Dependable IoT using blockchain-based technology

Avelino F. Zorzo*, Henry C. Nunes*, Roben C. Lunardi*†, Regio A. Michelin*† and Salil S. Kanhere‡
*Pontifical Catholic University of Rio Grande do Sul (PUCRS) - Porto Alegre, Brazil
†Federal Institute of Rio Grande do Sul (IFRS) - Porto Alegre, Brazil
‡University of New South Wales (UNSW) - Sydney, Australia
E-mail: avelino.zorzo@pucrs.br, {henry.nunes,roben.lunardi, regio.michelin}@acad.pucrs.br, salil.kanhere@unsw.edu.au

***Abstract*—In the last few years, novel approaches for using blockchain to solve Internet of Things (IoT) security and dependability issues have been proposed. Currently, different solutions were applied to Smart Homes, Smart Cities, Smart Grids, Supply Chains, Industry, and Vehicular Networks scenarios. Despite of that, the main advantages on the adoption of different architectures, models and algorithms proposed in the state of art of blockchain in IoT scenarios are not yet clear. This paper presents some discussion about the usage of blockchain technology in IoT environments and proposes a layer model of blockchains for IoT. In addition, we present an overview of the latest research regarding network architectures, consensus algorithms, data management, and applications. Finally, this paper presents open issues and future trends about blockchain in IoT.**

***Index Terms*—Blockchain, Internet of Things, Distributed Ledgers**

I. Introduction

Currently, there are billions of different devices collecting data and providing services through the Internet. Some of these devices collaborate to exchange information and to take smarter decisions. These kind of smart devices - or just things - became part of the environment called Internet of Things (IoT) [1]. However, these devices - usually with limited storage space and processing power - are more likely to be affected by attacks from malicious entities. For example, the Mirai botnet [2] used, mainly, IoT devices with their default configuration (specially default user and password) to attack a Dynamic Domain Name Server (DNS) provider, *i.e.* Dyn DNS. Thus, millions of devices, *e.g.* smart TVs, vacuum cleaners, and domestic routers, were used to produce this Distributed Denial of Service (DDoS) attack. Consequently, different applications and services, which were using this Dynamic DNS provider, became unavailable [2].

This type of problem could be avoided if new technologies were applied in an IoT environment. In 2008, the blockchain concept was introduced by Bitcoin [3], a peer-to-peer (P2P) cryptocurrency focused on tamper-resistance, resilience and non-repudiation. Due to the characteristics introduced by Bitcoin, some research discussed the benefits of adopting blockchain technology for IoT in order to mitigate security and dependability issues [4], [5], [6]. In recent years, several blockchain proposals have been introduced for different areas, for example, Smart Homes/Offices [7], [8], [9], Smart Vehicles [10], [11], [10], [12], Industrial IoT [13], [14], [15] and Smart Grids [16], [17], [18].

Despite the contribution in different IoT contexts, it is hard to compare the adoption of each blockchain proposal. For example, both Smart Vehicle and Smart Grid environments have sensitive user data, but in the former mobility is an important issue, while in the latter, the network is mostly static. Likewise, pricing and payments in Smart Grids are a key feature, while not necessarily in Smart Vehicles. Hence, it is important to categorize the different blockchain aspects, such as, communication technologies, concepts, or even types of applications, that can be used/applied in a dependable IoT environment.

Therefore, this work presents: (*i*) an overview about blockchains and the main proposals for IoT; (*ii*) a model to categorize the different blockchain aspects; (*iii*) main research contributions in each layer of the proposed model; (*iv)* some open issues and possible research directions.

The reminder of the paper is organized as follows. Section II presents an overview about main blockchain implementations and their main characteristics. Section III discusses the main blockchain proposals for IoT scenarios. Section IV presents the main contributions in each layer of the proposed blockchain layer model. Section V presents some open issues for blockchain in IoT and possible future research directions. Finally, we conclude the paper conveying final considerations.

II. Blockchain Background

Early in 2008, an "entity" (no one knows whether that "entity" is a person or group) published a paper through the Satoshi Nakamoto pseudonym (even today their identity remains hidden), describing a cryptocurrency called Bitcoin [3]. The paper presented an electronic cash system running over a peer-to-peer (P2P) network that allows two different parties to exchange some cryptocurrency directly, without using a third party to mediate the operation.

In Bitcoin, transactions involving two parties are created and stored in a block. Thus, each block contains a set of transactions. On one hand, these transactions are organized in a Merkle tree through a hash chain [19]. On the other hand, blocks are ordered and sequentially connected through the previous block hash value. The blockchain concept is based on this block link strategy, which differs from the hash chain used in the Merkle tree.

978-1-5386-8489-4/18/$31.00 ©2018 IEEE
DOI 10.1109/LADC.2018.00010

TABLE I
BLOCKCHAIN COMPARISON (DATA COLLECTED ON 08/27/2018)

	Chain Size (GB)	Chain Length (blocks)	Chain Access	Consensus	Main Usage
Bitcoin	212.11	539,220	Public	PoW	Monetary transactions
Ethereum	667.10	6,242,022	Public/Private	PoW	Transactions and Smart Contracts
Litecoin	18.78	1,483,290	Public	PoW	Monetary transactions
Ripple	N/A	N/A	Public	Adapted PBFT	Monetary transactions
BlackCoin	4.34	2,242,924	Public	PoS	Monetary transactions
IOTA	5.4	111,714	Public	PoW	Monetary and information transactions
Hyperledger Fabric	-	-	Permissioned	PBFT	Transactions and Smart Contracts

Before a block is inserted into the blockchain, first a consensus algorithm has to be executed. There are different types of consensus algorithms that might be executed before inserting a transaction in a block, for example, Proof-of-Work (PoW), Proof-of-Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT). Bitcoin, for example, uses PoW consensus algorithm (sometimes called a mining process), while BlackCoin [20] secures its blockchain through PoS algorithm. BlackCoin uses a process called minting, instead of mining, to validate transactions based on the amount of coins that the peers own.

Initially, blockchain was used as distributed public ledger for cryptocurrencies, for example, in Bitcoin or Litecoin [21]. However, lately, new concepts were added to blockchain making its applicability wider. For example, blockchains, such as Ethereum [22], introduced the smart contract concept, which allows a user to write a piece of code and add it to the blockchain. Furthermore, in terms of application areas, blockchains are also being used to make some operations faster than they were before. For example, the Ripple blockchain [23] consists of a decentralized permissioned ledger used in the banking system, and through that, changed the way banks are exchanging money.

Two other blockchains that are worth mentioning are the Hyperledger Fabric and IOTA:

- Hyperledger was presented by Linux Foundation, in December 2015, as an umbrella for different blockchain initiatives. Its main focus is to define a cross-industry open standard platform for distributed ledgers. Different types of blockchains can be implemented under Hyperledger, even to provide blockchain infrastructure as a service, *i.e.* Blockchain-as-a-Service (BaaS), and over this infrastructure developers are encouraged to create new applications. One implementation from Hyperledger, the Hyperledger Fabric [24] proposes a distributed ledger platform for running smart contracts. Fabric architecture is modular and uses PBFT consensus algorithm, however the consensus algorithm is executed only to *validate peers* that are also responsible for maintaining the ledger. Additionally, there are peers called *non-validating* in charge of connecting different clients and validating peer transactions. Thus, Hyperledger Fabric [25] works as a permissioned blockchain and, due to this characteristic, its chain size and length depend on its configuration and purpose (see Table I) [26].
- The IOTA blockchain proposal is focused to attend IoT needs [27]. Its main difference from the original blockchain is how data are organized. While in the original blockchain blocks are organized and linked sequentially, IOTA uses a Directed Acyclic Graph (DAG) to link blocks. The IOTA DAG is called Tangle and organizes blocks in a graph structure. Before a new block is inserted into the DAG, the insertion algorithm chooses two random unconfirmed blocks (blocks that are in the DAG but were not confirmed yet), confirms the PoW of these two blocks, and the new block points to these two, now confirmed, blocks. Important to mention that this new block, which has now been inserted into the DAG, will be confirmed when another block is inserted into the IOTA DAG. Transactions, in a block, can contain monetary values (similar to a regular cryptocurrency transaction) or a zero value, in that case the transaction holds, then, any other type of information. Although, IOTA has been used for IoT, it cannot be applied to low processing power IoT devices due to the PoW consensus algorithm [28].

Several other blockchain initiatives have been developed in the past years, for example SpeedyChain [8], Waves [29], Stellar [30], and it is very likely that new ones will be designed in the near future. It is important to mention that there is no blockchain standard yet, but several researchers are discussing the way blockchain is changing the way applications will be developed and how they will interoperate.

III. BLOCKCHAIN IN IoT

Analogous to the blockchain usage in other areas, IoT benefits from the resilience of blockchains. They can maintain a system working even in an attack to a device or its unavailability, avoiding single points of failure and giving high availability to the IoT network. The form in which information is appended to the blockchain ensures transparency, tampering resistance and non-repudiation.

However, there are problems regarding the use of blockchain in IoT. Among them, the most relevant one is related to the hardware capabilities of devices that run on the IoT context. This limitation implies the need for lightweight solutions and, as presented in Table I, most of the blockchain technologies size (measured in gigabytes) make them inapplicable for IoT. Even the BlackCoin blockchain, which is the smallest evaluated blockchain, might not be applicable since its size still too big for some of the IoT devices. This size is big mainly

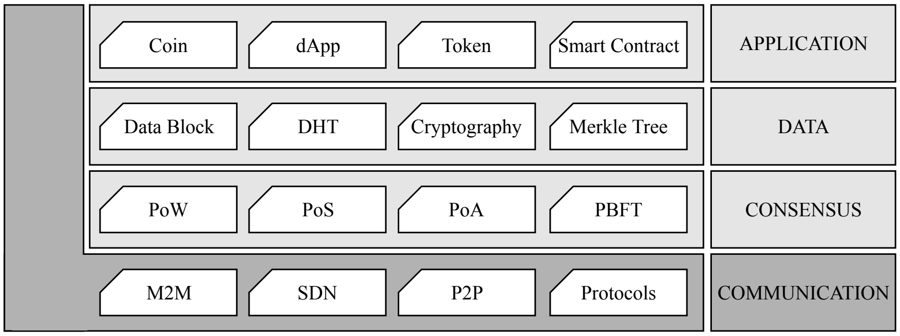

Fig. 1. Sample of concepts applied to each blockchain layer.

due to the public access property present in the blockchains, which is required to keep historical track of every transaction.

Another problem regarding hardware limitation is related to computing power of IoT devices. For example, some of the main blockchains, *i.e.* one that is used in the Bitcoin and IOTA, applies the PoW consensus algorithm, which uses hash brute force calculation and, therefore, demands a lot of time, processing power and energy to achieve consensus. Basically, the consensus algorithm, applied to the Bitcoin blockchain, ensures that peers, through work, validate each block that is going to be inserted into the blockchain. Hence, if someone would consider the PoW consensus algorithm in the IoT context, it would probably not fit the IoT devices restrictions. Table I shows the consensus algorithms that are used by some of the current blockchains.

The consensus algorithm is required in IoT context specially for its characteristic, where the network is public and there might not be trust among peers. Thus, consensus plays a crucial role for ensuring that each new block contains valid information, and any peer is able to verify the information stored in the blockchain. The unreliable peer environment, where a blockchain is executed, could be considered in order to provide a solution to a common authentication problem, which is related to have a third party involved. In an authentication context, the third party is responsible to assure the trust in each party involved in the authentication process.

In order to overcome these problems, some research proposed the adoption of an hierarchical P2P architecture [7] [10] [8] [11]. In this kind of architecture, supernodes (also called overlays or gateways) are responsible to control devices and to communicate with other supernodes in order to maintain the blockchain. Alternatively, other solutions propose the adoption of a blockchain separated from IoT devices, providing a blockchain service to IoT devices [13] [6]. Moreover, some proposals execute smart contracts on the blockchain supernodes, thus reducing processing on limited devices [4] [31] [32].

Although current research present strategies to overcome the issues of the adoption of blockchain in IoT, it is hard to compare and to adapt the proposed solutions for different scenarios. In order to do that, we proposed a blockchain layer model to present the main concepts and how they interact. We believe this can facilitate the adoption of the right blockchain solution.

IV. Blockchain Layer Model

In order to help understanding the different concepts that could be used and how they impact a blockchain, we categorize blockchains into four layers as presented in Fig. 1. This figure shows some of the algorithms or concepts that are associated to each layer. Fig. 1 does not present all the concepts that can be associated to each layer.

The next sections will detail each of the blockchain layers as presented in Fig. 1 and some of the technologies or concepts that are used in each layer.

A. Communication Layer

Communication between nodes can be performed using different network protocols. Due to hardware limitation, there are specific protocols recently proposed for IoT. For example, Özylmaz and Yurdakul [33] presented a work in progress for the adoption of blockchain using a LoRaWAN network. Also, Dey *et al.* [34] proposed the adoption of blockchain to maintain data from biosensors using the MQTT protocol [35]. Additionally, some proposals adopt blockchain in industrial environments using machine-to-machine (M2M) protocols [36] [37]. Although not common yet, communication can also be performed with recent network standards using, for example, Software Defined Networks (SDN) [38] [18]. The use of SDN allows more flexibility to design the network and the way devices can be accessed. Despite the new communication protocols that can/are used in IoT, most solutions adopt standard TCP/IP protocol to perform the communication in IoT environments [7], [8], [13], [32].

Moreover, there are different P2P architectures that can be used for setting up the network (see Fig. 2). This includes a completely distributed architecture, where each node is a full node, *i.e.*, each device communicates directly to other devices in the network. This kind of architecture requires that all devices have enough computing power, battery and other hardware requirements for maintaining the blockchain [36], [37]. This kind of architecture is mostly used in Smart Grids applications.

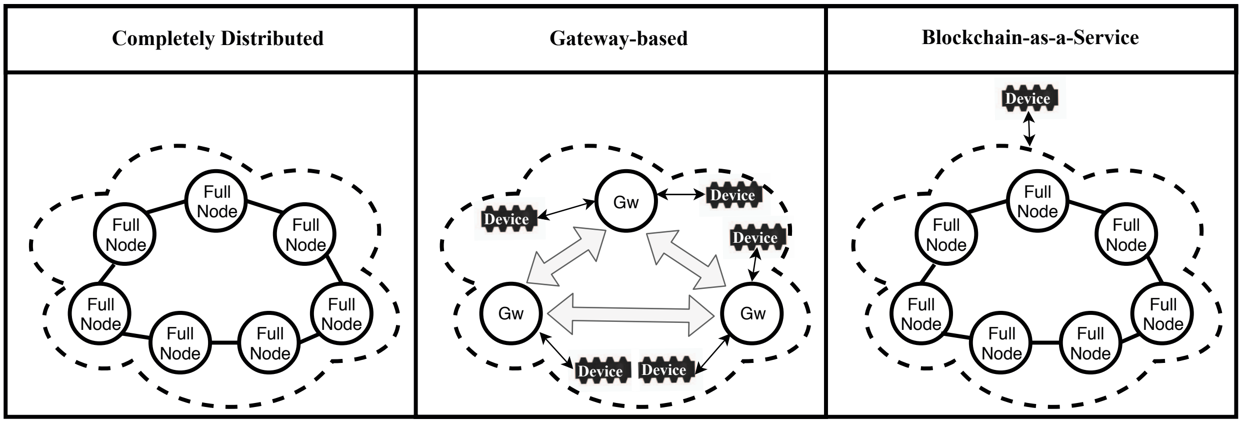

Fig. 2. P2P architectures used in blockchains.

In order to mitigate the hardware strict requirements problems, some proposals adopted a hierarchical P2P architecture (Gateway-based architecture in Fig. 2). In that environment, supernodes (also called gateways or overlays) are used to maintain a blockchain with devices information [7], [8]. This kind of solution leads to a reduction on the traffic generated through Smart Environments networks and decreases the vulnerability of the devices. However, these architectures are more susceptible to the Eclipse attack [39], *i.e.*, when a malicious gateway monopolizes device incoming and outcoming connections.

Another type of blockchain architecture separates the nodes that control the blockchain from the IoT network (see Fig. 2), providing Blockchain-as-a-Service (BaaS) [13], [6]. Consequently, most of, if not all, blockchain processing can be performed by a third-party infrastructure, reducing the computing cost for IoT devices. For example, in the work presented by Boudguiga *et al.* [13], IoT devices availability is updated in the blockchain through encrypted messages. However, the trust is delegated to a third-party authentication authority, hence, the IoT devices may become susceptible to security issues if the third-party blockchain or its API is compromised.

B. Consensus Layer

As mentioned before, there are different consensus algorithms [40] available to be used in blockchains to guarantee that a new block inserted in the blockchain is valid. The main algorithms that can be used in blockchains for IoT are:

- **Proof-of-Work (PoW)**: consists in solving a resourcing consuming puzzle to avoid an overload of information to be created. Usually, the task is composed by the generation of a hash for data with a minimum zeros at the beginning of the hash value. After the block is created, it is broadcast to other peers, and it can be easily verified (compare the received hash with the block hash). IOTA [27] is the most prominent adopter of PoW consensus for blockchain in IoT;
- **Proof-of-Stake (PoS)**: an alternative to the PoW algorithm, PoS uses a random selection of nodes based on wealth or aging of coins. PoS preserves a single branch, as only a single node is responsible for producing a block. Although PoS has the objective to reduce the processing needed to create a block, to the best of our knowledge, there is not a blockchain for IoT using PoS consensus;
- **Byzantine Fault Tolerance (BFT) based algorithms**: there are different implementation of BFT, for example, Practical Byzantine Fault Tolerance (PBFT). This algorithm requires that more than 2/3 of the nodes, in the network, vote that a new block is valid. One prominent work that uses PBFT was proposed by Zhou *et al.* [41].

There are other consensus algorithms, such as Proof-of-Space and Proof-of-Authority (PoA), and some other implementations of BFT, such as delegated Byzantine Fault Tolerance (dBFT) and Federated Byzantine Agreement (FBA). However, to the best of our knowledge, there are no proposal about their application for blockchain in IoT.

A seminal discussion about consensus algorithms for blockchain in IoT is presented in Christidis [4] research. This research investigated different consensus algorithms and concluded that the mechanism used in blockchains depends on two factors: the architecture in which it will be used and the attack vector that is intended to be mitigated. Consequently, the number of nodes and the processing overhead are important issues to be considered when choosing the consensus algorithm.

Although a consensus algorithm is a key aspect of a blockchain, most of the blockchain proposals for IoT did not discussed or evaluated their usage [42], [32], [8], [9], [11], [7]. Consequently, dependability, security and performance can be affected when a consensus algorithm is introduced in the blockchain.

C. Data Layer

Based on different research analysis, there are differences related to data structure and cryptography algorithms being applied to different blockchain solutions [3], [11], [43], [27].

Initially, the first blockchain proposals structured their data through blocks and transactions. The main difference is that

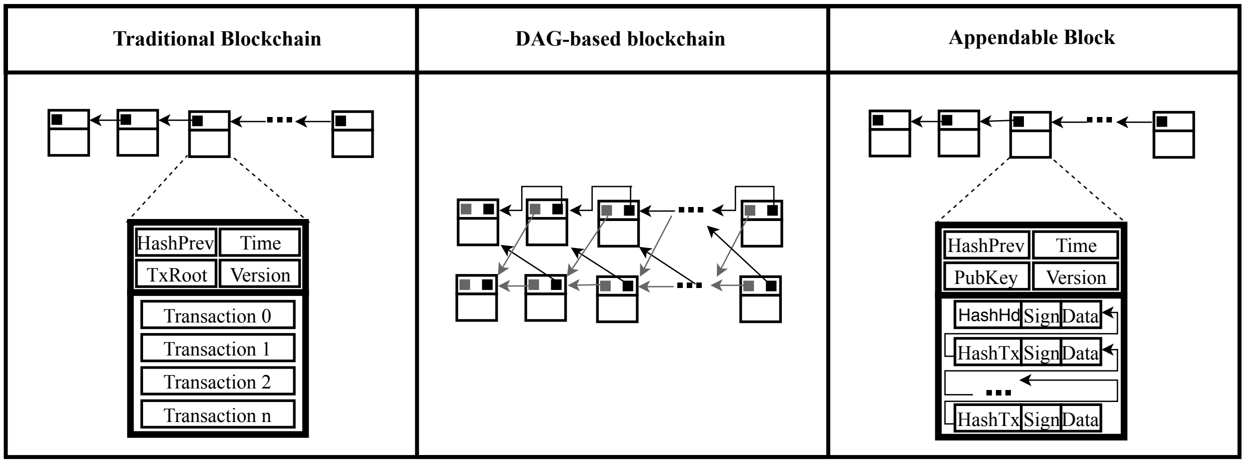

Fig. 3. Block structure.

transactions are the data structure where some information is stored. Alternatively, the block is used to store the information required to create the chain, *i.e.*, the structure is defined to support the link between blocks, where each block has a reference to its direct ancestral. Transactions are organized inside each block and could follow different arrangements, such as, Merkle tree [3], linked list [3], Direct Acyclic Graph (DAG) [27], contained immutable [3], [27], [25], appendable data inside a block [8], [11] or erasable [44] blocks. Some examples of how blocks and transactions are organized in a blockchain are described next:

- The Bitcoin blockchain uses a Merkle tree to arrange the transactions inside a block (see Fig. 4). In this case each block contains an immutable amount of transactions, *i.e.*, once the hash of transactions are inserted in the Merkle tree inside a block, no further action (adding or removing a transaction) can be taken (see Fig. 3 - Traditional Blockchain). Also, the Bitcoin blockchain uses a linked list to arrange the blocks list, keeping the sequence, and linking a previous block to its parent.
- In SpeedyChain the transactions are stored inside blocks, where the first transaction is linked to the block header (through block header hash), while other transactions are linked to the previous transaction, through the hash of the previous block (see Fig. 3 - Appendable Block). Thus, this leads to an appendable block, *i.e.*, a block that can still receive new transactions after inserted into the blockchain. In SpeedyChain, blocks are not immutable, however after the information is inserted both in block header and in transactions they are hashed, preserving their integrity.
- IOTA, uses a DAG structure (called Tangle) [27] to block arrangement in its blockchain. This DAG consists of a graph without direct cycles as shown in Fig. 3.

In order to support these data arrangements and still ensure security - data integrity and privacy - the cryptography algorithms are a central piece in this structure. Among algorithms applied to blockchains we could highlight asymmetric and symmetric ciphers to guarantee privacy, and hash functions to keep data integrity. For example, the Bitcoin blockchain applies the Elliptic Curve Digital Signature Algorithm (ECDSA) in order to create the public/private key pair, which is used as a wallet address, and for the block hash, it uses the SHA256 hash function. Ethereum [22], instead of using the SHA256, uses SHA3. SpeedyChain [11] relies in the SHA256 hash function and RSA for the asymmetric cryptography algorithm.

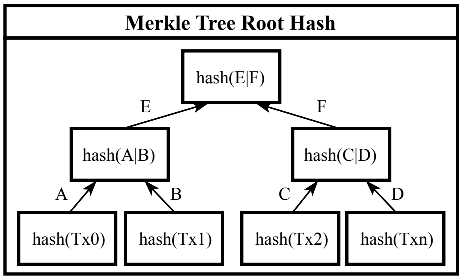

Fig. 4. Merkle tree structure.

D. Application Layer

The “Application” layer is responsible for managing the different applications that run using blockchain, for example, digital money or cryptocurrencies. Currently, there are several available cryptocurrencies [45]. Usually, a coin is used in transactions to represent a cryptocurrency exchange between two users in a blockchain. Basically, there are two manners to obtain a coin: acquiring (through a transaction) from a user or mining. In the IoT context, IOTA (and its coin MIOTA) [27] was created to be used for M2M payments. IOTA is, currently, the most known and representative cryptocurrency for IoT [46]. Coins can also be used in different applications, for example, Smart Grids [37].

Another type of application that can run on this layer is the one based on tokens. Tokens are a fraction of a coin from a blockchain and they can represent different assets or utilities. The main difference between a coin and a token, is that a coin represents a cryptocurrency in the blockchain, for example, an ether from the Ethereum blockchain; while a token does not necessarily represent cryptocurrency. The token definition from Ethereum is the most popular one and some standards for its use have already been defined, *i.e.* ERC-20 and ERC-721 [22].

Although cryptocurrencies and tokens were the most common uses for blockchains, its infrastructure enabled and disseminated the distributed programming paradigm in a way that had not been seen before. The blockchain infrastructure has been applied in application development and it is the basis for what has been called decentralized Applications (dApps) development [47]. The main attributes of dApps are decentralization, resilience, and transparency. This has opened a new frontier for developing, for example, dependable IoT applications. The decentralization and resilience properties are achieved by the way a blockchain is structured (see Section II), but basically, if one of the peers fails, any of the other peers can take over, thus avoiding the single point of failure in the application. There is no need of a centralized controller in a blockchain, and therefore, the application that runs on a blockchain infrastructure can improve its dependability attributes, i.e. availability, reliability, safety, confidentiality, integrity and maintainability [48]. Finally, the transactions ledger can be used in order to scrutiny the dApp execution behavior, as all operation results should be in a transaction.

Another concept that has opened new perspectives for developing dApps is smart contracts [22]. A smart contract allows the execution of an algorithm to solve a problem [1] inside a blockchain without the need for a central controller. The smart contract implementation is different depending on the blockchain, however a few key properties are common, like the auditability of the computation and generated information, the need for a consensus algorithm for the insertion of blocks in the blockchain, and the possibility of self-enforcing terms. Self-enforcing means that once a condition specified in a smart contract is met, the consequences will be processed. As most blockchains have a cryptocurrency, the consequences can involve monetary transactions. An example of self-enforcing could be applied to service level agreements (SLA) specified in a smart contract, where a fine is paid by the service provider if the service agreement is violated. This can be implemented using a smart contract that specifies that once the service is violated, the smart contract will enforce a fine on the provider in an automated form using the blockchain cryptocurrency.

Not all blockchains implement smart contracts in their infrastructure. The next section we present some discussion on the features of smart contracts applications that can be implemented in two blockchains, *i.e.* Ethereum and Hyperledger.

Smart Contracts

Since business logic can be applied to a smart contract, it has an ample scope of applications, such as resource allocation, traceability, auditability. A few examples that can be used to solve problems specific for IoT are [4]:

- Providing an IoT update service: a smart contract can be deployed and made accessible to a specific manufacturer of IoT devices. In the smart contract, the device can check the last version of firmware available and receive a hash of the newest version. If necessary, it can access a distributed file system and download the last firmware to update itself.
- Allowing a marketplace between devices: on blockchains that provide cryptocurrencies, a device can sell services to other devices. In the previous example a device with the latest firmware can sell the binaries to an outdated device, the payment can be made using cryptocurrencies in an automated way. Additionally, other services can be exchanged, such as disk storage or information from a device sensor.
- Management and control of an IoT network: a smart contract can keep a list of all the devices and users belonging to the IoT network with their permissions. This list is dynamic so new devices can be removed or added and permissions can be changed. Non-authorized entities are not allowed to interact with the devices in the network. All calls from the devices and information sharing can be managed through a smart contract in a centralized way or the smart contract can just inform a device that other devices are available for interaction. A publisher-subscriber pattern can also be used, so the smart contract can inform a device of specific events. For example, actuators to act at upon an event from a sensor. A similar scheme is proposed in Choi *et al.* [49].
- Routing and workload balancing: a new workload submitted to the IoT network can be managed by a smart contract. Smart contracts can analyze the actual tasks that the devices are responsible for, and depending on the workload on the devices, a load balancing algorithm can be applied and heavy loaded devices can share their tasks to not loaded devices.

These general examples show how powerful the utilization of blockchain and IoT can be. These kind of solutions can be applied to IoT sub-domains such as Smart Grids, Industry 4.0, Smart Cities, or Electric Vehicles.

Smart Grids is one of the application IoT areas in which smart contracts have been applied to. One of the causes is due to the effort for a more decentralized energy market, where energy can be more freely produced and consumed. This allows domestic users, for example, to sell exceeded energy produced, for example, from solar panels in their houses to an energy company. Smart contracts can be used also as a resource allocation manager, helping Smart Grids to route energy across a region in a more efficient way than traditional energy grids [50] [51]. This allows better energy distribution, reducing energy waste, and lesser need of investment in energy grids. The use of smart contracts and IoT to control access to energy in a house improves also auditability and increased

[1] The same class of problems that can be solved by a Turing machine.

transparency [52].

In the context of Smart Cities, smart contracts can solve access problems to disputed public services. For example, using the lottery algorithm proposed by Liao and Wang [53], IoT sensors can detect the availability of a public spot for parking. Cars in the region can apply, using a smart contract, to use that spot, in case of dispute for a spot, the lottery algorithm can decide in a transparent way which car can use it.

In the Electric Vehicles context, finding the best charging station available at the best cost and charging process can be improved by the use of smart contracts. Devices in the vehicle can detect the battery status of the car and, for example, when the charge is low, it can trigger an auction in a blockchain accessed by electric vehicles and charging stations. A station can make an offer to the smart vehicle based on its availability. The vehicle, based on the offers of multiple stations and his route, can decide which station to contract. If there is a cryptocurrency in the blockchain network, even the payment can be performed automatically. Similar auction system is proposed in Pustišek *et al.* [54]. The station access can be controlled by IoT devices, the access to the station can be scheduled and the access unlocked at the agreed time or the vehicle presence, this way facilitating the charging process [12].

Smart contracts can be used to encourage some behaviour to help in workload balance, such as traffic. Sensors can detect a traffic jam, with the use of smart contracts vehicles can receive an incentive or be enforced to take an alternative route. An incentive can be a payment, in cryptocurrency, to use the alternative route. To enforce, a fine can be applied to users who do not comply.

V. Open Issues & Future Research Directions

As previously discussed, the blockchain technology is in early stages of development and adoption by industry. Even research in academia has increased in recent years. Consequently, there are some issues, especially related to security and performance, that should be addressed before blockchains are fully applied to IoT environments.

Blockchain were conceived to be deployed in distributed (P2P) architectures. Consequently, security issues related to network and P2P vulnerabilities can be explored to attack the blockchain environment. These issues can affect users, applications and even the blockchain structure.

Security issues in the "Communication" layer (presented in Section IV-A) can be summarized, but not limited, to Sybil [55], DDoS [56] and Eclipse [39] attacks. For example, in an Eclipse attack, a malicious node can control the information that is shared with another node (*e.g.*, a gateway). Consequently, the information sent by this node can be omitted from the blockchain in the other nodes. In a hierarchical P2P architecture this kind of attack could be worse, since a supernode controls data from multiple devices. There is a lack of discussion in the literature about this attack and its impact in blockchains for IoT.

Also, there is no standard architecture for nodes that will maintain the blockchain in IoT networks. Consequently, these different architectures can lead to different security issues: for example, while a completely decentralized architecture leads to a processing demanding solution, it maintain a copy of the blockchain locally. In opposite, in a BaaS architecture nodes do not waste processing power to maintain the blockchain, but have to trust a third-party solution.

Additionally, common issues to establish trust in an untrusted environment are rising in the "Consensus" layer. Thus, depending on the applied algorithm, different pros and cons could be related to it. For example, there are some issues related to PoW algorithms such as, 51% [57], Bribery [58], and Double Spending [59] attacks. In the context of IoT, Bribery and Double Spending are not applicable in scenarios that do not use coins, but can affect scenarios with M2M payments. Additionally, PBFT can be a problem in scenarios with large amount of nodes due to the delay to transmit voting messages [15].

Moreover, several researchers are working in order to address the two most common problems of blockchains: performance - response time to add new blocks and transactions - [8], [57], [41] and scalability - capability of all IoT devices being able to interact with a blockchain - [60], [32], [33]. Although they present innovative solutions, they are in development and do not present an appropriate evaluation in real scenarios.

Furthermore, in the "Application" layer, there is almost no discussion on how a blockchain can be affected by unsecure APIs that access blockchain data. Also, smart contracts could be affected by problems related to blockchain solutions. For example, in comparison to traditional databases, the solution could present lower throughput [4]. This latency is caused by the mining process in some blockchains and could act as limiting factor, thus its application to real time solutions should be carefully evaluated before being used [31]. A deployed contract is permanent, in the Ethereum case, or have a great management cost to change, as in Hyperledger. Thus, the contract logic needs special attention to avoid flaws, which can be used to exploit vulnerabilities and expose a variety of risks to the network and users [4], [61], [62], [63], [64]. There are research initiatives [65] to help developers to avoid issues during the smart contract implementation. Despite of that, security issues in smart contracts can be further explored and discussed, as well the smart contract applications in IoT, such as: firmware update, M2M payment and transactions, and tracking devices.

There are many proposals related to the "Communication" layer, more specifically on network protocols and blockchain architecture. However, there is still no standard blockchain framework for IoT. Although, there are different studies to integrate the different distributed ledgers, such as the IEEE Blockchain Initiative[2] or the ITU-T Focus Group on Applica-

[2] https://blockchain.ieee.org/

tion of Distributed Ledger Technology (DLT)[3]. Additionally, the "Consensus" layer could be better explored and analyzed by academia in order to cover security and performance issues, especially for large scale IoT scenarios. Finally, in the "Application" layer, there is a lack of APIs for blockchains, as well few discussion of patterns for smart contracts.

Hence, although blockchain can be applied to different scenarios, there is still several open issues that have to be studied before the full potential of blockchains can be used in different IoT environments.

VI. Conclusion

The adoption of blockchain in IoT environments can bring key benefits in several areas, for example, Health, Financial, Transportation, Welfare, and so on. Those benefits are the same brought to any solution using blockchain, like transparency of operations performed in the network, no-repudiation of the generated information by the nodes, no single point of failure, and high availability.

To better use those advantages in different scenarios and in order to reach a superior IoT solution, it is important to understand how different blockchain technologies work. To support this understanding we proposed a blockchain layer model in Section IV that organizes a blockchain in communication, consensus, data and application layers. In our perception, the use of this model can give a clear view of the characteristics of a specific blockchain and where it should be used.

It is also important to keep in mind the issues related to the use of blockchains. Some of those issues are inherited from the use of P2P networks. Others come from the nature of blockchain of creating a trusted environment from untrusted peers. And, finally, from the hardware limitations in IoT devices. In Section V, we present some insights towards the mitigation or elimination of those issues and towards novel applications in IoT sub-domains.

Naturally, blockchain research and use has grown in the past years and they will present new challenges in the near future. At the moment, blockchain is still in the peak of inflated expectations in the Gartner Hype Cycle [66], and it is expected to reach its plateau of productivity between 5 to 10 years. Therefore, we will see a lot of research and applications of blockchains in the near future.

Acknowledgment

This study was financed in part by the Coordenao de Aperfeioamento de Pessoal de Nivel Superior Brasil (CAPES) Finance Code 001, Forense Science National Institute of Science and Technology (INCT) financed by CNPq, and HP Brasil using incentives of Brazilian Informatics Law. This work is also part of a joint research project between PUCRS and Totvs. We also thank to Australian Academy of Science for the Australia-Americas PhD Research Internship Program, the reviewer of paper, and the members of the Dependability and Security Research group (Conseg) at PUCRS.

[3] https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx

References

[1] S. Cirani, L. Davoli, G. Ferrari, R. Lone, P. Medagliani, M. Picone, and L. Veltri, "A Scalable and Self-Configuring Architecture for Service Discovery in the Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 508–521, Oct 2014.

[2] J. A. Jerkins, "Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code," in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan 2017, pp. 1–5.

[3] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Www.Bitcoin.Org*, p. 9, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[4] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[5] M. Conoscenti, A. Vetro, and J. C. D. Martin, "Blockchain for the internet of things: A systematic literature review," *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, pp. 1–6, 2016.

[6] M. Samaniego and R. Deters, "Blockchain as a service for iot," in *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)*, Dec 2016, pp. 433–436.

[7] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an Optimized BlockChain for IoT," in *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, ser. IoTDI '17. New York, NY, USA: ACM, 2017, pp. 173–178.

[8] R. C. Lunardi, R. A. Michelin, C. V. Neu, and A. F. Zorzo, "Distributed access control on iot ledger-based architecture," in *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, April 2018, pp. 1–7.

[9] L. Wu, X. Du, W. Wang, and B. Lin, "An out-of-band authentication scheme for internet of things using blockchain technology," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, March 2018, pp. 769–773.

[10] 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, DECEMBER 2017.

[11] R. A. Michelin, A. Dorri, R. C. Lunardi, M. Steger, S. S. Kanhere, R. Jurdak, and A. F. Zorzo, "SpeedyChain: A framework for decoupling data from blockchain for smart cities," *ArXiv e-prints*, Jul. 2018.

[12] X. Huang, C. Xu, P. Wang, and H. Liu, "Lnsc: A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13 565–13 574, 2018.

[13] 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 *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, April 2017, pp. 50–58.

[14] T. Aste, P. Tasca, and T. D. Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18–28, 2017.

[15] D. Miller, "Blockchain and the internet of things in the industrial sector," *IT Professional*, vol. 20, no. 3, pp. 15–18, May 2018.

[16] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2016.

[17] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, JULY 2018.

[18] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar, and J. J. P. C. Rodrigues, "Sdn-enabled multi-attribute-based secure communication for smart grid in iiot environment," *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, vol. 14, pp. 2629–2640, JUNE 2018.

[19] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, Nov. 1981.

[20] P. Vasin, "Blackcoin's proof-of-stake protocol v2," *https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf*, p. 2, 2014.

[21] Litecoin, "Litecoin - open source p2p digital currency." [Online]. Available: https://litecoin.org/

[22] E. Foundation, "Ethereum specification," Sep. 2018. [Online]. Available: https://github.com/ethereum/go-ethereum/wiki/Ethereum-Specification

[23] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," *https://ripple.com*, p. 8, 2014.

[24] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Workshop on Distributed Cryptocurrencies and Consensus Ledgers, 2016*, 2016.

[25] L. Foundation, "Hyperledger architecture," Sep. 2018. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.2/

[26] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, "A brief survey of cryptocurrency systems," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Dec 2016, pp. 745–752.

[27] I. Foundation, "Iota - next generation blockchain," Aug. 2018. [Online]. Available: https://iota.org/

[28] B. C. Florea, "Blockchain and internet of things data provider for smart applications," in *2018 7th Mediterranean Conference on Embedded Computing (MECO)*, June 2018, pp. 1–4.

[29] Waves, "Waves - get started with blockchain." [Online]. Available: https://wavesplatform.com/

[30] Stellar, "Stelar - get started with blockchain." [Online]. Available: https://www.stellar.org/

[31] S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, Feb 2017, pp. 464–467.

[32] O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, April 2018.

[33] K. R. zylmaz and A. Yurdakul, "Work-in-progress: integrating low-power iot devices to a blockchain-based infrastructure," in *2017 International Conference on Embedded Software (EMSOFT)*, Oct 2017, pp. 1–2.

[34] T. Dey, S. Jaiswal, S. Sunderkrishnan, and N. Katre, "Healthsense: A medical use case of internet of things and blockchain," in *2017 International Conference on Intelligent Sustainable Systems (ICISS)*, Dec 2017, pp. 486–491.

[35] U. Hunkeler, H. L. Truong, and A. J. Stanford-Clark, "Mqtt-s - a publish/subscribe protocol for wireless sensor networks." in *3rd International Conference on Communication Systems Software and Middleware*. IEEE, 2008, pp. 791–798.

[36] B. Shala, P. Wacht, U. Trick, A. Lehmann, B. Shala, B. Ghita, and S. Shiaeles, "Ensuring trustworthiness for p2p-based m2m applications," in *2017 Internet Technologies and Applications (ITA)*, Sept 2017, pp. 58–63.

[37] X. Wu, B. Duan, Y. Yan, and Y. Zhong, "M2m blockchain: The case of demand side management of smart grid," in *2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)*, Dec 2017, pp. 810–813.

[38] P. K. Sharma, S. Singh, Y. S. Jeong, and J. H. Park, "Distblocknet: A distributed blockchains-based secure sdn architecture for iot networks," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 78–85, 2017.

[39] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network," in *24th USENIX Security Symposium (USENIX Security 15)*. Washington, D.C.: USENIX Association, 2015, pp. 129–144.

[40] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 2084–2123, thirdquarter 2016.

[41] L. Zhou, L. Wang, Y. Sun, and P. Lv, "Beekeeper: A blockchain-based iot system with secure storage and homomorphic computation," *IEEE Access*, vol. 6, pp. 43 472–43 488, 2018.

[42] O. J. A. Pinno, A. R. A. Gregio, and L. C. E. D. Bona, "Controlchain: Blockchain as a central enabler for access control authorizations in the iot," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, Dec 2017, pp. 1–6.

[43] E. Foundation, "Ethereum white paper," Sep. 2018. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[44] A. Dorri, S. S. Kanhere, and R. Jurdak, "MOF-BC: A memory optimized and flexible blockchain for large scale networks," *CoRR*, vol. abs/1801.04416, 2018. [Online]. Available: http://arxiv.org/abs/1801.04416

[45] M. E. Peck, "Blockchains: How they work and why they'll change the world," *IEEE Spectrum*, vol. 54, no. 10, pp. 26–35, October 2017.

[46] CoinMarketCap, "Top 100 cryptocurrencies by market capitalization," Sep. 2018. [Online]. Available: https://coinmarketcap.com/

[47] F. Wessling, C. Ehmke, M. Hesenius, and V. Gruhn, "How much blockchain do you need? towards a concept for building hybrid dapp architectures," in *2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, May 2018, pp. 44–47.

[48] A. Avizienis, J. . Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, Jan 2004.

[49] S. S. Choi, J. W. Burm, W. Sung, J. W. Jang, and Y. J. Reo, "A blockchain-based secure iot control scheme," in *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, June 2018, pp. 74–78.

[50] S. Noor, W. Yang, M. Guo, K. H. van Dam, and X. Wang, "Energy demand side management within micro-grid networks enhanced by blockchain," *Applied Energy*, vol. 228, pp. 1385 – 1398, 2018.

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

[52] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "Gridmonitoring: Secured sovereign blockchain based monitoring on smart grid," *IEEE Access*, vol. 6, pp. 9917–9925, 2018.

[53] D. Liao and X. Wang, "Design of a blockchain-based lottery system for smart cities applications," in *2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC)*, Oct 2017, pp. 275–282.

[54] M. Pustiek, A. Kos, and U. Sedlar, "Blockchain based autonomous selection of electric vehicle charging station," in *2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)*, Oct 2016, pp. 217–222.

[55] J. R. Douceur, "The sybil attack," in *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, ser. IPTPS '01. London, UK, UK: Springer-Verlag, 2002, pp. 251–260.

[56] M. Vasek, M. Thornton, and T. Moore, "Empirical analysis of denial-of-service attacks in the bitcoin ecosystem," in *Financial Cryptography and Data Security*, R. Böhme, M. Brenner, T. Moore, and M. Smith, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 57–71.

[57] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16. New York, NY, USA: ACM, 2016, pp. 3–16.

[58] J. Bonneau, "Why buy when you can rent?" in *Financial Cryptography and Data Security*, J. Clark, S. Meiklejohn, P. Y. Ryan, D. Wallach, M. Brenner, and K. Rohloff, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 19–26.

[59] 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*, ser. CCS '12. New York, NY, USA: ACM, 2012, pp. 906–917.

[60] M. Conoscenti, A. Vetr, and J. C. D. Martin, "Peer to peer for privacy and decentralization in the internet of things," in *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)*, May 2017, pp. 288–290.

[61] N. Fotiou and G. C. Polyzos, "Smart contracts for the internet of things: Opportunities and challenges," in *2018 European Conference on Networks and Communications (EuCNC)*, June 2018, pp. 256–260.

[62] K. O'Hara, "Smart contracts - dumb idea," *IEEE Internet Computing*, vol. 21, no. 2, pp. 97–101, Mar 2017.

[63] G. Destefanis, M. Marchesi, M. Ortu, R. Tonelli, A. Bracciali, and R. Hierons, "Smart contracts vulnerabilities: a call for blockchain software engineering?" in *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, March 2018, pp. 19–25.

[64] N. Weaver, "Risks of cryptocurrencies," *Commun. ACM*, vol. 61, no. 6, pp. 20–24, May 2018.

[65] A. Mavridou and A. Laszka, "Designing secure ethereum smart contracts: A finite state machine based approach," in *Financial Cryptography and Data Security*. Springer International Publishing, 2018, pp. 1–18.

[66] Gartner, "Top 10 strategic technology trends for 2018," In https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018/, accessed in Setember, 8th 2018.