Blockchain

What Does It Mean to Industrial Electronics?: Technologies, Challenges, and Opportunities

Yu, Xinghuo; Tang, Changbing; Palensky, Peter; Colombo, Armando

DOI
10.1109/MIE.2021.3066332

Publication date
2022

Document Version
Final published version

Published in
IEEE Industrial Electronics Magazine

Technologies, Challenges, and Opportunities

XINGHUO YU, CHANGBING TANG, PETER PALENSKY, and ARMANDO WALTER COLOMBO

Blockchain: What Does It Mean to Industrial Electronics?

What Is Blockchain?

Imagine you want to send money to a friend overseas. Wouldn't it be good if you didn't have to pay hefty fees to the intermediaries, and your friend received the funds very quickly? Now imagine ordering parts to make a product in your manufacturing plant. Wouldn't it be great if you were able to verify where each part comes from and have access to a reliable certificate on its quality automatically? Also think about dealing with energy use or selling off your excess solar energy as a prosumer. Wouldn't it be nice if you could purchase cheaper energy or sell it profitably at ease?

Blockchain can resolve these challenges. Blockchain is a distributed ledger of transaction and data management technology that enables distributed nodes to collaboratively affirm transaction provenance via a decentralized consensus mechanism. The interest in blockchain has been increasing exponentially in both industry and academia because of its potential to revolutionize modern industries and businesses [1], [2].

The Concept of Blockchain

The term *blockchain* was coined in the 2008 article "Bitcoin: A Peer-to-Peer Electronic Cash System," by Nakamoto [3]. In a narrow sense, it is a chained data structure storing data blocks sequentially and a nontamperable and unforgeable distributed ledger that is secured cryptographically. Broadly speaking, it can be considered a new distributed infrastructure and computing paradigm using chained block data structures to store and validate data, node consensus algorithms to generate and update data, cryptography to secure data transmission and access,

Digital Object Identifier 10.1109/MIE.2021.3066332
Date of current version: 12 April 2021

1932-4529/22©2022IEEE

and smart contracts with automated scripts to program and manipulate data (Figure 1 illustrates how it works).

Currently, blockchain technology is regarded as a breakthrough that is changing the ways businesses and organizations operate [4]. Just like modern information technologies, such as big data, cloud computing, and the Internet of Things (IoT), it relies on existing technologies to deliver its promises.

The Journey of Blockchain

The development of blockchain technology has gone through three phases, namely, programmable currency, programmable finance, and programmable society, dubbed *Blockchain 1.0*, *2.0*, and *3.0*, respectively.

Soon after publishing [3], Nakamoto created software in 2009 to mine the foundation block, opening the era of Bitcoin. The initial interest in blockchain was in virtual currencies, i.e., for Blockchain 1.0, how much they were worth, how to mine, how to buy, and how to sell. A few years later, attention was placed on the technology itself, leading to a big step forward—Blockchain 2.0—marked by the publication of the "Ethereum Whitepaper" in 2013 [5].

Ethereum is a platform that offers a variety of modules allowing users to build applications. It works like building a house, where Ethereum provides building modules, such as the walls, roof, and floor, and customers need only to assemble the house using the modules. The core of Ethereum is the smart contract, which is an automated agent. However, Blockchain 2.0 could achieve only 70–80 transactions per second, which hindered its applications. Recent years have seen the emergence of Blockchain 3.0, which is a platform that is able to process the volumes of transactions necessary for mass adoption. It presents the future of blockchain: a decentralized Internet with data storage, smart contracts, cloud nodes, and open-chain networks, applicable to a wide range of fields, from finance to manufacturing, energy, logistics, medicine, and social networks. The journey of the blockchain developments is illustrated in Figure 2.

The Key Technologies of Blockchain

There are four key traditional technologies of blockchain: distributed storage, cryptography, consensus algorithms, and smart contracts (see Figure 3).

Distributed storage is used for data sharing and synchronization in a network composed of many distributed nodes in different physical addresses or organizations. Each participating node has complete data storage and is independent and peer-to-peer connected. Blockchain relies on distributed storage to ensure reliability and security of the data, and increasing the number of participating nodes would enhance their improvements. On one hand, the technology generates block hard forks to achieve transaction rollback and avoid malicious tampering of data. On the other hand, it leads to a significant increase in storage.

Cryptography is used for addressing information security issues. Famous algorithms include hashing algorithms, encryption and decryption algorithms, digital certificates and signatures, and zero-knowledge proofs [6]. Hash algorithms generate header information for each unit (block) in the blockchain. The connection between the blocks is achieved by including the previous block header information in the next block header. Meanwhile, hash-based tree structures, such as the Merkle tree, are used to organize the specific transactions or states in the block and store the summary information (root hash) in the block header, making it extremely difficult to tamper with. The storage structure of blockchain is like a zipper: after each data item is stored independently, a chain is formed, and any node can be traced. In this process, the signature is determined by cryptography, and a zero-knowledge proof plays an increasingly important role in convincing a verifier that a certain assertion is deemed correct without

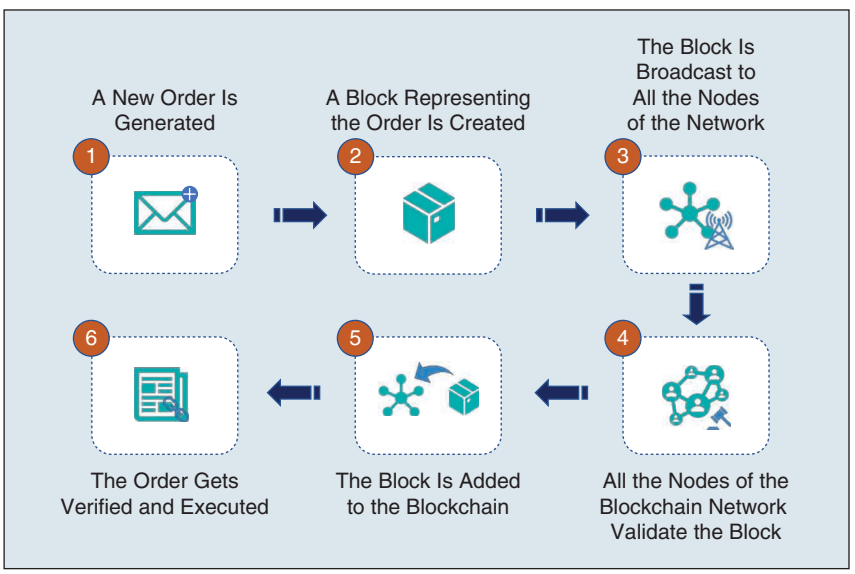

FIGURE 1 – How a blockchain works.

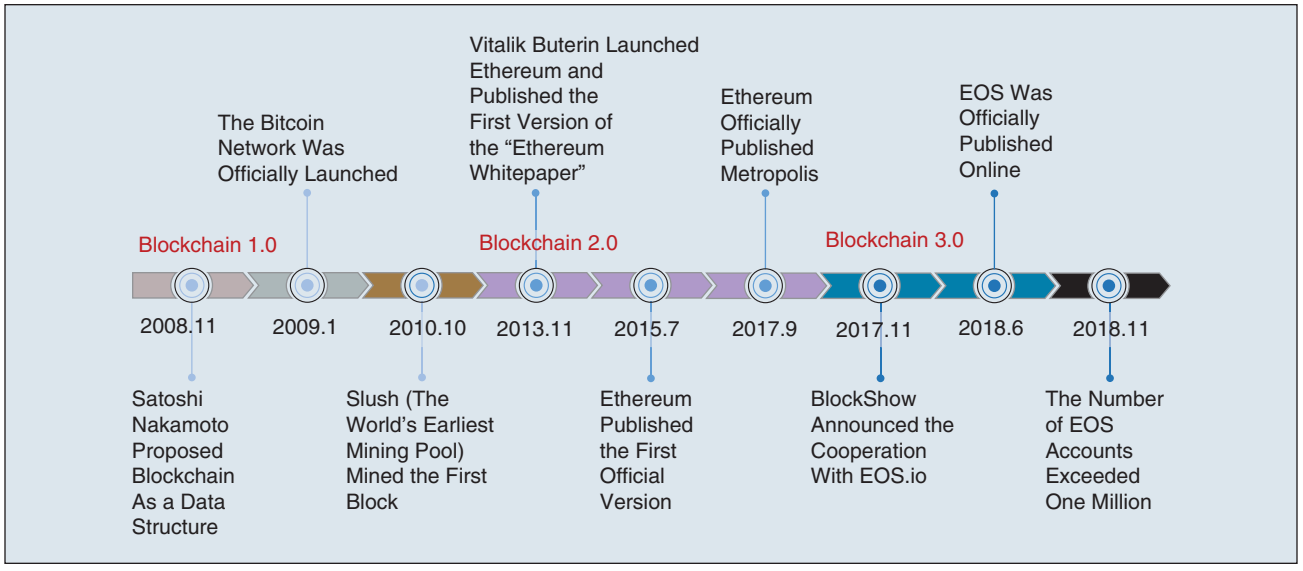

FIGURE 2 – The journey of blockchain. EOS: enterprise operating system.

providing any information to the verifier (e.g., Zcash [7] and zk-SNARKs [8]).

Consensus algorithms refer to how all nodes reach consensus to validate a record, which is used for both identification and tampering prevention to maintain decentralized multiparty mutual trust. In both public and private blockchains, all consensus algorithms achieve the same goal of determining which blocks are correct by checking how each block is added. Their differences lie in which blocks can be added on the chain at what rate, and what types of faults are allowed.

There are many different classifications for consensus algorithms [9]. According to the deployment mode, the blockchain consensus algorithms can be divided into public chain consensus, alliance chain consensus, and private chain consensus algorithms. With regard to the fault-tolerant type, they can be classified as Byzantine fault tolerant (BFT) and non-BFT. Considering the degree of consistency, they can also be divided into strong consensus and weak consensus algorithms. In this article, we classify the consensus algorithms into four types, namely, BFT-based, Proof-of-Work (PoW)-based, Proof-of-Stake (PoS)-based, and mixed-type consensus algorithms.

BFT-based consensus algorithms are based on traditional distributed consistency-checking techniques; some examples are Paxos [10], Raft [11], Practical BFT [12], Stellar Consensus Protocol [13], Algorand [14], and Sleepy Consensus [15]. PoW-based consensus algorithms aim to achieve capacity expansion of the blockchain (e.g., Bitcoin-Next Generation [16] and Elastico [17]) or improve the efficiency of the algorithm (e.g., Proof of Elapsed Time [18], Proof of Luck [19], Proof of Space [20], and Proof of Useful Work [21]). PoS-based consensus algorithms are used to solve the problem of "nothing at stake" [22], including Delegated Proof of State [23], Tendermint [24], Casper [25], and Proof of Unspent Transaction Output [26]. The mixed-type consensus algorithms draw lessons mainly from the consensus of PoW and PoS, including Proof of Stake Velocity [27], Proof of Burn [28], and Proof of Activity [29]. In short, all blockchain consensus algorithms focus primarily on three aspects: performance evaluation, adaptation and optimization, and consensus innovation under the new blockchain structure. For a comprehensive survey of various consensus algorithms, please refer to [30].

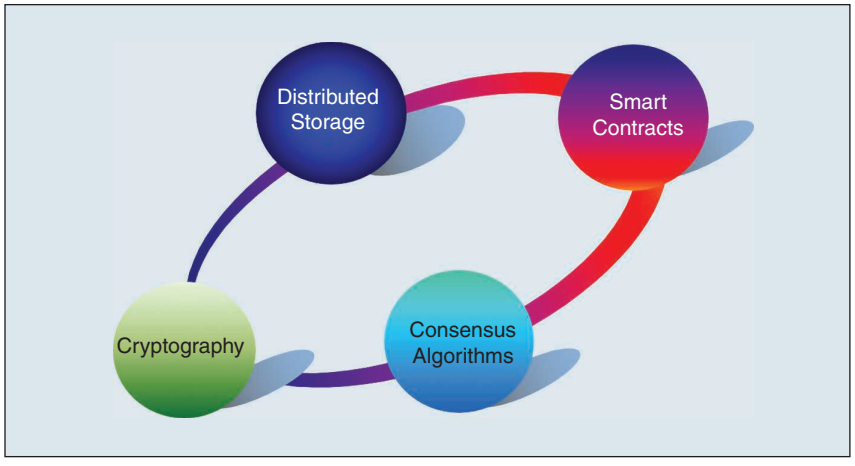

FIGURE 3 – The four key technologies of blockchain.

A smart contract refers to a computing protocol for disseminating, verifying, and performing a contract negotiation or fulfillment of a contract in an informational manner. Its concept was originated by Szabo in 1994 [31]. As a kind of embedded programming, smart contracts can be built into any blockchain data, trading, and tangible or intangible assets to form a programmable control system. The key property of a smart contract is that it does not rely on third-party or centralized

organization, which greatly reduces manual participation and cost with high efficiency and accuracy. It is noted that all smart contracts deployed on the blockchain public chain are visible and interactive, meaning that their vulnerabilities are made public.

A smart contract in blockchain is a set of codes automatically executed once an event triggers a clause in the contract. In the blockchain context, smart contracts are scripts stored on the blockchain, which are analogous to stored procedures in relational database management systems. According to the performance of the programming language or running environment, smart contracts can be divided into three types: script type, Turing-complete type, and verifiable-contract type [32]. Smart contracts have been successfully implemented on many blockchain systems, such as Ethereum [5] and Hyperledger Fabric [33]. Hyperledger Fabric has good flexibility, scalability, and versatility and supports various uncertain smart contracts and pluggable services. In short, the smart contract is implemented based on program code. Once deployed to the blockchain, it is not allowed to change, which eliminates the possibility of human intervention. However, there are still some limitations on the technology and implementation of smart contracts, especially the problems of stability and security. A comprehensive survey on this topic can be found in [34].

The Main Platforms of Blockchain

Blockchain platforms combining distributed storage, cryptography, consensus algorithms, and smart contracts together with network and data technologies are used for building blockchain-based systems. There are some quite generic platforms that can be used for different industrial domains, such as Ethereum and Hyperledger Fabric. Ethereum supports applications that use smart contracts, while Hyperledger Fabric provides good flexibility and versatility support for blockchain applications in domains such as finance, manufacturing, and logistics. Other platforms are more specialized and developed for specific domains, such as Energy Web Foundation (EWF) [35] and Obelisk [36] for smart energy systems, Provenance [37] for logistics, Gem [38] for health care, and Genesis of Things [39] for 3D manufacturing. Generally, the selection of a blockchain platform is dependent on the needs of the users. For example, multiple collaborative diverse companies can use a platform like Ethereum to implement smart contract capabilities over their network, while a group of energy providers can use one platform like EWF that supports energy trade applications.

The Key Issues and Challenges in Blockchain

Blockchain has now become a huge technical field that is profoundly changing industry, economy, and society. However, there are many issues and challenges, as discussed in the following sections.

Technological Issues

The breakthrough construction of blockchain technology is limited by a famous theory: *the impossible triangle theory*; i.e., scalability, security, and decentralization cannot be achieved at the same time (see Figure 4). For example, Bitcoin is highly decentralized and secure, but its performance (its so-called *scalability*) is very low. Because of frequent network congestion, traders have to pay more in the transaction process. Therefore, one challenge is to address the impossible triangle problem to balance scalability, security, and decentralization.

Scalability refers to the ability to handle high volumes of business data. As usual, there is always a tradeoff among costs, security, and performance. To achieve scalability, we should consider the usage context and the performance metrics, such as validation latency, transaction throughput, energy costs, computation costs, storage costs, number of nodes, and so on. For example, the throughput of a blockchain is not scalable when the network size grows. Promising solutions to improve the scalability of blockchains include primarily sharding [40] and cross-chain [41] techniques. Sharding technology is thought to be able to partition the network into different groups (shards) so that the compulsory duplication of communication, data storage, and computation overhead can be avoided for each participating node. These overheads must be incurred by all full nodes in traditional nonsharded blockchains. A cross-chain is a scheme that makes interconnection between blockchains possible. This interoperability is important for individuals and businesses as it helps them exchange values with minimal costs and risks.

Security is the most important issue for blockchain, involving software and hardware as well as protocols and messages required [42]. With the rapid development and wide application of blockchain, criminals may take advantage of the security loopholes to attack users, which exposes blockchain technology to many security threats and challenges. For example, in March 2014, some criminals used a distributed denial of service to attack the Bitcoin trading platform Mt. Gox, which resulted in 850,000 bitcoins stolen from the trading platform and more than US$450 million lost [43]. In June 2016, the Decentralized Autonomous Organization (DAO), the largest crowdfunding project of blockchain at that time, was attacked and lost about US$60 million [44].

We will now discuss the security of blockchain from the protocol layer, extension layer, and application layer perspectives. In the protocol layer, the security problems of blockchain include mainly encryption mechanism security (such as private key security), consensus mechanism security (such

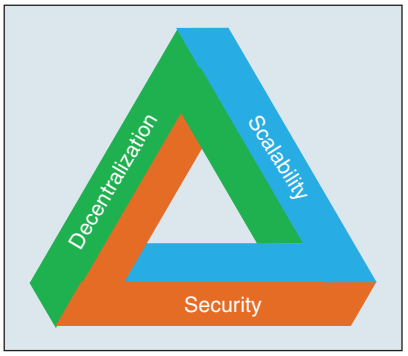

FIGURE 4 – The impossible triangle problem of blockchain.

as the double-spending attack, 51% attack, and coin age attack), and network communication security (such as the eclipse attack, routing attack, border gateway protocol attack, Sybil attack, and balance attack). In the extension layer, the security of blockchain is affected mainly by the vulnerability of the smart contract. Nikolić et al. classified the existing smart contract vulnerabilities as prodigal contracts, greedy contracts, suicidal contracts, and postmortem contracts [45]. In the application layer, when a user interacts with the blockchain system, an attacker may obtain the user's physical identity or other additional information by means of data mining, which leads to the user's privacy disclosure. The main securities include identity privacy security and transaction privacy security. For a comprehensive survey of blockchain security, please refer to [46].

Decentralization is a key to roll out blockchain applications, which may also compromise blockchain security. Most existing technologies are still centralization oriented. As an example, the Enterprise Operation System (EOS) [47] uses 21 "super nodes" to block out nodes in a certain order, thereby avoiding accounting in a large number of nodes, which would otherwise significantly increase levels in the transaction processing system. However, it has been questioned whether the power is too centralized, which is not conducive to network security. At present, because of the emergence of the Application Specific Integrated Circuit 6 (ASIC6) machine, the PC nodes of ordinary users can hardly participate in the competition of accounting rights. Besides, more than 80% of the computing power is spent on a few mining pools, in which the owners of the mining pools have considerable disbursement power in the Bitcoin world.

Regulatory and Legal Issues

While many countries are actively supporting adoption of the blockchain technology, there are no comprehensive regulations and industry standards yet. Currently, regulations for blockchain are mainly in the finance sector for combating crimes such as money laundering, extortion, and black-market transactions. For example, a total of US$761 million in digital currency was stolen by hackers from digital currency exchanges around the world in the first six months of 2018, according to CipherTrace, a U.S. digital currency security company. In comparison, only US$266 million was lost in 2017. China announced a ban on initial coin offering and shut down all domestic cryptocurrency exchanges in 2019 [48], leading to the challenge of using blockchain without digital currency. Furthermore, the technical rules themselves need to be regulated. The "distrusting" functions of blockchain cannot overcome the "dishonesty" problem of the technology setting itself, and the imbalance of rules wrapped in technology makes the regulation more difficult because of privacy concerns.

There are also significant legal issues in the context of docking and coordination within the existing legal systems. At present, there is no commonly accepted definition of a blockchain in legal systems or an agreement on which attributes are indispensable in each country. Furthermore, most current discussions on smart contracts are focused on how to implement programmable finance and replace intermediaries, ignoring the coordination and compatibility of smart contracts within existing legal systems, especially contracting laws. The ambiguity of semantic expressions and the variability of objective conditions require definitive legal interpretations, which are usually done by a credible third party (a law firm). But smart contracts completely depend on computer languages to stipulate authentication and execution among parties, begging the questions of whether the semantics of the contract terms can accurately express the intentions of the parties and whether the smart contracts can be legally recognized. Furthermore, during the execution of smart contracts, everything needs to comply with the preset code, regardless of the wishes of the parties. A mistake or change would require enormous effort to change the program code. The so-called *smart* contract is not so smart in this instance.

Other Challenges

Blockchain technology is still in its infancy, though it has broad appeal. Another challenge lies in its scalability when many participants are involved. Currently, the transaction chain is long, the centralization efficiency is low, the transparency is not transparent, and trust is lacking. These issues will have to be overcome for blockchain to become an important enabling technology in the emerging digital economy and society.

In terms of technology, the aspects of parallelization, consensus, cross-chain, and channel technologies are very important for the future. There has already been some good progress, including cryptographic security (such as zero-knowledge proofs [49] and ring signatures [50]), consensus mechanisms (such as verifiable random functions [51]), the infrastructure of blockchain (such as multichain, channel technology, and directed acyclic graphs), distributed file systems [such as InterPlanetary File System (IPFS) [52]], and identity management [such as decentralized identifiers (DIDs) [53] and self-sovereign identity (SSI) [54]], among others. For example, IPFS is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files, which makes storing and sharing large files more efficient. IPFS provides a high-throughput, content-addressed block storage model with content-addressed hyperlinks. A DID is a new type of identifier that enables verifiable, decentralized digital identity. Compared to typical, federated identifiers, DIDs have been designed so that they may be decoupled from identity providers, centralized registries, and certificate authorities. SSI is a new type of identity management, in which identity and the valuable data generated belong to the users themselves. SSI allows users to manage their own information by themselves, independently of any organizations.

In terms of applications, the current blockchain is still in the 2.0 stage, namely "application + blockchain," which refers to the interactions between the traditional services and blockchain services. Blockchain 3.0 is emerging, in

which all business operations would run on blockchains based on smart contracts in a decentralized manner.

Blockchain for Industrial Electronics

The fast development of blockchain has had a far-reaching impact on many areas, including technological, social, and economic fields. The field of industrial electronics (IE) is no exception. IE tackles the challenges in intelligent and computer control systems, robotics, factory communications and automation, flexible manufacturing, data acquisition and signal processing, vision systems, and power electronics. Key thematic areas, such as power and energy systems, manufacturing systems, robotics and mechatronics, and so on, are being impacted by blockchain, as we now briefly describe.

Power and Energy Systems

The power and energy sector is much affected by blockchain, just as any other sector [1], though things are usually happening a bit more slowly. Power networks are considered to be cyber-physical systems [55] or, if prosumers and community/society are included in the equation, cyber-physical-social systems (CPSSs). Blockchain technology, according to its promises, has a big future. Figure 5 shows how blockchain can be used in power-sharing applications. A prosumer first enters a contract as a user node through the blockchain network, where the seller's information is made available, while edge nodes equipped with certain computing and storage capabilities serve as miners to maintain the blockchain network. In each block generation cycle, the seller publishes its information of energy surplus to the network, and consumers then bid for the selling energy with successful bidder(s) chosen, and the amount of energy is then allowed for use. The transaction process is automatically completed by the smart contract, where the purchased energy flows from the seller to the buyer through the public grid, and the seller gets a payoff. Finally, the miners in the network package all of the transactions during this period. They then verify the transactions through consensus and generate new data blocks that are then added to the blockchain automatically as secured records.

However, the special features of power and energy CPSSs may mean that various parts of the blockchain technology need to be made more flexible and less resource intensive as the general blockchain technology is not entirely designed for power and energy systems. For example, there would be stringent requirements of power and energy CPSSs to be dynamically responsive across the three layers of the cyber, physical, and social worlds and also to be robust against intermittent uncertainties, such as renewable energies and electric vehicles. The uptake of blockchain in power and energy CPSSs requires a strong willingness of the community and industry to make it work under the increasingly uncertain and insecure environments as well as in the economic considerations of return of investments to utilities.

For example, currently the need for a "real" (i.e., distributed) blockchain may not always be there since the resource to be managed by the blockchain (e.g., a distribution network) is owned and operated by one central entity, which could just offer a database with an application programming interface or a trusted third party or permissioned ledger [56].

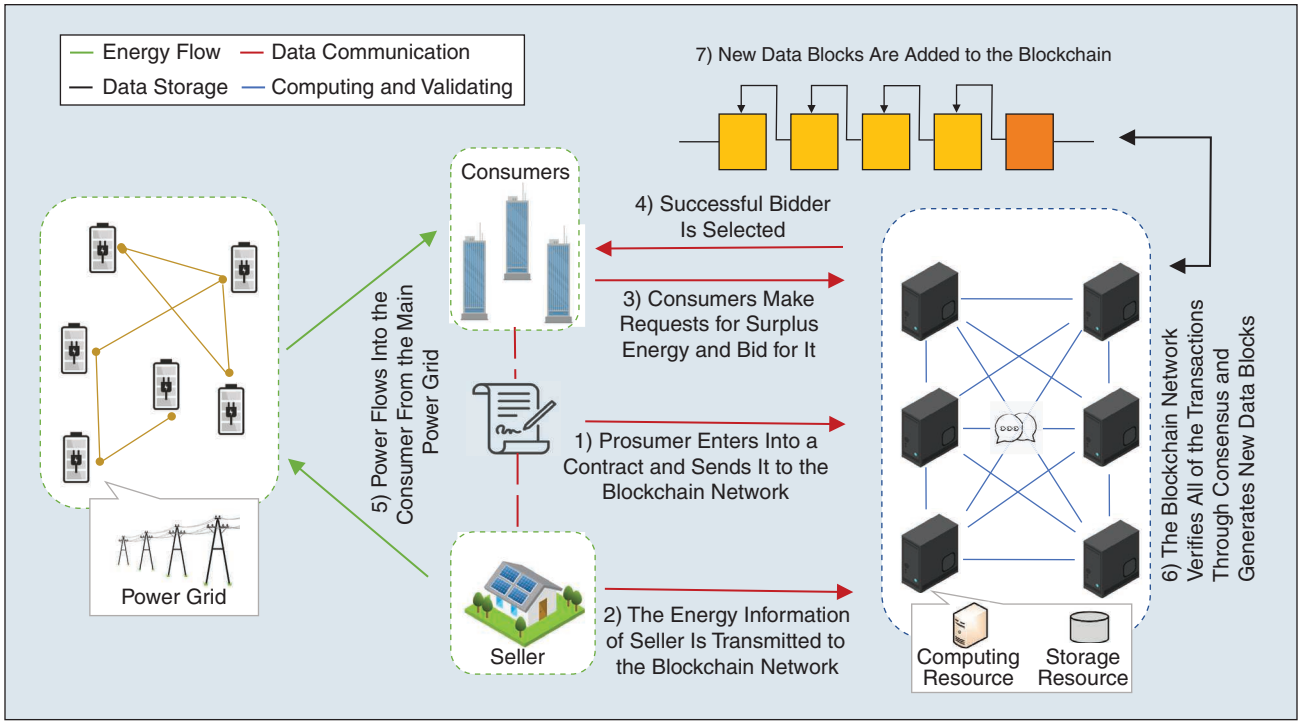

FIGURE 5 – A blockchain helps prosumers to match their needs.

A direct translation of a cryptocurrency into a crypto token for renewable energy amounts bears little complexity to distinguish between green and nongreen energies. This requires the consideration of more energy-oriented distributed storage, cryptography, and consensus algorithm techniques. For example, the Jouliette, a token based on blockchain implemented by a consortium around the Dutch distribution grid company Alliander, supports manual transactions, where customers can trade their Jouliettes, and also automated transactions, for the IoT to participate in this ecosystem. Distributed generation, such as photovoltaics, and intelligent loads, such as heat pumps, can organize themselves based on Jouliette transactions [57]. In China, a company called Energo in Shanghai is using blockchain to deal with trading clean and renewable energy [58], allowing producers to sell energy to consumers securely.

There have been many academic projects on blockchain for energy to improve distributed and local markets, manage distributed energy resources, and tokenize energy or access to energy, and so forth; see [59] and [60] for a list of such projects. Large-scale industrial rollouts of such ideas are, however, scarce. One most prominent example was given by the European transmission system operator (TSO) TenneT [61]. Germany's Sonnen and The Netherland's Vandebron deliver flexibility services to TenneT to be used in balancing actions. The flexibility comes from Tesla's and household batteries, organized via blockchain, using IBM technology. Encouraged by that, a new and even larger initiative was just launched: the Equigy platform [62]. TenneT (Germany and The Netherlands), Swissgrid (Switzerland), and Terna (Italy) team up to develop a cross-border blockchain platform for energy flexibility operations. TSOs traditionally run their assets by contracting large generation units for a variety of services, such as frequency reserves. Since many of these large fossil-fuel-based units are phased out, TSOs need to acquire these services from other parties in the grid. Replacing a few large generation units with many small renewable resources has many challenges, one of them being keeping enough flexible reserves for operations. Contracting thousands of resources in a transparent, easy, and flexible way is a perfect case for blockchain.

There are several technical challenges facing the adoption of blockchain in power and energy CPSSs [1]. The dynamical responsiveness of such systems requires the protocols and algorithms to be delay aware, security aware, and privacy aware as well as flexible enough to achieve tradeoffs in reaching consensus under the required latency and throughput. The blockchain network must be scalable as well. Another challenge is the resource constraints of the power and energy CPSSs, which make tamperproof data management difficult, especially considering the multiple types of data models. The security and timely processing of smart contracts are another challenge and may require some parallel processing mechanisms. These and many more activities ultimately lead to the development of standards [63]. While challenges such as transaction throughput can be addressed with the right blockchain design, other challenges, such as secure digital identities of embedded platforms, are equally important in power and energy systems but need to be solved in other ways. On top of that, the intrinsic challenges of a CPSS, such as matching market optima with physical feasibility, are still part of the application and are not "magically" solved by using a blockchain.

Manufacturing Systems in Industry 4.0

The manufacturing sector has witnessed rapid changes, driven by businesses and societies toward mass and extreme customization. New disruptive developments, such as software and hardware, cross-fertilization of concepts, and the integration of information, communication, and control technologies, in traditional industrial environments forge the core of current networked industrial infrastructures. These include cyberrepresentation of physical assets through digitalization of information across the enterprise, the value stream, and process engineering lifecycle as well as the digital thread from suppliers to customers in the supply chain. The technological, economic, and social impacts are so enormous that the overall process is regarded as the fourth Industrial Revolution, namely, Industry 4.0 [64].

The emerging disruptive technologies are already creating an innovation ecosystem for many industries. They are establishing entirely new markets and platforms for future growth. They are also facilitating the creation of new functionalities based on collaboration of heterogeneous physical systems in the cyberspace able to be exposed and/or consumed as services in a network, enabling continuous improvement of the quality of life for the "citizens in a secure digital society" [65], [66].

In such an Industry 4.0-compliant setting, countless assets, people (humans), machines, and products as well as IT components and systems within the enterprise architecture are able to asynchronously communicate and cooperate directly with each other to perform a set of defined service-oriented business transactions. The production, logistics, and business processes among assets are intelligently networked for a common value creation process. Cooperation through "services" is to be flexibly negotiated and agreed on in the Industry 4.0-conforming communication-information-business network of digitized assets [67].

Central to these is the asset administration shell (AAS), in which blockchain can find its way into the Industry 4.0 context [68]. To help asynchronously interact and handle business transactions, the AAS enables direct communication and cooperation among components (service providers and service consumers) to perform a desired business [69]–[72]. Figure 6 shows an exemplary Industry 4.0-compliant infrastructure, representing three different business processes performed by four AASs,

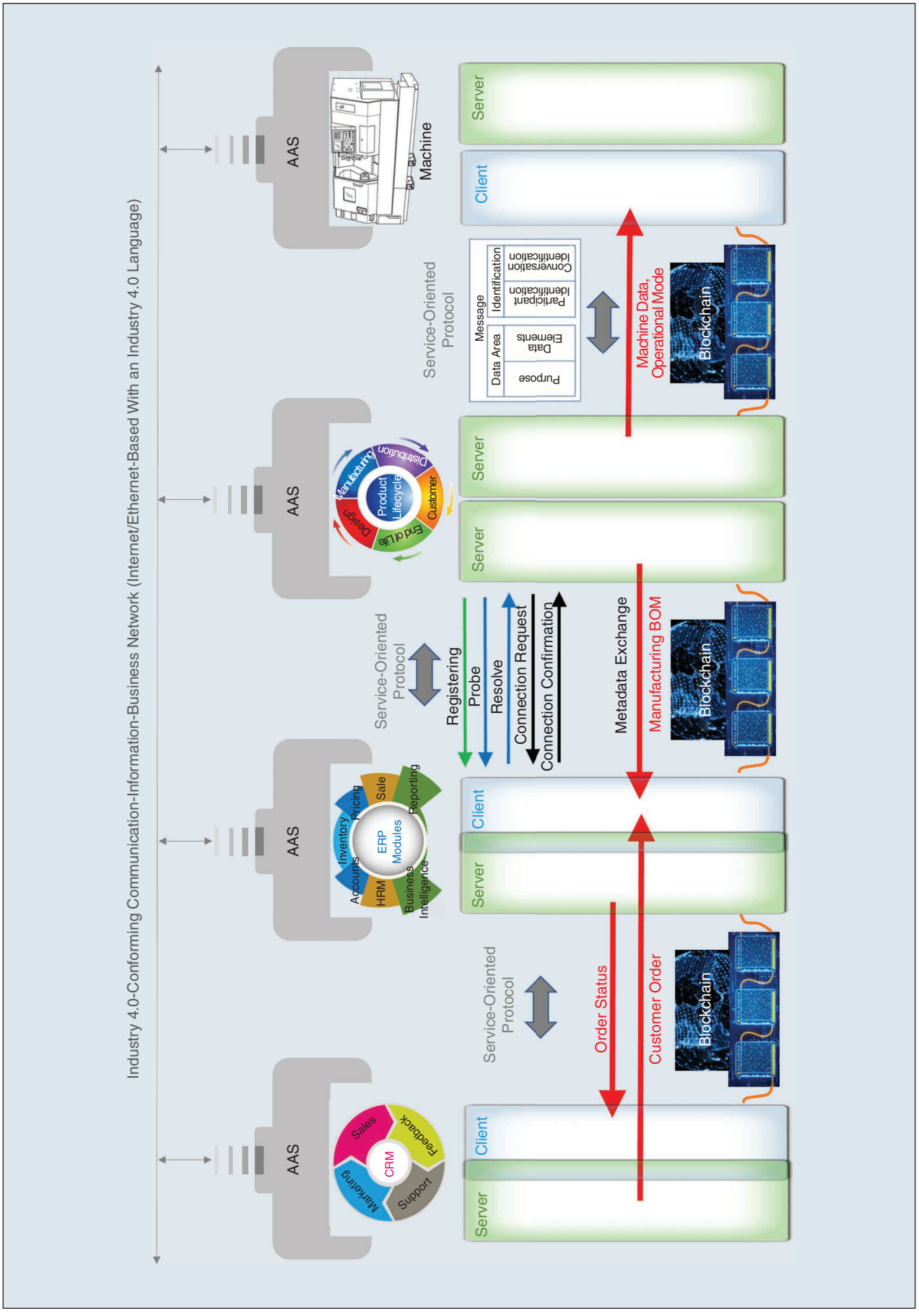

FIGURE 6 – Blockchain in Industry 4.0-compliant systems. CRM: customer relationship management; HRM: human resource management; ERP: enterprise resource planning; BOM bill of materials.

located at very different levels of an enterprise architecture with clearly different functionalities exposed as the Industrial Internet of Services (IIoS) [67]. Integrating blockchain technology within this solution provides reliability and the necessary trust among the AASs, allowing each of them to manage their own blocks and the blockchain-based service/business interaction protocol.

There have been numerous prototype implementations exploiting the features offered by blockchain in the industrial manufacturing sector with a focus on supply chain management. The benefits are enormous, including for example, reducing inventory costs and service times, automating trading and business negotiation processes, enhancing security and authentication, shortening production times, and monetizing ideas and capacities globally. Following the DIN SPEC 91345 (RAMI 4.0) [67] and considering the value stream and lifecycle dimension (International Electrotechnical Commission 62890) [79] as the basis for our example in Figure 6, the AAS-based digitalization aims to seamlessly manage all data, information, and knowledge generated throughout the asset lifecycle to achieve the desired business competitiveness.

The AAS-based approach allows smooth integration and sharing among the digitalized (cooperating) assets [68]. Major requirements, like interoperability, security, trust, and fundamental decentralization of decision-making processes, can easily be achieved by integrating the blockchain technology with the AAS. Essentially, this facilitates the realization of service-legal-agreements among digitalized assets with efficient consensus algorithms. Adequate open but secured information storage and customized blockchain information services, such as machine data or operational modes, can be shared between a digitalized product lifecycle management at the IT level and digitalized machines located at the operation technology levels of the enterprise. On one side, this AAS- and blockchain-based infrastructure not only can process the multisource and heterogeneous services from the two named assets but can also broadcast the exposed services to the Industry 4.0- and blockchain-conforming network. On the other side, the AAS- and blockchain-based application between IIoS-based business partners allows both vertical as well as horizontal integration, including managed consensus, e.g., for co-design and cocreation of enterprise resource planning (ERP) applications as well as quick and accurate tracking and tracing of manufacturing orders with an AAS-based digitalized customer relationship management (CRM). With the successful development of the proposed solution, service-based interoperability and cooperation among digitalized stakeholders (assets) in the entire value stream and lifecycle are guaranteed.

The Mobility Open Blockchain Initiative (MOBI) and OriginTrail [73] are other examples of blockchain-based solutions. MOBI was founded by automakers such as Renault, Ford, General Motors, and BMW, aiming to "build a vehicle digital identity prototype or car passport that can track and secure a vehicle's odometer and relevant data on distributed ledgers" [73]. OriginTrail aims to make supply chains more transparent by allowing interested parties to track an item's origin and process in primary industries, such as vegetable producer Natureta and dairy producer Celeia. Another example is IBM and Maersk (a leading shipping company), who tested blockchain technology in logistics operations [74]. In China, Alibaba established supET [75], a platform for blockchain applications in the industrial Internet. Numerous new use cases are being reported in other industrial manufacturing sectors like Industry 4.0, the Industrial IoT, and so on. This confirms potentials and challenges and also provides an outlook for future research and innovation opportunities to further exploit the advantages of the blockchain technology.

The challenges for the adoption of blockchain in manufacturing systems in Industry 4.0 lie in its role to enhance process optimization (e.g., logistics optimization and product lifecycle improvisation) and security and authentication (i.e., making parts tamperproof and cross-referencing them, providing identity management) [76]. While dynamical responsiveness is not required as much as it is for the power and energy systems, the complex and diverse nature of manufacturing systems would make scalability and flexibility the prominent issues. The enormous scale of IoT features in Industry 4.0 means there are huge amounts of critical and privacy-sensitive information that need to be protected from cyberattacks. However, because of limited resources, executing security functionalities is difficult to meet these security needs. This requires efficient consensus algorithms that can deal with the problems quickly in a distributed way. Identity management is another issue. The traditional methods of authentication, such as tokens or passwords, may not be useful. Finding a way to create trust among a big network of components/devices that is scalable and secure is a challenge, and this also applies to authorization, authentication, and integrity.

Robotics and Mechatronics and Other IE Areas

Blockchain has implications for many other key IE areas. For example, combining artificial intelligence (AI) with blockchain can improve efficiencies in swarm robotics or autonomous vehicles or can even help Bitcoin mining in a secure, flexible, and autonomous way, similar to that in power and energy systems. Swarm robotics is seen as an area benefiting from the combination of blockchain and AI. A team of autonomous robots work together in a "swarm" to perform tasks or operations; their collective behavior and interactive capabilities need to be robust and highly scalable. This can be enhanced by blockchain through advanced encryption techniques for optimal security for data across shared channels [77]. Blockchain also allows AI models and distributed large data sets to be shared, updated, and trained safely and securely, making wider adoption of AI possible [78].

Many systems and control issues can benefit from blockchain, especially in the multiagent system setting, where individual components cooperate to achieve a common goal quickly and securely in a distributed manner. However, the challenges facing the power and energy systems and manufacturing systems in Industry 4.0 are equally applicable, if not more so, to robotics and mechatronics and other IE areas. The dynamical responsiveness requirements would be more stringent, and resource-light and flexible blockchain platforms would be needed. The future of blockchain is very bright; however, the technological challenges involved in making it work are enormous.

Conclusion

In this article, we introduced the background and basic concepts of blockchain, its key features and technologies, as well as some future challenges and opportunities for blockchain in general. We specifically discussed the impact of blockchain on the future of major focal areas of the IEEE Industrial Electronics Society.

Biographies

Xinghuo Yu (x.yu@rmit.edu.au) earned his Ph.D. degree in control science and engineering from Southeast University, Nanjing, China, in 1988. He is an associate deputy vice chancellor, a distinguished professor, and a vice chancellor's professorial research fellow at the Royal Melbourne Institute of Technology, Melbourne, Victoria 3001, Australia. His research interests include control systems, complex and intelligent systems, smart grids, and energy systems. He has worked extensively in industrial information technologies. He is a Fellow of IEEE and a member of the IEEE Industrial Electronics Society.

Changbing Tang (tangcb@zjnu.edu.cn) earned his Ph.D. degree in electronic engineering from Fudan University, Shanghai, China, in 2014. He received his B.S. and M.S. degrees in mathematics and applied mathematics from Zhejiang Normal University at Jinhua, in 2004 and 2007. He is an associate professor in the Department of Electronics Information and Engineering, Zhejiang Normal University, Jinhua, 321004, China. His research interests include game theory, blockchain and its applications, networks, and distributed optimization. He was an Academician Pairing Training Program for Young Talents of Zhejiang Province in 2019. He is a Member of IEEE.

Peter Palensky (palensky@ieee.org) earned his Ph.D. degree from the Vienna University of Technology, Austria, in 2001. He is currently a full professor for intelligent electric power grids at the Delft University of Technology (TU Delft) and the scientific director of TU Delft's PowerWeb Institute, Delft, 2628CD, The Netherlands. His research interests include the digital transformation of power systems. He is a Senior Member of IEEE and a member of the IEEE Industrial Electronics Society.

Armando Walter Colombo (aw colombo@ieee.org) earned his Ph.D. degree in engineering from the University of Erlangen–Nuremberg, Germany, in 1998. He is a full professor in the Faculty of Engineering and director of the Institute for Industrial Informatics, Automation, and Robotics at the University of Applied Sciences Emden/Leer, Emden, D-26723, Germany. From 2001 to 2018, he was the director for Innovation Projects and Edison-Level-2 Group Senior Expert at Schneider Electric. His research interests include industrial-cyber-physical systems, Industry 4.0, the Internet-of-Things, and the Internet of Services. He is member of the IEEE Industrial Electronics Society (IES) Administrative Committee, chair of the IES Fellows Committee, IES representative to the IEEE Systems Council, and the co-editor-in-chief of *IEEE Open Journal of the Industrial Electronics Society*. He is a Fellow of IEEE and a member of the IEEE Industrial Electronics Society.

References

[1] N. U. Hassan, C. Yuen, and D. Niyato, "Blockchain technologies for smart energy systems: Fundamentals, challenges, and solutions," *IEEE Ind. Electron. Mag.*, vol. 13, no. 4, pp. 106–118, Dec. 2019.

[2] T. Aste, P. Tasca, and T. D. Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18–28, 2017. doi: 10.1109/MC.2017.3571064.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Bitcoin, White Paper, 2008. https://bitcoin.org/bitcoin.pdf (accessed 15 June 2020).

[4] P. K. Sharma, S. Singh, Y. S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sept. 2017. doi: 10.1109/MCOM.2017.1700041.

[5] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," GitHub, Inc., San Francisco, 2013. http://ethereum.org/ethereum.html (accessed 15 June 2020).

[6] L. Lu et al., "Pseudo trust: Zero-knowledge authentication in anonymous P2Ps," *IEEE Trans. Parallel Distrib. Syst.*, vol. 19, no. 10, pp. 1325–1337, Oct. 2008.

[7] D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox, "Zcash protocol specification," Version 2020.1.2, Zerocoin Electric Coin Co., Oakland, CA, Tech. Rep., Mar. 20, 2020.

[8] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct non-interactive zero knowledge for a von neumann architecture," in *Proc. 2014 USENIX Security Symp.*, San Diego, CA, Aug. 20–22, 2014, pp. 781–796.

[9] Y. Yuan, X. C. Ni, S. Zeng and F. Y. Wang, "Blockchain consensus algorithms: The state of the art and future trends," *Acta Automat. Sinica (in Chinese)*, vol. 44, no. 11, pp. 2011–2022, 2018.

[10] L. Lamport, "The part-time parliament," *ACM Trans. Comput. Syst.*, vol. 16, no. 2, pp. 133–169, 1998. doi: 10.1145/279227.279229.

[11] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *Proc. USENIX Annu. Tech. Conf.*, Philadelphia, June 19–20, 2014, pp. 305–320.

[12] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *Proc. Operating Syst. Des. Implement.*, vol. 99, pp. 173–186, Feb. 1999.

[13] D. Mazières, "The stellar consensus protocol: A federated model for internet-level consensus." Stellar. https://www.stellar.org/papers/stellar-consensus-protocol.pdf (accessed Sept. 20, 2020)

[14] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurencies." IACR. http://eprint.iacr.org/2017/454 (accessed Sept. 20, 2020)

[15] R. Pass and E. Shi. "The sleepy model of consensus." IACR. https://eprint.iacr.org/2016/918.pdf (accessed Sept. 20, 2020)

[16] I. Eyal, A. E. Gencer, E. G. Sirer, and R. V. Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *Proc. 13th USENIX Conf. Netw. Syst. Des. Implementation*, 2016, pp. 45–59.

[17] E. Kokoris-Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing bitcoin security and performance with strong consistency via collective signing," in *Proc. 25th USENIX Security Symp.*, 2016, pp. 279–296.

[18] J. P. Buntinx, "What is proof of elapsed time?" Accessed Sept. 20, 2020. [Online]. Available: https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp

[19] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol." IACR. https://eprint.iacr.org/2017/249.pdf (accessed Sept. 20, 2020)

[20] G. Ateniese, I. Bonacina, A. Faonio, and N. Galesi, "Proofs of space: When space is of the essence," in *Proc. 9th Int. Conf. Security Cryptogr. Netw.*, 2014, pp. 538–557.

[21] M. Ball, A. Rosen, M. Sabin, and P. N. Vasudevan, "Proofs of useful work." Allquantor. https://allquantor.at/blockchain-bib/pdf/ball2017proofs.pdf (accessed Sept. 20, 2020)

[22] S. King and S. Nadal, "PPcoin: Peer-to-peer crypto-currency with proof-of-stake," Self-published paper, vol. 19, Aug. 2012.

[23] D. Larimer, F. Schuh, and D. Larimer, "BitShares 2.0: Financial smart contract platform." BitShares. https://www.weusecoins.com/assets/

pdf/library/Bitshares%20Financial%20Platform.pdf (accessed Sept. 20, 2020)
[24] J. Kwon, "Tendermint: Consensus without mining." Tendermint. https://tendermint.com/static/docs/ten-dermint.pdf (accessed Sept. 20, 2020)
[25] "Ethereum's Casper protocol explained in simple terms." Finder. https://www.finder.com/ethereum-casper (accessed Sept. 20, 2020)
[26] A. Miller, A. Juels, E. Shi, B. Parno and J. Katz, "Permacoin: Repurposing Bitcoin work for long-term data preservation," in *Proc. IEEE Symp. Security Privacy*, 2014, vol. 1, pp. 475–490.
[27] L. Ren, "Proof of stake velocity: Building the social currency of the digital age." https://www.cryptoground.com/storage/files/1528454215-cannacoin.pdf (accessed Sept. 20, 2020)
[28] "Proof of burn." Bitcoin. https://en.bitcoin.it/wiki/Proof of burn (accessed Sept. 20, 2020)
[29] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending Bitcoins proof of work via proof of stake." IACR. http://eprint.iacr.org/2014/452 (accessed Sept. 20, 2020).
[30] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 2020. doi: 10.1109/comst.2020.2969706.
[31] N. Szabo, "Smart contracts." https://pipiwiki.com/wiki/Agoric_computing (accessed June 15, 2020).
[32] T. T. A. Dinh, R. Liu, M. H. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, 2018. doi: 10.1109/TKDE.2017.2781227.
[33] Hyperledger Project. Accessed: June 15, 2020. [Online]. Available: https://www.hyperledger.org/
[34] S. Wang, Y. Yuan, X. Wang, J. J. Li, R. Qin, and F. Y. Wang, "An overview of smart contract: Architecture, applications, and future trends," in *Proc. IEEE Intell. Veh. Symp. (IV)*, Changshu, China, June 26–30, 2018, pp. 108–113. doi: 10.1109/IVS.2018.8500488.
[35] "The energy web chain: Accelerating the energy transition with an open-source, decentralized blockchain platform," Energy Web Foundation, Zug, Switzerland. Accessed: Sept. 20, 2020. [Online]. Available: https://energyweb.org/wp-content/uploads/2018/10/EWF-Paper TheEnergyWebChain-v1-201810-FINAL.pdf
[36] "Initial coin offering," Solar Bankers, Prague, Czech Republic, White Paper. [Online]. Available: https://solarbankers.com/wpcontent/uploads/2017/10/SB-White-Paper_version2.pdf (accessed Sept. 20, 2020).
[37] J. Steiner and J. Baker, "Blockchain: The solution for transparency in product supply chains," Project Provenance Ltd., London, White Paper, 2015. [Online]. Available: https://www.provenance.org/whitepaper (accessed Sept. 20, 2020)
[38] G. Prisco, "The blockchain for healthcare: Gem launches Gem Health Network with Philips Blockchain Lab." BitCoin Magazine. [Online]. Available: https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gemlaunches-gem-health-network-with-philips-blockchain-lab-1461674938/ (accessed Sept. 20, 2020)
[39] Genesis of Things Project. Accessed: Sept. 20, 2020. [Online]. Available: http://www.genesisofthings.com/
[40] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang, and R. P. Liu, "Survey: Sharding in blockchains," *IEEE Access*, vol. 8, pp. 14,155–14,181, Jan. 2020. doi: 10.1109/ACCESS.2020.2965147.
[41] A. Zamyatin et al., "SoK: Communication across distributed ledgers," Imperial College London, London, UK, IACR Cryptology ePrint Archive, 2019: 1128, Tech. Rep., 2019.
[42] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, 2019. doi: 10.1109/COMST.2018.2863956.
[43] A. Jake and S. Nathalie-Kyoko. "Behind the biggest Bitcoin heist in history: Inside the implosion of mt.gox." The Daily Beast. https://www.thedailybeast.com/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion-of-mt-gox (accessed Sept. 20, 2020).
[44] V. Buterin. "Critical update re: Dao vulnerability." https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/ (accessed Sept. 20, 2020)
[45] I. Nikolić, A. Kolluri, I. Sergey, P. Saxena, and A. Hobor, "Finding the greedy, prodigal, and suicidal contracts at scale," in *Proc. 34th Annu. Comput. Security Appl. Conf.*, San Juan, PR, Dec. 2018, pp. 653–663.
[46] D. Dasgupta, J. M. Shrein, and K. D. Gupta, "A survey of blockchain from security perspective," *J. Banking Financial Technol.*, vol. 3, no. 1, pp. 1–17, 2019. doi: 10.1007/s42786-018-00002-6.
[47] "EOSIO/eos: An open source smart contract platform," GitHub, San Francisco, Oct. 2, 2018. https://github.com/pyun/eos (accessed Mar. 28, 2021).
[48] W. Song, Y. Li, and D. Yang, "Research on the application of blockchain in the energy power industry in China," *IOS J. Phys., Conf. Ser.*, vol. 1176, no. 4, p. 042079, 2019.
[49] A. Kosba, A, Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Security Privacy (SP)*, San Jose, CA, May 22–26, 2016, pp. 893–858.
[50] S. F. Sun, M. H. Au, J. K. Liu, and T. H. Yuen, "RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency Monero," in *Computer Security-ESORICS*. Cham: Springer-Verlag, 2017, vol. 10493, pp. 456–474.
[51] W. T. Li, S. Andreina, J. M. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Cham: Springer-Verlag, 2017, vol. 10436, pp. 297–315.
[52] H. W. Huang, J. R. Lin, B. C. Zheng, Z. B. Zheng, and J. Bian, "When blockchain meets distributed file systems: An overview, challenges, and open issues," *IEEE Access*, vol. 8, pp. 50,574–50,586, Mar. 2020. doi: 10.1109/ACCESS.2020.2979881.
[53] "Decentralized Identifiers (DIDs): Core architecture, data model, and representations." GitHub, San Francisco. https://w3c.github.io/did-core/ (accessed Sept. 20, 2020).
[54] "A gentle introduction to self-sovereign identity." Bits on Blocks. https://bitsonblocks.net/2017/05/17/gentle-introduction-self-sovereign-identity/ (accessed Sept. 20, 2020)
[55] X. Yu and Y. Xue, "Smart Grids: A cyber-physical systems perspective," *Proc. IEEE*, vol. 104, no. 5, pp. 1058–1070, 2016. doi: 10.1109/JPROC.2015.2503119.
[56] M. E. Peck, "Do you need a blockchain?" *IEEE Spectrum*, vol. 54, no. 10, pp. 38–60, Oct. 2017. doi: 10.1109/MSPEC.2017.8048838.
[57] ETIP SNET WG4. "Digitalization of the electricity system and customer participation," De Ceuvel, Amsterdam, The Netherlands, Tech. Position Paper WG4, Sept. 2018.
[58] "Starting from the micro power grid, Energo tries to build a decentralized energy transaction system using blockchain." Energo Labs, Shanghai, China, http://www.8btc.com/energo-labs-blockchain, in Chinese (accessed Jan. 25, 2018)
[59] A. S. Musleh, G. Yao, and S. M. Muyeen, "Blockchain applications in smart grid–review and frameworks," *IEEE Access*, vol. 7, pp. 86,746–86,757, June 2019. doi: 10.1109/ACCESS.2019.2920682.
[60] S. Johanning and T. Bruckner, "Blockchain-based peer-to-peer energy trade: A critical review of disruptive potential," in *Proc. 16th Int. Conf. European Energy Market (EEM)*, Ljubljana, Slovenia, 2019, pp. 1–8. doi: 10.1109/EEM.2019.8916268.
[61] K. Döppenbecker. "Undertaking energy transition interview with TenneT's Digital Transformation Lead René Kerkmeester." TenneT, 2019. https://www.tennet.eu/fileadmin/user_upload/ArtikelTenneT.pdf (accessed June 15, 2020)
[62] "Equigy platform gives European consumers access to tomorrow's sustainable energy market," TenneT, European, TenneT Press Release 23. Apr. 2020. Accessed Mar. 28, 2021. [Online]. Available: https://www.tennet.eu/#&panel1-1
[63] *Standard for Blockchain in Energy*, IEEE Standard P2418.5, 2018
[64] A. W. Colombo , S. Karnouskos, O. Kaynak, Y. Shi, and S. Yin, "Industrial cyber-physical systems: A backbone of the fourth industrial revolution," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 6–16, 2017. doi: 10.1109/MIE.2017.2648857.
[65] Federal Ministry of Education and Research (BMBF), Germany, "Innovations for the production, services and work of tomorrow (in German)," in *The New Hightech Strategy, Innovations for Germany*, 2014. [Online]. Available: https://www.bmbf.de/de/innovationen-fuer-die-produktion-dienstleistung-und-arbeit-von-morgen-599.html
[66] ZVEI, Zentralverband Elektrotechnik- und Elektronikindustrie e.V., Safety and Security in Industry 4.0. https://www.dke.de/resource/blob/1624282/f6372e8c85ee20491f6b7b967203ccbc/safety-security-im-bereich-industrie-4-0-prof–wegener-data.pdf (accessed May 24, 2020)
[67] *DIN SPEC 91335 RAMI4.0*. [Online]. Available: https://dx.doi.org/10.31030/2436156 (accessed June 15, 2020).
[68] "Platform Industry 4.0 and ZVEI, details of the asset administration shell." https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/Details-of-the-Asset-Administration-Shell-Part1.pdf?__blob=publicationFile&v=5 (accessed May 22, 2020).
[69] "Blockchain Technology In Industry 4.0," BitDeal. https://www.bitdeal.net/blockchain-in-industry-4-0 (accessed May 25, 2020)
[70] R. Rosa Righi, A. M. Alberti, and M. Singh, Eds., *Blockchain Technology for Industry 4.0*. Springer Nature, Singapore Pte Ltd., 2020.
[71] Blockchain – eine Technologie mit disruptivem Charalter (in German). https://www.vditz.de/fileadmin/media/bekanntmachungen/documents/vdi_publikation_blockchain_RZ_web_neu.pdf (accessed May 20, 2020)
[72] "Blockchain and Industry 4.0." Capgemini. https://www.capgemini.com/au-en/wp-content/uploads/sites/9/2018/10/Blockchain-and-Industry-4.0.pdf (accessed May 20, 2020)
[73] "What is blockchain technology and how is it changing the manufacturing industry?" The Manufacturer. https://www.themanufacturer.com/articles/blockchain-technology-changing-manufacturing-industry/ (accessed June 10, 2020)
[74] Application of Blockchain in manufacturing industry." Blockchain Expert. https://www.blockchainexpert.uk/blog/application-of-blockchain-in-manufacturing (accessed June 10, 2020)
[75] "Application of blockchain in industrial Internet by Ali Cloud." CQVIP. http://www.cqvip.com/QK/80675A/201822/7000940533.html, in Chinese (accessed June 12, 2020).
[76] A. Mushtaq, I.U. Haq, "Implications of Blockchain in industry 4.0," in *Proc. Int. Conf. Eng. Emerg. Technol.*, Lahore, Pakistan, Feb. 21, 2019, pp. 2409–2983.
[77] "How Blockchain and AI can help robotics technologies." Robotics Business Review. https://www.roboticsbusinessreview.com/ai/how-blockchain-and-ai-can-help-robotics-technologies/ (accessed June 9, 2020).
[78] R. Shroff, "When Blockchain meets Artificial Intelligence." Medium. https://medium.com/swlh/when-blockchain-meets-artificial-intelligence-e448968d0482 (accessed June 12, 2020).
[79] *IEC 62890:2020*, IEC Webstore. [Online]. Available: https://webstore.iec.ch/publication/30583