1

Introduction

Anwer Al-Dulaimi[1], Octavia A. Dobre[2], and Chih-Lin I[3]

[1] *5G Center of Excellence, EXFO, Montreal, Canada*
[2] *Faculty of Engineering and Applied Science, Memorial University of Newfoundland, St. John's, Canada*
[3] *China Mobile Research Institute, China*

1.1 Exploring Blockchain Technology

The blockchain is composed of a distributed database where digital pieces of information are made up in form of blocks that are stored in chains of public datasets. These blocks store information about: (i) transactions like the date, time, and value number of purchases; (ii) records of participations in transactions; and (iii) a unique code called a "hash" that distinguishes a block from another one [1]. A single block on the blockchain can store up to 1 MB of data allowing it to store a few thousand transactions, depending on the size of these operations. The state-of-the-art for blockchain consists of multiple blocks strung together. Therefore, any new data stored by any block will be added to the blockchains. On the other hand, to add a new block, it is necessary for a transaction to have occurred, verified by a network of computers, stored in a block, and that block to have been assigned a unique hash. Once a block is added to the blockchain, it becomes publicly available for anyone to view and that is what make data safe and not altered. For example, Bitcoin's blockchain allows everyone have access to transaction data, along with information about when ("Time"), where ("Height"), and by who ("Relayed By") the block was added to the blockchain [2].

To start, let's clarify the difference between public blockchain and private or federated blockchains. Public blockchains, like Bitcoin and Ethereum, are open to anyone who wants to participate in the network. They are decentralized and allow anyone to create and validate transactions without the need for permission or trust from a centralized authority, as shown in Figure 1.1. The security of the network is ensured through consensus mechanisms that incentivize participants to act in the best interest of the network. On the other hand, private or federated

Blockchains: Empowering Technologies and Industrial Applications, First Edition.
Edited by Anwer Al-Dulaimi, Octavia A. Dobre, and Chih-Lin I.

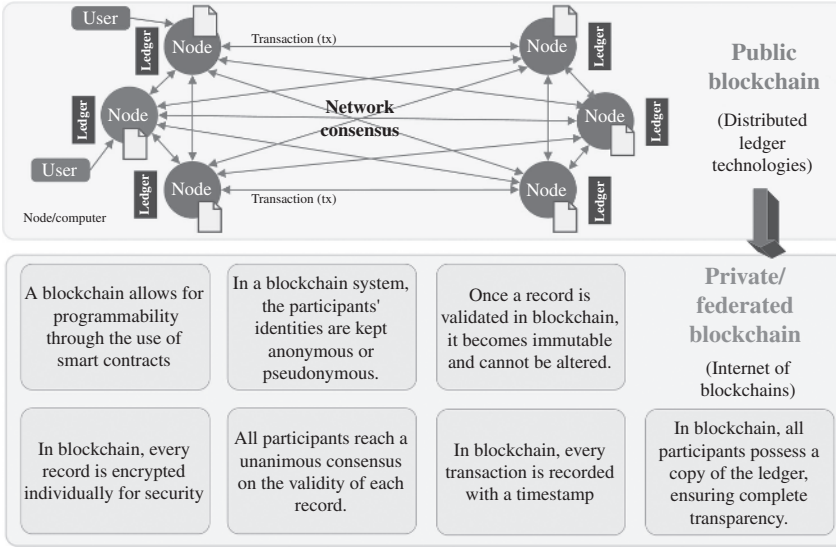

Figure 1.1 Blockchains & Distributed Ledger Technologies.

blockchains are controlled by a group of trusted entities who have been granted access to the network. These blockchains are often used in enterprise settings, where there is a need for greater control over the network and its participants. The nodes on the network are typically operated by known entities, such as businesses or organizations, and transactions are validated by a consensus mechanism agreed upon by those entities. The key difference between public and private or federated blockchains is the level of openness and accessibility of the network. Public blockchains are designed to be open to anyone, while private or federated blockchains are more restrictive and require permission to access. Additionally, public blockchains are often associated with cryptocurrencies and have a greater emphasis on security, while private or federated blockchains prioritize efficiency and control [3].

Each node or computer in the blockchain network maintains a local copy of the blockchain, which means that there are thousands or even millions of copies of the same blockchain. This distribution of blockchain copies makes the information more difficult to manipulate. Also, changing the contents of an existing block will change its hash code and that will require hackers almost to change every single block add afterwards. Those hash codes are created by a math function that transforms digital information into a string of numbers and letters. A hash code will change immediately if information is edited in any way making almost impossible for hackers to alter data. Similarly, blockchains employ "Proof of Work" system for any new participant computers to "prove" that they have done "work"

by solving a complex computational math problem. A computer becomes eligible to add a block only if it was able to solve one of these problems. However, adding blocks to the blockchain (Aka: mining) is very complicated, and the odds of solving a block are low. This is due to the design of the Bitcoin network's consensus mechanism, which is based on proof-of-work (PoW) [4]. In the Bitcoin network, miners compete to solve a complex mathematical problem called a hash function. The hash function is designed to be difficult to solve, requiring a significant amount of computational power and time. The first miner to solve the hash function is rewarded with a set amount of newly minted bitcoins and any transaction fees included in the block. The difficulty of the hash function is adjusted periodically to ensure that new blocks are added to the blockchain at a predictable rate. As more miners join the network and compete to solve the hash function, the difficulty is increased to maintain a consistent block time. The odds of solving a block on the Bitcoin network depend on several factors, including the current difficulty level, the amount of computational power dedicated to mining, and the randomness of the hash function. As of March 2023, the odds of a single mining node on the Bitcoin network solving a block and earning the block reward are estimated to be around 1 in 15 trillion attempts. However, it is important to note that the difficulty of mining new blocks is not the same across all blockchain networks. Some networks, such as Ethereum, use a different consensus mechanism called proof-of-stake (PoS) [5], which does not require the same level of computational power as PoW [6]. In a PoS system, block validators are chosen based on their stake in the network rather than their computational power, which can make the process of adding blocks to the blockchain less computationally intensive.

To understand the blockchain technology, it can be helpful to show the milestones to build the underlying components and functions of a sample blockchain. A typical process may include the following steps:

- **Define the target design for the blockchain**: Decide on the structure of the blockchain, including the block size, block interval time, consensus mechanism, and data storage format. This involved choosing the right programming language and development platform.
- **Write the code**: Use the chosen programming language to write the code for the blockchain. This includes creating the data structures, writing the smart contracts, and implementing the consensus algorithm.
- **Test the code**: This step will ensure that written code works as intended. This includes checking for bugs, verifying that the consensus mechanism is working correctly, and testing the smart contracts.
- **Deploy the blockchain**: Once the code has been tested and verified, it can be deployed on a network. This may involve any public blockchain network like Ethereum or creating a specialized private network.

- **Monitor the blockchain**: Once the blockchain is deployed, monitor it to ensure that it continues to function correctly. However, updates or modifications might be necessary on regular basis to address any issues that arise during operation.

Building a blockchain can be a complex undertaking that requires careful consideration of the use case and adherence to best practices in blockchain development. However, blockchain software development may consider prioritizing security at every stage through regular security audits and vulnerability testing. To test for vulnerabilities, it is necessary to perform various tests on the blockchain network and smart contracts. The tests may include penetration testing, fuzz testing, and code review [7]. Each of those tests will help to improve blockchain resiliency. For example, penetration testing involves simulating an attack on the system to identify potential weaknesses in the network, while fuzz testing involves providing unexpected inputs to the system to test how it responds to different inputs. Finally, code review involves analyzing the blockchain code to identify any vulnerabilities or weaknesses. Typically, vulnerability testing will be conducted regularly to identify and fix any potential security issues or defects that emerge during normal operations.

In summary, Blockchain technology has both short-term and long-term impacts on various industries. For short term, the implementation of blockchain has enabled companies to reduce costs and increase efficiency. By eliminating the need for intermediaries in transactions, blockchain has reduced transaction fees, processing times, and the risk of errors or fraud. It has also allowed for increased transparency, accountability, and traceability in supply chains, which can improve product quality and safety. For long term, blockchain has the potential to transform industries by enabling new business models and disrupting traditional ones. For example, blockchain-based decentralized marketplaces can allow for peer-to-peer transactions without the need for middlemen, while smart contracts can automate contractual agreements and eliminate the need for lawyers or other intermediaries. Overall, the impact of blockchain on industry will continue to evolve as the technology advances and more use cases are discovered.

1.2 Developing and Testing Blockchains: Software Development Approach

There are several software methods used to develop blockchain technology, some of the most well-known have been explained in Section 1.1 such as PoW and PoS, while delegated proof-of-stake is abbreviated as DPoS. As mentioned, PoW

is the original method used in the development of Bitcoin and involves miners solving complex mathematical problems to validate transactions and create new blocks on the blockchain. PoS, on the other hand, uses a consensus algorithm where validators must hold a certain amount of the cryptocurrency in order to validate transactions and create new blocks. DPoS is a variant of PoS that allows users to vote for delegates who can validate transactions and create new blocks on their behalf [8]. Other notable software methods used in blockchain development include Byzantine fault tolerance (BFT) and directed acyclic graph (DAG). BFT is a consensus algorithm that ensures the integrity of the blockchain even if some nodes on the network fail or are malicious [9]. DAG, on the other hand, uses a different structure than traditional blockchains and allows for more scalability and faster transactions [10]. Ultimately, the choice of software method used to develop a blockchain will depend on factors such as the goals of the project, the level of security required, and the size and complexity of the network [11]. These factors are carefully considered when choosing the most appropriate software method to ensure the success of blockchain project.

While conducting blockchain development, it is important to use specified test procedures in verifying the functionality of individual code modules. The test procedure typically involves writing test cases that simulate various inputs and outputs for each module, and then running these tests to ensure that the module behaves as expected. This can help identify any errors or bugs in the code early on, before the module is integrated into the larger blockchain system. Test procedures are particularly important in blockchain development, as errors in code can have significant consequences, such as security vulnerabilities or transaction errors. Figure 1.2 shows the key testing process that developers can use to verify the reliability and stability of code applications. The testing procedures are mapped to each module block to ensure that each function is developed as intended to operate in real-world deployments.

The computational resources needed for blockchain testing, in post-development validations, will depend on several factors, such as the complexity of the blockchain application, the type of testing being performed, and the size of the test network. In general, testing a blockchain application can be resource-intensive, as it involves running multiple nodes and simulating various scenarios to ensure the application's performance and security. To characterize the computational resources needed for blockchain normal operations, there are several factors that could be taken into consideration such as the specific blockchain network, the number of nodes participating in the network, the size of the blockchain, and the complexity of the consensus algorithm used. Typically, blockchain nodes require a computer with enough processing power, memory, and storage to

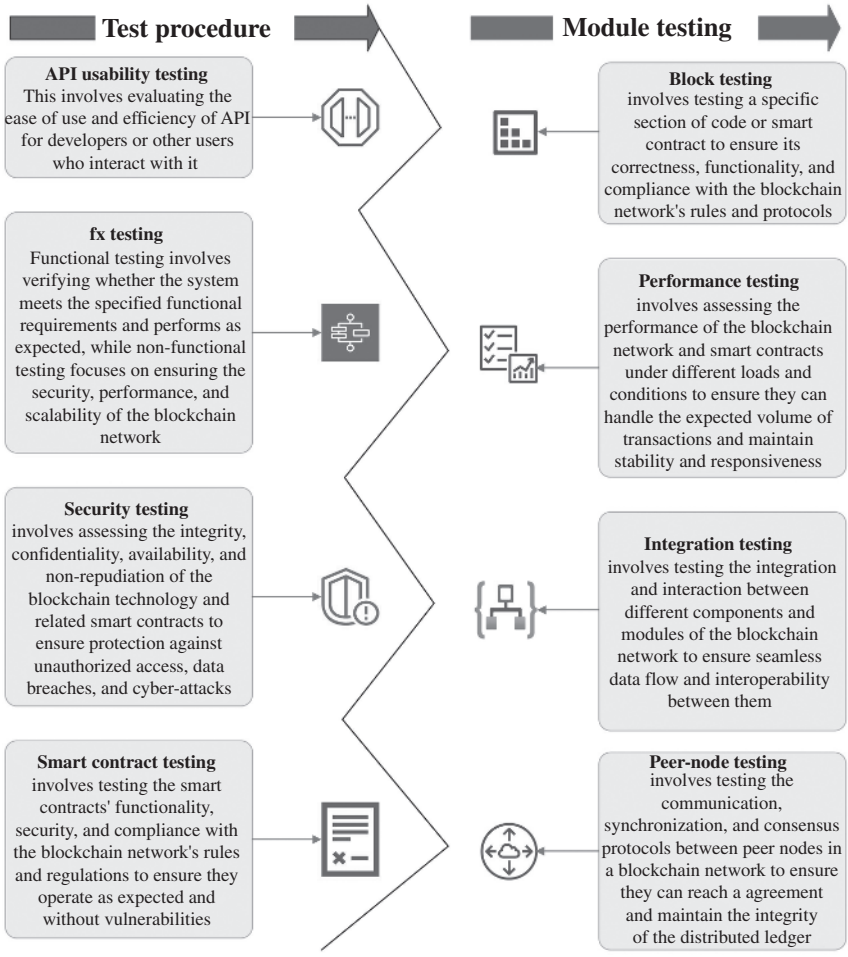

Figure 1.2 Testing Procedures and Relevant Blockchain Modules.

participate in the network and validate transactions. Some blockchain networks may also require specialized hardware, such as GPUs or ASICs, for mining new blocks. For example, Bitcoin's blockchain network requires nodes to have at least 2 GB of RAM, a multi-core processor, and around 300 GB of free disk space to store the entire blockchain. Ethereum, on the other hand, recommends a minimum of 4 GB of RAM, a 64-bit processor, and 200 GB of free disk space [12]. In addition to the hardware requirements, blockchain nodes also require a stable internet connection and sufficient bandwidth to send and receive transactions from other nodes in the network.

1.3 Blockchains and Cloud Integration

Cloud systems refer to the use of remote servers hosted on the internet to store, manage, and process data and applications. Instead of relying on local hardware and software resources, cloud systems provide on-demand access to computing power, storage, and other resources via the internet [13]. Cloud systems can be classified into three main categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS provides access to software applications, while PaaS provides a platform for developing and deploying applications, and IaaS provides virtualized computing resources such as servers, storage, and networking. Cloud services continue to dominate innovations through features such as scalability that allows cloud platforms to scale up or down depending on the needs of the user, accessibility that provide connectivity anywhere anytime to enabling remote work and collaboration, security measures to protect client's data, and automated backups and disaster recovery to ensure that data is not lost in the event of a disaster, etc. The commercial cloud service providers continue to evolve their platforms with new tools for software production and automated testing for telecom, finance, management, and many other applications. Integrating blockchain in cloud platforms can provide enhanced security and transparency in data transactions and storage, as well as improve efficiency and cost-effectiveness by reducing the need for intermediaries and increasing automation. For example, blockchain provides a secure and tamper-proof way of storing and sharing data, which can be useful for sensitive data such as financial transactions, medical records, or personal identity information. On the other hand, cloud computing provides a scalable and flexible way of storing and processing large amounts of data, but it can also be vulnerable to cyberattacks. Therefore, it is necessary to think out of the box and try to integrate blockchains as part of cloud-based systems to reduce the risk of data breaches and cyberattacks.

One approach is to look at creating trustable platforms equipped with blockchains at the cloud service provider sites. In one approach, future trustable computing platforms can employ Tactics, Techniques, and Procedures (TTPs) components as integral part of their design. The TTP provides the mechanism to perform a variety of actions to encounter cyberattacks against the platform such as tactics that can exploit attacker weaknesses, techniques that can neutralize the attack, procedures to counter an attack that may be able to disrupt the procedures themselves. The countering TTPs develop a deep understanding of the attacker capabilities and they are very flexible in adapting to changing circumstances [14]. Embedding blockchain technology into TTP can play a significant role in enhancing the security and effectiveness of hosting platforms. Blockchain technology

can secure TTPs so that only authorized personnel have access to management dashboards. The decentralized nature of the blockchain can also help to prevent unauthorized modifications or tampering of TTPs, ensuring that the information remains accurate and up to date. In addition, blockchain technology can enable the tracking of TTPs across multiple elements and interfaces allowing for real-time updates and coordination between different modules. This can improve the overall effectiveness of cloud operations, enabling faster response times and more effective decision-making. From a design perspective, blockchain-based identity solutions can securely and anonymously manage access to TTPs and other sensitive information without fear of being tracked or compromised. Clearly, blockchain enables new encounter mechanism that protects TTP itself and allows higher resiliency against advanced cyberattacks that targets defensive systems of victim platforms.

Another approach is to combine blockchain with cloud computing to improve cloud features such as scalability. Blockchain technology is designed in nature to be highly scalable and able to handle a large volume of transactions without sacrificing performance or security. Cloud computing also provides scalability by allowing cloud service providers to easily add or remove computing resources as needed. By combining these two technologies, cloud service providers can build highly scalable and efficient systems that can handle a large volume of transactions and data processing. Similarly, integrating blockchain can improve cost-effectiveness through more elastic pricing model where users pay only for the computing resources they need. Since blockchain technology reduces the need for intermediaries, cloud service providers would be able to reduce financial transaction costs by eliminating mediator fees and reducing processing times. In some other examples, blockchain could be the enabler for many other use cases such as:

- **Supply chain management**: Blockchain technology can be used to track the movement of goods along the supply chain, while cloud computing can provide a platform for sharing this information securely between different parties in the supply chain.
- **Decentralized storage**: Cloud computing can be used to provide a decentralized storage platform, where data is stored across multiple nodes in a blockchain network. This can provide enhanced security and reliability, as well as greater privacy for users.
- **Identity management**: Blockchain technology can be used to create a decentralized identity management system, while cloud computing can provide the infrastructure for hosting and managing this system.
- **Smart contracts**: Smart contracts are self-executing contracts with the terms of the agreement directly written into code. Combining blockchain and cloud computing can allow for more efficient execution and automation of these contracts.

- **Decentralized finance (DeFi)**: Blockchain technology can be used to create DeFi applications that operate on a peer-to-peer network, while cloud computing can provide the infrastructure for hosting and managing these applications [15].
- **Internet of Things (IoT)**: Blockchain and cloud computing can be used to create a secure and decentralized platform for managing IoT devices and data, allowing for greater privacy, security, and control for users [16].

Clearly, there are enormous advantages for combining blockchain and cloud computing. This would be a long journey for industry and academic to develop and test new ideas before defining what could be the cloud of the future.

1.4 Blockchain and Mobile Networking

The emergence of the fifth generation (5G) as a cloud-based network has been a game-changer in the evolution of mobile networks. Deploying 5G network functions, applications, and services as cloud-native containers creates complex architectures that can be scaled and updated easily without downtime. This approach builds upon software development features that enable cloud-based applications to become more scalable, resilient, and portable. In the context of 5G, cloud-native development empowers developers to create applications that can leverage the high bandwidth and low latency capabilities of 5G networks, including those that require real-time data processing such as augmented reality, virtual reality, and autonomous vehicles.

5G technology employs Massive-MIMO at the radio access network (RAN) side, enabling the use of multiple antennas at both the transmitter and receiver. This increases the capacity and efficiency of wireless networks. The edge cloud is another computing resource data center that is deployed closer to the edge of the network, the RAN, rather than in centralized data centers. The edge cloud fosters access to user plane traffic, leading to reduced latency and improved quality of experience (QoE) for real-time applications, such as video streaming and online gaming. 5G enables multiple vertical services operating in the form of different virtual networks on top of a physical network infrastructure. This technique is called network slicing, involving separating user services based on the user-requested Slice Service Type (SST), which is tagged to incoming user traffic. In such virtual and fully cloud-native domains, orchestrators are the software components responsible for coordinating and managing network resources and services to meet the requirements of different applications and users. The orchestrator automates processes such as rolling out services, scalability, and service recovery. These operations are performed through an orchestrator

application programming interface (API) that interfaces workflows and processes in a distributed computing environment.

Integrating blockchain technology into 5G and beyond systems is a complex process that requires careful planning and execution. The motivation for this integration is the fact that 5G and beyond are hosted by commercial clouds, which makes it mandatory to secure data exchange, identity management, and embedding smart contracts in data transactions. Therefore, choosing the right blockchain platform is also highly dependent on the targeted use cases for blockchain integration. There are several options to choose from, including public blockchains like Ethereum and private blockchains like Hyperledger Fabric. In such network-blockchain architecture, it may be necessary to determine the nodes, consensus mechanism, and data storage methods required for the blockchain system. In more advanced step, blockchain technology can be integrated with 5G system using two approaches:

- **Improving 5G functional design**: This includes developing APIs for data exchange between the blockchain and 5G systems and ensuring that the security protocols are in place to protect the integrity of the data. This could also see new 5G network functions (NFs) embedded with blockchain to manage the data exchange between NF modules or to secure data transactions between different core NFs or mobile edge clouds (MECs) and Core NFs.
- **Improving 5G operational design**: Integrating blockchain technology with a network orchestrator API is also another interesting approach to manage and coordinate workflows and processes in a distributed computing environment. Blockchain technology provides a decentralized, immutable, and tamper-proof ledger that can be used to record transactions and data in a secure and transparent way. When combined with an orchestrator API, it can provide a powerful tool for managing and coordinating complex workflows and processes. However, it is important to note that implementing such a system can be complex and requires a deep understanding of both blockchain technology and orchestrator APIs.

As technology moves toward sixth-generation (6G) networks, Artificial Intelligence (AI) is expected to be integral part of the telecom and hosting cloud systems leading to more sophisticated, smart, and optimized complex networks. Similarly, combining AI and blockchain technology in 6G networks holds immense potential to revolutionize the way we communicate and exchange data. With AI-powered algorithms, 6G networks can leverage predictive analytics to optimize network performance, anticipate network congestion, and enhance overall user experience. At the same time, blockchain technology can be used to secure and authenticate data exchanges, ensuring data integrity, privacy, and confidentiality. Both AI and blockchain can lead to more efficient and secure 6G networks, enabling a

wide range of innovative applications, such as autonomous vehicles, smart cities, and financial services. However, implementing AI and blockchain in 6G networks also presents significant challenges, such as management of real-time operations, interfacing with AI, and compliance with regulatory frameworks. Therefore, it is essential to develop a robust and standardized structure that can address these challenges and unlock the full potential of AI and blockchain on top of commercial cloud platforms.

1.5 Open Architecture and Blockchains

Open architecture refers to a system or platform that allows for interoperability and integration with other systems and platforms. In the context of software and technology, open architecture is typically characterized by the use of open standards, open protocols, and open interfaces, which enable different components to communicate and work together seamlessly. Open architecture is gaining more attention from mobile operators, particularly in terms of managing access to OTT (over-the-top) services. From a network infrastructure perspective, open architecture can enable greater interoperability with other networks and devices, as well as faster deployment of new services and applications. This style of architecture can also help mobile operators reduce vendor lock-in, as they can choose from a wider range of vendors and solutions that are compatible with open standards.

In terms of services, open architecture can enable mobile operators to offer more innovative and custom services to their customers. Open APIs allow mobile operators to collaborate with third-party developers to create new and unique services that leverage the capabilities of the network. For example, an open architecture approach can enable mobile operators to offer location-based services, such as personalized advertising or emergency services. Open architecture can also lead to greater transparency and collaboration between mobile operators and their customers. By using open standards and interfaces, mobile operators can provide customers with greater visibility into their network performance and usage, as well as more control over their services and data. This can help build trust and loyalty among customers, increase customer satisfaction and retention. Clearly, open architecture can be a key driver of innovation and differentiation for mobile operators since it enables them to leverage the power of collaboration and community-driven development. Blockchains, on the other hand, are decentralized digital ledgers that record transactions and other data in a secure and tamper-proof manner. Blockchains are typically used in the context of cryptocurrencies, such as Bitcoin, but they can also be used for a variety of other applications, such as supply chain management, identity verification, and digital

voting. When it comes to the intersection of open architecture and blockchains, there are a few key points to consider: First, many blockchain platforms are built with open architecture in mind, allowing developers to build on top of them using open standards and protocols. This can lead to greater interoperability and ease of integration with other systems and platforms. Second, some blockchain platforms, such as Ethereum, enable the creation of decentralized applications (DApps) that can run on top of the blockchain [17]. These DApps can be rebuilt using open architecture principles, allowing for greater flexibility and innovation. This approach transforms the concept of mobile network architecture from providing connectivity to traffic to facilitating accessibility to that service traffic.

In the context of mobile networks, the use of DApps in an open architecture can also enhance security to mobile networks by reducing the risk of data breaches and hacking attempts. This is because DApps are designed to operate on a distributed network, which makes it harder for a single point of failure to compromise the entire system. DApps can also streamline processes and reduce inefficiencies in mobile networks. For example, DApps can be used to automate billing processes or facilitate peer-to-peer payments, reducing the need for intermediaries and associated fees. This can provide users with a more seamless and user-friendly experience than traditional mobile applications. DApps has the flexibility to operate on a variety of devices and platforms providing a consistent experience across all connected devices. Clearly, this simplifies the interactions between mobile network infrastructure and 3rd-party providers when delivering real-time services to connected users. Therefore, it is likely to see a significant increase of DApps in mobile networks over the coming years. Open architecture creates more open, transparent, and inclusive system environment that empower users and promote collaboration. This is where industry is heading and this demonstrates more promising future for blockchain technologies in the field of mobile communications.

1.6 Open API and Monetization of Mobile Network Infrastructure

Open API is being promoted as a way to monetize mobile network infrastructure by providing third-party developers with open and standardized access to create and offer value-added services on top of the network. This can lead to new revenue streams for mobile network operators (MNOs) and increase the network's value for both customers and developers. To achieve this, MNOs need to offer APIs that expose network resources and functionality to third-party developers, who

can then create and offer services that utilize these APIs. MNOs can monetize these APIs by charging developers for access, usage, or revenue sharing models.

From blockchain perspective, there could be two different integration scenarios.

1.6.1 Using Blockchain Technology to Tokenize API Access

This involves the creation of a decentralized system for managing API access using digital tokens. Each token can have a unique identifier that is stored on the blockchain and can be used to track its ownership and usage [18]. Users can store their tokens in a digital wallet that is linked to their blockchain account. When a user wants to access an API, they transfer the appropriate amount of tokens from their wallet to the API provider's wallet. The API provider verifies the token transfer and grants access to the API for a specified period of time. The user can then use the API to access the relevant services or data. When the access period expires or the user no longer needs API access, they can redeem their tokens for the original payment or a proportionate refund. As all token transfers and API access events are recorded on the blockchain, operators can easily track the token ownership and usage, as well as detection of any fraudulent activity. This model provides a secure and transparent system for managing API access, while also allowing for easy tracking and auditing of token usage. It can also enable new business models, such as pay-per-use APIs, and provide a more flexible and decentralized alternative to traditional API access models.

1.6.2 Monetize Mobile Network Infrastructure

Another approach is using blockchain technology to monetize mobile network infrastructure considering resources and assets. In such model, mobile network infrastructure can be tokenized, and the tokens can be traded on a blockchain-based marketplace. These tokens can represent network resources such as bandwidth, processing power, and storage. By tokenizing network resources, MNOs can monetize underutilized network resources and provide an additional revenue stream. Obviously, MNOs can use blockchain technology to facilitate decentralized network sharing. By creating a blockchain-based platform, MNOs can allow other operators to access their network infrastructure on a pay-per-use basis. Smart contracts play an essential role here by automating billing and settlement processes. They can be used to automate the charging of network resources and the settlement of payments between different parties involved in the network. This can help to reduce transaction costs and increase the efficiency of the billing and settlement processes. Similarly, MNOs can use

blockchain technology to allow users to monetize their data by sharing it with third-party applications and services. The blockchain can provide transparency and security, ensuring that user data is only used for authorized purposes and that users are compensated fairly for their data. This model for infrastructure monetization offers solutions for deploying Private Network as a Service (PNAS) on top of 5G networks. It also helps to monetize resources using by 3rd-party applications, specifically IoT service providers.

1.7 Resiliency of Current Blockchain Models

Enabling any of current and future use cases running on a technology platform requires system resiliency and immunity against sudden failures. Overall, blockchain technology is designed to be resilient and decentralized, which means that it can continue to operate even if some nodes on the network fail or are compromised. However, the level of resiliency can vary depending on the specific blockchain model being used and there are some factors that could be used to evaluate blockchain resiliency. One of the biggest risks to blockchain resiliency is the 51% attack, where an individual or group gains control of over 50% of the computing power of a blockchain network. This can allow them to manipulate transactions, double-spend coins, and potentially compromise the integrity of the entire blockchain. Other risks include software bugs, which can lead to vulnerabilities and exploits, and human error, where mistakes in coding or configuration can cause significant damage. Additionally, the increasing centralization of blockchain networks due to the concentration of mining power in a few large mining pools can also pose a risk to resiliency. While blockchain technology is designed to be resilient, it is important to be aware of these potential risks and take steps to mitigate them to ensure the continued security and reliability of blockchain-based systems [19, 20].

The network size seems to have implications on resiliency. This is because a larger network can absorb more nodes going offline without compromising the overall network security. Bitcoin, for example, has a large network of nodes that are distributed around the world, which makes it highly resilient. By implementing the right security measures, blockchain platform can demonstrate resiliency. For example, multi-factor authentication and encryption can help prevent unauthorized access to nodes on the network, which can help maintain its resiliency. However, as with any technology, it is important to continuously monitor and improve security measures to ensure that the network remains resilient against potential threats. The quality assurance (QA) plays an important role in ensuring that blockchain-based systems are reliable, secure, and functional [21]. This validation cycle of monitoring, testing, and reporting should take place

on regular if not on real-time basis to identify any defects or vulnerabilities in the code. This includes functional testing, performance testing, security testing, and integration testing. For example, they may test smart contracts to ensure they behave as expected and do not have any vulnerabilities that could be exploited by attackers. This would be normally followed by code review to identify any potential issues in the codebase. In a typical industrialization process, automated testing is scheduled to ensure that blockchain-based systems meet regulatory requirements and standards. Later all testing results and limitations are documented for send-users. Since blockchain technology is anticipated to become a key driving element of many other systems, platforms, and networks, QA is likely to become an ongoing automated procedure with various testing profiles that are deployed per use case. It is also expected that AI will take the lead of this QA process to improve defects identification and probably manage automated fixes that will reshape the blockchains of the future.

1.8 Next Evolution in Blockchain Functions

Blockchain technology has rapidly evolved since the creation of the first blockchain, Bitcoin, in 2009. Since then, blockchain has found applications across various industries, from finance and healthcare to logistics and supply chain management. However, as the technology continues to mature, the question arises - what could be the next evolution in blockchain functions?

One potential area for blockchain's evolution is in the area of interoperability. Currently, most blockchains operate in silos, and there is no easy way to transfer value or data between them. However, interoperability solutions are being developed, such as cross-chain bridges and interoperability protocols, which could enable different blockchains to communicate with each other. This could facilitate seamless transactions between different blockchains and lead to the creation of an interconnected blockchain ecosystem. Another area for potential evolution is the integration of blockchain with other emerging technologies, such as AI, IoT, and edge computing [22]. Blockchain can provide secure and transparent data sharing, which could be leveraged by these technologies to enhance their capabilities. For example, IoT devices can be used to collect data, which can then be securely stored on a blockchain. AI algorithms can then analyze this data and provide insights that can be used to improve business processes. There is also a good opportunity for future evolution in blockchain functions is in the realm of governance and probably to become part of larger platform such as digital twins. Currently, most blockchain networks are governed by decentralized communities of users, which can make decision-making slow and difficult. However, new governance models are being developed that will

allow for more efficient decision-making while still maintaining the decentralized nature of blockchain networks.

Finally, we can expect to see significant advancements in the use cases for blockchain technology in the future. While blockchain networks are already being used for a wide range of applications, from supply chain management to digital identity verification [23], there are still many areas where blockchain technology could be applied. As new use cases are developed, we can expect to see even more sophisticated functions being developed on blockchain networks. However, if these challenges happen, blockchain technology has the potential to revolutionize many industries and change the way we interact with each other online.

1.9 Book Objectives and Organization

The main objective of this book is to provide a thorough understanding of the most recent developments in blockchains from both theoretical and industrial perspectives. The contributions in this book include all blockchain research initiatives that identify and discuss technical challenges as well as potential applications that continue expanding at an astonishing rate. From supply chain management to digital identity verification, blockchain technology has the potential to revolutionize many industries and change the way we interact with each other online. As such, there is a growing need for a new book on blockchains that explores the latest developments in this field and provide readers with a comprehensive view to blockchain use cases. By providing readers with a solid foundation in blockchain technology, the book can help to dispel misconceptions and promote a better understanding of its potential applications. Another important objective of this book is to provide readers with an understanding of the different types of blockchains that currently exist, including a review of public and private blockchains, as well as permissioned and permissionless blockchains. The book also reviews current and emerging use cases for blockchain technology, as well as an exploration of its potential to transform industries such as finance, healthcare, and mobile networking. By identifying the potential applications of blockchain technology, the book can help to inspire entrepreneurs and innovators to explore new ways of leveraging this technology.

Like any technology, blockchain faces technical challenges and this book shows methods to overcome drawbacks in design that could lead to wider adoption of blockchain technology, as well as an exploration of the social and ethical implications of its use. The book provides readers with analysis of the most recent research and development in this field, as well as a review of the latest trends and emerging innovations. By keeping readers up to date on the latest developments

in blockchain technology, this book can help to inspire new ideas and encourage further innovation. Finally, the book provides a discussion of best practices for implementing blockchain technology in real industrial domains that are associated with human life. This include a review of the technical, legal, and regulatory considerations involved in implementing blockchain technology to promote the responsible use of this technology and improve the chances of success for organizations that are considering its adoption. Our goal was always to discuss the technology enablers and provide real-life examples to improve readers' understanding and foster innovation at all levels.

To achieve the above objectives, this book has 11 chapters organized as following:

Chapter 1: Introduction

This chapter aims to educate readers on the functions of blockchain and explore various use cases, as well as futuristic improvements. Through this discussion, readers will gain a better understanding of the potential of blockchain technology.

Chapter 2: Enabling Technologies and Distributed Storage

This chapter examines the variety of storage systems that have been developed to address the shortcomings of centralized storage systems.

Chapter 3: Consensus and Distributed-Transaction Systems

This chapter provides a summary of the key developments that have enabled fault-tolerant consensus to be used in real-world applications. Additionally, it discusses recent developments, particularly within the context of distributed ledger systems and blockchain.

Chapter 4: Security, Privacy, and Trust of Distributed Ledgers Technology

This chapter describes the evolution of distributed databases into blockchain technology and provides guidance on integrating these databases with both new and legacy systems.

Chapter 5: Permissioned Blockchains

This chapter discusses the architecture and optimization of permissioned blockchains, with a focus on improving performance in a business setting.

Chapter 6: Attestation Infrastructures for Automotive Cybersecurity and Vehicular Applications of Blockchains

This chapter discusses automotive cybersecurity and the role of blockchain and distributed ledger technology in this field.

Chapter 7: Blockchains and Internet of Things

This chapter characterizes how the blockchain solution is well-suited to meet the decentralized requirements envisioned in the 5G context.

Chapter 8: Blockchains for Cybersecurity and AI Systems

This chapter examines the cybersecurity vulnerabilities of both public and private blockchain networks.

Chapter 9: 6G Resource Management and Sharing: Blockchain and O-RAN
This chapter explores the potential of blockchain for resource management and sharing in 6G through multiple application scenarios.

Chapter 10: Blockchains for Smart Healthcare Systems
This chapter explores the applications of blockchain in smart healthcare and the InterPlanetary File System (IPFS) for facilitating healthcare service delivery.

Chapter 11: Blockchain Standards
This chapter discusses the ongoing blockchain standards and relevant regulatory bodies responsible for their creation.

We would like to take a moment to express our sincere appreciation to the authors of each chapter in this book. Thank you for your hard work, dedication, and contribution to the field of blockchain. We hope that our readers will find these chapters informative, insightful, and enjoyable to read. Happy reading and exploring the fascinating world of blockchain!

References

1 Lee, S. and Seo, S.-H. (2022). Design of a two layered blockchain-based reputation system in vehicular networks. *IEEE Transactions on Vehicular Technology* 71 (2): 1209–1223.
2 Zhang, Y., Gai, K., Xiao, J. et al. (2022). Blockchain-empowered efficient data sharing in internet of things settings. *IEEE Journal on Selected Areas in Communications* 40 (12): 3422–3436.
3 Pourmajidi, W., Zhang, L., Steinbacher, J. et al. (2023). Immutable log storage as a service on private and public blockchains. *IEEE Transactions on Services Computing* 16 (1): 356–369.
4 Wang, T., Huang, D., and Zhang, S. (2022). Consensus algorithm analysis in blockchain: pow and raft. In: *Wireless Blockchain: Principles, Technologies and Applications*, 27–72. IEEE.
5 Yang, J., Paudel, A., and Gooi, H.B. (2021). Compensation for power loss by a proof-of-stake consortium blockchain microgrid. *IEEE Transactions on Industrial Informatics* 17 (5): 3253–3262.
6 Liu, Y., Wang, K., Lin, Y., and Xu, W. (2019). LightChain: a lightweight blockchain system for industrial internet of things. *IEEE Transactions on Industrial Informatics* 15 (6): 3571–3581.
7 Li, B., Pan, Z., and Hu, T. (2022). ReDefender: detecting reentrancy vulnerabilities in smart contracts automatically. *IEEE Transactions on Reliability* 71 (2): 984–999.

8 Xu, G., Liu, Y., and Khan, P.W. (2020). Improvement of the DPoS consensus mechanism in blockchain based on vague sets. *IEEE Transactions on Industrial Informatics* 16 (6): 4252–4259.

9 Jalalzai, M.M., Feng, C., Busch, C. et al. (2022). The hermes BFT for blockchains. *IEEE Transactions on Dependable and Secure Computing* 19 (6): 3971–3986.

10 Li, L., Huang, D., and Zhang, C. (2023). An efficient DAG blockchain architecture for IoT. *IEEE Internet of Things Journal* 10 (2): 1286–1296.

11 Li, G., Fan, Z.-P., and Wu, X.-Y. (2023). The choice strategy of authentication technology for luxury e-commerce platforms in the blockchain era. *IEEE Transactions on Engineering Management* 70 (3): 1239–1252.

12 "Running A Full Node", BitcoinCore Website. https://bitcoin.org/en/full-node#disable-listening (accessed 17 March 2023).

13 Tekin, N., Acar, A., Ahmet Aris, A. et al. (2022). Energy consumption of on-device machine learning models for IoT intrusion detection. *Internet of Things* 21: 1–13, article ID: 100670.

14 Timmins, J., Knight, S., and Lachine, B. Offensive cyber security trainer for platform management systems. In: *2021 IEEE International Systems Conference (SysCon)*, Vancouver, BC, Canada, vol. 2021, 1–8.

15 Li, Z., Xiao, B., Guo, S., and Yang, Y. (2023). Securing deployed smart contracts and DeFi with distributed TEE cluster. *IEEE Transactions on Parallel and Distributed Systems* 34 (3): 828–842.

16 Ghosh, U., Chakraborty, C., Garg, L., and Srivastava, G. (2022). *Intelligent Internet of Things for Healthcare and Industry*. Springer International Publishing.

17 Yue, K. et al. (2021). A survey of decentralizing applications via blockchain: the 5G and beyond perspective. *IEEE Communications Surveys & Tutorials* 23 (4): 2191–2217.

18 Wang, K.-Y., Lin, G., Kuo, K. et al. (2020). An empirical study of an open ecosystem model for inclusive financial services. In: *2020 IEEE International Conference on Services Computing (SCC)*, Beijing, China, 412–417.

19 Ping, J., Yan, Z., and Chen, S. (2023). A privacy-preserving blockchain-based method to optimize energy trading. *IEEE Transactions on Smart Grid* 14 (2): 1148–1157.

20 Aponte-Novoa, F.A., Orozco, A.L.S., Villanueva-Polanco, R., and Wightman, P. (2021). The 51% attack on blockchains: a mining behavior study. *IEEE Access* 9: 140549–140564.

21 Wu, H., Düdder, B., Wang, L. et al. (2022). Blockchain-based reliable and privacy-aware crowdsourcing with truth and fairness assurance. *IEEE Internet of Things Journal* 9 (5): 3586–3598.

22 Lo, S.K. et al. (2023). Toward trustworthy AI: blockchain-based architecture design for accountability and fairness of federated learning systems. *IEEE Internet of Things Journal* 10 (4): 3276–3284.

23 Sun, Z.-H., Chen, Z., Cao, S., and Ming, X. (2022). Potential requirements and opportunities of blockchain-based industrial IoT in supply chain: a survey. *IEEE Transactions on Computational Social Systems* 9 (5): 1469–1483.