Blockchain: What Does It Mean to Industrial Electronics?

1. WHAT IS BLOCKCHAIN?

Imagine you want to send money to a friend overseas. Wouldn't it be good if you don't have to pay hefty fees to the intermediaries and your friend receives it very quickly? Now imagine again ordering parts to make a product in your manufacturing plant. Wouldn't it be great if you are 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 for you to 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 which enables distributed nodes to collaboratively affirm transaction provenance via a decentralized consensus mechanism. The interest on 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

Blockchain was coined in the 2008 article "Bitcoin: A Peer-to-Peer E-Cash System" by Satoshi Nakamoto [3]. In a narrow sense, it is a chained data structure storing data blocks sequentially, and a non-tamperable and un-forgeable distributed ledger which 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, and smart contracts with automated scripts to program and manipulate data (Figure 1 shows how it works).

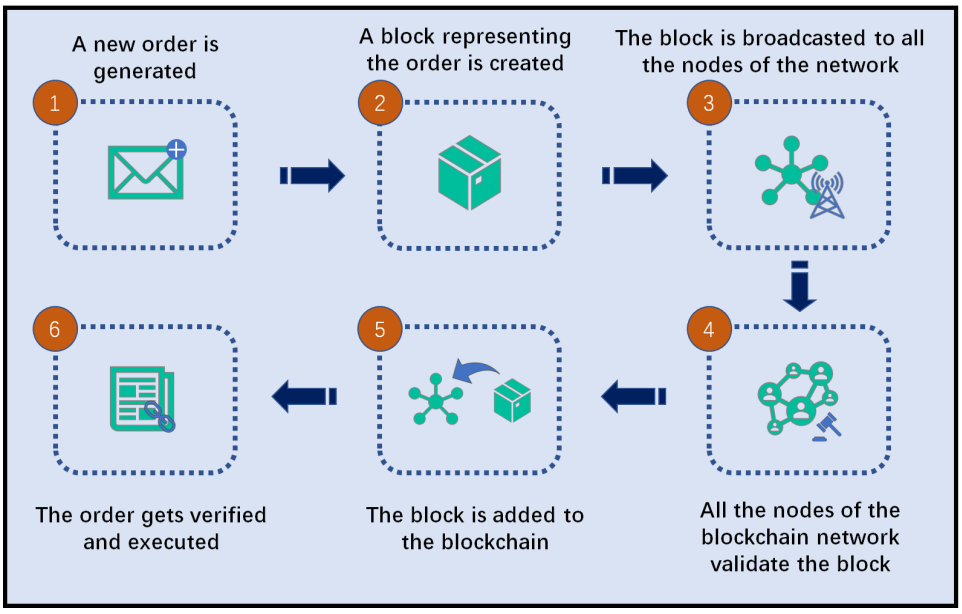

FIGURE 1 How a Blockchain works

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 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 as Blockchain 1.0, 2.0, and 3.0, respectively.

Soon after publishing [3], Satosh Nakamoto created a software in 2009 to mine the foundation block, opening the era of Bitcoin. The initial interest in Blockchain was on virtual currencies, i.e. *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 a big step forward – *Blockchain 2.0*, marked by the publication of the Ethereum White Book in 2013 [5]. Ethereum was a platform which offers a variety of modules allowing users to build applications. It works like building a house, where Ethereum provides building modules such as walls, roof, floor, and users only need to

assemble the house using the modules. The core of Ethereum is the smart contracting which is an automated agent. However, Blockchain 2.0 could only achieve 70 to 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 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.

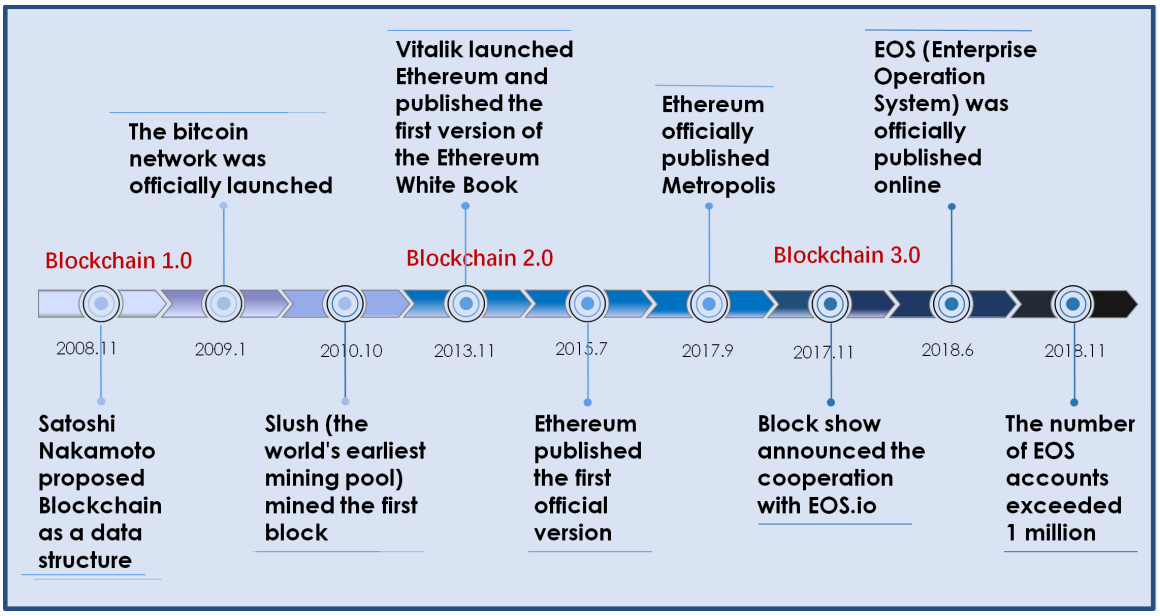

FIGURE 2- The journey of Blockchain.

Key Technologies of Blockchain

There are four key traditional technologies of the Blockchain, i.e., distributed storage, cryptography, consensus algorithms and smart contracts (see Figure 3).

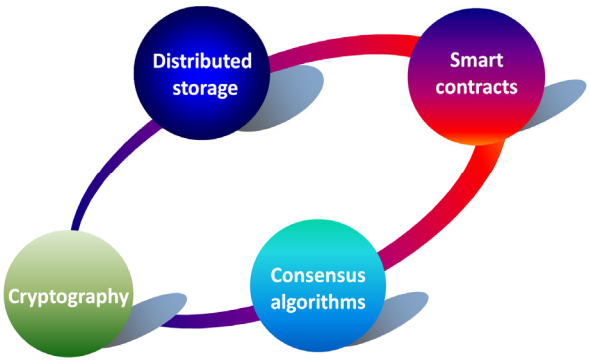

FIGURE 3- Four key technologies of Blockchain

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

Cryptography is 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 block header. Meanwhile, hash-based tree structures such as the Merkel 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. The storage structure of Blockchain is like a zipper: after each data is stored independently, a chain is formed and any node can be traced. In this process, the signature is determined by cryptography, and zero-knowledge proof plays an increasingly important role for convincing the verifier that certain

assertion is deemed correct without providing any information to it (e.g. Zcash [7], ZK-SNARKs [8]).

Consensus algorithms refer to how all nodes reach consensus to validate a record, which is for both identification and tampering prevention to maintain decentralized multi-party mutual trust. In both public and private Blockchain, 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 can add blocks 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, respectively. According to the fault-tolerant type, they can be divided into Byzantine fault-tolerant (BFT) and non-Byzantine fault-tolerant. Considering the degree of consistency, they can also be divided into strong consensus and weak consensus. In this paper, we classify the consensus algorithms into four types, namely, BFT-based consensus algorithm, PoW-based (Proof of Work-based) consensus algorithm, PoS-based (Proof of Stake-based) consensus algorithm, and the mixed type consensus algorithm. BFT-based consensus algorithm is based on the traditional distributed consistency checking techniques, such as Paxos [10], Raft [11], PBFT [12], Stellar Consensus Protocol (SCP) [13], AlgoRand [14], Sleepy Consensus [15]. PoW-based consensus algorithm aims to achieve capacity expansion of Blockchain (e.g. Bitcoin-NG [16] and Elastico [17]) or improve efficiency of algorithm (e.g. Proof of Elapsed Time, PoET [18], Proof of Luck, PoL [19], Proof of Space, PoSp [20] and Proof of Use Work, PoUW [21]). PoS-based consensus algorithm is to solve the problem of "nothing at stake" [22], including Delegated Proof of State (DPoS) [23], Tendermint [24], Casper [25], Proof of Unspent Transaction Output (PoUTXO) [26]. The mixed type consensus algorithms mainly draw lessons from the consensus of

PoW and PoS, including Proof of State Velocity (PoSV) [27], Proof of Burn (PoB) [28], and Proof of Activity (PoA) [29]. In short, all Blockchain consensus algorithms mainly focus on three aspects: performance evaluation, adaptation and optimization, and consensus innovation under the new Blockchain structure. For a comprehensive survey of various consensus algorithms, readers are referred to [30].

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 Nick Szabo in 1994 [31]. As a kind of embedded programming, smart contracts can be built in any Blockchain data, trading, tangible or intangible assets, and form a programmable control system. The key property of 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 is analogous to stored procedures in relational database management systems. According to the performance of 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, scalable and versatility, which supports various of 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].

Main Platforms of Blockchain

Blockchain platforms combining distributed storage, cryptography, consensus algorithms，smart contracts together with network and data technologies are used for building Blockchain-based systems. There are some quite generic platforms which 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 financial, 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 healthcare, and Genesis of things [39] for manufacturing 3D. Generally, the selection of a Blockchain platform is dependent on the needs of users. For example, multiple collaborative diverse companies can use a platform like Ethereum to implement smart contracts capabilities over their network, while a group of energy providers can use one platform like EWF that supports energy trade applications.

2. KEY ISSUES AND CHALLENGES IN BLOCKCHAIN

Blockchain has now become a huge technical field which is changing industry, economy and society profoundly. There are many issues and challenges as shown below.

Technological Issues

The breakthrough construction of Blockchain technology is limited by a famous theory: "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 (so-called scalability) is very low. Due to frequent network congestion, traders have to

pay more in the transaction process. Therefore, one challenge is to address the "Impossible Triangle" problem to balance among "scalability", "security" and "decentralization".

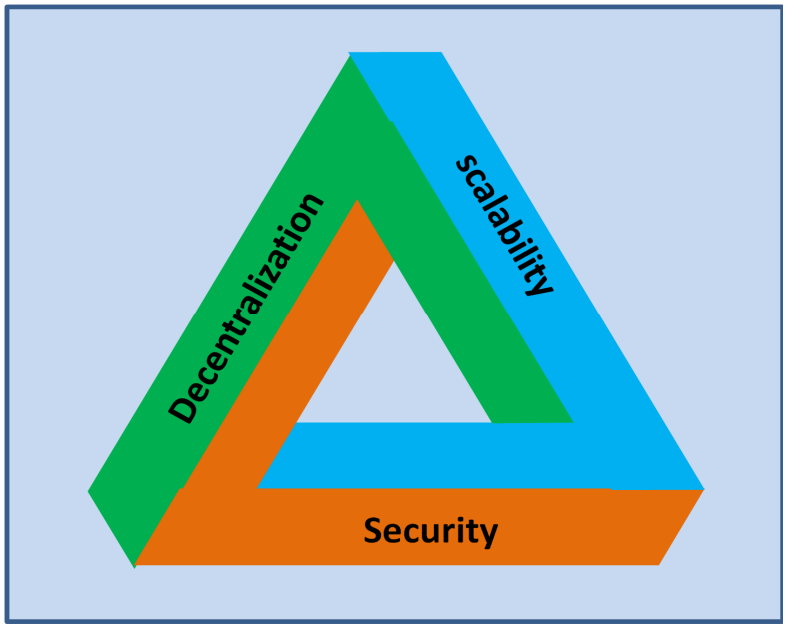

FIGURE 4- The impossible triangle problem of Blockchain.

Scalability refers to the ability to handle high volumes of business data. As usual, there is always a trade-off between costs, security and performance. To achieve scalability, we should consider the usage context and the performance metrics such as validation latency, transactions throughput, energy costs, computation costs, storage costs, number of nodes, etc. For example, the throughput of a Blockchain is not scalable when the network size grows. The promising solutions to improve the scalability of Blockchains mainly include 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, while these overheads must be incurred by all full nodes in traditional non-sharded-Blockchains. Cross-chain is a scheme that makes possible of the interconnection between Blockchains. 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, concerning 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 makes Blockchain technology exposed to many security threats and challenges. For example, in March 2014, some criminals used DDoS (distributed denial of service) to attack bitcoin trading platform Mt.Gox, which resulted in 850,000 bitcoins stolen from the trading platform and more than $450M lost [43]. In June 2016, "the Dao", the largest crowdfunding project of Blockchain at that time, was attacked and lost about $60M [44]. In the following, we will discuss the security of Blockchain from the protocol layer, the extension layer and the application layer perspectives. In the protocol layer, the security problems of Blockchain mainly include encryption mechanism security (such as private key security), consensus mechanism security (such as double spending attack, 51% attack and coin age attack) and network communication security (such as eclipse attack, routing attack, border gateway protocol (BGP) attack, Sybil attack and balance attack). In the extension layer, the security of Blockchain is mainly affected by the vulnerability of smart contract. Ivica et al. classified the existing smart contract vulnerabilities into prodigal contract, greedy contract, suicidal contract, and postmortem contract, respectively [45]. In the application layer, when the user interacts with the Blockchain system, the attacker may obtain the user's physical identity or other additional information by means of data mining, which lead to the user's privacy disclosure. The main securities include identity privacy security and transaction privacy security. For a comprehensive survey of Blockchain security, readers are referred to [46].

Decentralization is a key to roll out Blockchain applications, which may also compromise Blockchain security. Most existing technologies are still centralization-oriented. Taking EOS as an

example [47], it uses 21 "super nodes" to block out nodes in a certain order, thereby avoiding accounting in a large number of nodes which would otherwise increase significantly levels in the transaction processing system (TPS). However, it has been questioned that the power is too centralized, which is not conducive to network security. At present, due to the emergence of ASIC6 mining machine, 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 a considerable discourse power of the bitcoin world.

Regulatory and Legal Issues

While many countries are actively supporting adoption of the Blockchain technology, there have not been 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$761M worth of digital currency was stolen by hackers from digital currency exchanges around the world in the first six months of 2018, according to Cipher Trace a USA digital currency security company. In comparison, only US$266M were lost in 2017. China announced a ban on initial coin offering (ICO) and shut down all domestic cryptocurrency exchanges in 2019 [48], leading to a 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 technology setting itself, and the imbalance of rules wrapped in technology makes the regulation more difficult because of privacy concerns.

There are significant legal issues a well in the context of docking and coordination within the existing legal systems. At present, there is not commonly accepted definition of a Blockchain in legal systems, nor 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 usually done by a credible third party (law firms). But smart contracts completely depend on computer languages to stipulate authentication and execution among parties, begging the question of whether the semantics of the contract terms can accurately express intentions of the parties and the smart contracts can be legally recognized. Furthermore, during the execution of smart contracts, everything needs to comply with the pre-set code, regardless of the wishes of the parties. A mistake or change would require enormous efforts to change the program codes. The so-called "smart" is not so smart, in this instance.

Other Challenges

Blockchain technology is still in its infantry though has a 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 the trust is lacking. These 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 following aspects are very important for the future, such as parallelization, consensus, cross-chain and channel technologies. There have already been some good progresses, including cryptographic security (such as zero-knowledge proof [49], ring signature [50]), consensus mechanisms (such as Verifiable Random Function (VRF) [51]), infrastructure of Blockchain (such as multi-chain, channel technology, Directed Acyclic Graph (DAG)), distributed file system (such as Inter-Planetary File System (IPFS) [52]), and identity

management (such as Decentralized IDs (DIDs) [53], and Self-Sovereign Identity (SSI) [54]), etc. 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 efficiently. IPFS provides a high-throughput, content-addressed block storage model, with content-addressed hyperlinks. DIDs are 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 users themselves SSI makes users 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 refer to the interactions between the traditional services and the Blockchain services. Blockchain 3.0 is emerging in that all business operations would run on the Blockchains based on smart contracts in a decentralized manner.

3. BLOCKCHAIN FOR INDUSTRIAL ELECTRONICS

The fast development of Blockchain has far reaching impact on many areas ranging from technological, to social and economic fields. The field of Industrial Electronics (IE) is no exception. Industrial Electronics 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 thematical areas such as power and energy systems, manufacturing systems, robotics and mechatronics etc. are being impacted by Blockchain, which shall be briefly described below.

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 slower. Power networks are considered Cyber-Physical Systems (CPSs) [55], or if prosumers and community/society are included in the equation, Cyber-Physical-Social Systems (CPSSs). Blockchain technology by its promises has a big future. Figure 5 shows how Blockchain can be used in power sharing applications. A prosumer first enters contract as a user node through the blockchain network where 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, 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 to 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 payoff. Finally, the miners in the network package all the transactions during this period, then verify the transactions through consensus and generate new data blocks which are then added to the block chain as secured records automatically.

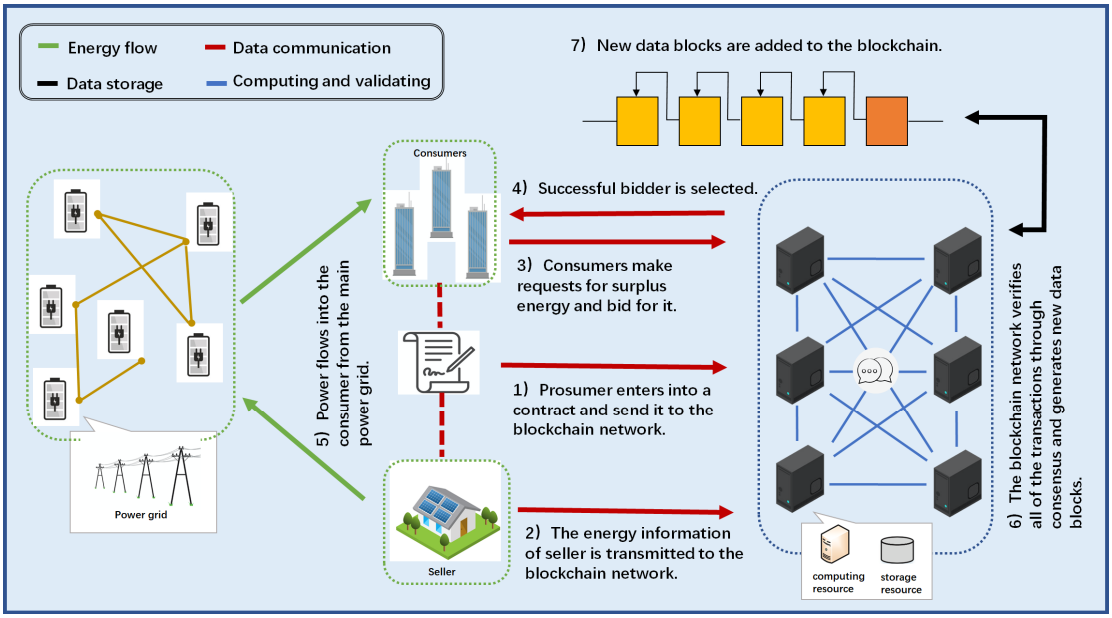

FIGURE 5- A Blockchain helps prosumers to match their needs

However, the special features of power and energy CPSS may mean that various parts of the Blockchain technology may 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, the stringent requirements of power and energy CPSS to be dynamically responsive across three

layers of the cyber, physical and social worlds, as well as to be robust against intermittent uncertainties such as renewable energies and electric vehicles. The uptake of Blockchain in power and energy CPSS requires 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 was not even 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 API or a trusted third party or permissioned ledger [56]. A direct translation of a crypto currency into a crypto token for renewable energy amounts bears little complexity to distinguish between green and non-green energies. This requires considering more energy-oriented distributed storage, cryptography, consensus algorithms 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 automated transactions for IoT to participate in this ecosystem. Distributed generation such as PV 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, tokenize energy or access to energy, and so forth, see [59] and [60] for a list of such projects. Large-scale industrial roll-out of such ideas are, however, scarce. One most prominent example was given by the European transmission system operator TenneT [61]. Germany's Sonnen and The Netherland's Vanderbron deliver flexibility services to TenneT to be used in balancing actions. The flexibility comes from Teslas 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. Transmission system operators (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 CPSS [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 consensus-reaching 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 CPSS which make tamperproof data management difficult especially due to multiple types of data models. The security and timely processing of smart contracts are another challenge where some parallel processing mechanisms may be needed. These and many more activities ultimately lead to the developments 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 elsehow. On top of that, the intrinsic challenges of a CPSS such as matching market optima with physical feasibility is still part of the application and is not “magically” solved with using a blockchain.

Manufacturing Systems in Industry 4.0

The manufacturing sector has witnessed rapid changes, driven by businesses and societies towards 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 including cyber-representation of physical assets through digitalization of information across the enterprise, the value stream and process engineering life-cycle as well as the digital thread from suppliers to customers in the supply chain. Their technological, economic and social impacts are so enormous that the overall process is regarded as the 4th Industrial Revolution, namely, Industry 4.0 [64].

The emerging disruptive technologies are already creating an innovation ecosystem for many industries, establishing entirely new markets and platforms for future growth and facilitating 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 in order to perform a set of defined service-oriented business transactions. The production, logistics and business processes between assets are intelligently networked for a common value creation process. Cooperation through "services" are to be flexibly negotiated and agreed in the Industry 4.0-conform communication-information-business network of digitized assets [67].

Central to these is the Asset Administration Shell (AAS) where Blockchain can find its way

into the Industry 4.0 context [68]. To help asynchronously interact and handle business transactions, AAS enables direct communication and cooperation between 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 process performed by 4 AAS, located at very different levels of an enterprise architecture with clearly different functionalities exposed as Industrial Internet of Services (IIoS) [67]. Integrating Blockchain technology within this solution provides reliability and the necessary trust between the AAS allowing each of them to manage the own blocks and the Blockchain-based Service-/Business Interaction Protocol.

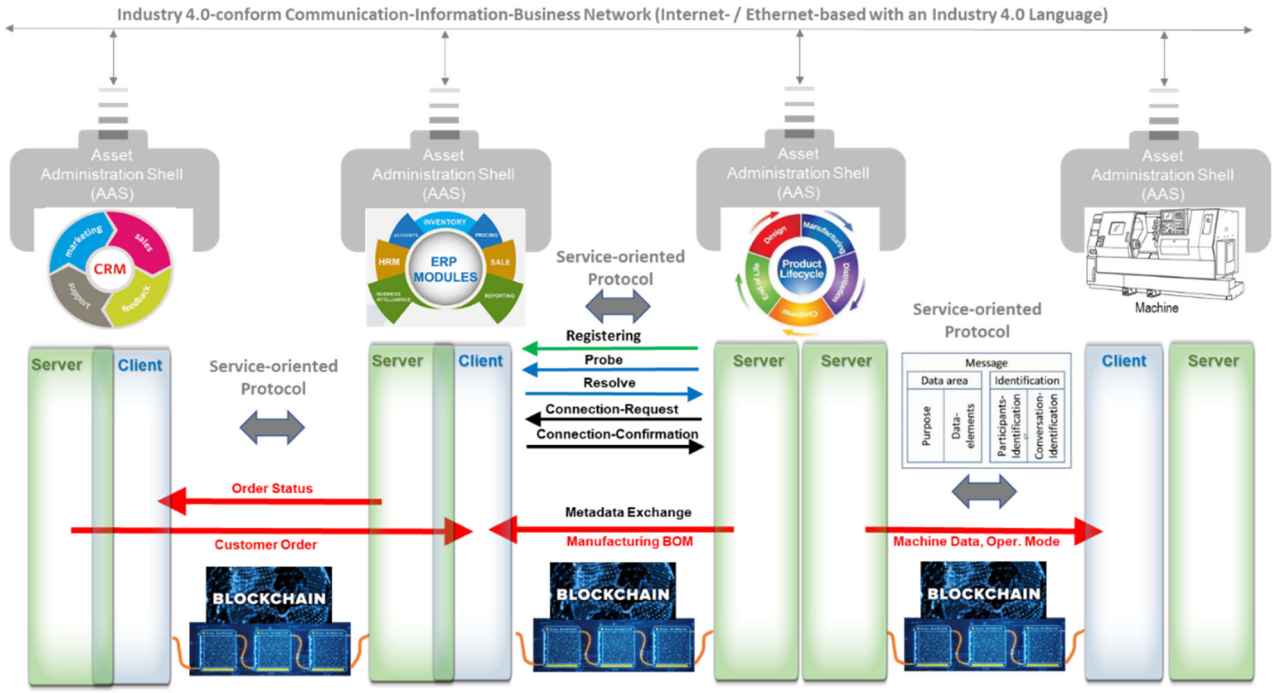

FIGURE 6- Blockchain into Industry 4.0-compliant Systems.

There has been a substantial number of prototype implementations exploiting the features offered by Blockchain in the industrial manufacturing sector with a focus on supply chain management. The benefits are enormous, for example, reducing inventory costs and service times, automating trading and business negation 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 Life Cycle dimension (IEC 62890) as 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 for achieving desired business competitiveness. The AAS-based approach allows a smoothly integration and sharing among the digitalized (cooperating) assets [68]. Major requirements like, interoperability, security, trust and fundamentally 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. As a matter of fact, adequate open but secured information storage and customized Blockchain information service such as Machine Data or Operational Modes can be shared between a digitalized PLM at the IT level and digitalized machines located at the OT (Operation Technology) levels of the enterprise. On one side, this AAS- and Blockchain-based infrastructure can not only process the multi-source and heterogeneous services from the two named assets, but also broadcast the exposed services to the Industry 4.0- and Blockchain-conform 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 co-creation of Enterprise Resource Planning applications, as well as quick and accurate tracking and tracing of manufacturing orders with an AAS-based digitalized CRM. With the successful development of the proposed solution, service-based interoperability and cooperation between digitalized stakeholders (assets) in the entire value stream and lifecycle is guaranteed.

The Mobility Open Blockchain Initiative (MOBI) and OriginTrail [73] are another examples of Blockchain-based solutions. MOBI was founded by automakers such as Renault, Ford, GM 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". 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) tested Blockchain technology in logistics operations [74]. In China, Alibaba established supET [75], a platform for Blockchain applications in industrial Internet. A considerable set of new use cases are being reported in other industrial manufacturing sectors like Industry 4.0, Industrial IOT, etc. This confirms potentials and challenges as well outlooks future research and innovation opportunities to further exploit the advantages of the Blockchain technology.

The challenges for adoption of Blockchain in manufacturing systems in Industry 4.0 lie in its role to enhance process optimisation (e.g. logistics optimisation and product life cycle improvisation) and security and authentication (i.e. making parts tamper-proof and cross-referenced, identify management) [76]. While the dynamical responsiveness is not required as much as the power and energy systems, the complex and diverse nature of manufacturing systems would make the scalability and flexibility the prominent issues. The enormous scale of IoT features in Industry 4.0 means there are huge amounts of critical information and privacy-sensitive information which need to be protected from cyber-attacks. However, due to the limited resources, executing security functionalities is difficult to meet the security needs. This requires efficient consensus algorithms which can deal with the problems in a distributed way fast. 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 which is scalable and secure is a challenge, and this also applies to authorization, authentication and integrity.

Robotics & Mechatronics, and Other IE Areas

Blockchain has implications to many other key IE areas. For example, combining AI with Blockchain can improve efficiencies in swarm robotics, autonomous vehicles, or they can even help bitcoin mining in a secure, flexible and autonomous way similar to power and energy systems. Swarm robotics is seen as an area benefiting from combination of Blockchain and AI. A team of autonomous robots work together in a "swarm" to perform tasks or operations; their collective behaviour 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 datasets to be shared, updated, and trained safely and securely, making wider adoption of AI possible [78]. In fact, many systems and control issues can benefit from Blockchain, especially in the multiagent system setting, where individual components cooperate to achieve a common goal fast 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 & mechatronics, and other IE areas. The dynamical responsiveness requirements would be more stringent and resources-light and flexible Blockchain platforms are needed. The future of Blockchain is very bright though technological challenges are enormous to make it work.

4. CONCLUSIONS

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

5. REFERENCES

1. N. U. Hassan, et al., “Blockchain technologies for smart energy systems: Fundamentals, challenges, and solutions,” IEEE Industrial Electronics Magazine, vol. 13, no. 4, pp. 106-118, December 2019.
2. T. Aste, et al., “Blockchain technologies: The foreseeable impact on society and industry,” Computer, vol. 50, no. 9, pp. 18-28, 2017.
3. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” White Paper, 2008. https://bitcoin.org/bitcoin.pdf (accessed 15 June 2020).
4. P. K. Sharma, et al., “DistBlockNet: a distributed blockchains-based secure SDN architecture for IoT networks,” IEEE Communications Magazine, vol 55, no. 9, pp. 78-85, September 2017.
5. V. Buterin, “Ethereum: A next-generation smart contract and decentralized application platform,” 2013. http://ethereum.org/ethereum.html (accessed 15 June 2020).
6. L. Lu, et al., “Pseudo trust: Zero-knowledge authentication in anonymous P2Ps,” IEEE Transactions on Parallel and Distributed Systems, vol. 19, no. 10, pp. 1325-1337, October 2008.
7. D. Hopwood, et al., “Zcash protocol specification,” Zerocoin Electric Coin Company, Oakland, CA, USA, Technical Report, 10 January, 2016.
8. E. Ben-Sasson, et al., “Succinct non-interactive zero knowledge for a von neumann architecture,” Proceedings of the 2014 USENIX Security Symposium, San Diego, CA, pp. 781-796, 20–22 August, 2014.
9. Y. Yuan, et al., “Blockchain consensus algorithms: the state of the art and future trends,”

Acta Automatica Sinica (in Chinese), vol. 44, no. 11, pp. 2011-2022, 2018.

10. L. Lamport, “The part-time parliament,” ACM Transactions on Computer Systems, vol. 16, no. 2, pp. 133-169 1998.
11. L. Lamport, et al., “In search of an understandable consensus algorithm,” Proceedings of the USENIX Annual Technical Conference, Philadelphia, PA, pp. 305-320, 19-20 June , 2014.
12. M. Castro, et al., “Practical byzantine fault tolerance,” Proceedings of the Operating Systems Design and Implementation, vol. 99, pp. 173–186, 1999.
13. D. Mazières, “The stellar consensus protocol: a federated model for internet-level consensus, ” [Online], available: https://www.stellar.org/papers/stellar-consensus-protocol.pdf, (accessed on 20 September 2020).
14. Y. Gilad, et al., “Algorand: scaling byzantine agreements for cryptocurencies,” [Online], available: http://eprint.iacr.org/2017/454, (accessed on 20 September 2020).
15. R. Pass and E. Shi, “The sleepy model of consensus,” [Online], available: https://eprint.iacr.org/2016/918.pdf, (accessed on 20 September 2020).
16. I. Eyal, et al., “Bitcoin-NG: a scalable blockchain protocol,” In: Proceedings of the 13th USENIX Conference on Networked Systems Design and Implementation. Santa Clara, USA: USENIX Association, 2016. 45-59.
17. E. K. Kogias, et al., “Enhancing bitcoin security and performance with strong consistency via collective signing,” In: Proceedings of the 25th USENIX Security Symposium. Austin, TX, USA: USENIX Association, 2016. 279-296.
18. J. P. Buntinx, “What is proof of elapsed time?” [Online], available: https://themerkle.com/what-is-proof-of-elapsed-time/, (accessed on 20 September 2020).
19. M. Milutinovic, et al., “Proof of luck: an efficient blockchain consensus protocol,” [Online],

available: https://eprint.iacr.org/2017/249.pdf, (accessed on 20 September 2020).

20. G. Ateniese, et al., “Proofs of space: when space is of the essence,” In: Proceedings of the 9th International Conference on Security and Cryptography for Networks. Amalfi, Italy: Springer, 2014. 538-557
21. M. Ball, et al., “Proofs of useful work,” [Online], available: https://allquantor.at/blockchain-bib/pdf/ball2017proofs.pdf, (accessed on 20 September 2020).
22. S. King and S. Nadal, “Ppcoin: Peer-to-peer crypto-currency with proof-of-stake,” Self-Published Paper, vol. 19, August, 2012.
23. D. Larimer, et al., “BitShares 2.0: Financial smart contract platform,” [Online], available: http://docs.bitshares.eu/downloads/bitshares-nancial-platform.pdf, (accessed on 20 September 2020).
24. J. Kwon, “Tendermint: consensus without mining,” [Online], available: https://tendermint.com/static/docs/ten-dermint.pdf, (accessed on 20 September 2020).
25. “Ethereum’s Casper protocol explained in simple terms,” [Online], available: https://www.finder.com/ethereum-casper, (accessed on 20 September 2020).
26. A. Miller, et al., “Permacoin: Repurposing bitcoin work for long-term data preservation,” 2014 IEEE Symposium on Security and Privacy, IEEE Computer Society, 2014, 1: 475-490.
27. L. Ren, “Proof of stake velocity: building the social currency of the digital age,” [Online], available: https://assets.coss.io/documents/white-papers/reddcoin.pdf, (accessed on 20 September 2020).
28. “Proof of burn,” [Online], available: https://en.bitcoin.it/wiki/Proof of burn, (accessed on 20 September 2020).
29. I. Bentov, et al., “Proof of activity: extending Bitcoins proof of work via proof of stake,”

[Online], available: http://eprint.iacr.org/2014/452, (accessed on 20 September 2020).

30. Y. Xiao, et al., “A survey of distributed consensus protocols for blockchain networks,” IEEE Communications Surveys & Tutorials, DOI: 10.1109/comst.2020.2969706, 2020.
31. N. Szabo, “Smart Contracts,” [Online], available: http://szabo.best.vwh.net/smart.contracts.html (accessed 15 June 2020).
32. T. T. A. Dinh, et al., “Untangling blockchain: A data processing view of blockchain systems,” IEEE transactions on knowledge and data engineering, vol. 30, no. 7, pp. 1366-1385, 2018.
33. “Hyperledger Project,” [Online], available: https://www.hyperledger.org/ (accessed 15 June 2020).
34. S. Wang, et al., “An overview of smart contract: architecture, applications, and future trends,” 2018 IEEE Intelligent Vehicles Symposium (IV), Changshu, China, pp. 108-113, 26-30 June, 2018.
35. “The energy web chain: Accelerating the energy transition with an open-source, decentralizedblockchain platform,” Energy Web Foundation, Zug, Switzerland.[Online]. Available:https://energyweb.org/wp-content/uploads/2018/10/EWF-PaperTheEnergyWebChain-v1-201810-FINAL.pdf (accessed on 20 September 2020).
36. “Solar Bankers: Initial coin offering whitepaper,” Solar Bankers, Prague, Czech Republic, White Paper. [Online]. Available: https://solarbankers.com/wp content/uploads/2017/10/SB-White-Paper_version2.pdf (accessed on 20 September 2020).
37. J. Steiner and J. Baker, ``Blockchain: The solution for transparency in product supply chains," Project Provenance Ltd., London, U.K., White Paper, 2015. [Online]. Available: https://www.provenance.org/whitepaper (accessed on 20 September 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 on 20 September 2020).

39. Genesis of Things Project. [Online]. Available: http://www.genesisofthings.com/, (accessed on 20 September 2020).
40. G. Yu, et al., "Survey: Sharding in blockchains," IEEE Access, vol. 8, pp. 14155–14181, 2020.
41. A. Zamyatin, et al., "Sok: Communication across distributed ledgers," IACR Cryptology ePrint Archive, 2019: 1128, Tech. Rep., 2019.
42. T. Salman, et al., "Security services using blockchains: A state of the art survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 858-880, 2019.
43. A. Jake and S. Nathalie-Kyoko, "Behind the biggest bitcoin heist in history: Inside the implosion of mt.gox," [Online], available: https://www.thedailybeast.com/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion-of-mt-gox, (accessed on 20 September 2020).
44. V. Buterin, "Critical update re: Dao vulnerability," [Online], available: https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/, (accessed on 20 September 2020).
45. N. Ivica, et al., "Finding the greedy, prodigal, and suicidal contracts at scale," ACSAC '18: Proceedings of the 34th Annual Computer Security Applications Conference, San Juan PR USA, pp. 653–663, December 2018.
46. D. Dasgupta, et al., "A survey of blockchain from security perspective," Journal of Banking and Financial Technology, vol. 3, no. 1, pp. 1–17, 2019.
47. "EOS: An open source smart contract platform," GitHub. 2 October 2018. Retrieved 2 October 2018.

48. W. Song, et al., “Research on the application of blockchain in the energy power industry in China,” IOS Journal of Physics: Conference Series, vol. 1176, 042079, 2019.
49. A. Kosba, et al., “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” 2016 IEEE Symposium on Security and Privacy(SP), San Jose, CA, USA, pp. 893-858, 22-26 May, 2016.
50. S. F. Sun, et al., “RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero,” Computer Security-ESORICS 2017. Lecture Notes in Computer Science, vol. 10493. Springer, Cham.
51. W. T. Li, et al., “Securing proof-of-stake blockchain protocols,” Data Privacy Management, Cryptocurrencies and Blockchain Technology. DPM 2017, CBT 2017. Lecture Notes in Computer Science, vol. 10436. Springer, Cham.
52. H. Huang, et al., “When blockchain meets distributed file systems: An overview, challenges, and open issues,” IEEE ACCESS, vol. 8, pp. 50574–50586, 2020.
53. “Decentralized Identifiers (DIDs): Core architecture, data model, and representations,” [Online], available: https://w3c.github.io/did-core/, (accessed on 20 September 2020).
54. “A gentle introduction to self-sovereign identity,” [Online], available: https://bitsonblocks.net/2017/05/17/gentle-introduction-self-sovereign-identity/, (accessed on 20 September 2020).
55. X. Yu and Y. Xue, “Smart Grids: A cyber-physical systems perspective,” Proceedings of the IEEE, vol. 104, no. 5, pp. 1058-1070, 2016.
56. M. E. Peck: “Do you need a blockchain?” IEEE Spectrum, vol 54, no. 10, October 2017
57. ETIP SNET WG4: Digitalization of the electricity system and customer participation. Technical Position Paper WG4, September 2018.

58. “Starting from the micro power grid, Energo tries to build a decentralized energy transaction system using blockchain” .http://www.8btc.com/energo-labs-blockchain , in Chinese (accessed on 25 January 2018).
59. A. S. Musleh, et al.,“Blockchain applications in smart grid–review and frameworks” IEEE Access, vol. 7, pp. 86746-86757, 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,” Proceedings of the 16th International Conference on the European Energy Market (EEM), Ljubljana, Slovenia, pp. 1-8, 2019, doi: 10.1109/EEM.2019.8916268.
61. K. Döppenbecker, “Undertaking energy transition”, interview with TenneT’s Digital Transformation Lead René Kerkmeester, 2019. https://www.tennet.eu/fileadmin/user_upload/ArtikelTenneT.pdf (accessed 15 June 2020).
62. TenneT: “Equigy platform gives European consumers access to tomorrow's sustainable energy market,” TenneT Press Release 23. April 2020
63. IEEE Standard P2418.5 - Standard for Blockchain in Energy, 2018
64. A. W. Colombo, et al., “Industrial cyber-physical systems: A backbone of the fourth industrial revolution,” IEEE Industrial Electronics Magazine, vol. 11, no. 1, pp. 6-16, 2017.
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.
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 on 24May 2020) .

67. DIN SPEC 91335 RAMI4.0. https://dx.doi.org/10.31030/2436156 (accessed 15 June 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 22 May 2020).
69. https://www.bitdeal.net/blockchain-in-industry-4-0 (accessed on 25 May 2020).
70. Blockchain Technology for Industry 4.0. Rodrigo da Rosa Righi et.al. (Eds.). Springer Nature 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 on 20 May 2020).
72. Blockchain and Industry 4.0. https://www.capgemini.com/au-en/wp-content/uploads/sites/9/2018/10/Blockchain-and-Industry-4.0.pdf (accessed on 20 May 2020)
73. https://www.themanufacturer.com/articles/blockchain-technology-changing-manufacturing-industry/ (accessed on 10 June 2020).
74. https://www.blockchainexpert.uk/blog/application-of-blockchain-in-manufacturing (accessed on 10 June 2020).
75. “Application of blockchain in industrial Internet by Ali Cloud” http://www.cqvip.com/QK/80675A/201822/7000940533.html, in Chinese (accessed on 12 June 2020).
76. A. Mushtaq, I.U. Haq, “Implications of blockchain in industry 4.0,” Proceedings of the 2019 International Conference on Engineering and Emerging Technologies, pp. 2409-2983, Lahore, Pakistan, 21-21 February 2019.

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 on 09 June 2020).

78. R. Shroff, “When blockchain meets Artificial Intelligence”, https://medium.com/swlh/when-blockchain-meets-artificial-intelligence-e448968d0482 (accessed on 12 June 2020).