Futuristic approach on Blockchain for the IoTs

Snehal Vairagade[1], Dr. Abhishek Badholia[2], Ramesh Kumar Yadav[3], Ashish Kumbhare[4], Naveen Kumar Vaishnav[5], Ravi Kiran Patnaik[6]
[1] *Research Scholar/ MATS University, Raipur*
[2] *Research Guide/ MATS University, Raipur*
[3,4,5,6]*Faculty Member/ ICFAI University, Raipur*

Abstract **- One of the most important challenges to IoT success is how to protect yourself and unlock billions of transactions with IoT devices per day, an issue that has persisted despite significant research efforts over the past few years. On the other hand, blockchain-based algorithms disrupt today's cryptocurrency markets and demonstrate great power, because they offer a distributed transaction log that cannot be interrupted or controlled by a single organization. While blockchain may present itself as the solution to all IoT security and privacy challenges, significant research efforts still need to be made to optimize computation-intact blockchain algorithms for robust power and performance on today's IoT devices. In this paper, we provide an overview of the existing literature on the IoT block chain topic and present a roadmap of research challenges that will need to be considered in order to implement the use of block chain technology in IoT.**

Index Terms **- Internet of Things, Research, Challenges, Block chain, Security, Privacy.**

1.INTRODUCTION

It is difficult to say which technology will impact and benefit our lives more than the Internet of Things (IoT). In a few years, cars, kitchen appliances, televisions, smartphones, auxiliary meters, internal sensors, thermostats, and almost anything we can think of will go online and be accessible from anywhere in the world [1]. The change brought about by the IoT cannot be compared - some say it will be similar to the construction of roads and railways that empowered the 18th to 19th Industrial Revolution and will take storms in all sectors of society and industry, from education, health care, smart home and intelligent city, manufacturing, mining, commerce, transportation, and monitoring, to name just a few [3].Over the past few years, researchers have focused more on addressing IoT accounting problems and communication problems [4 - 6]. While these topics are critical to IoT's success and need to be thoroughly investigated, the public has now widely acknowledged that they should be considered "hanging fruit" in relation to major IoT security and privacy issues, which has never been before in scope and size [7 - 11] and which will require a great deal of research effort to overcome. It is easy to assume that as long as humans, sensors, cars, robots, and drones can meet seamlessly in any part of the world, many threats will be unleashed today. As currently envisaged, IoT will use a moderate, customer-supported access model where IoT is implemented (i.e., data, money, or another valuable asset) between IoT organizations (i.e., any computer device or participants connected to -IoT) is entrusted with monolithic, unified service providers [12]. This model facilitates interoperability between IoT organizations and facilitates the data collection process.

However, it ultimately puts the IoT at risk for many security issues and privacy issues. In particular, internal service providers may make illegal use of IoT data, for example, multidisciplinary monitoring systems [13]. More importantly, a central data collection model can expose the system to hacking with dangerous activities, and adverse effects on citizens, as outlined in [14 - 17]. Another major challenge is the certification of IoT structures that will be distributed mainly in the wild without minimal surveillance [18; 19]. If left unchecked, problems with IoT authentication can produce botnets (e.g., Mirai [20]) and severe sybil attacks [21].An important idea to address the above challenges is to organize IoT transactions efficiently, so that no single business has the power to manage. Not only will power allocation provide security and privacy through construction, but it will also give users the ability to choose to share or sell their sensory data with external organizations

without intermediaries. Allocated controls also mean failures - which have plagued IoT since its inception [22; 23]. The ultimate goal, therefore, is to investigate low-cost IoT data access models, which will ensure that user data is not provided to centralized organizations or companies, but rather to the users' own assets. To date, technology and blockchain-based technologies and programs have expanded the cryptocurrency market and can be seen as important in achieving the complex goals of IoT security and privacy [24]. Although important algorithms and principles behind the blockchain have been known since the 70's (i.e., Merkle Trees [25], consensus techniques [26]), the first active blockchain application was first proposed in 2008 as part of the Bitcoin cryptocurrency [27] . Since then, it has been widely used in many types of non-financial applications, including transportation, power management, smart cities, drones / robots, and production; we examine the existing texts on the subject in section III. In short, the blockchain maintains a low level (or led) collection of transactions - we explain in detail what the blockchain is in Phase II. The ledger is unchanged, which means that previous transactions cannot be changed by any business that registers transactions on blockchain1 and are shared and synchronized across all participating nodes. In this way, the blockchain ensures that the ledger cannot be disturbed, and that all the data held by the blockchain is reliable. A harmonious algorithm, which involves solving a difficult problem to solve (e.g., looking for resources) but an easy-to-verify puzzle called proof-of-work (PoW), is used to mine new blocks in blockchain, and thus establish a network. trustworthy safe among unscrupulous organizations. For self-identification purposes, blockchain nodes may choose to use flexible public keys to prevent tracking. Many trades are put together to form a block that is inserted into the ledger by following the algorithm alignment. Each block inserts a previous block hash in this judge (hence the name blockchain). Any block correction (and thus a transaction) can be easily detected as the hash stored in the next block will not match.

The combination of blockchain and IoT has the potential to disrupt. Indeed, the blockchain can help IoT expansion in our community by offering the following benefits:

- Anonymity. IoT businesses can participate in the blockchain with public / private keys, which (if you so wish) do not disclose the actual business ownership;
- Depression in communities. Integrated traditional systems require that each transaction be guaranteed through a medium service (e.g., central bank) - which is undeniably translated into a working bottle. On the other hand, third-party authentication is no longer required in the blockchain, because algorithm algorithms maintain data compatibility.
- Non-rejection. The blockchain ensures that (i) transactions can be easily verified; and (ii) invalid transactions are not accepted - it is almost impossible to delete or reverse transactions once they have been blocked.

While the blockchain may look like a panacea for IoT security and privacy issues, there are still many research challenges that prevent its off-use use on many modern IoT networks. Indeed, many of the algorithms used by today's blockchain-based systems are not designed to work on devices with as much computer / power / bandwidth capabilities as in IoT. Several key challenges (discussed in detail in section V) need to be addressed, including: (i) the declining challenges posed by the need to achieve consensus among billions of miners; (ii) higher computational requirements due to the use of evidence (or similar) evidence of algorithms; and (iii) high delays due to duplication of measures (double expenditure that may not work in IoT).

Many functions refer to the blockchain as a fixed data framework, but it is a technological fraud to define it as static. In fact, there are precedents in which blockchain entries are changed after a network attack or misconduct [28]. In this paper, the term term is intended to be used to represent the complex structure of blockchain transformation [29].

The focus of this paper is to provide an overview of the state of the art related to the use of a block-based system to address IoT security and privacy issues, and to provide a roadmap for novel challenges and exciting challenges to the research community. We point out that in-depth research and comparison of existing blockchain-based IoT systems is not the main purpose of this paper. Instead, our main goal is to advance students and promote their research efforts in

developing the next generation of blockchain-based IoT system.

2.WHAT IS BLOCKCHAIN

From a computer perspective, a blockchain is a data structure in which entries (also called blocks) are stored and linked to each other in sequence. As shown in Fig. 1, the concept of a blockchain is very similar to a linked list, where each entry is linked to the next using a cursor. Although the two structures above are similar in concept, their implementation differs in some major respects.

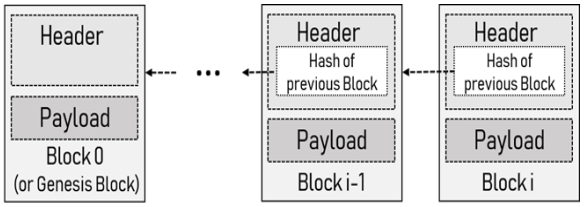

Figure 1: Blockchain structure

Each block is made up of headers and data uploads. While uploads are often used to keep a list of activities between blockchain users, the header is used to convey useful information about a block, such as its length and content. In addition, the header retains the 32-bit SHA256 [30] hash value of the previous block hash. The importance of such a field is twofold: in this way, (i) each block is consistently connected to the previous one; and (ii) the hash value of the th-block will depend on the hash value of block 1. The first element provides the most efficient way to connect all blockchain blocks, and the second, as discussed later, is used to prevent malicious attacks.

To understand this latest statement, it is important to first understand how the blockchain is produced and maintained over time Consensus Mechanisms. The purpose of the blockchain [27] is to enable guaranteed peer-to-peer transactions, organized in blocks, and stored within a distributed ledger. To achieve this goal, the blockchain is governed by legitimate algorithms that determine how the transaction team can be re-introduced into the log. Specifically, each new block can be added to a blockchain only if the majority of nodes in the network agree to its installation, that is, only if agreement is reached between blockchain users. Each node in the network keeps a local copy of the blockchain. When a new block reaches a consensus, it is distributed over the network. Therefore, each node adds a new block to its local copy of the blockchain. These processes make it easy to create more compatible blockchain copies, such that as soon as most nodes have the same copy of the blockchain, the network can be considered reliable and trustworthy.

Consistency is a very important blockchain concept. The initial implementation of the blockchain adopted an evidence-based consensus (PoW) approach [31], which provides a distributed way to maintain and validate the blockchain. The idea of PoW is to achieve harmony between network environments through hard-to-compute, but easy-to-valid, computational puzzles. For example, the Bitcoin blockchain asks its users (also called miners) to obtain a random 4-byte number, i.e., a nonce, such as the SHA256 hash value of a new block equal to or below the given threshold. While nonce calculations are complex and computer-hungry, ensuring that the nonce satisfies the limit requirement is too costly to calculate. Similarly, the first node that finds a candidate informs the blockchain network and distributes a new block. The found nonce, representing the miner's PoW, is examined by other nodes that determine whether the nonce is a real hashing puzzle solution or not. When nonce verification is successful, nodes add a new block to their localized blockchain and start working with a new block.

Although PoW is the most effective way to achieve compliance, it requires a large amount of computer power, which increases every year as more miners and transactions add to the blockchain [32]. For this reason, alternative approaches [33] have been considered in many blockchain structures. For example, Proof-of-Stake (PoS) methods [34; 35] apply the rules for determining the value of a coin, i.e., a pole, choosing which node in the network will add the next block to the blockchain. Similarly, proof-of-value (PoI) considers the pole as an important metric and - however, counts and metrics that measure miner's involvement in the network, such as number and volume of transactions.

As shown in Figure 1, the hash value of each block depends on the hash value of the previous blocks. Therefore, a change to any existing blockchain blocks can produce a different hash value for that block, which will then produce the entry value for all subsequent blocks with their hash values. The newly generated hash values will differ from those already

stored by all other nodes in the network, and due to the compatibility algorithm, corrupted blocks will be rejected in the blockchain.

Security Features

In general, compliance strategy ensures blockchain trust. However, there are cases where wealthy users can use the blockchain structure to change, duplicate or remove blocks [36]. Specifically, it is enough for an attacker to have more than 50% of the locations on the network to manage the whole blockchain. This attack, also called a 51% attack, is aimed at controlling the consensus approach to using the blockchain. This attack has been shown to be effective compared to many smaller crypto-currencies such as Verge, Bitcoin Gold and Zencash [37] - however, they have also threatened and even widespread crypto-currencies such as Bitcoin [38; 39]. Double dissolving [40; 41], which contains the frequency of one or more transactions, is the main target of a 51% attack. However, it has been shown that double expenditure can be achieved with or near the 50% threshold [42].To reduce attacks by 51%, additional block-based methods use better security techniques. For example, real-time authentication can be used to increase the attack limit to 99% [43], meaning that an attacker can only control a blockchain network if it has access to almost all nodes in the network. Another approach is to use PoS compliant methods where the value given to the proceeds of money (rather than computer power) makes 51% attacks less profitable to the attacker and less likely to occur.

3.OVERVIEW OF BLOCKCHAIN-BASED IOT SYSTEMS

Blockchain-based IoT programs have been investigated so far in the literature. As shown in Table I, we divided the papers into categories, each named after the most common IoT applications in these available days, namely, smart power, smart locations, robots, transportation and supply chain.

Application of Blockchain to IoT	Papers
Smart Energy	[44–50]
Smart Environments	[51–55]
Robotics	[56–59]
Transportation	[60–70]
Supply Chain	[71–73]
Others	[74–78]

Table I: Summary of Blockchain-based IoT systems

- Energy Strength. This field has attracted a lot of attention in the IoT community over the years [79]. Most of the proposed IoT systems use a blockchain to (i) maintain users' privacy and personal information; and (ii) protect the system from risky sales as users attempting to sell or purchase an unreasonable amount of energy [45; 46; 49]. Authors in [44; 47] propose auction programs where users can sell to a higher buyer their excessive power based on the auction specified in the smart contract, which is why the need for a third party auctioneer is eliminated. Moreover, Hahn et al. [44] used an auction on the campus power grid. Jan et al. [50] examined the use of blockchain to reconstruct current distribution power generation patterns to allow real-time transactions and dynamic trading contracts using an automated reliability method.
- Smart locations. Intelligent environments have long been widely used in industrial areas [80], in intelligent health care [81], smart cities [82] and smart homes [52; 55; 83]. In this context, the blockchain is used to ensure the availability and non-response of sensitive data collected in the wild, e.g., farmland [53; 54].
- Robots. Existing activity in the area has used the blockchain as a system to support secure and reliable air traffic (UAV) communications. Indeed, UAVs need to faithfully align their actions, exchange data and make collective decisions. Sharma et al. [59] introduced a system in which drones were programmed to use the blockchain to transfer data securely. In addition, Ferrer et al. [56] investigate the use of the blockchain to provide security, independence and participatory decision-making in robotic systems. The authors in [58] use a combination of blockchain and cloud storage to protect the integrity of drone-collected data.
- Transportation. Over the years, many IoT concepts have been used to design mobility systems for future generations [84 - 86]. The most promising feature is that smart cars will not be as computer-savvy as other IoT devices, such as

sensor platforms. Therefore, the blockchain is the person to be appointed to be the data exchange system between smart vehicles, as suggested by Steger et al. [68]. Similarly, Councilor et al. [60] monitor vehicle-related data (e.g., maintenance details and vehicle diagnostic reports) using a blockchain. Yuan et al. [70] use blockchain to design the construction of fully intelligent travel systems, including application, contract, incentive, permit, data, body layers and network. The blockchain has also been used to operate public key vehicle management systems [63], and by sharing general information without third party central management [61; 64]. Li et al. [62] proposes CreditCoin, a confidentiality system for sharing relevant information (e.g., risk, trail) between vehicles, in which participants are rewarded with cash tokens. Yang et al. [66] proposed a blockchain-based reputation system that measures the reliability of the messages received.

- Trading with others. Some programs are designed to improve cloud-based production performance and demand [71; 73]. A blockchain-based distribution framework for sharing information and services across businesses is presented in [72]. A collection of papers [74-78] of computer addresses, using IoT resources, among others.

4.BLOCKCHAIN TECHNOLOGIES FOR THE IOT

In this section, we discuss the most important blockchain technologies and features, and we discuss their application to the IoT

Smart Contracts: One of the most important challenges for IoT is to enable and control independent and self-contained machine communication (M2M) connections. In this particular case, it is very important in the development of management systems such as (i) communication to start automatically; and (ii) not required individual controls and ensuring the integrity of each communication / communication. The above problem is certainly insignificant, and its complexity is further exacerbated by the large number of connected devices and their complex design. It is important to note that the above problem is not only IoT, but also affects all those network building and systems where the lack of centralized enterprises makes central network management and management call for formal and automatic agreements.

The best example is blockchain, a system in which distribution organizations need to independently reach agreement on local implementation of complex algorithms. In this context, smart contracts [87] have been shown to be effective in solving the above challenges.

In short, smart contracts are software programs that specify and automatically enforce contracts between two or more parties. To understand how smart contracts work, we look at a case in which Alice rents a house to Bob. Bob is required to send a monthly payment to Alice. In a blockchain context, the above transactions can be easily incorporated into a smart contract. For example, in Ethereum's blockchain each smart contract is represented by a series of computer functions that are displayed in the programming language specified by the Application Binary Interface (ABI). Indeed, it is enough to write a few lines of code to generate and link a contract with Bob, such as monthly payments can be made automatically with the software system once the monthly deadline has expired. Therefore, smart contracts use effective methods of sending / receiving payments (e.g., rent) to / from other entities where one or more conditions (e.g. Although the previous model is simple, contractors can often implement complex operations and can be linked to another, thus forming a nest structure (e.g., sublease). The benefits of smart contracts are many, and their impact on IoT networks is significant, as discussed in [87]. First, as contracts are stored within the blockchain, their content is trusted between the parties as it cannot be altered or corrupted after being placed on the blockchain. Second, each contractor is given an undeniable address on the blockchain and can be directly accessed via the Internet, thus making the appropriate contracts ready to be accessed by remote IoT devices. Finally, the contracts contain a few lines of code that the devices can easily understand and perform.

Given the similarities between IoT and blockchain, and looking at the effectiveness and performance of smart contracts in blockchain applications, it makes sense to think that smart contractors can find useful programs in IoT to support independent and self-organized communication. Although the use of smart contracts on IoT is still being investigated, preliminary results already indicate that many IoT applications will

benefit from blockchain technology such as smart contracts. For example, the use of smart contracts to create access control systems that control access to the IoT network has been shown to be beneficial to IoT [88 - 92]. These functions work seamlessly with the blockchain to generate a real-time access control list that controls and defines access device resources.

Another example is the work in [87], in which the authors discuss the possibility of achieving smart purchasing monitoring through smart contracts. They show that, not only smart contracts can be used to control transactions and costs associated with production and export processes, but they can also be used to keep track of their position.

Software and content verification

The IoT system is well known as the most aggressive environment where very different devices (depending on the hardware and services offered) interact with both users and other devices. In this challenging situation, it is important to ensure that the software installed on each device (e.g., firmware, scripts) is up-to-date and satisfies the network security regulations and requirements. Although the large number of devices in the network makes it difficult to create processes that meet the above requirements in large networks, blockchain already offers embedded features that are fully functional, or partially, that solve the above problems.

As indicated in [75; 93], the distributed blockchain status can be used to store and distribute secure and certified firmware updates on the network. Specifically, a blockchain can be used to (i) store an update of the firmware itself, or a secure and reliable local address where the updated code can be downloaded and installed; and (ii) use PoW (or similar tools) to determine if the device has updated and verified firmware, thus deciding whether to trust it or not. Since blockchain is maintained through sync processes, it is possible to produce reliable blockchains that maintain all reliable and up-to-date firmware updates [75] that can be easily detected and downloaded by network nodes.

Another exciting blockchain technology application for IoT systems is likely to provide reliable licensing tools to prevent crime and secure patents for software / hardware developers [94] and content creators [95]. Indeed, IoT devices these days are capable of performing extreme and computer-sensitive functions and can be rearranged by downloading a variety of software applications from various developers. Although open source software is now widely used in many IoT environments, there are still several applications whose code can be purchased online through licenses. Purpose of [94] use blockchain technology to provide effective tools to validate software developer licenses to enforce their copyright.

5.THE ROAD AHEAD

We are now paving the way for research challenges related to the use of blockchain algorithms in IoT.

A. There is talk of Blockchain Scalability issues Incorporating blockchain technology into IoT means that downsizing issues need to be addressed. Most importantly, the presence of blockchain tools requires all nodes in the network

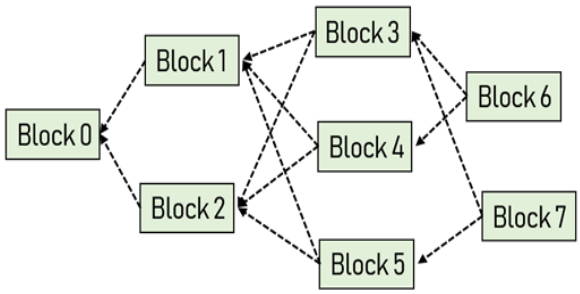

Figure 2: DAG blockchain (or Tangle).

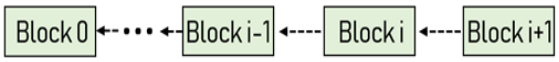

Figure 3. Traditional line blockchain

allow each transaction / block or store it locally. While these functions are easy on your computers or workstations, they may not allow for limited sensors with limited storage and computer resources. This problem is also exacerbated by the fact that the amount of data transfer, and thus the transaction required, which will be kept in the blockchain is large and increases over time [24; 96-98]. In other words, existing PoW and PoS-based compliance algorithms do not work directly to address long-term, reliable and awesome solutions for blockchain-based IoT systems. The most commonly used method of dealing with failure problems is the ability to integrate algorithms to reduce communication and computational computing [52; 90]. For example, Novo [90] proposes a measurable blockchain solution for IoT systems. At

the expense of additional communication delays, the proposed solution relies on an administrative hub that manages a group of IoT devices, thereby reducing the number of connections between objects and the blockchain, effectively producing non-blockchain configurations. A similar approach has been proposed by Dorri et al. [52], in which the authors designed a secure blockchain that protects the privacy of IoT applications.

Alternatives prefer to revisit the structure of the licensing processes and the blockchain itself to provide temporary IoT solutions. Specific examples are the crypto-currencies IoT Chain (ITC) [99] and IOTA. These funds are designed to provide IoT blockchain lightweight technology. Specifically, along with other currencies such as Byteball , ITC and IOTA aim to reconstruct an integrated blockchain structure to detect a disrupted network represented by a direct acyclic graph (DAG). The difference between traditional (direct) blockchain and DAG-based methods is shown in figs. 2 and 3 In DAG structures (also called tangle), blocks representing DAG vertices and edges are used to secure transactions. Specifically, for inclusion in the DAG, each new transaction A must approve any transaction B and C already submitted to the DAG. The transaction approval is indicated by the targeted margins from one transaction to another. Similarly, when A is included in DAG, it automatically produces two edges A B and A C extending the DAG further. The synergic use of DAGs and blockchain technology allows discarding the linear formation of traditional blockchains, simplifying transaction verification times and eliminating the need for mines as transactions are responsible for ensuring other transactions.

Safety and reliability for IoT Being able to remotely access one or more tools, combined with the opportunity to let them talk and communicate independently is certainly not a useful and wonderful thing. However, this inevitably brings with it many of the concerns arising from observation and observation integrity [7; 41]. IoT is vulnerable to various network attacks that undermine privacy, integrity, authenticity and discovery. These features are essential requirements of any modern communication network and various solutions have been suggested in the literature [7; 10; 41]. These surveys provide a comprehensive review of existing solutions for building secure and reliable IoT systems. On the other hand, however, they show that many security solutions are not common enough and require ad-hoc solutions that include new technologies and software.

The blockchain already uses a number of methods such as public / private encryption, hashing, acceptance and tolerance and its secure operation has been extensively investigated and verified by multiple communication systems. For this reason, the blockchain has been identified as an important technology for designing secure and reliable IoT systems [52; 67].

- Confidentiality: data confidentiality is accessed when the information provided (e.g., auditory data, transaction) can be accessed only by targeted devices. In this context, the public key encryption used to make blockchain transactions can be used seamlessly to encrypt communications and information to be stored, thus achieving confidentiality successfully;
- Integrity: to ensure that data accessed and stored on IoT devices is reliable, the reliability of the content must be guaranteed at all times. Also, blockchain helps provide useful ways to ensure data integrity. Remember that the integrity of each block in the blockchain is guaranteed by entering its hash value, and that the hash value of any block depends on the hash of previous blocks. Likewise, not only hashing on a blockchain ensures the integrity of a new block, but also extends the integrity check to all previous blocks. As shown in [67], the same concept can be applied to blockchain-based IoT networks to assess the integrity of sensory data, data transmitted and transactions between devices and users;
- Authorization and non-authorization: using embedded public encryption it is possible to use signature-based security measures, known for providing collaborative and non-compliant provision. Remember that any node B with public key of a given device A can i) determine encrypted messages using the private key A; and ii) encrypted messages with A public key. Since A secret key is known only to A, public key encryption does it is possible to use the private keys to make the A electric signature. This signature is used to verify A when communicating with other nodes (each node can verify the signature using the public key A); and may be

used for non-disclosure purposes to sign all transactions incorporated into an A-blocking blockchain, thus effectively providing proof of A's work in the blockchain.

6.CONCLUSION

In this paper, we have provided an overview of existing documents on the IoT blockchain topic, and presented a roadmap of research challenges that will need to be addressed in order to implement blockchain technology in IoT. First, we have briefly introduced the concept of blockchain in Phase II, followed by an overview of existing blockchain-based IoT applications in Phase III. Subsequently, we introduced the major IoT blockchain technology in phase IV. We concluded this paper by discussing a number of research challenges in Section V

REFERENCES

The heading of the References section must not be numbered. All reference items must be in 10 pt font. Please use Regular and Italic styles to distinguish different fields as shown in the References section. Number the reference items consecutively in square brackets (e.g. [1]).

[1] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things – A survey of topics and trends," Information Systems Frontiers, vol. 17, no. 2, pp. 261–274, 2015.

[2] Glen Martin (Forbes), "How The Internet Of Things Is More Like The Industrial Revolution Than The Digital Revolution," https://www.forbes.com/sites/oreilly media /2014 /02/10/more-1876-than-1995/#674c4e0b66d2.

[3] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233–2243, 2014.

[4] O. Bello and S. Zeadally, "Communication issues in the internet of things (iot)," in Next-Generation Wireless Technologies. Springer, 2013, pp. 189–219.

[5] S. Tayeb, S. Latifi, and Y. Kim, "A survey on iot communication and computation frameworks: An industrial perspective," in Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual. IEEE, 2017, pp. 1–6.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," Future generation computer systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[7] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the internet of things in the age of machine learning and software-defined networking," IEEE Internet of Things Journal, 2018.

[8] C. Bekara, "Security issues and challenges for the iot-based smart grid," Procedia Computer Science, vol. 34, pp. 532–537, 2014.

[9] M. FRUSTACI, P. Pasquale, A. Gianluca, and G. FORTINO, "Eval- uating critical security issues of the iot world: Present and future challenges," IEEE Internet of Things Journal, 2017.

[10] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," IEEE Internet Computing, vol. 21, no. 2, pp. 34–42, 2017.

[11] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on. IEEE, 2014, pp. 1–8.

[12] M. S. Ali, K. Dolui, and F. Antonelli, "IoT data privacy via blockchains and IPFS," in Proceedings of the Seventh International Conference on the Internet of Things. ACM, 2017, p. 14.

[13] M. S. Ali, K. Dolui, and F. Antonelli, "IoT data privacy via blockchains and IPFS," in Proceedings of the Seventh International Conference on the Internet of Things. ACM, 2017, p. 14.

[14] M. S. Ali, K. Dolui, and F. Antonelli, "IoT data privacy via blockchains and IPFS," in Proceedings of the Seventh International Conference on the Internet of Things. ACM, 2017, p. 14.

[15] Julia Powles (The Guardian), "Internet of things: the greatest mass surveillance infrastructure ever?" https://www.theguardian.com/ technology /2015/jul/15/internet-of-things-mass-surveillance, 2013.

[16] Dan Goodin, Ars Technica, "9 Baby Monitors Wide Open to Hacks that Expose Users' Most Private Moments," http://tinyurl.com/ya7w43e9, 2015.
[17] Jerry Hirsch, Los Angeles Times, "Hackers Can Now Hitch a Ride on Car Computers," http://www.latimes.com/business/autos/ la-fi-hy-car-hacking-20150914-story.html, 2015.
[18] Kelsey D. Atheron, Popular Science, "Hackers Can Tap into Hospital Drug Pumps to Serve Lethal Doses to Patients," available at: http://tinyurl.com/qfscthv, 2015.
[19] Darren Pauli, ITNews, "Hacked Terminals Capable of Causing Pace- maker Deaths," http://tinyurl.com/ycl4z9xf, 2015.
[20] S. Kalra and S. K. Sood, "Secure authentication scheme for IoT and cloud servers," Pervasive and Mobile Computing, vol. 24, pp. 210–223, 2015.
[21] R. Amin, N. Kumar, G. Biswas, R. Iqbal, and V. Chang, "A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment," Future Generation Computer Systems, vol. 78, pp. 1005–1019, 2018.
[22] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer, vol. 50, no. 7, pp. 80–84, 2017.
[23] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," IEEE Internet of Things Journal, vol. 1, no. 5, pp. 372–383, 2014.
[24] M. Gharbieh, H. ElSawy, A. Bader, and M.-S. Alouini, "Spatiotemporal stochastic modeling of iot enabled cellular networks: Scalability and stability analysis," IEEE Transactions on Communications, vol. 65, no. 8, pp. 3585–3600, 2017.
[25] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad hoc networks, vol. 10, no. 7, pp. 1497–1516, 2012.
[26] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the internet of things: A systematic literature review," in Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of. IEEE, 2016, pp. 1–6.
[27] R. C. Merkle, "Protocols for public key cryptosystems," in Security and Privacy, 1980 IEEE Symposium on. IEEE, 1980, pp. 122–122.
[28] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in 2017 IEEE International Congress on Big Data (BigData Congress), June 2017, pp. 557–564.
[29] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[30] K. D. Werbach, "Trust, but verify: Why the blockchain needs the law," 2017.
[31] A. Walch, "The path of the blockchain lexicon (and the law)," Rev. Banking & Fin. L., vol. 36, p. 713, 2016.
[32] F. I. P. S. PUBLICATION, "Secure Hash Standard (SHS)," FIPS PUB 180, vol. 4, 2012.
[33] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in Annual International Cryptology Conference. Springer, 1992, pp. 139–147.
[34] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," 2014.
[35] L. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, 2018, pp. 1545–1550.
[36] A. Kiayias, I. Konstantinou, A. Russell, B. David, and R. Oliynykov, "A provably secure proof-of-stake blockchain protocol." IACR Cryptology ePrint Archive, vol. 2016, p. 889, 2016.
[37] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in Big Data (BigData Congress), 2017 IEEE International Congress on. IEEE, 2017, pp. 557–564.
[38] D. Bradbury, "The problem with bitcoin," Computer Fraud & Security, vol. 2013, no. 11, pp. 5–8, 2013.
[39] Alyssa Hertig, "Blockchain's Once-Feared 51% Attack Is Now Becoming Regular," https: // www.coindesk.com/ blockchains-feared-51-attack-now-becoming-regular, 2018.
[40] Daniel Cawrey, "Are 51% Attacks a Real Threat to Bitcoin?" https://www.coindesk.com/ 51-attacks-real-threat-bitcoin, 2014.
[41] Roop Gill, "CEX.IO Slow to Respond as Fears of 51% Attack Spread,"

https://www.coindesk.com/cex-io-response-fears-of-51-attack-spread, 2014.

[42] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012, pp. 906–917.

[43] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, 2017.

[44] A. Hahn, R. Singh, C.-C. Liu, and S. Chen, "Smart contract-based campus demonstration of decentralized transactive energy auctions," in Power & Energy Society Innovative Smart Grid Technologies Confer- ence (ISGT), 2017 IEEE. IEEE, 2017, pp. 1–5.

[45] A. Laszka, A. Dubey, M. Walker, and D. Schmidt, "Providing privacy, safety, and security in iot-based transactive energy systems using distributed ledgers," in Proceedings of the Seventh International Con- ference on the Internet of Things. ACM, 2017, p. 13.

[46] F. Lombardi, L. Aniello, S. De Angelis, A. Margheri, and V. Sassone, "A blockchain-based infrastructure for reliable and cost-effective iot-aided smart grids," in Living in the Internet of Things: Cybersecurity of the IoT-2018. IET, 2018, pp. 1–6.

[47] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: towards sustainable local energy markets," Computer Science-Research and Development, vol. 33, no. 1-2, pp. 207–214, 2018.

[48] E. Mu¨nsing, J. Mather, and S. Moura, "Blockchains for decentralized optimization of energy resources in microgrid networks," in Control Technology and Applications (CCTA), 2017 IEEE Conference on. IEEE, 2017, pp. 2164–2171.

[49] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security," in Resilience Week (RWS), 2017. IEEE, 2017, pp. 18–23.

[50] H. Yan, B.-B. Huang, and B.-W. Hong, "Distributed energy transaction pattern and block chain-based architecture design," DEStech Transac- tions on Environment, Energy and Earth Sciences, no. epee, 2017.

[51] R. A. Michelin, A. Dorri, R. C. Lunardi, M. Steger, S. S. Kan- here, R. Jurdak, and A. F. Zorzo, "Speedychain: A framework for decoupling data from blockchain for smart cities," arXiv preprint arXiv:1807.01980, 2018.

[52] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy," arXiv preprint arXiv:1712.02969, 2017.

[53] A. S. Patil, B. A. Tama, Y. Park, and K.-H. Rhee, "A framework for blockchain based secure smart greenhouse farming," in Advances in Computer Science and Ubiquitous Computing. Springer, 2017, pp. 1162–1167.

[54] S. Ibba, A. Pinna, M. Seu, and F. E. Pani, "Citysense: blockchain- oriented smart cities," in Proceedings of the XP2017 Scientific Work-shops. ACM, 2017, p. 12.

[55] A. Palai, M. Vora, and A. Shah, "Empowering light nodes in blockchains with block summarization," in New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference on. IEEE, 2018, pp. 1–5.

[56] E. C. Ferrer, "The blockchain: a new framework for robotic swarm systems," arXiv preprint arXiv:1608.00695, 2016.

[57] A. Kapitonov, S. Lonshakov, A. Krupenkin, and I. Berman, "Blockchain-based protocol of autonomous business activity for multi- agent systems consisting of UAVs," in Research, Education and De- velopment of Unmanned Aerial Systems (RED-UAS), 2017 Workshop on. IEEE, 2017, pp. 84–89.

[58] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in iot using blockchain," in Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE. IEEE, 2017, pp. 261–266.

[59] V. Sharma, I. You, and G. Kul, "Socializing drones for inter-service operability in ultra-dense wireless networks using blockchain," in Proceedings of the 2017 International Workshop on Managing Insider Security Threats. ACM, 2017, pp. 81–84.

[60] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4forensic: An integrated lightweight blockchain framework for forensics

applications of connected vehicles," arXiv preprint arXiv:1802.00561, 2018.

[61] B. Leiding, P. Memarmoshrefi, and D. Hogrefe, "Self-managed and blockchain-based vehicular ad-hoc networks," in Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct. ACM, 2016, pp. 137–140.

[62] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "Creditcoin: A privacy-preserving blockchain-based incentive an-nouncement network for communications of smart vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 7, pp. 2204–2220, July 2018. accountability," ACM Transactions on Information and System Security (TISSEC), vol. 18, no. 1, p. 2, 2015.

[63] A. Hahn, R. Singh, C.-C. Liu, and S. Chen, "Smart contract-based campus demonstration of decentralized transactive energy auctions," in Power & Energy Society Innovative Smart Grid Technologies Confer- ence (ISGT), 2017 IEEE. IEEE, 2017, pp. 1–5.

[64] A. Laszka, A. Dubey, M. Walker, and D. Schmidt, "Providing privacy, safety, and security in iot-based transactive energy systems using distributed ledgers," in Proceedings of the Seventh International Con- ference on the Internet of Things. ACM, 2017, p. 13.

[65] F. Lombardi, L. Aniello, S. De Angelis, A. Margheri, and V. Sassone, "A blockchain-based infrastructure for reliable and cost-effective iot-aided smart grids," in Living in the Internet of Things: Cybersecurity of the IoT-2018. IET, 2018, pp. 1–6.

[66] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: towards sustainable local energy markets," Computer Science-Research and Development, vol. 33, no. 1-2, pp. 207–214, 2018.

[67] E. Mu¨nsing, J. Mather, and S. Moura, "Blockchains for decentralized optimization of energy resources in microgrid networks," in Control Technology and Applications (CCTA), 2017 IEEE Conference on. IEEE, 2017, pp. 2164–2171.

[68] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security," in Resilience Week (RWS), 2017. IEEE, 2017, pp. 18–23.

[69] H. Yan, B.-B. Huang, and B.-W. Hong, "Distributed energy transaction pattern and block chain-based architecture design," DEStech Transactions on Environment, Energy and Earth Sciences, no. epee, 2017.

[70] R. A. Michelin, A. Dorri, R. C. Lunardi, M. Steger, S. S. Kan- here, R. Jurdak, and A. F. Zorzo, "Speedychain: A framework for decoupling data from blockchain for smart cities," arXiv preprint arXiv:1807.01980, 2018.

[71] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy," arXiv preprint arXiv:1712.02969, 2017.

[72] A. S. Patil, B. A. Tama, Y. Park, and K.-H. Rhee, "A framework for blockchain based secure smart greenhouse farming," in Advances in Computer Science and Ubiquitous Computing. Springer, 2017, pp. 1162–1167.

[73] S. Ibba, A. Pinna, M. Seu, and F. E. Pani, "Citysense: blockchain- oriented smart cities," in Proceedings of the XP2017 Scientific Work-shops. ACM, 2017, p. 12.

[74] A. Palai, M. Vora, and A. Shah, "Empowering light nodes in blockchains with block summarization," in New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference on. IEEE, 2018, pp. 1–5.

[75] E. C. Ferrer, "The blockchain: a new framework for robotic swarm systems," arXiv preprint arXiv:1608.00695, 2016.

[76] A. Kapitonov, S. Lonshakov, A. Krupenkin, and I. Berman, "Blockchain-based protocol of autonomous business activity for multi- agent systems consisting of UAVs," in Research, Education and De- velopment of Unmanned Aerial Systems (RED-UAS), 2017 Workshop on. IEEE, 2017, pp. 84–89.

[77] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in iot using blockchain," in Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE. IEEE, 2017, pp. 261–266.

[78] V. Sharma, I. You, and G. Kul, "Socializing drones for inter-service operability in ultra-dense wireless networks using blockchain," in Proceedings of the 2017 International Workshop

on Managing Insider Security Threats. ACM, 2017, pp. 81–84.

[79] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," arXiv preprint arXiv:1802.00561, 2018.

[80] B. Leiding, P. Memarmoshrefi, and D. Hogrefe, "Self-managed and blockchain-based vehicular ad-hoc networks," in Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct. ACM, 2016, pp. 137–140.

[81] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 7, pp. 2204–2220, July 2018.

[82] S. Rowan, M. Clear, M. Gerla, M. Huggard, and C. M. Goldrick, "Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels," arXiv preprint arXiv:1704.02553, 2017.

[83] P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-vn: A distributed blockchain based vehicular network architecture in smart city," Journal of Information Processing Systems, vol. 13, no. 1, p. 84, 2017.

[84] M. Singh and S. Kim, "Intelligent vehicle-trust point: Reward based intelligent vehicle communication using blockchain," arXiv preprint arXiv:1707.07442, 2017.

[85] Z. Yang, K. Zheng, K. Yang, and V. C. Leung, "A blockchain- based reputation system for data credibility assessment in vehicular networks," in Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017 IEEE 28th Annual International Symposium on. IEEE, 2017, pp. 1–5.

[86] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," IEEE Communications Magazine, vol. 55, no. 12, pp. 119–125, 2017.

[87] M. Steger, A. Dorri, S. S. Kanhere, K. Ro¨mer, R. Jurdak, and M. Karner, "Secure wireless automotive software updates using blockchains: A proof of concept," in Advanced Microsystems for Automotive Applications 2017. Springer, 2018, pp. 137–149.

[88] C. Oham, R. Jurdak, S. S. Kanhere, A. Dorri, and S. Jha, "B-fica: Blockchain based framework for auto-insurance claim and adjudica- tion," arXiv preprint arXiv:1806.06169, 2018.

[89] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent trans- portation systems," in Intelligent Transportation Systems (ITSC), 2016 IEEE 19th International Conference on. IEEE, 2016, pp. 2663–2668.

[90] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial internet of things," Journal of Software Engineering and Applications, vol. 9, no. 10, p. 533, 2016

[91] Z. Li, W. Wang, G. Liu, L. Liu, J. He, and G. Huang, "Toward open manufacturing: A cross-enterprises knowledge and services exchange framework based on blockchain and edge computing," Industrial Man- agement & Data Systems, vol. 118, no. 1, pp. 303–320, 2018

[92] K. Rabah, "Overview of blockchain as the engine of the 4th industrial revolution," Mara Research Journal of Business & Management-ISSN: 2519-1381, vol. 1, no. 1, pp. 125–135, 2017.

[93] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, and R. Sirdey, "Towards better availability and accountability for iot updates by means of a blockchain," in Security and Privacy Workshops (EuroS&PW), 2017 IEEE European Symposium on. IEEE, 2017, pp. 50–58.

[94] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an internet of things environment," The Journal of Supercomputing, vol. 73, no. 3, pp. 1152–1167, 2017.

[95] M. Samaniego and R. Deters, "Hosting virtual iot resources on edge- hosts with blockchain," in Computer and Information Technology (CIT), 2016 IEEE International Conference on. IEEE, 2016, pp. 116– 119.

[96] M. Samaniego and R. Deters, "Hosting virtual iot resources on edge- hosts with blockchain," in Computer and Information Technology (CIT), 2016 IEEE International Conference on. IEEE, 2016, pp. 116– 119.

[97] A. Stanciu, "Blockchain based distributed control system for edge computing," in Control Systems

and Computer Science (CSCS), 2017 21st International Conference on. IEEE, 2017, pp. 667–671.

[98] F. Dalipi and S. Y. Yayilgan, "Security and privacy considerations for iot application on smart grids: Survey and research challenges," in Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on. IEEE, 2016, pp. 63–68.

[99] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," IEEE Internet of Things journal, vol. 1, no. 1, pp. 22–32, 2014.