronic physical illness or disabilities. Unfortunately, there is not an obvious bridge between well-being programs and academic outcomes. Hence, although there are several components and various programs available in schools that may positively influence children's well-being, there is little evidence to suggest that an integrated program exists that can detect stress and incidents of victimisation among students in real time.

In this study, we proposed a private permission blockchain platform to enable real-time intervention triggered by IoMT data that could be collected by mobile wearable sensors already attached to students due to chronic conditions. Given the unavailability of physical devices, the performance and capabilities of the proposed platform were evaluated and demonstrated with the use of an emulator under different loads of sensor-generated data. With this testbed, we investigated the impact of IoMT sensors on the blockchain platform based on two main criteria: the transaction latency and the computational resources. The results proved that the interaction between the sensors and the blockchain can be limited by the access modes deployed. This could have a detrimental effect on the sizing of the various entities and components within an IoMT architecture. Additionally, the rate at which the information was generated and exchanged between nodes proved to be a crucial factor in the performance of a highly distributed platform governed by a consensus algorithm.

Future analysis will investigate additional attributes and parameters for sensors in Industrial Internet of Things (IIoT) deployments to enrich the emulator's existing capabilities. Additionally, we are planning to develop a user-centric approach by designing a user interface-based use case usability study.

Author Contributions: Conceptualization, N.E., H.A.-K. and G.E.; Data curation, N.E. and M.B.; Formal analysis, N.E. and M.B.; Investigation, H.A.-K. and Z.A.; Methodology, N.E., M.B. and A.A.; Validation, G.E., P.P.; Visualization, N.E., H.A.-K. and G.E.; Writing—original draft, N.E., H.A.-K. and Z.A.; Writing—review & editing, P.P. and A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Innovate UK, grant number 133891.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bonell, C.; Humphrey, N.; Fletcher, A.; Moore, L.; Anderson, R.; Campbell, R. Why schools should promote students' health and wellbeing. *BMJ* **2014**, *348*, g3078. [CrossRef] [PubMed]
2. Long, R.; Roberts, N.; Loft, P. *Bullying in UK Schools*; House of Commons Library: London, UK, 2020.
3. Alhaboby, Z.A.; Barnes, J.; Evans, H.; Short, E. Cyber Victimisation of People with Chronic Conditions and Disabilities: A Systematic Review of Scope and Impact. *Trauma Violence Abus.* **2017**, *3*, 398–415.
4. Gibson-Young, L.; Martinasek, M.P.; Clutter, M.; Forrest, J. Are students with asthma at increased risk for being a victim of bullying in school or cyberspace? Findings from the 2011 Florida youth risk behavior survey. *J. Sch. Health* **2014**, *84*, 429–434. [CrossRef] [PubMed]
5. Hamiwka, L.D.; Cara, G.Y.; Hamiwka, L.A.; Sherman, E.M.; Anderson, B.; Wirrell, E. Are children with epilepsy at greater risk for bullying than their peers? *Epilepsy Behav.* **2009**, *15*, 500–505. [CrossRef]
6. Sentenac, M.; Gavin, A.; Arnaud, C.; Molcho, M.; Godeau, E.; Gabhainn, S.N. Victims of bullying among students with a disability or chronic illness and their peers: A cross-national study between Ireland and France. *J. Adolesc. Health* **2011**, *48*, 461–466. [CrossRef]
7. Menesini, E.; Salmivalli, C. Bullying in schools: The state of knowledge and effective interventions. *Psychol. Health Med.* **2017**, *22*, 240–253. [CrossRef]
8. Jadambaa, A.; Thomas, H.J.; Scott, J.G.; Graves, N.; Brain, D.; Pacella, R. Prevalence of traditional bullying and cyberbullying among children and adolescents in Australia: A systematic review and meta-analysis. *Aust. N. Z. J. Psychiatry* **2019**, *53*, 878–888. [CrossRef]
9. Hicks, J.; Jennings, L.; Jennings, S.; Berry, S.; Green, D.-A. Middle School Bullying: Student Reported Perceptions and Prevalence. *J. Child Adolesc. Couns.* **2018**, *4*, 195–208. [CrossRef]
10. Han, Z.; Zhang, G.; Zhang, H. School Bullying in Urban China: Prevalence and Correlation with School Climate. *Int. J. Environ. Res. Public Health* **2017**, *14*, 1116. [CrossRef]
11. Kowalski, R.M.; Giumetti, G.W.; Schroeder, A.N.; Lattanner, M.R. Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychol. Bull.* **2014**, *140*, 1073. [CrossRef]
12. Didden, R.; Scholte, R.H.J.; Korzilius, H.; de Moor, J.M.; Vermeulen, A.; O'Reilly, M.; Lang, R.; Lancioni, G.E. Cyberbullying among students with intellectual and developmental disability in special education settings. *Dev. Neurorehabilit.* **2009**, *12*, 146–151. [CrossRef] [PubMed]
13. Annerbäck, E.-M.; Sahlqvist, L.; Wingren, G. A cross-sectional study of victimisation of bullying among schoolchildren in Sweden: Background factors and self-reported health complaints. *Scand. J. Public Health* **2014**, *42*, 270–277. [CrossRef] [PubMed]
14. Zych, I.; Ortega-Ruiz, R.; Del Rey, R. Systematic review of theoretical studies on bullying and cyberbullying: Facts, knowledge, prevention, and intervention. *Aggress. Violent Behav.* **2015**, *23*, 21. [CrossRef]
15. Alhaboby, Z.A.; Evans, H.; Barnes, J.; Short, E. Disability and Cyber-Victimisation. In *The Image of Disability: Essays on Media Representations*; Schatz, A.E.G.J., Ed.; McFarland Press: Jefferson, NC, USA, 2017; pp. 167–180.

16. Taylor, L.A.; Saylor, C.; Twyman, K.; Macias, M. Adding insult to injury: Bullying experiences of youth with attention deficit hyperactivity disorder. *Child. Health Care* **2010**, *39*, 59–72. [CrossRef]
17. Chen, P.-Y.; Schwartz, I.S. Bullying and victimization experiences of students with autism spectrum disorders in elementary schools. *Focus Autism Other Dev. Disabil.* **2012**, *27*, 200–212. [CrossRef]
18. Kouwenberg, M.; Rieffe, C.; Theunissen, S.C.P.M.; de Rooij, M. Peer victimization experienced by children and adolescents who are deaf or hard of hearing. *PLoS ONE* **2012**, *7*, e52174. [CrossRef] [PubMed]
19. Zinner, S.H.; Conelea, C.A.; Glew, G.M.; Woods, D.W.; Budman, C.L. Peer victimization in youth with Tourette syndrome and other chronic tic disorders. *Child Psychiatry Hum. Dev.* **2012**, *43*, 124–136. [CrossRef]
20. Horowitz, J.A.; Vessey, J.A.; Carlson, K.L.; Bradley, J.F.; Montoya, C.; McCullough, B.; David, J. Teasing and Bullying Experiences of Middle School Students. *J. Am. Psychiatr. Nurses Assoc.* **2004**, *10*, 165–172. [CrossRef]
21. Kowalski, R.M.; Fedina, C. Cyber bullying in ADHD and Asperger Syndrome populations. *Res. Autism Spectr. Disord.* **2011**, *5*, 1201–1208. [CrossRef]
22. Sentenac, M.; Arnaud, C.; Gavin, A.; Molcho, M.; Gabhainn, S.N.; Godeau, E. Peer victimization among school-aged children with chronic conditions. *Epidemiol. Rev.* **2011**, *34*, 120–128. [CrossRef]
23. Willard, N.E. *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress*; Research Press: Champaign, IL, USA, 2007.
24. Fridh, M.; Lindström, M.; Rosvall, M. Subjective health complaints in adolescent victims of cyber harassment: Moderation through support from parents/friends—A Swedish population-based study. *BMC Public Health* **2015**, *15*, 949. [CrossRef] [PubMed]
25. Fridh, M.; Köhler, M.; Modén, B.; Lindström, M.; Rosvall, M. Subjective health complaints and exposure to peer victimization among disabled and non-disabled adolescents: A population-based study in Sweden. *Scand. J. Public Health* **2017**, *46*, 262–271. [CrossRef] [PubMed]
26. Mateu, A.; Pascual-Sánchez, A.; Martinez-Herves, M.; Hickey, N.; Nicholls, D.; Kramer, T. Cyberbullying and post-traumatic stress symptoms in UK adolescents. *Arch. Dis. Child.* **2020**, *105*, 951–956. [CrossRef] [PubMed]
27. Marciano, L.; Schulz, P.J.; Camerini, A.-L. Cyberbullying Perpetration and Victimization in Youth: A Meta-Analysis of Longitudinal Studies. *J. Comput. Mediat. Commun.* **2020**, *25*, 163–181. [CrossRef]
28. Fridh, M.; Lindström, M.; Rosvall, M. Associations between self-injury and involvement in cyberbullying among mentally distressed adolescents in Scania, Sweden. *Scand. J. Public Health* **2019**, *47*, 190–198. [CrossRef]
29. Bouazizi, A.; Zaibi, G.; Samet, M.; Kachouri, A. Wireless body area network for e-health applications: Overview. In Proceedings of the 2017 International Conference on Smart, Monitored and Controlled Cities (SM2C), Sfax, Tunisia, 17–19 February 2017; pp. 64–68.
30. Al-Khafajiy, M.; Baker, T.; Chalmers, C.; Asim, M.; Kolivand, H.; Fahim, M.; Waraich, A. Remote health monitoring of elderly through wearable sensors. *Multimed. Tools Appl.* **2019**, *78*, 24681–24706. [CrossRef]
31. Shapsough, S.; Hesham, A.; Elkhorazaty, Y.; Zualkernan, I.A.; Aloul, F. Emotion recognition using mobile phones. In Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–16 September 2016; pp. 1–6.
32. Lane, N.D.; Mohammod, M.; Lin, M.; Yang, X.; Lu, H.; Ali, S.; Doryab, A.; Berke, E.; Choudhury, T.; Campbell, A. Bewell: A smartphone application to monitor, model and promote wellbeing. In Proceedings of the 5th international ICST Conference on Pervasive Computing Technologies for Healthcare, Dublin, Ireland, 23–26 May 2011; pp. 23–26.
33. Hicks, J.; Ramanathan, N.; Kim, D.; Monibi, M.; Selsky, J.; Hansen, M.; Estrin, D. AndWellness: An open mobile system for activity and experience sampling. In Proceedings of the Wireless Health 2010, San Diego, CA, USA, 5–7 October 2010; pp. 34–43.
34. Epiphaniou, G.; Daly, H.; Al-Khateeb, H. Blockchain and Healthcare. In *Blockchain and Clinical Trial: Securing Patient Data*; Jahankhani, H., Kendzierskyj, S., Jamal, A., Epiphaniou, G., Al-Khateeb, H., Eds.; Springer International Publishing: Cham, Switzerland, 2019.
35. Ahmadi-Assalemi, G.; Al-Khateeb, H.; Maple, C.; Epiphaniou, G.; Alhaboby, Z.A.; Alkaabi, S.; Alhaboby, D. Digital Twins for Precision Healthcare. In *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*; Jahankhani, H., Kendzierskyj, S., Chelvachandran, N., Ibarra, J., Eds.; Springer International Publishing: Cham, Switzerland, 2020.
36. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *J. Med. Syst.* **2018**, *42*, 130. [CrossRef]
37. Chen, Y.; Ding, S.; Xu, Z.; Zheng, H.; Yang, S. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. *J. Med. Syst.* **2018**, *43*, 5. [CrossRef]
38. Jiang, S.; Cao, J.; Wu, H.; Yang, Y.; Ma, M.; He, J. BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Sicily, Italy, 18–20 June 2018; pp. 49–56.
39. Bocek, T.; Rodrigues, B.B.; Strasser, T.; Stiller, B. Blockchains everywhere—A use-case of blockchains in the pharma supply-chain. In Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017; pp. 772–777.
40. Bryatov, S.R.; Borodinov, A. Blockchain technology in the pharmaceutical supply chain: Researching a business model based on Hyperledger Fabric. In Proceedings of the International Conference on Information Technology and Nanotechnology (ITNT), Samara, Russia, 21–24 May 2019.

41. Siyal, A.A.; Junejo, A.Z.; Zawish, M.; Ahmed, K.; Khalil, A.; Soursou, G. Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives. *Cryptograms* **2019**, *3*, 3. [CrossRef]
42. Maslove, D.M.; Klein, J.; Brohman, K.; Martin, P. Using Blockchain Technology to Manage Clinical Trials Data: A Proof-of-Concept Study. *Jmir Med Inf.* **2018**, *6*, e11949. [CrossRef]
43. Albanese, G.; Calbimonte, J.-P.; Schumacher, M.; Calvaresi, D. Dynamic consent management for clinical trials via private blockchain technology. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 4909–4926. [CrossRef]
44. Ahmadi-Assalemi, G.; Al-Khateeb, H.M.; Epiphaniou, G.; Cosson, J.; Jahankhani, H.; Pillai, P. Federated Blockchain-Based Tracking and Liability Attribution Framework for Employees and Cyber-Physical Objects in a Smart Workplace. In Proceedings of the 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, 16–18 January 2019; pp. 1–9.
45. Epiphaniou, G.; Pillai, P.; Bottarelli, M.; Al-Khateeb, H.; Hammoudesh, M.; Maple, C. Electronic Regulation of Data Sharing and Processing Using Smart Ledger Technologies for Supply-Chain Security. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1059–1073. [CrossRef]
46. Dinh, T.T.A.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.C.; Wang, J. Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 1366–1385. [CrossRef]
47. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://downloads.coindesk.com/research/whitepapers/bitcoin.pdf (accessed on 1 December 2020).
48. Wood, G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Available online: https://gavwood.com/paper.pdf (accessed on 1 December 2020).
49. SelfKey. Understanding Public vs. Private Blockchain. Available online: https://selfkey.org/understanding-public-vs-private-blockchain/ (accessed on 1 December 2020).
50. Liu, J.; Li, X.; Ye, L.; Zhang, H.; Du, X.; Guizani, M. BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Lisbon, Portugal, 9–13 December 2018; pp. 1–6.
51. Gateways, B. Why BC Gateways is Using a Hybrid Blockchain. Available online: https://www.bcgateways.com/post/hybrid-blockchain (accessed on 1 December 2020).
52. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. *IEEE Access* **2019**, *7*, 22328–22370. [CrossRef]
53. Zhang, S.; Lee, J.-H. Analysis of the main consensus protocols of blockchain. *ICT Express* **2020**, *6*, 93–97. [CrossRef]
54. Salimitari, M.; Chatterjee, M. A Survey on Consensus Protocols in Blockchain for IoT Networks. *arXiv* **2018**, arXiv:1805.11390.
55. Chalaemwongwan, N.; Kurutach, W. Notice of Violation of IEEE Publication Principles: State of the art and challenges facing consensus protocols on blockchain. In Proceedings of the 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–12 January 2018; pp. 957–962.
56. Erginbay, U.; Yusuf, M. Blockchain Technology in Solar Energy. In *Architectures and Frameworks for Developing and Applying Blockchain Technology*; Nansi, S., Ed.; IGI Global: Hershey, PA, USA, 2019.
57. Hazari, S.S.; Mahmoud, Q.H. Comparative evaluation of consensus mechanisms in cryptocurrencies. *Internet Technol. Lett.* **2019**, *2*, e100. [CrossRef]
58. Dubovitskaya, A.; Xu, Z.; Ryu, S.; Schumacher, M.; Wang, F. Secure and Trustable Electronic Medical Records Sharing using Blockchain. *AMIA Annu. Symp. Proc.* **2018**, *2017*, 650–659.
59. Peixoto, H.; Guimarães, T.; Santos, M.F. A New Architecture for Intelligent Clinical Decision Support for Intensive Medicine. *Procedia Comput. Sci.* **2020**, *170*, 1035–1040. [CrossRef]
60. Hu, J.; Liu, K. Raft consensus mechanism and the applications. *J. Phys. Conf. Ser.* **2020**, *1544*, 012079. [CrossRef]
61. Li, D.; Wong, W.E.; Guo, J. A Survey on Blockchain for Enterprise Using Hyperledger Fabric and Composer. In Proceedings of the 2019 6th International Conference on Dependable Systems and Their Applications (DSA), Harbin, China, 3–6 January 2020; pp. 71–80.
62. Rachakonda, L.; Sundaravadivel, P.; Mohanty, S.P.; Kougianos, E.; Ganapathiraju, M. A Smart Sensor in the IoMT for Stress Level Detection. In Proceedings of the 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), Hyderabad, India, 17–19 December 2018; pp. 141–145.