Blockchain Security and Privacy Examined: Threats, Challenges, Applications, and Tools

Ahod Alghuried, Mohammed Alkinoon, Manar Mohaisen, An Wang, Cliff C. Zou, and David Mohaisen

***Abstract*—Blockchain technology has heralded a new era in digital innovation, revolutionizing our approach to designing and building distributed applications in the digital sphere. Essentially, blockchain technology operates as an immutable digital ledger, where each entry representing a digital transaction is indelible and cannot be altered once established. Initially designed as the fundamental framework for cryptocurrencies, blockchain has outgrown its original purpose, demonstrating significant potential in various industries and offering a variety of security and privacy features. To provide security and privacy features, blockchain systems employ different foundational notions and primitives while tackling diverse adversarial scenarios with various capabilities and goals. This study presents a fresh examination of the current state of applications, security and privacy notions and primitives, and threat models in blockchain systems. Additionally, this work highlights existing gaps in knowledge and outlines open questions, aiming to stimulate interest in further advancements in the field.**

I. Introduction

Blockchain technology has ushered in a new era of digital innovation, reshaping how we think about the design and engineering of distributed applications in the digital domain [1], [2]. Initially conceptualized as the underlying architecture for cryptocurrencies, blockchain has transcended its original applications, demonstrating significant potential in various sectors and lending various security and privacy features [3]. Technically, blockchain technology is akin to an immutable digital ledger where each entry in this ledger, representing a digital transaction, is permanent and unchangeable once made. Unlike a traditional ledger, the blockchain is distributed across numerous nodes (servers), making every transaction visible to all users and confirmed to all users only using consensus protocols [4]. Altering any entry would require changing the entire chain on all copies, an almost impossible task under most realistic attack scenarios. This ensures that the blockchain ledger remains a secure and transparent record of digital transactions [5]. The significance of decentralization extends beyond financial technology (FinTech) sector, profoundly impacting many sectors, including Internet of Things (IoT), Electric Vehicles (EVs), supply chain, healthcare systems, auction systems, electronic voting systems, and energy trading, among many others. For instance, supply chain management systems, one of the most promising applications of blockchain systems, are liberated from the need for central authority, enabling stakeholders to share information securely and directly.

This revolution in information sharing fosters enhanced transparency, traceability, and accountability, critical factors in a globally connected world [6]. However, the widespread adoption of blockchain technology brings forth a spectrum of security and privacy concerns. While ensuring data integrity, the immutable nature of blockchain raises questions about the right to be forgotten, a cornerstone of modern privacy laws like the General Data Protection Regulation (GDPR) [7]. Moreover, the public nature of many blockchain platforms poses additional challenges in balancing transparency with the need for confidentiality [8], [9]. Diverse primitives are developed, engineered, and deployed to address the multifaceted security, privacy, and operational aspects of blockchain systems. There are several aspects to these innovations, including decentralization, anonymity (including stealth addresses and pseudonyms), permission management, and a variety of cryptographic techniques (such as zero-knowledge proofs, differential privacy, multi-party computation, advanced digital signatures, and homomorphic encryption), as well as advances in data structures and hardware security. In different deployment scenarios, these primitives target specific threat models characterized by unique capabilities and adversarial objectives.

Because the landscape of the blockchain systems, their security and privacy primitives, the intended applications, and the threat aspects those primitives address are scattered, a systematic review of those aspects is necessary yet lacking. To this end, this paper delves into the intricate web of blockchain's security and privacy features, offering a comprehensive survey of the current landscape, challenges, and advancements. At the heart of blockchain's appeal is its promise of decentralization, lending its power to a range of applications. Initially conceptualized around the FinTech sector, blockchain provided a paradigm shift that has brought forth transparent, censorship-resistant transactions, smart contracts, and decentralized lending and borrowing protocols to such applications [10]. These advancements are pivotal for financial transactions and hold profound implications for data integrity and privacy. Similarly, features of blockchain systems are expected to bring in similar features in other applications and systems.

Objectives. This work aims to dissect blockchain technology's complex security and privacy issues by thoroughly surveying their landscape in the relevant communication and networking venues. We explore the existing challenges that stem from the technology's inherent characteristics and the innovative solutions emerging in response. The survey encompasses a range of applications, from healthcare to finance, highlighting

A. Alghuried, M. Alkinoon, C. Zou, and D. Mohaisen are with the Department of Computer Science at the University of Central Florida, Orlando, Florida 32816, USA. M. Mohaisen is with Northeastern Illinois University, Chicago, Illinois 60625. A. Wang is the Case Western Reserve University, Cleveland, Ohio 44106. D. Mohaisen is the corresponding author (email: mohaisen@ucf.edu).

how blockchain's versatility intersects with varied privacy and security demands. In delving into blockchain privacy and security, this paper also scrutinizes the tools and methodologies developed to enhance these aspects. The exploration is not limited to technical solutions but also encompasses regulatory and ethical considerations. As blockchain evolves, understanding the interplay between technology, regulation, and ethics becomes paramount in shaping its future trajectory.

Why Another Survey? As blockchain systems, applications, and their security and privacy are an extremely active research area, there has been many surveys in this space [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [4], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [2]. Those surveys address the security, privacy, and applications of blockchains. However, those surveys are limited in many ways. For instance, there have been several surveys that are solely dedicated to a single application, such as IoT [12], [28], [29], [32], [33], smart spaces [11], [24], [32], 5G [26], healthcare systems [13], [16], [31], machine learning [33], and auction [23], among others, limiting their scope. Second, concerning the security and privacy aspects, those surveys only tackle concerns [12], [13], [28], [30], [33] and largely ignore a systematic review of the techniques and primitives intended for the solutions. Finally, most of those surveys are dated, leaving a larger anticipated space and need for an updated look and comprehensive review of the security, privacy, applications, and threats in blockchain systems.

Various aspects distinguish our survey. First, our survey is comprehensive, covering a range of applications and primitives unexplored in the prior work. Second, our work considers an up-to-date review of the relevant works in the communication and networking community, a community with a different prospect on the security and privacy of blockchains. Third, this work considers the threat models in the form and capabilities associated with the surveyed primitives, which were previously unexplored. Overall, this paper provides an important, up-to-date, and comprehensive survey in this space.

Organization. The rest of this paper is organized as follows. In section II, we present the methodology used in building this survey. In section III, we review a sample of the applications of blockchain systems, the technical gap that blockchain systems fill for them, and how the security and privacy in such systems are addressed conceptually. More concretely, section IV reviews the actual primitives used for ensuring security and privacy in those applications. In section V, we review the threat models, in the form of capabilities and objectives, that the various primitives attempt to confine. In section VI, we put our work together through a brief discussion and takeaways, including open directions. Note that the challenges are embedded with each application and primitive.

II. Methodology

In the course of conducting this study, the primary emphasis has been on tackling the distinct elements outlined in section I. These include a thorough approach that is both current and prominent, with a specific concentration on reputable forums dedicated to the broader domain of security, privacy, and systems. To achieve this objective, the subsequent methodology was implemented to outline the examined literature.

Comprehensive. For a comprehensive study, we considered major publications in major venues specializing in security and privacy and focusing on blockchain with their relevant distributed systems and performance aspects. This includes various major security conferences, such as the IEEE Security and Privacy Symposium, The ACM Conference on Computer and Communications Security (CCS), ISOC Network and Distributed System Security (NDSS) Symposium, and USENIX Security, among others. Focusing on IEEE-sponsored venues, we also considered various IEEE conferences, such as the IEEE International Conference on Distributed Computing Systems (ICDCS), IEEE INFOCOM, IEEE Blockchain Conference, and IEEE International Conference on Blockchain and Cryptocurrency (ICBC), among others, and journals, such as IEEE IoT Journal, IEEE Transactions on Networks, Service, and Management, IEEE Systems Journal, and IEEE Transactions on Dependable and Security Computing, among others.

Up-to-date. While in the pursuit of having a comprehensive survey, we included various seminal publications from multiple points in the timeline of the development of blockchain systems. Our main focus has been on recent advances, focusing primarily on the last five years in developing blockchain systems, thus differentiating our work from most prior surveys and related works.

Pronounced. In making our survey more pronounced, we started by surveying the applications first, an attempt to explore the concrete notions and primitives of security and privacy and the threat models, putting them in perspective as they address actual threat capabilities and objectives, and meeting various design principles in the applications above. This differentiates our methodology from other publications, considering a more abstract representation of those applications and security and privacy expectations.

III. Blockchain Applications

Blockchains are promising in many applications. In this section, we review some of those applications, including IoT (§III-A), EVs (§III-B), FinTech ((§III-C), supply chain (§III-D), healthcare systems (§III-E), auctions (§III-F), electronic voting (§III-G), and energy trading (§III-H).

In reviewing those applications, we consider the specific challenges they face and how blockchains can help address those challenges with the appropriate design principles. Moreover, we summarize the takeaways and challenges that we believe require further attention from the research community in this specified application.

A. Internet of Things

The Internet of Things (IoT) encompasses a network of physical devices embedded with sensors, software, and communication modules that enable them to connect and exchange data with other devices and systems over a network, e.g., the Internet [36]. These devices range in complexity and can be ordinary household items like smart thermostats and refrigerators to more complex systems such as autonomous vehicles [37] and industrial machinery [38].

1) Overview and benefits: The benefit of IoT lies in harnessing real-time data, leading to enhanced operational efficiency, improved safety measures, and personalized user experiences [39], [40]. For instance, in smart cities, IoT technology helps manage traffic flow and energy use efficiently, while in healthcare, it facilitates continuous patient monitoring.

2) Challenges: IoT systems face significant challenges, particularly in ensuring security and privacy. The interconnected devices create a vast attack surface for cyber threats [41]. The decentralized nature of these systems, while offering flexibility and scalability, also complicates the enforcement of uniform security measures [42]. Additionally, the management of the enormous volume of data generated by these devices poses significant privacy and integrity issues, as this data often includes sensitive personal and commercial information [43]. The root causes of these challenges in IoT systems are manifold. The diversity of devices and lack of standardized protocols lead to interoperability issues and security vulnerabilities [44]. Each device, potentially having different security standards and protocols, contributes to a fragmented and insecure network [45]. Moreover, the traditional centralized models for data processing and storage are inadequate for managing the scale and complexity of data generated by IoT networks, leading to potential data breaches and inefficiencies [39], [46].

IoT faces several challenges, resulting in significant privacy and security risks due to a single point of failure, inefficient device updates, inconsistent protocols, and a lack of user awareness about security practices [47]. In centralized architectures, it becomes difficult to distribute updates promptly and uniformly apply robust security measures, leaving devices and networks vulnerable to attacks [47]. Additionally, the complexity of these systems often leads to users being uninformed about their devices' security and privacy risks [47]. Blockchain technology, with its decentralized approach, offers a potential solution to these issues by distributing data across the network, providing enhanced security and privacy.

3) Blockchain in IoT: Blockchain technology offers a promising solution to these IoT challenges. Its application in IoT systems involves using a decentralized and immutable ledger to record and store data exchanges between devices [48]. This ensures data integrity, transparency, and security, addressing the core issues of trust and privacy in IoT networks [49]. Blockchain enables secure, peer-to-peer transactions and interactions between devices without the need for a central authority, thereby enhancing efficiency and reducing vulnerability to single points of failure [39]. Smart contracts, a feature of blockchain, automate processes and agreements between devices in a secure and transparent way. This automation not only increases operational efficiency but also ensures compliance and reliability in device interactions [49].

Figure 1 delineates the pivotal components of an IoT blockchain system. Physical objects with sensors and connectivity features collect and interact with surrounding data [50]. The blockchain network operates as a distributed ledger, recording and verifying transactions and data from IoT devices in a transparent, tamper-proof manner [51]. The security of transactions in IoT systems heavily relies on consensus mechanisms, such as Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). Especially in scenarios with extensive device interaction and data exchange, the PBFT consensus mechanism emerges as a robust solution, ensuring consistency in a distributed network that might include hostile nodes [40], [48], [52].

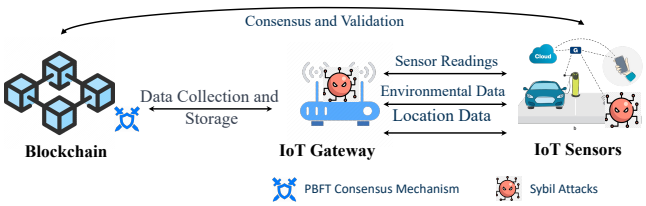

Fig. 1. A perspective on the IoT and the significance of blockchains and PBFT Consensus Mechanism in safeguarding security and privacy.

4) Challenges and Takeaways: Incorporating blockchain into the IoT presents an opportunity to elevate security and privacy, yet it demands a thorough evaluation of its drawbacks. While blockchain can fortify data security and assist in meeting regulatory requirements, challenges such as resource limitations in IoT devices, transparency issues with public blockchains, scalability concerns, and delays in achieving consensus need careful attention. A well-balanced design strategy is crucial to leverage the advantages of blockchain for secure and privacy-focused IoT solutions, ensuring optimal performance while maintaining data integrity.

Another challenge is how blockchain technology can be integrated into the IoT, including transaction fees and operational costs [53]. To address these issues, Wang *et al.*.[54] conducted a case study of IOTA, a blockchain model based on a Directed Acyclic Graph (DAG), which is used to examine these issues in depth. Among other benefits, their study promises reduced latency and enhanced transaction capacity, as well as eliminating transaction fees. Although IOTA has an edge over traditional blockchain systems like Bitcoin and Ethereum, with its higher throughput, it still struggles to meet the target of processing thousands of transactions per second (TPS), even after optimization. Moreover, transaction processing efficiency and the system's robustness depend on the volume of incoming transactions. These findings highlight the real challenges of using blockchain technology in IoT, especially the need for high transaction throughput without incurring significant fees or costs.

B. Electric Vehicles

The era of Electric Vehicles (EVs) heralds a transformative shift in transportation, intertwining environmental consciousness with technological advancement [55]. With their rise in popularity, EVs have evolved beyond mere transportation means; they are now dynamic data hubs capable of generating valuable insights for optimization and decision-making [56].

1) Overview and benefits: EVs are distinguished by their robust data collection, capturing essential metrics, such as energy usage, driving patterns, and charging behaviors [57]. This data is crucial for individual users, businesses, and governments, improving operational efficiency, driving sustainable practices, and informing policy development [58], [59].

2) Challenges: This revolution comes with challenges, especially in data management and privacy. The storage and processing of extensive EV data require secure and efficient systems [60]. Protecting this sensitive data from unauthorized access is a key concern, highlighting the need for enhanced security measures in the EV landscape [61].

3) Blockchains in EVs: Blockchain technology plays a transformative role in enabling EVs, providing a secure, decentralized framework for managing EV data. Its application in EV systems means every data transaction related to vehicle performance, charging station usage, or maintenance records is recorded on a blockchain. This ensures not only the security and integrity of the data but also its traceability and transparency where disputes may arise.

The decentralized nature of blockchain eliminates centralized vulnerabilities, significantly reducing the risk of data breaches [62]. Smart contracts, an integral part of the blockchain, can automate transactions and processes, from managing charging station payments to ensuring the efficient distribution of energy resources among EVs [60].

Duan *et al.*.[63] investigated smart contracts' utilization to improve electric vehicles' charging and discharging schedules based on electricity prices and grid load levels. This system aims to optimize EV charging patterns by considering electricity prices, which helps shift peak loads and enhance the power grid's stability. The use of smart contracts between users and charging stations facilitates real-time electricity price adjustments, incentivizes users through rewards or fines to follow optimal charging times, and ultimately contributes to a more stable and efficient energy distribution network. This automation streamlines operations and enhances the user experience while maintaining a high data privacy and security standard [64]. Moreover, blockchain can facilitate the creation of a shared, interoperable platform for various stakeholders in the EV ecosystem, including manufacturers, service providers, and consumers [65], [66]. This enhances collaboration and data sharing while maintaining strict privacy controls [55].

Practical blockchain use in the EV industry extends beyond handling payments for charging. It opens up opportunities for P2P energy transactions among EV owners and between EVs and the electrical grid. This approach enables owners to sell surplus energy, fostering a decentralized marketplace for energy. For instance, Khan [67] explored a blockchain-based framework that supports P2P energy exchanges and payments for EV charging where individuals generating additional electricity from renewable sources, such as solar panels, can sell their surplus to charging stations or directly to other EV owners. Transactions are conducted through digital wallets, ensuring trust, transparency, and security among all parties involved. By incorporating smart contracts on the Hyperledger Fabric platform, the system automates billing and payments, minimizing manual oversight and making the process of energy trading and charging more efficient for EVs.

The integration of blockchain technology and EVs has the potential to create a robust ecosystem that offers enhanced transparency, security, and efficiency, as illustrated in Figure 2. As shown, the system's architecture encompasses several critical components. Firstly, EVs generate and compile energy

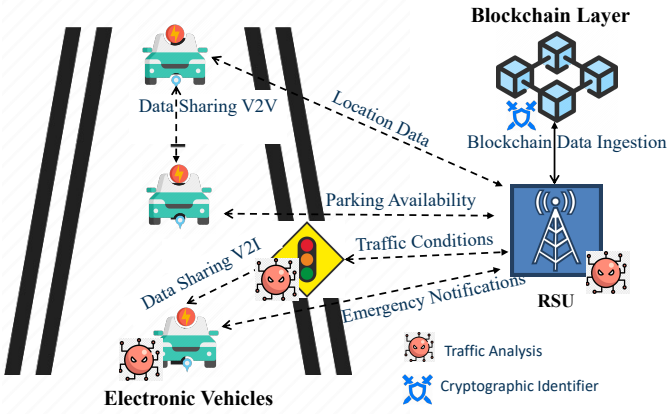

Fig. 2. Illustration of incorporating blockchain technology and Cryptographic Identifiers in EVs to enhance security and privacy.

consumption, charging, and performance data, which are then securely recorded on the blockchain as entries [62]. A cryptographic identifier uniquely identifies each entry, ensuring the ledger is immutable. Secondly, charging stations are equipped with communication modules, enabling interaction with EVs and recording charging transactions on the blockchain to ensure the data's authenticity and reliability [68]. Lastly, users can access and monitor their EV data using dedicated applications that utilize cryptographic identifiers to ensure transparency and control of their data [69].

4) Challenges and Takeaways: The security weaknesses within the EV infrastructure are of utmost importance. Striking a balance between personalized services and respecting privacy requires selective data sharing and minimization strategies. With its transparency and immutability, blockchain technology proves valuable for secure record-keeping and decentralized transactions. Nonetheless, achieving both user control over data and compliance with regulations is a complex task. It is crucial to find this equilibrium and tackle vulnerabilities to establish a resilient, privacy-centric EV ecosystem that seamlessly incorporates blockchain solutions.

C. Financial Technology

1) Overview and Benefits: In the dynamic landscape of modern economies, Financial Technology (FinTech) is a testament to the fusion of finance and cutting-edge technology [70]. FinTech systems have revolutionized the way financial transactions are conducted, ushering in an era of efficiency, security, and accessibility [71]. These systems enable seamless fund transfers, fostering economic activity and enhancing financial inclusion. They gather and process extensive data, including transaction histories, account details, credit scores, and broader financial behaviors, offering valuable insights into fiscal patterns and consumer trends [72].

Blockchain-based transactions are significantly cheaper, faster, and more secure than traditional credit card transactions. Traditional credit card methods differ significantly from blockchain-based ones in cost, response time, security, and privacy. Several hidden fees are associated with traditional credit card payments, including payment gateway fees, that

can significantly increase the cost to consumers, a factor often hidden from their view [73]. In contrast, blockchain technology can reduce or eliminate these hidden fees by bypassing third-party processors, although it introduces variable crypto-transaction fees based on network activity and blockchain type [73]. In contrast, while credit card transactions process quickly but are delayed by bank settlements, blockchain offers much faster response times, especially since private networks can outpace traditional and even public blockchains in terms of transaction speeds [73]. Decentralization, smart contracts, and consensus mechanisms minimize the risk of breaches associated with traditional credit cards, which are vulnerable to fraud and identity theft due to their reliance on centralized data storage [74]. Likewise, centralized storage of sensitive information in credit card transactions compromises privacy, mitigated by blockchain's ability to anonymize and encrypt user data, making transactions safer and more efficient [75].

2) Challenges: Despite the advancements, FinTech faces significant challenges, particularly in safeguarding data and ensuring transactional integrity [76]. The vast amounts of sensitive financial data managed by these systems are attractive targets for cyber threats [77]. Moreover, the need for quick and efficient transactions often has to be balanced against stringent security measures, creating a complex environment that demands innovative solutions [78].

3) Blockchain in FinTech: Blockchain technology emerges as a game-changer in FinTech [79]. By design, blockchain offers a decentralized platform that is secure, transparent, and immutable – ideal for handling sensitive financial transactions [79], [80]. Each transaction on the blockchain is recorded in a tamper-proof ledger, providing unparalleled security and reducing the risk of fraud and data breaches [76]. The decentralized aspect of blockchain aligns perfectly with the ethos of FinTech, removing the need for intermediaries and enabling direct peer-to-peer transactions [72]. This not only streamlines processes but also reduces transaction costs, enhancing the overall efficiency of financial services [81], [82].

The sensitive nature of FinTech applications brings about the need for additional metrics, including transaction throughput and latency, to evaluate the efficacy of these privacy measures. Threat modeling becomes crucial to pinpoint potential privacy risks to financial transactions, such as network breaches, malicious actors, and financial data leaks [81], [83], [84], [85], [86]. Consensus algorithms are required to assure transaction reliability while prioritizing privacy, integrating the previously mentioned methods into blockchain architecture [87], [78].

Financial security and privacy preservation is a complex endeavor involving multiple entities, as illustrated in Figure 3. The process commences when individuals use digital wallets to initiate transactions. These wallets store cryptographic keys and authorize payment transfers [88]. Once initiated, these transactions are broadcast to the network for processing. Payment processors, including miners, compete to validate and add these transactions to the blockchain, ensuring their immutability and integrity. Banks sometimes play an intermediary role, providing custodial solutions or facilitating fiat currency conversions. Concurrently, merchants receive payments

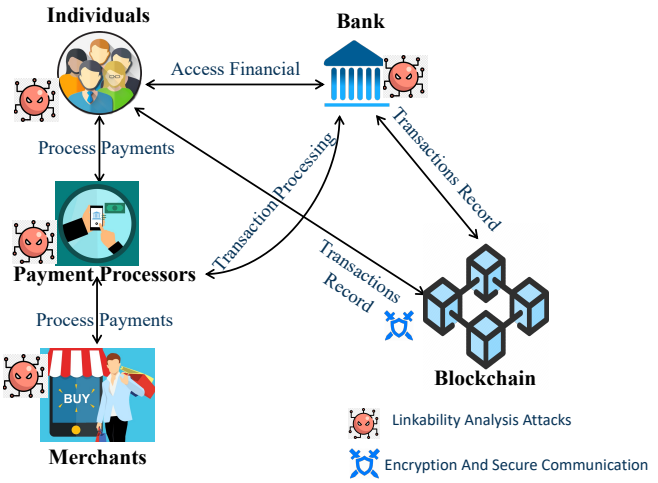

Fig. 3. Illustration of how incorporating a Financial Transaction on the Blockchain system with encryption and secure communication can enhance security and privacy.

for their goods or services [89], [90]. The process is fortified with encryption techniques and communication protocols to ensure transaction confidentiality and tamper resistance. With these safeguards in place, the blockchain system can robustly maintain the privacy and security of transactions. It effectively protects sensitive information's confidentiality while upholding the network's overarching integrity [87], [78].

4) Challenges and Takeaways: Advanced cryptographic techniques, such as ZKP, guarantee secure transactions and protect data privacy. However, reconciling anonymity with financial transparency aspects, such as Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations, poses a significant challenge. Moreover, the scalability hinges on inventive consensus mechanisms. The integration of conventional finance with privacy-centric DeFi necessitates careful deployment of encryption algorithms and practices. Achieving success in blockchain finance requires a delicate equilibrium, balancing user anonymity, regulatory adherence, and auditability to cultivate a secure and reliable financial ecosystem.

Givargizov [91] found that unstable financial and economic factors heavily influence the development of blockchain technologies globally. They suggest that there is an increased interest in blockchain technology as a secure and decentralized alternative for financial transactions during economic volatility. However, the fluctuating values of cryptocurrencies pose significant challenges to their adoption in the FinTech industry. Issues such as investment stability, regulatory acceptance, and integration with existing systems are significant obstacles that must be addressed to facilitate the broader adoption of blockchain-based cryptocurrencies in the financial sector.

D. Supply Chain

1) Overview and benefits: Another promising application space of blockchain systems is the supply chain, complex systems that deal with streamlining the process of converting raw materials to products and distributing them. Managing a supply chain involves many entities, as shown at a high level

in Figure 4, such as suppliers, manufacturers, distributors, and retailers, and this management process can be extremely complex due to the separate operation of the different entities with conflicting interests and incentives, precluding trust among them. Once digitized and streamlined, this very complexity of the supply chain system serves as the most prominent benefit, resulting in cutting costs.

2) Challenges: Traditional supply chains struggle with transparency issues, resulting in inefficiencies and increased costs, calling for digitization. Moreover, supply changes are essential and are often exposed to cyber attacks, hindering their utility. The interoperability in supply chains is yet another challenge that affects its sustainability in communicating orders, the associated forecast of demands, and fulfilling them. Because supply chains, and by their basic nature, rely on the interaction between various entities, there is a need to facilitate trustworthy and secure communication between them. Another challenge with supply challenges is their scale, where a digital system is required to accommodate a large number of transactions coming from different entities with potentially conflicting interests.

3) Blockchain in Supply Chains: Blockchain lends itself as a possible solution to this problem [92]. For instance, blockchain can help those entities to work together by providing an integrity fabric for interactions, thus enabling trustworthy and secure interactions. On the other hand, using blockchain for supply chains could lead to privacy concerns. Because all artifacts associated with the interactions between the different entities in the supply chain are visible on the blockchain, it is hard to prevent mining such data for insight that might leak privacy [76]. Thus, there is an obvious need to design blockchain primitives for the supply chain, enabling trustworthy and secure interactions while enabling privacy. In other words, such primitives would balance privacy with the guaranteed transparency of the blockchains [93].

Blockchain technology addresses these issues by providing a decentralized and transparent platform that offers real-time access to information about goods, transactions, and contracts for all participants [94], [93]. While this enhances efficiency and trust, the transparency of blockchain technology poses a significant challenge to supply chain privacy [92]. Storing transactions on the blockchain exposes sensitive data, including supplier-customer identities, pricing, and product details, to all participants, even those not directly involved in the transaction [87]. The immutability of blockchain data ensures transparency but complicates protecting sensitive information, which is a barrier to potential adopters [95], [96].

Ensuring privacy in the supply chain within the blockchain system requires a comprehensive approach to address various concerns, particularly those related to the potential of malicious insider attacks, as highlighted in Figure 4. The supply chain network consists of several stakeholders, including suppliers and consumers, each with specific roles and access permissions within the blockchain system. Implementing Role-Based Access Control (RBAC) allows access privileges based on predefined roles, ensuring that only authorized individuals can access specific data [97]. In this way, suppliers provide the necessary information about their products while consumers

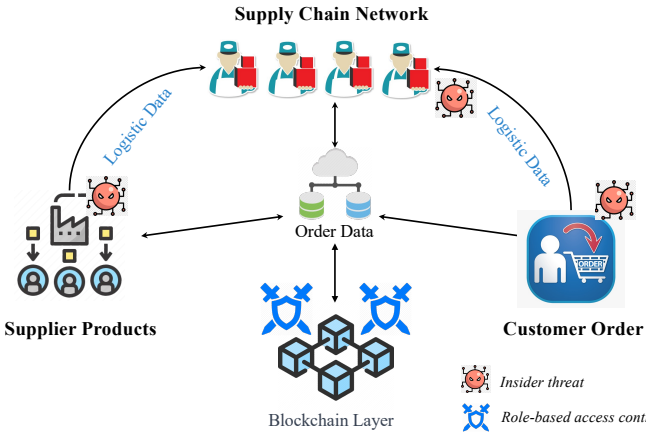

Fig. 4. A system view of the supply chain and the role of blockchains and role-based access control in ensuring security and privacy.

receive and utilize them. RBAC helps mitigate the risk of malicious insiders accessing or manipulating sensitive data, as access controls are tailored to each entity's role and responsibilities [98]. By implementing RBAC in the supply chain on the Blockchain system, privacy concerns can be addressed, reducing the potential impact of malicious insider attacks and enhancing data security [95], [96].

4) Challenges and Takeaways: The unintentional disclosure of sensitive information may result from immutable records, while the pursuit of transparency could potentially expose proprietary business data. Effective approaches to addressing this issue involve pseudonymization to safeguard sensitive data without compromising its usefulness and the implementation of robust access controls to limit data access to authorized entities. ZKPs provide a means to access and authenticate information without divulging the actual data, ensuring both privacy and data integrity. Adherence to data protection regulations is crucial, emphasizing encryption and other security measures. Controlled information disclosure and collaborative efforts with stakeholders ensure a balanced approach. To establish a secure and privacy-conscious blockchain supply chain system, it is imperative to prioritize privacy-enhancing techniques, technical compliance, and regulated data sharing.

E. Healthcare Systems

1) Overview and Benefits: The healthcare industry is undergoing a digital transformation. Healthcare is pivotal in promoting the well-being of individuals and communities by offering essential medical services, endorsing disease prevention and management, and driving medical research and innovation. Technological advancements in healthcare have enhanced diagnostics, treatment, and patient care, leading to improved health outcomes [99]. The healthcare system involves various stakeholders, such as patients, healthcare providers, insurers, and pharmaceutical companies, working in unison to ensure efficient healthcare delivery [100], [101].

2) Challenges: The digitization of healthcare, while advantageous, introduces numerous challenges. A notable issue

is the lack of interoperability between healthcare providers and systems, causing fragmented health records. This fragmentation can result in diagnostic delays and ineffective treatments. Data breaches and security threats pose a significant risk, potentially compromising patient privacy and data integrity [102], [101]. Administrative inefficiencies, such as complex billing procedures and redundant paperwork, amplify healthcare costs and operational challenges. A prevalent lack of transparency and trust among stakeholders curtails collaboration and impedes accurate assessment of healthcare outcomes. Additionally, healthcare systems' inherent complexity and fragmentation act as barriers to accessing timely care, especially for underserved groups [103], [104]. Addressing these challenges is crucial for elevating the quality and efficacy of the healthcare system. One potential solution is the incorporation of blockchain technology [105].

3) Blockchains in Healthcare Systems: Blockchain technology, characterized by decentralization, transparency, immutability, and security, promises to reshape healthcare data management and service delivery radically. It offers a secure platform for storing and managing healthcare data, with each transaction cryptographically linked and added to a series of blocks, ensuring data authenticity and accuracy [97], [41]. Advanced encryption techniques, such as ZKP and HE, can be deployed to protect patient data while allowing data sharing among authorized stakeholders, preserving privacy and compliance [101]. Blockchain minimizes data breaches and unauthorized access by decentralizing data and introducing stringent access controls. Its decentralized nature enhances interoperability across healthcare systems [106]. Smart contracts automate data exchanges, streamline workflows, minimize paperwork, and ensure data accuracy across the healthcare landscape [107]. Such robust interoperability provides healthcare professionals with comprehensive patient records, resulting in informed decisions and personalized care [108].

Blockchain can automate claim processing through smart contracts, ensuring swift and precise reimbursements, mitigating administrative errors, and reducing costs. The transparency and accountability of blockchains augment operational efficiency and deter fraudulent activities by various entities. By fostering transparency and immutability, blockchain fortifies trust among all healthcare stakeholders, encouraging secure data sharing and fostering research collaborations [108]. The blockchain's consensus mechanisms guarantee data reliability, promoting trust in clinical trials and research. Furthermore, its decentralized approach removes intermediaries, promoting direct interactions among all stakeholders and enhancing transparency and trust [3], [106].

By offering a secure data storage and sharing, blockchain can improve healthcare access for marginalized communities. Transferring medical records to new providers is easier, redundant tests are eliminated, and care coordination is better [109]. Further, blockchain solutions can improve telemedicine and remote healthcare services, providing quality healthcare to those living in remote areas. Blockchain's application to healthcare is an ideal solution to several enduring challenges in healthcare delivery and accessibility. [110], [111].

Figure 5 illustrates a healthcare system that employs

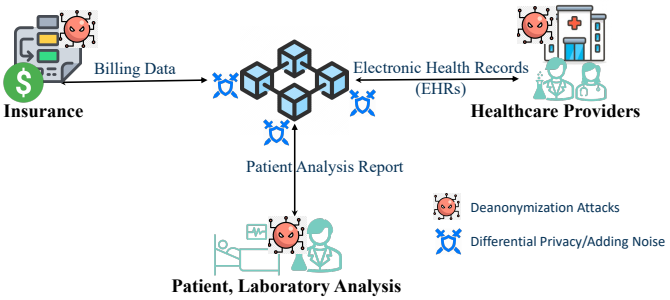

Fig. 5. Representation of a blockchain-based healthcare system with differential privacy and noise addition to improving security and privacy.

blockchain technology to ensure the safety and security of patient data. However, concerns persist about deanonymization attacks, where unauthorized parties aim to reveal personal identities using health records [101]. These attacks can compromise patient privacy, allow unauthorized access, or even lead to discrimination. To combat these threats, the healthcare system has incorporated differential privacy, which is a method that introduces controlled noise to data [110]. This adjustment makes it difficult to associate specific records with individuals yet allows for meaningful aggregated data analysis [112].

4) Challenges and Takeaways: Incorporating blockchain technology into healthcare regulations presents considerable challenges, especially when dealing with patient-centric identity and ethical considerations. Adopting patient-centric identity solutions can reduce vulnerabilities and enhance patient empowerment. Resolving ethical issues requires interdisciplinary collaboration, and educating healthcare professionals about the benefits and potential risks of blockchain is essential for informed adoption. The ongoing research and development are critical for navigating these complex challenges as advancements in the field continue. Ultimately, the successful integration of technological innovations and ethical considerations is essential to establish a secure and privacy-conscious healthcare ecosystem powered by blockchain technology.

F. Auctions

1) Overview and Benefits: The auction system has long served as a pivotal tool for individuals and businesses to engage in the buying and selling of goods and services. By analyzing auction data, entities can glean insights that guide informed decisions [80]. This data equips businesses with knowledge of market trends, consumer preferences, and pricing dynamics, enabling them to refine their offerings and strategies. For individuals, the auction system offers access to a vast array of products and services, allowing them to make purchasing decisions informed by real-time market insights [79]. The system champions transparency, fair competition, and price discovery, benefiting buyers and sellers in diverse industries. It's a flexible mechanism for efficient trade, spanning sectors like art, real estate, collectibles, commodities, and online marketplaces [79], [113].

2) Challenges: The auction system has many security challenges. The bidding process can occasionally seem obscure,

leading to skepticism among participants. Such opacity can spur concerns about fairness, potentially undermining trust in the outcomes. Limited access to auctions, whether due to geographic constraints or industry, can stymie participation, curtailing market liquidity and opportunities [113]. Intermediaries and centralized platforms might influence the auction process, bringing additional costs, delays, and susceptibility to fraud or manipulation [80]. The administrative burden stemming from manual paperwork can bog down the process, rendering transactions more cumbersome. Recognizing and addressing these challenges is vital for the continued viability and effectiveness of auctions [114], [115].

3) Blockchains in Auctions: Blockchain technology is poised to significantly enhance auction systems with its efficiency, security, and inclusivity promises. Blockchain's inherent traits, namely decentralization, transparency, immutability, and intelligent contracts, offer robust solutions to existing auction challenges. Leveraging this technology promises a smoother, more trustworthy auction process, benefiting all stakeholders [115], [113]. As depicted in Figure 6, the system adopts advanced privacy-preserving methods to address security and confidentiality issues. To ensure bidder privacy, a method is used that allows participants to submit their bids in an encrypted form. This encryption secures the bid details, protecting the bidder's privacy.

Blockchain's transparent ledger provides a fail-safe method for documenting auction transactions. Each transaction, bid, or offer is immutably recorded, ensuring a verifiable, integral process for participants. The decentralized facet of blockchain moots intermediaries, curtailing the risks they bring [113]. Smart contracts, self-executing contracts on the blockchain, guarantee adherence to auction rules, fostering trust [76], [79]. Additionally, blockchain's global reach dismantles geographical limitations, amplifying market liquidity. Decentralized platforms allow anyone, anywhere, to join auctions, broadening the prospective audience [76], [79]. This inclusivity nurtures competition, potentially aligning prices with actual market value. Blockchain's ability to automate tasks cuts down on paperwork. Smart contracts automate bid verifications, acceptances, and settlements, eschewing manual oversight [113].

Blockchain's inherent transparency ensures access to pertinent information, streamlining auction management. Its decentralized model trims costs and hikes efficiency, sidelining intermediaries [79]. All auction details, from bid histories to transaction logs, are securely ensconced on the blockchain, offering an auditable event sequence. This elevates the auction process's integrity and curtails risks, given blockchain's impenetrable security measures [80], [76].

4) Challenges and Takeaways: Smart contracts, given their inherent public visibility, carry the risk of unauthorized exposure of confidential bid information. Therefore, it is crucial to develop mechanisms that conceal bidding details while ensuring fairness and transparency in auctions. Balancing transparency and privacy presents a challenge, requiring careful considerations on which data to place on-chain and which to keep off-chain [116]. To protect privacy in auctions, implementing strict access controls, encrypting sensitive information, and adopting decentralized identity solutions prove beneficial. Regular audits of smart contracts and nodes can help identify potential vulnerabilities. The industry can also promote privacy-preserving techniques and uphold best practices through collaborative efforts.

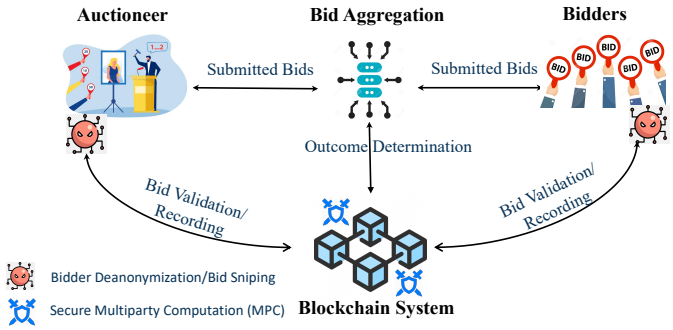

Fig. 6. A system view of the Auctions and multi-party computing.

Blockchain technology has the potential to significantly impact the auction process and its effectiveness, especially in real-world auctions where bidders adjust their bidding price and strategy based on prior bidding events. By incorporating many transactions into a single block for certification, blockchain can influence auctions in terms of transparency and trust. The inherent transparency of blockchain ensures that all bidding transactions within a block are visible and verifiable by all participants. This could lead to increased trust among bidders, as they can be certain that no hidden manipulations occur during the auction process [117].

G. Electronic Voting Systems

1) Overview and Benefits: Electronic voting systems have revolutionized the democratic process, offering a highly efficient method for casting and analyzing ballots. These systems gather valuable demographic data about voters, including age, gender, and location, facilitating the understanding of voting trends and candidate popularity. Additionally, electronic voting provides insights into voter turnout, a critical metric for comprehending voter behavior over time [118]. Stakeholders use this data to make informed decisions. Electronic voting advantages encompass enhanced accessibility, convenience, and efficiency, enabling remote voting, accurate vote counting, and swift election results. The process is safeguarded by advanced encryption techniques, ensuring the confidentiality and integrity of the entire process. Furthermore, the collected data serves businesses and organizations interested in analyzing voting demographics and patterns [119], [120].

2) Challenges: Electronic voting systems, despite their transformative potential, face several challenges. There are legitimate concerns about their vulnerability to hacking and manipulation due to their reliance on internet connectivity [121]. Ensuring the uniqueness and accurate authentication of voter identities presents a significant hurdle, potentially leading to fraud or the exclusion of valid voters. Moreover, the limited transparency and auditability of current systems raise substantial trust issues [122].

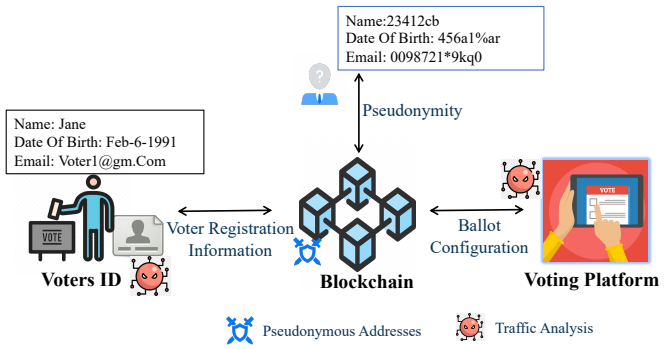

Fig. 7. illustration incorporating blockchain technology and pseudonymous addresses in E-voting to enhance security and privacy

3) Blockchains in Electronic Voting Systems: Blockchain technology emerges as a potential solution to enhance the security and reliability of electronic voting systems. It provides a tamper-proof, auditable ledger, improving voting security, transparency, and privacy. Each vote is recorded as a unique transaction, resistant to interference. The decentralized nature of blockchain, free from central authority, strengthens trust. Cryptographic techniques secure voter identities and choices, while smart contracts automate vote verification and counting, eliminating human errors [120], [118]

The Voting-based blockchain schemes leverage blockchain technology to enhance the security and efficiency of voting processes [123]. Traditional paper ballots face challenges related to storage and verification, while electronic systems, though efficient, rely on potentially untrustworthy centralized entities [121]. In contrast, blockchain-based systems address trust concerns with their distributed ledgers. These systems offer enhanced security compared to conventional electronic voting platforms and have been proposed to address concerns related to voter anonymity and voting process transparency [121]. Secure voting focuses on safeguarding against malicious intent, and decentralized voting ensures no central authority controls the voting mechanism.

Electronic voting in the blockchain is a system that leverages the transparency and immutability of blockchain technology to facilitate secure and trustworthy voting processes, as illustrated in Figure 7. In the voting process, voters are assigned pseudonymous addresses designed to protect their identities. Each voter is given a unique voter ID, which is linked to their pseudonymous address. The blockchain-based voting platform provides a secure and anonymous way for voters to vote [121]. However, it is worth noting that traffic analysis can potentially threaten the privacy of electronic voting. Analyzing the flow and patterns of transactions on the blockchain makes it possible to glean information about individual voters' voting behavior. Protective measures such as mixing services, ZKP, or cryptographic techniques can be employed to combat this issue [118]. These measures safeguard the transaction trail and prevent the correlation of pseudonymous addresses with voter identities. By implementing these protective measures, electronic voting in the blockchain arena can maintain voters' privacy while simultaneously promoting transparency and integrity in the voting process [118].

4) Challenges and Takeaways: Blockchain technology introduces the challenge of transparency with voter anonymity. The transparency feature of blockchain allows all participants to observe transactions, posing a potential risk to voter confidentiality. Deploying robust identity management solutions becomes crucial to preventing unauthorized access to voter data and addressing this issue. It is also essential to safeguard against data leakage through blockchain metadata, which could inadvertently expose sensitive voter details. Managing this risk can be achieved through encryption and selective disclosure methods. However, the immutability of blockchain, where data cannot be modified once recorded, complicates correcting errors or deleting data, potentially jeopardizing voter privacy. Therefore, creating mechanisms for error rectification that uphold the integrity of the blockchain requires careful planning.

Blockchain technology is an emerging solution for major electronic voting system challenges. These challenges include securing and guaranteeing the one-to-one mapping between a voter's physical and digital identification while ensuring verifiability and anonymity. To enhance privacy and anonymity in e-voting, Neziri [124] proposals suggest using blockchain for key management and storing anonymous votes on a separate blockchain. The system works by salting encrypted votes with a nonce, hashing them, and signing them with the voter's private key. By mixing the timestamp of votes and shuffling the order of cast votes, the system reduces the chances of linking votes to voters, assuring voter anonymity and privacy.

H. Energy Trading

1) Overview and Benefits: Energy trading involves the exchange of energy commodities to balance supply and demand. It offers significant benefits, with data related to energy production and consumer information serving to optimize energy generation and enhance customer experiences [125].

2) Challenges: The current energy trading system faces challenges such as inefficiency, limited accessibility, high transaction costs, and security and privacy risks with integrity violations, impacting overall acceptability [57], [92]

3) Blockchains in Energy Trading: Blockchain technology emerges as a solution. Moreover, blockchain provides a decentralized ledger for secure, real-time recording and authentication of energy trades, reducing transaction costs and promoting P2P trading [126], [127]. Moreover, it enhances transparency, instills trust, and eliminates intermediaries, streamlining the trading process by automating smart contracts [123], [125]. Moreover, blockchain technology has the potential to revolutionize the energy trading sector by addressing inefficiencies, enhancing transparency, reducing transaction costs, and promoting inclusive P2P trading [57], [128]

Energy trading blockchain unleashes the power of smart contracts to govern transactions between various players in the energy industry, including renewable energy generators, fossil fuel power generators, suppliers/retailers, and end users, as shown in Figure 8. Renewable energy generators produce clean energy, recorded and validated on the blockchain, while fossil fuel power generators contribute traditional energy sources

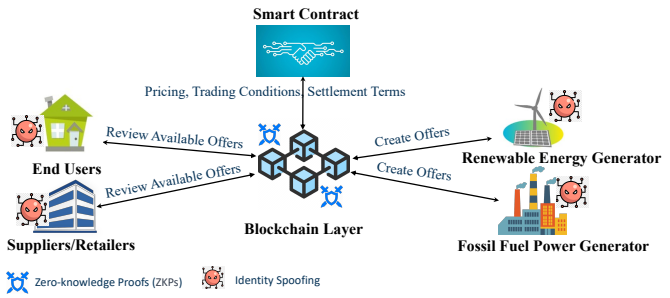

Fig. 8. A system view of energy trading and the role of blockchains and ZKPs in ensuring security and privacy.

for a diverse mix. Suppliers/retailers buy and sell energy commodities, and end users consume the energy.

The technology behind blockchain ensures transaction integrity and transparency, thereby reducing costs and enhancing efficiency by eliminating intermediaries. In addition, we use ZKPs to enhance security and privacy by validating transactions without revealing sensitive information. This enables secure data sharing while preserving privacy and the confidentiality of proprietary information [125], [126], [57], [128].

4) Challenges and Takeaways: The influence of blockchain on privacy in energy trading is multifaceted. While it enhances transparency and confidence, there is a potential risk of divulging proprietary information. However, solutions such as permissioned blockchains can alleviate this concern by restricting data access. P2P energy trading introduces additional complexities, as it may inadvertently reveal user consumption patterns. Therefore, ensuring participant anonymity while adhering to regulations is crucial. The future of blockchain in energy trading is expected to be shaped by advancements in data anonymization and consensus mechanisms, striking a balance between privacy and the benefits of the technology. To fully realize the potential of blockchain and safeguard sensitive information in this space, it is essential to incorporate privacy-enhancing features into the underlying blockchain protocols.

IV. Security and Privacy Techniques

Blockchains ensure the security and privacy in the applications we reviewed in section III through a range of techniques, including decentralization (§IV-A), anonymity techniques (§IV-B), permissions and access control (§IV-C), ZKP (§IV-F), differential privacy (DP) techniques (§IV-G), MPC (§IV-H), digital signatures (§IV-I), homographic encryption of HE (§IV-J), pseudonyms (§IV-D), confidentiality measures (§IV-K), stealth addresses (§IV-L), federated learning or FL (§IV-E), trusted execution environments or TEE (§IV-M), and specialized integrity data structures, such Merkle trees (§IV-N), which we review in the following.

A. Decentralization

In the context of distributed systems, decentralization means that the power and decision-making are distributed among various entities rather than being held by a single authority [132], [135]. While there is no exact mathematical definition for decentralization, quantitative measures, such as the Gini coefficient, can be used to assess the level of decentralization in a system. These measures consider how nodes, computing power, or control are distributed throughout a network [129].

TABLE I
A comparison of different representative works use of the notion of decentralization across various techniques used for enabling it.

Author	Ref.	Year	P2P	Crypto	DLT	PoS	PBFT	PoW	PoC	PoA
Chang *et al.*	[129]	2020	●					●		
Qu *et al.*	[130]	2020			●			●		
Shao *et al.*	[95]	2020	●	●	●				●	
Ferrari *et al.*	[1]	2020			●			●		
Jiang *et al.*	[126]	2020	●	●	●			●		
Xu *et al.*	[90]	2021	●	●						●
Lin *et al.*	[76]	2021	●	●	●			●		
Xiao *et al.*	[82]	2021	●					●		
Crain *et al.*	[131]	2021	●				●			
Const. *et al.*	[113]	2021		●	●				●	
Liu *et al.*	[132]	2022	●	●	●	●		●		
Wan *et al.*	[133]	2022	●	●	●			●		
Malik *et al.*	[92]	2022	●	●					●	
Qu *et al.*	[112]	2022	●	●		●				
Jayabalan *et al.*	[134]	2022	●	●	●			●		
Huang *et al.*	[121]	2022	●	●	●			●		
Xu *et al.*	[135]	2023	●	●	●		●			

1) Benefits of Decentralization: Distributed systems often require decentralization due to trust issues and the challenges related to relying on centralized intermediaries. For example, in EV applications, centralization can lead to concerns about data manipulation and limited transparency [133]. Centralized systems in FinTech are vulnerable to hacks, fraud, and censorship [132]. Supply chain systems face issues of accountability and transparency, which decentralized ledger systems can address [92]. In healthcare, centralized control of patient data and limited interoperability obstruct secure and efficient data sharing [112]. Decentralization can help overcome these challenges by distributing control and fostering transparency, security, and trust.

Blockchain is inherently decentralized, distributing computing power and storage across a network of nodes rather than relying on a central authority or server [132]. This structure enhances the network's resistance to attacks, as there is no singular point of vulnerability [130]. In decentralized blockchain systems, a network of nodes maintains a copy of the ledger. Transactions are added to the blockchain after undergoing a consensus mechanism where nodes validate the transaction's authenticity [135]. However, the integrity of decentralization and privacy can be undermined by specific attacks, like the *51% attack*, where a group controlling most of the network's power attempts to manipulate the ledger [90], [76].

2) Technical Challenges: Decentralization stimulates various issues and technical concerns, mainly in understanding and bounding the nodes' intent and the inherent latency issues associated with the distribution of decision-making.

❶ **Access by Fake Nodes.** One of the main issues with decentralization is the intent of nodes, which is addressed in several works by safeguarding against fake nodes (e.g., Sybil [136], [137], [138]) in applications such as healthcare systems [77]. Without losing generality, multi-factor and mutual authentication mechanisms are employed in such systems

to limit access of fake nodes to the open network system. Such mechanisms may include (pre-registered) authentication modalities such as password biometric factors, e.g., fingerprint, facial authentication modalities, etc. Such additional authentication factors enhance security and prevent fake node attacks from propagating their malice in the decentralized system [90].

❷ **Latency Concerns and Attacks.** In decentralized blockchains, latency is unavoidable and may interfere with the system's guarantees, particularly for applications requiring synchronous network operation [139], [140], [141], [142], [143], [144], [139]. The decentralization of blockchains introduces various attack vectors that can further impede this latency. Crain *et al.* [131] surveyed several of these attacks, including eclipse, DoS, and Sybil attacks [136], [137], all of which exploit blockchains' open and decentralized nature.

Blockchain systems may employ partially synchronous consensus algorithms or other techniques, such as sharding, to address these challenges and reduce latency, realizing close-to-synchronous networks and improving scalability. By leveraging sharding and load balancing, Crain *et al.* proposed the Red Belly Blockchain (RBBC) [131], a secure blockchain system with hundreds of geo-distributed consensus nodes. RBBC balances communication load among multiple proposers, thereby achieving scalability and addressing latency issues. Extensive experiments demonstrate that RBBC outperforms traditional leader-based PBFT and HoneyBadgerBFT consensus protocols in terms of latency, throughput, and scalability.

3) Techniques to Ensure Decentralization: Blockchain systems employ various methods to achieve decentralization.

❶ **Distributed Ledgers.** Using a distributed ledger system entails replicating and storing data across numerous network nodes, thereby eliminating the necessity for a central authority [135]. As such, this approach ensures transparency and accessibility for all participants with equal access to the same information. The consensus mechanisms employed by the system, such as PoW and PoS, allow participants to collectively agree on transaction validity and maintain the integrity of the blockchain without relying on a central entity. Such mechanisms enhance security and reliability by preventing unilateral control and promoting stakeholder trust [130], [76].

❷ **P2P Networking.** P2P networking allows for direct communication and information sharing among nodes without the involvement of intermediaries, constituting another mechanism for decentralization. This decentralized approach eliminates the need for centralized control and promotes a more democratized system. To ensure the security of the blockchain, cryptographic techniques are essential and are used alongside P2P networking[76]. Public-key cryptography ensures unique participant identities, while transactions are cryptographically signed to maintain authenticity and integrity [76], [132]. Furthermore, encryption techniques are employed to safeguard sensitive data stored on the blockchain, thereby ensuring privacy in a decentralized fashion [82].

❸**Smart Contracts.** Decentralization can also be facilitated by smart contracts. Smart contracts based on blockchain technology are contractual agreements that are programmatically executed according to predefined rules, without the need for intermediaries [95]. By eliminating the need for centralized authorities to enforce agreements, these contracts enable decentralized and trustless interactions [133].

Other Techniques for Decentralization. While those are the main techniques used for enabling decentralization in blockchain systems, there are also many other approaches that can be used to facilitate decentralized functions. For instance, a distributed ledger system that stores data at different nodes that are not necessarily controlled by the owner of such data would necessitate mechanisms for limiting access to this data in a transparent and consistent way, which makes authentication and authorization important. For instance, Jayabalan and Jeyanthi [134] discuss how blockchain can address the issue of a centralized client-server system in the healthcare industry coupled with access control in the healthcare systems application. The proposed framework incorporates blockchain-based architecture with an inter-planetary file system (IPFS) to store, share, and retrieve EHR securely. Moreover, in their design, hospitals and medical providers utilize strong (and multi-factor) authentication and authorization processes to prevent unauthorized access to patient data. The authenticity of patient data is further ensured using public-key infrastructure with explicit access delegation. In storing data with the security markers in a distributed and decentralized system, the hospital and doctor nodes are kept lightweight and only participate in generating and publishing data and storing only the abbreviated block for reference.

4) Decentralization in Blockchain Applications: Decentralization has proven to be a game-changing concept in most of the applications discussed in section III, particularly in the advancement of EVs and FinTech.

❶ **EVs.** In EVs and energy trading, for instance, decentralization has empowered EV owners to participate in P2P energy sharing [145], [146], effectively bypassing the reliance on centralized utility companies. This strategy has resulted in a more streamlined charging infrastructure and has eased the integration of renewable energy sources [133].

❷ **FinTech.** Similarly, in the domain of FinTech, Decentralized Finance (DeFi) platforms constructed on blockchain technology have ushered in a significant shift by eliminating intermediaries, reducing costs, and promoting financial inclusivity [82]. Introducing decentralization in FinTech has brought forth transparent and censorship-resistant transactions, smart contracts, and decentralized lending and borrowing protocols [1].

❸ **Supply Chain Systems.** Decentralization also manifests significant features in supply chain applications. For instance, supply chain platforms no longer rely on a central authority for information sharing, and stakeholders can securely share information, promoting transparency, traceability, and accountability. This also helps prevent counterfeiting and promotes responsible sourcing [92].

❹ **Healthcare Systems.** In healthcare systems, the decentralization through blockchain systems utilization improves data security, interoperability, and patient privacy. Patients also would have greater control over their health records, which can be securely shared among healthcare providers. This improves care coordination and reduces errors [112].

TABLE II
A COMPARISON OF VARIOUS TECHNIQUES USED TO ENABLE ANONYMITY IN REPRESENTATIVE WORKS.

Author	Ref.	Year	Pseudonymous Addresses	Group Signatures	Ring Signatures	MPC	ZKP	HE	Mixing
Sahai *et al.*	[93]	2020					●		●
Gabay *et al.*	[149]	2020	●				●		
Shi *et al.*	[31]	2020					●		
Jiang *et al.*	[126]	2020					●		
Baranwa*et al.*	[79]	2020				●	●	●	●
Li*et al.*	[150]	2020			●			●	●
Firoozjaei*et al.*	[120]	2020	●		●		●	●	
Liu*et al.*	[151]	2020		●	●				
Xiao *et al.*	[82]	2021							
Simoes *et al.*	[152]	2021							
Avizhe*et al.*	[153]	2021	●		●				
Liu*et al.*	[72]	2021				●		●	
Denis*et al.*	[39]	2021							
Lu*et al.*	[154]	2021	●					●	
Lin*et al.*	[76]	2021		●					
Wan *et al.*	[133]	2022	●		●		●		
Rasheed *et al.*	[38]	2022					●		
Almashaqbeh *et al.*	[155]	2022			●		●		●
Huang *et al.*	[121]	2022	●				●		
Qiao*et al.*	[87]	2022	●	●	●				
Nguyen*et al.*	[119]	2022					●	●	
Hardin*et al.*	[156]	2022	●						

❺ Auctions. Decentralized platforms on the blockchain systems will provide trust and transparency in auctions [147], in particular by eliminating intermediaries and using smart contracts for secure and fair bidding processes [113], [148].

❻ Voting. Voting systems benefit from decentralization by ensuring transparent and auditable elections. P2P energy trading platforms have also seen the benefits of decentralization, enabling direct transactions between producers and consumers, reducing reliance on centralized energy markets, and promoting efficient and transparent energy exchange [121], [126].

Numerous exemplary studies that leverage decentralization, including mechanisms such as P2P, crypto, DLT, PoS, PBFT, PoW, PoC, and PoA are presented in Table I.

B. Anonymity

To address some of the issues mentioned in section III, some blockchain designs allow users to engage in transactions and activities while preserving their anonymity.

1) Benefits of Anonymity: Anonymity empowers individuals to transact and communicate without the apprehension of exposing their personal information. Moreover, anonymity nurtures trust, security, and user empowerment by granting users authority over their privacy [82], [133], [93], [78]. Protecting participants' identities and sensitive data is paramount in a distributed system emphasizing anonymity. Applications like EVs, FinTech, and others mentioned in section III encompass transactions or interactions laden with sensitive details. Privacy becomes indispensable, with threats like identity theft, unauthorized access, and data breaches looming large [101], [106]. Without anonymity, participants in a distributed system can be exposed to various risks. In financial systems, individuals might prefer to keep their financial activities disconnected from their real-world identity [135], [157].

Similarly, patients in healthcare systems would typically want their medical histories to remain confidential. Electronic voting systems necessitate the concealment of voters' ballots to avert intimidation or coercion. Because of the security anonymity provides, individuals can interact within the distributed system with greater confidence [93], [38].

2) Technical Challenges: Applying digital signature schemes in blockchain networks introduces several challenges, especially in balancing the need for anonymity with system integrity and regulatory compliance. Firstly, while anonymity protects users' identities and enhances privacy, it complicates legal compliance and AML efforts. Regulators struggle to trace transactions back to individuals, making it difficult to enforce laws and regulations. This is particularly problematic in sectors like FinTech, where financial transactions must adhere to strict AML [135], [157]. Secondly, the implementation of privacy-enhancing technologies such as mixing services. These technologies require significant computational resources and can lead to scalability issues as the network grows [152], [149]. For instance, mixing services while enhancing anonymity by obscuring the origins of transactions can also increase the time and computational power needed to validate transactions, potentially slowing down the network. Lastly, ensuring the security of digital signature schemes themselves is a challenge. As the backbone of anonymity in blockchain networks, these schemes must be resilient against evolving cryptographic attacks [132]. The strength of cryptographic algorithms today might not be sufficient against future advances in quantum computing, posing a long-term threat to the security of blockchain networks [132], [151].

3) Techniques for Anonymity: Anonymity in distributed systems can be achieved through various mechanisms and techniques, including pseudonyms, mixing services, and other privacy-enhancing technologies.

Pseudonyms. Participants can use pseudonyms or temporary identities during interactions to hide their real identities effectively. Cryptographic keys, particularly public-private key pairs, are commonly used to generate and manage these pseudonyms. By separating real-world identities from system actions, anonymity is maintained [93], [69].

Mixing Services. Mixing services are intermediaries that promote anonymity by obscuring transaction traceability. These services receive inputs from several participants and redistribute the outputs, ensuring transactions are not associated with specific individuals. By blending transactions with others, participants amplify their anonymity, making their actions within the distributed system more difficult to trace. The challenge of tracing transactions back to their originators increases when transactions from different services are combined [152].

Other Techniques. Techniques such as ZKPs and ring signatures further enhance anonymity. ZKPs allow participants to validate a statement or transaction without disclosing additional details [149]. A ring signature lets a user sign a message on behalf of a group without revealing which specific member signed the message. This ensures that interactions

do not divulge personal information. Using ring signatures to sign messages makes determining the actual signer computationally challenging [132], [151]. These technologies protect privacy and enable anonymous transactions in distributed systems, allowing participants to function without revealing their real-world identities, further obscuring transaction traceability [149].

4) Anonymity in Blockchain Applications: Many applications discussed in section III require anonymity.

❶ **EVs.** It is vital to ensure the anonymity of EV owners during charging transactions to protect their identity and location [149]. This anonymity in charging allows owners to engage in activities without exposing their identity or compromising personal security. Such anonymity shields personal information from unauthorized access and upholds the privacy of EV owners [61] while enjoying the benefits of blockchains for integrity, transparency, and authenticity.

❷ **FinTech.** User identity and transaction protection are paramount in the FinTech sector. Individuals can engage in financial activities, like P2P or digital currency exchanges, without revealing their real-world identities [158], [159]. By utilizing techniques like ring signatures, ZKPs, or privacy-enhancing cryptocurrencies, FinTech applications can bolster privacy and anonymity [135].

❸ **Supply Chain.** In supply chains, participant anonymity protects sensitive business information. Suppliers and manufacturers can share insights about production processes, inventories, or pricing without revealing their identities or proprietary secrets. Supply chain systems can employ mechanisms, such as pseudonyms (temporary identities), to ensure secure interactions and uphold privacy [56].

❹ **Healthcare.** For healthcare systems, preserving the anonymity of patient medical records is imperative. Techniques like DP and MPC can guarantee patient anonymity while sharing medical records, research, or telemedicine [160]. This protection encourages individuals to seek medical help without privacy concerns and supports secure collaborations between healthcare providers [31], [6].

❺ **Auctions.** Auction systems must maintain bidder anonymity to thwart collusion, identity theft, or bid manipulation. Techniques such as blind signatures or cryptographic protocols allow participants to bid without exposing their intentions or identities. By fostering trust and ensuring fairness, anonymity retains the competitiveness of the auction process.

❻ **Electronic Voting.** In electronic voting systems, voter anonymity is vital to deter coercion and vote-buying [155]. Systems can ensure votes remain anonymous using cryptographic protocols like mix-nets or HE, allowing accurate vote tallying and result verification. Besides improving election integrity and promoting participation, anonymity reduces risks linked to voter suppression and identity exposure [121].

❼ **IoT.** IoT device communication benefits from anonymity, allowing devices to communicate without exposing their identity or location. This protects their privacy, prevents tracking, and bolsters overall security [120].

❽ **Energy Trading.** In energy trading, anonymity levels the playing field for smaller entities or newcomers against established players. With their vast resources and networks, the latter have inherent advantages in conventional energy markets. Smaller players can compete anonymously without exposing their identities or strategies, avoiding potential bias or retaliation from larger competitors. Shielding identities and trading strategies let them compete based on offerings, fostering an inclusive environment where innovation and competitive pricing can flourish [126], [92].

A wide range of research leveraging anonymity mechanisms, including pseudonymous addresses, group signatures, ring signatures, MPC, ZKP, HE and mixing techniques, is detailed in Table II.

TABLE III
A COMPARISON OF VARIOUS TECHNIQUES USED TO ENABLE PERMISSIONED BLOCKCHAIN DISTRIBUTED SYSTEM.

Author	Ref.	Year	Access Control	Hyperledger	Encryption	PBFT	PoA	PoC	PoS	ZKP	PoQ	Mixing
Bernabe *et al.*	[8]	2019	●	●	●					●		●
Shao *et al.*	[95]	2020	●		●			●		●		
Androu. *et al.*	[161]	2020			●					●		●
Vasyl. *et al.*	[162]	2020	●		●			●				
Lu*et al.*	[163]	2020	●		●						●	
Avizheh *et al.*	[153]	2021	●		●		●					
Krishna. *et al.*	[164]	2021	●		●							
Kong*et al.*	[165]	2021	●		●				●			
Liu*et al.*	[72]	2021	●		●							
Bosri*et al.*	[166]	2021	●		●				●			
Crain*et al.*	[131]	2021			●	●						
Peng*et al.*	[105]	2021	●	●	●					●		
Lin*et al.*	[76]	2021		●	●	●				●		
Chais.*et al.*	[118]	2021	●	●	●							
Malik *et al.*	[92]	2022	●	●	●			●		●		
Garcia *et al.*	[109]	2022		●	●			●				
Liu *et al.*	[167]	2023		●	●					●		

C. Permissioned Blockchain

Permissioned blockchains are a distinct category of blockchain systems that limit access to a select group of trusted participants. These individuals have the authorization to validate transactions and participate in the consensus process [153]. Contrary to public blockchains, where any individual can join the network or engage in mining, permissioned blockchains restrict these activities. While the exact definitions of permissioned blockchains can differ based on their design and the consensus algorithm in use, they typically incorporate cryptographic methods such as digital signatures, public-key cryptography, and consensus protocols to guarantee secure and restricted access to the blockchain network [95], [168].

1) Benefits of Permissions: In numerous distributed systems, including EVs, FinTech, and others highlighted in section III, ensuring controlled access and maintaining trust among participants is imperative. This is particularly essential for applications managing sensitive data and transactions. To uphold this controlled access and trust, entities might adopt a permissioned blockchain system, thereby allowing only recognized and trusted members to engage, validate transactions, and maintain the integrity of the network [8].

2) Technical Challenges: Implementing digital signature schemes in permissioned blockchains can impact the network's scalability and performance. Digital signatures require computational resources for generation, verification, and manage-

ment. As the number of transactions and participants increases, the computational overhead can lead to delays and reduced throughput, especially in networks that prioritize secure transactions over speed [95], [168].

Managing cryptographic keys in a permissioned blockchain is complex. Participants need to store their private keys securely, and the system must efficiently handle key revocation, renewal, and distribution while ensuring that compromised keys do not undermine the network's security. [153].

3) Techniques to Ensure Permissions: Permissioned blockchain operates on distinct methods and components to constitute a distributed system, mostly utilizing access control and identity management systems. For instance, a primary approach involves *restricting network access* to a predetermined set of participants or nodes, typically trusted entities such as specific organizations or individuals with defined roles [95]. *Access control* and *identity management mechanisms* are established to guarantee that only these authorized members can interact with the blockchain [153]. Consensus procedures are utilized to confirm the legitimacy of transactions introduced to the blockchain. In contrast to public blockchains, where anyone can contribute to the consensus—often leading to latency—permissioned blockchains can leverage more streamlined consensus algorithms like PBFT or PoA. These protocols depend on a curated group of trusted nodes to endorse transactions and preserve the network's integrity [167], [169].

4) Applications of Permissioned Blockchains: Several applications benefit from permissioned blockchain technology, including EVs and FinTech, as discussed in Section III. Each of these domains has a unique set of benefits and challenges associated with trust, security, transparency, and efficiency addressed by permissioned blockchains [8].

❶ **EVs.** EVs can benefit from permissioned blockchain technology, offering a secure and transparent transaction framework between EV owners and charging station providers [60]. Every charging event is meticulously recorded and verified on the blockchain, ensuring precision and preventing fraud and unauthorized data access. Furthermore, this technology facilitates collaboration between various entities, optimizing the efficiency and availability of charging services [8].

❷ **FinTech.** In FinTech, permissioned blockchain plays a pivotal role in augmenting the security, privacy, and efficiency of financial transactions [95]. It deploys cryptographic techniques and access control strategies, ensuring only authorized participants can access financial data and process transactions. This mitigates risks associated with fraud, identity theft, and unauthorized access. Moreover, it expedites and reduces the cost of cross-border transactions by bypassing intermediaries and refining the verification and settlement processes [161].

❸ **Supply Chain.** Permissioned blockchain can amplify transparency and traceability in supply chain networks. To guarantee product quality, curtail counterfeiting, and bolster logistical efficiency, stakeholders can record and authenticate the provenance, legitimacy, and movement of goods at every step [92]. This approach enables participants to securely share and access pertinent supply chain data, retaining confidentiality and promoting trust and collaboration [153].

❹ **Healthcare.** Permissioned blockchain offers a secure platform to manage and exchange sensitive patient data. It ensures that only authorized healthcare providers access patient information, safeguarding patient privacy via cryptographic methods and access controls [109]. Furthermore, it enhances diagnostic and treatment accuracy by enabling interoperability and sharing of medical records [164]. The technology also supports clinical research by safeguarding anonymized patient data, facilitating analysis, and advancing medical research [8].

❺ **Auctions.** Permissioned blockchains can elevate transparency, trust, and fairness in auctions. They enable verifying auction-related data, such as bidding history, item specifics, and transaction records, deter fraud and manipulation, and ensure fair play. Additionally, the technology allows for the automated and tamper-proof execution of auction rules [8].

❻ **Electronic Voting.** Voting processes can benefit from permissioned blockchain as well. Once recorded and encrypted on the blockchain, every vote becomes immutable and verifiable. An audit trail manifests a transparent record, validating the election's credibility and preventing vote tampering. This technology also allows citizens to cast votes from any location while preserving their privacy [8].

❼ **Energy Trading.** In energy trading, permissioned blockchain facilitates a decentralized, transparent marketplace, allowing participants to engage in P2P energy trades without intermediaries [153]. This reduces transaction costs, elevates market efficiency, and promotes the use of renewable energy [123]. The technology also supports real-time monitoring of energy production and utilization.

❽ **IoT.** Permissioned blockchain holds substantial promise for the IoT. Beyond bolstering the integrity and confidentiality of IoT data, its distributed design ensures secure data storage validated by multiple participants [163]. The blockchain's consensus mechanism confirms the legitimacy of transactions, instilling trust within the IoT framework. In essence, permissioned blockchain lays the groundwork for secure and private interactions among IoT devices, addressing prevalent concerns about privacy and security [167].

A comprehensive of distinguished research employing permissioned blockchain technologies, which include access control, hyperledger, encryption, PBFT, PoA, PoC, PoS, ZKP, PoQ, and Mixing mechanisms, is itemized in Table III.

D. Pseudonymity

Pseudonyms obscure the true identities of individuals during interactions and transactions on blockchain systems in what is termed pseudonymity [120]. Cryptographic techniques allow users to retain their privacy while engaging in blockchain activities. Each participant in the blockchain network receives a unique pseudonym or public key, serving as their identifier. For instance, Bitcoin addresses, which chronicle Bitcoin transactions, exemplify pseudonymity within the blockchain; pseudonyms link transactions and interactions instead of real-world identities [71]. Although transaction details are public, the true identities associated with these pseudonymous sender and receiver addresses remain obscured [161].

The privacy of blockchain applications remains paramount, with pseudonymity playing a pivotal role. Participants can

TABLE IV
A COMPARISON OF DIFFERENT REPRESENTATIVE WORKS USE OF THE NOTION OF PSEUDONYMITY ACROSS VARIOUS TECHNIQUES USED FOR ENABLING IT.

Author	Ref.	Year	Stealth Addresses	Hierarchical Deterministic	CoinJoin	mixing	Ring Signatures	ZKP
Jiang*et al.*	[126]	2020	●					●
Ferrari*et al.*	[1]	2020				●		
Androulaki*et al.*	[161]	2020				●		
Androulaki*et al.*	[170]	2020				●		
Zaghloul*et al.*	[71]	2020			●			
Li*et al.*	[150]	2020				●	●	
Firoozjaei*et al.*	[120]	2020					●	●
Liu*et al.*	[151]	2020					●	
Sahai*et al.*	[93]	2020				●		●
Gabay*et al.*	[149]	2020						●
Shi*et al.*	[31]	2020						●
Banupriya*et al.*	[88]	2021		●				
Xiao*et al.*	[82]	2021				●		
Simoes*et al.*	[152]	2021				●		
Denis*et al.*	[39]	2021				●		
Avizheh*et al.*	[153]	2021					●	
An*et al.*	[171]	2022	●					
Pan*et al.*	[172]	2022				●		
Almashaqbeh*et al.*	[155]	2022				●	●	●
Qiao*et al.*	[87]	2022					●	
Baranwa*et al.*	[79]	2022				●		●
Wan*et al.*	[133]	2022					●	●
Rasheed*et al.*	[38]	2022						●
Huang*et al.*	[121]	2022						●

undertake transactions and engage on the blockchain without exposing their identities [149]. They allow users to conceal their association with particular transactions or smart contracts, deterring others from correlating their activities to real-world identities, ensuring vital business or personal data stays safeguarded from unauthorized access [173].

Blockchain systems deploy cryptographic primitives like *public-key cryptography* to facilitate pseudonymity. Participants generate private and public keys: public keys function as pseudonyms, while private keys are used for digital signatures [88]. Pseudonymity involves the creation of distinctive pseudonyms or identifiers derived from participants' actual identities, achieved using one-way cryptographic functions [174]. Revering these pseudonyms without the corresponding private keys to uncover the original identities is computationally challenging. Techniques like ZKP, ring signatures, and mixers can further enhance pseudonymity [69], [133]. Employing these cryptographic tools augments anonymity, obfuscating individual transactions or activities [161].

1) Benefits of Pseudonymity: Pseudonymity bolsters the security of blockchain applications, making it more challenging for malevolent actors to steal personal data [120]. Pseudonymity empowers individuals to communicate freely without apprehension of backlash or unsolicited intervention, primarily if they aim to elude monitoring by authorities or other entities [56]. By preventing direct association with specific individuals or firms, pseudonymity in blockchain applications provides discreet transactions, protecting trade secrets and intellectual property. Additionally, it helps ensure compliance with privacy and data protection regulations [133].

2) Technical Challenges: Pseudonymity presents distinctive challenges, blending technological intricacies with privacy concerns. At its core, pseudonymity aims to veil users' identities, yet this concealment is not absolute [120]. The primary challenge lies in the balance between privacy and transparency. Blockchain's inherent openness, designed for verifiability and trust, paradoxically enables sophisticated analysis techniques to unravel pseudonymous veils potentially, exposing transaction patterns and user behaviors [161].

Another hurdle is the permanence of records. Once transactions are recorded, they are immutable, meaning any pseudonym associated with a transaction remains on the ledger indefinitely [69], [133]. While a cornerstone of blockchain security, this immutability complicates pseudonymity by making long-term privacy preservation a daunting task. Over time, accumulated transactions under a single pseudonym can become a trove of data, susceptible to de-anonymization by determined adversaries employing advanced data analysis tools [88]. The intersection of pseudonymity with regulatory compliance also poses a challenge. Regulations requiring identity verification for AML and combating the financing of terrorism (CFT) can conflict with the principles of pseudonymity, necessitating sophisticated solutions that reconcile privacy with legal obligations [69], [133].

3) Techniques to Ensure Pseudonymity: In blockchain applications, pseudonymity is realized through *various mechanisms* and *cryptographic techniques*. Participants use pseudonyms or cryptographic identifiers to transact and communicate on the blockchain without revealing their identities, preserving anonymity. Pseudonymity can be achieved using temporary or one-time addresses, which prevent tracing funds or information back to individuals [171], [97]. For example, privacy-centric blockchain networks like Monero use *one-time addresses* to obscure transaction details, making it challenging to link sender and receiver [161].

4) Pseudonymity in Blockchain Applications: Blockchain applications promote pseudonymity by using mixing services or protocols, such as CoinJoin. CoinJoin blends multiple transactions and participant funds, making tracking arduous and enhancing privacy [82]. By blending funds, participants' pseudonyms become even more obfuscated.

❶ **EVs.** In EVs, vehicle owners' privacy and charging routines are paramount. Blockchain technology enables EV charging stations to document and validate charging actions without divulging personal details [149]. Charging transactions on the blockchain can be authenticated and authorized by assigning each owner a unique pseudonym or cryptographic key, ensuring their privacy and preventing exposure of sensitive information like identity or location [56], [55].

As elaborated by Gabay *et al.* [149], EVs can undergo authentication using zero-knowledge verification methods by trusted entities like Electric Vehicle Service Providers (EVSPs) and charging stations. The EVSP operates as a facilitator, mediating the authentication procedure between charging points and EVs, employing pseudonymity to validate authorized EVs without accessing specific details like charging patterns or location. Charging stations get only anonymized identifica-

TABLE V
A COMPARISON OF DIFFERENT REPRESENTATIVE WORKS USE OF THE NOTION OF FL ACROSS VARIOUS TECHNIQUES USED FOR ENABLING IT.

Author	Ref.	Year	Smart Contract	MPC	HE	DP	Decentralized Data Storage	CNN model	PoQ
Que*t al.*	[130]	2020					●		
Lue*t al.*	[163]	2020				●	●		
Passerate*t al.*	[175]	2020		●	●		●		
Hue*t al.*	[176]	2021		●	●		●		
Miaoe*t al.*	[177]	2022	●		●	●	●		
Baie*t al.*	[178]	2022			●	●	●		
Guoe*t al.*	[179]	2022	●		●		●		
Qine*t al.*	[45]	2022					●		●
Lve*t al.*	[59]	2022				●	●		
Yange*t al.*	[180]	2022	●		●		●		
Jiae*t al.*	[44]	2022				●	●		
Zhaoe*t al.*	[181]	2023	●			●	●		
Alzubie*t al.*	[182]	2023					●	●	

tion codes, precluding any further data exposure. Beyond ensuring decentralized privacy for EVs during recharging, pseudonymity-enhanced blockchains deliver secure operations while preserving user discretion. This application shields EV owners' privacy, streamlining charging processes by restricting access to sensitive data through pseudonyms.

❷ **Healthcare.** EHRs on the blockchain replace personally identifiable information with cryptographic identifiers. For instance, patients can be assigned pseudonyms. Using these pseudonyms, EHR transactions and access logs are chronicled on the blockchain, ensuring data integrity and permanence [162]. Users on blockchain-based social networks can freely express their opinions without fear of consequences, fostering a diverse environment under the cloak of anonymity, preserving their identities [121].

❸ **Energy Trading.** In energy trading, pseudonyms, and pseudonymous addresses are commonly employed to safeguard participants' privacy and commercial interests. These measures ensure secure and transparent transactions without exposing sensitive details such as the identities, transaction history, and specific energy trading activities of participants [125].

Table IV presents a detailed research review exploring pseudonymity using methods like stealth addresses, hierarchical deterministic, CoinJoin, mixing, ring signatures, and ZKP.

E. Federated Learning

Federated Learning (FL), as a pioneering intersection of blockchain technology and distributed machine learning, unfolds a new era of cooperative intelligence [182]. This approach enables participants to refine machine learning models while steadfastly guarding raw data collaboratively, thus addressing the concern of data privacy [163]. The essence of FL lies in its capability to seamlessly integrate with blockchain technology, fostering a secure and decentralized framework for machine learning across various domains, notably healthcare, where it heralds a new dawn for precision in disease prediction without compromising data privacy [182], [163].

1) Benefits of Federated Learning: FL introduces a transformative approach to collaborative machine learning by ensuring robust data privacy and system scalability. The primary benefit of FL, when integrated with blockchain technology, is its unparalleled ability to preserve the privacy of participants' data [182]. FL mitigates potential privacy concerns by enabling collaborative training without sharing raw data, making it especially valuable in sensitive sectors like healthcare. Furthermore, it enhances the scalability of blockchain systems by distributing computational tasks, thereby reducing the load on any single node and improving the efficiency of machine learning across the network [163], [45].

2) Technical Challenges: Despite its numerous advantages, integrating FL with blockchain technology presents several challenges. The complexity of merging distributed machine learning with blockchain's decentralized architecture requires sophisticated technical solutions to ensure efficiency, scalability, and security [179], [163]. Data heterogeneity and quality across distributed nodes pose additional hurdles, potentially impacting the accuracy and reliability of collaborative models [163]. Moreover, the evolving landscape of cybersecurity threats necessitates continuous advancements in cryptographic techniques to protect against novel attacks[181]. Balancing the need for privacy with regulatory compliance also presents a significant challenge, as FL systems must navigate the requirements of various jurisdictions while preserving the anonymity and confidentiality of participants' data [177], [176].

3) Techniques to Ensure Federated Learning: Implementing FL within blockchain systems employs various advanced techniques to ensure data privacy and secure collaborative learning. Optimization algorithms such as stochastic gradient descent (SGD) are utilized to facilitate efficient model training. Meanwhile, cryptographic protocols, including MPC and secure enclaves, are instrumental in safeguarding the privacy of model parameters during aggregation [175]. These techniques, coupled with decentralized data storage and consensus mechanisms, form the backbone of FL, allowing for secure and privacy-preserving collaborative model training across distributed systems [45], [44], [177].

4) Applications of Federated Learning: FL has many applications, leveraging blockchain technology to create a secure and private framework for collaborative intelligence.

❶ **Healthcare.** FL allows secure analysis of patient data for disease prediction without compromising privacy [175], [180].

❷ **Finance.** benefits from improved fraud detection capabilities through collaborative analysis of transaction data [59].

❸ **EVs and IoT.** FL facilitates collaborative model training for autonomous driving, enhancing vehicle safety and decision-making processes. These applications exemplify the versatility and potential of FL to revolutionize various industries by sharing aggregated model updates through blockchain, thus ensuring data privacy and confidentiality [177], [175].

Various representative works utilizing FL measures, including smart contracts, MPC, HE, DP, Decentralized Data Storage, CNN models, and PoQ are shown in Table V.

TABLE VI
A COMPARISON OF DIFFERENT REPRESENTATIVE WORKS USE OF THE NOTION OF ZKP ACROSS VARIOUS TECHNIQUES USED FOR ENABLING IT.

Author	Ref.	Year	Schnorr Protocol	zk-SNARKs	NIZKs	Bulletproofs	MPC	Commitment Scheme	ECC	Boneh Scheme
Gabay *et al.*	[149]	2020		●						
Jiang *et al.*	[126]	2020							●	
Baranwa*et al.*	[79]	2020	●				●			
Xu*et al.*	[158]	2020		●				●		
Wang*et al.*	[173]	2020						●		
Firoozjaei*et al.*	[120]	2020		●						
Shao*et al.*	[95]	2020			●			●		
Baza *et al.*	[57]	2021	●	●						
Ma *et al.*	[96]	2021		●	●	●				●
Consta. *et al.*	[113]	2021		●			●			
Peng *et al.*	[105]	2021				●		●		
Constantinides*et al.*	[113]	2021						●		
Thyagarajan *et al.*	[183]	2021						●		●
Baza*et al.*	[184]	2021						●	●	
Huang *et al.*	[121]	2022								●
Sahai *et al.*	[93]	2022	●	●				●		
Wan *et al.*	[133]	2022		●						
Xu *et al.*	[185]	2022	●	●		●				
Liu *et al.*	[186]	2022		●						
Malik *et al.*	[92]	2022		●		●	●	●		
Almashaqbeh*et al.*	[155]	2022				●	●	●	●	
Nguyen *et al.*	[119]	2022		●				●		
Pan*et al.*	[172]	2022		●				●		

F. Zero-Knowledge Proofs

ZKP protocols are cryptographic protocols that allow the provider to prove to a verifier the truthfulness of a statement without divulging any additional information [149]. Verifying transactions and data integrity without exposing sensitive details is possible with ZKPs in blockchain systems. By providing a mathematical definition of privacy-preserving protocols, one party (the prover) can convince another party (the verifier) that a statement is true while preserving confidentiality [57]. This minimizes the risk of data leaks and misuse. ZKPs employ complex algorithms and cryptographic techniques to ensure security and privacy in a blockchain network. These include computational puzzles, public-key cryptography, cryptographic hash functions, and non-interactive proofs [96].

1) Benefits of ZKPs: In a distributed system, where multiple entities collaborate while sharing data and performing computations, ZKPs play a crucial role in safeguarding sensitive information and ensuring the integrity of the system [187]. Privacy-preserving transactions are a prominent application of ZKPs in distributed systems. In the context of a distributed ledger and blockchain network, ZKPs can be used to verify transactions without disclosing details [188]. Participants can verify a transaction's validity and keep the sender, recipient, and transaction amount confidential with ZKPs. In a transparent and auditable environment, privacy is preserved [96].

Distributed systems benefit from ZKPs. It allows multiple parties to collaborate on encrypted information while preserving privacy by enabling collaborative analysis and computation without revealing sensitive data [125]. Moreover, ZKPs improve access control and authentication, ensuring secure verification of credentials and group membership [113]. By providing privacy and confidentiality, audits that protect sensitive data are more efficient. By verifying certifications and quality checks without disclosing proprietary information, ZKPs can demonstrate compliance with regulations. [93].

2) Technical Challenges: Despite their potential, ZKPs face significant challenges in blockchain integration. The complexity and computational intensity of ZKPs can lead to scalability issues, as the generation and verification of proofs may demand substantial resources, slowing down transaction processing [189]. Another challenge is the technical barrier to entry; implementing ZKPs requires deep cryptographic expertise, limiting their accessibility to a broader range of developers and applications [95]. Interoperability between different blockchain platforms and ZKP systems also presents a hurdle, as varying implementations and standards can hinder seamless integration. Furthermore, while ZKPs enhance privacy, they must navigate a regulatory landscape that increasingly demands transparency and data access for compliance purposes, posing a potential conflict between the privacy ZKPs offer and regulatory requirements [189]. Lastly, the evolving nature of quantum computing poses a long-term threat to the cryptographic foundations of ZKPs, necessitating ongoing research and adaptation to ensure future-proof security [93].

3) Techniques to Ensure ZKPs: ZKPs encompass a variety of cryptographic techniques, each contributing uniquely to enhancing security and privacy within blockchain technologies.
❶ **Schnorr Protocol.** is a pivotal technique in cryptography, celebrated for its elegance, security, and efficiency. It operates on the discrete logarithm problem, forming the backbone of digital signatures within various cryptographic applications [79]. Unlike other signature schemes, the Schnorr Protocol is lauded for its simplicity and the reduced size of its signatures, which significantly enhances the efficiency of verification processes. This protocol is particularly advantageous in blockchain environments, where it facilitates non-interactive zero-knowledge proofs, allowing for anonymous transactions without compromising scalability [93], [57].
❷ **zk-SNARKs.** stand at the forefront of privacy-preserving cryptographic technologies. zk-SNARKs enable a prover to attest to the truth of a statement without revealing any information beyond the validity of the statement [149]. zk-SNARKs is instrumental in creating secure, private transactions on blockchain platforms, as it eliminates the need to disclose sensitive information while verifying transactions. The succinct nature of zk-SNARKs ensures that proofs are compact and verification times are minimal, addressing critical scalability and privacy concerns in blockchain ecosystems [96], [158].
❹ **Bulletproofs.** represent a significant advancement in ZKPs, offering a non-interactive zero-knowledge proof mechanism without needing a trusted setup [96], [105]. This attribute makes bulletproofs particularly appealing for blockchain applications, as it circumvents the security vulnerabilities associated with a trusted setup. Moreover, bulletproofs are characterized by their scalability and efficiency, facilitating the creation of shorter proofs and faster verification [92].

4) ZKPs in Blockchain Applications: The main issue in distributed systems that call for ZKPs is ensuring the privacy and confidentiality of sensitive data exchanged within applications, such as EVs, FinTech, and others discussed in section III.

❶ **EVs.** ZKPs can address concerns related to sharing energy consumption data while preserving the privacy of individual users [149]. ZKPs can enhance transaction security by allowing verification of the validity of financial claims without revealing transaction details [187]. In EVs, ZKPs can ensure privacy while verifying transaction integrity. It is also possible for EV owners to demonstrate that they have sufficient funds to charge their vehicles without divulging any personal information or balance. Moreover, ZKPs facilitate secure vehicle-to-grid (V2G) communications, ensuring energy transactions are secure, confidential, and tamper-proof [133]. Authentication is vital for ride-sharing services to prevent impersonation attacks and ensure overall security. To achieve this, the driver and rider must authenticate each other in a manner that safeguards sensitive information [65], [172]. One approach, as outlined by *et al.* [184], involves the rider demonstrating knowledge of the private key associated with the public key used for reservation by generating a signature on a randomly selected challenge presented by the driver. The rider then sends the signature to the driver, who verifies it against the public key. This authentication process is conducted in a ZKP manner, meaning the rider does not have to disclose their private key to the driver. This approach ensures the authentication process is secure and reliable for the rider and the driver.

❷ **Supply Chain.** To protect confidential business data and ensure the source of product legitimacy, ZKPs are utilized in the supply chain [96]. Supply chain management uses ZKPs to enhance transparency and traceability while protecting confidentiality. Validating product authenticity and mitigating fraud and unauthorized data access requires this capability [92]. The ZKPs empower supply chain participants to maintain a high degree of trust and uphold the integrity of their operations, thus fostering a more robust and secure environment [109].

❸ **Healthcare Systems.** Medical records and sensitive patient data can be securely shared while maintaining patient privacy and confidentiality with ZKPs in healthcare systems [105]. A ZKP serves both to secure the transfer of data and to protect the privacy of patients simultaneously in healthcare systems. By using this functionality, healthcare providers and researchers can perform computational operations on sensitive patient data without having to physically access the data themselves [107]. In turn, this eases privacy concerns and facilitates interoperability, ultimately advancing healthcare technology.

❹ **Auctions.** ZKPs ensure anonymity for bidders and provide fairness and verifiability [113]. ZKPs are used to ensure that auctions are secure and verifiable. They enable bidders to prove the validity of their bids while safeguarding the exact bid value, preserving their competitive edge. This ensures fairness, mitigates collusion and maintains transparency [113].

❺ **Electronic Voting.** Electronic voting systems use ZKPs to ensure voter privacy, vote integrity, and coercion prevention. Voters can validate their eligibility with ZKPs without disclosing individual candidates, enhancing privacy and security. In addition, they guarantee the verifiability of the final election results [121]. By preserving voter privacy, ZKPs enable verifiable voting in electronic voting systems.

❻ **Energy Trading.** P2P energy transactions can be secure with ZKPs while ensuring participants' energy usage and financial information remain anonymous. With the help of ZKPs, these applications can balance transparency and trust while protecting sensitive data [38]. To this end, ZKPs play a crucial role in energy trading by ensuring the integrity of energy measurement and billing while facilitating secure and private transactions. By utilizing ZKPs, energy producers can prove energy generation data is accurate and genuine without disclosing sensitive information to others. In addition to enhancing trust, this also reduces fraud risks [186].

❼ **FinTech (DeFi).** In DeFi, ZKPs are critical assets [95]. By guaranteeing the verification of ownership and transfers, ZKPs enable confidential and secure transactions [90]. As ZKPs conduct anonymous identity verification, they significantly reduce identity theft vulnerability [155], [95]. In addition, ZKPs ensure the integrity of financial statements during audits and compliance procedures [78].

❽ **IoT.** ZKPs offer valuable features to IoT systems by strengthening privacy and security. ZKPs can be used for authentication, verification of data integrity, and adherence to predefined parameters within the IoT context. In addition to facilitating secure data exchange, ZKPs also allow devices to verify the validity of data without disclosing its actual content, preventing unauthorized tampering and maintaining data integrity. Furthermore, ZKPs prevent data leakage by allowing devices to prove that they possess specific attributes without divulging more information. As a result of secure authentication, data integrity verification, and privacy-preserving interactions, ZKPs enhance privacy and security in IoT systems [188].

For example, Rasheed *et al.* [38] propose a method for protecting privacy in IoT ecosystems using ZKPs and blockchain technology. In addition to anonymous authentication, data integrity, device privacy, and detection of Sybil and IoT server spoofing attacks, the proposed security system incorporates several layers of protection. With the ZKP protocol, IoT devices can remain anonymous through multiple modes, while blockchain technology is designed to ensure data integrity and defend against various attacks. Combining ZKPs and blockchains is an approach to address the privacy and security concerns associated with IoT ecosystems by demonstrating the system's resilience against data modification, data injection, and spoofing attacks [190], [172].

In table VI, a range of research studies employing ZKP techniques, such as the Schnorr protocol, zk-SNARKs, NIZKs, bulletproofs, MPC, ECC and Boneh Scheme are presented.

G. Differential Privacy

The fundamental objective of DP is to enable the sharing of aggregated statistical data from a dataset while simultaneously preserving the privacy of each participant [90]. Introducing random noise to the data makes it increasingly challenging to link specific data points with their respective individuals [178]. Differentiable privacy protects individual transactions or smart contract interactions as sensitive information, such as transaction amounts or contract details, cannot be readily derived from publicly available blockchain information [193].

1) Benefits of DP: DP prevents adversaries from deducing specific information about the data contribution of individual

TABLE VII
A COMPARISON OF VARIOUS TECHNIQUES USED TO ENABLE DP DISTRIBUTED SYSTEM.

Author	Ref.	Year	Noise	Encryption	Randomization	Perturbation	MPC
Han *et al.*	[191]	2020	●		●		
Liu*et al.*	[192]	2020	●	●	●	●	●
Lu*et al.*	[163]	2020	●	●	●		
Gai*et al.*	[36]	2020	●				
Xu *et al.*	[90]	2021	●	●			
Zhao *et al.*	[193]	2021	●		●		
Xu *et al.*	[9]	2021	●	●		●	
Wei *et al.*	[194]	2021	●		●	●	
Zhang *et al.*	[128]	2022	●	●	●		
Liu *et al.*	[186]	2022	●	●	●		
Qu*et al.*	[112]	2022	●		●		
Zhao *et al.*	[181]	2023	●	●	●	●	

individuals by introducing randomization and noise into the data or analysis process [193]. In doing so, it controls how much information an adversary can deduce about an individual from the output of a computation or analysis, regardless of the amount of auxiliary information available to the adversary [44]. By incorporating DP techniques, distributed systems can protect the privacy of sensitive data while enabling useful collaborative data analysis, allowing participants to contribute their data. Having confidence in the privacy protections in place enhances trust and encourages participation [90].

The use of DP techniques enhances the identification management of blockchain systems [191]. DP ensures that the linkage between users' real-world identities and their blockchain addresses remains confidential by applying privacy-preserving mechanisms to user identities, such as noise addition or data perturbation [128], [192]. By doing so, user privacy is protected and identity theft or unauthorized tracking is minimized.

2) Technical Challenges: The concern in distributed systems that calls for DP is the preservation of privacy in a collaborative environment where multiple participants share and process data [90]. Participants contribute their data to a shared platform or network in a distributed system. The traditional privacy protection mechanisms may not be sufficient to address the privacy concerns in such systems [178]. As a primary concern, data inference or linkage attacks pose the potential for privacy breaches, in which adversaries exploit patterns or correlations across multiple data points in order to infer confidential information [193]. An analysis of transaction data in a blockchain network, for example, may reveal patterns or relationships that reveal individuals' identities or confidential information [178]. DP arises as a solution for addressing these privacy concerns in distributed systems [90]. DP is based on a mathematical framework that offers a strong guarantee of privacy. DP ensures that an individual's data contribution remains private even when adversaries possess auxiliary information or are able to perform arbitrary computations [193].

3) Technique to Ensure DP: DP is controlled by a parameter called epsilon (ε), quantifying the system's privacy protection level. Per the randomized response definition, a mechanism is ε-differentially private when the probability of obtaining a specific output result remains consistent, irrespective of whether the input dataset is D or D', the private one, even if the only difference between the two datasets is the data of a single individual. This ensures that the mechanism's output or inference remains unaffected by including or excluding any individual's data in the dataset [193].

4) DP in Blockchain Applications: DP techniques enable privacy-preserving blockchain-based data sharing. Statistical analysis can be performed while protecting individual privacy by adding carefully calibrated noise or perturbations to the data [90], [178]. As a result, even with access to aggregate data, it is difficult to identify specific individuals' data, safeguarding sensitive data in blockchain-based systems [44].

To this end, DP is a highly valuable tool with a diverse range of applications across various domains, including smart contracts in general, EVs, FinTech, and many more. Those applications face a number of challenges, including the need to balance data sharing, analysis, and individual privacy.

❶ **General Smart Contracts.** DP can be applied during smart contract execution to protect the data. As a result of DP techniques, it is possible to obfuscate the inputs and intermediate results of computations within smart contracts, preventing unauthorized access to sensitive data [178]. By doing so, smart contracts on the blockchain can be executed more securely while maintaining the privacy of the parties involved [191]. Various privacy techniques can also enable private and secure blockchain data analytics. Incorporating these mechanisms into data analysis processes can allow for the extraction of statistical insights and trends while maintaining the privacy of individual data points [128], [44].

❷ **EVs.** The protection of data privacy is a crucial concern for EV owners. To address this issue, DP methods can be employed to safeguard charging patterns and location data, thereby enabling researchers and policymakers to obtain valuable insights into EV usage patterns while still preserving the privacy of individual users [128]. Noise addition or data aggregation algorithms can be utilized to ensure the anonymity and privacy of EV owners [194].

❸ **FinTech.** DP is advantageous for financial institutions leveraging blockchains. By employing privacy-preserving techniques such as noise addition or data perturbation, these entities have effectively shielded transaction details stored on the blockchain from exposure [36]. Furthermore, DP has played a pivotal role in risk management and fraud detection by enabling the analysis of transaction patterns while preserving customer privacy [90]. It has facilitated compliance with privacy regulations, ensuring adherence to privacy standards, fostering customer trust, and enabling secure data collaboration while protecting sensitive financial information [36].

❹ **Healthcare Systems.** DP offers a solution by protecting sensitive medical information while enabling analysis and research. EHRs can be aggregated and shared without compromising patient anonymity. Through the use of DP techniques, medical researchers and institutions are able to gain valuable insights from patient data without compromising their privacy [9], [110]. Additionally, in energy trading, DP techniques are employed to protect sensitive information pertaining to energy consumption and trading strategies [135]. This allows market participants to share aggregated data

TABLE VIII
A COMPARISON OF VARIOUS TECHNIQUES USED TO ENABLE MPC IN BLOCKCHAIN DISTRIBUTED SYSTEM.

Author	Ref.	Year	Secret Sharing	HE	Garbled Circuits	Bilinear Pairings	Blivious Transfer	ZKP
Hu*et al.*	[176]	2020	●	●				
Ghosh*et al.*	[5]	2020	●		●			
Liu*et al.*	[72]	2020		●				
Liu*et al.*	[192]	2020	●	●				
Constan.*et al.*	[113]	2021	●	●				
He*et al.*	[77]	2021	●					
Yang*et al.*	[195]	2021	●	●	●	●	●	
Malik*et al.*	[92]	2021	●	●				●
Krishn.*et al.*	[164]	2022						
Yang*et al.*	[196]	2022	●	●	●		●	
Thyaga.*et al.*	[183]	2022	●			●		●
Nguyen*et al.*	[119]	2022	●	●				●
Guan*et al.*	[197]	2022		●				
Song*et al.*	[89]	2022	●	●	●			
Baranwa*et al.*	[79]	2023	●	●				●

while preserving privacy, ensuring protection over confidential information [135], [128].

❺ IoT. IoT systems can greatly benefit from implementing DP. This technique safeguards individual users' data privacy while allowing for meaningful analysis and data sharing [36]. By adding noise or perturbation to data, DP ensures that individual data points cannot be traced back to specific individuals. This privacy-enhancing method enables secure and private data collection from a variety of IoT devices [36]. It also allows for the aggregation and analysis of data while protecting sensitive individual users' information. With DP, the risk of revealing any user's information remains low, and IoT systems can extract valuable insights and perform data-driven tasks while ensuring users' privacy and gaining their trust [9], [193].

Table VII showcases a range of exemplary projects that employ differential privacy techniques, such as noise, encryption, randomization, perturbation, and coupled with MPC.

H. Multi-Party Computation

MPC refers to the computation of private data possessed by multiple participants in a decentralized fashion [198]. MPC enables secure and privacy-preserving calculations within a distributed network. Within MPC, a set of participants, each with unique input, engages in a cryptographic protocol [72]. This allows them to compute a function using their private inputs without revealing them. In essence, if there are parties denoted as $P_1, P_2, \ldots, P_n$ each holding private inputs $x_1, x_2, \ldots, x_n$, the goal is to calculate the function $f(x_1, x_2, \ldots, x_n)$ without exposing individual inputs to other parties. Such a protocol, rooted in cryptography, ensures the privacy of every participant [5], [164]. Typically, these protocols rely on cryptographic primitives like oblivious transfer [199], [200], [201], garbled circuits [202], [203], [204], [205], or HE [195].

1) Benefits of MPC: MPC empowers entities to perform computations collaboratively while ensuring the privacy of their respective inputs. MPC protocols leverage cryptographic techniques such as encryption, secret sharing, and HE to facilitate privacy-preserving computations. These techniques enable participants to engage in intricate functions, e.g., statistical analyses, machine learning, and other privacy-focused algorithms, all while preserving data privacy [164], [206].

Given blockchain technology's decentralized nature, it harmonizes with MPC, enabling participants to retain control over their data while harnessing the computational prowess of the network [72]. Thus, within blockchain systems, MPC not only preserves participant data but also leverages the inherent transparency and immutability features of blockchain [176].

MPC has been instrumental in blockchain systems, playing a role in providing privacy-preserving and secure computation capabilities. By integrating MPC techniques, blockchain networks can enhance privacy and foster collaboration [72].

2) Technical Challenges: The demand for MPC in blockchain systems primarily stems from the challenge of processing sensitive data while upholding its privacy [196]. While blockchain technology is acclaimed for its transparency and immutability, it faces the predicament of securing sensitive data encompassing transaction specifics, account balances, and personal particulars. Traditional computational methodologies centralize data, exacerbating the risk of unauthorized access and potential breaches of confidential information [5].

3) Techniques to Ensure MPC: MPC facilitates confidential transactions. Participants can compute on encrypted inputs without revealing the underlying data. Sensitive transaction details, such as transaction amounts or the identities of senders and recipients, remain private. Confidential transactions maintain user privacy within the blockchain network and support verification and transparency [77]. Also, MPC aids blockchains in the private negotiation of common trust anchors, vital for interoperability across various networks [113].

To address privacy challenges, Bishakh *et al.* [5] propose an MPC-based method. Using MPC, multiple parties can collaborate on a function using private inputs without disclosing them. Among participating blockchain networks, a common trust anchor is computed using MPC. Networks share partial information, safeguarding the complete trust anchor during negotiations. The collaboration ensures the determination of the common trust anchor using secure MPC protocols, preserving the privacy of individual trust anchor details [5]. This strategy bolsters privacy and trust in cross-network interactions.

MPC supports secure data sharing in blockchain networks. Parties can compute using private inputs without revealing actual data. This capability permits sensitive data sharing for data analysis, machine learning, and other computations. By integrating MPC, financial institutions can enhance risk assessment and fraud detection while preserving privacy [113].

MPC is also pivotal in creating privacy-centric consensus mechanisms for blockchains [113]. In traditional consensus algorithms, like PoW and PoS, participants might have to divulge certain information, risking their privacy [72]. Incorporating MPC techniques allows participants to contribute computational power and validate transactions, all while ensuring their privacy [92]. MPC-based protocols also facilitate participant identification and authentication without compromising personal data. This fosters decentralized identity systems on the blockchain, reducing reliance on centralized entities and elevating user privacy and security [72].

4) MPC in Blockchain Applications: Applications ranging from EVs to FinTech can substantially benefit from MPC, which we review below.

❶ **EVs.** In EVs, MPC facilitates private and secure charging transactions. Such protocols ensure efficient charging while protecting user data, identity, and location, thus elevating trust in EV charging infrastructures [72].

❷ **FinTech.** MPC's contributions to blockchain-based FinTech are notable, empowering secure transactions, smart contract execution, and data analysis. Using MPC, users can safely compute financial algorithms without jeopardizing data privacy. For instance, by coupling FL and MPC, Jingwei *et al.* [72] suggested an approach where multiple entities can jointly train FL models without sharing personal data. The combination of FL and MPC ensures data privacy while facilitating collaborative model training.

❸ **Supply Chain.** Supply chain management can also leverage MPC for secure data sharing, allowing for efficient coordination, inventory management, and traceability [92].

❹ **Healthcare Systems.** In blockchain-based healthcare systems, MPC ensures the secure sharing of patient data, medical records, and research findings while complying with stringent privacy regulations [195].

❺ **Auctions.** Blockchain-based auctions benefit from MPC, ensuring bid confidentiality and fairness [113].

❻ **Electronic Voting.** MPC integration into voting provides voters unparalleled privacy and security. The MPC protocols safeguard votes, bolstering trust in e-voting processes.

❼ **IoT.** IoT devices can also utilize MPC to bolster data privacy and security. MPC in IoT ensures data protection, enhancing overall network security [196].

❽ **Energy Trading.** In blockchain-based energy trading, MPC plays a vital role in secure computations related to pricing and optimization, fostering efficient energy markets [196].

Pivotal studies utilizing diverse MPC methods, such as secret sharing, HE, garbled circuits, bilinear pairings, oblivious transfer, and ZKP, are displayed in Table VIII

I. Digital Signature Schemes

1) Benefits of Digital Signatures: A digital signature scheme is vital for blockchain system implementations, addressing several core issues, one of which is authentication. When numerous participants are involved in blockchain transactions, verifying each participant's legitimacy and ensuring transactions originate from a genuine source is paramount [87]. Digital signatures play a pivotal role in confirming the sender's identity and the integrity of the transmitted data [154]. Data integrity is another primary concern for blockchain systems. A blockchain's operation hinges on its recorded data remaining unaltered during transmission and storage, with immutability being its cornerstone. Digital signatures offer cryptographic proof that data remains unchanged, underlining their importance in safeguarding data integrity [207], [81].

Digital signature schemes in blockchain applications ensure authenticity, integrity, and data security. Within the blockchain network, these signatures confirm the identity and integrity of participants. Leveraging public-private key cryptography, these schemes enhance trust and transparency by fostering secure and tamper-resistant interactions [57].

TABLE IX
A COMPARISON OF DIFFERENT REPRESENTATIVE WORKS USE OF THE NOTION OF DIGITAL SIGNATURE SCHEME ACROSS VARIOUS TECHNIQUES USED FOR ENABLING IT.

Author	Ref.	Year	ECDSA	Schnorr	BLS	Ring	Group
Xu *et al.*	[158]	2020	●				
Omar *et al.*	[41]	2020	●				
Wang *et al.*	[78]	2020				●	
Firoozjaei *et al.*	[120]	2020	●			●	
Zhang *et al.*	[64]	2020					●
Zaghloul *et al.*	[71]	2020	●				
Shao *et al.*	[95]	2020	●				
Mei *et al.*	[62]	2021	●				
Chaisawat *et al.*	[118]	2021	●				
Avizhe *et al.*	[153]	2021				●	
Xu *et al.*	[90]	2021				●	
Banupriya *et al.*	[88]	2021				●	
Lin *et al.*	[76]	2021					●
Lin *et al.*	[207]	2021	●	●	●		
Thyaga. *et al.*	[81]	2022	●	●	●		
Garcia *et al.*	[109]	2022	●				
Qiao *et al.*	[87]	2022					●
Zhang *et al.*	[208]	2022		●			
He *et al.*	[77]	2022		●			
Jia *et al.*	[70]	2022				●	
Zhao *et al.*	[209]	2022					●

In supply chain management, blockchain technology tracks goods and verifies their authenticity. Senders use private keys to sign each stage of the supply chain, ensuring transaction authenticity [87]. Recipients then verify this using the sender's public key. Similarly, digital signature schemes are used in blockchain applications to sign documents. Users employ their private keys to sign documents digitally, and blockchain-based notary services validate the authenticity and integrity of these documents. Once authenticated, anyone with access to the document's public key can verify it [183].

For blockchain applications like cryptocurrencies, transactions are safeguarded using digital signature schemes [82]. When initiating a transaction, the sender signs the details with their private key. This signature verifies the transaction, prevents unauthorized modifications, and establishes the sender's asset ownership. Cryptocurrencies, including Bitcoin and Ethereum, rely on digital signatures to confirm wallet ownership [82]. Thyagarajan *et al.* [81] discussed atomic swaps, a decentralized asset exchange protocol. Participants like Alice and Bob have unique digital signatures associated with their blockchain addresses. These signatures' verification establishes trust, allowing participants to create and sign swap transactions. Once signed transactions are broadcasted to their respective blockchain networks and validated, an atomic swap follows predetermined conditions.

2) Technical Challenges: One primary challenge is the need for robust cryptographic algorithms to withstand quantum computing threats. As quantum computing advances, it poses a risk to the cryptographic security of digital signatures, potentially enabling the decryption of private keys without authorization [82]. Another significant challenge is the scalability of blockchain networks. The verification process of digital signatures requires computational resources, which can lead to network congestion and increased transaction fees as

the number of transactions rises. This scalability issue hinders the widespread adoption of blockchain technologies, especially in systems requiring high transaction throughput [87]

Managing private keys securely is a crucial concern. Users must securely store their private keys, as losing them can result in the irreversible loss of assets. Additionally, if a malicious party obtains a user's private key, they can impersonate the user and authorize transactions fraudulently [154]. Lastly, regulatory and legal challenges exist. The legal recognition of digital signatures varies by jurisdiction, affecting the enforceability of blockchain-based contracts and transactions. Ensuring compliance with global regulations while maintaining the decentralized nature of blockchain is complex [57].

3) Techniques to Ensure Digital Signatures: Blockchain systems ensure the integrity and security of digital messages and transactions through digital signature schemes. Cryptographic methods, including digital signatures, are employed to verify the authenticity of digital documents [82]. To create a digital signature, the sender applies their private key to a hash function, producing a fixed-size hash value representing the message's contents. This hash value forms a unique digital signature when combined with the private key. The recipient calculates the hash value using the same function and verifies the signature with the sender's public key, confirming the message's authenticity. This process ensures that the message remains secure and unchanged during transmission, preventing unauthorized alterations [87].

4) Digital Signatures in Blockchain Applications: In the blockchain applications discussed in section III, digital signatures are pivotal in securing the authenticity and integrity of transactions and data, offering protection against threats.

❶ **FinTech.** Digital signatures have notably enhanced blockchain financial transactions. Participants use their private keys to generate signatures, which are then attached to the transaction [82]. For instance, when transferring cryptocurrency tokens, the sender's digital signature ensures the transaction's authenticity and integrity. This approach makes blockchain transactions more secure and transparent, eliminating the need for intermediaries [81], [183].

❷ **Supply Chain.** Digital signatures are also integral to supply chain security. Participants sign data using private keys, which others can verify with the associated public keys. This ensures that data has not been altered and originates from the expected source. For example, participants in a food supply chain can digitally sign tracking information, providing stakeholders with authentic and traceable data [87].

❸ **Healthcare Systems.** In healthcare, digital signatures bolster data integrity, authenticity, and non-repudiation. Patient records, for instance, can be digitally signed and stored on a secure and decentralized blockchain. This ensures that healthcare data remains consistent and originates from a legitimate entity. These signatures, combined with encryption, bolster data security and patient care [210].

❹ **EVs.** For EVs utilizing blockchain, digital signatures validate transactions and ensure that only authorized parties, such as charging stations and EVs, participate in the transaction. Moreover, signatures validate charging data, preventing alterations. In energy trading, digital signatures foster trust and accountability between EVs and charging stations [57], [207].

❺ **IoT.** By integrating IoT with blockchain, digital signatures enhance data security. Devices generate digital signatures for data, like access logs, which can be verified on the blockchain. This approach increases the reliability of IoT data, offering secure, transparent transactions [210].

Some research employing various digital signature techniques, including ECDSA, Schnorr signatures, BLS, ring signatures, and group signatures, are outlined in Table IX.

TABLE X
COMPARISON OF REPRESENTATIVE WORKS UTILIZING HE ACROSS VARIOUS TECHNIQUES FOR ENABLING HE.

Author	Ref.	Year	FHE	PHE	VHE	ElGamal Encryption	Threshold HE	Paillier Cryptosystem	Proxy Re-Encryption
Yahayaet al.	[127]	2020		●				●	
Zondaet al.	[211]	2020	●						●
Huet al.	[176]	2021	●						
Liuet al.	[72]	2021	●				●		
Luet al.	[154]	2021						●	
Kongeet al.	[165]	2021					●	●	
Fengeet al.	[212]	2021					●		
Wengeet al.	[213]	2021					●	●	
Maet al.	[96]	2021	●						
Gengeet al.	[214]	2021	●					●	
Huangeet al.	[168]	2021	●				●		
Wuet al.	[52]	2021	●						
Lvet al.	[215]	2021	●				●		
Liuet al.	[206]	2021	●			●	●		
Almasheet al.	[155]	2022	●			●			
Nguyeneet al.	[119]	2022					●	●	
Hardineet al.	[156]	2022							●
Songeet al.	[89]	2022			●		●		
Jiaet al.	[44]	2022	●					●	
Miaoet al.	[177]	2022	●					●	
Guaneet al.	[197]	2022	●						●
Huangeet al.	[121]	2022	●			●	●		
Lieet al.	[216]	2022	●						
Lieet al.	[217]	2022	●						

J. Homomorphic Encryption

HE is a powerful cryptographic technique that can be applied to blockchain systems. It allows for computations on encrypted data without requiring decryption [44]. This ensures both privacy and security during data manipulation and computation. While blockchain systems traditionally encrypt data and transactions to protect sensitive information, any computation would necessitate decrypting the data first, thereby potentially exposing it [212].

HE encompasses three algorithms: *KeyGen*, *Encrypt*, and *Decrypt*. Through this scheme, computations can be executed on encrypted data. The resulting output ciphertexts, when decrypted, are consistent with results from operations performed directly on the plaintexts. Some HE schemes, known as additive HE, can handle addition operations on ciphertexts, while others might only facilitate multiplication [155].

1) Benefits of HE: HE enhances the security and privacy in blockchain networks. For instance, Song *et al.* [89] addressed the growing threats to blockchain networks and Bitcoin exchanges in particular, emphasizing the importance of detection

and prediction services. They propose a privacy-preserving anomaly detection framework in blockchain networks using vector HE to protect transaction data privacy. Additionally, HE supports privacy in smart contracts by allowing computations on encrypted data without exposing the plaintext, ensuring the secure execution of smart contracts.

When integrated into a blockchain system, HE becomes part of the transaction validation and execution processes. Blockchain nodes can perform computations on encrypted data during these processes without revealing sensitive information, enhancing data security [119], [118]. HE is particularly suitable for self-executing smart contracts with predetermined conditions, as these contracts can perform operations on encrypted data without exposing the plaintext. This allows for the execution of complex business logic without the risk of data exposure [215], [179]. For example, in Electric Vehicle (EV) systems, smart contracts can utilize HE to process encrypted location data, enabling distance calculations for charging stations while preserving the EV owner's privacy [165].

2) Technical Challenges: A primary challenge in blockchain systems is safeguarding the privacy of sensitive data. HE addresses numerous privacy-related challenges in blockchain. Industries like healthcare, finance, and businesses require the utmost privacy for data and transactions on the blockchain. With HE, computations can be performed on encrypted data, eliminating the need to decrypt it first [155].

In blockchain systems, ensuring the secure execution of smart contracts while maintaining the confidentiality of sensitive data presents a significant challenge. HE provides a solution by allowing smart contracts to operate securely on encrypted data, preserving the privacy of underlying information. For instance, in the case of EVs, HE can safeguard sensitive location and transaction data during navigation and routing optimization functions [127]. Blockchain networks frequently require data sharing and collaboration among participants, but sensitive data must be protected. HE facilitates secure data sharing and collaboration by enabling computations on encrypted data, ensuring data confidentiality [127]. Additionally, preserving data integrity and the reliability of computations are critical in blockchain systems, both of which can be achieved through HE, ensuring that computations on encrypted data produce trustworthy results [119].

3) Techniques to Ensure HE: There are several categories of HE, which are reviewed in the following.

Partially Homorphic Encryption. The Partially HE algorithm (PHE) supports either addition or multiplication, but not both simultaneously [44]. For instance, the Paillier cryptosystems provide a PHE that supports the addition of encrypted data. The mathematical foundation of this system is modular arithmetic, rooted in the decisional composite residual assumption [44]. A blockchain-based privacy and reputation computing system, as elaborated by Geng *et al.* [214], leverages PHE. Since service rating values are private, they are encrypted. Given that customer data on the blockchain comprises both public and private data, PHE allows for computations using these rating values without revealing them, ensuring privacy with minimal computational overhead [89].

Fully Homomorphic Encryption. In 2009, Gentry introduced the Fully HE scheme (FHE). This scheme's mathematical underpinnings and security assumptions are intricate, involving advanced concepts such as lattice-based cryptography. FHE enables diverse computations on encrypted data, encompassing operations like addition, multiplication, and other more intricate procedures [176]. Employing HE in blockchain systems allows computations on encrypted data while preserving the underlying data's privacy and integrity. This is crucial in sectors where data security and privacy are paramount [177].

Selecting an appropriate HE scheme in a blockchain system should be tailored to the application's specific requirements and constraints. PHE and FHE offer varying levels of computational capability. Once an encryption scheme is chosen, integrating key generation, encryption, decryption algorithms, and protocols is essential. The KeyGen algorithm generates encryption and decryption keys, and other necessary public parameters. The Encrypt algorithm transforms data into ciphertext, while the Decrypt algorithm reverses this process [155].

4) HE in Blockchain Applications: HE significantly enhances security and privacy in various blockchain applications.

❶ **FinTech.** In financial transactions, it allows secure computations on encrypted financial data, ensuring the confidentiality of sensitive information during transactions. For example, it enables private payments under specific conditions, guaranteeing the safety of financial details [154], [155]

❷ **EVs.** In the context of EVs on the blockchain, HE addresses challenges related to data privacy and security. It facilitates secure and private communication between EVs and grid facilities, optimizing EV charging and safeguarding user data like location. Additionally, it supports efficient scheduling, reducing charging waiting times and ensuring a better user experience. HE also promotes anonymity in the EV ecosystem, enabling secure and private communication and trading while protecting user identities and transactions [127].

❸ **Electronic Voting.** In the domain of blockchain-based voting, HE allows computations on encrypted votes without decryption, ensuring the privacy of individual votes. It enables aggregating, counting, and verifying encrypted votes without compromising their confidentiality, resulting in a transparent and trustworthy voting system. This is especially vital in e-voting systems, as it reduces the risks of unauthorized access and manipulation, enhancing voter trust and security [119].

❹ **IoT.** In the IoT on the blockchain, HE is essential for the secure sharing of sensitive data. Data protection is paramount with an increasing volume of data generated by IoT devices. A blockchain-enabled FL model, supported by HE, addresses these security concerns, ensuring data and model sharing while preserving privacy and accuracy. This comprehensive solution, which integrates HE, blockchain, and FL, has been substantiated through security analysis and experimental results, demonstrating its effectiveness and performance [44].

Research works utilizing a variety of homomorphic encryption techniques, such as FHE, PHE, VHE, ElGamal Encryption, Threshold HE, the paillier cryptosystem, and proxy re-encryption, are detailed in Table X.

TABLE XI
A COMPARISON OF DIFFERENT REPRESENTATIVE WORKS USE OF THE NOTION OF CONFIDENTIALITY MEASURES ACROSS VARIOUS TECHNIQUES USED FOR ENABLING IT.

Author	Ref.	Year	Access Control	MPC	HE	Off-Chain	Ring Signatures	ZKP
Bernabe*et al.*	[8]	2019	●					
Jiang*et al.*	[126]	2020				●		●
Li*et al.*	[150]	2020			●		●	
Firoozjaei*et al.*	[120]	2020			●		●	●
Liu*et al.*	[151]	2020					●	
Sahai*et al.*	[93]	2020						●
Gabay*et al.*	[149]	2020						●
Shi*et al.*	[31]	2020						●
Liu*et al.*	[72]	2020	●	●	●			
Shao*et al.*	[95]	2020	●					
Vasylkovskyi*et al.*	[162]	2020	●					
Lu*et al.*	[163]	2020	●					
Xiao*et al.*	[218]	2020				●		
Avizhe*et al.*	[153]	2021	●			●	●	
Lu*et al.*	[154]	2021			●			
Krishnamoorthi*et al.*	[164]	2021	●			●		
Kong*et al.*	[165]	2021	●					
Bosri*et al.*	[166]	2021	●					
Peng*et al.*	[105]	2021	●					
Chaisawat*et al.*	[118]	2021	●					
Constantinides*et al.*	[113]	2021		●		●		
Cong*et al.*	[169]	2021				●		
Liu*et al.*	[219]	2021				●		
Almashaqbeh*et al.*	[155]	2022					●	●
Qiao*et al.*	[87]	2022					●	
Baranwa*et al.*	[79]	2022		●	●			●
Wan*et al.*	[133]	2022					●	●
Rasheed*et al.*	[38]	2022						●
Huang*et al.*	[121]	2022						●
Nguyen*et al.*	[119]	2022			●			●
Jayabalan*et al.*	[134]	2022				●		
Malik*et al.*	[92]	2022	●					
Guan*et al.*	[197]	2022		●				
Ghosh*et al.*	[5]	2022		●				
Zhang*et al.*	[128]	2022				●		
Zhou*et al.*	[68]	2023		●				

K. Confidentiality Measures

As blockchain systems proliferate across different industries, ensuring confidentiality becomes critical to protect sensitive information from unauthorized access or disclosure. The increasing adoption of blockchain technology necessitates understanding how to maintain confidentiality within these decentralized networks [134]. Confidentiality within blockchain systems involves protecting sensitive data and transactions to ensure that only authorized participants have access to them. This confidentiality bolsters user trust by ensuring both privacy and secure communication between participants [156].

1) Benefits of Confidentiality: Confidentiality is central to blockchain systems, shielding sensitive information and preserving user privacy. By leveraging cryptographic methods and access controls, blockchain systems can maintain data confidentiality across transactions and participants [156]. Public and private key cryptography is fundamental, allowing participants to encrypt information using public keys and decrypt it using private ones. Access controls, on the other hand, manage visibility within the blockchain, ensuring that only those with the right permissions can access critical data [211], [162].

2) Technical Challenges: Since blockchain applications often house sensitive data, e.g., identities and transaction records, addressing confidentiality is essential. Participant privacy is crucial; without adequate confidentiality protocols, this data could be exposed, threatening privacy [210]. By embedding confidentiality safeguards, blockchain protects participants' identities and personal details. Furthermore, some blockchain applications necessitate business confidentiality. Proprietary algorithms, trade secrets, and other valuable business data need protection from potential exposure to competitors. By embedding confidentiality tools, businesses can safeguard vital information within the blockchain [156], [211].

Another concern is revealing exact transaction amounts. Even if the transaction details are transparent, disclosing precise amounts can risk financial details and business associations. Tools like confidential transactions can obscure these specific amounts, preserving their confidentiality [150]. In industries like healthcare and finance, regulatory compliance is essential. Blockchain applications must align with data protection regulations. By introducing confidentiality measures, the protection of sensitive data is ensured, facilitating regulatory compliance [210]. Moreover, incorporating security directly into blockchain is vital, especially when managing sensitive data like medical records or legal documentation [150].

3) Techniques: The confidentiality in blockchain revolves around preserving sensitive data from unwarranted access or disclosure. Various measures, such as data encryption, decentralization, smart contracts, ZKP, and private or permissioned blockchains, ensure that sensitive information remains secure. These strategies collectively highlight blockchain technology's commitment to catering to diverse confidentiality needs, providing robust security for critical data [210], [7].

4) Confidentiality in Blockchain Applications: ZKP is among the most potent tools in the cryptographic arsenal. Because of their fundamental abstract nature, their utilization is almost identical in the various applications. They enable participants to affirm the authenticity of data without revealing the data itself [218], [211]. Blockchain systems sometimes employ off-chain data storage solutions to protect exceptionally sensitive or voluminous data. By keeping this data off-chain, the technology reduces exposure risks while benefiting from blockchain's inherent transparency and immutability [150], [7]. Coupled with ZKP, off-chain techniques can be used to prove various properties of the data without sharing it.

Various representative works utilizing the confidentiality measures through access control, MPC, HE, off-chain transactions, ring signatures, and ZKP are shown in Table XI.

L. Stealth Addresses

Stealth addresses maintain privacy within financial blockchains like Bitcoin and Ethereum. When a transaction is made to a specific payee, the payer generates a one-time stealth address using cryptographic methods, preventing the link between the payer and payee [220]. Ripple introduces blinded tags to enhance privacy further, making transactions appear random to external parties while maintaining their significance for the intended recipient [221].

When receiving funds, individuals create a cryptographic key pair, a public key and a private key. Asymmetric cryptography is fundamental to stealth addresses. Recipients share their

TABLE XII
A COMPARISON OF DIFFERENT REPRESENTATIVE WORKS USE OF THE NOTION OF STEALTH ADDRESSES AND TEE ACROSS VARIOUS TECHNIQUES USED FOR ENABLING IT.

Author	Ref.	Year	ECC	DDH	ZKPs	Ring Signature	Intel SGX	Smart Contract	MPC
Bernabe*et al.*	[8]	2019	●		●	●			
Jiang*et al.*	[126]	2020	●		●				
Zaghloul*et al.*	[71]	2020	●	●	●	●			
Xiao*et al.*	[218]	2020					●	●	
Lee*et al.*	[220]	2021	●						
Brotsis*et al.*	[221]	2021	●	●	●	●			
Liu*et al.*	[80]	2021					●	●	
An*et al.*	[171]	2022		●					
Malik*et al.*	[92]	2022			●				
He*et al.*	[77]	2022					●		●
Hardin*et al.*	[156]	2022					●	●	
Liu*et al.*	[186]	2022			●		●	●	

public key on the blockchain to enable secure fund transfers. Senders, in turn, create a unique stealth address, also known as a one-time random address, using random data and complex cryptographic operations like elliptic curve multiplication [71]. This stealth address remains independent of the recipient's identity or primary public key, ensuring enhanced privacy and security in blockchain transactions [221].

1) Benefits of Stealth Addresses: Stealth addresses are an indispensable tool aiming to preserve privacy and anonymity. They combine cryptographic methodologies and specific protocol implementations, ensuring that transactions remain untraceable. To enable stealth addresses, a user generates a cryptographic key pair. When initiating a transaction, the sender generates a one-time address, and through elliptic curve cryptography, associates a distinct address with the transaction, rendering it challenging to trace back to the original public key. By performing cryptographic operations internally within the blockchain and segregating keys, participants can retain their privacy and anonymity [8], [88].

2) Technical Challenges: The blockchain's inherent transparency is a double-edged sword by guaranteeing both trustworthiness and accountability [171]. Nevertheless, this transparency also presents difficulties for users seeking to maintain privacy regarding their identities and transactions. Without privacy-centric measures like stealth addresses, it becomes possible for observers to trace transactions back to particular individuals or entities. Such transparency could lead to the unintended surveillance of participants, thereby jeopardizing their financial confidentiality on the blockchain. Over time, this could potentially result in profiling, tracking, or the aggregation of transactional data [8], [71].

An and Chen [171] underscore the necessity of securing examination marking processes while retaining transparency, fairness, and privacy. They propose *ExamChain*, a consortium blockchain-based solution that not only fully shields sensitive information but also equips educational authorities with audit capabilities. *ExamChain* allows off-site candidate marking and offers a ledger-based tracking of the evaluation process. Traditional methods of transferring exam scripts, given the involvement of several intermediaries, are vulnerable to security threats and potential cheating. Incorporating stealth addresses into these systems serves as a robust defense, guaranteeing the confidentiality of candidates' identities, responses, scores, and even the identities of the markers.

3) Stealth Addresses in Blockchain Applications: Stealth addresses are utilized in various applications, some of which we review in the following.

❶ **FinTech.** In FinTech, stealth addresses are frequently employed to ensure transactional privacy. Cryptocurrencies like Bitcoin harness stealth addresses to mask the identities of recipients. By generating unique one-time addresses for every transaction, these systems prevent efforts to trace and link transactions to recipient identities or public keys. Similarly, *Monero*, drawing from Cryptonote technology, incorporates one-time addresses to accentuate privacy [8], [221].

❷ **Supply Chain.** In supply chain applications, stealth addresses offer increased security and privacy by anonymizing transactions and concealing participant identities. This helps protect intellectual property and sensitive business relationships, as unique addresses are used for each transaction. This practice ensures confidential business transactions, a crucial element for maintaining competitive advantages and safeguarding sensitive business dealings. [92].

❸ **Healthcare System.** In healthcare applications of blockchain, ensuring patient data privacy is a top priority. Systems like *MedRec* use stealth addresses to securely and privately access patient data, allowing authorized entities to share healthcare information while maintaining confidentiality. The growing adoption of stealth addresses across various sectors highlights their importance in maintaining data privacy and security in decentralized environments [220].

Studies deploying stealth addresses and TEE, incorporating techniques such as ECC, DDH, ZKPs, ring signatures, Intel SGX, smart contracts, and MPC, are presented in Table XII.

M. Trusted Execution Environment

TEE is a secure computing environment that protects blockchain applications from privileged software attacks and hardware breaches. It safeguards code and runtime states within a secure *enclave*, enhancing security. TEE offers essential features like integrity measurement and remote attestation, which ensures code integrity. Combining a secure *Enclave*, remote attestation, and isolation mechanisms strengthens blockchain system security and trustworthiness, even in compromised environments [156]. TEEs provide memory protection and isolated execution, making it possible to create secure and trustworthy decentralized blockchain applications and enhance the security of sensitive processes [80].

1) Benefits of TEE: By merging hardware and software capabilities, the TEE establishes secure zones for crucial data and operations within distributed systems, thus establishing a resilient security framework [218]. By certifying the integrity of code execution and data exchange, the TEE thwarts tampering attempts, fostering trust among participants. This environment ensures that sensitive information remains confidential, fortifying privacy [80], [218].

Integrating TEEs into distributed systems offers substantial enhancements in privacy and security. Distributed systems,

with their interconnected nodes, are vulnerable to security breaches [218]. TEEs address these concerns by creating secure enclaves for sensitive data operations. When selecting a TEE, compatibility, functionality, and security features are crucial factors. Technologies like Intel SGX and ARM TrustZone exemplify such features. TEEs should be strategically incorporated into the system's architecture, with a focus on components like smart contracts, consensus mechanisms, and data storage, to maximize their effectiveness [218], [156].

In TEE-reinforced distributed systems, secure enclaves act as protected areas where computations maintain confidentiality and authenticity. Specific protocols or software interfaces are necessary to establish a secure link between the TEE and the broader system [156]. TEE implementation significantly improves data security, incorporating encryption, access control, and secure data storage. Techniques like ZKP and HE further enhance data security. Integrating TEEs into distributed consensus mechanisms bolsters integrity assurances within consensus protocols [218]. TEEs also help mitigate vulnerabilities when interacting with external data sources, ensuring authentic retrieval and data processing [156], [80], [218].

2) Technical Challenge: Blockchains, characterized by their extensive node networks, face various data security challenges, operational security issues, and potential threats from unauthorized access, tampering, and malicious attacks. This environment of mistrust creates complexities in sharing sensitive information and impedes equitable execution [80]. The TEE was introduced to address these challenges.

3) TEE in Blockchain Applications: TEEs are robust solutions that address the persistent security and privacy challenges faced by blockchain technology irrespective of the application—since they work at a lower level of abstraction. They create secure enclaves for critical computations, strengthening the security infrastructure and preventing unauthorized access, manipulation, or data tampering. TEEs extend their protective capabilities to secure transactions, private data, smart contracts, and external system integration, enhancing data authenticity and reducing vulnerabilities in blockchain applications [156], [218], [80].

Among other applications, TEEs are instrumental in ensuring patient data confidentiality in the electronic healthcare systems. They enable private computations on sensitive data, safeguard patient privacy, and support secure health data sharing [218]. TEEs also maintain data integrity, ensuring consistency when exchanging health information across different systems. In TEE-enhanced blockchain ecosystems, immutable audit trails enhance transparency and accountability [80]. TEEs secure the storage and processing of consent-related data, preserving patient privacy and choices. Healthcare blockchain applications fortified with TEEs elevate security, data integrity, privacy, interoperability, and patient consent, making them indispensable in the healthcare domain [156].

N. Merkle Trees and Authenticated Data Structures

A Merkle tree, often called a hash tree or binary hash tree, ensures the accuracy and consistency of large data sets. Invented by Ralph Merkle in 1979, this binary tree structure represents individual data blocks, while non-leaf nodes represent hash values derived from their child nodes. Leaf nodes are formed by hashing data blocks using a cryptographic hash function [71]. Parent nodes are created by pairing and rehashing leaf node values, culminating in a single Merkle root. This root concisely represents the entire dataset within a blockchain's block header. To verify data, comparing the Merkle root hash suffices over inspecting each block individually. Data block authenticity within the Merkle tree can be validated by presenting the corresponding leaf hash and the path of intermediary hashes leading to the root. By merging the leaf node hash with the intermediate hashes along the path, data block integrity can be verified [71].

1) Benefits and Technical Challenges: In blockchain systems, Merkle trees play a crucial role in improving privacy by facilitating efficient data verification while ensuring confidentiality. Instead of examining every transaction or data entry, users can compare a transaction's hash value with the Merkle root in the block header, enhancing computational efficiency [222]. Furthermore, Merkle trees introduce a mechanism known as Merkle proofs that allows users to verify transactions without revealing the complete content of the entire block. By presenting a sequence of hash values, participants can establish the inclusion of a transaction within the tree, thereby ensuring both data privacy and integrity [223]. Lightweight clients also benefit from Merkle trees, as full nodes can verify transactions without needing the complete blockchain history, making the blockchain more accessible for those with constrained computing resources [224].

2) Techniques to Ensure Security: The Merkle tree-based blockchain system, proposed by Lee and Park [223], protects intelligent surveillance systems while maintaining object privacy. By incorporating Merkle trees, the blockchain system secures the integrity of video data, readily detecting any tampering or altered hash values in subsequent blocks. This proactive security measure reinforces privacy protection, reduces bandwidth consumption, and ensures secure synchronization.

Merkle trees provide a secure and effective method for general distributed systems to verify data integrity and consistency across nodes. Distributed systems need to validate data integrity efficiently. Merkle roots and paths enable nodes to compare sets of hashes instead of examining individual blocks, reducing network bandwidth and computational needs [222]. Additionally, Merkle trees also enable data synchronization and incremental updates. For quick updates without recalculating the whole tree, only the changed leaf nodes and their parent nodes need recomputation. This capability decreases synchronization overhead among distributed nodes when data changes frequently [223], [224].

For fault tolerance and data consistency, comparing the Merkle root hash across nodes is helpful to identify any disparities in the data. A hash check for each block quickly identifies any unauthorized changes or tampering, elevating security, mainly when data is distributed across nodes or sent to multiple users in a system [71]. Additionally, Merkle trees facilitate the creation of cryptographic proofs, such as Merkle proofs, which can confirm the existence of specific data blocks within a system. Data validation, auditing, and transaction verification are crucial in distributed systems, in-

cluding blockchain applications [158].

3) Merkle Trees in Blockchain Applications: Addressing the integration challenges of blockchain applications, as discussed in section III, Merkle Trees stand out as a practical solution, particularly in contexts like IoT and healthcare.

❶ **IoT.** IoT devices, typically with limited computational power, benefit significantly from the efficiency and speed of Merkle Trees in verifying voluminous data sets. Instead of processing all the data, a Merkle proof can validate specific transactions using the Merkle root, enabling even minor devices to engage with the blockchain [71], [224].

❷ **Healthcare Systems.** healthcare, where patient data privacy is crucial, Merkle Trees allows medical data verification without fully revealing patient records. Participants can validate specific data entries without accessing the complete block, using Merkle proofs to affirm data authenticity without exposing sensitive patient information [222]. With their hierarchical hashing approach, Merkle Trees bolsters data integrity in blockchain applications, balancing preserving privacy and ensuring swift data verification [223], [224].

V. Threat Models

To complete the picture of the applications and security and privacy notions, we investigate blockchain threat models in the following section, particularly emphasizing various threat capabilities in the context of privacy and concerns. Although several surveys have outlined the threats on blockchain systems in general, and cryptocurrencies in particular, including understanding their attack surface (e.g., [21], [225]), this section only outlines the general threat capabilities and objectives. The interested reader in more details about the attack surface of blockchains should refer to the above-mentioned surveys.

A. Threat Capabilities

Privacy has become paramount as blockchain technology continues to evolve, characterized by the convergence of data transparency and security. Given blockchain's immutable and decentralized nature, privacy threats have emerged as a primary concern, especially as individuals and entities increasingly adopt the technology [38]. Several threats related to blockchain privacy (and security in general) exist, including risks associated with pseudonymity and vulnerabilities in smart contracts. These threats can compromise both the privacy and the overall security of data within the network [101].

Among the security vulnerabilities and identity threats, the primary concern revolves around *ciphertext* attacks. These attacks aim to decode encrypted blockchain data without proper authorization by targeting the encrypted data itself [95]. A successful breach could reveal sensitive transaction details, jeopardizing both individual privacy and the integrity of the blockchain ledger [72], [167]. Moreover, *spoofing* attacks pose a significant threat, where malicious entities forge fake identities to gain unauthorized access or even subvert blockchain networks. Such attacks can corrupt users' confidence in the system and the security of transactions [38], [9]. Related to this vulnerability are attacks that exploit the power of *network-level adversaries*, which could disrupt the underlying network through *network partition* [21], [139], [140], [141], [142], [226], [227], [228], [229], [230] or routing attack capabilities [231], [232], [233], [234], [235], [236], thus affecting the consensus mechanisms and allowing application-level attacks.

Another vulnerability in blockchains, ironically one of its strengths, is its susceptibility to *Sybil* attacks [166]. These attacks involve the creation of numerous false identities to undermine consensus mechanisms by attenuating their effectiveness [237], [77], [238], [239]. *Replay* attacks represent another source of concern involving the deceptive reuse of intercepted valid transactions, which can potentially result in unauthorized data exposure [50], [65].

The *man-in-the-middle (MITM)* attacks exploit unintentional data leaks from secondary sources to compromise encryption protocols and jeopardize data privacy. Moreover, *MITM* attacks inspect cryptographic protocols to identify weaknesses that might compromise data privacy [207], [240]. In edge *insertion* attacks, nodes are added to the network's periphery to distort consensus and impair data integrity [152], [192]. The purpose of *key-only* attacks in cryptographic, analytical, and control threats is to compromise cryptographic keys to gain unauthorized access to sensitive information [153], [82].

The *adaptive* attacks pose ongoing threats to data confidentiality in addition to continuously altering their strategies based on feedback from their victims [241]. *Known message and chosen message (CMA)* attacks involve selecting and analyzing specific messages to identify patterns or confidential transaction details [82]. By revealing hidden information patterns that may breach user privacy, misuse of data mining can despoil user anonymity [121], [165]. Malicious nodes may disrupt consensus mechanisms during interception and modification attacks [242], while byzantine attacks may disrupt networks during byzantine attacks [76], [38].

During network analysis, which is used to study traffic patterns, the user identity may be inadvertently revealed; a 51% attack [21], in which one entity controls the majority of computing power, can austerely destroy the integrity of transactions and data [100], [243], [9]. *Collision* attacks have a singularly undermining objective: to challenge the integrity of the cryptographic foundations of blockchain technology [76], [188]. By finding two distinct inputs that produce the same hash output, attackers aim to demonstrate vulnerabilities in the blockchain's hashing algorithm, thereby questioning the entire network's security and reliability [103], [195]. The ramifications of successful collision attacks are profound, including the potential for double-spending, forging transactions, or otherwise compromising the blockchain's immutability [162], [102].

B. Threat Objectives

The frequent attacks of blockchain are attributed to its decentralization and inherent application value, which makes it more advantageous over other applications. Comprehension of the principal goals of the numerous threat vectors is crucial for risk elimination and mitigation [197].

In the context of privacy, studies revealed that the main objective of threat vectors is blockchain anatomy breaches.

Two main types of anatomy breach attacks were identified: 1) to reveal connections between different blockchain addresses and 2) to map real-world identities like names or addresses to specific blockchain nodes and transactions [104], [164].

De-anonymization. attacks in blockchain technology seek to strip away the layers of privacy that protect the identities behind blockchain operations or transactions [244]. The primary concern with these attacks is their potential to compromise the integrity and credibility of digital currencies. For instance, *double spending* attacks, where the same digital tokens are used more than once, pose a significant threat [136]. These attacks not only question the reliability of the currency but also endanger the data's integrity through tactics like *poisoning and sandwich* attacks [245]. Poisoning involves injecting malicious or inaccurate data into the blockchain, whereas sandwich attacks place malicious transactions around a target to influence its outcome [112]. Additionally, *reconstruction* attacks aim to piece together fragmented data across the blockchain, further unveiling original information [178].

Linkability. Contrasting with de-anonymization, *linkability* attacks do not necessarily seek to uncover real-world identities but instead focus on establishing connections between separate transactions or accounts belonging to a single user [136]. These attacks exploit the public nature of blockchain transactions, undermining the privacy and anonymity that blockchain aims to provide [97]. By linking transactions or addresses, attackers can compile comprehensive profiles of users, revealing their transaction patterns and financial behaviors. Such information could lead to targeted phishing, exposure of financial habits, or a general loss of trust in a blockchain's security and privacy capabilities [97], [6], [128].

Both de-anonymization and linkability attacks present profound challenges to the privacy protections offered by blockchain networks. They enable attackers to construct detailed profiles of users' financial activities, significantly reducing the anonymity blockchain networks aim to provide [97], [6]. This exposure makes users susceptible to targeted phishing and social engineering attacks. Moreover, the successful execution of these attacks can erode confidence in blockchain technology, potentially affecting user adoption and the overall growth and security of the network [136].

In the first scenario, a *hijacking* attacks in the blockchain domain aim to gain unauthorized access to an active session between participants, targeting the very heart of the blockchain's security mechanisms. The primary objective of such attacks is to intercept or assume control over a session to facilitate malicious activities, ranging from the theft of sensitive information to the execution of unauthorized transactions [128]. These attacks exploit the network's communication protocols, positioning attackers to masquerade as legitimate entities within the network [136]. The implications of hijacking are far-reaching, with potential outcomes including the manipulation of transaction data, theft of digital assets, and the introduction of malicious code or data into the blockchain [137]. By compromising both the integrity and confidentiality of the network, hijacking attacks pose significant risks to users and undermine the overall security framework of the blockchain [76].

Byzantine attacks introduce malicious behavior into nodes. The aim is to disrupt the blockchain's consensus mechanism, potentially integrating false data into the blockchain [137]. Such attacks erode the network's integrity, fostering confusion and disagreement among nodes. This can severely delay or outright prevent the achievement of consensus, leading to forks or orphaned blocks that create inconsistencies in the transaction history [119]. The resultant disruption threatens the blockchain's reliability and the accuracy of its data, compromising the system's overall stability [137]. While forks and orphaned blocks are typically considered structural phenomena within blockchain networks, they can be exploited or inadvertently caused by malicious activities, such as Byzantine attacks [136], [137], [135]. The objective in such scenarios is to leverage these occurrences to create divergent versions of the blockchain or to capitalize on the ensuing confusion and inconsistency. These situations challenge the maintenance of a consistent transaction history, potentially facilitating double-spending attacks or ledger manipulation [119].

SYN floods and DoS attacks disrupt the normal functioning of blockchain networks. By overwhelming nodes with superfluous requests, attackers aim to degrade network performance, delay transaction processing, and disrupt service availability [246], [79]. The ultimate goal is to inflict financial losses and reputational damage on the affected entities. These attacks target the foundational aspect of blockchain's value proposition, its reliability and uptime, thereby shaking the confidence of users and investors in the system's robustness and security [136], [137]. Moreover, *statistical* attacks on blockchain compromise the anonymity and privacy that are hallmark features of this technology. By analyzing transaction patterns and blockchain data, attackers aim to identify and link transactions to real-world identities, thereby stripping away the veil of privacy that users expect [178]. The ultimate goal is to exploit this de-anonymized information for blackmail, targeted phishing attacks, or financial fraud. Beyond personal gain, these attacks can undermine the perceived security and privacy benefits of blockchain, potentially deterring adoption and eroding trust in the system [188].

VI. Conclusion

Blockchain technology, initially pivotal in cryptocurrencies, is expanding its reach, enhancing security and privacy in various domains. In the IoT sector, it plays a crucial role in safeguarding user privacy and connecting devices while keeping data confidential. For EVs, blockchain provides a reliable system for tracking and verifying origins and movements, ensuring regulatory compliance and fostering trust.

In FinTech, blockchain excels in securing transactions and safeguarding user data and financial assets. It bolsters supply chain traceability and authenticity, addressing issues of counterfeiting and fraud. In healthcare, blockchain's immutability guarantees patient record security and consistency.

Blockchain applications, such as electronic auctioning and voting, bring about operational improvements, ensuring system integrity through transparency and authenticity. Its versatility is also evident in energy trading, where it minimizes fraud, enhancing stakeholder trust and market reliability.

Blockchain employs various data security and privacy techniques to address such aspects of various applications. Decentralization mitigates single-point failure risks; anonymity and pseudonyms protect user identities. Access controls, ZKP, and DP ensure secure and private data interactions. MPC and HE allow secure computations on encrypted data, maintaining privacy. In transactions, stealth addresses enhance discretion.

TEE and decentralized machine learning, such as FL, further secure data operations. The use of Merkle trees in blockchain ensures efficient data verification.

Open Directions. Decentralization in blockchain technology brings the risk of data leakage across the network, requiring a balance between transparency and data protection. Anonymity, permissioned blockchains, and pseudonymity offer privacy but face challenges. Non-cryptographic techniques like FL must guard against data exposure, although it is unclear to reason about their guarantees provably, which is an open question. Advancements in cryptographic methods, including ZKP, DP, MPC, digital signatures, HE, TEE, and Merkle Trees, are reshaping blockchain privacy, reinforcing user autonomy, confidentiality, and data integrity, making privacy a foundational element of blockchain's future. However, many of those primitives, such as ZKP, TEE, and HE, are not yet mature enough to address the scale of blockchain systems, making their improvements an open direction. Addressing the security and privacy in the applications secured through blockchains requires a finer understanding of their threat models, making understanding the adversarial capabilities and objectives through a rigorous attack surface analysis paramount.

REFERENCES

[1] V. Ferrari, "Privacy in Financial Information Networks: Directions for the Development of Legal Privacy-Enhancing Financial Technologies," in *Blockchain and Applications - 2nd International Congress, BLOCKCHAIN 2020, L'Aquila, Italy, 17-19 June, 2020*, ser. Advances in Intelligent Systems and Computing, vol. 1238. Springer, 2020, pp. 157–160.

[2] A. A. Khalil, J. Franco, I. Parvez, A. S. Uluagac, H. Shahriar, and M. A. Rahman, "A Literature Review on Blockchain-enabled Security and Operation of Cyber-Physical Systems," in *46th IEEE Annual Computers, Software, and Applications Conferenc, COMPSAC*. IEEE, 2022, pp. 1774–1779.

[3] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11 717–11 731, 2021.

[4] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A Survey of Distributed Consensus Protocols for Blockchain Networks," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020.

[5] B. C. Ghosh, D. Vinayagamurthy, V. Ramakrishna, K. Narayanam, and S. Chakraborty, "Privacy-Preserving Negotiation of Common Trust Anchors Across Blockchain Networks," in *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2022, Shanghai, China, May 2-5, 2022*. IEEE, 2022, pp. 1–5.

[6] G. Wu, S. Wang, Z. Ning, and B. Zhu, "Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System," *IEEE J. Biomed. Health Informatics*, vol. 26, no. 5, pp. 1917–1927, 2022.

[7] D. Schmelz, K. Pinter, P. Niemeier, and T. Grechenig, "Towards Informational Self-determination: Data Portability Requests Based on GDPR by Providing Public Platforms for Authorised Minimal Invasive Privacy Protection," in *Blockchain and Applications - 3rd International Congress, BLOCKCHAIN 2021, Salamanca, Spain, 6-8 October, 2021*, ser. Lecture Notes in Networks and Systems, vol. 320. Springer, 2021, pp. 106–116.

[8] J. B. Bernabé, J. L. Cánovas, J. L. H. Ramos, R. T. Moreno, and A. F. Skarmeta, "Privacy-Preserving Solutions for Blockchain: Review and Challenges," *IEEE Access*, vol. 7, pp. 164 908–164 940, 2019.

[9] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan, and M. A. Imran, "BeepTrace: Blockchain-Enabled Privacy-Preserving Contact Tracing for COVID-19 Pandemic and Beyond," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3915–3929, 2021.

[10] M. Peng, J. Hu, H. Lin, X. Wang, and W. Lin, "A Privacy-Enhanced Mobile Crowdsensing Strategy for Blockchain Empowered Internet of Medical Things," in *20th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2021, Shenyang, China, October 20-22, 2021*. IEEE, 2021, pp. 387–396.

[11] O. Fadi, K. Zkik, A. E. Ghazi, and M. Boulmalf, "A Survey on Blockchain and Artificial Intelligence Technologies for Enhancing Security and Privacy in Smart Environments," *IEEE Access*, vol. 10, pp. 93 168–93 186, 2022.

[12] P. M. Rao, S. Jangirala, S. Pedada, A. K. Das, and Y. Park, "Blockchain Integration for IoT-Enabled V2X Communications: A Comprehensive Survey, Security Issues and Challenges," *IEEE Access*, vol. 11, pp. 54 476–54 494, 2023.

[13] E. R. D. Villarreal, J. García-Alonso, E. Moguel, and J. A. H. Alegria, "Blockchain for Healthcare Management Systems: A Survey on Interoperability and Security," *IEEE Access*, vol. 11, pp. 5629–5652, 2023.

[14] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of Blockchains in the Internet of Things: A Comprehensive Survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019.

[15] T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal, and M. Guizani, "A Comprehensive Survey on the Applications of Blockchain for Securing Vehicular Networks," *IEEE Commun. Surv. Tutorials*, vol. 24, no. 2, pp. 1212–1239, 2022.

[16] M. S. Arbabi, C. Lal, N. R. Veeraragavan, D. Marijan, J. F. Nygård, and R. Vitenberg, "A Survey on Blockchain for Healthcare: Challenges, Benefits, and Future Directions," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 1, pp. 386–424, 2023. [Online]. Available: https://doi.org/10.1109/COMST.2022.3224644

[17] Z. Chen, L. Zhu, P. Jiang, C. Zhang, F. Gao, J. He, D. Xu, and Y. Zhang, "Blockchain Meets Covert Communication: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 24, no. 4, pp. 2163–2192, 2022.

[18] K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain Meets Cloud Computing: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 2009–2030, 2020.

[19] M. U. Hassan, M. H. Rehmani, and J. Chen, "Anomaly Detection in Blockchain Networks: A Comprehensive Survey," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 1, pp. 289–318, 2023.

[20] R. Huo, S. Zeng, Z. Wang, J. Shang, W. Chen, T. Huang, S. Wang, F. R. Yu, and Y. Liu, "A Comprehensive Survey on Blockchain in Industrial Internet of Things: Motivations, Research Progresses, and Future Challenges," *IEEE Commun. Surv. Tutorials*, vol. 24, no. 1, pp. 88–122, 2022.

[21] M. Saad, J. Spaulding, L. Njilla, C. A. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, "Exploring the Attack Surface of Blockchain: A Comprehensive Survey," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 1977–2008, 2020.

[22] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security Services Using Blockchains: A State of the Art Survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 858–880, 2019.

[23] Z. Shi, C. de Laat, P. Grosso, and Z. Zhao, "Integration of Blockchain and Auction Models: A Survey, Some Applications, and Challenges," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 1, pp. 497–537, 2023.

[24] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2794–2830, 2019.

[25] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.

[26] K. Yue, Y. Zhang, Y. Chen, Y. Li, L. Zhao, C. Rong, and L. Chen, "A Survey of Decentralizing Applications via Blockchain: The 5G and Beyond Perspective," *IEEE Commun. Surv. Tutorials*, vol. 23, no. 4, pp. 2191–2217, 2021.

[27] Y. Zuo, J. Guo, N. Gao, Y. Zhu, S. Jin, and X. Li, "A Survey of Blockchain and Artificial Intelligence for 6G Wireless Communica-

tions," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 4, pp. 2494–2528, 2023.

[28] L. D. Xu, Y. Lu, and L. Li, "Embedding Blockchain Technology Into IoT for Security: A Survey," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10 452–10 473, 2021.

[29] Z. Liao, X. Pang, J. Zhang, B. Xiong, and J. Wang, "Blockchain on Security and Forensics Management in Edge Computing for IoT: A Comprehensive Survey," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 2, pp. 1159–1175, 2022.

[30] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, "Blockchain Security: A Survey of Techniques and Research Directions," *IEEE Trans. Serv. Comput.*, vol. 15, no. 4, pp. 2490–2510, 2022.

[31] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Comput. Secur.*, vol. 97, p. 101966, 2020.

[32] N. Y. Douha, M. H. Bhuyan, S. Kashihara, D. Fall, Y. Taenaka, and Y. Kadobayashi, "A survey on blockchain, SDN and NFV for the smart-home security," *Internet Things*, vol. 20, p. 100588, 2022.

[33] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet Things*, vol. 11, p. 100227, 2020.

[34] Q. Bao, B. Li, T. Hu, and X. Sun, "A survey of blockchain consensus safety and security: State-of-the-art, challenges, and future work," *J. Syst. Softw.*, vol. 196, p. 111555, 2023.

[35] S. Latif, Z. Idrees, Z. E. Huma, and J. Ahmad, "Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 11, 2021.

[36] K. Gai, Y. Wu, L. Zhu, Z. Zhang, and M. Qiu, "Differential Privacy-Based Blockchain for Industrial Internet-of-Things," *IEEE Trans. Ind. Informatics*, vol. 16, no. 6, pp. 4156–4165, 2020.

[37] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and A. S. Uluagac, "Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 50–57, 2018.

[38] A. Rasheed, R. N. Mahapatra, C. Varol, and N. Karpoor, "Exploiting Zero Knowledge Proof and Blockchains Towards the Enforcement of Anonymity, Data Integrity and Privacy (ADIP) in the IoT," *IEEE Trans. Emerg. Top. Comput.*, vol. 10, no. 3, pp. 1476–1491, 2022.

[39] N. Denis, S. Chabridon, and M. Laurent, "Bringing Privacy, Security and Performance to the Internet of Things Through Usage Control and Blockchains," in *Privacy and Identity Management. Between Data Protection and Security - 16th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Privacy and Identity 2021, Virtual Event, August 16-20, 2021, Revised Selected Papers*, ser. IFIP Advances in Information and Communication Technology, vol. 644. Springer, 2021, pp. 57–72.

[40] F. Loukil, C. G. Guegan, K. Boukadi, A. Benharkat, and E. Benkhelifa, "Data Privacy Based on IoT Device Behavior Control Using Blockchain," *ACM Trans. Internet Techn.*, vol. 21, no. 1, pp. 23:1–23:20, 2021.

[41] A. A. Omar, A. K. Jamil, M. S. H. Nur, M. M. Hasan, R. Bosri, M. Z. A. Bhuiyan, and M. S. Rahman, "Towards A Transparent and Privacy-preserving Healthcare Platform with Blockchain for Smart Cities," in *19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020, Guangzhou, China, December 29, 2020 - January 1, 2021*. IEEE, 2020, pp. 1291–1296.

[42] M. Abdel-Basset, N. Moustafa, and H. Hawash, "Privacy-Preserved Cyberattack Detection in Industrial Edge of Things (IEoT): A Blockchain-Orchestrated Federated Learning Approach," vol. 18, no. 11, 2022, pp. 7920–7934. [Online]. Available: https://doi.org/10.1109/TII.2022.3167663

[43] R. Shashidhara, N. Ahuja, M. Lajuvanthi, S. Akhila, A. K. Das, and J. J. P. C. Rodrigues, "SDN-chain: Privacy-preserving protocol for software defined networks using blockchain," *Secur. Priv.*, vol. 4, no. 6, 2021.

[44] B. Jia, X. Zhang, J. Liu, Y. Zhang, K. Huang, and Y. Liang, "Blockchain-Enabled Federated Learning Data Protection Aggregation Scheme With Differential Privacy and Homomorphic Encryption in IIoT," *IEEE Trans. Ind. Informatics*, vol. 18, no. 6, pp. 4049–4058, 2022.

[45] Z. Qin, J. Ye, J. Meng, B. Lu, and L. Wang, "Privacy-Preserving Blockchain-Based Federated Learning for Marine Internet of Things," *IEEE Trans. Comput. Soc. Syst.*, vol. 9, no. 1, pp. 159–173, 2022.

[46] A. Lekssays, L. Landa, B. Carminati, and E. Ferrari, "PAutoBot-Catcher: A blockchain-based privacy-preserving botnet detector for Internet of Things," *Comput. Networks*, vol. 200, p. 108512, 2021.

[47] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. A. Maglaras, "Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges," *IEEE Access*, vol. 8, pp. 32 031–32 053, 2020.

[48] J. Liu, G. Zhang, R. Sun, X. Du, and M. Guizani, "A Blockchain-based Conditional Privacy-Preserving Traffic Data Sharing in Cloud," in *2020 IEEE International Conference on Communications, ICC 2020, Dublin, Ireland, June 7-11, 2020*. IEEE, 2020, pp. 1–6.

[49] R. Goyat, G. Kumar, M. Alazab, M. Conti, M. K. Rai, R. Thomas, R. Saha, and T. Kim, "Blockchain-Based Data Storage With Privacy and Authentication in Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14 203–14 215, 2022.

[50] K. Li and R. Shi, "A Flexible and Efficient Privacy-Preserving Range Query Scheme for Blockchain-Enhanced IoT," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 720–733, 2023.

[51] H. Chai, S. Leng, J. He, K. Zhang, and B. Cheng, "CyberChain: Cyber-twin Empowered Blockchain for Lightweight and Privacy-Preserving Authentication in Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 4620–4631, 2022.

[52] Y. Wu, H. Dai, H. Wang, and K. R. Choo, "Blockchain-Based Privacy Preservation for 5G-Enabled Drone Communications," *IEEE Netw.*, vol. 35, no. 1, pp. 50–56, 2021.

[53] Y. Wang, K. Li, Y. Tang, J. Chen, Q. Zhang, X. Luo, and T. Chen, "Towards Saving Blockchain Fees via Secure and Cost-Effective Batching of Smart-Contract Invocations," *IEEE Trans. Software Eng.*, vol. 49, no. 4, pp. 2980–2995, 2023.

[54] T. Wang, Q. Wang, Z. Shen, Z. Jia, and Z. Shao, "Understanding Characteristics and System Implications of DAG-Based Blockchain in IoT Environments," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14 478–14 489, 2022.

[55] S. M. Danish, K. Zhang, and H. Jacobsen, "A Blockchain-Based Privacy-Preserving Intelligent Charging Station Selection for Electric Vehicles," in *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2020, Toronto, ON, Canada, May 2-6, 2020*. IEEE, 2020, pp. 1–3.

[56] A. Boualouache, H. Sedjelmaci, and T. Engel, "Consortium Blockchain for Cooperative Location Privacy Preservation in 5G-Enabled Vehicular Fog Computing," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 7087–7102, 2021.

[57] M. Baza, A. B. T. Sherif, M. M. E. A. Mahmoud, S. Bakiras, W. Alasmary, M. M. Abdallah, and X. Lin, "Privacy-Preserving Blockchain-Based Energy Trading Schemes for Electric Vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 9369–9384, 2021.

[58] B. Li, R. Liang, D. Zhu, W. Chen, and Q. Lin, "Blockchain-Based Trust Management Model for Location Privacy Preserving in VANET," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3765–3775, 2021.

[59] P. Lv, L. Xie, J. Xu, X. Wu, and T. Li, "Misbehavior Detection in Vehicular Ad Hoc Networks Based on Privacy-Preserving Federated Learning and Blockchain," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 4, pp. 3936–3948, 2022.

[60] C. Zhang, L. Zhu, C. Xu, and K. Sharif, "PRVB: Achieving Privacy-Preserving and Reliable Vehicular Crowdsensing via Blockchain Oracle," *IEEE Trans. Veh. Technol.*, vol. 70, no. 1, pp. 831–843, 2021.

[61] B. Luo, X. Li, J. Weng, J. Guo, and J. Ma, "Blockchain Enabled Trust-Based Location Privacy Protection Scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 2034–2048, 2020.

[62] Q. Mei, H. Xiong, Y. Zhao, and K. Yeh, "Toward Blockchain-Enabled IoV with Edge Computing: Efficient and Privacy-Preserving Vehicular Communication and Dynamic Updating," in *IEEE Conference on Dependable and Secure Computing, DSC 2021, Aizuwakamatsu, Japan, January 30 - February 2, 2021*. IEEE, 2021, pp. 1–8.

[63] B. Duan, K. Xin, and Y. Zhong, "Optimal Dispatching of Electric Vehicles Based on Smart Contract and Internet of Things," *IEEE Access*, vol. 8, pp. 9630–9639, 2020.

[64] C. Zhang, L. Zhu, C. Xu, C. Zhang, K. Sharif, H. Wu, and H. Westermann, "BSFP: Blockchain-Enabled Smart Parking With Fairness, Reliability and Privacy Protection," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6578–6591, 2020.

[65] H. Shen, J. Zhou, Z. Cao, X. Dong, and K. R. Choo, "Blockchain-Based Lightweight Certificate Authority for Efficient Privacy-Preserving Location-Based Service in Vehicular Social Networks," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6610–6622, 2020.

[66] N. Naik and P. Jenkins, "Governing Principles of Self-Sovereign Identity Applied to Blockchain Enabled Privacy Preserving Identity

Management Systems," in *IEEE International Symposium on Systems Engineering, ISSE 2020, Vienna, Austria, October 12 - November 12, 2020*. IEEE, 2020, pp. 1–6.

[67] P. W. Khan and Y.-C. Byun, "Blockchain-based peer-to-peer energy trading and charging payment system for electric vehicles," *Sustainability*, vol. 13, no. 14, p. 7962, 2021.

[68] X. Zhou, D. He, M. K. Khan, W. Wu, and K. R. Choo, "An Efficient Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 72, no. 1, pp. 81–92, 2023.

[69] Q. Feng, D. He, S. Zeadally, and K. Liang, "BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks," *IEEE Trans. Ind. Informatics*, vol. 16, no. 6, pp. 4146–4155, 2020.

[70] Y. Jia, S. Sun, Y. Zhang, Q. Zhang, N. Ding, Z. Liu, J. K. Liu, and D. Gu, "${\sf PBT}$PBT: A New Privacy-Preserving Payment Protocol for Blockchain Transactions," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 1, pp. 647–662, 2022.

[71] E. Zaghloul, T. Li, M. W. Mutka, and J. Ren, "Bitcoin and Blockchain: Security and Privacy," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10 288–10 313, 2020.

[72] J. Liu, X. He, R. Sun, X. Du, and M. Guizani, "Privacy-Preserving Data Sharing Scheme with FL via MPC in Financial Permissioned Blockchain," in *ICC 2021 - IEEE International Conference on Communications, Montreal, QC, Canada, June 14-23, 2021*. IEEE, 2021, pp. 1–6.

[73] S. J. Chowdhury, E. Aich, S. Reno, and M. Ahmed, "Utilizing Hyperledger Based Private Blockchain Technology to Secure Credit Card Payment System," *2022 25th International Conference on Computer and Information Technology (ICCIT)*, 2022.

[74] E. Balagolla, W. N. C. Fernando, R. Rathnayake, M. Wijesekera, A. Senarathne, and K. Y. Abeywardhana, "Credit Card Fraud Prevention Using Blockchain," *2021 6th International Conference for Convergence in Technology (I2CT)*, 2021.

[75] S. Kim and S. Kim, "Correction to: E-commerce payment model using blockchain," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 10, p. 14369, 2023.

[76] C. Lin, D. He, X. Huang, X. Xie, and K. R. Choo, "PPChain: A Privacy-Preserving Permissioned Blockchain Architecture for Cryptocurrency and Other Regulated Applications," *IEEE Syst. J.*, vol. 15, no. 3, pp. 4367–4378, 2021.

[77] G. He, W. Su, S. Gao, N. Liu, and S. K. Das, "NetChain: A Blockchain-Enabled Privacy-Preserving Multi-Domain Network Slice Orchestration Architecture," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 1, pp. 188–202, 2022.

[78] Z. Wang, B. Wen, and Z. Luo, "Towards on Blockchain Data Privacy Protection with Cryptography and Software Architecture Approach," in *Blockchain and Trustworthy Systems - Second International Conference, BlockSys 2020, Dali, China, August 6-7, 2020, Revised Selected Papers*, ser. Communications in Computer and Information Science, vol. 1267. Springer, 2020, pp. 205–217.

[79] P. R. Baranwal, "Blockchain Based Full Privacy Preserving Public Procurement," in *Blockchain - ICBC 2020 - Third International Conference, Held as Part of the Services Conference Federation, SCF 2020, Honolulu, HI, USA, September 18-20, 2020, Proceedings*, ser. Lecture Notes in Computer Science, vol. 12404. Springer, 2020, pp. 3–17.

[80] B. Liu, S. Xie, Y. Yang, R. Wang, and Y. Hong, "Privacy preserving divisible double auction with a hybridized TEE-blockchain system," *Cybersecur.*, vol. 4, no. 1, p. 37, 2021.

[81] S. A. K. Thyagarajan, G. Malavolta, and P. Moreno-Sanchez, "Universal Atomic Swaps: Secure Exchange of Coins Across All Blockchains," in *43rd IEEE Symposium on Security and Privacy, SP 2022, San Francisco, CA, USA, May 22-26, 2022*. IEEE, 2022, pp. 1299–1316.

[82] R. Xiao, W. Ren, T. Zhu, and K. R. Choo, "A Mixing Scheme Using a Decentralized Signature Protocol for Privacy Protection in Bitcoin Blockchain," *IEEE Trans. Dependable Secur. Comput.*, vol. 18, no. 4, pp. 1793–1803, 2021.

[83] H. Alasmary, A. Khormali, A. Anwar, J. Park, J. Choi, A. Abusnaina, A. Awad, D. Nyang, and A. Mohaisen, ",Analyzing and Detecting Emerging Internet of Things Malware: A Graph-Based Approach," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8977–8988, 2019.

[84] A. Mohaisen, O. Alrawi, and M. Mohaisen, "AMAL: High-fidelity, behavior-based automated malware analysis and classification," *Comput. Secur.*, vol. 52, pp. 251–266, 2015.

[85] A. Mohaisen and O. Alrawi, "Unveiling Zeus: automated classification of malware samples," in *22nd International World Wide Web Conference, WWW*. International World Wide Web Conferences Steering Committee / ACM, 2013, pp. 829–832.

[86] A. Mohaisen, A. G. West, A. Mankin, and O. Alrawi, "Chatter: Classifying malware families using system event ordering," in *IEEE Conference on Communications and Network Security, CNS 2014, San Francisco, CA, USA, October 29-31, 2014*. IEEE, 2014, pp. 283–291. [Online]. Available: https://doi.org/10.1109/CNS.2014.6997496

[87] S. Qiao, V. Madathil, and K. Anyanwu, "Integrating Group Signatures in Complex Decentralized Marketplace Transactions for Improved Buyer Privacy," in *IEEE International Conference on Blockchain, Blockchain 2022, Espoo, Finland, August 22-25, 2022*. IEEE, 2022, pp. 139–148.

[88] S. Banupriya, K. Kottursamy, and A. K. Bashir, "Privacy-preserving hierarchical deterministic key generation based on a lattice of rings in public blockchain," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2813–2825, 2021.

[89] Y. Song, F. Wei, K. Zhu, and Y. Zhu, "Anomaly Detection as a Service: An Outsourced Anomaly Detection Scheme for Blockchain in a Privacy-Preserving Manner," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 4, pp. 3794–3809, 2022.

[90] Z. Xu, M. Qi, Z. Wang, S. Wen, S. Chen, and Y. Xiang, "IB2P: An image-based privacy-preserving blockchain model for financial services," in *2021 IEEE International Conference on Blockchain, Blockchain 2021, Melbourne, Australia, December 6-8, 2021*. IEEE, 2021, pp. 552–558.

[91] I. Givargizov, "UNSTABLE FINANCIAL AND ECONOMIC FACTORS IN THE WORLD AND THEIR INFLUENCE ON THE DEVELOPMENT OF BLOCKCHAIN TECHNOLOGIES," *International Humanitarian University Herald. Economics and Management*, 2023.

[92] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "PrivChain: Provenance and Privacy Preservation in Blockchain enabled Supply Chains," in *IEEE International Conference on Blockchain, Blockchain 2022, Espoo, Finland, August 22-25, 2022*. IEEE, 2022, pp. 157–166.

[93] S. Sahai, N. Singh, and P. Dayama, "Enabling Privacy and Traceability in Supply Chains using Blockchain and Zero Knowledge Proofs," in *IEEE International Conference on Blockchain, Blockchain 2020, Rhodes, Greece, November 2-6, 2020*. IEEE, 2020, pp. 134–143.

[94] A. Shahzad, K. Zhang, and A. Gherbi, "Privacy-preserving smart grid traceability using blockchain over IoT connectivity," in *SAC '21: The 36th ACM/SIGAPP Symposium on Applied Computing, Virtual Event, Republic of Korea, March 22-26, 2021*. ACM, 2021, pp. 699–706.

[95] W. Shao, C. Jia, Y. Xu, K. Qiu, Y. Gao, and Y. He, "AttriChain: Decentralized traceable anonymous identities in privacy-preserving permissioned blockchain," *Comput. Secur.*, vol. 99, p. 102069, 2020.

[96] S. Ma, Y. Deng, D. He, J. Zhang, and X. Xie, "An Efficient NIZK Scheme for Privacy-Preserving Transactions Over Account-Model Blockchain," *IEEE Trans. Dependable Secur. Comput.*, vol. 18, no. 2, pp. 641–651, 2021.

[97] L. Liu, X. Li, M. H. Au, Z. Fan, and X. Meng, "Metadata Privacy Preservation for Blockchain-Based Healthcare Systems," in *Database Systems for Advanced Applications - 27th International Conference, DASFAA 2022, Virtual Event, April 11-14, 2022, Proceedings, Part I*, ser. Lecture Notes in Computer Science, vol. 13245. Springer, 2022, pp. 404–412.

[98] C. Zhang, L. Zhu, C. Xu, K. Sharif, R. Lu, and Y. Chen, "APPB: Anti-Counterfeiting and Privacy-Preserving Blockchain-Based Vehicle Supply Chains," *IEEE Trans. Veh. Technol.*, vol. 71, no. 12, pp. 13 152–13 164, 2022.

[99] C. Zha, H. Yin, and B. Yin, "Data Ownership Confirmation and Privacy-Free Search for Blockchain-Based Medical Data Sharing," in *Blockchain and Trustworthy Systems - Second International Conference, BlockSys 2020, Dali, China, August 6-7, 2020, Revised Selected Papers*, ser. Communications in Computer and Information Science, vol. 1267. Springer, 2020, pp. 619–632.

[100] S. Cao, J. Wang, X. Du, X. Zhang, and X. Qin, "CEPS: A Cross-Blockchain based Electronic Health Records Privacy-Preserving Scheme," in *2020 IEEE International Conference on Communications, ICC 2020, Dublin, Ireland, June 7-11, 2020*. IEEE, 2020, pp. 1–6.

[101] S. Chen, X. Fu, H. Si, Y. Wang, S. Gao, and C. Wang, "Blockchain for Health IoT: A privacy-preserving data sharing system," *Softw. Pract. Exp.*, vol. 52, no. 9, pp. 2026–2044, 2022.

[102] J. Liu, T. Liang, R. Sun, X. Du, and M. Guizani, "A Privacy-Preserving Medical Data Sharing Scheme Based on Consortium Blockchain," in *IEEE Global Communications Conference, GLOBECOM 2020, Virtual Event, Taiwan, December 7-11, 2020*. IEEE, 2020, pp. 1–6.

[103] L. Tan, K. Yu, N. Shi, C. Yang, W. Wei, and H. Lu, "Towards Secure and Privacy-Preserving Data Sharing for COVID-19 Medical Records:

A Blockchain-Empowered Approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 1, pp. 271–281, 2022.

[104] N. Naren, A. Tahiliani, V. Hassija, V. Chamola, S. S. Kanhere, and M. Guizani, "Privacy-Preserving and Incentivized Contact Tracing for COVID-19 Using Blockchain," *IEEE Internet Things Mag.*, vol. 4, no. 3, pp. 72–79, 2021.

[105] Z. Peng, C. Xu, H. Wang, J. Huang, J. Xu, and X. Chu, "P^{2}B-Trace: Privacy-Preserving Blockchain-based Contact Tracing to Combat Pandemics," in *SIGMOD '21: International Conference on Management of Data, Virtual Event, China, June 20-25, 2021*. ACM, 2021, pp. 2389–2393.

[106] M. F. Younis, W. Lalouani, N. Lasla, L. Emokpae, and M. Abdallah, "Blockchain-Enabled and Data-Driven Smart Healthcare Solution for Secure and Privacy-Preserving Data Access," *IEEE Syst. J.*, vol. 16, no. 3, pp. 3746–3757, 2022.

[107] S. Qahtan, K. Y. Sharif, A. A. Zaidan, H. A. Alsattar, O. S. Albahri, B. B. Zaidan, H. Zulzalil, M. H. Osman, A. H. Alamoodi, and R. T. Mohammed, "Novel Multi Security and Privacy Benchmarking Framework for Blockchain-Based IoT Healthcare Industry 4.0 Systems," *IEEE Trans. Ind. Informatics*, vol. 18, no. 9, pp. 6415–6423, 2022.

[108] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, "NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates," *Softw. Pract. Exp.*, vol. 52, no. 4, pp. 841–867, 2022.

[109] R. D. Garcia, G. S. Ramachandran, R. Jurdak, and J. Ueyama, "A Blockchain-based Data Governance with Privacy and Provenance: a case study for e-Prescription," in *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2022, Shanghai, China, May 2-5, 2022*. IEEE, 2022, pp. 1–5.

[110] G. Wu, S. Wang, Z. Ning, and J. Li, "Blockchain-Enabled Privacy-Preserving Access Control for Data Publishing and Sharing in the Internet of Medical Things," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8091–8104, 2022.

[111] S. A. Alansari, M. M. Badr, M. M. E. A. Mahmoud, W. Alasmary, F. Alsolami, and A. M. Ali, "Efficient and Privacy-Preserving Infection Control System for Covid-19-Like Pandemics Using Blockchain," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2744–2760, 2022.

[112] Y. Qu, S. Chen, L. Gao, L. Cui, K. Sood, and S. Yu, "Personalized Privacy-Preserving Medical Data Sharing for Blockchain-based Smart Healthcare Networks," in *IEEE International Conference on Communications, ICC 2022, Seoul, Korea, May 16-20, 2022*. IEEE, 2022, pp. 4229–4234.

[113] T. Constantinides and J. Cartlidge, "Block Auction: A General Blockchain Protocol for Privacy-Preserving and Verifiable Periodic Double Auctions," in *2021 IEEE International Conference on Blockchain, Blockchain 2021, Melbourne, Australia, December 6-8, 2021*. IEEE, 2021, pp. 513–520.

[114] S. Thakur, J. G. Breslin, and S. Malik, "Privacy-Preserving Energy Trade Using Double Auction in Blockchain Offline Channels," in *Blockchain and Applications, 4th International Congress, BLOCKCHAIN 2022, L'Aquila, Italy, 13-15 July 2022*, ser. Lecture Notes in Networks and Systems, vol. 595. Springer, 2022, pp. 289–302.

[115] K. Qin, L. Zhou, and A. Gervais, "Quantifying Blockchain Extractable Value: How dark is the forest?" in *43rd IEEE Symposium on Security and Privacy, SP 2022, San Francisco, CA, USA, May 22-26, 2022*. IEEE, 2022, pp. 198–214.

[116] E. Erdin, M. Cebe, K. Akkaya, E. Bulut, and A. S. Uluagac, "A Heuristic-Based Private Bitcoin Payment Network Formation Using Off-Chain Links," in *IEEE International Conference on Blockchain, Blockchain 2019, Atlanta, GA, USA, July 14-17, 2019*. IEEE, 2019, pp. 294–301.

[117] P. M. Shelke, R. Mirajkar, S. Dedgaonkar, R. N. Bhimanpallewar, C. Shewale, and S. Kadam, "Enhancing Auction Systems with Blockchain Technology," *International Journal on Recent and Innovation Trends in Computing and Communication*, 2023.

[118] S. Chaisawat and C. Vorakulpipat, "Towards Achieving Personal Privacy Protection and Data Security on Integrated E-Voting Model of Blockchain and Message Queue," *Secur. Commun. Networks*, vol. 2021, pp. 8 338 616:1–8 338 616:14, 2021.

[119] T. D. T. Nguyen and M. T. Thai, "zVote: A Blockchain-based Privacy-preserving Platform for Remote E-voting," in *IEEE International Conference on Communications, ICC 2022, Seoul, Korea, May 16-20, 2022*. IEEE, 2022, pp. 4745–4750.

[120] M. D. Firoozjaei, R. Lu, and A. A. Ghorbani, "An evaluation framework for privacy-preserving solutions applicable for blockchain-based internet-of-things platforms," *Secur. Priv.*, vol. 3, no. 6, 2020.

[121] J. Huang, D. He, Y. Chen, M. K. Khan, and M. Luo, "A Blockchain-Based Self-Tallying Voting Protocol With Maximum Voter Privacy," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 5, pp. 3808–3820, 2022.

[122] L. Jin, S. Hao, Y. Huang, H. Wang, and C. Cotton, "DNSonChain: Delegating Privacy-Preserved DNS Resolution to Blockchain," in *29th IEEE International Conference on Network Protocols, ICNP 2021, Dallas, TX, USA, November 1-5, 2021*. IEEE, 2021, pp. 1–11.

[123] A. S. Yahaya, N. Javaid, R. Khalid, M. Imran, and M. Guizani, "A Blockchain-based Privacy-Preserving Mechanism with Aggregator as Common Communication Point," in *2020 IEEE International Conference on Communications, ICC 2020, Dublin, Ireland, June 7-11, 2020*. IEEE, 2020, pp. 1–6.

[124] V. Neziri, I. Shabani, R. Dervishi, and B. Rexha, "Assuring Anonymity and Privacy in Electronic Voting with Distributed Technologies Based on Blockchain," *Applied Sciences*, 2022.

[125] D. Hou, J. Zhang, S. Huang, Z. Peng, J. Ma, and X. Zhu, "Privacy-Preserving Energy Trading Using Blockchain and Zero Knowledge Proof," in *IEEE International Conference on Blockchain, Blockchain 2022, Espoo, Finland, August 22-25, 2022*. IEEE, 2022, pp. 412–418.

[126] S. Jiang, X. Zhang, J. Li, H. Yue, and Y. Zhou, "Secure and Privacy-preserving Energy Trading Scheme based on Blockchain," in *IEEE Global Communications Conference, GLOBECOM 2020, Virtual Event, Taiwan, December 7-11, 2020*. IEEE, 2020, pp. 1–6.

[127] A. S. Yahaya, N. Javaid, R. Khalid, M. Imran, and N. Naseer, "A Blockchain based Privacy-Preserving System for Electric Vehicles through Local Communication," in *2020 IEEE International Conference on Communications, ICC 2020, Dublin, Ireland, June 7-11, 2020*. IEEE, 2020, pp. 1–6.

[128] X. Zhang, S. Jiang, Y. Liu, T. Jiang, and Y. Zhou, "Privacy-Preserving Scheme With Account-Mapping and Noise-Adding for Energy Trading Based on Consortium Blockchain," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 1, pp. 569–581, 2022.

[129] T. Chang and D. Svetinovic, "Improving Bitcoin Ownership Identification Using Transaction Patterns Analysis," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 50, no. 1, pp. 9–20, 2020.

[130] Y. Qu, L. Gao, T. H. Luan, Y. Xiang, S. Yu, B. Li, and G. Zheng, "Decentralized Privacy Using Blockchain-Enabled Federated Learning in Fog Computing," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5171–5183, 2020.

[131] T. Crain, C. Natoli, and V. Gramoli, "Red Belly: A Secure, Fair and Scalable Open Blockchain," in *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*. IEEE, 2021, pp. 466–483.

[132] Y. Liu, Z. Xiong, Q. Hu, D. Niyato, J. Zhang, C. Miao, C. Leung, and Z. Tian, "VRepChain: A Decentralized and Privacy-Preserving Reputation System for Social Internet of Vehicles Based on Blockchain," *IEEE Trans. Veh. Technol.*, vol. 71, no. 12, pp. 13 242–13 253, 2022.

[133] Z. Wan, T. Zhang, W. Liu, M. Wang, and L. Zhu, "Decentralized Privacy-Preserving Fair Exchange Scheme for V2G Based on Blockchain," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 4, pp. 2442–2456, 2022.

[134] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy," *J. Parallel Distributed Comput.*, vol. 164, pp. 152–167, 2022.

[135] M. Xu, Z. Zou, Y. Cheng, Q. Hu, D. Yu, and X. Cheng, "SPDL: A Blockchain-Enabled Secure and Privacy-Preserving Decentralized Learning System," *IEEE Trans. Computers*, vol. 72, no. 2, pp. 548–558, 2023.

[136] M. Saad, L. Njilla, C. A. Kamhoua, and A. Mohaisen, "Countering Selfish Mining in Blockchains," in *International Conference on Computing, Networking and Communications, ICNC 2019, Honolulu, HI, USA, February 18-21, 2019*. IEEE, 2019, pp. 360–364.

[137] M. Saad, J. Kim, D. Nyang, and D. Mohaisen, "Contra-$_*$: Mechanisms for countering spam attacks on blockchain's memory pools," *J. Netw. Comput. Appl.*, vol. 179, p. 102971, 2021.

[138] T. Rajab, A. A. Khalil, M. H. Manshaei, M. A. Rahman, M. Dakhilalian, M. Ngouen, M. Jadliwala, and A. S. Uluagac, "Feasibility Analysis for Sybil Attacks in Shard-Based Permissionless Blockchains," *Distributed Ledger Technol. Res. Pract.*, vol. 2, no. 4, pp. 1–21, 2023.

[139] M. Saad, V. Cook, L. N. Nguyen, M. T. Thai, and A. Mohaisen, "Partitioning Attacks on Bitcoin: Colliding Space, Time, and Logic," in *39th IEEE International Conference on Distributed Computing Systems, ICDCS 2019, Dallas, TX, USA, July 7-10, 2019*. IEEE, 2019, pp. 1175–1187.

[140] M. Saad, A. Anwar, S. Ravi, and D. Mohaisen, "Revisiting Nakamoto Consensus in Asynchronous Networks: A Comprehensive Analysis of Bitcoin Safety and ChainQuality," in *CCS '21: 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, Republic of Korea, November 15 - 19, 2021*. ACM, 2021, pp. 988–1005.

[141] M. Saad, S. Chen, and D. Mohaisen, "Root Cause Analyses for the Deteriorating Bitcoin Network Synchronization," in *41st IEEE International Conference on Distributed Computing Systems, ICDCS 2021, Washington DC, USA, July 7-10, 2021*. IEEE, 2021, pp. 239–249.

[142] ——, "SyncAttack: Double-spending in Bitcoin Without Mining Power," in *CCS '21: 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, Republic of Korea, November 15 - 19, 2021*. ACM, 2021, pp. 1668–1685.

[143] M. Saad and D. Mohaisen, "Three Birds with One Stone: Efficient Partitioning Attacks on Interdependent Cryptocurrency Networks," in *44th IEEE Symposium on Security and Privacy, SP 2023, San Francisco, CA, USA, May 21-25, 2023*. IEEE, 2023, pp. 111–125.

[144] M. Saad, V. Cook, L. N. Nguyen, M. T. Thai, and D. Mohaisen, "Exploring Partitioning Attacks on the Bitcoin Network," *IEEE/ACM Trans. Netw.*, vol. 30, no. 1, pp. 202–214, 2022.

[145] W. Tushar, C. Yuen, H. M. Rad, T. K. Saha, H. V. Poor, and K. L. Wood, "Transforming Energy Networks via Peer-to-Peer Energy Trading: The Potential of Game-Theoretic Approaches," *IEEE Signal Process. Mag.*, vol. 35, no. 4, pp. 90–111, 2018.

[146] Y. Wu, Y. Wu, J. M. Guerrero, and J. C. Vasquez, "Decentralized transactive energy community in edge grid with positive buildings and interactive electric vehicles," *International Journal of Electrical Power & Energy Systems*, vol. 135, p. 107510, 2022.

[147] Z. Shi, C. de Laat, P. Grosso, and Z. Zhao, ",Integration of Blockchain and Auction Models: A Survey, Some Applications, and Challenges," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 1, pp. 497–537, 2023.

[148] S. Wu, Y. Chen, Q. Wang, M. Li, C. Wang, and X. Luo, "CReam: A Smart Contract Enabled Collusion-Resistant e-Auction," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 7, pp. 1687–1701, 2019.

[149] D. Gabay, K. Akkaya, and M. Cebe, "Privacy-Preserving Authentication Scheme for Connected Electric Vehicles Using Blockchain and Zero Knowledge Proofs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5760–5772, 2020.

[150] W. Li, L. Chen, X. Lai, X. Zhang, and J. Xin, "BPCEX: Towards Blockchain-based Privacy-preserving Currency Exchange," in *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2020, Toronto, ON, Canada, May 2-6, 2020*. IEEE, 2020, pp. 1–9.

[151] X. Liu, H. Huang, F. Xiao, and Z. Ma, "A Blockchain-Based Trust Management With Conditional Privacy-Preserving Announcement Scheme for VANETs," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4101–4112, 2020.

[152] J. E. Simões, E. Ferreira, D. S. Menasché, and C. A. V. Campos, "Blockchain Privacy Through Merge Avoidance and Mixing Services: a Hardness and an Impossibility Result," *SIGMETRICS Perform. Evaluation Rev.*, vol. 48, no. 4, pp. 8–11, 2021.

[153] S. Avizheh, M. Nabi, S. Rahman, S. Sharifian, and R. Safavi-Naini, "Privacy-Preserving Resource Sharing Using Permissioned Blockchains - (The Case of Smart Neighbourhood)," in *Financial Cryptography and Data Security. FC 2021 International Workshops - CoDecFin, DeFi, VOTING, and WTSC, Virtual Event, March 5, 2021, Revised Selected Papers*, ser. Lecture Notes in Computer Science, vol. 12676. Springer, 2021, pp. 482–504.

[154] W. Lu, Z. Ren, J. Xu, and S. Chen, "Edge Blockchain Assisted Lightweight Privacy-Preserving Data Aggregation for Smart Grid," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 2, pp. 1246–1259, 2021.

[155] G. Almashaqbeh and R. Solomon, "SoK: Privacy-Preserving Computing in the Blockchain Era," in *7th IEEE European Symposium on Security and Privacy, EuroS&P 2022, Genoa, Italy, June 6-10, 2022*. IEEE, 2022, pp. 124–139.

[156] T. Hardin and D. Kotz, "Amanuensis: provenance, privacy, and permission in TEE-enabled blockchain data systems," in *42nd IEEE International Conference on Distributed Computing Systems, ICDCS 2022, Bologna, Italy, July 10-13, 2022*. IEEE, 2022, pp. 144–156.

[157] S. Gao, Q. Su, R. Zhang, J. Zhu, Z. Sui, and J. Wang, "A Privacy-Preserving Identity Authentication Scheme Based on the Blockchain," *Secur. Commun. Networks*, vol. 2021, pp. 9 992 353:1–9 992 353:10, 2021.

[158] L. Xu, L. Chen, Z. Gao, K. Kasichainula, M. Fernandez, B. Carbunar, and W. Shi, "PrivateEx: privacy preserving exchange of crypto-assets on blockchain," in *SAC '20: The 35th ACM/SIGAPP Symposium on Applied Computing, online event, [Brno, Czech Republic], March 30 - April 3, 2020*. ACM, 2020, pp. 316–323.

[159] J. Chen, Y. Wang, Y. Zhou, W. Ding, Y. Tang, X. Wang, and K. Li, "Understanding the Security Risks of Decentralized Exchanges by Uncovering Unfair Trades in the Wild," in *8th IEEE European Symposium on Security and Privacy, EuroS&P*. IEEE, 2023, pp. 332–351.

[160] R. D. Garcia, G. S. Ramachandran, R. Jurdak, and J. Ueyama, "Blockchain-Aided and Privacy-Preserving Data Governance in Multi-Stakeholder Applications," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 4, pp. 3781–3793, 2022.

[161] E. Androulaki, J. Camenisch, A. D. Caro, M. Dubovitskaya, K. Elkhiyaoui, and B. Tackmann, "Privacy-preserving auditable token payments in a permissioned blockchain system," in *AFT '20: 2nd ACM Conference on Advances in Financial Technologies, New York, NY, USA, October 21-23, 2020*. ACM, 2020, pp. 255–267.

[162] V. Vasylkovskyi, S. Guerreiro, and J. S. Sequeira, "BlockRobot: Increasing Privacy in Human Robot Interaction by Using Blockchain," in *IEEE International Conference on Blockchain, Blockchain 2020, Rhodes, Greece, November 2-6, 2020*. IEEE, 2020, pp. 106–115.

[163] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT," *IEEE Trans. Ind. Informatics*, vol. 16, no. 6, pp. 4177–4186, 2020.

[164] P. A. Krishnamoorthi, S. Shahid, and O. Boydell, "Preserving Privacy in Private Blockchain Networks," in *Blockchain - ICBC 2021 - 4th International Conference, Held as Part of the Services Conference Federation, SCF 2021, Virtual Event, December 10-14, 2021, Proceedings*, ser. Lecture Notes in Computer Science, vol. 12991. Springer, 2021, pp. 118–128.

[165] Q. Kong, L. Su, and M. Ma, "Achieving Privacy-Preserving and Verifiable Data Sharing in Vehicular Fog With Blockchain," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 4889–4898, 2021.

[166] R. Bosri, M. S. Rahman, M. Z. A. Bhuiyan, and A. A. Omar, "Integrating Blockchain With Artificial Intelligence for Privacy-Preserving Recommender Systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1009–1018, 2021.

[167] W. Liu, Z. Wan, J. Shao, and Y. Yu, "HyperMaze: Towards Privacy-Preserving and Scalable Permissioned Blockchain," *IEEE Trans. Dependable Secur. Comput.*, vol. 20, no. 1, pp. 360–376, 2023.

[168] Z. Huang, J. Zheng, and M. Xiao, "Privacy-Enhanced Crowdsourcing Data Trading based on Blockchain and Stackelberg Game," in *IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems, MASS 2021, Denver, CO, USA, October 4-7, 2021*. IEEE, 2021, pp. 621–626.

[169] R. Cong, Y. Liu, K. Tago, R. Li, H. Asaeda, and Q. Jin, "Individual-Initiated Auditable Access Control for Privacy-Preserved IoT Data Sharing with Blockchain," in *IEEE International Conference on Communications Workshops, ICC Workshops 2021, Montreal, QC, Canada, June 14-23, 2021*. IEEE, 2021, pp. 1–6.

[170] P. V. Klaine, L. Zhang, B. Zhou, Y. Sun, H. Xu, and M. A. Imran, "Privacy-Preserving Contact Tracing and Public Risk Assessment Using Blockchain for COVID-19 Pandemic," *IEEE Internet Things Mag.*, vol. 3, no. 3, pp. 58–63, 2020.

[171] H. An and J. Chen, "ExamChain: A Privacy-Preserving Onscreen Marking System Based on Consortium Blockchain," *IEICE Trans. Inf. Syst.*, vol. 105-D, no. 2, pp. 235–247, 2022.

[172] Y. Pan, Y. Zhao, X. Liu, G. Wang, and M. Su, "FPLotto: A fair blockchain-based lottery scheme for privacy protection," in *IEEE International Conference on Blockchain, Blockchain 2022, Espoo, Finland, August 22-25, 2022*. IEEE, 2022, pp. 21–28.

[173] L. Wang, X. Lin, E. V. Zima, and C. Ma, "Towards Airbnb-Like Privacy-Enhanced Private Parking Spot Sharing Based on Blockchain," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 2411–2423, 2020.

[174] Q. Kong, R. Lu, F. Yin, and S. Cui, "Blockchain-Based Privacy-Preserving Driver Monitoring for MaaS in the Vehicular IoT," *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3788–3799, 2021.

[175] J. Passerat-Palmbach, T. Farnan, M. McCoy, J. D. Harris, S. T. Manion, H. L. Flannery, and B. Gleim, "Blockchain-orchestrated machine learning for privacy-preserving federated learning in electronic health data," in *IEEE International Conference on Blockchain, Blockchain 2020, Rhodes, Greece, November 2-6, 2020*. IEEE, 2020, pp. 550–555.

[176] S. Hu, J. Li, C. Zhang, Q. Zhao, and W. Ye, "The Blockchain-Based Edge Computing Framework for Privacy-Preserving Federated Learning," in *2021 IEEE International Conference on Blockchain, Blockchain 2021, Melbourne, Australia, December 6-8, 2021*. IEEE, 2021, pp. 566–571.

[177] Y. Miao, Z. Liu, H. Li, K. R. Choo, and R. H. Deng, "Privacy-Preserving Byzantine-Robust Federated Learning via Blockchain Systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 2848–2861, 2022.

[178] S. Bai, G. Yang, G. Liu, H. Dai, and C. Rong, "NttpFL: Privacy-Preserving Oriented No Trusted Third Party Federated Learning System Based on Blockchain," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 4, pp. 3750–3763, 2022.

[179] Y. Guo, H. Xie, Y. Miao, C. Wang, and X. Jia, "FedCrowd: A Federated and Privacy-Preserving Crowdsourcing Platform on Blockchain," *IEEE Trans. Serv. Comput.*, vol. 15, no. 4, pp. 2060–2073, 2022.

[180] F. Yang, Y. Qiao, M. Z. Abedin, and C. Huang, "Privacy-Preserved Credit Data Sharing Integrating Blockchain and Federated Learning for Industrial 4.0," *IEEE Trans. Ind. Informatics*, vol. 18, no. 12, pp. 8755–8764, 2022.

[181] Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, and Y. Liu, "Correction to "Privacy-Preserving Blockchain-Based Federated Learning for IoT Devices"," *IEEE Internet Things J.*, vol. 10, no. 1, p. 973, 2023.

[182] J. A. A. Alzubi, O. A. Alzubi, A. Singh, and M. Ramachandran, "Cloud-IIoT-Based Electronic Health Record Privacy-Preserving by CNN and Blockchain-Enabled Federated Learning," *IEEE Trans. Ind. Informatics*, vol. 19, no. 1, pp. 1080–1087, 2023.

[183] S. A. K. Thyagarajan and G. Malavolta, "Lockable Signatures for Blockchains: Scriptless Scripts for All Signatures," in *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*. IEEE, 2021, pp. 937–954.

[184] M. Baza, N. Lasla, M. M. E. A. Mahmoud, G. Srivastava, and M. Abdallah, "B-Ride: Ride Sharing With Privacy-Preservation, Trust and Fair Payment Atop Public Blockchain," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1214–1229, 2021.

[185] S. Xu, X. Cai, Y. Zhao, Z. Ren, L. Du, Q. Wang, and J. Zhou, "zkrpChain: Towards multi-party privacy-preserving data auditing for consortium blockchains based on zero-knowledge range proofs," *Future Gener. Comput. Syst.*, vol. 128, pp. 490–504, 2022.

[186] Z. Liu, C. Hu, H. Xia, T. Xiang, B. Wang, and J. Chen, "SPDTS: A Differential Privacy-Based Blockchain Scheme for Secure Power Data Trading," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 4, pp. 5196–5207, 2022.

[187] J. Zhao, H. Huang, C. Gu, Z. Hua, and X. Zhang, "Blockchain-Assisted Conditional Anonymity Privacy-Preserving Public Auditing Scheme With Reward Mechanism," *IEEE Syst. J.*, vol. 16, no. 3, pp. 4477–4488, 2022.

[188] W. Lv, S. Wu, C. Jiang, Y. Cui, X. Qiu, and Y. Zhang, "Towards Large-Scale and Privacy-Preserving Contact Tracing in COVID-19 Pandemic: A Blockchain Perspective," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 1, pp. 282–298, 2022.

[189] A. Biryukov and S. Tikhomirov, "Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis," in *IEEE European Symposium on Security and Privacy, EuroS&P 2019, Stockholm, Sweden, June 17-19, 2019*. IEEE, 2019, pp. 172–184.

[190] T. Li, H. Wang, D. He, and J. Yu, "Blockchain-Based Privacy-Preserving and Rewarding Private Data Sharing for IoT," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 15 138–15 149, 2022.

[191] L. M. Han, Y. Zhao, and J. Zhao, "POSTER: Blockchain-Based Differential Privacy Cost Management System," in *ASIA CCS '20: The 15th ACM Asia Conference on Computer and Communications Security, Taipei, Taiwan, October 5-9, 2020*. ACM, 2020, pp. 925–927.

[192] X. Liu, P. Zhou, T. Qiu, and D. O. Wu, "Blockchain-Enabled Contextual Online Learning Under Local Differential Privacy for Coronary Heart Disease Diagnosis in Mobile Edge Computing," *IEEE J. Biomed. Health Informatics*, vol. 24, no. 8, pp. 2177–2188, 2020.

[193] Y. Zhao, J. Zhao, J. Kang, Z. Zhang, D. Niyato, S. Shi, and K. Lam, "A Blockchain-Based Approach for Saving and Tracking Differential-Privacy Cost," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8865–8882, 2021.

[194] D. Wei, N. Xi, J. Ma, and J. Li, "Protecting Your Offloading Preference: Privacy-aware Online Computation Offloading in Mobile Blockchain," in *29th IEEE/ACM International Symposium on Quality of Service, IWQOS 2021, Tokyo, Japan, June 25-28, 2021*. IEEE, 2021, pp. 1–10.

[195] H. Yang, J. Shen, J. Lu, T. Zhou, X. Xia, and S. Ji, "A Privacy-Preserving Data Transmission Scheme Based on Oblivious Transfer and Blockchain Technology in the Smart Healthcare," *Secur. Commun. Networks*, vol. 2021, pp. 5 781 354:1–5 781 354:12, 2021.

[196] Y. Yang, J. Wu, C. Long, W. Liang, and Y. Lin, "Blockchain-Enabled Multiparty Computation for Privacy Preserving and Public Audit in Industrial IoT," *IEEE Trans. Ind. Informatics*, vol. 18, no. 12, pp. 9259–9267, 2022.

[197] Z. Guan, X. Zhou, P. Liu, L. Wu, and W. Yang, "A Blockchain-Based Dual-Side Privacy-Preserving Multiparty Computation Scheme for Edge-Enabled Smart Grid," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14 287–14 299, 2022.

[198] O. G. Bautista, M. H. Manshaei, R. Hernandez, K. Akkaya, S. Homsi, and A. S. Uluagac, "MPC-ABC: Blockchain-Based Network Communication for Efficiently Secure Multiparty Computation," *J. Netw. Syst. Manag.*, vol. 31, no. 4, p. 68, 2023.

[199] F. Zhang, W. He, R. Cheng, J. Kos, N. Hynes, N. M. Johnson, A. Juels, A. Miller, and D. Song, "The Ekiden Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts," *IEEE Secur. Priv.*, vol. 18, no. 3, pp. 17–27, 2020.

[200] I. Bentov, Y. Ji, F. Zhang, L. Breidenbach, P. Daian, and A. Juels, "Tesseract: Real-Time Cryptocurrency Exchange Using Trusted Hardware," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, London, UK, November 11-15, 2019*. ACM, 2019, pp. 1521–1538.

[201] E. Cecchetti, F. Zhang, Y. Ji, A. E. Kosba, A. Juels, and E. Shi, "Solidus: Confidential Distributed Ledger Transactions via PVORM," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*. ACM, 2017, pp. 701–717.

[202] C. Guo, J. Katz, X. Wang, and Y. Yu, "Efficient and Secure Multiparty Computation from Fixed-Key Block Ciphers," in *2020 IEEE Symposium on Security and Privacy, SP 2020, San Francisco, CA, USA, May 18-21, 2020*. IEEE, 2020, pp. 825–841.

[203] R. Zhu, C. Ding, and Y. Huang, "Efficient Publicly Verifiable 2PC over a Blockchain with Applications to Financially-Secure Computations," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, London, UK, November 11-15, 2019*. ACM, 2019, pp. 633–650.

[204] H. Zhong, Y. Sang, Y. Zhang, and Z. Xi, "Secure Multi-Party Computation on Blockchain: An Overview," in *Parallel Architectures, Algorithms and Programming - 10th International Symposium, PAAP 2019, Guangzhou, China, December 12-14, 2019, Revised Selected Papers*, ser. Communications in Computer and Information Science, vol. 1163. Springer, 2019, pp. 452–460.

[205] F. Ganji, S. Tajik, D. Forte, and J. Seifert, "Blockchain-enabled Cryptographically-secure Hardware Obfuscation," *IACR Cryptol. ePrint Arch.*, p. 928, 2019.

[206] J. Liu, K. Fan, H. Li, and Y. Yang, "A blockchain-based privacy preservation scheme in multimedia network," *Multim. Tools Appl.*, vol. 80, no. 20, pp. 30 691–30 705, 2021.

[207] C. Lin, D. He, X. Huang, N. Kumar, and K. R. Choo, "BCPPA: A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 12, pp. 7408–7420, 2021.

[208] Y. Zhang, B. Li, J. Wu, B. Liu, R. Chen, and J. Chang, "Efficient and Privacy-Preserving Blockchain-Based Multifactor Device Authentication Protocol for Cross-Domain IIoT," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22 501–22 515, 2022.

[209] Y. Zhao, X. Yang, Y. Yu, B. Qin, X. Du, and M. Guizani, "Blockchain-Based Auditable Privacy-Preserving Data Classification for Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2468–2484, 2022.

[210] H. Ghayvat, S. Pandya, P. Bhattacharya, M. Zuhair, M. Rashid, S. Hakak, and K. Dev, "CP-BDHCA: Blockchain-Based Confidentiality-Privacy Preserving Big Data Scheme for Healthcare Clouds and Applications," *IEEE J. Biomed. Health Informatics*, vol. 26, no. 5, pp. 1937–1948, 2022.

[211] D. Zonda and M. Meddeb, "Proxy re-encryption for privacy enhancement in Blockchain: Carpooling use case," in *IEEE International Conference on Blockchain, Blockchain 2020, Rhodes, Greece, November 2-6, 2020*. IEEE, 2020, pp. 482–489.

[212] J. Feng, L. T. Yang, R. Zhang, and B. S. Gavuna, "Privacy-Preserving Tucker Train Decomposition Over Blockchain-Based Encrypted Industrial IoT Data," *IEEE Trans. Ind. Informatics*, vol. 17, no. 7, pp. 4904–4913, 2021.

[213] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "DeepChain: Auditable and Privacy-Preserving Deep Learning with Blockchain-Based Incentive," *IEEE Trans. Dependable Secur. Comput.*, vol. 18, no. 5, pp. 2438–2455, 2021.

[214] Z. Geng, Y. He, C. Wang, G. Xu, K. Xiao, and S. Yu, "A Blockchain based Privacy-Preserving Reputation Scheme for Cloud Service," in *ICC 2021 - IEEE International Conference on Communications, Montreal, QC, Canada, June 14-23, 2021*. IEEE, 2021, pp. 1–6.

[215] Z. Lv, L. Qiao, M. S. Hossain, and B. J. Choi, "Analysis of Using Blockchain to Protect the Privacy of Drone Big Data," *IEEE Netw.*, vol. 35, no. 1, pp. 44–49, 2021.

[216] J. Li, S. Li, L. Cheng, Q. Liu, J. Pei, and S. Wang, "BSAS: A Blockchain-Based Trustworthy and Privacy-Preserving Speed Advisory System," *IEEE Trans. Veh. Technol.*, vol. 71, no. 11, pp. 11 421–11 430, 2022.

[217] T. Li, W. Liu, S. Xie, M. Dong, K. Ota, N. N. Xiong, and Q. Li, "BPT: A Blockchain-Based Privacy Information Preserving System for Trust Data Collection Over Distributed Mobile-Edge Network," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8036–8052, 2022.

[218] Y. Xiao, N. Zhang, J. Li, W. Lou, and Y. T. Hou, "PrivacyGuard: Enforcing Private Data Usage Control with Blockchain and Attested Off-Chain Contract Execution," in *Computer Security - ESORICS 2020 - 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14-18, 2020, Proceedings, Part II*, ser. Lecture Notes in Computer Science, vol. 12309. Springer, 2020, pp. 610–629.

[219] D. Liu, C. Huang, J. Ni, X. Lin, and X. Shen, "Blockchain-Based Smart Advertising Network With Privacy-Preserving Accountability," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2118–2130, 2021.

[220] D. Lee and M. Song, "MEXchange: A Privacy-Preserving Blockchain-Based Framework for Health Information Exchange Using Ring Signature and Stealth Address," *IEEE Access*, vol. 9, pp. 158 122–158 139, 2021.

[221] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, "On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance," *Comput. Networks*, vol. 191, p. 108005, 2021.

[222] C. Stach, C. Gritti, D. Przytarski, and B. Mitschang, "Can blockchains and data privacy laws be reconciled?: a fundamental study of how privacy-aware blockchains are feasible," in *SAC '22: The 37th ACM/SIGAPP Symposium on Applied Computing, Virtual Event, April 25 - 29, 2022*. ACM, 2022, pp. 1218–1227.

[223] D. Lee and N. Park, "Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree," *Multim. Tools Appl.*, vol. 80, no. 26, pp. 34 517–34 534, 2021.

[224] C. Pighini, A. Vezzoni, S. Mainini, A. G. Migliavacca, A. Montanari, M. R. Guarneri, E. G. Caiani, and A. Cesareo, "SynCare: An Innovative Remote Patient Monitoring System Secured by Cryptography and Blockchain," in *Privacy and Identity Management. Between Data Protection and Security - 16th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Privacy and Identity 2021, Virtual Event, August 16-20, 2021, Revised Selected Papers*, ser. IFIP Advances in Information and Communication Technology, vol. 644. Springer, 2021, pp. 73–89.

[225] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses," *ACM Comput. Surv.*, vol. 53, no. 3, pp. 67:1–67:43, 2021.

[226] M. Tran, I. Choi, G. J. Moon, A. V. Vu, and M. S. Kang, "A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network," in *2020 IEEE Symposium on Security and Privacy, SP 2020, San Francisco, CA, USA, May 18-21, 2020*. IEEE, 2020, pp. 894–909.

[227] M. Tran, A. Shenoi, and M. S. Kang, "On the Routing-Aware Peering against Network-Eclipse Attacks in Bitcoin," in *30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021*. USENIX Association, 2021, pp. 1253–1270.

[228] J. Ha, S. Baek, M. Tran, and M. S. Kang, "On the Sustainability of Bitcoin Partitioning Attacks," in *Financial Cryptography and Data Security - 27th International Conference, FC 2023, Bol, Brač, Croatia, May 1-5, 2023, Revised Selected Papers, Part II*, ser. Lecture Notes in Computer Science, vol. 13951. Springer, 2023, pp. 166–181.

[229] H. Heo, S. Woo, T. Yoon, M. S. Kang, and S. Shin, "Partitioning Ethereum without Eclipsing It," in *30th Annual Network and Distributed System Security Symposium, NDSS 2023, San Diego, California, USA, February 27 - March 3, 2023*. The Internet Society, 2023.

[230] S. Baek, H. Nam, Y. Oh, M. Tran, and M. S. Kang, "Short Paper: On the Claims of Weak Block Synchronization in Bitcoin," in *Financial Cryptography and Data Security - 26th International Conference, FC 2022, Grenada, May 2-6, 2022, Revised Selected Papers*, ser. Lecture Notes in Computer Science, vol. 13411. Springer, 2022, pp. 663–671.

[231] Y. Sun, M. Apostolaki, H. Birge-Lee, L. Vanbever, J. Rexford, M. Chiang, and P. Mittal, "Securing internet applications from routing attacks," *Commun. ACM*, vol. 64, no. 6, pp. 86–96, 2021.

[232] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies," in *2017 IEEE Symposium on Security and Privacy, SP 2017, San Jose, CA, USA, May 22-26, 2017*. IEEE Computer Society, 2017, pp. 375–392.

[233] M. Apostolaki, G. Marti, J. Müller, and L. Vanbever, "SABRE: Protecting Bitcoin against Routing Attacks," in *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*. The Internet Society, 2019.

[234] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse Attacks on Bitcoin's Peer-to-Peer Network," in *24th USENIX Security Symposium, USENIX Security 15, Washington, D.C., USA, August 12-14, 2015*. USENIX Association, 2015, pp. 129–144.

[235] B. Alangot, D. Reijsbergen, S. Venugopalan, and P. Szalachowski, "Decentralized Lightweight Detection of Eclipse Attacks on Bitcoin Clients," in *IEEE International Conference on Blockchain, Blockchain 2020, Rhodes, Greece, November 2-6, 2020*. IEEE, 2020, pp. 337–342.

[236] E. Heilman, "Mirror worlds, eclipse attacks and the security of Bitcoin and the RPKI," Ph.D. dissertation, Boston University, USA, 2022.

[237] H. Wu, B. Düdder, L. Wang, S. Sun, and G. Xue, "Blockchain-Based Reliable and Privacy-Aware Crowdsourcing With Truth and Fairness Assurance," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3586–3598, 2022.

[238] M. Saad, L. Njilla, C. A. Kamhoua, J. Kim, D. Nyang, and A. Mohaisen, "Mempool optimization for Defending Against DDoS Attacks in PoW-based Blockchain Systems," in *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2019, Seoul, Korea (South), May 14-17, 2019*. IEEE, 2019, pp. 285–292.

[239] M. Saad, M. T. Thai, and A. Mohaisen, "POSTER: Deterring DDoS Attacks on Blockchain-based Cryptocurrencies through Mempool Optimization," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security, AsiaCCS 2018, Incheon, Republic of Korea, June 04-08, 2018*. ACM, 2018, pp. 809–811.

[240] B. Chen, L. Wu, H. Wang, L. Zhou, and D. He, "A Blockchain-Based Searchable Public-Key Encryption With Forward and Backward Privacy for Cloud-Assisted Vehicular Social Networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5813–5825, 2020.

[241] C. Huang, Y. Zhao, H. Chen, X. Wang, Q. Zhang, Y. Chen, H. Wang, and K. Lam, "ZkRep: A Privacy-Preserving Scheme for Reputation-Based Blockchain System," *IEEE Internet Things J.*, vol. 9, no. 6, pp. 4330–4342, 2022.

[242] Y. Wang, W. Ding, K. Li, and Y. Tang, "Understanding Ethereum Mempool Security under Asymmetric DoS by Symbolic Fuzzing," *CoRR*, vol. abs/2312.02642, 2023.

[243] Y. Sharma and B. Balusamy, "A Novel Approach for Privacy Preservation in Blockchain Network Using Tensor Product and a Hybrid Swarm Intelligence," *Int. J. Mob. Comput. Multim. Commun.*, vol. 12, no. 4, pp. 52–71, 2021.

[244] M. Keshk, B. P. Turnbull, N. Moustafa, D. Vatsalan, and K. R. Choo, "A Privacy-Preserving-Framework-Based Blockchain and Deep Learning for Protecting Smart Power Networks," *IEEE Trans. Ind. Informatics*, vol. 16, no. 8, pp. 5110–5118, 2020.

[245] K. Li, Y. Wang, and Y. Tang, "DETER: Denial of Ethereum Txpool sERvices," in *2021 ACM SIGSAC Conference on Computer and Communications Security, CCS*. ACM, 2021, pp. 1645–1667.

[246] H. Yu, I. Nikolic, R. Hou, and P. Saxena, "OHIE: Blockchain Scaling Made Simple," in *2020 IEEE Symposium on Security and Privacy, SP 2020, San Francisco, CA, USA, May 18-21, 2020*. IEEE, 2020, pp. 90–105.