12

Achieving Security and Privacy in NG-IoT using Blockchain Techniques

Vasiliki Kelli[1], Anna Triantafyllou[1], Panagiotis Radoglou-Grammatikis[1], Thomas Lagkas[2], Vasileios Vitsas[2], Panagiotis Fouliras[3], Igor Kotsiuba[4], and Panagiotis Sarigiannidis[1]

[1]University of Western Macedonia, Greece
[2]International Hellenic University, Greece
[3]University of Macedonia, Greece
[4]iSolutions Labs, Ukraine
E-mail: vkelly@uowm.gr; atriantafyllou@uowm.gr; pradoglou@uowm.gr; tlagkas@cs.ihu.gr; vitsas@it.teithe.gr; pfoul@uom.gr; igor.kotsiuba@isolutions.com.ua; psarigiannidis@uowm.gr

Abstract

The centralization of data is a current practice in information systems that do not fit into the novel next-generation computing concept. Such a paradigm aims to support the distribution of information, processing, and computing power. Blockchain is a technology supporting the recording of information for distributed and decentralized, peer-to-peer applications, which has emerged in the last decade, with the initial focus being on the finance sector. A highly valuable feature of blockchain is its capability of enhancing the security of data due to the immutability of the information stored on the ledger. In this chapter, the definition, details, applications, and benefits of this technology will be explored. In addition, the ways in which blockchain increases security and privacy will be described. Finally, the pairing of blockchain with other next-generation, cutting-edge technologies will be investigated.

Keywords: Blockchain, security, privacy, peer-to-peer.

 DOI: 10.1201/9781032632407-15

This chapter has been made available under a CC-BY-NC 4.0 license

12.1 Introduction – What Is Blockchain?

Technology has become an aspect of daily life for most of the world's population. Intelligent devices able to capture, gather, process, and distribute information have become a necessity for an ever-increasing number of domains, ranging from the simplistic use of smart home gadgets to the highly critical medical sector. Intelligent devices have become such an integral part of contemporary society, which each human is estimated to own 9.3 devices, by the year of 2025 [1]. Such a massive number of data-driven devices is expected to significantly increase the volume of data to be processed and stored. After all, Internet of Things (IoT) contributed to the creation of the concept of Big Data, which is defined as highly variable data, produced at high velocity, and is arriving in big volumes. Next-generation IoT (NG-IoT) is a novel concept in computing, aiming to extend IoT in a human-centric, distributed manner. As such, objects, services, and technologies offered to the end-users are combined to achieve optimal end-user satisfaction, while the processing of data occurs in the edge, closer to the user, yielding faster response times.

Contemporary information systems mostly focus on processing and storing data in a central manner. This means that data travels from each data source to a central entity for further management. However, this task is becoming increasingly difficult due to the high volume and variety of the produced information; as such, the effective storage and rapid analysis of data becomes the main concern. In addition, centralization is often associated with security and privacy issues, due to data traveling through unsecure channels to the central entity, or due to the single-point-of-failure problem, which dictates that the entire process will fail, if the central entity's operation is disrupted.

The issues described in the paragraphs above have contributed to a current effort to shift from the use of the concept of centralization in IoT to the concept of decentralization. Consequently, information, processing, and other aspects are distributed across devices, recanting the single-point-of-failure problem. The significance of the shift toward decentralization has become prominent due to the rise of the NG-IoT concept in computing, where instead of relying on cloud solutions for data processing, all management occurs in various distributed edge nodes, closer to the end-user.

Blockchain is the technology mostly associated with decentralization and thus plays a key role in the NG-IoT concept. Although this technology became well-known through the launch of the first digital cryptocurrency, Bitcoin, in 2009, the idea was initially described by a person under the

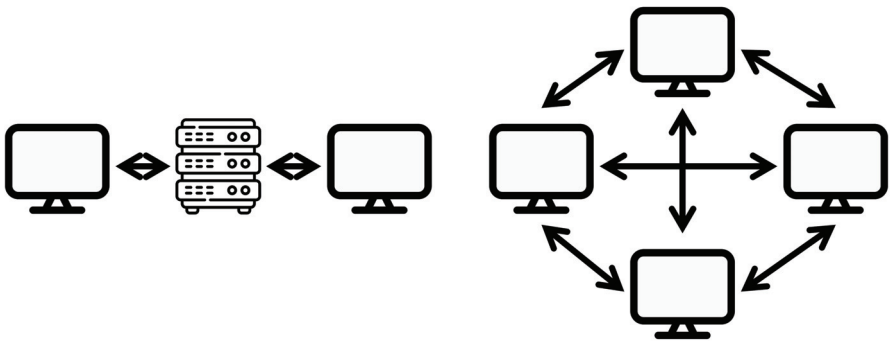

Figure 12.1 Centralized systems (left) and decentralized systems (right).

pseudonym "Satoshi Nakamoto" in 2008 [12], [13]. The concept behind blockchain states that it serves as a system to record information, in an immutable manner. This information is duplicated, and every participant in the blockchain network owns a copy of it. In particular, a blockchain is a digital ledger of transactions cryptographically signed and grouped into blocks. Each new block is cryptographically linked to the previous one, while it undergoes validation through a consensus decision by the network's members, in order to be added to the blockchain [2]. Due to blockchain's function of distributing copies of the data on the chain across the network, conflicts regarding data differences due to malicious actions are easily resolved, while its cryptographic nature boosts security [11]. Since blockchains follow an append-only policy and every member owns a copy, it is impossible for old blocks to be deleted or modified, making data on the chain tamper-resistant [14].

In order to cryptographically sign and link blocks to each other, hash functions are used by blockchain technology. Hashing refers to the application of a function to an input of any kind, leading to an output, or digest, of a specific size. Well-known hash functions include secure hash algorithm 256 (SHA-256), which produces an output of 256 bits, message-digest 5 (MD-5), which digests the input into 128 bits, and SHA-1, which produces a 160-bit output. Hash functions are one-way, meaning that they cannot be reversed, while the slightest change to the input will lead to a digest vastly different [15]. This makes hash functions optimal for verifying the veracity of data stored in the blocks. In addition, it is impossible to find inputs that lead to the same digest. As such, the utilization of hashing is able to highly elevate the security in blockchain technology.

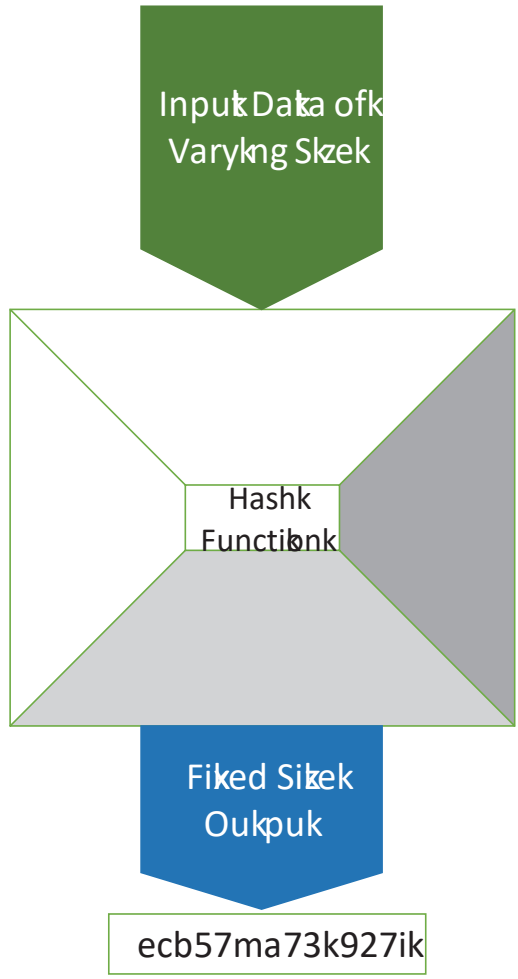

Figure 12.2 Hash function operation.

Figure 12.3 depicts a basic diagram of a blockchain network. As discussed, each block contains transactions, the calculated hash of its header, and the hash of the previous, or parent block. In blockchains, the first block created is called the genesis block and it is the only one that does not contain the hash of the previous block [3]. The header hash is generated by taking as an input information such as the timestamp, the block's data, and the parent block's hash. Hashing allows traceability of potentially malicious changes, contributing to blockchain's secure nature.

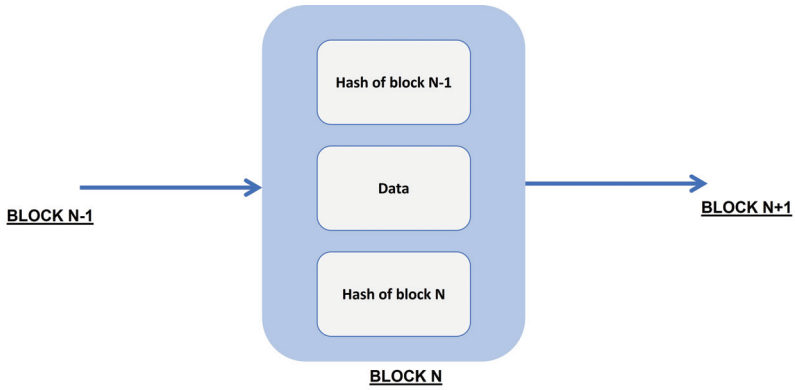

Figure 12.3 Blockchain architecture.

Blockchain is a versatile, easily integrable technology promising to elevate the security levels of the respective application areas. The versatility of this technology comes from the fact that it can be used in varying ways – from verifying transactions to securely storing any kind of data. Thus, blockchain has become an integral part of NG-IoT, as it can be effectively combined with other NG-IoT technologies and concepts such as artificial intelligence (AI), federated learning, cybersecurity, and edge and cloud computing [22]. Blockchain can support secure sharing of model updates in a centralized federated learning setting, as the model updates can be wrapped as transactions and stored in the blocks; thus, their integrity can be ensured by the federated clients [23]. In addition, blockchain can support a fully peer-to-peer AI training systems, where model updates are stored directly on the chain by the participants in the peer-to-peer network [24]. Finally, blockchains can be used for logging of actions, authentication, and authorization in a critical NG-IoT setting, as a cybersecurity solution [25], [26].

12.2 Permission-less and Permissioned Blockchain

Blockchains are categorized based on who can publish new blocks. If there is no restriction on who can append new blocks on the chain, then the blockchain is considered to be permission-less. On the other hand, if only certain entities are allowed to publish new blocks on the chain, then the blockchain is considered to be permissioned.

Permission-less or public blockchains allow anyone with access to the network to read and publish new blocks and make transactions [16]. Usually,

such blockchain networks are used primarily in the finance sector and, more specifically, in cryptocurrencies. As such, blockchains that are categorized as permission-less are open-source and free for anyone to download them and take participation in the network. However, such blockchains face probable security threats as entities can have free access to the network and thus some may try to maliciously publish blocks. Consensus mechanisms, explained in Section 12.3, aim to resolve such issues.

In contrast with permission-less blockchains, permissioned blockchain networks rely on a central or decentralized entity to allow access to the chain. In case a centralized entity is responsible for granting access, then this entity should be trustworthy. Private and consortium blockchains are both permissioned, with the former being administered by a single entity, while the latter is being administered by a group of organizations. If users are not registered by the entity to the network, then they are not able to publish new blocks, while they may not be able to read blocks, as reading can be restricted by the entity of authority. In case users have permission to join the network, they should prove through methods such as certificates that they are allowed to access to blockchain. Such blockchain networks are predominantly utilized by organizations that prefer to keep their transactions and data private and more secure. Organizations may employ permissioned blockchain to manage inventory and their supply chain, amongst other options. Permissioned blockchains may be especially useful in NG-IoT use cases where sensitive data is stored on the ledger, such as hospitals and smart grids; thus, authentication should be required to obtain the stored information.

Finally, hybrid blockchains combine the characteristics of both a permissioned and a permission-less blockchain network. Specifically, the members of the network are able to regulate and allow the accessibility of the network to other users, while the hybrid blockchain users decide whether transactions are made public [4]. This makes hybrid blockchains a customizable approach to blockchain networks.

12.3 Consensus Mechanisms

As blockchain networks are composed of distributed and trustless systems, a mechanism to allow all the nodes to reach an agreement on the validity of the blocks to be published and the status of the ledger is required. This issue is especially highlighted due to the lack of a trustworthy central authority able to regulate and manage all actions in the network. In addition, malicious actions may be an issue for permission-less ledgers, due to the unregulated

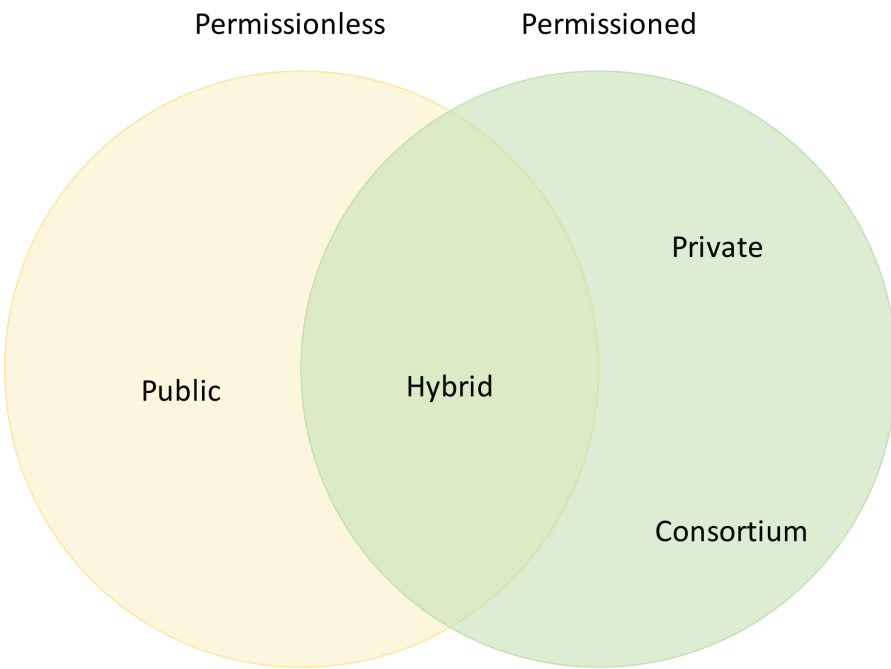

Figure 12.4 Permissioned and permission-less blockchains.

nature of such blockchains, and thus actors may attempt to alter the state of the blockchain. To address this concern, consensus mechanisms are used by the blockchain to allow the nodes to achieve trust and security between them and reach an agreement regarding the state of the decentralized ledger.

Proof of work (PoW), otherwise known as mining, is a procedure in which the participants of the mining process are required to calculate the hash value of the header of the block to be appended to the ledger [17]. Specifically, the hash value should remain below a given target value. To achieve this, miners have to find a nonce number, which is able to yield a lower or equal hash value, when added to the block's header. When a miner is able to solve the puzzle and find a nonce that yields a lower hash value, they send the block with the nonce found to the rest of the network for verification. The rest of the nodes hash the block header with the nonce, verify the work conducted by the miner, and proceed by appending the new block to their copy of the blockchain [5]. PoW consensus model was first seen in Bitcoin. As the calculation of the nonce is quite a challenging task with high computational difficulty, the miner able to find the nonce is usually rewarded.

For the Bitcoin blockchain, the publishing miner receives cryptocurrency as a reward mechanism.

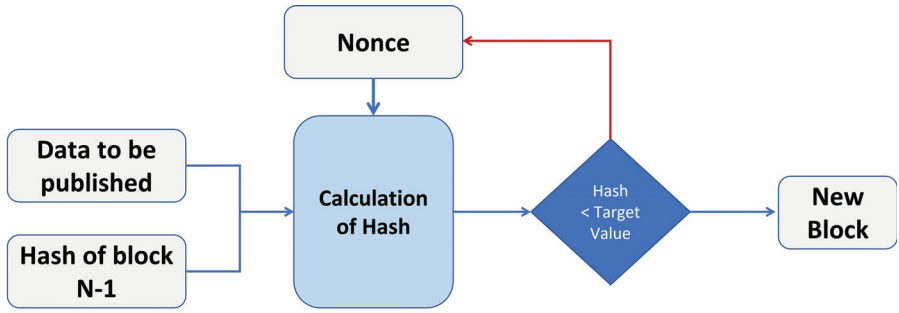

Figure 12.5 PoW consensus model.

Proof of stake (PoS) is another technique for achieving agreement in a trustless environment. The concept of PoS is based on the fact that the node with more stake in the blockchain is less likely to attack the system [18]. In essence, in a cryptocurrency setting, nodes can stake or lock coins in the system. A validating node is chosen in a semi-random manner, as the decision is also based on how many coins the node has staked for the procedure. Once the block is validated and published in the blockchain, the validator receives a reward in the blockchain's cryptocurrency. Such a consensus model does not require the computational and processing effort the PoW model requires and is not as energy-demanding as the latter [19].

12.4 Smart Contracts

Smart contracts, initially introduced in 1994 by a computer scientist and cryptographer named Nick Szabo, aim at the utilization of blockchain technology for automating the execution of a contract [20]. Specifically, smart contracts are computer programs that are able to self-execute when the conditions

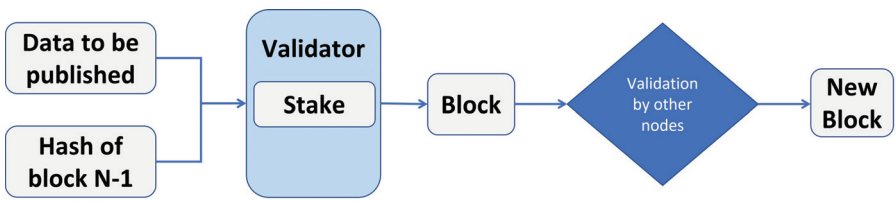

Figure 12.6 PoS consensus model.

described in the terms are fulfilled, similarly to regular contracts. Those terms are enclosed in the smart contract's code, and if an event described in the terms occurs, the smart contract is triggered and executed.

Since smart contracts leverage blockchain technology, they benefit from blockchain's secure, immutable, and tamper-resistant nature. Reliability is also ensured as all activities are trackable and verifiable through the distributed ledger. To define a smart contract, the participating parties agree on its conditions, which are then translated into code following "if/then" statements, to describe the possible scenarios [21]. Next, the smart contract is stored in the blockchain network, as displayed in Figure 12.7. This means that all participants in the network have a replica of the contract. In case a condition that is included into the description of the contract is met, then the transaction described gets executed.

Although smart contracts have a wide area of possible applications, as they are applicable to the legal industry, real estate, healthcare, insurance, and logistics, they are most predominantly seen in the finance sector. Specifically, smart contracts can contribute to adding transparency in financial transactions. A simple example would be the purchase of goods by a buyer; if money is deposited, then the order is confirmed by the seller.

A relatively new type of smart contracts is the Ricardian Smart Contract. In contrast with regular smart contracts, the Ricardian contracts are legally

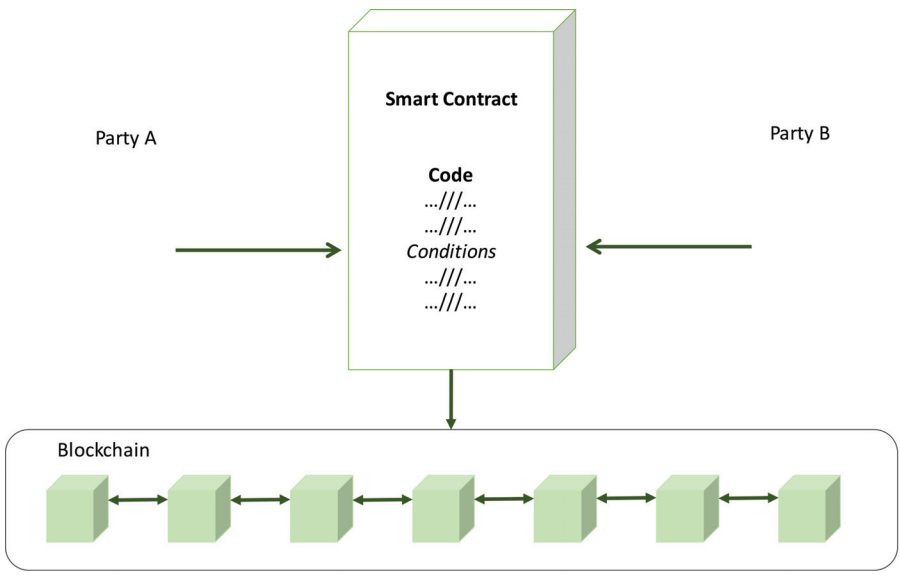

Figure 12.7 Smart contracts.

binding between the participating entities. Similar to smart contracts, they use blockchain to function and they are also verified by the blockchain network. The emerging concept of NG-IoT heavily supports the transition to a ubiquitous computing era, through human-centric advancements. Therefore, Ricardian Smart Contracts contribute to NG-IoT's aim as a human-centric blockchain application, as such contracts are presented both in a human-readable format, as well as a computer-readable format. Such a shift from static agreements to dynamic, legally binding computer code facilitates the transition to a pervasive computing era through NG-IoT, where agreements become automatically enforced, transparent, and verifiable through a peer-to-peer manner. Overall, smart contracts are a secure and reliable way to facilitate and automate the agreement procedures between the participating entities.

12.5 Blockchain Applications for Security and Privacy

Blockchain technology is considered to be the foundation of cryptocurrencies, as the concept of it was initially introduced in a cryptocurrency context [27]. Although blockchain was first designed for such applications, its utility has since been expanded and blockchain technology has become applicable in a wide area of industries [11]. This occurs not only due to blockchain's secure nature but also due to its distributed, peer-to-peer aspect. Contemporary businesses are striving to disengage from traditional centralized solutions and are currently leaning toward the utilization of decentralized systems.

Decentralization allows industries to eliminate the necessity of trusting a single central entity. This is why blockchain technology is an attractive solution for multiple areas where the establishment of trust in an untrustworthy environment is needed. Blockchain especially benefits modern supply chain systems. Supply chains are defined as the activities that contribute to the journey of materials from the initial suppliers to the final customers [6]. Some supply chain activities are product development, production, and logistics. In such a context, blockchains can be used for locating the origins of a product, providing open access to supply chain data and automating the process of transactions through the utilization of smart contracts.

Another application of blockchain would be the very timely concept of smart property. Smart property is a combination of NG-IoT and blockchain, which provides and controls ownership of a smart object through the blockchain infrastructure through the utilization of smart contracts. This is especially useful due to the emergence of smart objects and their vast

integration in contemporary lifestyle. As such, the distributed objects in a human-centric NG-IoT ecosystem are assigned to an appropriate owner through smart contracts. Nick Szabo explains the concept of smart property through an example where in case a person misses a payment for a car loan, then a smart contract would revoke the digital keys to operate the car [7].

Blockchain's reliability and immutability has made this technology an asset of high value to critical industries as well. Such application areas require data to remain unaltered and require tamper-proof history of transactions. This is the reason why blockchains are especially useful in the healthcare industry. Due to their decentralized nature, blockchains are excellent for storing and managing access to electronic medical records (EMRs), which is an electronic representation of a patient's health-related data [28], [30]. As such, EMRs can be presented to the participants of the network in a uniform format, achieving interoperability between different institutions, which is one of the main goals of NG-IoT. This is especially useful in case a patient needs to receive treatment in a foreign country; their records can be made immediately accessible to the medical personnel in the distributed NG-IoT ecosystem, taking appropriate actions. Furthermore, in accordance with the General Data Protection Regulation (GDPR) introduced in the European Union, patients can have control over their data, choosing to make their EMRs available to the respective data consumer [8], [29]. Finally, blockchains can be utilized for the challenging task of remote patient monitoring through smart contracts, where patient sensor data is checked by a smart contract and if an emergency occurs, the authorized medical personnel gets timely notified [9].

Finally, this peer-to-peer technology shows great potential for integration in the cybersecurity industry, due to the multitude of benefits it offers. Specifically, another important application of the blockchain technology would be the attestation of devices and services. In an NG-IoT network that consists of multiple heterogeneous intelligent objects where security is highly critical, it is of essence to verify the integrity of the software running on the devices. Blockchain can be used to establish trust through distributed attestation in an unreliable IoT and NG-IoT ecosystem [10]. Due to the immutability that characterizes blockchain, data regarding the identification of devices in the network can be stored in the ledger; this way, unregistered devices with possibly malicious code will not be able to impact the critical network. Finally, blockchains may be utilized for logging events in a critical infrastructure. As such, the output of systems responsible for security, such as intrusion

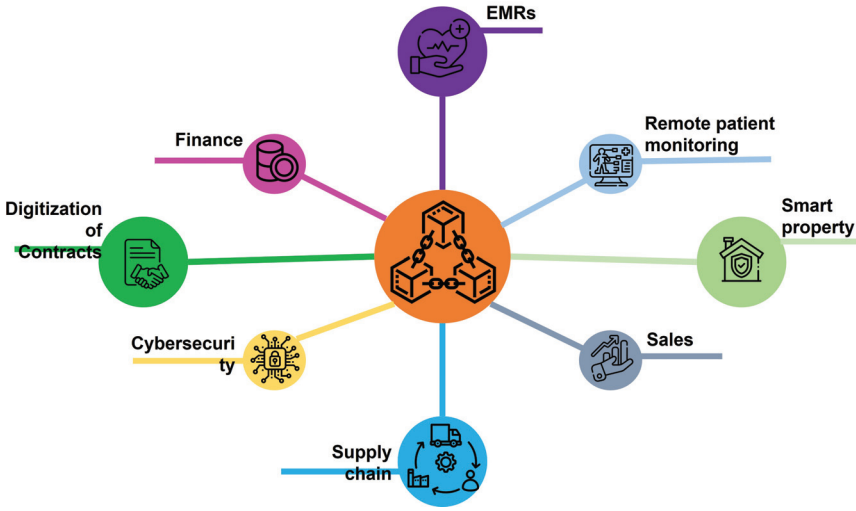

Figure 12.8 Examples of blockchain application.

detection systems (IDS), can be registered in the chain providing traceability and transparency of events.

12.6 Conclusion

The rise of the utilization of heterogeneous intelligent devices in an NG-IoT ecosystem has led to the necessity for decentralization of tasks and processes. Furthermore, the novel concept of NG-IoT calls for the interplay of emerging technologies through a human-centric, decentralized manner. In addition, a growing number of industries and businesses are striving to disengage from centralized solutions for the management of processes, data storage, and securing their systems. This way, the single-point-of-failure issue that centralized solutions may encounter is eliminated. Blockchain technology allows the secure decentralization of those processes. Due to its cryptographic nature, blockchain is immutable, transparent, and is able to establish trust in an unreliable environment. As described in this chapter, blockchain is the key component for multiple industries, including the financial industry, supply chains, healthcare, and cybersecurity. To this end, this trustworthy peer-to-peer technology promises to transform and secure the respective application areas, through its highly valuable benefits.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No. 957406 (TERMINET).

References

[1] B. Safaei, A. M. Hosseini Monazzah, M. Barzegar Bafroei and A. Ejlali, "Reliability Side-Effects in Internet of Things Application Layer Protocols," 2017.

[2] D. Yaga, P. Mell, N. Roby and K. Scarfone, "Blockchain technology overview," 2018.

[3] A. Bosu, A. Iqbal, R. Shahriyar and P. Chakraborty, "Understanding the motivations, challenges and needs of Blockchain software developers: a survey," *Empirical Software Engineering,* August 2019.

[4] A. Alkhateeb , C. Catal , G. Kar and A. Mishra, "Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review,"*Sensors,* February 2022.

[5] C. Natoli, J. Yu, V. Gramoli and P. Veríssimo, "Deconstructing Blockchains: A Comprehensive Survey on Consensus, Membership and Structure," 2019.

[6] D. Dujak and D. Sajter, "Blockchain Applications in Supply Chain," in *SMART Supply Network*, 2019.

[7] G. Foroglou and A. Lali Tsilidou, "Further applications of the blockchain," 2015.

[8] C. C. Agbo, Q. H. Mahmoud and . J. M. Eklund, "Blockchain Technology in Healthcare: A Systematic Review," *Healthcare,* April 2019.

[9] F. B. Ashraf and R. Reaz, "IoT-Blockchain in Remote Patient Monitoring," 2021.

[10] U. Javaid, M. N. Aman and B. Sikdar, "Defining trust in IoT environments via distributed remote attestation using blockchain," 2020.

[11] D. M. H. Miraz and M. Ali, "Blockchain Enabled Enhanced IoT Ecosystem Security," 2018.

[12] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[13] J. Ducrée, "Satoshi Nakamoto and the Origins of Bitcoin – The Profile of a 1-in-a-Billion Genius," 2022.

[14] P. Xi, X. Zhang, L. Wang, W. Liu and S. Peng, "A Review of Blockchain-Based Secure Sharing of Healthcare Data," *Applied Sciences,* August 2022.

[15] D. Li, P. Ding, Y. Zhou and Y. Yang, "Controlled Alternate Quantum Walk based Block Hash Function," 2022.
[16] M. Ayenew, H. Lei, X. Li, Q. Weizhong, E. Abeje, W. Xiang and A. Tegene, "Enhancing the performance of permissionless blockchain networks through randomized message-based consensus algorithm," *Peer-to-Peer Networking and Applications,* November 2022.
[17] Y. PoTsang, C. H. Wu and C. K. Man Lee, "BlockTrainHK: An online learning game for experiencing blockchain concepts," *SoftwareX,* July 2022.
[18] E. Deirmentzoglou, G. Papakyriakopoulos and C. Patsakis, "A Survey on Long-Range Attacks for Proof of Stake Protocols," *IEEE Access,* February 2019.
[19] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen and E. Dutkiewicz, "Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities," *IEEE Access,* June 2019.
[20] N. Szabo, "Formalizing and Securing Relationships on Public Networks," *First Monday,* September 1997.
[21] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han and F.-Y. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* November 2019.
[22] Y. Lu, X. Huang, Y. Dai, S. Maharjan and Y. Zhang, "Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT," *IEEE Transactions on Industrial Informatics*, June 2020.
[23] S. Awan, F. Li, B. Luo and M. Liu, "Poster: A Reliable and Accountable Privacy-Preserving Federated Learning Framework using the Blockchain," November 2019.
[24] U. Majeed and C. S. Hong, "FLchain: Federated Learning via MEC-enabled Blockchain Network," September 2019.
[25] W. Pourmajidi and A. Miranskyy, "Logchain: Blockchain-Assisted Log Storage," July 2018.
[26] D. Li, W. Peng, W. Deng and F. Gai, "A Blockchain-Based Authentication and Security Mechanism for IoT," July 2018.
[27] S. Singh and N. Singh, "Blockchain: Future of financial and cyber security," December 2016.
[28] X. Zhang and S. Poslad, "Blockchain Support for Flexible Queries with Granular Access Control to Electronic Medical Records (EMR)," May 2018.

[29] "General Data Protection Regulation Info" [Online]. Available:https://gdpr-info.eu/

[30] V. Kelli, P. Sarigiannidis, V. Argyriou, T. Lagkas and V. Vitsas, "A Cyber Resilience Framework for NG-IoT Healthcare Using Machine Learning and Blockchain," June 2021.