applied sciences

MDPI

Review

Blockchain and IoT Convergence—A Systematic Survey on Technologies, Protocols and Security

Alessandra Pieroni [1], Noemi Scarpato [2] and Lorenzo Felli [1,3,*]

[1] Department of Innovation and Information Engineering, Guglielmo Marconi University, Via Plinio 44, 00193 Rome, Italy; a.pieroni@unimarconi.it

[2] Department of Human sciences and Promotion of the quality of life, San Raffaele Roma Open University, Via Val Cannuta 247, 00166 Rome, Italy; noemi.scarpato@uniroma5.it

[3] I.T. Department, ISPRA—The Italian Institute for Environmental Protection and Research, Via Vitaliano Brancati 48, 00144 Rome, Italy

[*] Correspondence: lorenzo.felli@isprambiente.it

Received: 13 August 2020; Accepted: 14 September 2020; Published: 26 September 2020

Abstract: The Internet of Things (IoT) as a concept is fascinating and exciting, with an exponential growth just beginning. The IoT global market is expected to grow from 170 billion USD in 2017 to 560 billion USD by 2022. Though many experts have pegged IoT as the next industrial revolution, two of the major challenging aspects of IoT since the early days are having a secure privacy-safe ecosystem encompassing all building blocks of IoT architecture and solve the scalability problem as the number of devices increases. In recent years, Distributed Ledgers have often been referred to as the solution for both privacy and security problems. One form of distributed ledger is the Blockchain system. The aim of this paper consists of reviewing the most recent Blockchain architectures, comparing the most interesting and popular consensus algorithms, and evaluating the convergence between Blockchain and IoT by illustrating some of the main interesting projects in this research field. Furthermore, the paper provides a vision of a disruptive research topic that the authors are investigating: the use of AI algorithms to be applied to IoT devices belonging to a Blockchain architecture. This obviously requires that the devices be provided with adequate computational capacity and that can efficiently optimize their energy consumption.

Keywords: IoT; blockchain; distributed ledgers; privacy; scalability

1. Introduction

Exploring and understanding the different components of an Internet of Things (IoT) architecture, detecting vulnerability areas in each component, and exploring the appropriate technologies to detect any weaknesses are essential to address the IoT security [1] and privacy issues. In October 2016 a DNS provider called Dyn Inc. suffered a DDoS cyberattack [2] that originated from tens of millions of IP addresses. One of the sources of the attack was devices like printers, DVRs and other appliances that are connected to the Internet, known as the “Internet of Things”. A Malware called Mirai infected these devices and launched the distributed denial-of-service (DDoS) attacks. The number of attacks involving IoT devices during 2018 increased, with 32.7 million IoT incidents reported last year [3]. The main drawback in this scenario was their reliance on a centralized cloud infrastructure and the lack of safety protocols [4]. A decentralized approach, based on tamper-proof digital ledger exchange of data, would overcome many of the problems associated with the centralized cloud approach. A Blockchain allows users to sign, secure, and verify every transaction. It is highly challenging to edit or remove blocks of data that are saved on the ledger [5]. A large number of Blockchain architectures have been released but all follow the same basic rules:

- Use of encryption to sign transactions between the parties.

- Transactions are stored on a distributed ledger over a peer-to-peer network.
- Reaching consensus using a decentralized approach.

The ledger is made up of sequentially linked blocks of transactions, cryptographically signed, which form a Blockchain. The aim of this paper consists of analyzing the main concepts of IoT and Blockchain technologies and evaluating in detail the synergies and the connections between the two architectures, highlighting the most appropriate research articles that enable the studying, the comparison and the classification of the most interesting IoT–Blockchain projects already deployed or in developing stage.

2. Key Contribution

Creating a synergy between Blockchain architectures and the IoT world would allow for much safer devices that are now in common use, paving the way for new possibilities in a variety of application areas. Think of the healthcare world [6], where many IoT devices already collect sensitive information and the discovery of vulnerabilities is a daily problem, with all the privacy issues that can result. In recent years, many studies have been done on the integration between IoT and Blockchain, for example thinking of Blockchain as a component serving the IoT device [7]. A number of papers have focused on how to solve the safety aspects of IoT devices [8–11]. To improve the reading and understanding of the projects submitted, this article addresses the main aspects of Blockchain technology, such as encryption and consensus algorithms, addresses the main security issues of the various types of IoT devices and identifies where the Blockchain can be used as a solution. Section 8 presents the main use cases related to Blockchain & IoT. Furthermore, the authors intend to introduce at the end of this paper their future research interest that consist of using AI techniques to enhance the capability of IoT devices in Blockchain architectures in order to face with complex big data management systems, predictive models in several research fields, e.g., e-health and mobility [12–15].

3. Workflow

To carry out this review, we have analyzed and presented the Blockchain–IoT projects that represent the most innovative solutions that can currently be tested on the world scene, choosing them mainly according to the following criteria:

- Number of citations of whitepapers and related articles on Google scholar, Microsoft academic and semantic scholar.
- Novelty of the proposed solution.
- Market capitalization if any.

The strategy used to search for articles within the above mentioned search engines began by using the keywords present in this article in conjunction with specific terms such as "Consensus", "Convergence", "RFID", "RSA", "Weakness" mainly using the Boolean operator "AND". If source code exists, this has been installed and tested. Only English language articles have been considered.

4. Internet of Things

The term Internet of Things (IoT) refers to the concept of extending Internet connectivity beyond conventional platforms to daily elements to take advantage of the immediate connection, communication, storage and processing of the information gathered from the surrounding environment. Embedded with Internet connectivity and other forms of hardware sensors, these devices are present in today's smart homes and will be the cornerstones for future smart cities. Defined from an idea by Kevin Ashton in 1999 while working on RFID technology at MIT (Massachusetts Institute of Technology), IoT concept underlies a new, augmented way to interact with daily tasks and activities by both human beings and machines.

4.1. IoT Weaknesses

4.1.1. Cloud Infrastructure

To date, the technology behind IoT systems, simple by its very nature, has led to complex protocols with conflicting configurations. Almost all of today's Internet of Things ecosystems are based on centralized systems. Centralized clouds and network equipment involved in these architectures are exponentially expensive as the number of devices increases. In this centralized model, IoT devices are authenticated, identified and communicate their data in real time or semi-real time mode with the cloud. In a highly connected smart-city scenario, where private homes, offices, streets with their traffic lights, transportation and pedestrians produce a mass of data every second, the cloud infrastructure need to scale, leading to a price increase. As the environments become smarter, the higher the cost of this type of infrastructure will be. IoT devices are subject to various types of vulnerabilities and often if a device connected to the cloud infrastructure is breached, the whole infrastructure is at risk. Below is a list of the main security issues affecting the cloud infrastructure related to IoT devices:

1. Wrapping attack: This attack occurs by duplicating the user credentials during the log in process, and the SOAP2 messages that are exchanged during the connection setup between the web browser and the server are modified by the attackers [16].
2. Eavesdropping: under the term eavesdropping fall the techniques used to intercept communications that occur within a channel established between two authorized users [16].
3. Flooding attack/DOS attack: The goal of a DOS attack is to consume all the available resources of a server to make the system unresponsive to legitimate traffic [16].
4. Data Stealing problem. This type of attack involves hacking the data and security of cloud systems by stealing system access credentials.
5. Man-in-the-Middle Attack (MITM): in this case the attacker succeeds in gaining access to the communication channel between two legitimate users, being able to both intercept and modify the information without making anyone aware of it [16].
6. Reflection Attack: This type of attack is perpetrated in challenge-response type systems that use the same communication protocol in both directions. The idea behind this type of attack is to trick the victim by asking him for a solution (response) to his own challenge [16].
7. Replay Attack: The replay attack is a form of cyberattack that targets computer networks in order to take possession of an authentication credential communicated from one host to another, and then propose it again by simulating the identity of the issuer. Usually the action is carried out by an attacker who interposes himself between the two communicating sides or from a spoofed IP [16].
8. Brute force/Dictionary attack: in a brute force attack, a series of attempts are made to guess the credentials of a certain system, based on information generated through specific dictionaries or by specific rules.

4.1.2. Sensors and Devices: Perception Layer

Perception layer collects all information/data from physical environment like temperature, speed, time, humidity etc. It is nothing but collection of sensors, actuators which forms Wireless Sensor Network (WSN). In this layer many of the Cloud attack are present but adapted to the specific protocols used at this level (RFID, WSN, NFC, BLUETOOTH etc.). Other common vulnerabilities concern to identity and password theft. Attackers adopt several mechanisms to find passwords, using known dictionaries and vulnerabilities in password creation programs.

Common password hack:

- Brute force/Dictionary Attack: This attack is launched by guessing passwords containing all possible combinations of letters, numbers and alphanumeric character or by using precomputed dictionary of passwords [16].

- Social hacking: This attack exploits human weaknesses. Instead of using a generic dictionary, private information of the target person is collected, and a tailored dictionary is created.

RFID common vulnerabilities [17,18] :

- DoS Attack: denial-of-Service attack is accomplished by flooding the targeted machine with superfluous requests from a fake RFID device.
- Eavesdropping: an antenna is used to record communications between legitimate RFID tags and readers. Eavesdropping attacks can be done in both directions: tag to reader and reader to tag
- Skimming: in this case, the attacker observes the information exchanged between a legitimate tag and legitimate reader. Through the extracted data, the attacker attempts to make a cloned tag which imitates the original RFID tag. Very dangerous in case of RFID chips in credit cards, passports and another personal RFID hardware.
- Replay Attack: similar to a MITM attack, in Replay attacks, the communicating signal between the tag and the reader is intercepted, recorded and replayed.

NFC common vulnerabilities [19,20]:

- Phishing attack: phishing is a type of scam carried out on the Internet by a malicious attacker trying to deceive the victim by convincing them to provide personal information, financial data or access codes, pretending to be a reliable entity in a digital communication.
- User Tracking: in case tags use the same unique ID for anti-collision technique, an attacker can easily track them by compromising the secrecy of the entire NFC system.
- Relay attack: this concerns the intrusion within a communication between device and NFC, the ability to read data coming from the source device and send it back to the destination device.
- Eavesdropping: the attack is perpetrated via an antenna used to record communications between NFC devices. Although NFC communication takes place between very close devices, this type of attack is feasible. The purpose of the attack can be two-fold, theft of information or corrupting the information exchanged, making it useless.
- Spoofing: some mobile devices are configured to run automatically the commands received by NFC tags. In a spoofing attack, a third party pretends to be another entity to induce a user to touch his device against the tag programmed specifically to execute malicious code.

5. Distributed Ledgers

Blockchain technology was introduced by a single entity or group under the name of Satoshi Nakamoto in 2008 and the code of its implementation was published a year later in 2009 in the document 'Bitcoin: A Peer-to-Peer Electronic Cash System' [21]. The Blockchain is essentially a distributed and transactional database shared by the various nodes of the network. The validity and integrity of the data is maintained by chaining the transactions contained in the blocks using hash functions that prevent them from being modified without consent. Bitcoin uses the public key infrastructure (PKI) mechanism [22]. In PKI, the user has a couple formed by a public and a private key. The public key is used as the address of the user's wallet, while the private key is used to sign transactions. A block is accepted by the network on average every 10 min through a consensus mechanism. The new chain with the new block on top will spread quickly in all the nodes of the network.

Inside each node there is a key-value database in which the blocks containing the transactions that have reached consensus will be written. Each node validates the new blocks. Although the search for the hash that satisfies the consensus called Proof of Work takes on average 10 min regardless of the network's computational capacity, checking the correctness of these hashes is extremely fast. This method creates a linear chain of blocks on which all nodes agree (Figure 1). This chain of blocks is the public ledger technique of Bitcoin, called Blockchain.

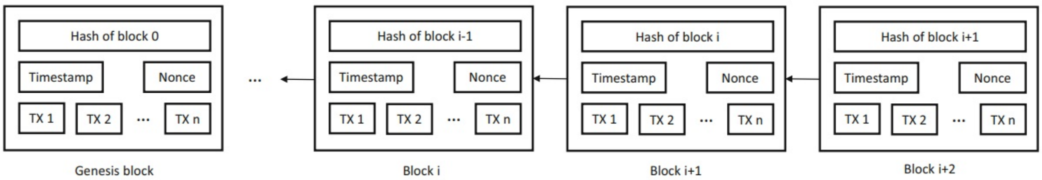


Figure 1. Blockchain structure. (Zheng et al. 2016 [23]).

5.1. Blockchain vs. Classical Vulnerability

A decentralized Blockchain approach to the Internet of Things makes many of the classic attacks unenforceable. Adopting a secure, tamper-evident peer-to-peer communication model to process billions of transactions between IoT devices can also significantly reduce the costs associated with installing and maintaining various network and cloud systems and distribute computing and storage needs across the billions of devices that form the Internet of Things networks. This will also prevent the "single point of failure" vulnerability, where the failure of a single node in a network can lead the entire network to a halting collapse. In Blockchain, message exchanges between devices can be treated in the same ways as financial transactions in a Bitcoin network. Devices rely on cryptographically signed transactions and digital smart contracts thus guaranteeing a level of security that was previously unobtainable. The fact that Blockchain cryptographically verifies the transactions eliminates the possibility of man-in-the-middle attack, replay and all other classical "device-to-cloud" attacks. Some of these attacks, however, have been borrowed and adapted against the new Blockchain architecture:

- Eavesdropping: Using different nodes listening in the p2p network it is possible to deanonymize many Blockchains revealing the IP addresses of specific wallet address owners [24]. To solve this issue, Blockchain architectures have been created that allow for a higher level of anonymity [25].
- Replay attack: In case of a fork in a Blockchain, an attacker can use a signed transaction on the first Blockchain and replicate it as it is on the second since the private keys on both chains are identical. Replay protection is fairly trivial to implement and it has become a de-facto prerequisite for any forked chain. For example, Bitcoin Cash created replay protection for their chain by implementing a unique marker that would allow the Bitcoin Cash nodes to distinguish transactions spent on the legacy Bitcoin chain as independent from the Bitcoin Cash chain.
- Sybil Attack: To create many connections in a Blockchain it is necessary to start many nodes at the same time. An attack of this kind can be used to capture users' IPs or study the topology of the network, falling back as a type of attack to be very similar to Eavesdropping. Mining process is protected by consensus-building algorithms that are specifically designed to avoid this type of attack.
- MITM (Man-In-The-Middle) attack: There is no way to listen to a transaction and steal data because of the encryption systems used to sign communications within Blockchain networks. It is possible, however, if we expand the mesh of the definition of MITM attack, embracing not only the network but also the software that is part of it, identify some vulnerabilities such as editing the destination wallet in the transactions sent by the hardware ledger wallet or the theft of funds from wallets generated by weak private keys, where an attacker who possess the private key waits "in the middle" for a transaction to steal the funds in the very next block.
- Brute force/Dictionary attack: No way to brute force a private key correctly generated. The problems arise from the unsafe generation of the private key. Unfortunately, some wallets generate private keys directly from user-defined passwords without using any random numbers. This exposes users to this type of attack.
- Phishing attack: There is no architecture that is free from this type of attack because it does not depend on the intrinsic security of the software or hardware used, but exclusively on the human ability to understand and avoid being cheated.

Table 1 shows a comparison overview of vulnerabilities by type of architecture.

Table 1. Vulnerability comparison.

Attack	Cloud	RFID	NFC	Blockchain
Wrapping	X			
Eavesdropping	X	X	X	
Flooding	X			
Stealing Account	X			
MITTM	X	X	X	
Browser	X			
Reflection	X			
Session Hijacking	X			
Replay	X	X	X	
Brute force	X			
DoS/DDoS	X	X	X	
Skimming		X		
Phishing	X		X	X
User tracking			X	
Spoofing	X		X	

5.2. *Consensus*

Any node in the network can add information to its chain and share it in the network. It is, therefore, necessary that the other nodes in the network have a foolproof method to agree on the correctness of the information before any changes are added to the chain. Trust is a crucial aspect of this process, as no one can be sure of the reliability of the node that is adding information. It is critical that all new information must be reviewed and confirmed before it is accepted. In other words, to achieve this goal, a distributed review system called "consensus" is needed that definitively solves the problem of trust between nodes. In computing, a consensus algorithm is a process used to reach agreement on a single data value between distributed processes or systems. Consensus algorithms are designed to achieve reliability in a network that involves multiple potentially unreliable nodes. For a centralized network it is crucial that each participant read the same info. On the other hand, for a de-centralized system that means ensuring a sufficiently large number of nodes in the network are in agreement with what the transaction history is, and how to validate a transaction. This is what establishes the peculiar version of the truth in the Blockchain environment. A multitude of consensus-building algorithms have been developed over the years, and not all of them are suitable for use in an IoT architecture. Table 2 shows a comparison between the most used consensus algorithms in terms of type, scalability, finality a speed.

Table 2. General comparison between Consensus mechanism.

	PoW	PoS	DPoS	pBFT
Type	Permissionless	Both	Both	Permissioned
Scalability	Medium	High	High	Low
Finality	Probabilistic	Probabilistic	Probabilistic	Deterministic
Transaction/s	Low	High	High	High

5.2.1. Pow

The first algorithm ever used to reach a global consensus was the Proof of Work (Pow) [26]. The PoW has long been the most widely used method to achieve consensus within Blockchain architectures [27]. PoW, by searching for hash functions whose difficulty depends on the computational power of the entire network, makes it difficult to build a valid block and connect it to a Blockchain. Modifying a block requires the revalidation of the block itself, plus the revalidation of all subsequent blocks. The older the block to modify, the greater the number of validations needed. If you consider that only a few miners or groups of miners can generate new blocks every 10 min, even the change of the newly validated block is extremely expensive. This difficulty protects the chain of blocks from tampering; the longer the chain of blocks, the more difficult it is to reverse any previously recorded transaction. To manipulate the block chain, an attacker must have more than 50% of the entire PoW-based network's computing power. Although PoW provides an elegant solution for the global consensus of distributed ledgers, it has several inherent drawbacks first and foremost the electricity consumption required. This is of primary importance especially when thinking in terms of IoT where energy efficiency, computing power and installed memory have limits to be taken into account.

5.2.2. PoS

To avoid the problems associated with achieving consensus through excessive power consumption, an efficient alternative to PoW called Proof of Stake (PoS) has been introduced [28]. The system consists of a group of validator nodes that alternate by casting a vote on the next block, and the weight of each validator node's vote is directly proportional to the amount of its tied deposit. Safety and energy efficiency are among the most significant advantages of PoS. Improper behavior by a node can lead to the loss of the tied deposit. The Blockchain can thus operate more efficiently without the need for intensive energy consumption by the network obtaining as a direct consequence an economic stability of the network: the greater the amount tied by a node, the greater the probability that its behavior in the network will be correct.

5.2.3. DPoS

Unlike the PoS consensus system, the DPoS can be thought of as a representative democratic system [23]. This feature is implemented thanks to the opportunity for network participants to give their vote to one or more delegates to represent their stake in the network. DPoS offers several benefits for IoT applications:

- Pooling: Many small nodes can share their stakes, thus obtaining a higher chance together to participate in the proposals and in the vote for the next block, and share the rewards afterwards.
- Suitable for Resource-constrained nodes: Nodes with limited resources can choose their delegates and avoid running the node 24 h.
- Haigh availability: Single nodes can choose new delegates for each new block. This flexibility provides a high availability for the network reaching consensus.

5.2.4. pBFT

The Practical Byzantine Fault Tolerance (pBFT) is an algorithm born before the advent of Blockchain and was introduced by Castro [29,30] in 1999 as an efficient and attack-resistant algorithm to reach agreements in a distributed asynchronous network. The main architecture of a pBFT system consists of providing a practical Byzantine state machine replica that tolerates Byzantine failures by assuming that there are independent node failures and manipulated messages propagated by specific independent nodes. The main advantages of a pBFT system is the impressive execution time in reaching consensus and verifying valid transactions. The negative aspect is related to the extreme network overconnection and the high number of exchanged messages that can increase exponentially as the number of network nodes increases. As demonstrated by Castro on his paper [29], pBFT offers safety, availability and confidence in propagating accurate messages if at least two thirds of the network nodes are honest. The network cost of pBFT is really minimal compared to unreplicated network system. The model works very well only with small networks, because of the cumbersome amount of communication required between the nodes.

5.2.5. Others

1. Proof of Burn [31]: the probability for a specific node to success in mining new block is directly proportional to the number of coins burned by itself. The burning process consists of sending

tokens to a specific address that cannot send tokens. These tokens are thus 'burned' in the sense that they are no longer in circulation and therefore inaccessible. This is a similar idea to PoW but without wasting real world energy. Proof of burn has many of the same criticisms as PoS; the consensus is determined by the richest nodes in the network.

2. Proof of capacity [32,33]: Similar to Proof of Work, but uses storage instead of computation. Cryptographically signed data is written to the local storage according the following rules:

    - A very slow hash function is computed and stored. In the process, the hard drives are filled with groups of the precomputed hashes, and each group contains 4096 pairs.
    - While mining, a deadline time from a specific pair for each group is calculated. This deadline time represents the time to wait for mining another block after the last one.
    - The right to mine the next block is granted to the node who have the shortest deadline.

3. The Tangle [34,35]: the most famous alternative to standard Blockchain structures, 'The Tangle' use a DAG (Direct Acyclic Graph) to store transactions. Better explanation of this method used to achieve a different kind of consensus is reviewed in Section 8.1.
4. Hashgraph Consensus [36]: Similar to IOTA's Tangle, a DAG is created but following different rules. The new data structure named Hashgraph uses a gossip protocol to spread information throughout the network, and a virtual voting mechanism to achieve consensus involving random sync and validation between nodes. Any node can view the world from the perspective of any other node since last sync. In this way each node can determine if a given set of information or transactions is valid by checking if at least two thirds of the network's nodes have witnessed specific transaction.

Table 3 shows the different consensus versions used in major blockchain projects

Table 3. Popular Blockchain consensus mechanisms.

Project	PoW	~PoW	PoS	~PoS	DPoS	~DPoS	pBFT	~pBFT
Bitcoin [21]	SHA256							
Ethereum [37]	Ethash							
Litecoin [38]	Scrypt							
Monero [39]	CryptoNight							
HDAC [40]		EPoW						
Lynx [41]		HPoW						
Komodo [42]		dPoW						
Purple [43]		SSPoW						
Dash [44]			X					
Stellar [45]			X					
Cosmos [46]			X					
Vericoin [47]				PoST				
Shield [48]				PoS Boo				
XSN [49]				TPoS				
Reddcoin [50]				PoSV				
Cardano [51]				Ouroboros CA				
Tron [52]					X			
Bitshares [53]					X			
Steem [54]					X			
Ark [55]					X			
Lisk [56]					X			
EOS [57]						BFT DPoS		BFT DPoS
Zilliqa [58]							X	
Sawtooth [59]							X	
Neo [60]								DBFT

5.3. Cryptography and Hashing

Cryptography is the branch of cryptology that deals with "hidden writings", i.e., methods to make a message "blurred" so that it is not comprehensible/intelligible to people not authorized to read it. Cryptography before the modern age was synonymous to encryption and the use of these techniques date back as far as the ancient Egyptians, and have roots spanning all throughout history. Cesar Cipher and the World War II Enigma machine are two of the most iconic examples of historical encryption techniques. Blockchain technology makes use of cryptography in multiple different ways, from generating wallet keys, to securing transaction handling.

5.3.1. Cryptographic Hash Algorithm

A hash function is any function that can be used to map data of arbitrary size onto data of a fixed size [61]. This kind of functions are also useful in cryptography where this kind of functions allows one to easily verify whether some input data map onto a given hash value, but if the input data is unknown it is deliberately difficult to reconstruct it by knowing the stored hash value. Hash algorithm is the most commonly used cryptographic algorithm in the Blockchain architecture [62]. In Blockchain, hash algorithm is mainly used for wallet address creation, data integrity, data encryption, consensus computing and to link blocks together. It can compress messages of arbitrary length into binary strings of fixed length in a limited and reasonable time, and output hash value. Hash function has the characteristics of unidirectionality, hiding, collision resistant and puzzle friendliness (hard to find the right hash for a block, but easy to verify). Most used hash functions in Blockchain architectures include MD5 [63,64], SHA1 [65], SHA256 [63], and SM3 [66].

5.3.2. Asymmetric Encryption Algorithm

The real novelty of the last century is the invention of a cryptographic technique, called Asymmetric cryptography, that uses different keys to encrypt and decrypt a message, facilitating the task of key distribution. In Asymmetric cryptography the secret key is divided into two parts, a public and a private key. The public part ca be shared, while the private key must be kept secret. The public key can be made public for the sender to encrypt the information to be sent, and the private key can be used for the receiver to decrypt the received encrypted content. Blockchain technology uses cryptography as a means of ensuring transactions are done safely, while securing all information and storages of value. Therefore, anyone using Blockchain can have complete confidence that once something is recorded on a Blockchain, it is done so legitimately and in a manner that preserves security. The most commonly used and secure asymmetric encryption algorithms are Rivest–Shamir–Adleman (RSA [67]) and Elliptic-curve cryptography (ECC [68]).

6. Blockchain: Strengths and Weaknesses

Like any other software architecture, the Blockchain has both positive and negative aspects. Below is a list of the main ones:

Pros:

- Decentralization: As a decentralized and distributed technology, all transactions are decentralized, and verified by the network itself removing any single point of failure in a network of devices.
- Security: The use of public/private key pairs to sign transactions, specific hash functions to link block together and the peculiar consensus algorithms, gives to Blockchain systems a high resistance to tampering.
- Cost reduction: according to a Santander FinTech study [69], distributed ledger technology could reduce financial services infrastructure cost between US$15 billion and $20 billion per annum by 2022, providing the possibility to decommission legacy systems and infrastructures and significantly reduce IT costs.

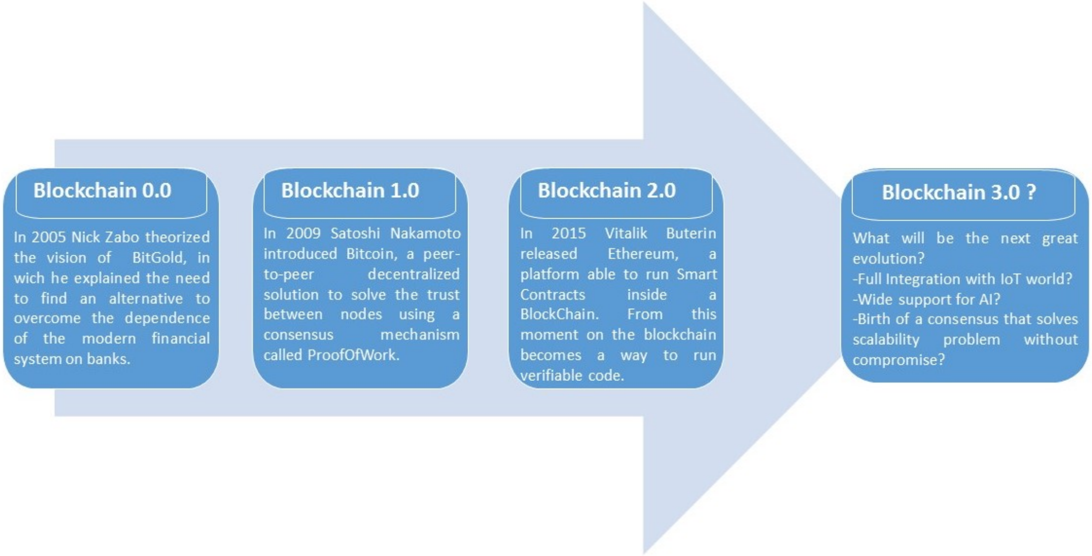
- Privacy & Transparency: The chain and its content are public and readable by anyone. Anyone can read and verify the honesty of every transaction but link a wallet(address) to a specific identity is not allowed by the protocol. There are some hacking strategies, however [70], to link a Blockchain address to a specific IP. To overcome this type of weakness, in addition to the use of Tor or VPN networks, specific Blockchain privacy-oriented projects have been developed [25,39]

Drawback[71]:

- Legal issues: In a decentralized environment where nodes exist around the planet, there is no way to establish a common jurisdiction. Different countries have very different approaches to titles, ownership, contracts, trademarks and liabilities. Some governments have made cryptocurrencies illegal in their territories [72].
- Volatility: All cryptocurrencies are from high to extremely high volatile. Cryptocurrency markets are not regulated, some exchange has suspicious volumes [73], and most of cryptocurrencies has very low volume compared to Bitcoin, exposing them to high speculative activity.
- Storage: Usually, to run a full node, the entire Blockchain should be synchronized locally (i.e., Bitcoin needs 200GB). This high demand for storage space makes adoption in IoT systems extremely complicated.
- Transaction speed: Bitcoin is restricted by mining block time and block capacity to handling up to 7 transactions per second while VISA has the peak capacity to handle 24,000 transactions per second [74]. Actually, no decentralized Blockchain project can reach such an order of magnitude.
- Lack of maturity and standards: Distributed Ledgers is an emerging technology. Many Blockchain projects are not production ready, partially untested, and will require early adopters to accept significantly increased risk levels over the next five to seven years.

7. Blockchain–IoT Projects

Although still early in the IoT adoption cycle, there are nevertheless many signs the market is maturing and more and more IoT devices are becoming a consistent part of our everyday lives [75–78]. The Blockchain concept has been in evolution for a decade (Figure 2), from the earliest solution like Bitcoin to the present multipurpose variations in different fields. However, Blockchain technology is continually improving its features and is striving to find an increasingly efficient implementation [79,80]. This paper summarizes the present and outline future development trends of Blockchain technology applied to IoT devices.



Blockchain 0.0

In 2005 Nick Zabo theorized the vision of BitGold, in wich he explained the need to find an alternative to overcome the dependence of the modern financial system on banks.

Blockchain 1.0

In 2009 Satoshi Nakamoto introduced Bitcoin, a peer-to-peer decentralized solution to solve the trust between nodes using a consensus mechanism called ProofOfWork.

Blockchain 2.0

In 2015 Vitalik Buterin released Ethereum, a platform able to run Smart Contracts inside a BlockChain. From this moment on the blockchain becomes a way to run verifiable code.

Blockchain 3.0 ?

What will be the next great evolution?
-Full Integration with IoT world?
-Wide support for AI?
-Birth of a consensus that solves scalability problem without compromise?

Figure 2. Blockchain evolution.

7.1. IOTA

IOTA [34,35] is the project with highest market cap [81] between all the IoT–Blockchain projects analyzed in this paper. The validation process is not based on consensus, no classical mining scheme, no fee required for the transactions. The data structure used to handle the transaction is a direct acyclic graph-based ledger called 'The Tangle' [35], in which when a node submits a transaction the system uses Markov Chain Monte Carlo (MCMC) algorithm to select two unconfirmed transactions to check if these do not produce conflicting results (Figures 3 and 4).

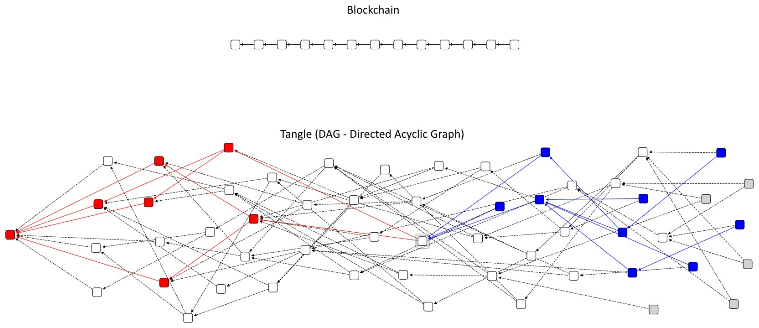


Figure 3. Classical Blockchain structure vs. Tangle.

IOTA uses Proof of Work as an anti-Sybil [82] measure. In this way the consensus and validation are done by the whole network of active participants by giving everyone an equal say in the network regarding the transaction making process. This is a radical shift of mind because differently from canonical Blockchain schemas, the Tangle is probabilistic. Full consensus for a transaction is only reached once (almost) all network participants have repeatedly certified that the transaction is more valid than another transaction. There is no global consistency in the tangle architecture. There is eventual consistency. This is related to the CAP theorem [83]. If a transaction is referenced directly or indirectly by every new transaction then it can be considered "confirmed" with high likelihood. Advantages over traditional Blockchain technology:

- Highly Scalable: Instead of storing transactions in blocks with a limited size, each transaction lives on its own and must approve two other transactions. With this method, the number of transactions that can be handled in a certain amount of time increases with the number of transactions.
- No fees: Each node validates its own and two other transactions. No block-mining required.
- Availability: Very high availability tanks to the Tangle architecture with no transaction to be inserted and mined in blocks with the danger of never being verified.
- Partition-Tolerant: Very High partition-tolerant system except for the presence of Coordinators.
- Quantum Computing resistant: A quantum-resistant algorithm called the Winternitz One-Time Signature Scheme is used to providing much better inherent security against the future quantum computer threat.

Main drawbacks:

- Coordinators: Is meant for assuring security in the early stage of the network as it grows. It will be eventually removed when the network becomes sufficiently large. Presently is a limit for decentralization and for partition-tolerance of the system.
- Milestones: Will be eliminated in the future but are important to avoid attack to the structure. Without them, the size of the ledger would grow to sizes too big to be handled by most nodes, primarily by IoT devices.
- Low consistency: There is no global state which everybody agrees to. Only after milestones, but will be eliminated in the future.

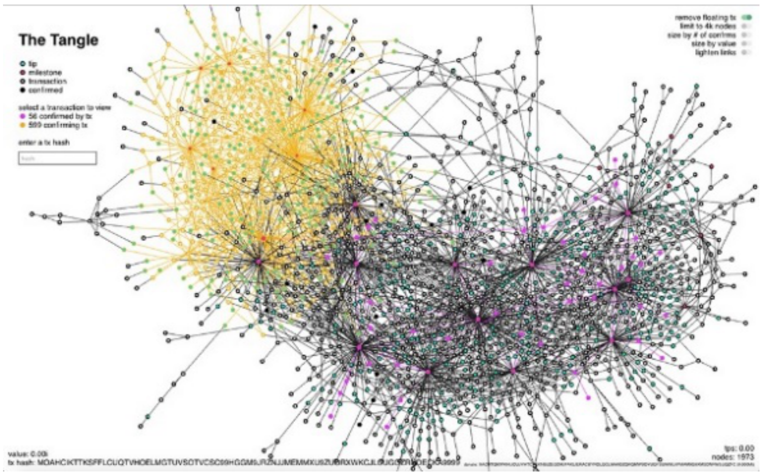


Figure 4. The Tangle live from http://tangle.glumb.de/.

7.2. VeChain

VeChain [84] is the second largest IoT/Blockchain family project by market cap to date. Largely based on Geth, the Go implementation of the Ethereum protocol, but with changes to support an alternative consensus algorithm called "Proof-of-Authority" , this project is a Blockchain-based platform that records the truth of what happens at every stage of the supply chain. Founded in 2015 by Sunny Lu, the former CIO of Louis Vuitton China, he combined his expertise in luxury goods with Blockchain technology to create an IoT application for supply-chain management. The VeChain client, "Thor Core" was designed to store supply-chain data and execute applications based on smart contracts. Every user who runs a node must do a KYC which aside token also track their reputation. VeChain economy consist of two different kind of coins:

- VeChain Token(VET): Store of value and smart payment currency.
- Thor power(VTHO): Same as gas for Ethereum but using a different coin from the base one. This coin is consumed every time a change to the Blockchain is necessary.

Two different kind of nodes exists in the VeChain Blockchain:

1. Authority node: There will only be 101 Authority Nodes and they validate all Blockchain transactions. Specific features are required to be elected as Authority node: KYC process, dedicated hardware and a minimum quantity of 250.000.000 VET blocked till the mainnet launch. There has been a lot of discussion in the VeChain community whether the identity of the 101 Authority Nodes should be publicly known. Single individuals with an Authority node can become a target once their identity gets publicly know. Enterprises that are currently owning an Authority node can also prefer to stay anonymous because they are not ready to publicly announce that they are using Blockchain technology or to stay ahead of competitors. A total of 30% of all gas (VTHO) consumed by Blockchain transaction is rewarded to the 101 Authority Masternode owners. To date no official list of Authority node exists, but only very few actors have confirmed their status: DNV GL [85], CAHrenheit [86].
2. Economic node: The VeChain Economy Masternode is different to the Authority Masternode in that it seeks to provide stability to the VeChain ecosystem by acting as a sort of tool to give dividend.

7.3. WaltonChain

WaltonChain [87] has a specific focus on RFID solution (the name of the project came from Charles Walton best known as the first patent holder for the RFID devices. As of VeChain they developed their in-house RFID solution. The firm claims that the RFID chips have improved sensitivity due to the optimized noise suppression technology used. They offer improved security for each IoT device as they use asymmetric random password pair generation and these are unique, authentic, and tamper-resistant. The mainchain called WaltonChain manages various sub chains, tracks WaltonCoin transactions and cross-subchain transactions, and executes smart contracts. The mainchain uses their unique Proof of Stake and Trust, an upgrade of PoS, consensus algorithm. When selecting the next block producer, PoST takes into account the quantity of staked WTC coins as well as the reputation of the nodes. Architecturally speaking, WaltonChain ecosystem uses an overall structure including a parent chain and subchains (or child chains) where the parent chain is WaltonChain and the token used for circulation and payment is called Waltoncoin.

7.4. IoTeX

Differently from WaltonChain, IoTeX [88] keep control on subchains maintaining a general consensus. By the other side, if one subchain is compromised, the root and therefore the others will have privacy breach. To ensure the integrity of the whole system, the consensus algorithm used is a specialized DPoS, in which 21–50 delegates are voted in and elected to mine for a certain number of blocks generated. IoTeX uses multiple Blockchains to interact with different segments of IoT devices or nodes based on the type of data or function. Transactions, unlike Bitcoin, are confidential using an interesting RingCT2.0 modified signature technique. The solution is to employ a secure multi-party computation (SMPC) protocol among a set of bootstrapping nodes of the Blockchain to generate secret domain parameters. The lightweight address system used does not require receiving addresses to scan the entire network to become aware of incoming transactions. IoT devices need to be light in terms of hardware resource, not able to record the full transaction history locally, and, in case of DPoS, the overhead for an IoT device that backs up online is not easily affordable. To address the problem, IoTeX implemented a periodic Checkpoint creation, solution already announced for Ethereum's upcoming Casper implementation. Each Checkpoint can be verified based on the previous Checkpoint, so that the light client can quickly follow the entire Blockchain without download a large number of public keys and signatures and then verify them all.

7.5. Ambrosus

Ambrosus (AMB) is a project that is looking to develop Blockchain tracking software for the food and pharmaceutical industry. They plan on combining high-tech sensors, smart contracts, and Blockchain protocols to create a secure supply chain where suppliers and consumers alike can track products to ensure authenticity, origin, proper handling and compliance in all areas. The Ambrosus protocol is based on the Ethereum Blockchain. The architecture is built in 4 different layers:

1. AMB-TRACE: Sensors and devices that generate data
2. AMB-EDGE-GATEWAY: Collect, preanalyze and push data
3. AMB-NET: Collect data in centralized data bases and in the Ethereum Blockchain
4. AMB-DASH: Dashboard tools to visualize data

7.6. HDAC

The Hyundai Digital Asset Company (HDAC) is created in 2017 through the cooperation of Hyundai BS&C, DEXKO, Doublechain, and Hyundai-Pay. The consensus mechanism is a modified Proof of Work protocol called ePoW where 'e' stands for 'Equitable chance' and 'Energy saving'. HDAC ePoW is an algorithm developed to reduce the mining monopoly by applying the block window concept. If a node succeeds in mining, no new block can be mined by the same node during the block window application period. Even if a greedy node neglects this mechanism and succeeds in mining a new block, it will not be recognized as a valid block by the HDAC Blockchain network. A private permissioned Blockchain network is a Blockchain with access privileges and may not be accessed by every node freely unlike a public Blockchain. The HDAC public Blockchain is permissionless and act as a coordinator for several private permissioned IoT-oriented Blockchains. To realize this interconnection HDAC Blockchain uses Bridge Node intermediaries that perform key configurations and access control through registration and pre-authentication operations. The block time has been set to 3 min, the maximum block size is up to 8 MB. Another interesting feature is the use of quantum random numbers [89] for a private Blockchains to create a very much effective and safe wallet, private key, and public keys address than pseudo-random number generator in use today.

7.7. IoTChain

Currently ranked around the 300th place in the market cap ranking of cryptocurrency market [90], IoTChain [91] differs from other projects in the way it implements the consensus. IoTChain uses Practical Byzantine Fault Tolerance (pBFT) to achieve main chain consensus, and use the DAG's IOTA structure for subchains. Until the mainnet swap occurs, the ITC tokens are based on Ethereum's ERC-20 standard [92] These tokens give a user the right to use a specific device. Single Payment Verification (SPV) derived from Bitcoin protocol, is used to verify the presence of a transaction inside a block without download the entire Blockchain. They also introduce the concept of ChainCode verification to preserve and remunerate personal data. Any company who intends to do big data analysis, receive aggregated data without access specific user data. After the execution of the analysis, users will be remunerated for being part of the analysis.

7.8. Others

There are an increasing number of Blockchain–IoT projects that have been implemented and are still in the start-up phase. Next the main ones:

- Vite [93] is one of the few existing projects that use a DAG structure with smart contract mechanism. The project extends the capability of the Solidity language (Solidity++) introducing an asynchronous architecture. The architecture relies on a DAG ledger structure called block-lattice. Like IOTA's project, VITE generates snapshot but using a new hierarchical HDPoS consensus algorithm; each account chain in the ledger generates local consensus results, and the snapshot chain at the highest level selects the final global consensus from the local consensus results.
- Nucleus Vision [94]: Using a sensor the people who decide to enter a shop are remunerated via mobile app using Nucleus Vision architecture. The sensor can sense mobile Id, temperature, motion, pressure, acceleration and sound. A deep learning infrastructure is used to optimize supply–demand.
- Ruff [95]: Ruff use DPoS for the consensus, specialized node to control the network. They have a development board kit and a JavaScript library to build IoT systems to connect.
- Modum [96]: Modum is a supply-chain system that integrates Blockchain technology, smart contracts and sensory devices into a single, passive solution. Core business of Modum is targeted to pharmaceutical companies that must employ expensive temperature-stabilized trucks and containers via 3rd party logistics providers to transport medicine. Modum offers a solution to substantially reduce these costs, by integrating a temperature sensor into medicinal shipments to monitor its temperature. All data is recorded into the Ethereum Blockchain, ensuring full transparency, accountability and data integrity.
- CPChain [97]: Cyber Physical Chain (CPChain) use a modified Byzantine Fault Tolerance algorithm (LBFT) to reach the consensus. They use an architecture called PDash in which the data is separated from the transactions using distributed data storage (IPFS) for data, and a Blockchain for the transactions.
- Yee [98]: To avoid data overload at node level, Yee project introduces a new concept for the distribution and retrieval of validated data across the network using a distance function and a corresponding routing table rule to retrieve relevant data from the correct nodes. To validate

transaction, the project introduces a third-party node called YeeWallet. Therefore, no direct transaction to Blockchain, but a hybrid permissioned/permissionless Blockchain.

8. Blockchain and IoT Main Use Cases

Every year IoT devices become more and more capable in terms of RAM and CPU, opening the door to a wide range of new use cases. The synergy with distributed ledgers is currently being tested in many application areas. Below are the main 4 areas (Figure 5) in which the Blockchain–IoT synergy is enjoying greater success and the largest number of projects.

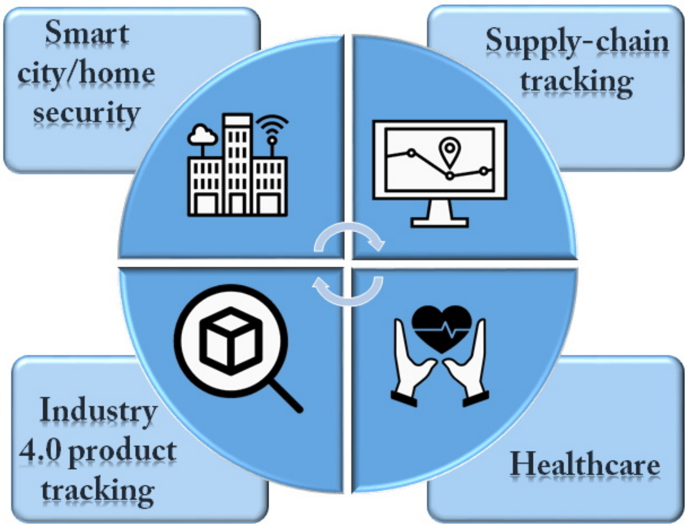


Figure 5. Blockchain and IoT main use cases.

8.1. Smart City/Home Security

In the new concept of smart city falls a multitude of innovations and new use cases purely technological that allow the coverage of areas previously unthinkable. Smart traffic lights, autonomous vehicles supervision, environment monitoring and tourist services are just some of the possible areas of interest where Blockchain and IoT can drive change. The birth of distributed renewable energy resources has reshaped the role of energy consumers from pure consumers to prosumers who can also generate and sell energy. New peer-to-peer networks were born that allow this kind of energy trading. However, ensuring security and trust within the network between commercial entities in the distributed energy sector is a complex challenge. The advent of Blockchain technology offers the opportunity to ensure secure energy trading on P2P networks. Some recent studies use Blockchain technologies to address these challenges, from consortium-based Blockchain [99], to privacy preserving transactions [100].

8.2. Healthcare

Healthcare becomes one of the main socio-economic problems due to the aging population while it also poses new challenges in traditional health services due to limited hospital resources. The recent SARS-CoV-2 pandemic has shown how entire national health services can go into crisis. Recent advances in the field of wearable health devices in health data bring opportunities in the promotion of remote health services at home or in clinics. Privacy protection and security assurance are crucial and still open challenges. Securing the IoT devices operating on healthcare networks using a Blockchain can potentially overcome these challenges. Griggs et al. [101] presented an architecture in which data generated by medical sensors are managed and shared through the use of smart contract. Throughout the whole procedure, privacy can be kept thanks to the underneath Blockchain.

An innovative solution has been introduced by Rahman et al. [102] where a Blockchain-based mobile edge computing framework is used for an in-home therapy management.

8.3. Industry 4.0 Product Tracking

The manufacturing industry in recent years is experiencing an improvement from automated production to so-called "smart production" [103]. Blockchain and IoT can help manage the incredible amount of data from the various supply chains: product design, raw material supply, manufacturing, recycling, distribution, retail and after-sales service. All this data raises a problem of interoperability that can be solved through a secure peer-to-peer standard based on a Blockchain network [104]. The rise of 5G networks provides a tremendous boost to the IoT devices that will run on them. In the Industrial sector many challenges and interesting scenarios are opening for this type of devices running on Blockchain networks [105]. Updating the firmware of the IoT devices is a crucial problem in the industry because these devices need to be updated regularly to remedy security breaches. A classic firmware upgrade scheme involves the use of cloud servers. If the cloud server is compromised, the device update is blocked and in the worst case, it could allow malicious firmware to be uploaded to company components. Pillai et al. [106] propose a Blockchain-based solution for managing firmware updates in IoT. It preserves the integrity of firmware by linking the latest version information by previous versions information with the help of a smart contract mechanism.

8.4. Supply-Chain Tracking

In industry, a supply chain is a set of activities, information, components and resources involved in delivering a product or service to a consumer. A final product often consists of multiple components forged and delivered by different manufacturers across countries. Deploy an anti-fraud technology in every part of the supply chain can be extremely expensive. Many studies have shown how the use of the Blockchain/IoT combination can efficiently solve the problem. Kim et al. [107] analyze a traceability ontology and translate some of its representations to smart contracts that execute a provenance trace and enforce traceability constraints on the Ethereum Blockchain platform. Kshetri [108] examines how Blockchain and IoT is likely to affect key supply-chain management objectives such as cost, quality, speed, dependability, risk reduction, sustainability and flexibility. Large IT-companies such as IBM, PWC , Almaviva and many others have their own frameworks currently in production in many supply chains based on Blockchain and IoT.

9. One Step Forward: Artificial Intelligence in a Blockchain–IoT Architecture: A Disruptive Research Vision

Recently, the application of artificial intelligence techniques in IoT systems has brought numerous advantages to the implementation of Blockchains. This obviously requires that the devices are provided with adequate computational capacity and that are able to efficiently optimize their energy consumption [109–112]. As example the use of IoT sensors with computational capacity will allow the activation of anti-fraud mechanisms that can prevent the incorrect activation of the exchange of cryptocurrency in the Blockchain due to tampering with IoT sensors. This will lead to an increase in security in the distributed ledgers which is the basis of the Blockchain technology. Furthermore, the processing of big data is an increasingly topical issue [113] and the companies that deal with it have the legal and moral responsibility to safeguard the data entrusted to them. Blockchains and AI can have a substantial impact on the way they are managed. All data on the Blockchain are validated and they cannot be tampered. This means that Blockchains are the perfect storage facility for sensitive or personal data that if treated with care using AI, can help unlock valuable personalized experiences for users. A good example is the healthcare, where data is used to detect, diagnose and prevent diseases [114–116]. In the near future it will be crucial to understand how AI, IoT and Blockchain can be used together. It might be useful to understand how AI can help Blockchain and vice versa.

Some of the applications would be big data management for AI, predictive models [117], investment management platforms.

10. Conclusions

This paper has provided a systematic review by discussing the application prospects of Blockchain technology in the IoT industry, the foundations of both systems, and the strategic importance of the Blockchain–IoT convergence. 500 articles and whitepapers has been screened as documented in PRISMA 2009 flowchart (Supplementary File S2). Some were discarded as non-innovative, too generic or not sufficiently IoT-oriented. At the end of the study 118 sources were used for the drafting of the article, including 23 online available Internet resource. 36 are whitepapers with a high risk of bias. In order to mitigate the bias issue, we proceeded to analyze the projects that had source code available and we also tested the related Blockchains. In summary, Blockchain technology has huge potential in IoT systems like supply chain, medical transportation and smart city [77]. But like any system still in an embryonic state, there are many challenges to be faced and risks to be considered. Specifically, this paper first introduced the principal security risks connected to IoT systems in Section 4, then the core theory of Blockchain technology, going deep into the 'consensus' algorithms and cryptography concepts in Section 5, ending with an excursus on the main projects in the Blockchain–IoT area. PRISMA 2009 checklist (Supplementary File S1) has been compiled. The following conclusions were drawn:

- Europe hosts the most important project, but Asia is the most powerful in promoting the link between Blockchain and IoT.
- The number of projects in Blockchain–IoT domain is growing fast and many are already in production stage.
- Big international players like Microsoft, Volkswagen, Fujitsu and countries like China have established important partnerships with existing projects.
- In financial terms, cryptocurrency traded on exchanges suffers extreme volatility, those related to the Blockchain and IoT world are also of a considerable scarcity of volumes.

Here are the remaining open issues and research directions:

- Storage: one of the main advantages of the Blockchain is its decentralization, but the ledger must be stored on the nodes themselves and IoT devices have low computational resources and very low storage capacity.
- Processing Power: Encryption and consensus algorithms can be very CPU-intensive and IoT systems have different types of devices which have very different computing capabilities [118], and not all of them will be able to run the same encryption algorithms at the required speed.
- Legal and Compliance: Blockchain is the very first architecture able to connect the entire world without a central control. Connecting countries with different laws without a legal supervision is a serious issue for both manufacturers and service.
- Scalability: In the Blockchain world there is a famous trilemma that says that if you want security and decentralization, it will be necessary to sacrifice scalability. Overcoming the Blockchain trilemma will lead to a new level of adoption for distributed ledgers.

Finally, the authors have briefly presented the future research trend that includes the introduction of AI mechanisms to enhance the capability of IoT devices in Blockchain systems.

Supplementary Materials: The following are available online at http://www.mdpi.com/2076-3417/10/19/6749/s1, Supplementary File S1: PRISMA 2009 checklist, Supplementary File S2: PRISMA 2009 flow diagram.

Author Contributions: Conceptualization, L.F. and A.P.; Methodology, A.P. and N.S.; Validation, A.P.; Investigation, L.F.; Resources, L.F.; Data curation, L.F. and A.P.; Writing—Original draft, L.F. and A.P.; Writing—Review and editing, L.F., A.P. and N.S.; Supervision, A.P. and N.S. All authors have read and agreed to the published version of the manuscript.

Funding: The APC was funded by Università degli Studi Guglielmo Marconi.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

PoW	Proof of concept
PoS	Proof of Stake
DPoS	delegated Proof of Stake
pBFT	Practical Byzantine Fault Tolerance
IoT	Internet of Things
DNS	Domain name server
DDoS	Distributed denial-of-service
RFID	Radio-frequency identification
SOAP2	Simple object access protocol v.2
MITM	Man-in-the-middle attack
SaaS	Software as a service
NFC	Near-field communication
PoS	Point of Sale
PKI	Public key infrastructure
DAG	Direct Acyclic Graph
KYC	Know your customer
IPFS	InterPlanetary File System

References

1. Giuliano, R.; Mazzenga, F.; Neri, A.; Vegni, A.M. Security access protocols in IoT capillary networks. *IEEE Internet Things J.* **2016**, *4*, 645–657. [CrossRef]
2. 3rd Cyberattack 'Has Been Resolved' After Hours of Major Outages. 2016. Available online: https://www.nbcnewyork.com/news/local/major-websites-taken-down-by-internet-attack/2040013/ (accessed on 10 August 2020).
3. SonicWall. 2018 SonicWall Annual Threat Report. 2018. Available online: https://d3ik27cqx8s5ub.cloudfront.net/sonicwall.com/media/pdfs/resources/2018-snwl-cyber-threat-report.pdf (accessed on 10 August 2020).
4. Tawfik, M.; Almadani, A.; Alharbi, A.A. A Review: The Risks And weakness Security on the IoT. *IOSR J. Comput. Eng.-(Iosr-Jce)* **2017**, 12–17, e-ISSN: 2278-0661, p-ISSN: 2278-8727.
5. Bastiaan, M. Preventing the 51%-Attack: A Stochastic Analysis of Two Phase Proof of Work in Bitcoin. In Proceedings of the 22nd Twente Student Conference on IT, Enschede, The Netherland, 23 January 2015.
6. Kulkarni, A.; Sathe, S. Healthcare applications of the Internet of Things: A Review. *Int. J. Comput. Sci. Inf. Technol.* **2014**, *5*, 6229–6232.
7. Samaniego, M.; Deters, R. Blockchain as a Service for IoT. In Proceedings of the 2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData), Berlin, Germany, 4–8 April 2016; pp. 433–436.
8. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
9. Minoli, D.; Occhiogrosso, B. Blockchain mechanisms for IoT security. *Int. Things* **2018**, *1*, 1–13. [CrossRef]
10. Novo, O. Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Int. Things J.* **2018**, *5*, 1184–1195. [CrossRef]
11. Ding, S.; Cao, J.; Li, C.; Fan, K.; Li, H. A novel attribute-based access control scheme using blockchain for IoT. *IEEE Access* **2019**, *7*, 38431–38441. [CrossRef]
12. Pieroni, A.; Noemi, S.; Brilli, M. Industry 4.0 revolution in autonomous and connected vehicle a non-conventional approach to manage big data. *J. Theor. Appl. Inf. Technol.* **2018**, 96, 10–18.
13. Scarpato, N.; Pieroni, A.; Di Nunzio, L.; Fallucchi, F. E-health-IoT universe: A review. *Management* **2017**, *21*, 46. [CrossRef]

14. Pieroni, A.; Scarpato, N.; Brilli, M. Performance Study in Autonomous and Connected Vehicles a Industry 4.0 Issue. *J. Theor. & Appl. Inf. Technol.* **2018**, *96*.
15. Arcidiacono, G.; Pieroni, A. The revolution lean six sigma 4.0. *Int. J. Adv. Sci. Eng. Inf. Technol.* **2018**, *8*, 141–149. [CrossRef]
16. Sumitra, B.; Pethuru, C.R.; Misbahuddin, M. A Survey of Cloud Authentication Attacks and Solution Approaches. *Int. J. Innov. Res. Comput. Commun. Eng.* **2014**, *2*, 6245–6253.
17. El Mouaatamid, O.; Lahmer, M.; Belkasmi, M. Internet of Things Security: Layered classification of attacks and possible Countermeasures. *Electron. J. Inf. Technol.* **2016**, *9*, 66–80.
18. Mitrokotsa, A.; Rieback, M.R.; Tanenbaum, A.S. Classifying RFID attacks and defenses. *Inf. Syst. Front.* **2010**, *12*, 491–505. [CrossRef]
19. Van Oort, L. Tap Track, NFC Relay Attacks. 2016. Available online: https://www.taptrack.com/article/blog/nfc-relay-attacks/ (accessed on 10 August 2020).
20. Dua, A. How Secure Is NFC Technology? 2019. Available online: https://rfid4u.com/how-secure-is-nfc-technology/ (accessed on 10 August 2020).
21. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 10 August 2020).
22. Housley, R. Public Key Infrastructure (PKI). In *Wiley Online Library*; 15 April 2004. Available online: https://onlinelibrary.wiley.com/doi/abs/10.1002/047148296X.tie149 (accessed on 10 August 2020).
23. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352. [CrossRef]
24. Biryukov, A.; Khovratovich, D.; Pustogarov, I. Deanonymisation of clients in Bitcoin {P2P} network. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014.
25. Sasson, E.B.; Chiesa, A.; Garman, C.; Green, M.; Miers, I.; Tromer, E.; Virza, M. Zerocash: Decentralized anonymous payments from bitcoin. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 18–21 May 2014; pp. 459–474.
26. Jakobsson, M.; Juels, A. Proofs of Work and Bread Pudding Protocols. In Proceedings of the Secure Information Networks: Communications and Multimedia Security, Leuven, Belgium, 20–21 September 1999; Springer: Berlin, Germany; pp. 258–272.
27. Cryptoslate. Proof-of-Work Coins. 2019. Available online: https://cryptoslate.com/cryptos/proof-of-work/ (accessed on 10 August 2020).
28. GoChain Team. Peercoin Explained: The Proof of Stake Pioneer. Available online: https://bitfalls.com/2018/03/11/peercoin-explained-proof-stake-pioneer/ (accessed on 10 August 2020).
29. Castro, M.; Liskov, B. Practical Byzantine Fault Tolerance. In Proceedings of the Third Symposium on Operating Systems Design and Implementation SE - OSDI '99, New Orleans, LA, USA, 22–25 February 1999; USENIX Association: Berkeley, CA, USA; pp. 173–186.
30. Castro, M.; Liskov, B. Practical byzantine fault tolerance and proactive recovery. *Acm Trans. Comput. Syst.* **2002**, *20*, 398–461. [CrossRef]
31. Karantias, K.; Kiayias, A.; Zindros, D. Proof-of-burn. In *International Conference on Financial Cryptography and Data Security*; Springer: Cham, Switzerland, 2020; pp. 523–540.
32. Gauld, S.; von Ancoina, F.; Stadler, R. The Burst Dymaxion. Available online: https://www.burst-coin.org/wpcontent/uploads/2017/07/The-Burst-Dymaxion1.00.pdf (accessed on 10 August 2020).
33. Dziembowski, S.; Faust, S.; Kolmogorov, V.; Pietrzak, K. Proofs of space. In *Annual Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 585–605.
34. Popov, S. The Tangle, IOTA Whitepaper. *White Pap.* **2017**. Available online: http://www.descryptions.com/Iota.pdf (accessed on 10 August 2020).
35. Popov, S. Saa, Finardi, Equilibria in the Tangle. *Comput. Ind. Eng.* **2019**, *136*, 160–172. [CrossRef]
36. Baird, L. *The Swirlds Hashgraph Consensus Algorithm: Fair, fast, Byzantine Fault Tolerance*; Technical Report SWIRLDS-TR-2016 1; Swirlds, Inc.: Richardson, TX, USA, 2016. Available online: https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf (accessed on 10 August 2020).
37. Buterin, V.; Dryja, T.E. Ethash. Available online: https://eth.wiki/en/concepts/ethash/ethash (accessed on 10 August 2020).

38. Lee, C. Litecoin Project. *Github*, 2019. Available online: https://github.com/litecoin-project/litecoin (accessed on 10 August 2020).
39. Van Saberhagen, N. Cryptonote v 2.0. 2013. Available online: https://cryptonote.org/whitepaper.pdf (accessed on 10 August 2020).
40. The Hdac Team. Hdac: Transaction Innovation—IoT Contract & M2M Transaction Platform based on Blockchain. 2018. Available online: https://github.com/Hdactech/doc/wiki/Whitepaper (accessed on 10 August 2020).
41. The Lynx Team. Technical White Paper 1.1. *White Pap.* **2019**. Available online: http://cdn.getlynx.io/2019-03-17_Lynx_Whitepaper_v1.1.pdf (accessed on 10 August 2020).
42. Komodo Team. Komodo: An Advanced Blockchain Technology, Focused on Freedom. Available online: https://komodoplatform.com/wp-content/uploads/2018/05/2018-05-09-Komodo-White-Paper-Full.pdf (accessed on 10 August 2020).
43. Octavian Oncescu. Purple Protocol—A Scalable Platform for Decentralized Applications and Tokenized Assets. Available online: https://purpleprotocol.org/whitepaper/ (accessed on 10 August 2020).
44. Diaz, D.; Duffield, E. The Dash Whitepaper. Available online: https://github.com/dashpay/dash/wiki/Whitepaper (accessed on 10 August 2020).
45. Mazieres, D. The stellar consensus protocol: A federated model for internet-level consensus. *Stellar Dev. Found.* **2015**, *32*. Available online: http://www.scs.stanford.edu/~dm/20160606-scp-talk.pdf (accessed on 10 August 2020).
46. Kwon, J.; Buchman, E. Cosmos: A Network of Distributed Ledgers. Available online: https://cosmos.network/resources/whitepaper (accessed on 10 August 2020).
47. Pike, D.; Nosker, P.; Boehm, D.; Grisham, D.; Woods, S.; Marston, J. Proof-of-Stake-Time Whitepaper. Available online: https://www.vericoin.info/downloads/VeriCoinPoSTWhitePaper10May2015.pdf (accessed on 10 August 2020).
48. Shield. PoS Boo, MNs and QP in Detail. Available online: https://medium.com/@shieldxsh/pos-boo-mns-and-qp-in-detail-6b9e61e3acee (accessed on 10 August 2020).
49. StakeNet Team. Trustless Proof of Stake (TPoS), Wallet Staking and Pooled Staking. Available online: https://stakenet.io/TPoS_Factsheet.pdf (accessed on 10 August 2020).
50. Ren, L. Proof of Stake Velocity: Building the Social Currency of the Digital Age. Self-Published White Paper. Available online: https://www.cryptoground.com/storage/files/1528454215-cannacoin.pdf (accessed on 10 August 2020).
51. Kiayias, A.; Russell, A.; David, B.; Oliynykov, R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2017*; Springer: Berlin, Germany, 2017; pp. 357–388.
52. The Tron Foundation. Advanced Decentralized Blockchain Platform. Available online: https://tron.network/static/doc/white_paper_v_2_0.pdf (accessed on 10 August 2020).
53. Schuh, F.; Larimer, D. Bitshares 2.0: General Overview. Available online: http://docs.bitshares.org/downloads/bitshares-general.pdf (accessed on 10 August 2020).
54. Larimer, D.; Scott, N.; Zavgorodnev, V.; Johnson, B.; Calfee, J.; Vandeberg, M. Steem An Incentivized, Blockchain-based Social Media Platform. 2016. Available online: https://assets.ctfassets.net/sdlntm3tthp6/resource-asset-r407/41cc9041e3d76a683feba1bc33ce5fdf/26069ed0-86be-43a3-9fb2-1523d3b52512.pdf (accessed on 10 August 2020).
55. ARK.io. Ark Ecosystem Whitepaper. Available online: https://ark.io/Whitepaper.pdf (accessed on 10 August 2020).
56. Beddows, O.; Kordek, M. The Lisk Protocol. Available online: https://lisk.io/documentation/lisk-protocol/index.html (accessed on 10 August 2020).
57. Larimer, D. EOS. IO Technical White Paper. Available online: https://github.com/EOSIO/Documentation (accessed on 10 August 2020).
58. Team, Z. The Zilliqa Technical Whitepaper. *Retrieved Sept.* **2017**, *16*, 2019.
59. Steeley L. Introduction to Sawtooth PBFT. Available online: https://www.hyperledger.org/blog/2019/02/13/introduction-to-sawtooth-pbft (accessed on 10 August 2020).

60. Team, N. NEO White Paper: A Distributed Network for the Smart Economy. Available online: https://docs.neo.org/docs/en-us/basic/whitepaper.html (accessed on 10 August 2020).
61. Rogaway, P.; Shrimpton, T. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In *International Workshop on Fast Software Encryption*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 371–388.
62. Wang, M.; Duan, M.; Zhu, J. Research on the Security Criteria of Hash Functions in the Blockchain. In Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, ACM Asia Conference on Computer and Communications Security, Incheon, Korea, 4–8 June 2018; Association for Computing Machinery: New York, NY, USA, 2018.
63. Rachmawati, D.; Tarigan, J.T.; Ginting, A.B.C. A comparative study of Message Digest 5(MD5) and SHA256 algorithm. In Proceedings of the Journal of Physics: Conference Series, 2nd International Conference on Computing and Applied Informatics 2017, Medan, Indonesia, 28–30 November 2017; IOP Publishing: Bristol, UK, 2018.
64. Gupta, P.; Kumar, S. A comparative analysis of SHA and MD5 algorithm. *Architecture* **2014**, *1*, 5.
65. Eastlake, D.; Jones, P. *US Secure Hash Algorithm 1 (SHA1)*; RFC Editor, USA. Available online: https://dl.acm.org/doi/book/10.17487/RFC3174 (accessed on 10 August 2020).
66. Kircanski, A.; Shen, Y.; Wang, G.; Youssef, A.M. Boomerang and slide-rotational analysis of the SM3 hash function. In *International Conference on Selected Areas in Cryptography*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 304–320.
67. Boneh, D. Twenty years of attacks on the RSA cryptosystem. *Not. AMS* **1999**, *46*, 203–213.
68. Koblitz, N. Elliptic curve cryptosystems. *Math. Comput.* **1987**, *48*, 203–209. [CrossRef]
69. Belinky, M.; Rennick, E.; Veitch, A. The Fintech 2.0 Paper: Rebooting Financial Services. *Santander InnoVentures/Oliver Wyman/Anthemis*, 2015. Available online: https://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2015/jun/The_Fintech_2_0_Paper_Final_PV.pdf (accessed on 10 August 2020).
70. Kaminsky, D. Black ops of TCP/IP 2011. *Black Hat USA* **2011**. Available online: https://www.slideshare.net/dakami/black-ops-of-tcpip-2011-black-hat-usa-2011 (accessed on 10 August 2020).
71. consultancy.uk. Blockchain Technology: How it Works, Main Advantages and Challenges. Available online: https://www.consultancy.uk/news/13484/blockchain-technology-how-it-works-main-advantages-and-challenges (accessed on 10 August 2020).
72. coin.dance. Bitcoin Legality by Country. Available online: https://coin.dance/poli/legality (accessed on 10 August 2020).
73. TheTIE. Exchange Real Trading Volume Investigation. Available online: https://docs.google.com/spreadsheets/d/13_L5V9elxQ3xps62BeYVyr_Wu-9vfyAyN5tGqLNoV9Y/edit#gid=1415549973 (accessed on 10 August 2020).
74. Visa.com. Visa Acceptance for Retailers Available online: https://usa.visa.com/run-your-business/small-business-tools/retail.html (accessed on 10 August 2020).
75. Evans, D. The internet of things: How the next evolution of the internet is changing everything. *Cisco White Pap.* **2011**, *1*, 1–11.
76. Bahga, A.; Madisetti, V.K. Blockchain platform for industrial internet of things. *J. Softw. Eng. Appl.* **2016**, *9*, 533–546. [CrossRef]
77. Pieroni, A.; Scarpato, N.; Di Nunzio, L.; Fallucchi, F.; Raso, M. Smarter city: Smart energy grid based on blockchain technology. *Int. J. Adv. Sci. Eng. Inf. Technol.* **2018**, *8*, 298–306. [CrossRef]
78. Orecchini, F.; Santiangeli, A.; Zuccari, F.; Pieroni, A.; Suppa, T. Blockchain technology in smart city: A new opportunity for smart environment and smart mobility. In *International Conference on Intelligent Computing & Optimization*; Springer: Cham, Switzerland, 2018; pp. 346–354.
79. Atlam, H.F.; Alenezi, A.; Alassafi, M.O.; Wills, G. Blockchain with internet of things: Benefits, challenges, and future directions. *Int. J. Intell. Syst. Appl.* **2018**, *10*, 40–48. [CrossRef]
80. Reyna, A.; MartíN, C.; Chen, J.; Soler, D. On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190.
81. CoinMarketCap. IOTA Capitalization. Available online: https://coinmarketcap.com/currencies/iota/ (accessed on 10 August 2020).

82. Douceur, J.R. The sybil attack. In *International Workshop on Peer-to-Peer Systems*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 251–260.
83. Brewer, E. CAP twelve years later: How the" rules" have changed. *Computer* **2012**, *45*, 23–29.
84. Team, V. Vechain Whitepaper. Available online: https://whitepaper.io/document/578/vechain-whitepaper (accessed on 10 August 2020).
85. DNV GL Buys Stake in VeChain and Announces Authority Masternode Status Medium. Available online: https://medium.com/@bsc44/dnv-gl-buys-stake-in-vechain-and-announces-authority-masternode-status-c42992a16a2e (accessed on 10 August 2020).
86. Cahrenheit. Introducing Cahrenheit. *Medium*. 2018. Available online: https://medium.com/@Cahrenheit/introducing-cahrenheit-cb017bf5dd6b (accessed on 10 August 2020).
87. Team, W. Waltonchain White Paper (V 1.0.4). Available online: https://www.digitalcoindata.com/whitepapers/walton-whitepaper.pdf (accessed on 10 August 2020).
88. Team, I. IoTeX: A Decentralized Network for Internet of Things Powered by a Privacy-Centric Blockchain. 2018. Available online: https://whitepaper.io/document/131/iotex-whitepaper (accessed on 10 August 2020).
89. Herrero-Collantes, M.; Garcia-Escartin, J.C. Quantum random number generators. *Rev. Mod. Phys.* **2017**, *89*, 015004.
90. CoinMarketCap. CoinMarketCap. IoTChain Capitalization. Available online: https://coinmarketcap.com/currencies/iot-chain/ (accessed on 10 August 2020).
91. Team, I. IoTChain Whitepaper. Available online: https://iotchain.io/whitepaper/ITCWHITEPAPER.pdf (accessed on 10 August 2020).
92. Buterin, V. A next-generation smart contract and decentralized application platform. *White Pap.* **2014**, *3*. Available online: https://people.cs.georgetown.edu/~clay/classes/fall2017/835/papers/Etherium.pdf (accessed on 10 August 2020).
93. Liu, C.; Wang, D.; Wu, M. Vite: A High Performance Asynchronous Decentralized Application Platform. Available online: https://static.coinpaprika.com/storage/cdn/whitepapers/6393951.pdf (accessed on 10 August 2020).
94. The Nucleus Team. Connecting the unconnected. *White Pap.* **2018**. Available online: https://cryptorating.eu/whitepapers/Nucleus-Vision/light-paper.pdf (accessed on 10 August 2020).
95. Ruff IoT Blockchain Whitepaper. Available online: https://cryptorating.eu/whitepapers/Ruff-Chain/WhitePaper.html (accessed on 10 August 2020).
96. Data Integrity for Supply Chain Operations, Powered by Blockchain Technology. Available online: https://modum.io/sites/default/files/documents/2018-05/modum-whitepaper-v.-1.0.pdf?utm_source=icogrind (accessed on 10 August 2020).
97. Decentralized Infrastructure for Next Generation Internet of Things. Available online: https://cpchain.io/download/CPChain_Whitepaper_English.pdf/ (accessed on 10 August 2020).
98. Yee: A Blockchain-Powered & Cloud based Social Ecosystem. Available online: https://doc.yeeco.io/YeeCo-V0.2-EN.pdf (accessed on 10 August 2020).
99. Li, Z.; Kang, J.; Yu, R.; Ye, D.; Deng, Q.; Zhang, Y. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3690–3700.
100. Aitzhan, N.Z.; Svetinovic, D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Trans. Dependable Secur.* **2018**, *15*, 840–852.
101. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J. Med. Syst.* **2018**, *42*, 130.
102. Rahman, M.A.; Hossain, M.S.; Loukas, G.; Hassanain, E.; Rahman, S.S.; Alhamid, M.F.; Guizani, M. Blockchain-based mobile edge computing framework for secure therapy applications. *IEEE Access* **2018**, *6*, 72469–72478.
103. Kusiak, A. Smart manufacturing. *Int. J. Prod.* **2018**, *56*, 508–517.
104. Liu, X.L.; Wang, W.M.; Guo, H.; Barenji, A.V.; Li, Z.; Huang, G.Q. Industrial blockchain based framework for product lifecycle management in industry 4.0. *Robot.-Comput.-Integr. Manuf.* **2020**, *63*, 101897. [CrossRef]
105. Mistry, I.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. *Mech. Syst. Signal Process.* **2020**, *135*, 106382. [CrossRef]

106. Pillai, A.; Sindhu, M.; Lakshmy, K.V. Securing firmware in Internet of Things using blockchain. In Proceedings of the 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Tamil Nadu, India, 15–16 March 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 329–334.
107. Kim, H.M.; Laskowski, M. Toward an ontology-driven blockchain design for supply-chain provenance. *Intell. Syst. Account. Financ. Manag.* **2018**, *25*, 18–27. [CrossRef]
108. Kshetri, N. 1 Blockchain's roles in meeting key supply chain management objectives. *Int. J. Inf. Manag.* **2018**, *39*, 80–89. [CrossRef]
109. Iazeolla, G.; Pieroni, A. Energy saving in data processing and communication systems. *Sci. World J.* **2014**, *2014*, 452863. [CrossRef] [PubMed]
110. Pieroni, A.; Iazeolla, G. Engineering QoS and energy saving in the delivery of ICT services. In *Sustaining Power Resources through Energy Optimization and Engineering*; IGI Global: Hershey, PA, USA, 2016.
111. Iazeolla, G.; Pieroni, A. Power management of server farms. *Appl. Mech. Mater.* **2014**, *492*, 453–459. [CrossRef]
112. Bracciale, L.; Loreti, P.; Detti, A.; Paolillo, R. Melazzi Lightweight named object: An ICN-based abstraction for IoT device programming and management. *IEEE Internet Things J.* **2019**, *6*, 5029–5039. [CrossRef]
113. Arcidiacono, G.; De Luca, E.W.; Fallucchi, F.; Pieroni, A. The use of Lean Six Sigma methodology in digital curation. In Proceedings of the First Workshop on Digital Humanities and Digital Curation Co-Located with the 10th Conference on Metadata and Semantics Research (MTSR 2016), Goettingen, Germany, 22 November 2016.
114. Ferroni, P.; Zanzotto, F.M.; Riondino, S.; Scarpato, N.; Guadagni, F.; Roselli, M. Breast cancer prognosis using a machine learning approach. *Cancers* **2019**, *11*, 328. [CrossRef]
115. Ferroni, P.; Zanzotto, F.M.; Scarpato, N.; Riondino, S.; Nanni, U.; Roselli, M.; Guadagni, F. Risk Assessment for Venous Thromboembolism in Chemotherapy-Treated Ambulatory Cancer Patients. *Med Decis. Mak.* **2016**, *37*, 234–242. [CrossRef]
116. Guadagni, F.; Scarpato, N.; Patrizia, F.; D'Ottavi, G.; Boavida, F.; Roselli, M.; Garrisi, G.; Lisi, A. Personal and sensitive data in the e-health-IoT universe. In *International Internet of Things Summit*; Springer: Cham, Switzerland, 2015; pp. 504–514.
117. Cardarilli, G.C.; Nunzio, L.D.; Fazzolari, R.; Giardino, D.; Matta, M.; Patetta, M.; Re, M.; Spanò, S. Approximated computing for low power neural networks. *Telkomnika* **2019**, *17*, 1236–1241. [CrossRef]
118. Cardarilli, G.C.; Di Nunzio, L.; Fazzolari, R.; Re, M.; Silvestri, F.; Spanò, S. Energy consumption saving in embedded microprocessors using hardware accelerators. *Telkomnika* **2018**, *16*, 1019–1026. [CrossRef]