future internet

MDPI

Editorial

Special Issue on Security and Privacy in Blockchains and the IoT Volume II

Christoph Stach [1,*] and Clémentine Gritti [2,†]

[1] Institute for Parallel and Distributed Systems, University of Stuttgart, Universitätsstraße 38, 70569 Stuttgart, Germany
[2] Department of Computer Science and Software Engineering, University of Canterbury, Christchurch 8041, New Zealand
* Correspondence: christoph.stach@ipvs.uni-stuttgart.de; Tel.: +49-711-68588-433
† Current address: Digital Security Department, Eurecom, Sophia Antipolis, 06410 Biot, France.

In this day and age, data are indispensable commodities and have become an integral part of our daily lives. In fact, it is no coincidence that data are referred to as the oil of the 21st century, as they are the key drivers for all kinds of smart services: In the private sector, we rely on streaming providers to recommend songs or videos tailored to our preferences. In the healthcare sector, we benefit from the fact that important information, such as emergency data or a medication plan, is automatically registered and merged in an electronic patient file and thereby made immediately available to treating physicians. In manufacturing, predictive maintenance, i.e., the proactive maintenance of machines at an early stage, can minimize downtimes and, thus, delays in the production process. Besides these three examples from the domains of smart homes, smart healthcare, and smart manufacturing, there are countless other smart services in these and virtually any other conceivable domain. Such smart services are enabled primarily by the continuous collection and comprehensive analysis of data.

From a technical point of view, two key requirements have to be addressed: On the one hand, there is a need to capture, quantify, and interconnect a wide range of aspects. This can be achieved by means of the Internet of Things (IoT). Here, physical everyday objects are equipped with sensors and connectivity capabilities. Such objects are usually referred to as smart things. The sensors are able to record data about their environment and map them to a digital twin—a virtual representation of the everyday object they are connected to. For their part, these digital twins can create networks to communicate captured information with their surroundings. On the other hand, it is necessary to make the collected data reliably available to all authorized stakeholders. Distributed ledger technologies (DLTs) enable the management and provisioning of shared data collections in a trusted manner. To this end, there is not a central instance that maintains (and thus controls) the data, but the data are managed in multiple replicas across a distributed network. Here, it is ensured that any changes are always reflected in all copies of the ledger and that all parties involved agree on the currently valid state of the ledger using a consensus mechanism. Blockchain is the most prevalent example of distributed ledger technology, which is why these two terms are often used synonymously.

However, since data are not simply commodities that facilitate and enrich our everyday lives thanks to smart services but also have a high economic value, security aspects must be given special consideration in any activities involving data processing. For instance, it is essential to ensure that access to the collected data can be restricted, that data tampering can be prevented, and that the availability of the data cannot be impaired, e.g., by illegitimate deletion or denial-of-service attacks. These aspects are addressed by the three IT protection goals of 'confidentiality', 'integrity', and 'availability'. In addition to the established CIA triad, consisting of the aforementioned three IT protection goals, the protection goal 'privacy' is assuming an increasingly decisive role nowadays. This special status is due to

check for updates

Citation: Stach, C.; Gritti, C. Special Issue on Security and Privacy in Blockchains and the IoT Volume II. *Future Internet* **2023**, *15*, 272. https://doi.org/10.3390/fi15080272

Received: 5 August 2023
Accepted: 14 August 2023
Published: 16 August 2023

the fact that smart things are ubiquitous in our everyday lives. As a result, more and more sensitive data are being collected and processed, providing comprehensive insights into the personal lives of the data subjects.

In this Special Issue, fourteen research articles and three literature reviews therefore address research questions in the thematic area of security and privacy in blockchains and the IoT, while Volume I [1] addresses general security and privacy aspects in the context of blockchain technologies and the IoT, the focus of Volume II is rather on a holistic understanding that, for instance, takes into account mutual effects between individual protection goals and end-to-end security measures from acquisition to provisioning. The seventeen papers in Volume II are outlined in the following.

Articles. In the opening research article, Stach [2] highlights the similarities and differences between physical goods, such as oil, and virtual goods, such as data, in terms of handling and processing. Here, it becomes apparent that raw data, just like crude oil, needs to be refined in order to be useful. Therefore, an end-to-end data platform called REFINERY Platform is designed to enable effective and efficient data handling. The work focuses on the special characteristics of data and their implications for modern data management, covering challenges in data acquisition, refinement, storage, and delivery. In data processing, specific attention is paid to protection goals such as confidentiality, integrity, availability, and authenticity, as well as compliance with data protection laws such as the European General Data Protection Regulation (GDPR). In this way, the REFINERY Platform represents an information retrieval and provision platform that enables data to be handled in a trustworthy manner. Any data-heavy application benefits from such a platform.

One example of such a data-heavy application is presented by Fragkou et al. [3] in the form of the Internet of Battlefield Things (IoBT). This relatively novel application domain is about a concept in which various devices on the battlefield—both smart military equipment that makes autonomous decisions and conventional human-controlled military devices—are interconnected. The work focuses on a fundamental problem in IoBT networks, namely the routing of information and the calculation of a backbone network. To overcome these issues, the authors model the IoBT network as a multilayer network and adopt the concept of dominance to select a set of nodes as a backbone for the IoBT network. However, the domination concept of single-layer networks cannot be transferred straightforwardly to the more complex IoBT networks. To this end, the authors introduce the Cross-layer Connected Dominating Set (CCDS) algorithm, which is specifically designed for IoBT networks. Compared to state-of-the-art approaches, CCDS achieves more compact network spanners, while still ensuring network-wide flow of information.

It is evident that confidential communication between devices is mandatory in a setting such as the IoBT. Virtual Private Network (VPN) technology allows us to establish private and secure communication channels over the Internet. Gentile et al. [4] therefore analyze in their paper the performance of different open-source firmware and operating systems for deploying VPNs in outdoor locations with poor network connectivity. For this purpose, they compare the performance of OpenWrt 21.x, Debian 11 x64, and Mikrotik 7.x as server-side operating systems, and various client-side operating systems, including Windows 10/11, iOS 15, and Android 11. As VPNs establish secure connections between client devices and remote endpoints by encrypting traffic, the applied VPN protocol also has an effect on the achievable level of security and performance parameters such as latency and throughput. The main goals of the research are therefore to identify algorithms that ensure efficient data transmission and encryption, achieve compatibility with existing VPN infrastructure, and enable the use of open firmware on constrained routers.

In addition to secure communications, it is also essential to monitor the IoT devices in terms of the software running on them. In this regard, the early detection of cyberattacks plays a key role. Therefore, Lightbody et al. [5] study whether malicious behavior of IoT devices can be detected based on their power consumption behavior. To this end, they identify unique power usage patterns for typical operations performed on an IoT device. A Raspberry Pi 3 model B and a DragonBoard 410c, two of the most common

IoT systems today, are used for this purpose. If the energy consumption of an operation deviates noticeably from the expected pattern, this is an indication of an attack. In particular, the authors consider reconnaissance, brute force, and denial of service attacks. The findings in the paper demonstrate that this non-intrusive side-channel method is a useful addition to existing protection measures. Despite the focus on low-power IoT devices, the findings can be applied to any type of computing system, up to high-performance computers.

In the IoT context, not only the data transmission and the IoT devices pose potential threats but also the gathered data themselves. As more and more personal data are involved, the processing of such data inevitably raises privacy concerns. Therefore, Stach et al. [6] investigate which privacy-enhancing technologies (PETs) can be used to systematically conceal certain information patterns contained in the data without compromising the overall data utility. However, in a highly heterogeneous landscape like the IoT, there is no compelling one-size-fits-all solution to this end. Accordingly, the authors identify the required data processing tasks and the resulting privacy or confidentiality concerns for seven representative IoT use cases and propose suitable PETs for all types of data involved. A SWOT-like analysis (strengths, weaknesses, opportunities, and threats) reveals open challenges, e.g., how to configure and deploy these PETs or how to prevent the misuse of such PETs. The paper draws conclusions on how to overcome these challenges.

Besides IoT, i.e., mainly data acquisition and interconnection topics, this Special Issue also deals with blockchain technologies. These were originally intended for the management of digital currencies, i.e., rather homogeneous data and simple data structures. However, the inherent distributed, tamper-resistant, and immutable nature as a data store makes blockchain a key technology whenever data need to be shared securely within trustless environments. Five papers therefore discuss other emerging use cases for blockchain technologies. For instance, Ahmed et al. [7] introduce the concept of Self-Sovereign Banking Identity (SSBI), a blockchain-based self-sovereign identity system, to address challenges in open finance and open banking. In open finance, financial service providers are not only able to retrieve transactional details from bank customers but also have write access to such information. In such a scenario, privacy leakage and misuse obviously need to be prevented. The SSBI prototype therefore relies on industry-standard bank cards that allow users to grant fine-grained permission for data sharing with financial service providers to ensure that no detailed personal identity or financial information is disclosed. The prototype implementation, based on Veramo SDK and Ethereum, demonstrates that SSBI can overcome the limitation of signing curves on current state-of-the-art Java Card approaches.

Santos et al. [8] look at another application case for blockchain technologies. In their studies, they have identified the limitations of loyalty platforms, i.e., programs designed to increase customer loyalty and encourage repeat purchases on behalf of specific brands by offering some type of reward for each purchase. Their main problems arise from rewards, which are seen as insufficient incentives by many customers and still cause high costs for brands. Furthermore, there is no option for customers to manage their earned loyalty points across different platforms. The authors therefore propose a blockchain-based approach to manage customer data from multiple loyalty programs on a single meta platform. The accurate and secure handling of transactions and loyalty points is ensured by means of smart contracts. The application of these blockchain technologies not only enables a more seamless, efficient, and user-friendly experience for customers but also creates advantages for brands in terms of reduced costs and increased customer loyalty.

Blockchain technologies can also be applied in the agricultural business. In their paper, Rocha et al. [9] analyze the benefits, disadvantages, challenges, and opportunities associated with the use of blockchain-based approaches in this sector. For this purpose, they conducted interviews with ten agribusiness professionals working with blockchain technologies to gain insights into their practical experiences. To this end, they applied a two-phase survey approach, in which the same participants were consulted again two years later, in order to reflect shifts in their assessment. In general, blockchain technologies play an increasingly important role in this application area, especially with regard to governance

and information flow within supply chains. However, the findings of the study also clearly reveal that the transition to blockchain-based solutions also entails drawbacks, e.g., high implementation costs. These drawbacks are also critically assessed by the authors. Overall, they come to the conclusion that the benefits and opportunities associated with blockchain application in agribusiness outweigh the challenges and disadvantages.

Another application for blockchain technologies is the management of certificates in public key infrastructures (PKIs). In this regard, Honecker et al. [10] discuss how DLTs can address the challenges of modern PKIs, namely their heavy focus on a central certificate authority (CA) that manages the root certificates. Since security in PKIs is based on certificate chains, tampering with or blocking access to the root certificate compromises the entire chain and thus renders the PKI useless or inoperable. To this end, the authors therefore propose using a DLT-based data storage. Due to the decentralized nature of DLTs, attackers would only be able to compromise the CA if they had access to all nodes. Furthermore, DLTs establish trust in the authenticity of the certificates provided. The authors additionally adapt the Near-Field Communication Key Exchange scheme, which enables lightweight handling of keys. Evaluation results show that by using blockchain technologies that support smart contracts, the security of the certificates can be increased, but at the expense of performance, e.g., in terms of execution times.

The entertainment industry has also realized the potential of blockchain technologies. Digital assets are increasingly distributed as non-fungible tokens (NFTs), which can be verifiably linked to a specific user, e.g., unique player items in a video game, while this can be solved relatively easily from a technical point of view via blockchain entries certifying ownership and authenticity, player perception of such techniques is still largely unresearched. Paajala et al. [11] therefore study the opinion of gamers towards the inclusion of such blockchain-based features in games. Based on a game called IkuneRacer, they investigate how players perceive transparency, trust, and user-generated content in blockchain-based games. Their overall research goal is to evaluate whether the implementation of blockchain technologies in games influences player engagement and retention. In this context, it is observed that a combination of asset ownership and user-generated content has a positive effect on the willingness to devote time to a game.

With such applications for blockchain technologies, the volume of stored data is increasing, and the underlying data structures are becoming more and more complex. Accordingly, the demand to carry out comprehensive data analytics directly in the blockchain is on the rise as well. In DLTs, however, data access is usually realized via low-level block data instead of high-level data assets, which makes such analytics significantly more difficult. Current blockchain analytics tools address this challenge by using an internal middleware that maps high-level user queries to low-level data interfaces. To improve the analytics capabilities of such tools, Vinceslas et al. [12] introduce an abstraction layer that provides blockchain data in aggregated and pre-processed form to block explorers and other analytics dashboards. The work aims to improve the auditability and intuitiveness of DLTs by providing users with lightweight data interfaces such as dashboards. The benefits of the proposed abstraction layer architecture are illustrated by means of an industrial case study.

Similar to IoT-based applications, the extensive accumulation of data from a wide range of domains raises confidentiality and privacy concerns in the context of blockchain as well. For this purpose, Xu et al. [13] consider the data collected using 3D sensing technology. Such sensors create point clouds, i.e., annotated geometric information which is arranged in a 3D space. This technology is used, for instance, in autonomous driving. In such a use case, the data are always related to a driver in one way or another, so special attention must be paid to data security, e.g., in terms of access, processing, and sharing. To this end, the authors present SAUSA, an approach that combines blockchain technologies with concepts of software-defined networking (SDN). SAUSA monitors and controls any kind of interaction with the point cloud data. Using a hybrid on-chain/off-chain storage strategy, less sensitive metadata can be stored in a distributed data store, whereas sensitive payload

data can reside on a private storage. This way, SAUSA enables efficient and resilient point cloud applications while still giving users full control over their data.

Such an approach is suitable whenever it is possible to share no or very little data with certain parties. In the context of elections, however, this is not possible as the election results have to be verifiable, i.e., it must be ensured that no votes are cast illegitimately and that every legitimate vote is counted. Notwithstanding, privacy has a high priority with regard to elections as well since it must be ensured that a vote can be cast confidentially and that it cannot be traced back to the voter. Sallal et al. [14] address this paradox by leveraging blockchain technologies. In their proposed PVPBC e-voting system, a permissioned distributed ledger and smart contracts are applied, achieving effective authorization while preserving revocable anonymity properties. The adopted Selene voting scheme ensures that voters can easily verify that their votes are accurately captured by the system, without having to deal with the underlying cryptographic complexity. This way, not only the most crucial security requirements for e-voting systems are addressed—e.g., fairness, verifiability, and privacy—but experimental results also demonstrate that PVPBC is highly scalable.

In the final research article, the two thematic blocks of this Special Issue—namely, IoT and blockchain technology—are brought together. In this paper, Xevgenis et al. [15] discuss next-generation networks, which aim to provide features such as ultra-low latency, high availability, and wide service coverage to users. This is achieved by the integration of SDN and network function virtualization. To improve elasticity and dynamics and reduce the necessity for human interaction, the Zero-touch Service Management (ZSM) framework can achieve complete end-to-end automation of network service management, even across different domains. However, this raises security concerns. The authors argue that the use of blockchain technology in a trustless environment such as the ZSM can create inherent security in terms of data integrity and transaction validity. For this reason, they introduce an architecture for multi-domain network infrastructures that are managed via ZSM, yet the management functions are implemented as smart contracts. The authors discuss different blockchain systems that are suitable for this purpose and provide implementation guidelines for their proposed architecture.

Reviews. This Special Issue is complemented by three interesting literature reviews. The first review is focused on how a network can be secured using blockchain technology. Ismail et al. [16] specifically consider wireless sensor networks (WSNs), which are the enabler technology for the IoT. Since the devices deployed in these networks are usually rather rudimentary, they often lack sufficient security measures, which is why they are prone to cyberattacks. In their work, the authors therefore address the question of which protection goals are particularly relevant in WSNs and which unique characteristics of WSNs impede security measures. Furthermore, they investigate which cyberattacks are particularly prevalent and effective in the WSN context and how they affect the WSN. As existing security measures are insufficient against these attacks, the paper proposes the inclusion of blockchain technologies and machine learning techniques in WSNs. It also identifies challenges in this regard and discusses different implementation strategies to ensure reliable cyberattack detection and cyberattack prevention.

The second review covers a specialized application domain involving WSN technologies. Sayeed et al. [17] examine the Internet of Robotic Things (IoRT), which supplements the IoT with concepts of cloud computing and artificial intelligence to enable cyber-physical systems to make autonomous decisions and carry out appropriate actions. The IoRT can be leveraged in various fields, including manufacturing, healthcare, security, and transportation. In their review, the authors outline the techniques used in IoRT, the relevant architectures in the IoRT landscape, and the capabilities of cyber-physical systems in this context. The gained insights provide the foundation for taxonomies that reflect the different classes into which IoRT environments can be categorized. The review also addresses security aspects that are characteristic for the IoRT. It is noticeable that there are still major limitations related to data security, for which the authors also suggest the use of blockchain

technologies. The paper concludes with open research questions, including ethical issues, trust issues, and data quality issues.

The final review brings the blockchain topic to the forefront. Blockchain technology offers a high level of data protection, as all data are stored in an immutable manner, and tampering with the data is impossible. However, this very characteristic is also an inherent problem of this technology when it comes to data privacy. Data protection laws such as the GDPR grant data subjects a right to rectification (Art. 16 GDPR) as well as a right to erasure (Art. 17 GDPR). That is, whenever personal data are stored in a blockchain-based data repository, there have to be redacting capabilities. Abd Ali et al. [18] therefore investigate which concepts towards a mutable blockchain, which allows controlled and supervised amendments to specific content, are discussed in research. In this respect, they also identify the particular implementation challenges that a redactable blockchain has to overcome and address security criteria that must still apply despite the redacting capabilities. Based on their findings, the authors outline future research directions and open issues in the field of effective redaction mechanisms for blockchain technologies.

The seventeen excellent papers included in this Special Issue provide a well-rounded overview of the current state of the art and current state of research in the field of security and privacy issues in blockchain technologies and the IoT. In this respect, it illustrates how versatile and complex this topic area is. On the one hand, the literature reviews highlight the potential of these technologies and how they can significantly facilitate our everyday lives in all kinds of domains, but also which open research questions still need to be solved in the future when it comes to security and privacy. On the other hand, the research articles present highly innovative approaches to overcome such problems without having to sacrifice the conveniences that blockchain technologies and the IoT have to offer. This Special Issue is therefore aimed at developers and researchers seeking to implement effective and efficient blockchain-based and/or IoT-based solutions as well as users of such technologies who want to learn more about their capabilities but also their limitations and about future trends in this field of research.

As guest editors, we would like to take this opportunity to thank all authors for submitting their interesting and informative manuscripts to Volume II of this Special Issue. We would further like to acknowledge all the reviewers, whose thorough and substantive reviews have helped to improve the quality of the manuscripts and without whom this Special Issue would not have been possible. Last but not least, we would like to express our special thanks to the MDPI editorial team, who have strongly supported us in the work on this Special Issue.

Author Contributions: All authors have read and agreed to the published version of the manuscript.

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

References

1. Stach, C. (Ed.) *Security and Privacy in Blockchains and the IoT*; MDPI: Basel, Switzerland, 2023. [CrossRef]
2. Stach, C. Data Is the New Oil—Sort of: A View on Why This Comparison Is Misleading and Its Implications for Modern Data Administration. *Future Internet* **2023**, *15*, 71. [CrossRef]
3. Fragkou, E.; Papakostas, D.; Kasidakis, T.; Katsaros, D. Multilayer Backbones for Internet of Battlefield Things. *Future Internet* **2022**, *14*, 186. [CrossRef]
4. Gentile, A.F.; Macrì, D.; De Rango, F.; Tropea, M.; Greco, E. A VPN Performances Analysis of Constrained Hardware Open Source Infrastructure Deploy in IoT Environment. *Future Internet* **2022**, *14*, 264. [CrossRef]
5. Lightbody, D.; Ngo, D.M.; Temko, A.; Murphy, C.C.; Popovici, E. Attacks on IoT: Side-Channel Power Acquisition Framework for Intrusion Detection. *Future Internet* **2023**, *15*, 187. [CrossRef]
6. Stach, C.; Gritti, C.; Bräcker, J.; Behringer, M.; Mitschang, B. Protecting Sensitive Data in the Information Age: State of the Art and Future Prospects. *Future Internet* **2022**, *14*, 302. [CrossRef]
7. Ahmed, K.A.M.; Saraya, S.F.; Wanis, J.F.; Ali-Eldin, A.M.T. A Blockchain Self-Sovereign Identity for Open Banking Secured by the Customer's Banking Cards. *Future Internet* **2023**, *15*, 208. [CrossRef]
8. Santos, A.F.; Marinho, J.; Bernardino, J. Blockchain-Based Loyalty Management System. *Future Internet* **2023**, *15*, 161. [CrossRef]

9. Rocha, G.d.S.R.; Mühl, D.D.; Chingamba, H.A.; de Oliveira, L.; Talamini, E. Blockchain, Quo Vadis? Recent Changes in Perspectives on the Application of Technology in Agribusiness. *Future Internet* **2023**, *15*, 38. [CrossRef]
10. Honecker, F.; Dreyer, J.; Tönjes, R. Comparison of Distributed Tamper-Proof Storage Methods for Public Key Infrastructures. *Future Internet* **2022**, *14*, 336. [CrossRef]
11. Paajala, I.; Nyyssölä, J.; Mattila, J.; Karppinen, P. Users' Perceptions of Key Blockchain Features in Games. *Future Internet* **2022**, *14*, 321. [CrossRef]
12. Vinceslas, L.; Dogan, S.; Sundareshwar, S.; Kondoz, A.M. Abstracting Data in Distributed Ledger Systems for Higher Level Analytics and Visualizations. *Future Internet* **2023**, *15*, 33. [CrossRef]
13. Xu, R.; Chen, Y.; Chen, G.; Blasch, E. SAUSA: Securing Access, Usage, and Storage of 3D Point CloudData by a Blockchain-Based Authentication Network. *Future Internet* **2022**, *14*, 354. [CrossRef]
14. Sallal, M.; de Fréin, R.; Malik, A. PVPBC: Privacy and Verifiability Preserving E-Voting Based on Permissioned Blockchain. *Future Internet* **2023**, *15*, 121. [CrossRef]
15. Xevgenis, M.; Kogias, D.G.; Karkazis, P.A.; Leligou, H.C. Addressing ZSM Security Issues with Blockchain Technology. *Future Internet* **2023**, *15*, 129. [CrossRef]
16. Ismail, S.; Dawoud, D.W.; Reza, H. Securing Wireless Sensor Networks Using Machine Learning and Blockchain: A Review. *Future Internet* **2023**, *15*, 200. [CrossRef]
17. Sayeed, A.; Verma, C.; Kumar, N.; Koul, N.; Illés, Z. Approaches and Challenges in Internet of Robotic Things. *Future Internet* **2022**, *14*, 265. [CrossRef]
18. Abd Ali, S.M.; Yusoff, M.N.; Hasan, H.F. Redactable Blockchain: Comprehensive Review, Mechanisms, Challenges, Open Issues and Future Research Directions. *Future Internet* **2023**, *15*, 35. [CrossRef]

Short Biography of Authors

Dr. rer. nat. Christoph Stach is a postdoctoral researcher at the Applications of Parallel and Distributed Systems department of the University of Stuttgart. He completed their studies in computer science at the University of Stuttgart in 2009. In 2017, he received their Ph.D. in computer science from the University of Stuttgart for their research in the area of information security and data privacy in mobile applications. Following their successful doctorate, he was appointed Academic Councilor at the Institute for Parallel and Distributed Systems of the University of Stuttgart. From June 2020 to September 2021, he held the deputy professorship in Data Engineering at the University of Stuttgart. Today, he is head of the working area of Information Systems and Applications at the Applications of Parallel and Distributed Systems department of the University of Stuttgart. His current research focuses on concepts and tools required to enable trustworthy and demand-oriented data provisioning for users, such as data scientists and data analysts. To this end, their research addresses research questions regarding data acquisition, data management, data security, and data protection.

Clémentine Gritti received the M.Sc. degree in computer science from Grenoble Alpes University, France, in 2012, and the Ph.D. degree in computer science from the University of Wollongong, Australia, in 2017. She has been a Lecturer at the Computer Science and Software Engineering Department, University of Canterbury since 2020. At the end of 2023, she will join the digital security team at Eurecom, France, as a research fellow. She previously worked on several research projects dealing with information security and privacy for electronic health and electronic voting. Her current research interests include design and evaluation of public-key cryptographic protocols for security and privacy in various environments, such as cloud computing, the Internet of Things, and blockchain.