Sustainable Energy, Grids and Networks 28 (2021) 100553

Contents lists available at ScienceDirect

Sustainable Energy, Grids and Networks

journal homepage: www.elsevier.com/locate/segan

Standardization of the Distributed Ledger Technology cybersecurity stack for power and energy applications

Sri Nikhil Gupta Gourisetti [a], Ümit Cali [b,*], Kim-Kwang Raymond Choo [c], Elizabeth Escobar [d], Christopher Gorog [e], Annabelle Lee [f], Claudio Lima [g], Michael Mylrea [h], Marco Pasetti [i], Farrokh Rahimi [j], Ramesh Reddi [k], Abubakar Sadiq Sani [l]

[a] Pacific Northwest National Laboratory, Richland, WA, USA
[b] Norwegian University of Science and Technology, Trondheim, Norway
[c] University of Texas at San Antonio, San Antonio, TX, USA
[d] Duke Energy Corp., Charlotte, NC, USA
[e] BlockFrame Inc., Colorado Springs, CO, USA
[f] Nevermore Security, Evergreen, CO, USA
[g] BEC-Blockchain Engineering Council, Houston, TX, USA
[h] National Resilience Inc., Washington, DC, USA
[i] University of Brescia, Department of Information Engineering, Brescia, Italy
[j] Open Access Technology International Inc., Minneapolis, MN, USA
[k] CybSecBCML Inc., Raleigh, NC, USA
[l] University of Greenwich, School of Computing and Mathematical Sciences, London, UK

ARTICLE INFO

Article history:
Received 4 August 2021
Received in revised form 20 October 2021
Accepted 24 October 2021
Available online 29 October 2021

Keywords:
Distributed Ledger Technology (DLT)
Blockchain
Power systems
Distributed energy resource (DER)
Cybersecurity
Smart grid

ABSTRACT

The global trend toward integration of distributed energy resources is opening doors to advanced, complex, and distributed marketplaces. Such advanced ecosystems, where utility-owned and non utility-owned assets can contribute toward grid operations, generally require distributed communication and grid architectures. We posit the potential of using Distributed Ledger Technologies (DLTs) in supporting such applications, although their full potential has not been fully used, for example in designing long-term scalable solutions in operational technology applications. This is partly due to the lack of standardization across and between different DLTs, as well as other supporting building blocks (*e.g.*, communication protocols). This paper attempts to address this gap by proposing a DLT cybersecurity stack specifically designed for researchers, DLT technology developers, and end users (such as utilities). The DLT cybersecurity stack has been notionally mapped to related cybersecurity components, namely the Open Systems Interconnection (OSI) model, the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, and existing Smart Grid architecture frameworks. In addition, the paper discusses several cybersecurity implications, and demonstrates the potential uses of the DLT cybersecurity stack through multiple power and energy use cases. It is important to note that the stack can be also applied to the DLT use cases that are outside the power and energy domain. This work was performed by the Cybersecurity Task Force under the IEEE P2418.5 Blockchain for Energy Standard working group that part of the IEEE Power and Energy Society's Smart Buildings, Loads, and Customer Systems (SBLC) technical committee.

1. Introduction

Grid modernization has given impetus to innovative power grid applications, with the potential of improving the reliability, efficiency, flexibility, and control of energy resources that are increasingly distributed and renewable [1–3]. These changes, however, have introduced new cybersecurity implications and challenges for utility and market operators [4–6]. In other words, improving the confidentiality, availability and especially the integrity of power grid data and communications in transit is

* Corresponding author.
E-mail addresses: gigupta@ualr.edu (S.N.G. Gourisetti), umit.cali@ntnu.no (Ü. Cali), raymond.choo@fulbrightmail.org (K.-K.R. Choo), elizabeth.escobar-fernandes@duke-energy.com (E. Escobar), cgorog@blockframetech.com (C. Gorog), ablee@nevermoresecurity.com (A. Lee), clima@blockchain-eng.org (C. Lima), michael.mylrea@resilience.com (M. Mylrea), marco.pasetti@unibs.it (M. Pasetti), farrokh.rahimi@oati.net (F. Rahimi), ramesh.m.reddi@cybsecbcml.com (R. Reddi), s.sani@greenwich.ac.uk (A.S. Sani).

https://doi.org/10.1016/j.segan.2021.100553

imperative in satisfying the emerging requirements of modern power systems, by offering secure and trustworthy operations.

In recent times, blockchain – also referred in the literature as Distributed Ledger Technology (DLT) – has been viewed as a potential technology that could unlock new opportunities and features for the modern power systems and markets [7]. Several articles in the scientific literature have reported that DLTs can be leveraged to manage cybersecurity in smart grids, by also emphasizing that, if not properly implemented, applications of DLT in power grid operations also may introduce potential cybersecurity issues. Ref. [8] recently proposed a comprehensive survey on the use of DLTs for the cybersecurity of smart grids, considering both applications and technological perspectives. Ref. [9] identified significant security challenges of smart grid scenarios that can be addressed by DLTs. Ref. [10] investigated how the combined application of the Internet of Things (IoT) paradigm and DLTs could introduce significant transformations across several industries, including the power and energy sector. Ref. [11] demonstrated how DLT can be used to provide improved security in operational Supervisory Control and Data Acquisition (SCADA) networks. Ref. [12] presented an architecture for peer-to-peer energy markets that can guarantee operational constraints are respected and payments are fairly rendered, without relying on a centralized utility or microgrid aggregator. Ref. [13] explored the application of blockchain and smart contracts to improve smart grid cyber resiliency and secure transactive energy applications. Ref. [14] explored how a Keyless Signature Blockchain Infrastructure (KSBI) technology may help securing critical energy infrastructure from evolving cyber threats and vulnerabilities. Finally, Ref. [15] emphasized the need for future developments and solutions to overcome challenges that are associated with the standardization of the energy DLT applications.

Despite the importance of cybersecurity, existing literature and standardization bodies have not sufficiently and systematically investigated the broad range of cybersecurity concerns and perspectives associated with the use of DLTs in power grid applications [16]. To fill this gap, this study, conducted by the cybersecurity task force under the IEEE P2418.5 Standard for Blockchain in Energy working group [17–19], posits the importance of standardization in DLTs by identifying and systematically analyzing existing literature gaps concerning the cybersecurity of DLTs in power and energy applications. Several of the questions addressed in this paper are listed below:

- What is DLT and how does it work, particularly in the context of a Smart Grid?
- What is a potential conceptual framework that would ease use case exploration and adoption?
- What are the potential DLT-related cybersecurity risks?
- What does standardization mean for the energy and power grid applications?
- What does a DLT technical stack look like and how does it complement existing frameworks?

The objective of this paper is to address the above questions and pioneer the standardization efforts for DLT-based power and energy applications. On this note, we will now explain the novel contributions of this paper. Based on our review of the existing literature, this study discusses the (identified) DLT-related cybersecurity risks and proposes a seven-layer DLT cybersecurity stack that comprises several relevant (cybersecurity) components and attributes. The existing Smart Grid architecture frameworks, such as GridWise [20] and the Smart Grid Architecture Model (SGAM), the Open Systems Interconnection (OSI) model, and the Transmission Control Protocol/Internet Protocol (TCP/IP) suite model are mapped to the seven-layer stack. A set of relevant (energy-related) use cases are proposed and used as illustrations to demonstrate the usability and applicability of the seven-layer DLT cybersecurity stack. For each use case, a detailed and easy to follow explanation for some of the technology and security properties that underpin blockchain is proposed, with extended discussions on potential cybersecurity gaps.

The aim of this study is to establish the cybersecurity foundations for the IEEE P2418.5 Standard for Blockchain in Energy working group. The proposed cybersecurity stack can be used as an architectural framework that is synergistic with the function of power grid applications. Furthermore, the DLT cybersecurity stack is designed to be used with existing cybersecurity and DLT applicability models [21,22]. With this contribution and improved standardization, risk averse energy utilities may be more open to exploring the potential opportunities around blockchain technology; for example, storing and securing grid communications and data. At the same time, utilities may take advantage of new power grid automation and innovation that can help increase the reliability, flexibility, and control opportunities introduced by grid modernization. The proposed cybersecurity stack also is designed to be compatible with existing and emerging DLT offerings. The authors followed three principles to assure technology neutrality. First, we strictly avoid the use of any particular DLT as part of the study conducted. This principle is followed to conduct a fully impartial study of the presented subject from a DLT offering perspective. Second, we demonstrate the construction or development of a DLT or a software of similar nature. This principle is followed to avoid inadvertent dictation of a use of particular consensus or DLT architecture. Presented work unanimously applies to all DLT architectures agnostic to the underlying parameters such as consensus, ledger structure, and smart contract framework. Third, we avoid accidentally or intentionally contradicting any ethical and engineering constructs guided by the core principles of the IEEE Standards Association [23].

The paper is organized as follows. Section 2 provides a contextual overview and definitions of DLT related attributes. Section 3 articulates the potential cybersecurity benefits, risks, and attack surface implications pertaining to DLT-based power and energy applications. Section 4 presents the proposed DLT cybersecurity stack and its mapping to SGAM, TCP/IP, and OSI models. This section also discusses several cybersecurity considerations. Section 5 illustrates five high-impact power and energy use cases, demonstrates the use case mapping to the seven layer DLT cybersecurity stack, and articulates use case specific cybersecurity considerations. The final section concludes this paper and describes future work.

2. Definitions of DLT related attributes

This section provides an overview of key definitions that are relevant to DLT and its application to power and energy applications.

CIA: The cybersecurity objective triad is Confidentiality, Integrity, and Availability (CIA). In most Information Technology (IT) systems the primary security objective is confidentiality. In contrast, for Operational Technology (OT) systems, the primary security objective is availability, partly evidenced by the ransomware attacks on smart grids. One of the few exceptions is automated metering for which confidentiality is critical.

DLT: A DLT enables recording data in multiple systems (nodes) in an asynchronous fashion while allowing multiple parties to read the data. The key characteristics of DLT are:

Asymmetric cryptography: Asymmetric (public and private key) cryptography is typically implemented by DLTs to ensure non-repudiation and data integrity.

Non-repudiation: Non-repudiation ensures that the individual/device that digitally signs the data with their private key

cannot deny that they have signed the data. The private key is known only by the owner and is not shared. The associated public key is used by the receiver to verify that the transmitted data has not been altered in transmission. The public key may be sent to multiple recipients/devices.

Specifically, the private key of the sender is used in the generation of a message digest that is sent with the message. The message is sent in the clear, that is, the data is not encrypted. The receiver of the message generates a message digest using the public key of the sender. The two message digests must match to ensure the data has not been altered in transmission. Asymmetric cryptographic does not include data encryption for confidentiality. Current blockchain/DLT implementations do not include symmetric key cryptography as an inherent component. Depending on the specific DLT implementation, symmetric key cryptography for confidentiality may augment the asymmetric cryptography.

Immutability: Once a transaction is recorded [24], it is very difficult to delete or rollback that transaction. This ensures the provenance of the transaction. Immutability is implemented using sequential hashing and a digital signature.

Anonymity: Each transaction is digitally signed with a private key that is known only by the owner. Therefore, the "real" identity of the owner is not revealed.

Traceability: Every transaction added to the ledger is digitally signed and timestamped. This provides for a link to the previous block. Therefore, a full history back to the beginning can be reconstructed .

Data integrity: This includes tamper evidence by providing the ability to identify data modification and tamper resistance, which is the difficulty of modifying past transaction records. Data integrity is implemented using cryptographic digital signatures. Data integrity mechanisms are used to identify any data tampering (it is worth noting that it is not possible currently to prevent data tampering).

Transactions are digitally signed with the private key of the sender and verified by the receiver using the associated public key of the sender. A timestamp and a hash of the transaction (Merkle tree) are also included in the transaction.

A cryptographic hash function maps strings of bits to fixed-length strings of bits. The function should satisfy the following two properties:

1. *One way*: It is computationally infeasible to find for a given output an input which maps to this output, and
2. *Collision resistant*: For a given input, it is computationally infeasible to find a second input that maps to the same output.

DLT Classes: There are two general classes of DLT: private (permissioned) and public (permissionless) [25].[1] In a public architecture, all of the following conditions apply:

- Anyone in the system can participate.
- Read/write access is open to all participants.
- Any node can participate in the consensus process.
- Transactions are visible to all participants.

This means that the DLT state and its transactions are transparent and accessible to everyone. Any node joining a public DLT network can validate transactions including those from rogue nodes. To mitigate attacks from malicious nodes, the DLT network implements a consensus algorithm. Currently, several consensus algorithms exist, such as Proof of Work (PoW) [25], Proof of Stake (PoS), Proof of Authority (PoA) [26], Proof of Control (PoC), Proof of Burn (PoB) [27], Byzantine Fault Tolerance (BFT)-based consensus [28,29], *etc.* These help ensure that the system will arrive at consensus and continue to operate even when node(s) fail or are corrupted. In a private architecture, the following conditions apply:

- Only participants with permissions can participate.
- Read and write access requires permissions.
- Transactions are visible to participants who have been granted permission.

Consequently, only authorized and trusted entities can participate in the activities within the DLT. By allowing only authorized entities to participate in activities within the DLT, a private architecture can help ensure the privacy of the chain data.

For the energy sector, private DLTs are recommended if there is sensitivity of the power grid application data. This requires implementation of identification and authentication security controls for participating devices and individuals. In addition, security gains also require that the blockchain and associated applications, operating systems, *etc.* are developed, deployed and managed with cybersecurity best practices. DLT is not a panacea, and many deployments have failed in the absence of cybersecurity basics. A comparative analysis of public permissionless and private permissioned blockchains is provided in Appendix.

3. DLT standardization and cybersecurity characteristics for the energy sector

The IEEE P2418.5 Blockchain in Energy Standards Working Group (WG) aims to propose, develop, and disseminate a set of standardization procedures and a framework to generate holistic and applicable DLT related guidelines for the energy industry by also aiming at the following objectives:

- Design, offer and develop an inter-operable, safe, open, and applicable standardization framework that is based on the solid reference architecture framework for the energy sector (mainly for the power industry, and partially oil and gas industry).
- Conceptualize the initial reference architecture framework and map selected energy use cases where blockchain technology can be implemented with the proposed framework. The energy use cases are identified by the WG members, industrial surveys, and detailed literature reviews continuously.
- Further develop the initially proposed reference architecture framework by interacting with other IEEE Standardization WGs and other related organizations such as the IEEE Blockchain enabled Transactive Energy (BCTE) Initiative in a coordinated way that aims to effectively enable coordination and create synergies. Some essential tasks, such developing initial architecture, development of demonstration projects and further communication activities, are accomplished in initiatives with IEEE BCTE ; and
- Publicize the outcomes of the WG with the global audience via articles, position papers, reports, newsletter, panels, webinars and standards documents.

The IEEE P2418.5 WG in built on the Task Forces (TFs): (1) Use Cases, (2) Interoperability, (3) Cybersecurity, and (4) Smart Contracts. The general structure of the IEEE P2418.5 WG is depicted in Fig. 1.

Interoperability and scalability are some of the key factors for technology real-world deployment. Such maturity can be achieved through standardizing the underlying building blocks

[1] The authors recognize that there are experimental architectural and implementations that could be categorized as *Hybrid* and may not fall under either of the classes. Due to its evolving nature, *hybrid* class is not discussed in this paper but may be considered in future publications.

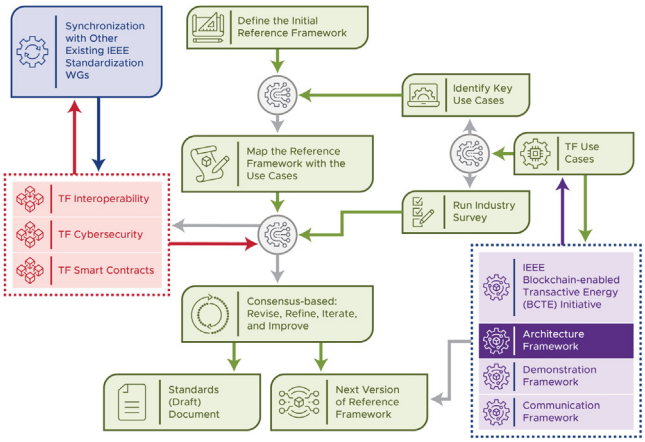

Fig. 1. General structure of the IEEE SA P2418.5 Working Group.

such as protocols, data structures, hierarchical functions within the technology, *etc.* This section provides a detailed overview of various cybersecurity risks, benefits, attack surfaces, and key technical questions and considerations that can be addressed through standardization.

3.1. Cryptographic key management and performance impact

DLT relies on the use of cryptographic algorithms, specifically asymmetric (public/private) cryptography and secure hash algorithms. Specification of the cryptographic algorithms and key management processes (*e.g.*, generation, storage, escrow, distribution, revocation, update) is not included in a general DLT document. However, these algorithms and processes are critical to the effectiveness and security of a DLT. Typically, a Public Key Infrastructure (PKI) is implemented that is responsible for all key management activities. Using a blockchain-based key management system that is integrated with an existing X.509 PKI is recommended. This will require the implementation of a Certificate Authority (CA) responsible for generating and distributing digital certificates. A certificate revocation list or Online Certificate Status Protocol (OCSP) maintains the list of certificates that are no longer valid.

To mitigate vulnerabilities related to weak or flawed implementation of the cryptography, validated cryptographic algorithms and cryptographic modules should be implemented. If key management is not implemented correctly, the integrity of the DLT can be compromised. Credentialing the participants is important to ensure integrity, non-repudiation, and authentication.

Performance impact: For the OT environment, performance and latency are critical. Cryptographic key management is performance intensive. If used in the OT environment, this needs to be assessed. If the DLT is implemented in the corporate domain, this is not as significant an issue.

3.2. Cybersecurity benefits

At a technology level, the majority of the DLT benefits could be grouped under two areas: (1) integrity, *i.e.*, tamper evidence, and resistance and (2) availability and network fault tolerance. The list of benefits may grow when a DLT is evaluated in the context of a use case. In this subsection, the above two benefits are briefly discussed:

Tamper Evidence and Resistance: Outside of the financial tech space, DLTs typically are presented as solutions due to their tamper resistance properties that make them useful as robust audit logs that ensure the integrity of data. In a DLT, historical records are generally bound to the current state of the database via cryptographic hash functions. Due to the computational hardness of attacking this association (finding targeted hash collisions), malicious changes to past records are unlikely to be successful and are likely to be detected.

By default, conventional databases are not designed to be tamper-evident in this manner. Attackers with root access to machines where the database is stored have the ability to change its contents. Without sufficient monitoring, attacks may even go undetected. In addition, many of these databases are centralized, meaning that there are single or few points that an attacker needs to target to tamper with data. DLTs are naturally designed to require monitoring by a fairly large network, so to successfully tamper with data on the DLT, an attacker potentially needs to target the entire (or majority of) the network (*e.g.* Sybil Attacks, as discussed later in this subsection) to accomplish this. This gives DLTs a degree of robustness to attack that conventional databases do not typically have by design in a distributed trust setting.

Availability and Network Fault Tolerance: Centralized datastores often have limited access to networks that can be easily disrupted by single, localized events (such as a power failure, loss of network connectivity, adverse weather, natural disasters, or adversarial attack). These events prevent users from pulling the data that they need when they need it and making necessary changes. In a DLT, the maintenance and access of the data is redundantly provided by the whole network. This gives distributed ledger users the ability to safely access the ledger by communicating with most participating nodes on the network. This increased level of access makes the data very available in a manner that is tolerant to abrupt connectivity issues in the network. It should be noted that this is not a unique benefit to distributed ledgers as distributed databases (no Blockchain-like architecture) have existed for a while.

3.3. Cybersecurity risks

Similar to the benefits discussed in the above section, cybersecurity risks may change when DLT is analyzed in the context of a use case. The objective of this subsection is to briefly discuss known risks that were captured in the literature, namely (1) attacks on the cryptography [25], (2) denial of service (DoS) [30,31], (3) Sybil attacks [32], (4) selfish mining attacks, (5) unauthorized access [33,34], and 6) bugs in smart contracts.

Attacks on Cryptography: DLTs rely heavily on cryptography to enforce their security properties and enable certain capabilities that are not normally possible or feasible without cryptography. Due to the nature of the field, the security of most cryptographic capabilities is based on fundamental, unproven assumptions about the hardness of certain computational problems. If these assumptions are not fully implemented, there are almost certainly weaknesses in the application that use them. For instance, some standardized cryptographic schemes rely on the difficulty of factoring large composite integers into their prime factors. Even now, an efficient algorithm for integer factorization is not known to exist nor is there a known proof of computational hardness. For example, there have been a number of studies that revealed vulnerabilities in various cryptographic primitives that underpin (popular) DLTs [35–37].

This is not merely an existential problem. Many DLT implementations use cryptography that has been around for nearly two decades and for which security was calibrated to specified security levels, performance requirements, and known offensive techniques at the time. Because expectations in computing power grow as time progresses, cryptography has a limited shelf-life, usually on the order of a few decades. The anticipated introduction of scalable quantum computers that can crack these

standards has pushed cryptographers and standardization bodies, such as the National Institute of Standards and Technology (NIST), to seek replacement cryptographic methods. NIST has an ongoing competition to design and evaluate next generation, post-quantum cryptography. The potential loss in security due to quantum computing has led to a great interest in adapting more secure cryptographic primitives for the DLT systems and transition plans. This concern is primarily applicable to asymmetric cryptographic algorithms. The current view is that symmetric and hash algorithms still will be useful when quantum computing becomes commercially available. The recommendation will be to use longer key sizes for symmetric algorithms and larger hash sizes.

Denial of Service: DLT architectures tend to heavily rely on network connectivity to quickly propagate state changes through the decentralized system. For many designs, the communication overhead scales along with the size of the network, security level, and sophistication of the interactions. This makes these decentralized systems highly susceptible to DoS attacks mounted by adversaries. Distributed ledger systems can significantly slow down, become more expensive to operate, or even stall with a sufficient amount of interference. In most cases, it is fairly inexpensive to generate and simulate multiple identities or connections to a distributed network, requiring that mechanisms be added to deter them. This is generally addressed by imposing a cost (largely seen in a PoW or stake mechanism) or by limiting access to the network by requiring permissions (largely seen in PoA or voting based consensus).

Sybil Attack: Many DLTs rely heavily on their consensus network to make the correct determination about the current state of the chain. This often requires delegating the trust for this task to the majority (greater than 50%) of participants on the network. Having more honest participants verifying transactions and changes on a blockchain increases the network's resilience to a colluding majority that attempts to cheat.

A Sybil attack is characterized by the use of constructed identities or an atypical amount of resources to attempt to artificially create a colluding majority. For consensus networks based on raw votes, a Sybil attacker would create many fake identities to control more votes. If the attackers can obtain a controlling share of the network, they can force through changes that they wish. Because false identities can be fairly cheap to create, some blockchain implementations opt for consensus mechanisms that have a bias toward compute power. In this setting, a 51% a Sybil attack must control the majority of the network's compute power rather than identities. In multiple PoW blockchain DLTs, this is typically measured as a hash rate—the rate at which hashes are computed in an attempt to brute force search for a valid hash input (thus validating the proposed block).

Sybil attacks can affect both permissionless and permissioned DLTs, although different resources are required to mount an attack in each setting. Permissioned DLTs that rely on compute power for network consensus are open to increased risk since an authorized attacker no longer has to compete with global compute power, but simply whatever computational power is being dedicated by the rest of the network (usually far smaller). Permissioned DLTs could instead use a proof of majority or PoA consensus mechanism to mitigate this threat. It is important to note that these design principles for permissioned DLTs do not prevent Sybil attacks themselves; they are simply moving the security problem elsewhere and relying on the ability of network operators to correctly enforce access controls to mitigate attacks. Networks that employ stringent enough access controls and countermeasures for identity-based attacks may not benefit from distributed trust because a significant portion of the trust is centralized on the network operators. In these settings, a regular database (centralized or distributed) with cryptographic signatures for attestation could be sufficient instead of a DLT-based solution.

Selfish Mining Attack: In an ideal proof-of-work based blockchain DLT, miners are generally incentivized to publish a successfully mined (validated) block immediately to get the payout. A selfish mining attack involves a miner that holds off on publishing a successfully mined block to continue mining subsequent blocks. This allows a selfish miner to have a competitive advantage to mining their own private chain, because if they are to publish it later, it is more likely to be longer (has more PoW) and accepted by the network. Any other chains that other miners have been building will have been wasted. This is detrimental to the network because a certain fraction of compute power is being wasted and not being spent on maintaining the integrity of the blockchain. Distributed ledger developers can adapt to this by choosing parameters that reduce the advantage that selfish miners can gain and the likelihood that they can succeed.

Unauthorized Access: A permissioned DLT is susceptible to similar vulnerabilities as to a normal enterprise logon system. If an attacker can compromise the credentials of an authorized participant, they can obtain access to sensitive information and be able to perform unauthorized operations. Sufficient cyber monitoring and strict user authentication can mitigate this problem, but the most ideal approach is to have the system designed to be robust to unauthorized accesses and naturally limit potential damage or compromise. User authentication controls are typically outside the scope of DLT.

Bugs in Smart Contracts: One of the appeals of smart contracts is that they are intended to always function in an exacting manner as defined in their code. In the financial world, this creates a situation in which parties are virtually guaranteed to receive the digital commodities (or funds) if they satisfy the conditions of the contract, regardless of any legislative or judicial body rules. This can greatly reduce the amount of risk undertaken by parties that are willing to satisfy and fulfill the terms of a smart contract. In some situations, the presence of arbitration, judges, or other legal counsel helps resolve ambiguities and steer conduct toward satisfying the intended spirit of the contract rather than what it technically says. Smart contracts are formally specified instructions that behave similar to computer code. Just as computer programs are susceptible to catastrophic bugs and errors, smart contracts are too. An example is provided by the Directed Acyclic Graph (DAO) attack, as explained in [38].

The attacks described above generally apply to all DLT implementations, including those in the financial sector, typically cryptocurrency. The assessments on the most common attacks on DLT focus on permissionless DLTs, the financial sector, and cryptocurrencies such as Bitcoin [39,40]. Included in the cryptocurrency attack list are exchange hack, ransomware, 51% attack, phishing for private keys, investment scam, and extortion. In general, these attacks are specific to the application – finance and cryptocurrency – rather than on the DLT infrastructure.

Disconnection between Physical and Cyber Layers: Many activities relevant to the power and energy domain could benefit from some of the security properties that DLTs include. It is important to remember that DLT solutions do not come with the ability to assure that cyber record keeping will match with real world events. The protections that DLTs employ only apply to the virtual records that are created. There is not much to stop an adversary from fabricating/falsifying the data and pushing them to the DLT. For example, if DLT is used for a supply chain management solution where a QR code or barcode is attached to a physical asset, the physical asset can be represented in the DLT through the unique identifier associated with the physical asset. In such a case, the human intermediaries would update the state of the

asset. Although the DLT would help track the entire history of the asset, other mechanisms should be in place to make sure that the data entered by the human intermediaries is accurate in the first place. A potential solution to address such a challenge would be to have a sensor that can automatically update the virtual profile of the physical asset with minimal human intervention. Many solutions have been explored at a theoretical level, but fully deployed/in-production practical solutions are yet to be seen.

Implementations and Specifications Disagreement: Even if a DLT design is guaranteed secure in a theoretical setting, these systems often have vulnerabilities introduced during implementation. Unfortunately, system modeling and software engineering tooling is not yet advanced enough to make the development process robust against small errors in critical sections of the codebase. Rigorous evaluation, assessment, and testing frameworks are needed to make sure that a distributed ledger system will function as intended and not leave an exploitable bug that compromises the security of the entire network. Note: this potential vulnerability is applicable to all systems, not just DLTs.

3.4. Attack surface and DLT usability analysis

Because the power and energy systems are very high value targets for attackers, the use case development team should have peripheral security measures in addition to any of the security attributes of the DLT. Relying only on DLT-based attributes may not provide comprehensive security. If the DLT is not configured and deployed properly, there is always a risk of increased attack surface due to DLTs.

Because power and energy system operations require extensive verification of physical properties of machines, systems, and materials, peripheral verification and validation measures might be needed pertaining to the physical systems. DLTs can only ensure certain virtual, cyber properties about the data and digital commodity that may represent the physical system or participate on behalf of the physical system. Furthermore, DLTs can potentially be a benefit to the management of results from verification processes.

In addition, DLTs that rely heavily on security provided by consensus mechanisms may only be appropriate for some of the power and energy use cases. Existing distributed ledger systems are (ideally) designed so that the benefit from performing an attack against the consensus mechanisms will come at too great of a cost. This provides some game-theoretic security, since it is not rational to perform an attack that does not optimize payout. However, certain classes of attackers could be willing to pay significant amounts to perform the attacks and thwart the system. Alternatives to consensus, such as verifiable proofs provided by Succinct Non-Interactive Argument of Knowledge (SNARK) [41], that have cryptographic levels of security, could be more useful. Discussion and comparison of consensus-alternatives are beyond the scope of this paper.

Given that DLTs still are evolving, there are many critical research questions regarding the use of DLTs that the use case developer should consider addressing:

1. What are the trust gaps in the use case that are not effectively addressed by existing methods? In such use cases, could private/permissioned DLTs become the trust anchor and ensure integrity of the data and the processes?
2. What are the engineering requirements of the use case or application that would theoretically benefit from DLT? How would those requirements map to DLT features? Would the application need all the features of a DLT (*e.g.*, immutable ledger, smart contracts/chaincode platforms, *etc.*) [42]?
3. What are the cybersecurity requirements of the use case? What peripheral systems are needed in a DLT-based solution to ensure that security constraints are met?
4. Are there any availability-driven requirements? In such a case, would DLTs inherent latency and throughput limitations negatively impact the use case?
5. What are the economic implications (return on investment) of using DLT as compared to existing and non-DLT solutions? Economic implications may include platform deployment costs, workforce training and development costs, *etc.*;
6. Can DLT evolve based on advancements in cryptography (*e.g.*, by using post-quantum cryptography and zero knowledge proofs)? If not, can a chosen DLT be morphed or customized with high/advanced security features?
7. What are the security (*e.g.*, cybersecurity, physical security, *etc.*) trade-offs between DLT vs non-DLT solutions for a use case?
8. What are the long-term scalability and interoperability limitations and challenges?
9. Based on the above considerations, what is the prioritized list of power and energy use cases or use case subsystems that would benefit from DLT?
10. What are the scalability limitations? Particularly for the power and energy environment with performance limitations and latency concerns, what are the use case scalability thresholds, and can DLT satisfy those requirements? For example, is there some limit in the number of DLT nodes that can be deployed without significantly adversely impacting performance?
11. What are the data storage and accessibility requirements that need to be satisfied by the DLT?

Once the use case architecture is determined, an attack surface analysis should be performed to identify the attack vectors and select the mitigation strategies. These attack vectors may be, for example, specific to the DLT that is implemented, the timing source, or the cryptographic key management infrastructure.

4. DLT cybersecurity stack

This section presents the blockchain/DLT layers, architectural definitions, and pertaining components across the layers. Following the layer definition, this section presents mapped architectures between the DLT cybersecurity stack and the OSI model, TCP/IP model, and SGAM. Furthermore, cybersecurity considerations and potential cybersecurity attributes across the blockchain/DLT layers are discussed. The scope of the presented stack incorporates DLT including but not limited to blockchains. Discussed technical attributes of this section leverages some of the existing research [43–45].

4.1. Layers and definitions

Application layer: This layer contains applications, software, scripts, programs that can be used by the users (*e.g.*, human users and nodes) to interact with the DLT. In a sense, these software applications are above the DLT core and therefore do not fully belong to the DLT. However, these applications should be developed based on the boundary conditions and rules defined by the blockchain. Applications should be developed following System Development Life Cycle (SDLC) processes and ensure cyber security by design. Defense-in-breadth, secure software testing processes, patching, and configuration management should be in place throughout the application lifecycle. This applies to all applications, not just DLT applications. Elements of the application layer have the ability to trigger rulebases and program code

(such as smart contracts, chain code, atomic swaps, *etc.*) that reside in the execution layer (below). These software applications have the ability to perform two-way communication: (1) downward communications that lead inside the DLT (starting from the execution layer) and (2) upward communications that are outside the DLT. These upward communications can be performed through application programming interfaces (API), Oracles, *etc.* Other elements of this layer include user interface/graphical user interface (UI/GUI), performance analysis applications such as Hyperledger Caliper™, *etc.* Elements of this layer may be considered as off-chain processes or on the fence of DLT and the outside world.

Execution layer: This layer contains the DLT rules, program logic such as smart contracts, chain code, *etc.* The software applications from the application layer trigger the code and rules in the execution layer and instruct the code in the execution layer that results in the execution of a transaction. In cases where the execution layer code requires data from off-chain databases, the code can trigger oracles that reside in the application layer (or between the application layer and outside world) to fetch data/information from off-chain sources to the execution layer code.

Consensus layer: The consensus layer is a critical component of DLT technologies, especially blockchains. This layer facilitates distributed trust, ownership, and control. In this, wide-spread consensus forming nodes across different geographical and network locations work independently toward consensus of transactions. There are two common consensus types: (1) proof-based consensus and (2) voting-based consensus. Examples of proof-based consensus are Proof of Work, Proof of Authority, Proof of Stake, Proof of Elapsed Time (PoET), *etc.* Furthermore, some of those proof-based consensus are tailored across adoptions. Examples of such tailored proof-based consensus approaches include Greedy Heaviest-Observed Sub-Tree (GHOST-PoW), sharding-PoW, DAG-PoW, *etc.* Unlike the proof-based consensus, voting-based consensus does not require the consensus forming nodes to "prove" their work, stake, authority, *etc.* Instead, voting-based consensus often relies on the process of an independent set of nodes presumably performing the same logical computations (or running program logic such as chaincode) to generate a solution/answer/vote. A vote from a consensus-forming node could lean toward approval or disapproval of a transaction. Depending on the rules defined, a certain threshold of approval votes needs to be reached for a transaction to be approved and for the block creation process. Examples of voting-based consensus include Practical Byzantine Fault Tolerance (PBFT), Istanbul-BFT, Hybrid BFT, *etc.* Consensus has two main properties: (1) indicates an agreement among the distributed nodes and synchronizes them and (2) validates transactions and ensures reliable and fault-tolerant operations.

Data model layer: This layer handles functions and operations related to the blockchain creation itself in addition to ledger maintenance tasks. Note that this layer does not define the final ledger state, a global consensus is required to approve the final transactions and block creations. However, the process of grouping the transactions into the block, creating a block (or appending to the ledger), maintaining a common state of the ledger, *etc.* are handled in this layer. Functions in this layer are primarily related to data orchestration processes but in the context of distributed databases, ledgers, *etc.* Examples of such processes are grouping or arranging the transactions into blocks, appending the block to the distributed ledger, and replicating the identical and updated data-structure/ledger across the network, *etc.* This level of network-wide replicability (achieved through the communication infrastructure discussed in the network layer) eliminates single points of failure through attacks related to compromised nodes, data manipulation and injection to corrupt a ledger node, *etc.* Compromising a set of nodes does not compromise the entire network. Therefore, immutability and distributed trust can be related to the processes in the data model layer. Security aspects related to digitally signing the transactions in a block through asymmetric cryptography, generating the hash of the block through SHA-256 (or more secure) algorithm fall under the data model layer. The content of a block or structure of a block depends on the blockchain/DLT technology. However, the underlying security components related to digital signature and hashing processes may be common across many DLT technologies. Aspects discussed under this layer may be mostly contextual to blockchain DLTs. Equivalent/similar processes in non-blockchain DLTs will be captured in forthcoming iterations of the DLT cybersecurity stack.

When transactions are submitted to a blockchain network, the transactions are ordered in a block. For energy transactions, specific data attributes must be present on the transaction such as: date, timestamp, certificate type, tracking system ID, certificate data, renewable fuel type, renewable facility location, project name, utility to which the project is interconnected, emissions rate of the renewable source, certificate ID along with other attributes associated with the certificate [46].

Network layer: The network layer corresponds to the communication infrastructure that is needed to facilitate transactions, information and data sharing between the nodes. Protocols and methods to facilitate discovery and communication between the peer nodes belong in this layer. If nodes are expected to transact by digitally signing data-in-transit or engage in verification and validation of the transactions, such processes should be defined in this layer. Protocol suites such as the Recursive Length Prefix (RLPx), Transport Layer Security (TLS), and other secure node-to-node handshaking mechanisms should be identified under this layer. It is recommended to use standard protocols instead of custom defining new/proprietary protocols. It is worth noting that RLPx is used in the Ethereum blockchain and it is not widely used across other DLTs. Hyperledger Fabric and some private blockchain use TLS for secure handshaking.

Infrastructure layer: This layer corresponds to the virtual and physical computers or software agents that participate as the authorized blockchain nodes. The nodes should be capable of performing cryptographic operations (such as digital signature and hashing), maintaining and varying the identity of other nodes and providing its identity information for authentication and authorization by the network/other nodes. Depending on the DLT, security aspects related to Membership Service Provider (MSP), Active Directory (AD) fall within this layer. Hence, tools and processes that facilitate access controls, define identity of the nodes, and ensure permissions belong in this layer as part of the nodes. Furthermore, aspects related to on-chain and off-chain storage infrastructure.

Physical layer: In several use cases, this layer may not have any relevance. The use of DLT-based industrial use cases where IoT devices and sensors play central role is an emerging trend [47]. However, in use cases where sensors and IoT devices are expected to participate in blockchain, those systems are expected to be part of this layer. The sensor systems may not have the capacity or capability to directly join as nodes in the DLT. In such cases, the sensors would need to interact with the middleware agents that are part of the infrastructure layer to participate in the DLT network.

The summary scheme of the proposed DLT cybersecurity stack is provided in Table 1.

4.2. Cybersecurity mapping to the DLT cybersecurity stack

Before articulating the technical attributes of various cybersecurity components and their relation to the blockchain layers, here are the critical definitions:

Table 1
The proposed IEEE P2418.5 DLT cybersecurity stack. CFT: Crash Fault Tolerance; UID: Unique Identifier; OS: Operating System.

Application layer	Applications that trigger rule-bases and program code. APIs, UI/GUIs, Oracles, distributed applications, marketplace & monetization, *etc.*
Execution layer	Rule-bases and program code. Examples: smart contracts, chaincode, atomic sweeps, tokens, *etc.*
Consensus layer	Consensus protocols: proof-based, voting-based, *etc.* Examples: PoW, PoA, PoS, BFT, CFT, round-robin, endorsing
Data model layer	Data (and time) synchronization. Ordering services, block creation, chain structure, hashing, *etc.*
Network layer	Peer-to-peer transaction broadcast/discovery. Connectivity, runtime, telecommunications, network parameters
Infrastructure layer	Data storage entities. Logical blockchain nodes: Virtual Machines/clusters/Kubernetes, *etc.*
Physical layer	Systems participating on behalf of the users. Examples: Sensors, IoT devices with UID, OS, *etc.*

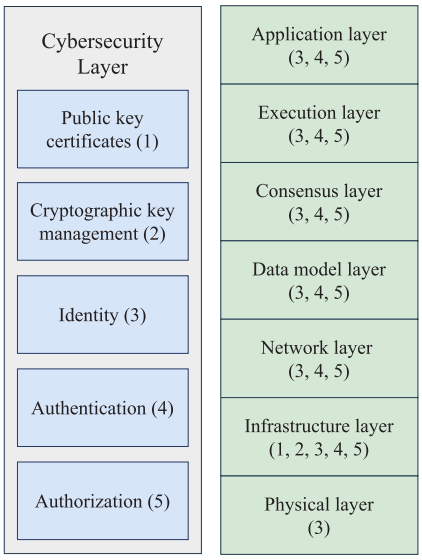

Fig. 2. The P2418.5 DLT cybersecurity stack with associated cyber security attributes.

1. *Public key certificate*: A data structure that contains an entity identifier(s), the entity public key (including an indication of the associated set of domain parameters) and possibly other information, along with a signature on that data set that is generated by a trusted party, *e.g.*, a certificate authority, thereby binding the public key to the included identifier(s).
2. *Cryptographic key management*: The activities involved in the handling of cryptographic keys and other related parameters (*e.g.*, initialization vectors and domain parameters) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output into cryptographic modules, use and destruction.
3. *Identity*: The set of attribute values (*e.g.*, characteristics) by which an entity is recognizable and that is sufficient to distinguish that entity from any other entity.
4. *Authentication*: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
5. *Authorization*: Access privileges that are granted to an entity; the right or a permission that is granted to a system entity to access a system resource. Node participants are provided with a specific set of privileges based on the role of the participant. For example, privileges could be used to define which participants can only read transactions (auditors), and which ones can read and submit transactions (buyers/sellers), while others can have elevated privileges to add or remove participants (admins).

The diagram of Fig. 2 illustrates the allocation of the cybersecurity layers to the layers in the DLT cybersecurity stack. Allocation does not mean that the cybersecurity functionality must be implemented in the layer. The allocation will depend on the DLT that is implemented. The objective is to ensure that the cybersecurity controls are considered at each of the DLT layers. Also, because the focus is on DLT, security controls such as configuration management, auditing, and system monitoring are out of scope of this document.

Below is the list of considerations, assumptions, and contextual information pertaining to the above figure and are specific to blockchain/DLT.

1. Physical layer has a lot of cybersecurity concerns such as data security and privacy across different vendors and manufacturers. These concerns can be addressed through public key certificates, identity, and/or authentication. Many of these cybersecurity controls are outside the scope of blockchain/DLT.
2. Sensor gateways can handle cryptographic key management, where asymmetric keys may be stored encrypted or in a hardware security module to minimize the impact from security attacks. Note that gateways and sensors are considered part of the infrastructure.
3. Certificate verification may occur at the node/system to minimize security and concerns such as single point of failure attacks.
4. 100% mapping with SGAM cannot be expected. For example, the sub-activity or sub-process of an activity/process in a layer of the SGAM can be carried out in another layer of the SGAM to provide and enhance continuity of the (main) activity.
5. Auditing and access control are not inherent components of blockchain/DLT.
6. Network layer security is provided at the network layer to protect network communications across packets routing.
7. Identity, Authentication, and Authorization (IAA) could happen in one or more layers depending on the DLT in use. For instance, IAA might happen at the application layer in Hyperledger Fabric. In this work, identity attributes such as names, Media Access Control (MAC) addresses, and/or IP addresses can go to respective layers. Also, IAA may be implemented outside the DLT.
8. Data may be rechecked for integrity at each layer based on the structure of the received information to support the identification of potential vulnerabilities across all layers.

4.3. TCP/IP and OSI mapping to the blockchain cybersecurity stack

In this section, the TCP/IP and OSI models are mapped to the DLT cybersecurity stack based on the functionalities of the stack layers. A well-defined set of services are made available within each of these layers. As shown in Fig. 3, the application and execution layers of the blockchain stack handle all functions (such as application lifecycle management) carried out by the TCP/IP model application layer and the OSI model application, presentation, and session layers.

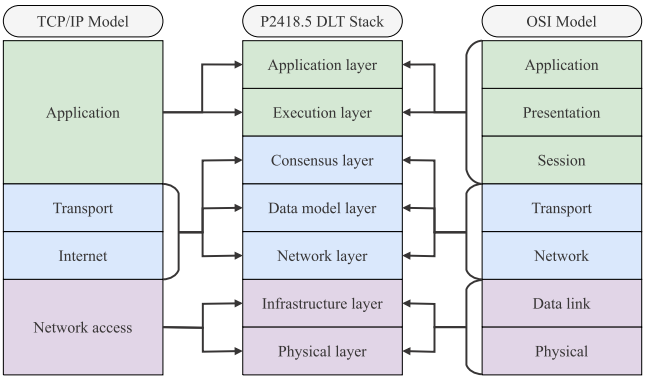

Fig. 3. The P2418.5 DLT cybersecurity stack mapped against OSI and TCP/IP models.

The integrated functions of the blockchain stack consensus, data model, and network layers are associated with the TCP/IP model transport and internet layers as well as the OSI model transport and network layers. Functions like group-based decision-making on transactions, broadcasting the transactions, and providing the communication infrastructure needed for facilitating the transactions via the blockchain stack fits into the ability to establish and exchange transactions using the TCP/IP or OSI model.

Furthermore, the functions of the blockchain stack infrastructure and physical layers are carried out by the network access layer of the TCP/IP model and the data link and physical layers of the OSI model. In this case, the logical representation of blockchain nodes (and other entities) via the blockchain stack corresponds with the specification of the nodes and means of data delivery between the nodes via the TCP/IP or OSI model.

4.4. SGAM mapping to the DLT blockchain cybersecurity stack

SGAM is a reference model that aims to address Smart Grid architectural frameworks in a multi-layer structure. The SGAM reference architecture consists of the following five main interoperability layers:

- Business layer
- Function layer
- Information layer
- Communication layer
- Component layer.

The SGAM interoperability layers are designed to present a traceable and simplified high-level presentation of smart grids reference architecture and their functionalities. The SGAM interoperability layers take into account previous similar frameworks described in the GridWise Architecture Council (GWAC) Stack [48].

A schematic diagram depicting the mapping of the GridWise to SGAM interoperability layers is shown in Fig. 4 and then discussed in the following paragraphs.

Business Layer: The business view and perspectives are presented in this layer. Energy policy regulatory, business model development and power market (economic) points of views and structures are accommodated under this layer.

Function Layer: This layer deals with the functions, services and their interactions with other layers and various actors (stakeholders) and physical implementations in terms of use cases, applications, and systems.

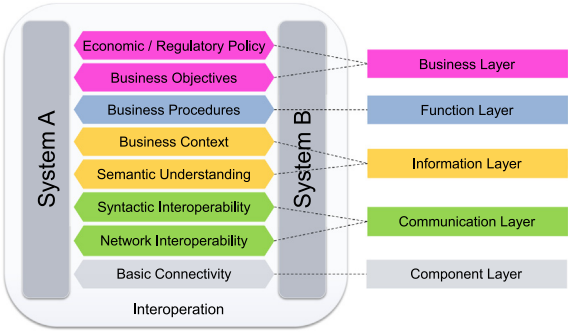

Fig. 4. Mapping of the GridWise to SGAM interoperability layers [48].

Information Layer: The information that is generated, processed, transmitted and stored between functions, actors, components and systems are represented in this layer. DLT and other similar information-driven technology and frameworks are accommodated under the information layer.

Communication Layer: The communication protocols, mechanisms, functions and technologies are addressed under this layer by linking them to corresponding smart grids use cases.

Component Layer: Physical components of smart grids such as power generation, transmission and distribution systems and their measurement, control, protection, telecommunication and monitoring equipment are emphasized under this layer.

A one-to-one mapping of the SGAM and the DLT cybersecurity stack is not possible. But it is possible to refer to some layers and functionality of the SGAM framework and investigate if there will be a need to further develop similar smart grid frameworks to satisfy the needs of emerging digitalization technologies such as blockchain DLT. The mapping of the DLT cybersecurity stack against the SGAM model is described in the following, and then reported in the schematic diagram of Fig. 5.

- The Component Layer of SGAM can be linked to the physical and infrastructure layers of the DLT cybersecurity stack.
- The Communication Layer of SGAM is linked to the DLT network layer.
- The Information Layer of SGAM is linked to the DLT data model layer.
- The Function Layer of SGAM is linked to the DLT consensus and application layers.
- The Business Layer is not directly linked to the proposed DLT cybersecurity stack but is indirectly reflected under the DLT application layer by considering the business logic behind the use cases.

The diagram of Fig. 6 illustrates the attributes that are relevant to the energy sector, cybersecurity, and to both. This is not a comprehensive list to include all cybersecurity controls, but highlights the major categories. As described above, several of these attributes are not inherent components of DLT.

The existing regulatory frameworks[2] that govern the energy sector require the implementation and auditability of granular security controls, hardening of devices participating in the generation and delivery of energy across the grid, network segmentation, and protection of the data and the grid. All of the above factors are most appropriately suited by a permissioned blockchain network that is only accessible to authorized network participants and supports enforcing security controls.

[2] NERC: North American Electric Reliability Corporation in the USA; NIS Directive: Network and Information Security Directive in the European Union; FERC: Federal Energy Regulatory Commission in the United States; NEM: National Electricity Market in Australia

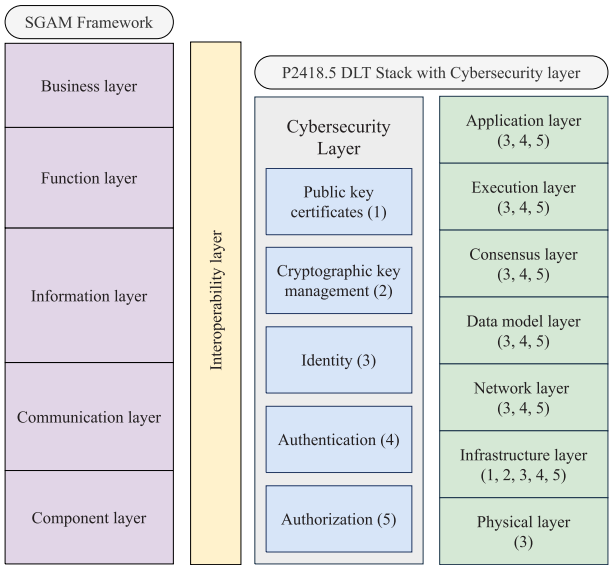

Fig. 5. The P2418.5 DLT cybersecurity stack mapped against the SGAM model.

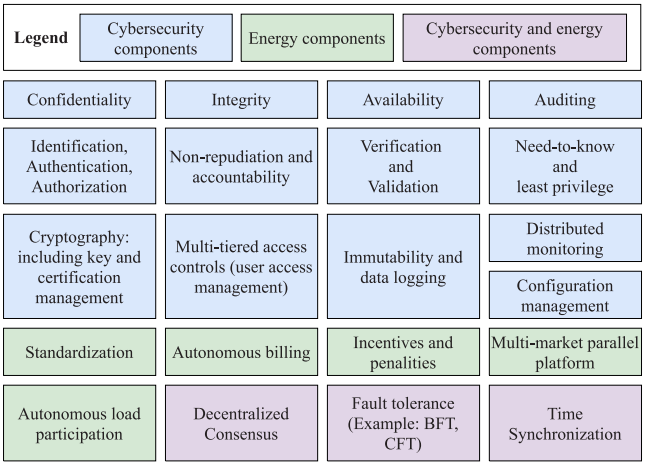

Fig. 6. Cybersecurity attributes and considerations pertaining to DLT applications in power and energy use cases.

5. Blockchain use cases

The objective of this section is to theoretically demonstrate the usability of the previously discussed DLT cybersecurity stack. Five different power and energy use cases are discussed and mapped to the DLT cybersecurity stack. The use cases discussed in this section are as follows:

1. Distributed Energy Resource (DER) Integration
2. Environmental Commodity Management and Trading
3. Microgrid Applications
4. Electric Vehicle (EV) Charging
5. Supply Chain.

Similar to most power and energy use cases, permissioned DLTs with PoA or voting-based consensus are potentially the most appropriate architectures. The reason behind the above recommendation is due to the nature of the power and energy ecosystem where only a known set of participants will be allowed to transact on DLT. Following subsections will discuss each of the above use cases, sequence of operations, and use case components in the context of DLT (using the stack). Note that all of these use cases may have fairly similar cybersecurity considerations and pitfalls. Use case specific threat models and attack trees are beyond the scope of this paper and will be a strong consideration for future work. The selected general cybersecurity considerations pertaining to the power and energy use cases are described below:

1. DLT implementations across these use cases are subject to several well-known threats such as malware, Distributed Denial of Service (DDoS), Man-in-the-Middle (MitM), ransomware, *etc.* Specific to the application layer of the DLT cybersecurity stack, if the distributed applications are based on web technologies, the majority of the top 10 security risks discussed by the Open Web Application Security Project (OWASP) are applicable to the use case [49]. In addition to those, insecure key management and data privacy risks due to the lack of well-defined access controls are critical risks to address. More details around cybersecurity risks are discussed in the earlier sections of this paper;
2. All of the below discussed use cases may involve autonomous systems that could interact with DLT. Without human-in-the-loop, autonomous and secure system initialization and verification is required. Failing to invoke the initialization and verification process for all required processes could lead to unintended malfunctioned operations. In such a semi-autonomous environment, secure registration of the devices should be built into the DLT solution process. This may involve the asset owners registering their devices through a portal while the smart contract validates the asset at verification. Throughout the asset lifecycle, the smart contract may perform needed verification before elevating the asset to perform approved operations. A robust registration system could potentially mitigate threats originating from rogue unregistered entities;
3. Similar to non-DLT applications, identity management is required. Public/private key pairs and pseudo identity may be in scope of the use case. The participating entities may use their identity information and request to perform certain operations through their associated DLT nodes. In such a setting, hierarchical or multi-party authentication and authorization mechanisms could assist to mitigate unauthorized operations. The smart contracts should be programmed to watch for undesired requests or triggers. Respected authority nodes should be notified in case of faulty operations or attempts but the nodes;
4. In most use cases, data provenance and non-repudiation could be invaluable to ensure accountability and secure intended operations. Some of the DLT inherent components associated with peripheral cryptographic measures such as related to identity management can assist with data provenance and non-repudiation. These are critical to not only ensure intended behavior or the system but also to trace back to the transnational origin if needed. Along these lines, verification of transactions to show machine state and communication integrity of the transaction creation process and logging should be built into the use case;
5. When DLT is used for a use case, identify the impacts or value-added to certain cybersecurity attributes such as the confidentiality, integrity, availability, authentication and authorization process, auditability, trust, and transparency. Depending on the use case, those attributes may require different levels of attention and methods to achieve them may vary. As discussed in previous sections, data integrity is maintained through cryptographic hashing of the transactions and the reconciliation of the transaction takes place

in real time. Existing Authentication, Authorization and Accountability systems deployed across the enterprise to control access, enforce access policies and auditability along with existing Public Key Infrastructure solutions should be used with the DLT implementation. Data encryption takes place outside of the DLT implementation. Data encryption, handling Personally Identifiable Information (PII), and data confidentiality shall be the responsibility of the data owner. In most cases, confidentiality is peripheral to DLT and not integral to DLT. Other peripheral security measures include perimeter security systems such as network and application firewalls. Network and application firewalls play a critical role as data moves through from the application layer to the network layer and vice versa. Network segmentation is another important peripheral security consideration to reduce attack vectors. The final peripheral security consideration is related to baseline configuration management: (1) limit administration or elevated access to add devices to the DLT network, (2) enforce multi-factor authentication for users with elevated access and implement solutions that track changes/deltas on the node configuration, and (3) log every transaction that modifies network or node configuration.

5.1. Use case 1: DER integration

This use case examines how a Blockchain-enabled platform can facilitate integration of DERs in grid operations. The term DER as used here includes distributed generation, conventional demand response, energy efficiency, energy storage, and electric vehicle chargers. DERs may be owned and/or operated by different entities including residential, commercial and industrial consumers, or the utilities themselves. To distinguish consumers who own and operate DERs from passive consumers, the term "prosumer" is often used to denote consumers with local sources of energy generation and storage as active agents of the power system. Non-utility owned and operated DERs impact the utility operation and business models in fundamental ways. A distribution system level utility needs to deal with large number of active grid-edge devices and systems from the operational point of view where the system has some challenges in terms of control and visibility. However, the customer-owned DERs tend to reduce the amount of electrical power provided by the utility while triggering additional costs in terms of utility operations which are associated with by their unpredictability and variability from the business point of view.

The increased costs include higher wear and tear of distribution equipment as a result of frequent control to follow DER variations, increased losses due to phase unbalances resulting from unevenly distributed DERs on the distribution phases, or unbalanced operation (rooftop solar generating on one phase and EV charging on another phase), to mention a few examples.

Currently, many utilities have administrative retail programs and rates for different classes of DERs, such as roof-top solar and EVs. This approach is not sustainable with increasing levels of DERs as it falls short of addressing the temporal and locational differentiation of DERs and their impact on the grid [50]. From this perspective, the undergoing paradigm shift toward transactive energy opens a new venue to address this problem [51, 52].

With the incentive-compatible design of transactive markets, DERs can support grid operations by offering flexibility of generation, consumption, or both. The term Distributed Flexible Resources (DFRs) is used in some regions (*e.g.*, Europe) to signify participation of DERs in distribution and bulk power operations. The term DER as used here includes DFRs.

A properly designed transactive market would accommodate both Peer-to-Market (P2M) and Peer-to-Peer (P2P) transactions. Adding Blockchain to the mix can help augment security and streamline settlement processes.

5.1.1. Use case setup

This use case considers a Blockchain-based transactive energy system platform from [53] designed to facilitate P2P and P2M transactive exchanges for DER integration leveraging Blockchain technology. The following questions are addressed:

1. How would a blockchain DLT cybersecurity stack be leveraged in such a blockchain-based transactive energy platform?
2. How would the underlying cybersecurity issues be addressed by leveraging blockchain?

To explore answers to the above questions, the schematic diagram of Fig. 7, adapted from [53], is included here to more clearly illustrate how the various applications and processes relate to the DLT Cybersecurity stack.

As explained in [53] the Transactive Distribution System Platform (T-DSP) includes both on-the-chain and off-the-chain applications. Some of the off-the-chain applications are used by the distribution utility for grid management and dissemination of advisory grid related price signals through the T-DSP interface to the Blockchain nodes.

An off-the-chain interface of significance is that of metering and telemetry from the physical DER assets in the field. These metering and telemetry inputs trigger the execution of Smart Contracts. However, they are prone to tampering, metering errors, and telemetry disruptions. As explained in [53], two of the off-the-chain T-DSP applications, namely, IoT Supervisory Control and Data Acquisition and State Estimator provide a reference signal to help in detection of anomalies in metering and telemetry signals. The Smart Contracts can use both off-the-chain signals (direct telemetry and metering signals from the DER meters and sensors), as well as state estimated values, to trigger contract execution based on a set of rules thus minimizing intentional tampering with, or inadvertent errors of, metering and telemetry signals.

5.1.2. Cybersecurity gaps/considerations

In reference to the seven layers of the DLT cybersecurity stack, the main elements of the Blockchain-enabled Transactive Energy (BCTE) platform are summarized in Table 2 and described in the following.

DERs are susceptible to DoS attacks, mainly due to exploitation of outdated firmware. These attacks could result in the shutdown of DER sites and communication outages between DER devices and a DLT. For example, consider a setting where an attacker exploited an outdated firmware of a firewall at a DER site. In this case, such exploitation can have an adverse effect on the operations of the DER site, allow unauthorized access to the DER devices at the site, cause communication outages between the devices, and further affect real-time access to the DLT.

As indicated above, off-the-chain data that are input to the DLT are particularly prone to tampering before they get to the Blockchain. This includes data from sensors, IoT devices, telemetry, and metering inputs to the Blockchain. Security threats include malware, web app threats, DDoS, ransomware, insecure key management systems, and attacks on the DER integration processes and operation. Blockchain fork issues and majority attacks are also issues of concern.

The following cybersecurity controls: confidentiality, integrity, authentication, auditability, authorization and access control, trust, transparency, and availability are important for the following operations. Many of these cybersecurity controls are outside the scope of DLT:

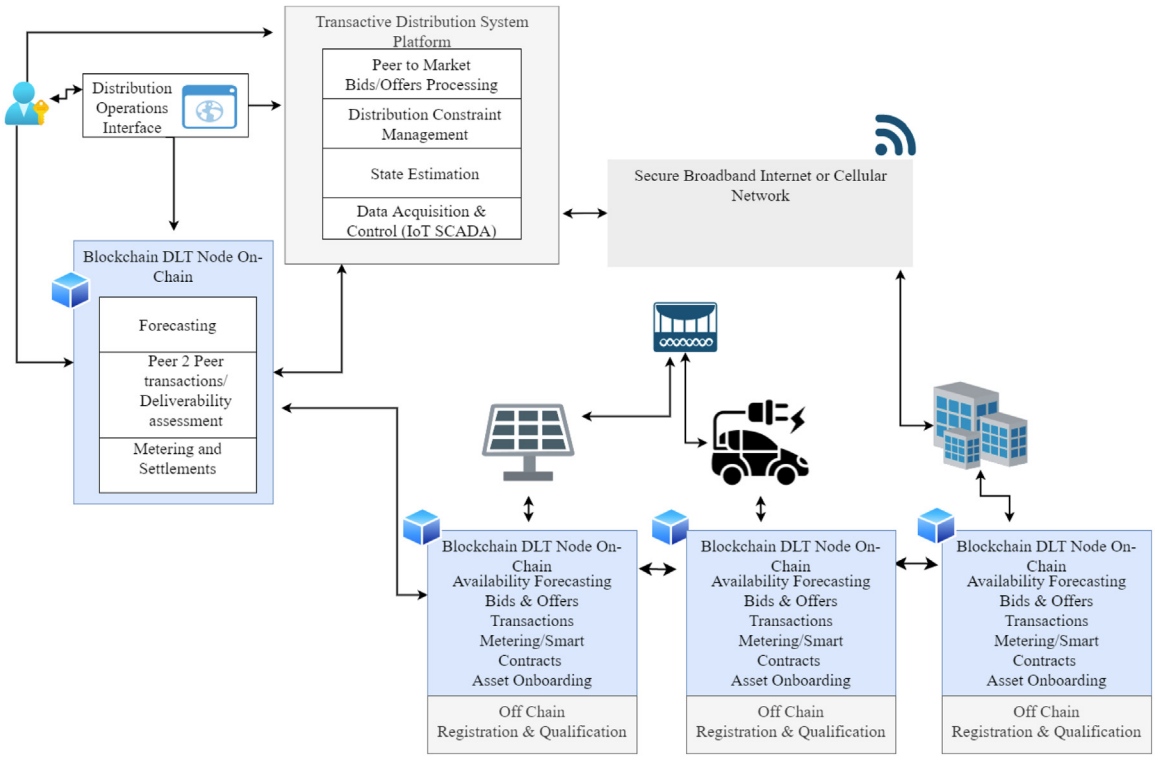

Fig. 7. DER Integration. Schematic description of the relation between DER applications and processes and the DLT Cybersecurity stack. T-DSP: Transactive Distribution System Platform.
Source: Adapted from [53].

- System initialization.
- Requesting registration to ensure registered and pre-approved entities participate.
- Public/private key pairs and pseudo identity pertaining to the participating entities should be securely exchanged and maintained.
- Request to access to DER services should be conducted in a platform-defined sequential manner.
- Hierarchical authentication should be implemented.
- Transaction details should be shared between authorized entities in a timely manner.
- Transactions should be created, approved, and finalized in a timely, secure, and verifiable manner.
- After transaction verification, they should be written to the ledger and ordered.
- Transactions should be sent/issued to the intended nodes. Ledgers of all nodes should be updated with the transaction details (or pertaining hashes while the details are stored in an off-chain database).

5.2. Use case 2: Environmental commodity management and trading

Environmental commodities are non-tangible energy credits. The value of these credits comes from the need of market participants to produce and consume cleaner forms of energy. Renewable Energy Credits (REC) are equivalent to a fixed amount of energy (*e.g.*, 1 MW h) energy generated from a renewable source such as solar, wind, and hydro. The lower the carbon footprint, the higher the value of the REC. Those assets can be issued, tracked and traded in real time on a DLT network through a secure and fully auditable record of transactions while preventing the risk of double counting. The token is a digital representation of the physical asset and bound to physical limitations such as maximum supply. Once a token is exchanged, subsequent processes can take place on-chain or off-chain to execute the exchange of the commodity. The reference system level architecture of a decentralized Environmental Commodity Management and Trading (ECMT) solution is depicted in Fig. 8.

The benefit offered by the distributed ledger technology is that it provides reconciliation and settlement across multiple systems that play a role in the exchange. Agility in the settlement and reconciliation of transactions through smart contracts can provide a higher liquidity and eliminate the risk of double counting.

The distributed ledger technology has the potential to offer the following benefits:

- Create a distributed database of transactions available to trading participants to increase transparency.
- Increase the speed of exchange, minimize transaction backlog, remove roadblocks pertaining to intermediaries and reduce overall cost by using smart contracts to complete the settlement in real time.
- Automate manual tasks by enforcing payment releases through smart contracts, where the buyer has the funds in escrow and as soon as the order fulfillment is recorded, the funds are automatically released.
- Increase transparency and auditability by recording all transactions on the immutable ledger.
- Offer redundancy and availability pertaining to the transactions performed by the nodes and recorded on the ledger. Such a system is equivalent to a decentralized clearing house.
- Provide proof of ownership and provenance by facilitating a means to record the trackable information about the source of the energy generation and consumption.
- Offer flexibility to let the participant trade the energy at a micro (kW h) or macro (MW h) scale.

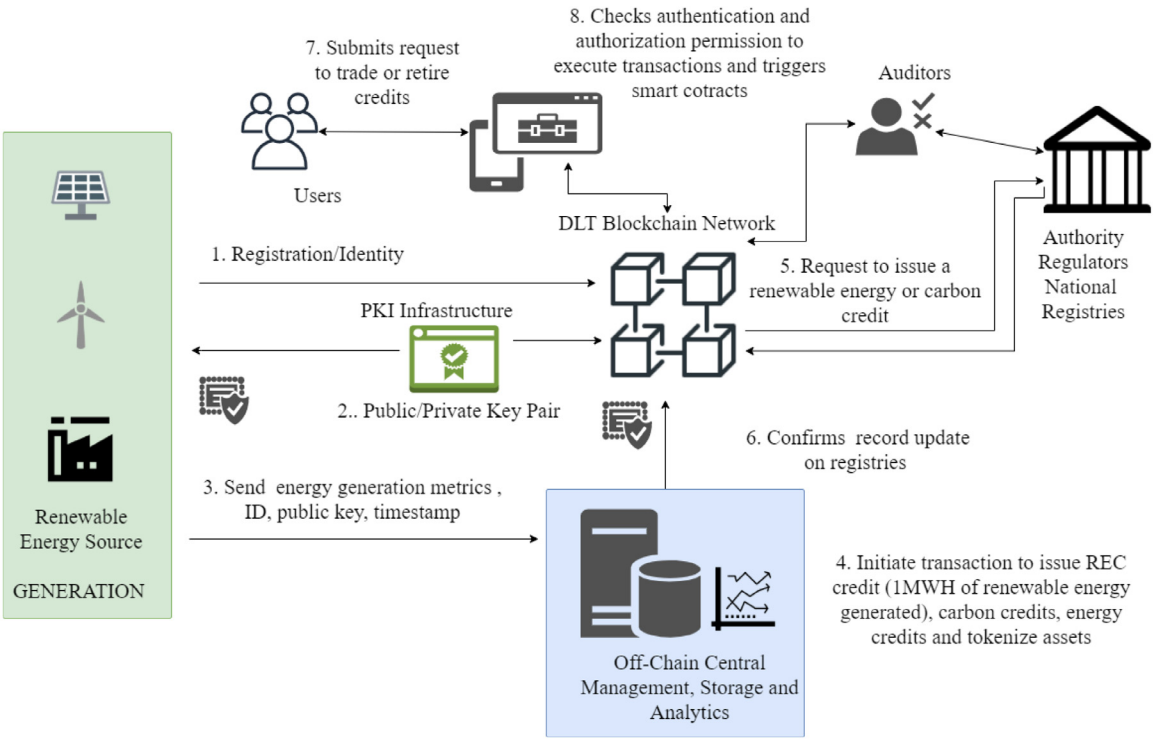

Fig. 8. Environmental Commodity Management and Trading. System level architecture diagram of a decentralized environment commodity tracking and trading solution.

5.2.1. DLT cybersecurity stack considerations

Node participants that are vetted and approved to join the DLT ecosystem must have valid certificates including asymmetric key pairs. In addition, a specific set of privileges are assigned based on the role of the participant. Some organizations have developed software to provide compatibility between smart meters and certain DLT offerings [54]. Overall the most important benefit that the DLT provides is the proof of source and ownership of the energy generated regardless of where the electricity travels in the grid. Fig. 9 shows a conceptual use of the DLT cybersecurity stack to the use case.

The distributed nature and the multi-party involvement of the use case is evident from the above sequence of operations. Table 3 reports the DLT-specific attributes and considerations. The key operations in this use case are REC creation, REC flows to the trading platform, REC Trading transactions, REC retirement, REC arbitrage, and REC auditing.

5.2.2. Cybersecurity gaps/considerations

As renewable energy suffers from insecure connections and communications, this may result in REC being vulnerable to active MitM attacks. Typically, REC does not offer the following features: (1) multi-factor authentication; (2) key establishment; and (3) data integrity and data confidentiality. As an example, a REC that belongs to an asset is forwarded to a DLT based REC trading platform. There is no security guarantee for the connection and communication between the asset and the platform because multi-factor authentication, data integrity, and data confidentiality are not used. An attacker can easily manipulate such a connection and communication.

5.3. Use case 3: Microgrid applications

Most of the time, a microgrid is a self-sufficient cluster of decentralized electricity sources, storage systems, and loads that provide service within specific spatial boundaries such as a university campus or a community. A microgrid can be grid-tied or off-the-grid island mode. When the microgrid is operated in grid-tied mode, the power is exchanged with the central power grid. When the microgrid is operated in off-the-grid mode, power is exchanged only between the sources, storage systems and loads locally within the microgrid.

Because of the growth of microgrids, a secure decentralized grid control system is needed compared to the traditional centralized grid control system. DLT has the potential to facilitate information exchange and integrity verification in such a distributed environment. The following are typical microgrid applications that fall under this use case [55]:

1. *P2P renewable energy trading*: A P2P trading network is used in many microgrids. The microgrid prosumers and consumers can use a blockchain based P2P renewable energy trading platform to complete transactions.
2. *Voltage regulation*: In microgrids, overvoltage and undervoltage situations lead to severe damage. DLT and smart contract based applications could be potentially used to track and manage the power flow related data between various prosumer and consumer nodes in the microgrid.
3. *Transaction energy model*: DLT and smart contracts may be used at the microgrid level and interact with the system wide transaction grid including transactive (prosumer) nodes (more details are discussed in the above DER integration use case subsection).

Given these assumptions and observations, the Microgrid use case requirements mapped to the DLT cybersecurity stack are summarized in Table 4.

5.3.1. Cybersecurity gaps/considerations

Security attacks such as modified software updates, forged data, and reuse of certificates have continued to impact operations of microgrids and its applications such as P2P renewable

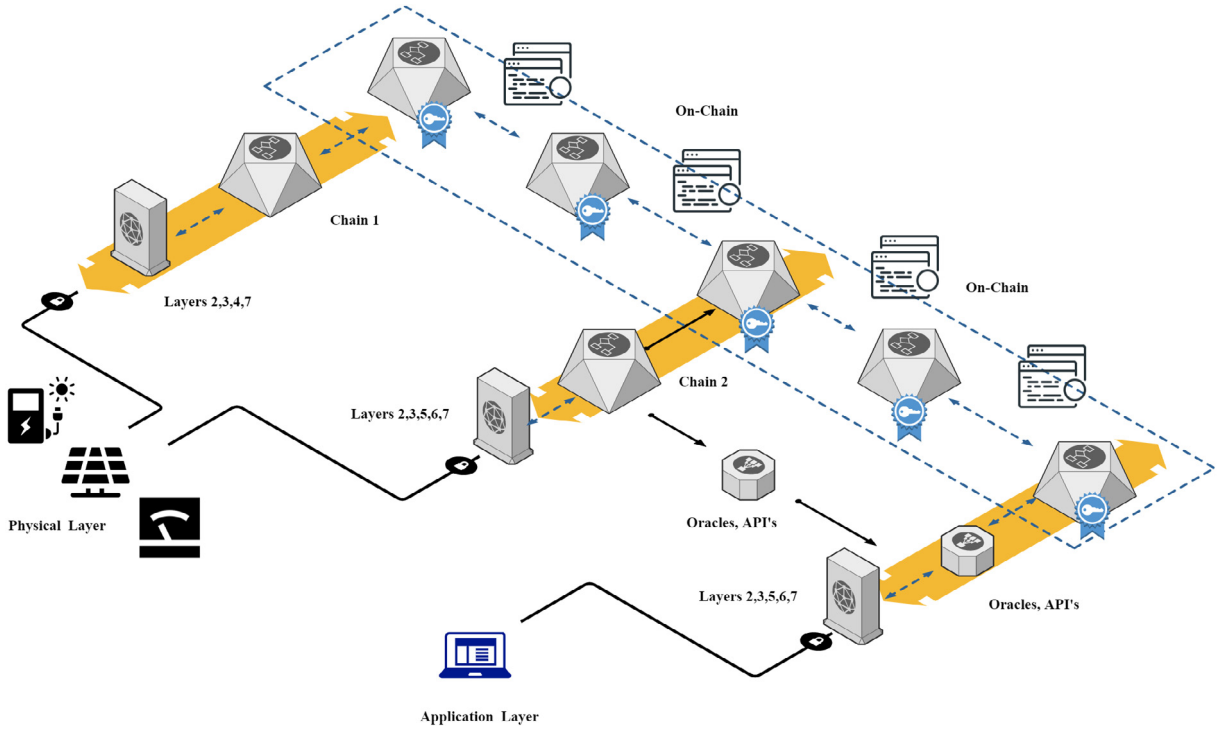

Fig. 9. Environmental Commodity Management and Trading. DLT network diagram with off-chain and a main on-chain with multiple nodes and correlation to the DLT cybersecurity stack.

energy trading that use the DLT for data storage and verification. In these attacks, an adversary exploits legitimate assets or services to destabilize the microgrid. To mitigate these attacks, cryptographic protocols have been designed to enhance the security of the microgrid. However, this design introduces additional computational and communication overheads that affect the performance of the microgrid.

5.4. Use case 4: EV charging

The large penetration of EVs in urban environments is expected to pose relevant challenges for the management of modern power grids. The main expected adverse impacts include increased peak demand, voltage instability, power quality issues (*e.g.*, voltage and harmonics variations), increased power losses, and degraded grid equipment (*e.g.*, increased thermal aging effects in transformers due to overloading) [56].

From this perspective, DLT could represent a key-enabling technology for the implementation of secure and efficient transactions between the several actors involved in this process. In the following, implementation of the DLT cybersecurity stack for the management of EV charging is analyzed by defining the main actors involved in the process, the type and content of the communication among each of the actors, and the required EV charging management services.

5.4.1. Domains and actors

Two main domains can be identified concerning the management and control of the charging of EVs, namely, the EV domain and the grid domain. The EV domain includes all the actions required for the provisioning of EV charging services to end users, while the grid domain comprises all the actions required for the integration and harmonization of EV charging with utilities and market operators.

As depicted in Fig. 10, five actors can be identified, as described in the following:

EV and EV User: Because the charging of an EV depends on both the EV user and the EV itself, the main actor involved in the EV charging (in both the terms of the content and the type of the communication) is generally a combination of the two distinct entities.

Electric Vehicle Supply Equipment (EVSE) and Supervisory System: This entity could be (1) the supervisor of the charging station (typically equipped with more than one EVSE), (2) the supervisor of the infrastructure where the EVSE is installed (*e.g.*, the building energy management system [BEMS] of a large building, or the energy management system [EMS] of a complex system, such as a university campus or a large private infrastructure), or (3) the home energy management system (HEMS) of a single family house.

Aggregator: This entity acts as intermediary between the EV domain and the grid domain.

Electricity Market: The electricity market interacts with the EV domain by collecting aggregated power demand forecasts and by providing price signals.

Power Utility: The power utility (generally the distribution system operator [DSO]) interacts with the EV domain by collecting aggregated power demand measurements and by providing demand–response requests, such as active power limitations, or ancillary service requirements.

5.4.2. EV charging scenarios

Three main EV charging scenarios are described in the following.

Home Charging: This is the simplest EV charging scenario, representing the installation of a limited number of EVSEs (typically equal to the number of EVs owned by the family) in single-family homes. As the charging infrastructure is fully private, there is no need for user identification, authorization, and billing of the EV charging. In addition, as the users are homogeneous, the coordination of charges can be managed without the need for a reservation system. In this scenario, the power demand of EVs is

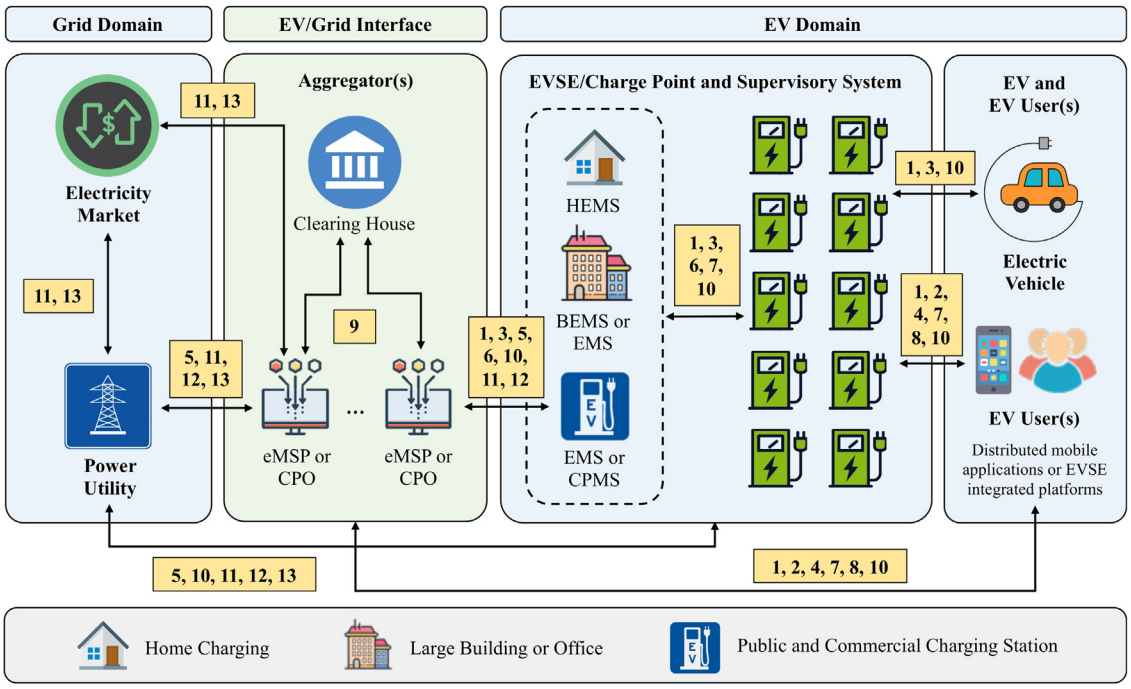

Fig. 10. EV Charging. Schematic diagram of the EV charging reference system. Yellow blocks indicate the EV Charging and interoperability functions, namely: 1: Authorization; 2: Billing; 3: EV Charging; 4: Handle Registration; 5: Manage Grid; 6: Operate Charge Point; 7: Provide EVSE/Charge Point Information; 8: Reservation; 9: Roaming; 10: Smart Charging; 11: Price Signal(s); 12: Demand/Response; 13: Aggregated Demand.

usually limited (or scheduled) by a supervisory entity, such as a HEMS.

Large Building or Office: In terms of complexity, this scenario stands in the middle between home charging stations and the public and commercial charging stations. It represents the installation of several EVSE in large residential buildings or workplaces. Even if the charging infrastructure is fully private, user identification and authorization are generally applied. Because the users are homogeneous (*i.e.*, they are tenants of the same building or workers at the same office), the billing service is not strictly required. For the same reason, the coordination of charges can be managed with or without a dedicated reservation system.

Public and Commercial Charging Station: This scenario comprises both public and commercial applications, such as governmental facilities, restaurants, and airports, and city or highway rest area charging points . These stations are intended to provide heterogeneous groups of customers high power supply capabilities, with charging times comparable (with the well-known limitations) to conventional filling stations. Because the charging service is fully public, user identification and authorization must be applied. In addition, because the users are heterogeneous (*i.e.*, they could access the service with or without the subscription to an existing charging program), the billing service may be required. For the same reason, a dedicated reservation service for the coordination of charges must be implemented.

The main characteristics of the three reference scenarios considered in this study are summarized in Table 5.

5.4.3. Communication functions

As suggested by [58], ten different functions can be considered when considering the communications involved in the management of EV charging, as listed in the following.

Authorization: Authorization of initiating the charging process at a given Charge Point (CP); it also includes identification.

Billing: Billing is he process of sending an invoice to customers for the EV charge service.

EV charging: This is the management of the actual charging process (*i.e.*, energy flowing), excluding the related administrative process.

Handle registration: This is the handling of communication for registrations and subscriptions.

Manage grid: This is the ability of the charge point to handle requests to the grid, such as the amount of required demand capacity.

Operate charge point: The ability of remotely managing and operating the charge point. This includes upgrading firmware, setting a charge point to available, unavailable, or reserved, configuring charge points, managing errors, *etc.*

Provide charge point information: This is the ability to provide information about a charge point. This kind of information can be both static (*e.g.*, location or level) as well as dynamic (*e.g.*, availability or power limitation).

Reservation: This is the process offered to EV users to reserve a charge point.

Roaming: This is exchange of information (primarily authorization) to enable EV users to charge at different charge points of different e-Mobility Service Providers (eMSPs) and Charge Point Operators (CPOs) by using the same identification.

Smart charging: all forms of interoperability between the EV and the grid domains, ranging from simple stop and restart during a charging session, to energy profile charging.

The communication between the different actors of the system does not occur only when the EV is plugged into or close to the EVSE, but also when the EV is in motion. Examples are mobile communications involved in the reservation of charges, for the state of estimation of the EV mobility (*e.g.*, for EV charging forecasts), and for other services as described in [57].

5.4.4. Application to the DLT cybersecurity stack

When looking at the scenarios described above, DLT can be applied in most of the related interoperability functions. Indeed, DLT could be used to handle billing, payments, reservations, roaming, and authentication. Furthermore, smart contracts could be used

Table 2
DER integration use case requirements mapped to the DLT cybersecurity stack.

Application layer	One can distinguish on-the-chain and off-the-chain applications among the Blockchain-enabled transactive energy platform application. On-the-chain applications would be implemented in the DLT application later. These include availability and capability forecasting, exchange and processing of bids, offers, and transactions, triggering of smart contracts based on a combination of metering and telemetry signals, and consequent settlements. These Blockchain applications also facilitate tracking and certification of origin of the DER resource behind the product (energy, reserves, *etc.*).
Execution layer	The DLT execution Layer includes the smart contracts using both on-the-chain and off-the-chain triggers. Smart contracts may use the sensor, metering and telemetry data from DER assets, as well as state estimated data, along with a set of rules and thresholds to trigger smart contract execution.
Consensus layer	A permissioned Blockchain was assumed for the DER integration platform. Various consensus mechanisms are possible including proof-of-stake and proof-of-authority. There is also an off-the-chain "pseudo-consensus" mechanism embodied in the state estimator application, with the important distinction from DLT consensus mechanisms that it uses redundant measurements and a number of physical laws (Kirchhoff's, Ohm's, *etc.*) to identify anomalous data from those passing checks for reasonableness and cross consistency .
Data model layer	This layer includes the registered asset models and parameters and their relationships. This layer in combination with off-the-chain data helps detect the point of origin and blocks created related to the products sourced from the DER assets. It is external to the DLT.
Network layer	The network layer includes the underlying blockchain platform protocols such as Hyperledger, Ethereum, *etc.*
Infrastructure layer	The DLT infrastructure layer is comprised of the nodes that are part of the DLT trading platform.
Physical layer	This layer includes the interfaces with the sensors at DER sites providing the heartbeat (availability of the asset), as well as asset level telemetry and metering. Depending on the design of the DER participation model, the metering and telemetry may be from individual assets, premises where the assets are located, or upstream substations. It is external to the DLT.

to program additional features, such as those implementing smart charging functions.

Each EV charging system (CP or even a single EVSE) could create blockchain transactions to implement the following functions: authorization, billing, and reservation. Blockchain transactions also can be created to manage roaming (involving CPOs, eMSPs, and the Clearing House). DLTs can be used to facilitate through smart contracts, the implementation of interoperability functions at any level of the system, namely: between EV/EV Users and EVSE, between CPOs and eMSPs (also including roaming), and between CPOs/eMSPs/EVSE and DSOs. EV users may directly interact with the DLT-based system through mobile applications and may not have any related system that would be part of the physical layer.

Given these assumptions and observations, the EV use case requirements mapped to the DLT cybersecurity stack are summarized in Table 6.

Table 3
Environmental commodity use case requirements mapped to the DLT cybersecurity stack.

Application layer	Decentralized applications can be created to run using the DLT as a distributed database; integration through APIs can enable applications to trigger smart contracts and exchange digital tokens with other users. Oracle, APIs and gateways enable integration and interoperability between different blockchain protocols. Tracking, certification of the origin of the energy resource, accounting, and auditing are the main applications that manage the REC data.
Execution layer	Smart contracts can automate issuing, trading, and retiring non-tangible energy credits; for example, when clean energy is generated by a solar PV farm. Smart contracts may need access to non-DLT external data that could be facilitated through APIs (above layer). Through oracles and API, smart contracts can be generated to trigger: (1) issuing commodities, for example, issuing a REC once 1 MW h of clean energy is generated by a renewable source; or issuing carbon credits from projects that have reduced, avoided or destroyed one metric ton of GHG; (2) proof of source and ownership (each device participating in the distributed ledger has a private and public key); and (3) trading and transferring ownership.
Consensus layer	When evaluating consensus algorithms, it is important to consider the impact in speed, latency, and volume of transactions that will be generated and must be processed through the DLT solution. A permissioned DLT should be strongly considered and compatible consensus algorithms should be used.
Data model layer	When transactions are submitted to the blockchain network, the transactions are ordered in a block. For energy transactions, specific data attributes must be present on the transaction such as: date, timestamp, certificate type, tracking system identification, certificate data, renewable fuel type, and renewable facility location. RECs can be labeled at the point of origin and blocks could be created with REC data (transactions) in the DLT based trading platform.
Network layer	Within the blockchain network, several chains can be created with different sets of permissions. Specific network protocols depend on the DLT should be used.
Infrastructure layer	The DLT network may consist of middleware that interfaces with the physical world and the DLT. This would also involve the infrastructure to host the DLT nodes.
Physical layer	This layer pertains to sensors, IoT devices and smart meters report energy production and consumption. Devices can be configured to export the data directly to an off-chain network to develop machine learning and data analytic models that can forecast load and energy generation more accurately.

5.4.5. Cybersecurity gaps/considerations

EVs are susceptible to relay and spoofing attacks from illegitimate signals. These attacks could allow compromised assets that already have access to the DLT to manipulate the rate of charging or change charging requests. For example, consider the setting in which a compromised asset manipulates a legitimate signal. In this case, an illegitimate signal could be made available on the DLT (by the compromised asset) and accessed by honest assets, thereby affecting the EV capabilities such as charging rates. The compromised asset could continue to generate illegitimate signals, which can stop the EV from charging or detecting legitimate signals. This is not a direct attack on the DLT but rather shows the potential impact of compromised or illegitimate data on the DLT.

Table 4
Microgrid use case requirements mapped to the DLT cybersecurity stack.

Application layer	Distributed applications that can be used by the peers/DERs to participate in the renewable energy trading platform belong to this layer.
Execution layer	The business logic pertaining to the renewable energy trading platform that is outside the scope of DLT will run through the smart contract or equivalent. The distributed applications from the above layer will address their queries or requests to the execution layer software (such as smart contracts).
Consensus layer	Various consensus algorithms may be used in this use case. Because this is a closed ecosystem with known or pre-approved participants, a consensus that is appropriate for a permissioned setting is recommended. Examples of such consensus include PoA, BFT-based consensus, *etc.*
Data model layer	Information/transactions related to the renewable energy trades between the peers will be recorded in the blocks. Registration of these peers and microgrid DERs could be treated as transactions and recorded to the ledger.
Network layer	Specific protocols may augment the DLT platform communication protocols.
Infrastructure layer	This includes individual DLT notes pertaining to the participating entities from the Microgrid such as the DER and load owners.
Physical layer	The physical layer may include microgrid systems such as the microgrid controller, DER, *etc.* Depending on the microgrid use case, the physical layer may not have any DLT associated element while the owner will interact with the blockchain starting from the infrastructure layer

Table 5
Main characteristics of the three referenced EV charging scenarios considered in this study. Scenario 1: Home Charging; Scenario 2: Large Building or Office; Scenario 3: Public and Commercial Charging Station. CPMS: Charge Point Management System. EVSE power data was derived from [57].

Parameter	Scenario 1	Scenario 2	Scenario 3
Number of users	Typically single user	Multiple subscribed users	Multiple unsubscribed users
Number of EVSE	Typically single EVSE	Multiple EVSE	Multiple EVSE
EVSE Power	From 3.6 to 7.2 kW	Up to 22 kW	Up to 80 kW or more
Type of Users	Homogeneous (family members)	Homogeneous (tenants or workers)	Heterogeneous (public service)
Authorization	Not required	Required	Required
Billing Services	No	No	Yes
Reservation	No	Yes	Yes
Grid Services	Yes, by means of a HEMS	Yes, by means of a BMS or an EMS	Yes, by means of EMS or CPMS

5.5. Use case 5: Grid security and supply chain

Modern supply chains consist of products from many vendors and software from countless sources. It also is beneficial to energy providers to have multiple sources of supply for each component to provide redundancy and alternate supply options to protect against single provider shortages. For the purpose of verifying entities that are contributing to supply chains, it is desirable to use the strength offered by DLT for connecting data items related to manufacturers, vendors, and end system applications [59]. Verification of distributed suppliers leads to product accountability, leading to the security of the overall supply chain and subsequently a more secure framework for operational grid assets.

The premise of this use case is as follows: DLT is used for distribution of grid asset Identity Non-Fungible Tokens (I-NFT), which contain unique device identifiers and cryptographic components required for secure management. The I-NFT is additionally used to support grid security as the base components for all common security features that are built into the I-NFT. Cryptographic components and protected operations to support the grid assets through all stages of the supply chain are shown in Fig. 11.

In conjunction with the I-NFT deployed in end nodes, the DLT service provides the ability to provision them at various stages in the supply chain. Repeated provisioning of I-NFTs at different stages in the life cycle of grid assets enables the availability of required cryptographic components within the I-NFT needed for each stage of the supply chain. The continued provisioning enables the tracking of the lifecycle of the grid assets on the DLT as well as the identification of current status and/or disposition of the grid assets over time.

5.5.1. Domains and actors

Manufacturing scope: This first stage scope is responsible for the protection and security of the first stage of provisioning only. Contractual relationships and uniquely enforced processes, personnel restriction, and special-purpose hardware protect this stage. Once turned over from this stage, the DLT service takes ownership and overwrites transport keys to become the primary supply chain register.

Vendor scope: The DLT registrar assigned in the previous scope takes ownership of the process. This level provides interpreted and unique I-NFT creation such that hardware security modules enable processes sealed from human access to create and distribute I-NFT to the grid assets.

Table 6
EV charging use case requirements mapped to the DLT cybersecurity stack.

Application layer	P2P applications that can integrate EV software, users' mobile applications, central aggregator (management system), DLT network, and the charging software layer.
Execution layer	Smart contracts are implemented on the DLT platform. Smart contracts may need access to non-DLT external data that could be facilitated through APIs.
Consensus layer	Consensus that is appropriate for permissioned setting is required. Examples of such consensus can include PoA, BFT-based consensus, *etc.*
Data model layer	The data model functions are expected to rely between the central aggregator and the DLT network operations.
Network layer	Specific protocols depend on the underlying DLT platform.
Infrastructure layer	Individual DLT nodes pertaining to EVs, charging stations, and central aggregators are included in this layer.
Physical layer	The charging station system/sensor could have an associated node (connected to the infrastructure layer). Depending on the implementation, EV sensors may have an associated node, but, in most cases, the EV owner may have the node.

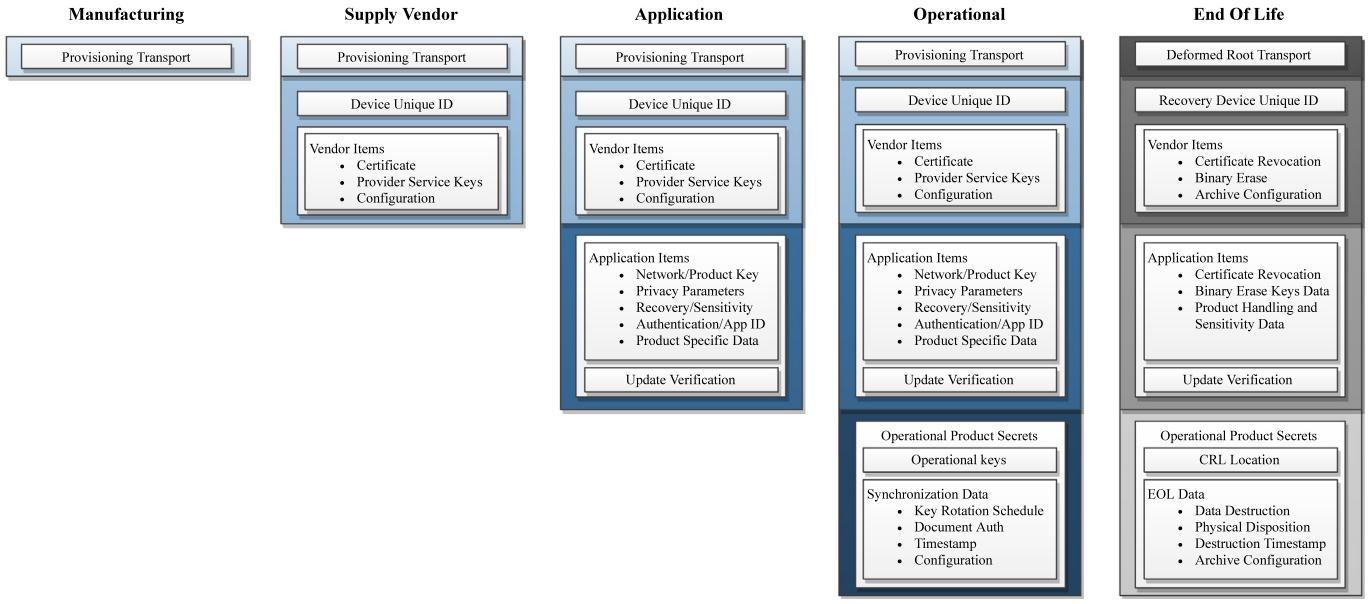

Fig. 11. Grid Security and Supply Chain. Supply Chain I-NFT Components.

Application scope: I-NFTs for this stage encompass operational components linked to a particular network segment or product line. I-NFT components support cryptographic communications, trust root, and extended security/privacy features for physical security and logical data operations.

Operational scope: Components within the I-NFT are used to extend and augment operations by creating derived- or temporary-use components.

End of life scope: Services supported by the DLT provider support the discontinued existence for a grid asset eco-system-enabled device. DLT end-of-life services provide security value for both supply chain and operational DER security. The primary feature offered by this stage represents solutions similar to Certificate Revocation with the expanded revocation of right-to-operate or removal of trusted status.

5.5.2. Application and physical security

In conjunction with the end node I-NFT distribution, the use of special I-NFT containment cyber physical integrated circuit components provide for additional physical hardening. This combination of cyber physical device and DLT provides hardened protected wallet features for the grid asset [60].

The pairing of I-NFT and DLT with this use case provides distributed grid security capability acting as an underlying framework for zero-trust in operational networks where any grid asset's trusted state is verified by DLT [60]. Individual document exchanges digitally signed with I-NFT components enable DLT verified proof of origin leveraged for many application uses such as: digital signed sensor reading, software update verification, and operational message verification.

5.5.3. Application to the DLT cybersecurity stack

Relationships for this use case exist for each level of the DLT cybersecurity stack. This use case spans the entire supply chain and uses the DLT to connect physical and digital supply chain components. For this, the top of the stack contains the industry-level coordination that will enable several applications to support cross-industry supporting services and tools for management for large-scale supply chains.

Each DLT execution is an instance of services provided as products are manipulated within the supply chain. The transition of supply from one owner to another, results in the creation of a consumable I-NFT placed into a DLT transaction. The coordination of services between parties that are not trusted requires governance, frameworks, and relational models, which are defined in many of the intermediate layers of the DLT cybersecurity stack. Lower layers encompass the individual instances of supporting supply chain distributed software or hardware operated by service providers. Table 7 maps the anticipated relationships in more detail.

5.5.4. Cybersecurity gaps/considerations

Supply chains are vulnerable to inheriting the security issues of third-party suppliers of the grid. These security issues, such as stolen security credentials and ransomware, can cause a cascading effect on grid operations. For example, a reliance on compromised third-party suppliers can affect the inter-connections and inter-dependencies between several components and services in the grid. In this case, such reliance can hinder the ability to meet the grid security and supply chain requirements such as availability and integrity. To potentially counter such attacks, utilities should implement monitoring controls and collect threat information.

6. Conclusions and the way forward

Modernization of the grid includes the integration of renewable energy sources, such as wind and solar PV. To take advantage of these new resources, the overall architecture is changing from centralized control and management to distributed and decentralized control. With this significant architecture change, new operational methods are being considered. This paper provides an initial foundation for the P2418.5 standardization process for cybersecurity DLT. Specifically, we undertook the following:

1. An overview on how DLT may be used in energy utilities was provided. The key cybersecurity benefits of DLT

Table 7
Grid security and supply chain mapped to the DLT cybersecurity stack.

Application layer	The application layer contains supporting registers, each of which would service an industry, set of products, or geographical region for the grid assets. This layer also may contain UI applications (*e.g.*, dashboard and mobile apps.). There may be a need for separate applications to differentiate between vendor-to-supplier coordination, vendor-to-consumer coordination among other combinations.
Execution layer	Smart contracts produce and store I-NFTs and store the state of grid asset on the distributed ledger.
Consensus layer	Consensus is used to track ownership and originating registers for I-NFT. The nodes associated with the known permissioned entities would be eligible to participate in consensus. Depending on the coordination (*e.g.*, vendor-to-supplier, vendor-to-consumer, *etc.*), the consensus forming rules would vary.
Data Model layer	The data model includes the definition of the I-NFT and any predefined attributes and their values. Examples of the attribute–value pairs include identity information, timestamp, proof of data, *etc.*
Network layer	Specific protocols depend on the underlying DLT platform.
Infrastructure layer	Individual DLT nodes are used for distribution of the grid asset I-NFT. Furthermore, the manufactures/vendors, suppliers, consumers, *etc.* may have their individual peer nodes hosted on physical or virtual infrastructures. The production, distribution, and integration of supporting software and cyber-physical I-NFT devices would be contained within this level.
Physical layer	The use of special I-NFT containment cyber-physical integrated circuit components for the grid asset would belong to this layer. Any peripheral sensors or data acquisition systems that are responsible to report the state of the asset or state parameters of the asset belong in this layer.

are to provide data integrity and immutability for storing and securing grid communications and data. Cryptography, one of the core elements of DLT, has been discussed. Relevant cybersecurity attributes and considerations to DLT applications in power and energy use cases were also investigated.
2. We posited that a private permissioned architecture is more likely to be deployed in the majority of the energy DLT use cases (*e.g.*, partly due to the sensitive nature of the sector), in which only authorized and trusted entities can participate. Additional security controls such as identification and authentication for participating devices and individuals need to be included. A discussion of the cybersecurity risks associated with DLT, including potential vulnerabilities and attack vectors also was provided.
3. We also demonstrated the utility of the proposed DLT cybersecurity stack comprising layers, architectural definitions, security controls, and applicable components, and mapped to the widely used TCP/IP, OSI, and SGAM models, with several use cases.

Future work pertains to performing in-depth analysis of the DLT cybersecurity stack, and further improving the proposed concepts. Here are the potential next steps of the task force:

1. Explore the application of the DLT cybersecurity stack to various use cases with protocol-specific details;
2. Continue using the DLT cybersecurity stack to develop a security guidance and framework to evaluate DLTs applicability to use cases;
3. Facilitate coordination with other DLT related working groups inside and outside IEEE;
4. Augment the DLT cybersecurity stack as needed to facilitate the evolving nature of the DLT.

CRediT authorship contribution statement

Sri Nikhil Gupta Gourisetti: Conceptualization, Investigation, Analysis, Writing of the article. **Ümit Cali:** Conceptualization, Investigation, Analysis, Writing of the article. **Kim-Kwang Raymond Choo:** Conceptualization, Investigation, Analysis, Writing of the article. **Elizabeth Escobar:** Conceptualization, Investigation, Analysis, Writing of the article. **Christopher Gorog:** Conceptualization, Investigation, Analysis, Writing of the article. **Annabelle Lee:** Conceptualization, Investigation, Analysis, Writing of the article. **Claudio Lima:** Conceptualization, Investigation, Analysis, Writing of the article. **Michael Mylrea:** Conceptualization, Investigation, Analysis, Writing of the article. **Marco Pasetti:** Conceptualization, Investigation, Analysis, Writing of the article. **Farrokh Rahimi:** Conceptualization, Investigation, Analysis, Writing of the article. **Ramesh Reddi:** Conceptualization, Investigation, Analysis, Writing of the article. **Abubakar Sadiq Sani:** Conceptualization, Investigation, Analysis, Writing of the article.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The content presented in this article documents the activities of the IEEE P2418.5 and IEEE Blockchain Transactive Energy (BCTE) working group members. This includes the IEEE Standards Association (SA), IEEE Power and Energy Society (PES) Smart Building, Loads and Customer System (SBLC) Technical Committee, and the IEEE Blockchain Initiative/IEEE Future Directions. We acknowledge these organizations for sponsoring and promoting some of these initiatives.

Appendix. Comparison of blockchains

The objective of this appendix is to provide a thorough comparative analysis between public permissionless and private permissioned blockchains (see Tables A.8–A.16).

Table A.8
Immutability of the Ledger.

Permissionless/Public	Permissioned/Private/Enterprise
Immutability refers to the notion that the content entered into the ledger cannot be changed or edited. In blockchain/DLT, this means that any change is identified. It is still possible to maliciously alter the data. Therefore, a ledger creates and reads properties and lacks edit and delete properties.	The immutability aspect of the ledgers is maintained in the private/permissioned blockchains. The cryptographic linkage between the blocks of transactions that are recorded in the ledger addresses the integrity security objective. The principle of hash-based cryptographic linkage between the blocks is the same for all blockchains (private, public, hybrid).

Table A.9
Identity of the Participants.

Permissionless/Public	Permissioned/Private/Enterprise
In most cases, there is almost no sense of identity and the users are considered to be anonymous. The node's information (human or a device) is not associated with transactions and the data records in the ledger. This may be an undesirable feature in some applications (such as in power and energy applications). Non-repudiation is limited to the individual node addresses, *i.e.*, transactions can be traced to the individual node addresses, but the true entity-based identity (human or device) is unknown.	The philosophy of enterprise/private blockchains is geared toward solving problems that can use blockchain technology in a restricted multi-organizational facet to facilitate the solution to the entire business network. Therefore, anonymity and transparency are augmented with identity management and permission management. To achieve this, the enterprise blockchain uses a MSP. MSP is a directory of all valid members and their identities pertaining to the channel. Some blockchains facilitate MSP by building upon an organization's or business network Lightweight Directory Access Protocol (LDAP), Active Directory, oAuth, and similar technologies. Unlike public blockchains, non-repudiation can be associated with a particular entity (human or device) in private blockchain architectures because the transaction relationship can be traced to the node (human or device) and not just the node address.

Table A.10
Data transparency.

Permissionless/Public	Permissioned/Private/Enterprise
All of the data is expected/assumed to be fully transparent. However, due to the anonymity of the participants, it is extremely difficult (or near impossible) to associate the data record or transaction to an individual/entity. This may be an undesirable feature in some applications (such as in power and energy applications).	In most cases, total transparency is replaced with the ability to define access control rules; ultimately, governance policies are placed in the hands of the business network/coalition. The multi-organizational network can collectively define the rules around read and write access, as well as transaction initiation access guided by the well-known access control principles such as least privilege and need-to-know to facilitate needed confidentiality and need-based availability. This lets the business network control who can read what data and who can do what with the data. Often Access Control Lists and MSP could be used to assign and maintain permissions.

Table A.11
Smart contracts.

Permissionless/Public	Permissioned/Private/Enterprise
Smart contracts do not exist in some of the early adoptions of blockchain (such as Bitcoin). Ethereum introduced smart contracts. Earlier blockchains which were mostly public/permissionless introduced their own proprietary smart contracts language, such as solidity for Ethereum. One of the biggest drawbacks with the earlier blockchain smart contract architecture is the inability to upgrade them over time. For example, in Ethereum, the solidity language-based smart contract is deployed across Ethereum nodes as bytecode. Once deployed, the bytecode is permanent on the blockchain until a fully replaced smart contract is released.	Private/enterprise blockchains carried on this property given its immense value. The challenge around smart contract versioning and maintainability is addressed in most private/enterprise blockchains. Therefore, the technology adopters can fix the bugs and release newer versions overtime. In addition, the private/enterprise blockchains eliminated the need to develop smart contracts in any proprietary language. These smart contracts can be written in well-known languages, such as JavaScript, Python, Golang, *etc.* Software lifecycle management principles are integral to the smart contract development process in most private/enterprise blockchains.

Table A.12
High-level functions of the node (decentralization *vs.* quasi-decentralization).

Permissionless/Public	Permissioned/Private/Enterprise
At a high level, every node in a public blockchain performs three functions: (1) each node is responsible for keeping a copy of the ledger; (2) all nodes would execute any requested smart contract (*e.g.*, if an entity called a function out of a smart contract, that function is executed by all of the nodes in the network); and (3) nodes attempt to keep their copy of the ledger in sync with all of the copies of the ledger on the network. The goal is to have the same data in the same order in all of the ledgers on the network. This achieves full decentralization but a high price of extremely slow transactional speeds and the lack of control on a node's functions. Public/permissionless blockchains do not control aspects such as who can join the blockchain, who can form consensus, what the minimum/maximum number of nodes is, *etc.*	Most private and enterprise blockchains split this functionality and spread them across multiple classes of nodes. Such blockchains are neither fully centralized nor fully decentralized. They may fall under the category of quasi-decentralized infrastructures while continuing to mitigate a single point of failure. These networks, therefore, are not fully peer-to-peer, but have the needed redundancy, fail over, and fault tolerance. This infrastructural change increases the scalability factor. For example: Hyperledger Fabric has three types of nodes. First, there are committing nodes that keep redundant copies of ledgers. Second, there are endorsing nodes that execute any requested smart contract code and also keep a redundant copy of the ledger without adding any overhead. Third, there are ordering nodes that handle the data ordering and ledger synchronization functions. In permissioned blockchains, the authority organizations or entities can control the number of nodes that would form consensus (*e.g.*, endorsement nodes in Hyperledger Fabric), who can join the network and the number of nodes that should be on the blockchain network. In regard to identifying that number, it depends on the nodes that need to transact, and the contractual terms between the organizations that would dictate the number of consensus nodes (such as endorsing and ordering nodes in Fabric) that an organization can have. The key is to have enough consensus forming nodes that the network is Byzantine fault tolerant (see previous sections for details).

Table A.13
Trust.

Permissionless/Public	Permissioned/Private/Enterprise
Most permissionless and public blockchains went with the notion of ensuring secure transaction of digital commodities without the need of reconciliation and trust establishment between transacting entities.	Because enterprise and private blockchain solutions are geared more to applications with well-defined boundaries and business networks, these blockchains are designed to function in a partial or fully trust environment.

Table A.14
Consensus mechanism.

Permissionless/Public	Permissioned/Private/Enterprise
Append-only ledgers are managed by group consensus. Blockchain nodes attempt to stay in-sync with each other using the idea of group consensus. The concept of group consensus, to some extent, is central to the ability of any participating node to participate in the consensus forming process. Under group consensus, nodes verify if the data was recorded correctly. However, the nodes lack the ability to verify the truth of the data itself.	In the enterprise solutions, group consensus is replaced with participant-consensus. Based on the defined rules, the participants may know each other. Therefore, participants have the ability to agree upon transactional terms and expect the rest of the network to accept their transaction and their terms. The transacting entities could have a rule set or policy for certain nodes to validate and approve their transaction in addition to their mutual agreement. However, unlike the permissionless/public blockchains with PoW consensus (discussed in later sections), there is no requirement for the involvement of the entire network.

Table A.15
Shared ledger.

Permissionless/Public	Permissioned/Private/Enterprise
The ledger is shared with all the nodes and several redundant copies of the ledger exist on the network (addresses single point of failure). Therefore, all nodes own and maintain a copy of the ledger. The governing rules around the ledger are defined at the overall blockchain network level.	The concept of a global ledger is replaced with localized ledgers to facilitate need-based availability. Starting from the Hyperledger Fabric blockchain, many blockchains have been honing this concept. For example, Hyperledger Fabric does not have a single global ledger. Instead, it requires the end user coalition to establish their own channel on Fabric's network. The ledger is fully localized and only visible to that channel, and the business network can define the security rules and processes as they desire. This concept ties back to the elimination of the group consensus that is described previously. In such a non-global architecture, there is no one place where all data is stored. Therefore, an attacker would not obtain all of the data by attacking certain nodes on the network (addresses single point of failure).

Table A.16
Traceability in the ledger.

Permissionless/Public	Permissioned/Private/Enterprise
Cryptocurrency-based blockchains, such as Bitcoin, are primarily used to track the history of Bitcoin. However, Ethereum extended that capability to track any feasible digital asset, including ether (Ethereum cryptocurrency).	The ability to track any digital asset through the ledger is carried on by the private and enterprise blockchains.

References

[1] S. Sayed, T. Hussain, A. Gastli, M. Benammar, Design and realization of an open-source and modular smart meter, Energy Sci. Eng. 7 (4) (2019) 1405–1422.

[2] M.I. Henderson, D. Novosel, M.L. Crow, Electric power grid modernization trends, challenges, and opportunities, IEEE Power Energy Mag. 15 (5) (2017).

[3] B. Kroposki, P. Skare, R. Pratt, T. King, A. Ellis, Grid modernization laboratory consortium - testing and verification, in: 2017 Ninth Annual IEEE Green Technologies Conference, GreenTech, IEEE, Denver, CO, USA, 29-31 March, 2017, pp. 238–245, http://dx.doi.org/10.1109/GreenTech.2017.41.

[4] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, A. Al Ali, Smart grid cyber security: Challenges and solutions, in: 2015 International Conference on Smart Grid and Clean Energy Technologies, ICSGCE, IEEE, Offenburg, Germany, 20-23 Oct., 2015, pp. 170–175, http://dx.doi.org/10.1109/ICSGCE.2015.7454291.

[5] P.A. Giglou, S. Najafi Ravadanegh, Defending against false data injection attack on demand response program: A bi-level strategy, Sustain. Energy Grids Netw. 27 (2021) http://dx.doi.org/10.1016/j.segan.2021.100506.

[6] J. Khazaei, Cyberattacks with limited network information leading to transmission line overflow in cyber-physical power systems, Sustain. Energy Grids Netw. 27 (2021) http://dx.doi.org/10.1016/j.segan.2021.100505.

[7] D. Tapscott, A. Tapscott, Blockchain Revolution: How the Technology behind Bitcoin and Other Cryptocurrencies Is Changing the World, Portfolio, 2016, p. 348.

[8] P. Zhuang, T. Zamir, H. Liang, Blockchain for cybersecurity in smart grid: A comprehensive survey, IEEE Trans. Ind. Inf. 17 (1) (2021) 3–19, http://dx.doi.org/10.1109/TII.2020.2998479.

[9] M.B. Mollah, J. Zhao, D. Niyato, K.Y. Lam, X. Zhang, A.M. Ghias, L.H. Koh, L. Yang, Blockchain for future smart grid: A comprehensive survey, IEEE Internet Things J. 8 (1) (2021) 18–43, http://dx.doi.org/10.1109/JIOT.2020.2993601.

[10] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303, http://dx.doi.org/10.1109/ACCESS.2016.2566339.

[11] K. Kaur, A. Hahn, S.N.G. Gourisetti, M. Mylrea, R. Singh, Enabling secure grid information sharing through hash calendar-based blockchain infrastructures, in: 2019 Resilience Week, RWS, IEEE, San Antonio, TX, USA, 4-7 Nov., 2019, pp. 200–205, http://dx.doi.org/10.1109/RWS47064.2019.8971819.

[12] E. Munsing, J. Mather, S. Moura, Blockchains for decentralized optimization of energy resources in microgrid networks, in: 2017 IEEE Conference on Control Technology and Applications, CCTA, IEEE, Maui, HI, USA, 27-30 Aug., 2017, pp. 2164–2171, http://dx.doi.org/10.1109/CCTA.2017.8062773.

[13] M. Mylrea, S.N.G. Gourisetti, Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security, in: 2017 Resilience Week, RWS, IEEE, Wilmington, DE, USA, 18-22 Sep., 2017, pp. 18–23, http://dx.doi.org/10.1109/RWEEK.2017.8088642.

[14] M. Mylrea, S.N.G. Gourisetti, R. Bishop, M. Johnson, Keyless signature blockchain infrastructure: Facilitating NERC CIP compliance and responding to evolving cyber threats and vulnerabilities to energy infrastructure, in: 2018 IEEE/PES Transmission and Distribution Conference and Exposition, T&D, IEEE, Denver, CO, USA, 16-19 April, 2018, pp. 1–5, http://dx.doi.org/10.1109/TDC.2018.8440380.

[15] U. Cali, C. Lima, Energy informatics using the distributed ledger technology and advanced data analytics, Cases on Green Energy and Sustainable Development, IGI Global, 2020, pp. 438–481, http://dx.doi.org/10.4018/978-1-5225-8559-6.ch016.

[16] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, A. Peacock, Blockchain technology in the energy sector: A systematic review of challenges and opportunities, Renew. Sustain. Energy Rev. 100 (February 2018) (2019) 143–174, http://dx.doi.org/10.1016/j.rser.2018.10.014.

[17] Y. Sang, U. Cali, M. Kuzlu, M. Pipattanasomporn, C. Lima, S. Chen, IEEE SA Blockchain in energy standardization framework: Grid and prosumer use cases, in: 2020 IEEE Power & Energy Society General Meeting, PESGM, IEEE, Montreal, QC, Canada, 2-6 Aug., 2020, pp. 1–5, http://dx.doi.org/10.1109/PESGM41954.2020.9281709.

[18] IEEE Standard Association P2418.5 Working Group, IEEE SA P2418.5 - Standard for Blockchain in Energy, IEEE Standard Association, 2020, URL: https://standards.ieee.org/project/2418_5.html.

[19] U. Cali, C. Lima, X. Li, Y. Ogushi, Dlt / blockchain in transactive energy use cases segmentation and standardization framework, in: 2019 IEEE PES Transactive Energy Systems Conference, TESC, IEEE, Minneapolis, MN, USA, 8-11 July, 2019, pp. 1–5, http://dx.doi.org/10.1109/TESC.2019.8843372.

[20] GridWise Architecture Council, GridWise Transactive energy framework. Version 1.0, 2015, URL: https://www.gridwiseac.org/pdfs/te_framework_report_pnnl-22946.pdf.

[21] S.N.G. Gourisetti, M. Mylrea, H. Patangia, Evaluation and demonstration of blockchain applicability framework, IEEE Trans. Eng. Manage. 67 (4) (2020) 1142–1156, http://dx.doi.org/10.1109/TEM.2019.2928280.

[22] Y.J. Song, Design of binary sequences with optimal frame synchronization property, in: 2000 IEEE International Symposium on Information Theory, ISIT, IEEE, Sorrento, Italy, 25-30 June, 2000, p. 353, http://dx.doi.org/10.1109/isit.2000.866651.

[23] IEEE Standard Association, Develop standards: Who oversees the process?, 2020, URL: https://standards.ieee.org/develop/develop-standards/govern.html.

[24] B. Marr, A complete beginner's guide to blockchain, 2017, URL: https://www.forbes.com/sites/bernardmarr/2017/01/24/a-complete-beginners-guide-to-blockchain/?sh=2245f1f06e60.

[25] D. Yaga, P. Mell, N. Roby, K. Scarfone, NIST Internal Report 8202: Blockchain Technology Overview, Technical Report, National Institute of Standards and Technology, Gaithersburg, MD, 2018, http://dx.doi.org/10.6028/NIST.IR.8202, arXiv:1906.11078.

[26] M. Alofs, Blockchain: Proof of authority, 2018, URL: https://newsignature.com/articles/blockchain-proof-of-authority/.

[27] M. Gill, What is proof of burn?, 2018, URL: https://99bitcoins.com/what-is-proof-of-burn/.

[28] M. Castro, B. Liskov, Practical Byzantine fault tolerance and proactive recovery, ACM Trans. Comput. Syst. 20 (4) (2002) 398–461, http://dx.doi.org/10.1145/571637.571640.

[29] C. Cachin, Architecture of the hyperledger blockchain fabric, 2016, URL: https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf.

[30] B. Putz, G. Pernul, Detecting blockchain security threats, in: 2020 IEEE International Conference on Blockchain, Blockchain 2020, IEEE, Rhodes, Greece, 2-6 Nov., 2020, pp. 70–76, http://dx.doi.org/10.1109/Blockchain50366.2020.00046.

[31] N. Smart, Crypto Assets: Introduction to Digital Currencies and Distributed Ledger Technologies, Technical Report, European Union Agency for Cybersecurity (ENISA), 2021.

[32] H. Knudsen, J.S. Notland, P.H. Haro, J. Li, Consensus in blockchain systems with low network throughput: A systematic mapping study, in: 3rd Blockchain and Internet of Things Conference, BIOTC 2021, Association for Computing Machinery, Ho Chi Minh City, Vietnam, 8-10 July, 2021, pp. 15–23, http://dx.doi.org/10.1145/3475992.3475995.

[33] S. Kaur, S. Chaturvedi, A. Sharma, J. Kar, A research survey on applications of consensus protocols in blockchain, Secur. Commun. Netw. 2021 (6693731) (2021) http://dx.doi.org/10.1155/2021/6693731.

[34] N. Kolokotronis, K. Limniotis, S. Brotsis, C. Pavué, G. Bendiab, S. Shiaeles, CYBER-TRUST Blockchain Security Analysis (I). Deliverable D7.4 of the of the Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things poject co-funded by the Horizon 2020 Framework Programme of the European Union, Grant Agreement nr. 786698, Technical Report, Cyber-Trust Consortium, 2021.

[35] A. Singh, R.M. Parizi, Q. Zhang, K.K.R. Choo, A. Dehghantanha, Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities, Comput. Secur. 88 (2020) 101654, http://dx.doi.org/10.1016/j.cose.2019.101654.

[36] S. Wang, C. Wang, Q. Hu, Corking by forking: Vulnerability analysis of blockchain, in: 2019 IEEE Conference on Computer Communications, INFOCOM, IEEE, Paris, France, 29 April-2 May, 2019, pp. 829–837, http://dx.doi.org/10.1109/INFOCOM.2019.8737490.

[37] H. Liu, Z. Yang, Y. Jiang, W. Zhao, J. Sun, Enabling clone detection for ethereum via smart contract birthmarks, in: 2019 IEEE/ACM 27th International Conference on Program Comprehension, ICPC, IEEE, Montreal, QC, Canada, 25-26 May, 2019, pp. 105–115, http://dx.doi.org/10.1109/ICPC.2019.00024.

[38] O.G. Güçlütürk, The DAO hack explained: Unfortunate take-off of smart contracts, 2018, URL: https://ogucluturk.medium.com/the-dao-hack-explained-unfortunate-take-off-of-smart-contracts-2bd8c8db3562.

[39] J. Barragan, J. Jefferies, D. Jevans, Top 10 Blockchain Attacks, Vulnerabilities and Weaknesses, Technical Report, Cloud Security Alliance, 2021.

[40] M.B. Lourenço, L. Marinos, ENISA Threat Landscape 2019/2020 - The year in review, Technical Report, European Union Agency for Cybersecurity (ENISA), 2020, URL: https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020.

[41] H. Mayer, zk-SNARK explained: Basic principles, 2017, URL: https://blog.coinfabrik.com/wp-content/uploads/2017/03/zkSNARK-explained_basic_principles.pdf.

[42] S.N.G. Gourisetti, S.E. Widergren, M.E. Mylrea, P. Wang, M.I. Borkum, A.M. Randall, B.P. Bhattarai, Blockchain Smart Contracts for Transactive Energy Systems, Technical Report, Pacific Northwest National Lab. (PNNL), Richland, WA, 2019, http://dx.doi.org/10.2172/1658380.

[43] J.H. Mosakheil, Security threats classification in blockchains, in: Culminating Projects in Information Assurance, Vol. 48 (Ph.D. thesis), Herberger School of Business, 2018, p. 141, URL: https://repository.stcloudstate.edu/msia_etds/48.

[44] H. Anwar, Web 3.0 blockchain technology stack: The comprehensive guide, 2018, URL: https://101blockchains.com/web-3-0-blockchain-technology-stack/.

[45] V. Acharya, A.E. Yerrapati, N. Prakash, Oracle Blockchain Services Quick Start Guide, Packt Publishing, 2019, p. 350.
[46] United States Environmental Protection Agenc (EPA), Renewable energy certificates (RECs), 2021, URL: https://www.epa.gov/statelocalenergy/clean-energy-finance-using-renewable-energy-certificates-achieve-local.
[47] J. Wang, W. Chen, L. Wang, Y. Ren, R.S. Sherratt, Blockchain-based data storage mechanism for industrial internet of things, Intell. Autom. Soft Comput. 26 (5) (2020) 1157–1172, http://dx.doi.org/10.32604/iasc.2020.012174.
[48] CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart grid reference architecture, 2012, URL: https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf.
[49] OWASP Foundation, Top 10 web application security risks, 2020.
[50] F. Rahimi, S. Mokhtari, From ISO to DSO: Imagining a new construct – an independent system operator for the distribution network, Fortnightly Mag. (2014).
[51] F. Rahimi, A. Ipakchi, F. Fletcher, The changing electrical landscape: End-to-end power system operation under the transactive energy paradigm, IEEE Power Energy Mag. 14 (3) (2016) 52–62, http://dx.doi.org/10.1109/MPE.2016.2524966.
[52] F.A. Rahimi, S. Mokhtari, Distribution management system for the grid of the future: A transactive system compensating for the rise in distributed energy resources, IEEE Electrif. Mag. 6 (2) (2018) 84–94, http://dx.doi.org/10.1109/MELE.2018.2816846.
[53] F. Rahimi, S. Mokhtari, Grid-edge blockchain-based transactive energy platform design and implementation, IEEE Electrif. Mag. 9 (3) (2021).
[54] J. St. John, A blockchain-enabled smart meter for clean power trading? 2020, URL: https://www.greentechmedia.com/articles/read/a-blockchain-enabled-smart-meter-for-clean-power-trading.
[55] A. Goranovic, M. Meisel, L. Fotiadis, S. Wilker, A. Treytl, T. Sauter, Blockchain applications in microgrids: An overview of current projects and concepts, in: 43rd Annual Conference of the IEEE Industrial Electronics Society, IECON, IEEE, Beijing, China, 29 Oct.-1 Nov., 2017, pp. 6153–6158, http://dx.doi.org/10.1109/IECON.2017.8217069.
[56] H. Shareef, M.M. Islam, A. Mohamed, A review of the stage-of-the-art charging technologies, placement methodologies, and impacts of electric vehicles, Renew. Sustain. Energy Rev. 64 (2016) 403–420, http://dx.doi.org/10.1016/j.rser.2016.06.033.
[57] S. Rinaldi, M. Pasetti, E. Sisinni, F. Bonafini, P. Ferrari, M. Rizzi, A. Flammini, On the mobile communication requirements for the demand-side management of electric vehicles, Energies 11 (5) (2018) http://dx.doi.org/10.3390/en11051220.
[58] D. Hall, N. Lutsey, Emerging best practices for electric vehicle charging infrastructure, in: The International Council on Clean Transportation, ICCT, (October) The International Council on Clean Transportation (ICCT), Washington, DC USA, 2017, URL: http://www.theicct.org/sites/default/files/publications/EV-charging-best-practices_ICCT-white-paper_04102017_vF.pdf.
[59] M. Mylrea, S.N.G. Gourisetti, Blockchain for supply chain cybersecurity, optimization and compliance, in: 2018 Resilience Week, RWS, IEEE, Denver, CO, USA, 20-23 Aug., 2018, pp. 70–76, http://dx.doi.org/10.1109/RWEEK.2018.8473517.
[60] S.S. Saha, C. Gorog, A. Moser, A. Scaglione, N.G. Johnson, Integrating hardware security into a blockchain-based transactive energy platform, in: 2020 52nd North American Power Symposium, NAPS, IEEE, Tempe, AZ, USA, 11-13 Oct., 2021, pp. 1–6, http://dx.doi.org/10.1109/naps50074.2021.9449802.