The Intersection of Blockchain and 6G Technologies

Tri Nguyen*, Lauri Lovén*, Juha Partala and Susanna Pirttikangas

Abstract A blockchain is an immutable and secure public database for transactions, distributed among its participants. Further, it provides a trustless, decentralized environment for conducting the transactions between the participants, voiding the need for central authorities. A number of blockchain applications have been proposed for 5G mobile networks, including trusted cloud radio, network slice brokering, and secure and trustworthy IoT for vehicular ad-hoc networks. The unprecedented speed and capacity, massive connectivity, and the novel services anticipated in the 6G networks are expected to further enhance the performance of the blockchain-based applications. In addition, new enabling technologies that facilitate novel and innovative applications on blockchain will further expand in the 6G era. Such applications include, for example, blockchain-enhanced edge computing, device-to-device communication, and dynamic spectrum management. In this chapter we introduce the main aspects of blockchain technology, including architecture, data models, and vulnerabilities. We highlight a number of applications related to mobile networks, and consider the intersection of 6G and blockchain in relation to enabling technologies and 6G services. Finally, we look at the challenges related to blockchain-based applications.

Key words: 6G, blockchain-based 6G, blockchain, blockchain-based applications, smart contract.

Tri Nguyen, Lauri Lovén, Juha Partala, Susanna Pirttikangas
Faculty of Information Technology and Electrical Engineering, University of Oulu, Finland,
e-mail: {firstname.lastname}@oulu.fi

* These authors contributed equally.

1 Introduction

Satoshi Nakamoto, Feb. 2009

"The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve."

Bitcoin [88] cryptocurrency first appeared in 2008 in relative obscurity. Yet, over the last decade Bitcoin has attracted enormous attention due to the skyrocketing value of its assets, multiplying ten-thousandfold. While a number of competing cryptocurrencies have since emerged, Bitcoin's head start ensured its popularity and, consequently, the highest market capitalization.

Behind Bitcoins success is its technology, which voids the need for trusted intermediaries in monetary transactions. In more detail, instead of trusted intermediaries, Bitcoin's transactions are distributed among a large of crowd anonymous participants, utilizing a core foundation called *blockchain*. Blockchain is, in essence, a public database distributed among a network of participants. It relies on a unique chronological chain of immutable data blocks, shared among all participants, and constantly growing as a result of mounting transactions.

As a potential key component for decentralized systems in general, blockchain technology has been intensively studied for applications besides monetary transactions. Common among these applications is the requirement for trust, that is, an assumption that the actions taken and data provided by some participants are not fraudulent or false. Such applications include, for example, tracking of parcels in a logistic network [97, 120], keeping records of land-owners [11, 118, 31], or billing systems in multi-party environments [56, 145]. These applications have, historically, relied on a central authority to provide the trust and manage the book-keeping. Instead, blockchain aims at a *trustless* system, distributing trust among the participants using a consensus mechanism, potentially voiding the need for central authorities.

On the other hand, 6G mobile networks promise to improve latency, data rates, spectrum efficiency, user mobility, connectivity density, network energy efficiency and configurability, and area traffic capacity. Building upon these improvements, 6G will offer an environment for the growth of interactive services and technologies [1, 150, 137, 114, 109, 33].

In particular, multi-functionalization, artificial intelligence (AI), and Internet of Things (IoT) stand to benefit from 6G. In more detail, the billions of IoT devices expected to be deployed in the 6G era and communicating with each other as well as with AI agents residing in the cloud or on the edge will require unprecedented performance from the underlying network [79, 1, 96].

Blockchain is also expected to flourish in the 6G era, with three drivers in particular promoting the interplay of blockchain and 6G technologies. First, blockchain requires heavy communication among participants to guarantee the consistency and integrity of the ledger. 6G promises to have the capacity to support the resulting burden on the network. For example, moving from 5G to 6G, the development from ultra-reliable low-latency communication (URLLC) to massive URLLC will improve blockchain latency, reliability and traffic capacity.

Second, decentralizing services and reducing the need for trusted parties, blockchain technology is considered a state-of-the-art solution for next-generation connectivity [1, 30, 109, 4, 90]. Indeed, the 6G network can benefit from blockchain-based solutions in functionalities such as spectrum sharing, device-to-device content caching, and resources management.

Third, in addition to blockchain, a whole ecosystem of technological enablers is expected to expand further in the 6G era [1, 21]. The interplay of these enablers with blockchain will further benefit some platforms and services. For example, IoT stands to benefit both from the performance of the 6G networks as well as the decentralization and transparency provided by blockchain. Further, many applications, platforms and verticals, such as vehicular edge networks, smart cities, sharing economy, and social compliance, are expected to benefit from the combination [81, 90].

In this chapter, we will study two of the above drivers, namely, the potential benefits blockchain has to offer for 6G networks and services, and the interplay of blockchain with key enabling technologies for 6G. Further, we provide an overview of the blockchain technology and related concepts, and look into blockchain-based applications leveraging mobile networks. Finally, we look at the challenges related to blockchain-based applications.

The overview of blockchain technology is presented in Sect. 2, and blockchain applications described in Sect. 3. The combination of 6G and blockchain is presented in Sect. 4, challenges presented in Sect. 5, and Sect. 6 concludes the chapter.

2 Blockchain

While distributed databases have been around since at least the 70s [32], blockchain components started to come together in 1990 when Haber & Stornetta proposed the secure time-stamping of digital files to prevent modifications [49]. Further, Bayer et al. [12] proposed Merkle trees [86], that is, complete binary trees built based on a one-way function, to enhance the efficiency and reliability of the time-stamping. Block data integrity was verified by Mazieres & Shasha [84] and Li et al. [68], while Bitcoin's Proof-of-Work (PoW) consensus mechanism is partly based on work on the consensus mechanisms of earlier digital currency such as b-money [29], hashcash (with reusable PoW) [43], and especially bitgold [117]. Furthermore, Bitcoin relies on technologies such as asymmetric cryptography (1973) [25], peer-to-peer (P2P) networks (e.g. Shawn Fanning's Napster, 1999) [42] and cryptographic hash functions such as SHA-2 (2001) [19].

The growth of blockchain has ushered in new applications such as smart contracts. The principle of smart contracts was introduced by Szabo [116] in 1996, who defined

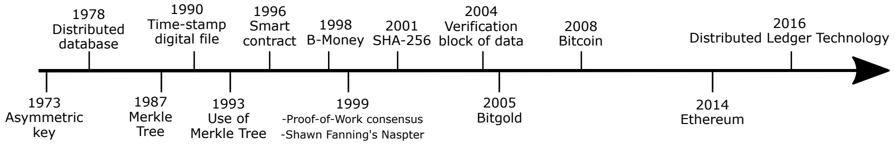

Fig. 1 Timeline of the technologies contributing to blockchain

a smart contract as a protocol that transfers and automatically executes transactions after satisfying specific conditions. In 2014, the concept was successfully realized on the Ethereum blockchain platform [128]. The availability of smart contracts further broadens the scope of blockchain-based interactive applications.

Inspired by the popularity of blockchain, a range of distributed ledger technologies (DLT) have emerged since 2016. A more general concept than blockchain, a DLT still aims to distribute a database among participants, but it is more flexible in terms of structure, design, and network architecture. As such, blockchain is one type of a distributed ledger, while distributed ledgers are instances of distributed databases.

The timeline of technologies contributing to the growth of blockchain is depicted in Fig. 1.

2.1 Architecture

Blockchain architecture can be divided in two components: network architecture and data architecture. Blockchain network architecture refers to the means of communication for node discovery and maintenance, the routing protocols used, and the data encryption schemes used in transmission. Blockchain data architecture, as illustrated in Fig. 2, refers to the relationships between its data structures as well as the cryptographic schemes used to ensure data integrity and immutability.

In more detail, a blockchain can be decomposed in three parts, namely, the transactions, the data blocks, and the chain of blocks. Transactions use the hash function and asymmetric cryptography to preserve integrity and authenticity, respectively, while, data blocks use a hash pointer and a Merkle tree [86] to guarantee both the integrity and the order of transactions. Finally, each block refers to the preceding one with a hash pointer, calculated from the entire part of that preceding block, ensuring the integrity of the whole chain. The first block of the chain is called the genesis block.

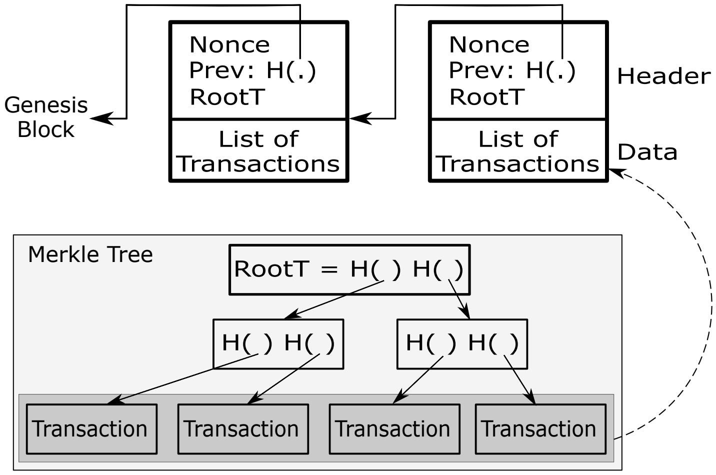

Fig. 2 Blockchain comprises a linear chain of linked blocks, each of which consists of a block header part and a block data part. The header stores metadata, including a PoW result (nonce), a hash value of the previous block (Prev), and a root value of Merkle tree transactions (RootT). The RootT value of each block is the final value of a Merkle Tree [86] containing the transactions and their hash values. Two hash values of two transactions are concatenated to form a higher tier value until reaching the root of the tree (RootT)

2.2 Data models

According to Belotti et al. [17], blockchains have four types of data models used for tracking transactions: the Unspent Transaction Output (UTXO) model, the account-based model, UTXO$^+$, and the key-value model.

Popularized by Bitcoin, an UTXO represents a digital asset, defined by its chain of ownership listing all its previous owners. To calculate the balance of a Bitcoin participant, the chain of ownership of all received UTXOs is followed before summing their values. A transaction, that is, a transfer of assets between two participants, requires a verification of the UTXOs that are used as inputs for generating the new transaction. Each transaction on a new block, in turn, consists of a set of new outputs from preceding transactions.

As a consequence, the aggregate of all UTXO states is the blockchain state. The UTXO model makes verification of this state expensive, as it requires tracking the full history all transactions. Further, data is duplicated, as output of old transactions become input for new transactions. The UTXO model should thus be applied only when there are few operations affecting the state of the whole blockchain, as with cryptocurrencies.

While the UTXO model is adopted by a number of blockchain-based cryptocurrencies, Ethereum is the first blockchain using an account-based model. The account-based model has each account managing its own transactions, with all accounts in the system forming the global blockchain state. Further, the model supports smart contracts by way of different types of accounts. Ethereum, for example, uses externally owned accounts to keep track of balance, and contract accounts to hold executed code and internal states. Hence, the account-based model provides blockchain-based systems intuitiveness and efficiency for blockchain state operations.

The UTXO$^+$ model aims augment the UTXO model towards the account-based model, without actually implementing accounts. However, the result is seen as complex and unintuitive to use [17]. Corda [20] is an example of a blockchain implementing the UTXO$^+$ model.

The key-value model (table-data model) is currently actively studied, as it can support both the transaction-based blockchain state or the account-based state, depending on the application, thus providing for a wide range of use cases. For example, the Hyperledger Fabric blockchain [8] utilizes the key-value model to represent a collection of key-value pairs for digital currency as well as for asset exchanges. Fabcoin [8], a cryptocurrency based on the Hyperledger Fabric, implements UTXO on the key-value model.

2.3 Consensus Mechanism

Consensus protocol is the most important method for facilitating trust in the decentralized blockchain network. A high abstraction level network communication protocol, the consensus protocol has an important role in forming the blockchain and ensuring the integrity of its data, shared among a number of untrusted participants. In particular, consensus protocol decides which transactions form blocks, and which blocks are chained together.

Blockchain consensus protocol consists of elements such as proposal, propagation, validation, and finalization, and the incentive strategy [131]. While the exact details vary between different blockchain implementations, the Bitcoin blockchain first has a participant, finding the nonce and finishing her PoW, proposing a collection of transactions for a block. The proposed block is propagated to all other participants and then validated to avoid conflicts. Finally, the block is accepted as the next extension to the blockchain, if it fulfills certain conditions such as adding to the longest branch, as exemplified by Bitcoin. Without any intermediaries, the incentive strategy of blockchain consensus protocol is to encourage the participants to obey the protocol by means of a reward, consisting of digital assets newly created in the system.

Bitcoin's remarkable success has brought also consensus mechanisms in the spotlight, greatly increasing research interest on the subject. Yet, consensus mechanisms were first introduced decades ago with, for example, the Byzantine General Problem [64] (BGP) proposed already in 1982.

Indeed, before blockchain, BGP was considered as the prime candidate for a consensus mechanism. In more detail, BGP describes a group of generals attempting to attack a city with a uniform strategy. To decide upon the strategy, the generals have to communicate amongst each other and find consensus on which plan to follow –

only some of the generals are actually enemy spies, seeking to thwart consensus or twist it to favor an inferior strategy.

In 1992 and 1999, the PoW [38, 53] and the Practical Byzantine Fault Tolerance (PBFT) [22] protocols were introduced as potential solutions for reaching consensus. Their ideas have been taken into use by the two main types of the blockchain, public and private (see Section 2.4), with PoW-based Nakamoto consensus implemented for example by the public Bitcoin blockchain, and the PBFT-based by the private YAC blockchain [87].

2.4 Access

Based on access to transaction data, blockchains implementations can be divided into three categories: public, private, and consortium chains [74, 152, 125]:

- A public (open-access, permissionless) blockchain allows all participants full control, including access, contribute, or maintain blockchain's data.
- A private (permissioned) blockchain gives access to transaction data for specific pre-defined participants only.
- A consortium blockchain allows authorized participants to manage and contribute to the blockchain. Participants are authorized by default nodes at the beginning, or by requirements specific to the particular blockchain model.

The three alternatives embody a trade-off between centralization and performance. In more detail, a decentralized blockchain where participants have full control on transaction data, verifying and managing blocks, requires an enormous number of messages sent between the participants to build consensus and ensure chain integrity. As a result, performance suffers, with the cost of computation rising and transaction latency and throughput getting worse. On the other hand, a highly centralized system can be made very efficient, with high throughput and low latency.

The concept of centralization is intimately linked with trust. A highly decentralized system, a public blockchain is *trustless*. It needs no trusted parties, that is, some specific, pre-defined nodes, to manage transactions, instead relying on the consensus protocol to ensure integrity. Conversely, private, centralized blockchains place trust on a central authority to manage the chain. Aiming for the middle-ground, consortium blockchains attempt to mitigate the strict division between public and private blockchains by setting up a trusted group of participants to maintain transactions.

Alternatively, blockchain-based systems can be characterized by their decentralization, immutability, integrity, and auditability [17]. As described above, decentralization refers to how blockchain data and the management of the data is distributed among the participants. *Integrity* of the blockchain data must be guaranteed to build trust among participants. Failing integrity, blockchain data can become conflicted or compromised by malicious participants. Moreover, visibility of blockchain data to different parties at different parts of the network contributes to the *auditability* and the *traceability* of data for blockchain-based applications.

2.5 Vulnerabilities

Blockchain presents a number of attack surfaces, subjecting the dependent services and applications to numerous vulnerabilities. Blockchain's vulnerabilities can be roughly divided into protocol vulnerabilities, encompassing issues with blockchain's architecture and protocols, and smart contract vulnerabilities, with issues related to the smart contract programming language and the virtual machine executing the contracts.

2.5.1 Protocol vulnerabilities

Blockhain aims to distribute an immutable chain of data blocks among the participants. This purpose may be compromised by malicious participants, seeking to break the integrity of the data blocks for their own benefit. While some blockchain-specific attacks are introduced below, blockchain may also be vulnerable to attacks on the network layers. Such attacks include, for example, DNS attacks and distributed denial of services [108].

Sybil attack, Selfish mining. A *fork* is a situation where two groups of participants have different blocks in their chain, creating two competing *branches* of the chain. Forks are classified into pre-determined *hard forks*, and *soft forks* which appear without warning. Rare events, hard forks may be created legitimately, with a group participants creating a new branch for an application requiring a new blockchain network. For example, in 2017, the *Bitcoin cash* cryptocurrency [55] was established by a group of Bitcoin developers as a hard fork from classic Bitcoin to improve the size of blocks.

A soft fork, however, is the result of a protocol error. It may be unintentional, or the result of malicious nodes trying to compromise the integrity of the blockchain. Examples include a Sybil attack [36], where a malicious entity employs multiple system identities to unfairly promote a dishonest block, and selfish mining [40], where a group of colluding participants forces the remaining honest participants into wasting their computing resources, thus creating an incentive for the honest participants to join the dishonest group.

Majority attack. A majority attack (or 51% attack) aims to break the consensus for the benefit of a dishonest group, comprising more than 50% of the votes of the participants. In more detail, a majority attack targets the consensus process, based on majority voting. The attack aims, for example, to reverse a transaction by injecting a faulty block into the blockchain. The dishonest group could, for example, first sell bitcoins and then reverse the sales transaction, keeping both the Bitcoins and the sales proceeds [71].

2.5.2 Smart Contract Vulnerabilities

The two main types of vulnerabilities for blockchain-based smart contracts are those in the programming language, and those in the virtual machines, running the code for the contracts [9]. In more detail, smart contracts are computer programs, executed on the virtual machines running on the participant computing nodes. As such, smart contracts are subject to bugs and expose new attack surfaces. Below, we introduce some examples of such vulnerabilities in the Ethereum blockchain and its programming language Solidity, along with sources for more information.

Call to the unknown. Failing to look up a function with a given signature in a target contract, a remote function call will revert to a fallback function. Cleverly setting up the fallback, a malicious contract may inject code to be run by the target, making the program flow of the target contract unpredictable [9].

Re-entrancy attack. A re-entrancy attack [9] also exploits a fallback function, with a malicious contract recursively draining another smart contract of its assets. In more detail, a smart contract exposing an interface for credit withdrawal should update their balance before sending credits to the caller. Otherwise, the malicious contract may set up a special fallback function, triggered upon the arriving credits, to make another withdrawal, which again triggers the fallback, and so on. The DAO attacks[2] in mid-2016 exploited this vulnerability to steal ca. $60M in ether.

Over- and underflow attacks. The variable types of the smart contract programming language may suffer from over- and underflow attacks [23, 108]. In Solidity, for example, a `uint256` type variable is represented by eight bits, with a minimum value of 0 and a maximum value of $2^{256} - 1$. If the value of an `uint256` type variable exceeds the maximum by one, it rolls over back to zero, and vice versa. An underflow attack exploits this behavior, employing a transfer which subtracts the attackers balance beyond the minimum, ending up with an extremely high number of credits[3].

Short address attack. The Ethereum Virtual Machine (EVM) has a bug related to the ERC20 standard[4] [23, 108]. The EVM pads a user address with extra 0's in the end if the address is shorter than a certain length. If there is a user address with a genuine 0 in the end, an attacker can impersonate that user by using her address, with the trailing 0 removed, as the EVM will append the missing zero. Moreover, this issue amplifies the number of tokens in the case of transfer.

Immutable bugs. To maintain user trust, smart contracts cannot be changed once published on the blockchain, acting independently according to their program code. Thus, if a smart contract has bugs or vulnerabilities, blockchain offers no direct methods for fixing those bugs. As a result, the resources accumulated by the contract may be at a risk [9].

Generating randomness. Smart contracts sometimes employ pseudo-random numbers, generated with a seed value from an external source. The contracts, however, are distributed, deployed simultaneously at all the participant nodes. A contract

[2] https://www.coindesk.com/understanding-dao-hack-journalists

[3] https://nvd.nist.gov/vuln/detail/CVE-2018-10299

[4] https://eips.ethereum.org/EIPS/eip-20

function running at different nodes thus should, in most cases, return the same results, or risk inconsistency between nodes.

As a solution, smart contracts often use the hash values of future blocks as their random seed. Identical to all nodes once available, such a seed guarantees identical pseudo-random numbers generated with that seed. A hash value of a future block is, however, unknown at the time of contract deployment, seemingly ensuring randomness. However, given enough resources, a malicious group of participants may influence the formation of the chain of blocks such that the future block and its hash value can, to some extent, be known at contract deployment time [9].

3 Applications

Blockchain-based applications have gone through three major evolutionary steps. To begin with, the success of Bitcoin attracted attention in cryptocurrencies and the transfer and exchange of digital monetary assets. However, the community using digital currencies remains small. Many issues prevent cryptocurrencies from reaching a wider audience, including a limited capacity for uses beyond the low-latency transfer of digital assets between two users.

To support a wider range of use cases, attention moved towards blockchain-based smart contracts. The first blockchain with smart contracts was Ethereum, whose Ethereum Virtual Machine (EVM) is a Turing-complete machine supporting arbitrary operations. With the EVM, Ethereum provides a platform not only for smart contracts with digital enforcement of their conditions, but also for decentralized applications (Dapp) comprising a number of contracts and serving financial and semi-financial use cases. Even further, a number of Dapps could be combined into a decentralized autonomous organization (DAO), a virtual entity whose entire lifecycle is executed on the blockchain.

Vitalik Buterin, May. 2014

A smart contract is the simplest form of decentralized automation, and is most easily and accurately defined as follows: a smart contract is a mechanism involving digital assets and two or more parties, where some or all of the parties put assets in and assets are automatically redistributed among those parties according to a formula based on certain data that is not known at the time the contract is initiated.

Finally, DLTs widened the scope from blockchain technology to more general distributed ledger implementations which adjust and modify the technology to satisfy application-specific requirements. Due to their flexibility, DLTs are expected to become popular especially in IoT applications where potentially billions of devices converse, requiring high performance and adaptability from the ledger.

The best-known example of a DLT for IoT is the IOTA [98], a ledger whose transaction data is stored in *tangle*, a directed acyclic graph (DAG). In more detail, instead of a linear chain of linked data blocks as in a blockchain, tangle is a graph of transactions, each of which refers to two previous ones. As a result, tangle promises the ledger a definitive performance boost in comparison to the linear blockchain.

3.1 IoT

Current centralized IoT systems incur high maintenance cost for the vendor while violating the *security through transparency* principle [24]. Blockchains and DLTs could mitigate these issues by providing a platform for smart contracts encapsulating the required functionality and with operations verified by the customers, thus both decentralizing the IoT system and increasing its transparency.

Smart cities provide a potential application vertical for blockchain and DLT based IoT applications, improving transparency, democracy, decentralization and security [132]. Other important blockchain application verticals include supply chain management, health care and transportation.

Use of blockchain for supply chain management was first considered in 2016 [119]. Blockchain-based supply chain management provides a trusted environment for data exchange and tracking, promising to ensure the continued quality of products in transit while reducing the probability of mislays. Further, smart contracts support transparent and automatic execution and verification of the supply chain management processes. Improving on traceability, a blockchain-based supply chain provides product tracking traces, helping to forecast demand and reduce the risk of fraud and counterfeit [37].

For healthcare, blockchain could help scaling up and decentralizing the communication and management of current systems, comprising many independent applications for parties such as hospitals, patients, and pharmacies. Moreover, the immutability of blockchain records and support for data provenance make data auditing easier, improving the traceability of stored data as well as the management of critical digital assets such as insurance transactions and patient consent records. Further, blockchain-based healthcare applications improve fault tolerance and security by means of the their decentralized architecture as well as the inbuilt consensus mechanisms and cryptographic schemes [51]. Current blockchain-based healthcare applications include medical record management, insurance claim process, data sharing for telemedicine, opioid prescription tracking, and storage of health care data [63, 146]. However, if sensitive data is stored on the blockchain, it needs to be protected so that its validity can be also verified. Simple encryption may not be sufficient, but zero-knowledge argument schemes need to be applied instead.

For transportation, first blockchain use cases involve vehicle communication and identity management [67, 69], where the need for trust in a heterogeneous network of vehicles can be reduced. Further, blockchain can be applied for mobility-as-a-service [91], where a number of mobility service providers such as taxicabs, public transportation operators and private ride share providers can be brought together behind a single interface, changing focus from a provider-centric view to a user based one. Transparent and verifiable, blockchain-based mobility-as-a-service reduces the need of the service providers to trust each other by way of the trustless blockchain protocol.

3.2 Security

Blockchain can be employed in a number of applications in the security vertical, providing decentralization, trust, integrity, and immutability.

For example, conventional reputation systems are centralized, suffering from single points of failure. Blockchain can help decentralize the systems [151, 66]. Schaub et al. [110] used blockchain for a reputation system for e-commerce, employing blockchain as a public database for feedback from users to product/service providers. Encouraged by the success of blockchain-based reputation system, a number of application areas such as crowdsensing [70, 151], vehicular ad hoc network [140], robotics [35], and education [113] take advantave of blockchain to obtain trust, privacy and data integrity [16].

Further, traditional Public key infrastructure (PKI) and Domain Name System (DNS) are based on a centralized architecture, which requires the trust of users and suffers from malicious certificates, man in the middle attacks, denial of service attacks, DNS cache poisoning, and DNS spoofing [142, 59]. With a decentralized, tamper-proof, and public database, blockchain promises to help with the problems. Indeed, a number of studies propose blockchain-based solutions for DNS [44, 50, 59], public key infrastructure (PKI) [10, 5, 78, 94, 59] and border gateway protocol (BGP) [50, 107]. Moreover, blockchain has been proposed to replace certification authorities such as those behind Domain Name System Security Extensions (DNSSEC) or Secure Sockets Layer (SSL) with a trustless reputation system [121].

Event logs are essential as rich resources of information for forensic investigations [106], providing evidence of problems, bugs and incidents in the systems [144]. As a result, the first target of experienced attackers is the elimination of the log trace on the attack history [15].

To prevent tampering, event logs need to be decentralized, and excel on integrity and trustworthiness [144]. Blockchain can provide a decentralized and tamper-proof logging system, guaranteeing the immutability and integrity of the log data [28, 99, 115].

For malware detection, blockchain can be used as a shared database of malware signatures [93, 46, 45], enhancing malware detection accuracy and reducing their spread.

4 Blockchain and 6G

Blockchain may benefit 6G networks in numerous ways. In particular, blockchain offers decentralization, trust management, data integrity, as well as self-organization and self-sustainability.

First, based upon a decentralized P2P network, blockchain can improve on the reliability and availability of 6G services by removing some of their single points of failure. Furthermore, blockchain promotes a trustless environment where 6G stakeholders do not need to rely on individual authorities to ensure integrity of the services [141]. Such an environment could be a benefit in, for example, heterogeneous networks, where multiple operators are employed for connections. Using blockchain, a set of services, perhaps implemented as smart contracts, may be universally available for stakeholders, without the need for operators to arbitrate or hand over responsibilities.

Second, the integrity of blockchain data is guaranteed. As such, 6G service events could be stored on blockchain, ensuring auditability and traceability of those services by third parties.

Third, blockchain-based smart contracts are autonomous entities, capable of supporting self-organization and self-sustainability. In more detail, self-organization in a network aims to simplify its management and optimization. A smart contract can observe the operating environment of a 6G service, define trigger conditions, and launch operations based on those triggers to adjust the operating environment. Moreover, the contracts can cross stakeholder borders, ensuring fairness with trustless operation and aiming for global optimization instead of local.

For example, employing spectrum sharing or resource management as self-organizing contracts, the network can react efficiently to system demands. Further, a smart contract may manage access control, keeping track of access conditions and tracing access history for critical assets such as data assets stored on the blockchain.

The impact of blockchain on select enabling technologies for 6G as well as anticipated 6G services are further detailed in the subsections below.

4.1 Enabling technologies

Network Function Virtualization. Network function virtualization (NFV) refers to replacing fixed network components such as load balancers or firewalls with virtualized components (*virtualized network functions*, VNF) which are easy to deploy, migrate and chain together. NVF thus reduces the need for custom hardware and simplifies network management, lowering both capital and operative expenses.

However, the orchestration of VNFs in distributed systems presents several vulnerabilities. To identify and track potential security events, NFV requires auditability and traceability of communication traffic and VNF update history. Such information could be managed by a blockchain-based application [105]. Further, blockchain can provide NFV with authentication, access control, permission management, resource management, and a trustless environment for the heterogeneous NFV stakeholders [7].

Cloud Computing. Cloud computing refers to a computing model where computing resources such as networks, servers, storage, applications, and related services are centralized in ubiquitous, convenient and on-demand resource pools, universally accessible via the Internet and offered with minimal management effort for those requiring such resources [85]. For mobile networks, cloud computing offers a platform for NFV as well as, for example, for cloud-based radio access networks (C-RAN), where certain base station functions are centralized as a pool of base station resources [129].

Blockchain can provide cloud-based services in 6G with security, traceability and provenance by, for example, verifying the identity of stakeholders and controlling data access [149] and storing metadata such as access logs [6]. Further, Yang et al. [136, 134] propose a blockchain-based architecture for trusted cloud radio over optical network, based on a decentralized tripartite agreement among vendors, network operators, and network users.

Another application to enhance trust, Yang et al. [135] study using smart contracts on a permissioned blockchain to construct a secure and reliable environment for IoT devices to trade their assets, safe from DDoS attacks. Further, Ma et al. [82] propose blockchain-based distributed key management architecture for IoT access control, encompassing a cloud system and a set of fog systems. Finally, Malomo et al. [83] propose smart contracts for minimizing the breach detection gap in a federated cloud environment comprising several cloud service providers.

Edge computing. Edge computing promises to reduce the communication delay between devices and cloud-based applications while reducing data rates and enhancing privacy. The promises are realized by distributing the cloud-based applications on a continuum between the devices, nearby computing servers at network hubs or base stations, and the cloud [79, 96, 48].

Blockchain is a potential solution for improving many aspects of edge computing [139]. For example, Guo et al. [47] propose an authentication scheme based on a consortium blockchain running on edge servers. The scheme ensures provenance and traceability by storing authentication data and event logs on the chain, while smart contracts provide functions for the authentication service. Further, Wang et al. [123] study an anonymous authentication and key agreement protocol for smart grid, where smart contracts keep record of public keys and provide autonomous triggers for key operations such as updates.

Moreover, a number of studies propose blockchain for edge resource orchestration and brokerage [76, 130, 77], with smart contracts providing a trusted marketplace for resource sales and allocation as well keeping a record of the transactions. Yang et al. [133] propose a trusted, cross-domain routing scheme maintaining topology privacy in a heterogeneous multi-access edge computing (MEC) system, while Rahman et al. [101] study a smart contract application providing metadata extraction, storage, analysis, and access control.

Federated Learning. Federated learning is a distributed machine learning architecture. A network of nodes each train a neural network model based on local data, assumed independent and identically distributed across the nodes. A central node combines the local models into a global one, maintaining user privacy, and distributes the global model back to the local nodes [138].

As such, federated learning proposes a centralized architecture, requiring the coordination of a central node with storage for a global model. Blockchain could decentralize the architecture [100, 60, 127], voiding the need for explicit coordination and single points of failure. Moreover, tracking the lifecycle of the models as well as access to those models on the blockchain enhances transparency and trust [80].

Further, blockchain can incentivize local nodes to participate in model sharing while discouraging freeriding [58], and manage a reputation system for nodes to ensure high-quality local models [58]. Finally, blockchain could provide a distribution architecture for local model training [111] as well as distributed storage for a federated learning application shifting high-quality data from a distributed large data pool [34].

4.2 6G Services

Spectrum Sharing and Management. Data-intensive services and applications such as big data processing, multimedia streaming and AR/VR/XR require high performance data transmissions. However, physical constraints may present a barrier for 5G network operators aiming to support those services [89]. Further, spectrum fragmentation and the current, fixed spectrum allocation policy reduce the availability of spectrum resources [112]. Blockchain can mitigate spectrum management with, for example, two particular on-chain applications: a secure database, and a self-organized spectrum market [72].

Firstly, blockchain can provide a public, secure database for spectrum management. Since blockchain guarantees the integrity of the contained data, it can record information on, say, TV white spaces and other spectrum bands [126]. Further, blockchain may store access history of unlicensed spectrum bands, promoting fairness among users. Moreover, spectrum auction results and transactions between primary users (PUs) and secondary users (SUs) could be stored on-chain to prevent frauds by PUs, guarantee the non-repudiation of auction payments, and prevent unauthorized access by secondary users SUs [61, 62].

Secondly, decentralized and sensing-based dynamic spectrum access can employ blockchain, storing spectrum sensing data to support SUs on selecting spectrum bands with a low utilization rate [95]. In such a solution, the SUs are not only sensing nodes, but also fully-fledged blockchain participants, contributing to the consensus and verifying blocks. An incentive strategy like blockchain-based cryptocurrency reward can encourage participation.

Further, implemented as a blockchain-based smart contract, spectrum management can self-organize. A self-organized spectrum is intricately linked to the implementation of services such as spectrum sensing service or trading of transmission capacity [14, 13]. In more detail, the SUs determine requirements and policies through smart contracts, while the sensing devices later agree and join on those contracts. Hence, mobile network operators can purchase spectrum sensing services from user devices, reducing capital expenses in the deployment of spectrum sensors.

Finally, a self-organized spectrum manager can provide also identity and credibility management services for the spectrum market [102]. Service seekers are registered on-chain where their access credentials can be verified across operator borders.

Information Sharing. The rising data rates call for securely and efficiently sharing the data among users. Blockchain, providing a transparent, immutable, trustless and decentralized storage, can mitigate that sharing [41]. While storing the actual content in blockchain is likely not feasible due to the high overhead costs, blockchain can manage data access and key management in particular.

As examples, Zhang & Chen [148] and Wang et al. [124] propose solutions where access to sensitive data is managed with smart contracts, while Bhaskaran et al. [18] study smart contracts on a permissioned blockchain to manage user consent.

Resource Management. Decentralized, heterogeneous networks in 5G and 6G require the distribution of computation, capacity, and bandwidth, calling for efficient resource management. However, current resource management solutions are centralized, introducing single points of failure.

As an example, blockchain radio access network [65, 75] balances spectrum usage in a mobile network. A smart contract controls access to the network based on cost, demand, and service time.

Interference Management. Devices operating on the same spectrum in a small cell may interfere with each other's connections, reducing overall quality of service. El Gamal & El Gamal aim to reduce interference with a blockchain based incentivization scheme [39]. Further, blockchain can provide a distributed database for cross-tier interference and control access to that data for the benefit of user devices [73].

D2D communication. Device-to-Device (D2D) communication is expected to rise significantly in volume in the coming years [54], especially due to the fast growth in the deployment of IoT devices. Blockchain can provide D2D communication with a trustless environment, authenticating and authorizing the parties, caching data, and ensuring the integrity of the communication [57, 147].

Network Slicing. Network slicing is a method for creating virtual communication channels over the physical mobile network with predictable key performance indicators, targeted for customers and use cases requiring guaranteed performance such as critical communication networks [52]. As a use case for NVF, network slicing provides a unified view of VNFs and virtual networks [3].

A number of studies have proposed using blockchain for network slicing brokering and resource management in a secure, automatic, and scalable manner [143, 2, 103]. Further, blockchain can provide a trustless environment for stakeholders [92].

5 Challenges

While providing numerous opportunities, the integration of blockchain with 6G mobile networks is not without its challenges, especially in terms of privacy, security and performance. Indeed, while the inherent transparency of blockchain builds trust and promotes verifiability and traceability, it may also impact the privacy of the participants.

Further, the security of blockchain systems is not solely based on cryptographic algorithms, but also on the safety and liveness of the consensus. Safety guarantees the agreement of the network in the presence of multiple faulty participants. Liveness ensures that the network always decides for the acceptance or the rejection of a message. These characteristics are related to properties of the consensus such as validity, integrity/agreement, and termination [27, 104]. By the consensus mechanism we achieve decentralization, but lose performance.

Indeed, the effect on performance is one of the main research questions regarding the application of blockchain in 6G. Blockchain is not optimal for applications that require very low latency. In particular, the consensus mechanism requires significant local computations with verifications, proposals, consensus computations, and related cryptographic tasks. Moreover, without centralized authorities, blockchain protocols incur a heavy overhead cost for bandwidth due to the transmissions required to build consensus. For example, blockchain transactions are transmitted twice to all participants, first at the transaction and then in the confirmed block. Further, while cryptographic protocols such as zero-knowledge argument schemes can mitigate the privacy issues, their application will further affect the performance of the system.

Finally, forks also hurt blockchain performance, as multiple blocks may need to be collected before data on the chain can be considered valid [122]. For example, Bitcoin's fork solution is a collection of seven consecutive blocks before the decision on a valid block [26]. Due to the awaiting period of block-sequence, the system can decide on the branch gaining the most approval of participants. For example, in Bitcoin, the longest branch gathers the attention of the most powerful computation of the system.

Nevertheless, a PoW consensus similar to Bitcoin will not be optimal for the applications envisioned for 6G due to the massive computational overhead required. A more efficient consensus mechanism with less latency on the block confirmation is needed. There are alternatives such as proof-of-stake, but research is needed to determine their efficiency for the services presented in this chapter.

6 Conclusion

Blockchain is a potential technology for the next generation of mobile networks. 6G expands the scope and applications of blockchain with unprecedented speed, capacity, latency, and connectivity. In return, blockchain offers 6G services with decentralization, trustlessness, transparency, integrity of data, and self-organization.

We introduced the main aspects of blockchain technology, including architecture, data models, and vulnerabilities. We highlighted a number of applications related to mobile networks, and considered the intersection of 6G and blockchain in relation to enabling technologies and 6G services. Finally, we discussed the challenges inherent in blockchain-based applications, especially in terms of privacy, security and performance.

7 Acknowledgements

This work is supported by TrustedMaaS and B-TEA projects by the Infotech institute of the University of Oulu, and the Academy of Finland 6Genesis Flagship (grant 318927).

References

1. Aazhang, B., Ahokangas, P., Lovén, L., et al.: Key drivers and research challenges for 6G ubiquitous wireless intelligence (white paper), 1 edn. 6G Flagship, University of Oulu, Oulu, Finland (2019)
2. Adhikari, A., Rawat, D.B., Song, M.: Wireless network virtualization by leveraging blockchain technology and machine learning. In: Proceedings of the ACM Workshop on Wireless Security and Machine Learning, pp. 61–66 (2019)
3. Afolabi, I., Taleb, T., Samdanis, K., Ksentini, A., Flinck, H.: Network slicing and softwarization: A survey on principles, enabling technologies, and solutions. IEEE Communications Surveys & Tutorials **20**(3), 2429–2453 (2018)
4. Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., Gurtov, A.: Overview of 5g security challenges and solutions. IEEE Communications Standards Magazine **2**(1), 36–43 (2018)
5. Alexopoulos, N., Daubert, J., Mühlhäuser, M., Habib, S.M.: Beyond the hype: On using blockchains in trust management for authentication. In: 2017 IEEE Trustcom/BigDataSE/ICESS, pp. 546–553. IEEE (2017)
6. Ali, S., Wang, G., Bhuiyan, M.Z.A., Jiang, H.: Secure data provenance in cloud-centric internet of things via blockchain smart contracts. In: 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), pp. 991–998. IEEE (2018)
7. Alvarenga, I.D., Rebello, G.A., Duarte, O.C.M.: Securing configuration management and migration of virtual network functions using blockchain. In: NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium, pp. 1–9. IEEE (2018)
8. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al.: Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the thirteenth EuroSys conference, pp. 1–15 (2018)
9. Atzei, N., Bartoletti, M., Cimoli, T.: A survey of attacks on ethereum smart contracts (sok). In: International conference on principles of security and trust, pp. 164–186. Springer (2017)
10. Axon, L., Goldsmith, M.: Pb-pki: A privacy-aware blockchain-based pki (2016)

11. Barbieri, M., Gassen, D.: Blockchain-can this new technology really revolutionize the land registry system? In: Responsible Land Governance: Towards an Evidence Based Approach: Proceedings of the Annual World Bank Conference on Land and Poverty, pp. 1–13 (2017)
12. Bayer, D., Haber, S., Stornetta, W.S.: Improving the efficiency and reliability of digital time-stamping. In: Sequences II, pp. 329–334. Springer (1993)
13. Bayhan, S., Zubow, A., Gawłowicz, P., Wolisz, A.: Smart contracts for spectrum sensing as a service. IEEE Transactions on Cognitive Communications and Networking **5**(3), 648–660 (2019)
14. Bayhan, S., Zubow, A., Wolisz, A.: Spass: Spectrum sensing as a service via smart contracts. In: 2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), pp. 1–10. IEEE (2018)
15. Bellare, M., Yee, B.: Forward-security in private-key cryptography. In: Cryptographers' Track at the RSA Conference, pp. 1–18. Springer (2003)
16. Bellini, E., Iraqi, Y., Damiani, E.: Blockchain-based distributed trust and reputation management systems: a survey. IEEE Access **8**, 21127–21151 (2020)
17. Belotti, M., Božić, N., Pujolle, G., Secci, S.: A vademecum on blockchain technologies: When, which, and how. IEEE Communications Surveys & Tutorials **21**(4), 3796–3838 (2019)
18. Bhaskaran, K., Ilfrich, P., Liffman, D., Vecchiola, C., Jayachandran, P., Kumar, A., Lim, F., Nandakumar, K., Qin, Z., Ramakrishna, V., et al.: Double-blind consent-driven data sharing on blockchain. In: 2018 IEEE International Conference on Cloud Engineering (IC2E), pp. 385–391. IEEE (2018)
19. Brown, K.: Announcing approval of federal information processing standard (fips) 197, advanced encryption standard (aes). National Institute of Standards and Technology, Commerce (2002)
20. Brown, R.G., Carlyle, J., Grigg, I., Hearn, M.: Corda: an introduction. R3 CEV, August **1**, 15 (2016)
21. Burkhardt, F., Patachia, C., Lovén, L., et al.: 6G white paper on validation and trials for verticals towards 2030's. 6G Flagship, University of Oulu, Oulu, Finland (2020)
22. Castro, M., Liskov, B., et al.: Practical byzantine fault tolerance. In: OSDI, vol. 99, pp. 173–186 (1999)
23. Chen, H., Pendleton, M., Njilla, L., Xu, S.: A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. ACM Computing Surveys (CSUR) **53**(3), 1–43 (2020)
24. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. Ieee Access **4**, 2292–2303 (2016)
25. Cocks, C.C.: A note on non-secret encryption. CESG Memo (1973)
26. Conti, M., Kumar, E.S., Lal, C., Ruj, S.: A survey on security and privacy issues of bitcoin. IEEE Communications Surveys & Tutorials **20**(4), 3416–3452 (2018)
27. Coulouris, G.F., Dollimore, J., Kindberg, T.: Distributed systems: concepts and design. pearson education (2005)
28. Cucurull, J., Puiggalí, J.: Distributed immutabilization of secure logs. In: International Workshop on Security and Trust Management, pp. 122–137. Springer (2016)
29. Dai, W.: B-money. Consulted **1**, 2012 (1998)
30. Dai, Y., Xu, D., Maharjan, S., Chen, Z., He, Q., Zhang, Y.: Blockchain and deep reinforcement learning empowered intelligent 5g beyond. IEEE Network **33**(3), 10–17 (2019)
31. Daniel, D., Ifejika Speranza, C.: The role of blockchain in documenting land users' rights: The canonical case of farmers in the vernacular land market. Frontiers in blockchain **3**, 19 (2020)
32. Davenport, R.: Distributed database technology—a survey. Computer Networks (1976) **2**(3), 155–167 (1978)
33. DOCOMO, N.: White paper 5g evolution and 6g. Accessed on **1** (2020)
34. Doku, R., Rawat, D.B., Liu, C.: Towards federated learning approach to determine data relevance in big data. In: 2019 IEEE 20th International Conference on Information Reuse and Integration for Data Science (IRI), pp. 184–192. IEEE (2019)

35. Dorigo, M., et al.: Blockchain technology for robot swarms: A shared knowledge and reputation management system for collective estimation. In: Swarm Intelligence: 11th International Conference, ANTS 2018, Rome, Italy, October 29–31, 2018, Proceedings, vol. 11172, p. 425. Springer (2018)
36. Douceur, J.R.: The sybil attack. In: International workshop on peer-to-peer systems, pp. 251–260. Springer (2002)
37. Dujak, D., Sajter, D.: Blockchain applications in supply chain. In: SMART supply network, pp. 21–46. Springer (2019)
38. Dwork, C., Naor, M.: Pricing via processing or combatting junk mail. In: Annual International Cryptology Conference, pp. 139–147. Springer (1992)
39. El Gamal, A., El Gamal, H.: A single coin monetary mechanism for distributed cooperative interference management. IEEE Wireless Communications Letters **8**(3), 757–760 (2019)
40. Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM **61**(7), 95–102 (2018)
41. Fan, K., Ren, Y., Wang, Y., Li, H., Yang, Y.: Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5g. IET Communications **12**(5), 527–532 (2017)
42. Fanning, S., Parker, S.: Napster (1999)
43. Finney, H.: Rpow-reusable proofs of work. Internet: https://cryptome. org/rpow. htm (2004)
44. Fromknecht, C., Velicanu, D., Yakoubov, S.: A decentralized public key infrastructure with identity retention. IACR Cryptol. ePrint Arch. **2014**, 803 (2014)
45. Fuji, R., Usuzaki, S., Aburada, K., Yamaba, H., Katayama, T., Park, M., Shiratori, N., Okazaki, N.: Investigation on sharing signatures of suspected malware files using blockchain technology. In: International Multi Conference of Engineers and Computer Scientists (IMECS), pp. 94–99 (2019)
46. Gu, J., Sun, B., Du, X., Wang, J., Zhuang, Y., Wang, Z.: Consortium blockchain-based malware detection in mobile devices. IEEE Access **6**, 12118–12128 (2018)
47. Guo, S., Hu, X., Guo, S., Qiu, X., Qi, F.: Blockchain meets edge computing: A distributed and trusted authentication system. IEEE Transactions on Industrial Informatics **16**(3), 1972–1983 (2019)
48. Haavisto, J., Arif, M., Lovén, L., Leppänen, T., Riekki, J.: Open-source rans in practice: an over-the-air deployment for 5g mec. arXiv preprint arXiv:1905.03883 (2019)
49. Haber, S., Stornetta, W.S.: How to time-stamp a digital document. In: Conference on the Theory and Application of Cryptography, pp. 437–455. Springer (1990)
50. Hari, A., Lakshman, T.: The internet blockchain: A distributed, tamper-resistant transaction framework for the internet. In: Proceedings of the 15th ACM Workshop on Hot Topics in Networks, pp. 204–210 (2016)
51. Hölbl, M., Kompara, M., Kamišalić, A., Nemec Zlatolas, L.: A systematic review of the use of blockchain in healthcare. Symmetry **10**(10), 470 (2018)
52. Höyhtyä, M., Lähetkangas, K., et al.: Critical Communications Over Mobile Operators' Networks: 5G Use Cases Enabled by Licensed Spectrum Sharing, Network Slicing and QoS Control. IEEE Access **6**, 73572–73582 (2018). DOI 10.1109/ACCESS.2018.2883787
53. Jakobsson, M., Juels, A.: Proofs of work and bread pudding protocols. In: Secure Information Networks, pp. 258–272. Springer (1999)
54. Jameel, F., Hamid, Z., Jabeen, F., Zeadally, S., Javed, M.A.: A survey of device-to-device communications: Research issues and challenges. IEEE Communications Surveys & Tutorials **20**(3), 2133–2168 (2018)
55. Javarone, M.A., Wright, C.S.: From bitcoin to bitcoin cash: a network analysis. In: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, pp. 77–81 (2018)
56. Jeong, S., Dao, N.N., Lee, Y., Lee, C., Cho, S.: Blockchain based billing system for electric vehicle and charging station. In: 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 308–310. IEEE (2018)

57. Jiang, L., Xie, S., Maharjan, S., Zhang, Y.: Joint transaction relaying and block verification optimization for blockchain empowered d2d communication. IEEE Transactions on Vehicular Technology **69**(1), 828–841 (2019)
58. Kang, J., Xiong, Z., Niyato, D., Xie, S., Zhang, J.: Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory. IEEE Internet of Things Journal **6**(6), 10700–10714 (2019)
59. Karaarslan, E., Adiguzel, E.: Blockchain based dns and pki solutions. IEEE Communications Standards Magazine **2**(3), 52–57 (2018)
60. Kim, H., Park, J., Bennis, M., Kim, S.L.: Blockchained on-device federated learning. IEEE Communications Letters (2019)
61. Kotobi, K., Bilén, S.G.: Blockchain-enabled spectrum access in cognitive radio networks. In: 2017 Wireless Telecommunications Symposium (WTS), pp. 1–6. IEEE (2017)
62. Kotobi, K., Bilen, S.G.: Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access. ieee vehicular technology magazine **13**(1), 32–39 (2018)
63. Kuo, T.T., Kim, H.E., Ohno-Machado, L.: Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association **24**(6), 1211–1220 (2017)
64. Lamport, L., Shostak, R., Pease, M.: The byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS) **4**(3), 382–401 (1982)
65. Le, Y., Ling, X., Wang, J., Ding, Z.: Prototype design and test of blockchain radio access network. In: 2019 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1–6. IEEE (2019)
66. Lee, Y., Lee, K.M., Lee, S.H.: Blockchain-based reputation management for custom manufacturing service in the peer-to-peer networking environment. Peer-to-Peer Networking and Applications **13**(2), 671–683 (2020)
67. Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C.P.A., Sun, Z.: Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal **4**(6), 1832–1843 (2017)
68. Li, J., Krohn, M.N., Mazieres, D., Shasha, D.E.: Secure untrusted data repository (sundr). In: OSDI, vol. 4, pp. 9–9 (2004)
69. Li, L., Liu, J., Cheng, L., Qiu, S., Wang, W., Zhang, X., Zhang, Z.: Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Transactions on Intelligent Transportation Systems **19**(7), 2204–2220 (2018)
70. Li, M., Weng, J., Yang, A., Lu, W., Zhang, Y., Hou, L., Liu, J.N., Xiang, Y., Deng, R.H.: Crowdbc: A blockchain-based decentralized framework for crowdsourcing. IEEE Transactions on Parallel and Distributed Systems **30**(6), 1251–1266 (2018)
71. Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q.: A survey on the security of blockchain systems. Future Generation Computer Systems (2017)
72. Liang, Y.C.: Blockchain for dynamic spectrum management. In: Dynamic Spectrum Management, pp. 121–146. Springer (2020)
73. Lin, D., Tang, Y.: Blockchain consensus based user access strategies in d2d networks for data-intensive applications. IEEE Access **6**, 72683–72690 (2018)
74. Lin, I.C., Liao, T.C.: A survey of blockchain security issues and challenges. IJ Network Security **19**(5), 653–659 (2017)
75. Ling, X., Wang, J., Bouchoucha, T., Levy, B.C., Ding, Z.: Blockchain radio access network (b-ran): Towards decentralized secure radio access paradigm. IEEE Access **7**, 9714–9723 (2019)
76. Liu, Y., Yu, F.R., Li, X., Ji, H., Leung, V.C.: Resource allocation for video transcoding and delivery based on mobile edge computing and blockchain. In: 2018 IEEE Global Communications Conference (GLOBECOM), pp. 1–6. IEEE (2018)
77. Liu, Y., Yu, F.R., Li, X., Ji, H., Leung, V.C.: Decentralized resource allocation for video transcoding and delivery in blockchain-based system with mobile edge computing. IEEE Transactions on Vehicular Technology **68**(11), 11169–11185 (2019)

78. Longo, R., Pintore, F., Rinaldo, G., Sala, M.: On the security of the blockchain bix protocol and certificates. In: 2017 9th International Conference on Cyber Conflict (CyCon), pp. 1–16. IEEE (2017)
79. Lovén, L., Leppänen, T., Peltonen, E., Partala, J., Harjula, E., Porambage, P., Ylianttila, M., Riekki, J.: Edgeai: A vision for distributed, edge-native artificial intelligence in future 6g networks. In: The 1st 6G Wireless Summit, pp. 1–2. Levi, Finland (2019)
80. Lu, Y., Huang, X., Dai, Y., Maharjan, S., Zhang, Y.: Blockchain and federated learning for privacy-preserved data sharing in industrial iot. IEEE Transactions on Industrial Informatics **16**(6), 4177–4186 (2019)
81. Lu, Y., Zheng, X.: 6g: A survey on technologies, scenarios, challenges, and the related issues. Journal of Industrial Information Integration p. 100158 (2020)
82. Ma, M., Shi, G., Li, F.: Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the iot scenario. IEEE Access **7**, 34045–34059 (2019)
83. Malomo, O.O., Rawat, D.B., Garuba, M.: Next-generation cybersecurity through a blockchain-enabled federated cloud framework. The Journal of Supercomputing **74**(10), 5099–5126 (2018)
84. Mazieres, D., Shasha, D.: Building secure file systems out of byzantine storage. In: Proceedings of the twenty-first annual symposium on Principles of distributed computing, pp. 108–117 (2002)
85. Mell, P., Grance, T.: The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology (2012)
86. Merkle, R.C.: A digital signature based on a conventional encryption function. In: Conference on the theory and application of cryptographic techniques, pp. 369–378. Springer (1987)
87. Muratov, F., Lebedev, A., Iushkevich, N., Nasrulin, B., Takemiya, M.: Yac: Bft consensus algorithm for blockchain. arXiv preprint arXiv:1809.00554 (2018)
88. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)
89. Nguyen, D.C., Pathirana, P.N., Ding, M., Seneviratne, A.: Blockchain for 5g and beyond networks: A state of the art survey. Journal of Network and Computer Applications p. 102693 (2020)
90. Nguyen, T., Tran, N., Loven, L., Partala, J., Kechadi, M.T., Pirttikangas, S.: Privacy-aware blockchain innovation for 6g: Challenges and opportunities. In: 2020 2nd 6G Wireless Summit (6G SUMMIT), pp. 1–5. IEEE (2020)
91. Nguyen, T.H., Partala, J., Pirttikangas, S.: Blockchain-based mobility-as-a-service. In: 2019 28th International Conference on Computer Communication and Networks (ICCCN), pp. 1–6. IEEE (2019)
92. Nour, B., Ksentini, A., Herbaut, N., Frangoudis, P.A., Moungla, H.: A blockchain-based network slice broker for 5g services. IEEE Networking Letters **1**(3), 99–102 (2019)
93. Noyes, C.: Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning. arXiv preprint arXiv:1601.01405 (2016)
94. Orman, H.: Blockchain: The emperors new pki? IEEE Internet Computing **22**(2), 23–28 (2018)
95. Pei, Y., Hu, S., Zhong, F., Niyato, D., Liang, Y.C.: Blockchain-enabled dynamic spectrum access: cooperative spectrum sensing, access and mining. In: 2019 IEEE Global Communications Conference (GLOBECOM), pp. 1–6. IEEE (2019)
96. Peltonen, E., Bennis, M., Capobianco, M., Debbah, M., Ding, A., Gil-Castiñeira, F., Jurmu, M., Karvonen, T., Kelanti, M., Kliks, A., et al.: 6g white paper on edge intelligence. arXiv preprint arXiv:2004.14850 (2020)
97. Perboli, G., Musso, S., Rosano, M.: Blockchain in logistics and supply chain: A lean approach for designing real-world use cases. IEEE Access **6**, 62018–62028 (2018)
98. Popov, S.: The tangle. cit. on p. 131 (2016)
99. Pourmajidi, W., Miranskyy, A.: Logchain: blockchain-assisted log storage. In: 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 978–982. IEEE (2018)

100. Preuveneers, D., Rimmer, V., Tsingenopoulos, I., Spooren, J., Joosen, W., Ilie-Zudor, E.: Chained anomaly detection models for federated learning: An intrusion detection case study. Applied Sciences **8**(12), 2663 (2018)
101. Rahman, M.A., Rashid, M.M., Hossain, M.S., Hassanain, E., Alhamid, M.F., Guizani, M.: Blockchain and iot-based cognitive edge framework for sharing economy services in a smart city. IEEE Access **7**, 18611–18621 (2019)
102. Raju, S., Boddepalli, S., Gampa, S., Yan, Q., Deogun, J.S.: Identity management using blockchain for cognitive cellular networks. In: 2017 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE (2017)
103. Rawat, D.B., Alshaikhi, A.: Leveraging distributed blockchain-based scheme for wireless network virtualization with security and qos constraints. In: 2018 International Conference on Computing, Networking and Communications (ICNC), pp. 332–336. IEEE (2018)
104. Raynal, M.: Fault-tolerant message-passing distributed systems: an algorithmic approach. Springer (2018)
105. Rebello, G.A.F., Alvarenga, I.D., Sanz, I.J., Duarte, O.C.M.: Bsec-nfvo: A blockchain-based security for network function virtualization orchestration. In: ICC 2019-2019 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE (2019)
106. Reilly, D., Wren, C., Berry, T.: Cloud computing: Forensic challenges for law enforcement. In: 2010 International Conference for Internet Technology and Secured Transactions, pp. 1–7. IEEE (2010)
107. Saad, M., Anwar, A., Ahmad, A., Alasmary, H., Yuksel, M., Mohaisen, A.: Routechain: Towards blockchain-based secure and efficient bgp routing. In: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 210–218. IEEE (2019)
108. Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D.H., Mohaisen, D.: Exploring the attack surface of blockchain: A comprehensive survey. IEEE Communications Surveys & Tutorials (2020)
109. Saad, W., Bennis, M., Chen, M.: A vision of 6g wireless systems: Applications, trends, technologies, and open research problems. arXiv preprint arXiv:1902.10265 (2019)
110. Schaub, A., Bazin, R., Hasan, O., Brunie, L.: A trustless privacy-preserving reputation system. In: IFIP International Conference on ICT Systems Security and Privacy Protection, pp. 398–411. Springer (2016)
111. Shae, Z., Tsai, J.: Transform blockchain into distributed parallel computing architecture for precision medicine. In: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), pp. 1290–1299. IEEE (2018)
112. Sharma, S.K., Bogale, T.E., Le, L.B., Chatzinotas, S., Wang, X., Ottersten, B.: Dynamic spectrum sharing in 5g wireless networks with full-duplex technology: Recent advances and research challenges. IEEE Communications Surveys & Tutorials **20**(1), 674–707 (2017)
113. Sharples, M., Domingue, J.: The blockchain and kudos: A distributed system for educational record, reputation and reward. In: European conference on technology enhanced learning, pp. 490–496. Springer (2016)
114. Strinati, E.C., Barbarossa, S., Gonzalez-Jimenez, J.L., Kténas, D., Cassiau, N., Dehos, C.: 6g: The next frontier. arXiv preprint arXiv:1901.03239 (2019)
115. Sutton, A., Samavi, R.: Blockchain enabled privacy audit logs. In: International Semantic Web Conference, pp. 645–660. Springer (2017)
116. Szabo, N.: The idea of smart contracts. Nick Szabo's Papers and Concise Tutorials **6** (1997)
117. Szabo, N.: Bit gold.(2005) (2005)
118. Thakur, V., Doja, M., Dwivedi, Y.K., Ahmad, T., Khadanga, G.: Land records on blockchain for implementation of land titling in india. International Journal of Information Management **52**, 101940 (2020)
119. Tian, F.: An agri-food supply chain traceability system for china based on rfid & blockchain technology. In: 2016 13th international conference on service systems and service management (ICSSSM), pp. 1–6. IEEE (2016)
120. Tijan, E., Aksentijević, S., Ivanić, K., Jardas, M.: Blockchain technology implementation in logistics. Sustainability **11**(4), 1185 (2019)

121. Vyshegorodtsev, M., Miyamoto, D., Wakahara, Y.: Reputation scoring system using an economic trust model: a distributed approach to evaluate trusted third parties on the internet. In: 2013 27th International Conference on Advanced Information Networking and Applications Workshops, pp. 730–737. IEEE (2013)
122. Wan, L., Eyers, D., Zhang, H.: Evaluating the impact of network latency on the safety of blockchain transactions. In: 2019 IEEE International Conference on Blockchain (Blockchain), pp. 194–201. IEEE (2019)
123. Wang, J., Wu, L., Choo, K.K.R., He, D.: Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure. IEEE Transactions on Industrial Informatics **16**(3), 1984–1992 (2019)
124. Wang, S., Zhang, Y., Zhang, Y.: A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. Ieee Access **6**, 38437–38450 (2018)
125. Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y., Kim, D.I.: A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access **7**, 22328–22370 (2019)
126. Weiss, M.B., Werbach, K., Sicker, D.C., Bastidas, C.E.C.: On the application of blockchains to spectrum management. IEEE Transactions on Cognitive Communications and Networking **5**(2), 193–205 (2019)
127. Weng, J., Weng, J., Zhang, J., Li, M., Zhang, Y., Luo, W.: Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive. IEEE Transactions on Dependable and Secure Computing (2019)
128. Wood, G., et al.: Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper **151**(2014), 1–32 (2014)
129. Wu, J., Zhang, Z., Hong, Y., Wen, Y.: Cloud radio access network (c-ran): a primer. IEEE Network **29**(1), 35–41 (2015)
130. Xia, C., Chen, H., Liu, X., Wu, J., Chen, L.: Etra: Efficient three-stage resource allocation auction for mobile blockchain in edge computing. In: 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), pp. 701–705. IEEE (2018)
131. Xiao, Y., Zhang, N., Lou, W., Hou, Y.T.: A survey of distributed consensus protocols for blockchain networks. IEEE Communications Surveys & Tutorials **22**(2), 1432–1465 (2020)
132. Xie, J., Tang, H., Huang, T., Yu, F.R., Xie, R., Liu, J., Liu, Y.: A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Communications Surveys & Tutorials **21**(3), 2794–2830 (2019)
133. Yang, H., Liang, Y., Yuan, J., Yao, Q., Yu, A., Zhang, J.: Distributed blockchain-based trusted multi-domain collaboration for mobile edge computing in 5g and beyond. IEEE Transactions on Industrial Informatics (2020)
134. Yang, H., Wu, Y., Zhang, J., Zheng, H., Ji, Y., Lee, Y.: Blockonet: blockchain-based trusted cloud radio over optical fiber network for 5g fronthaul. In: Optical Fiber Communication Conference, pp. W2A–25. Optical Society of America (2018)
135. Yang, H., Yuan, J., Yao, H., Yao, Q., Yu, A., Zhang, J.: Blockchain-based hierarchical trust networking for jointcloud. IEEE Internet of Things Journal **7**(3), 1667–1677 (2019)
136. Yang, H., Zheng, H., Zhang, J., Wu, Y., Lee, Y., Ji, Y.: Blockchain-based trusted authentication in cloud radio over fiber network for 5g. In: 2017 16th International Conference on Optical Communications and Networks (ICOCN), pp. 1–3. IEEE (2017)
137. Yang, P., Xiao, Y., Xiao, M., Li, S.: 6g wireless communications: Vision and potential techniques. IEEE Network **33**(4), 70–75 (2019)
138. Yang, Q., Liu, Y., Chen, T., Tong, Y.: Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST) **10**(2), 1–19 (2019)
139. Yang, R., Yu, F.R., Si, P., Yang, Z., Zhang, Y.: Integrated blockchain and edge computing systems: A survey, some research issues and challenges. IEEE Communications Surveys & Tutorials **21**(2), 1508–1532 (2019)
140. Yang, Z., Yang, K., Lei, L., Zheng, K., Leung, V.C.: Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things Journal **6**(2), 1495–1505 (2018)

141. Ylianttila, M., Kantola, R., Gurtov, A., Mucchi, L., Oppermann, I., Yan, Z., Nguyen, T.H., Liu, F., Hewa, T., Liyanage, M., et al.: 6g white paper: Research challenges for trust, security and privacy. arXiv preprint arXiv:2004.11665 (2020)
142. Yu, J., Ryan, M.: Evaluating web pkis. In: Software Architecture for Big Data and the Cloud, pp. 105–126. Elsevier (2017)
143. Zanzi, L., Albanese, A., Sciancalepore, V., Costa-Pérez, X.: Nsbchain: A secure blockchain framework for network slicing brokerage. arXiv preprint arXiv:2003.07748 (2020)
144. Zawoad, S., Dutta, A., Hasan, R.: Towards building forensics enabled cloud through secure logging-as-a-service. IEEE Transactions on Dependable and Secure Computing (1), 1–1 (2016)
145. Zhang, H., Deng, E., Zhu, H., Cao, Z.: Smart contract for secure billing in ride-hailing service via blockchain. Peer-to-Peer Networking and Applications **12**(5), 1346–1357 (2019)
146. Zhang, P., Schmidt, D.C., White, J., Lenz, G.: Blockchain technology use cases in healthcare. In: Advances in computers, vol. 111, pp. 1–41. Elsevier (2018)
147. Zhang, R., Yu, F.R., Liu, J., Huang, T., Liu, Y.: Deep reinforcement learning (drl)-based device-to-device (d2d) caching with blockchain and mobile edge computing. IEEE Transactions on Wireless Communications (2020)
148. Zhang, X., Chen, X.: Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network. IEEE Access **7**, 58241–58254 (2019)
149. Zhang, Y., He, D., Choo, K.K.R.: Bads: Blockchain-based architecture for data sharing with abs and cp-abe in iot. Wireless Communications and Mobile Computing **2018** (2018)
150. Zhang, Z., Xiao, Y., Ma, Z., Xiao, M., Ding, Z., Lei, X., Karagiannidis, G.K., Fan, P.: 6g wireless networks: Vision, requirements, architecture, and key technologies. IEEE Vehicular Technology Magazine **14**(3), 28–41 (2019)
151. Zhao, K., Tang, S., Zhao, B., Wu, Y.: Dynamic and privacy-preserving reputation management for blockchain-based mobile crowdsensing. IEEE Access **7**, 74694–74710 (2019)
152. Zheng, Z., Xie, S., Dai, H.N., Wang, H.: Blockchain challenges and opportunities: A survey. Work Pap.–2016 (2016)