IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 27, 2021, accepted December 8, 2021, date of publication December 23, 2021, date of current version January 5, 2022.

Digital Object Identifier 10.1109/ACCESS.2021.3138353

Evolution of Internet of Things From Blockchain to IOTA: A Survey

MAYS ALSHAIKHLI[1], TAREK ELFOULY[2], OMAR ELHARROUSS[1], (Member, IEEE), AMR MOHAMED[1], (Senior Member, IEEE), AND NAJMATH OTTAKATH[1]

[1]Computer Science and Engineering Department, College of Engineering, Qatar University, Doha, Qatar
[2]Department of Electrical and Computer Engineering, Tennessee Technological University, Cookeville, TN 38501, USA

Corresponding author: Mays Alshaikhli (200753008@qu.edu.qa)

ABSTRACT Internet of Things (IoT) is the new paradigm to the scaling nature of things and their elements, interconnected, exchanging data over a network supported with nodes. The Ubiquitous use of tiny devices and embedded sensor frameworks has pushed IoT to the forefront of emerging technologies used in many applications like peer-to-peer networks, smart energy grids, home and building automation, vehicle to vehicle communication, and wearable computing devices. This massive growth and extensive use brought forth security risks that could hinder its commencement in many novel applications. The number of interconnected devices leads the way to several entry points for intruders and, along with it, security risks. The sensitive nature of the IoT applications such as health, automation, and energy grids cannot afford security risks. Traditional security mechanisms will not design or develop to secure such an emerging technology as IoT. Existing technologies have to be relied on with the non-existence of security mechanisms for this purpose. Distributed Ledger Technology (DLT) is one such technology that can reduce the security risks in IoT. The central node vulnerability that can compromise the whole system can be mitigated by eliminating the need for a central node by using the distributed ledger. Blockchain, a distributed ledger technology, has attracted tremendous attention and harnessed in itself a real-world value. However, computationally costly with limited scalability is not entirely suited for the IoT environment. IoT Application (IOTA) technology is the distributed ledger technology that can provide unlimited scalability specifically suitable for the IoT industry. This survey provides an in-depth introduction to how blockchain performs and its constraints in its nature as a generic platform for DLT. In contrast, IOTA is introduced as the technology for IoT, the next-generation blockchain overcoming blockchain's limitations for its use in IoT.

INDEX TERMS IoT, security, IOTA, blockchain.

I. INTRODUCTION

The ''things'' in IoT have reached household appliances and entertainment to wearables, all connected through the internet. The internet of Things (IoT) has had a striking impact on the way we associate with our surroundings [1]–[3]. According to Gartner's forecast, by 2020, we will have about 20.6 billion connected things or more [4]. The idea that all things are super connected to everything, through which information is collected, monitored, and controlled via the internet to interact and interconnect with users, is the central concept of this ubiquitous technology [5], [6]. With the overestimated number of things connecting the IoT to the world, there is no doubt we are already inside the IoT world. These billions of IoT devices will have confidential and private information, which could cause severe repercussions if compromised [7]. Due to equipment constraints and energy requirements, IoT devices are at high risk in security [8]. A significant amount of data is used and passed through the network between the devices, which is one of IoT's main attributes. This ecosystem of manipulating data over the network can add to the security risks related to IoT [9]. An excellent delineation of the requirement would be that of 2016 when the Dyn cyberattack caused millions of internet addresses to be compromised and servers to be brought down temporarily. It targeted Dyn systems by denial of service attacks (DDoS). This simple malware attack infected and hijacked innumerable IoT devices [10]–[12].

There is no conspicuous technique for achieving this vision of IoT. In the traditional, centralized platform, nodes receive

The associate editor coordinating the review of this manuscript and approving it for publication was Yanli Xu.

raw data and services from other nodes in data acquisition networks through a central platform having control over the data stream. This entitles significant infrastructure and maintenance expenses and so with the growth of the network cost increases. In terms of performance perspective, centralized servers can sometimes cause a bottleneck and can be a single point of failure, which can interrupt the whole process. Looking at the distributed approach, collaboration is the main key between different application platforms and intelligence is culminated onto the nodes (edge computing). The advantages of the distributed platform in an IoT environment are mentioned in [13]. Nevertheless, no unequivocal analysis has been done for the security and performance mechanisms of blockchain and IOTA [98] built using the distributed platform. To comprehend these techniques and know its actual value, a thorough study of the distributed approach is required.

Collaborating with participants in other networks in order to accomplish a shared objective in IoT applications is the current IoT initiative that embraces distributed computing concepts. Further discussion is still required for developing a decentralized architecture as well as for edge computing [14].

A. RESEARCH MOTIVATION AND CONTRIBUTION

This survey was motivated by current advancements in IoT-enabled Smart City systems. IoT provides the structure and protocols for the smart system's sensing, actuation, communication, and processing technologies. The rapid growth of technology in several IoT industries has created new challenges in maintaining the efficient operation of smart systems. This paper will benefit potential researchers and stakeholders in this field in comprehending the architecture of IoT and the various distributed ledger technologies used in IoT (IOTA and Blockchain), security vulnerabilities, mitigation strategies, and advanced technology potentials. The key contributions of this paper are listed as follows:

1. We overview IoT technology and we provide a general taxonomy to classify its applications.
2. We analyze the IoT benefits and risks as well as its features and security requirements.
3. We survey in details the recent existing solution (blockchain technology) and its drawbacks.
4. We present the IOTA Technology as the solution for the IoT environment.
5. We present a detailed comparison of blockchain and IOTA based on their performances and security, advantages, and disadvantages.

The rest of the paper is organized as follows. The concept of Internet of things, its application, its benefits and risks, its security requirements and device requirements are all described in section II. The blockchain model and its limitation is discussed in section III. The IOTA model, its features and its advantages as well as its drawbacks are explained in section IV. An introduction to different communication systems will be briefed in section V. A comparison between IOTA and blockchain is presented in section VI.

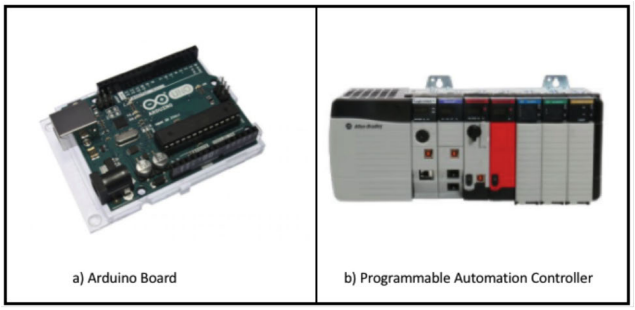


FIGURE 1. Tools with ability for connecting between IoT devices.

IOTA security terms are discussed in section VII. Research work is explained in section VIII and the conclusion is discussed in section IX.

II. INTERNET OF THINGS

Internet of Things is most popularly known as one of the unique concepts of this century that are going on in computers, networking, and technology. The internet is the most important and transformative technology ever invented that connect people, sometimes called ''the Internet of people.''

There is a new emerging form of the internet, and it is poised to change the world again but not by connecting people; this time, it is about connecting things, or in other words,'' Internet of Things'' [15]. What is the Internet of Things or simply IoT? As the name indicates Internet of Things connects things to the internet to share their experiences with other things by adding the ability to sense, communicate and control. IoT will allow things to interact and collaborate with other things. Many things were manufactured and built before the Internet of Things. Fortunately, some tools and systems allow us to add sensing and communications to these existing things, such as the Arduino Board, which is an open-source platform dependent on simple to utilize software and hardware. These boards can peruse contributions on a sensor and do what we need by sending many instructions to the microcontroller on the board [16]. Another tool is the Programmable Automation Controller (PAC) as shown in Figure (1); this device, in a broad sense, can sense and communicate with things [17]. Nowadays, we have many connected devices to the internet, from work computers, personal computers, tablets, smartphones, smart refrigerators, and smart TVs. All these devices contain sensors taking information from natural physical objects and uploading it to the internet. It is a world that's constantly changing all around us due to these sensors connected to the Internet [18].

A. IoT APPLICATIONS

As IoT reaches out to be the Internet of everything, the organizations are progressively interested in utilizing the knowledge obtained from the various opportunities that emerged in parallel with the IoT and benefit from their significant advantages like expanding productivity and enhancing resource

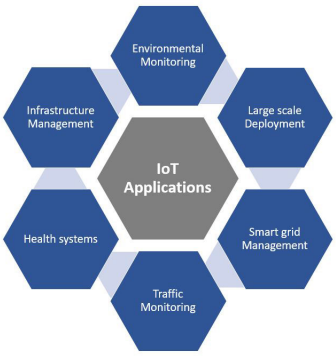


FIGURE 2. IoT Applications.

efficiencies with this innovative technology. We need IoT in many fields as in Figure (2) such as:

1) ENVIRONMENTAL MONITORING

IoT environmental monitoring is essential for protecting the environment and surroundings. There are three essential applications of IoT environmental monitoring which are beneficial for the environment. They are: waste management systems, Vehicle tracking systems, and intelligent weather stations. The IoT solves waste-water management problems by using wireless sensors that provide real-time monitoring of waste. The Proximus IoT platform, for example, not only monitors and alerts about the waste collection but also consumes far less energy compared to the 4G network, thereby increasing the efficiency along with reducing energy costs [19]. The vehicle tracking system follows vehicles in real-time and displays the status of the vehicle. An example is the vehicle tracking system (VTS) framework that uses GPS and vehicle programming [20]. The intelligent weather station promises more fine-grain data, accurate and flexible compared to existing broad instruments such as radars and satellites [19].

2) INFRASTRUCTURE MANAGEMENT

An adequately managed infrastructure provides a solution for the current challenges of global warming and sustainability. An example of an efficient infrastructure management system is data collecting devices such as cameras that produce vast amounts of data. Data collected can help in many applications, including data about vehicles' movement, mobility behavior, or data about energy and water consumption by buildings. Intelligent mobility, intelligent energy, intelligent buildings, and many other intelligent infrastructure applications can emerge from collecting such data, leading to a concept called smart cities [21]. These cutting-edge urban cities can actualize infrastructures (water, power, gases, and transport) for communication and management to improve citizens' comfort while ensuring environmental protection. The convergence of the digital and physical world controlled the facilities and production of the industrial IoT. A network of machines works side-by-side and collaborates seamlessly with people freed up to perform more creative tasks—smart manufacturing, powered by Industrial IoT. IoT in Industry will lead to improved solutions that allow manufacturers to respond more quickly to their customers [22].

3) ENERGY MANAGEMENT

Energy management is a problem. Power outages represent an annual cost of $150 Billion in the US market, and equipment failures cause nearly one-third of those outages. In many cases, plant operators and building managers cannot identify old or faulty equipment before it fails, causing a power outage. Today, cloud-based energy management solutions are taking capabilities to a new level. Energy service companies ESCOs and their customers can now understand energy operations taking steps to reduce cost, mitigate risks, and address environmental concerns [23].

4) MEDICAL AND HEALTHCARE SYSTEMS

IoT is transforming medical and health care systems. Connected Patients generate more data and enable clinicians to identify and address their needs more effectively. The patient can access many healthcare services from home, where home systems utilize IoT devices to monitor patient health and share data with care providers, which can drastically improve the diagnosis and treatment. Embedding intelligent systems with the patient will allow monitoring patients easily from their homes in a real-time manner. Emergency services or family members can receive alerts from a built-in sensosr that can track movements from inside one's home. Integration of Near field communications (NFC) enables innovative packaging with Radio Frequency Identification (RFID) and data sharing through wireless applications to monitor the patient records by reducing the need for repeated prescriptions and reducing waste. Conditional assessments can be done on patients through wearable technologies embedded into their apparel, which could track essential vital signs, thereby saving time and cost by potentially displacing invasive testing methods. Production of targeted medicine has evolved through current advances in biotechnology where medicines are administered based on individual patients' needs, which can increase successful healing rates, reduce side effects, and have their treatments done at home [23].

5) BUILDING AND HOME AUTOMATION

IoT has transformed how homeowners live by transforming one's home into a smart home. While current homes have many associated devices, researchers predict smart homes' future to connect hundreds and thousands of connected devices. Innovative home solutions keep on hitting the market considering purchaser demand. Home automation controlled by IoT will keep on opening new revenue resources for organizations while enabling them to associate with clients to convey more value, and better client care [24].

6) TRANSPORT SYSTEMS

Nowadays, public bicycles have been more popular than ever in numerous countries. IoT now is assuming a critical job in driving the world forward on streets on rails. IoT devices are making travel more secure as well as more efficient. It is a powerful change to transportation that grows more complicated each day with the need to create an environment that allows travelers to keep moving quickly and safely [25].

7) LARGE SCALE DEPLOYMENTS

The smart city is where the IoT comes to life. By 2019, 68% of the government sector will have implemented IoT technology to create smart cities [26]. IoT empowers sensors used in buildings, homes, and vehicles to reform everything in a city, from social insurance movement. About 80% of government pioneers accept that the IoT will change the future of business, and 76% trust it will expand advancement. Today, everything from a city streetlight to police equipment all transmits data. Thus, the data's security and availability are essential in city systems because it is real-time data. Today, 36% of various buildings and devices across their city suffering from transmitting their data between each other, and this means when an incident occurs in one part of the city, it will not get noticed until it occurs. Today only 23% of cities have connected traffic, and transportation systems [27]. Over 6-10 global government leaders believe the IoT will enhance the experience of city residents. The Internet of Things can allow a city to better involve with visitors by offering personalized services and delivering relevant and timely information [26], [27].

B. IoT BENEFITS AND RISKS

The IoT is a cutting-edge technology invented to make daily jobs possible. IoT digitizes physical sensors, devices, and networks. It associates individuals with things and things to other things in a real-time environment. IoT devices' networks can overgrow, bringing about exponential increment in the variety, velocity, and general volume of information; this information opens doors for information creation and revenue generation opportunities. The real test for the IoT environment is collecting a massive volume of data from different sources in a real-time approach. Some of the IoT's most significant advantages are [28], [29]:

1) COMMUNICATION

Device to Device (D2D) connectivity enabled by IoT technology can make communication of devices increasingly straightforward, prompting enhanced communication with one another with enhanced efficiency, quicker results, and better quality.

2) AUTOMATION AND CONTROL

Through IoT technology, daily jobs become automated without any human intervention. The quality of services got considerably improved because of automation enabled by this technology.

3) ACCESS INFORMATION

Information will be easily accessible regardless of data location, providing convenience for people to work remotely even if they are not physically present at their workplace. This approach proved significant in the COVID-19 Pandemic, which forced many businesses to transfer to online and remote operations.

4) MONITORING

With IoT, it is easier to collect more information than before. For instance, monitoring the exact air quality level at home is now possible with better accuracy, monitoring the change in air quality in a certain location such as schools could be of great importance. This monitoring is continuous and accurate and could be enhanced by increasing the number of sensors or mobile participants if the data is being collected through mobile crowd sensing.

5) COST-EFFECTIVE

The financial aspect is perhaps the most significant advantage in IoT as it saves money. The processing and monitoring of data with IoT cost less than what is required otherwise. This approach allows IoT to expand the adoption of connected devices and make IoT systems more efficient.

Here, we list some of the disadvantages or difficulties of adopting the Internet of Things technology [28], [29]:

6) COMPLEXITY

Depending on the technology being used, a small loophole in one node or device could affect the entire system due to an immense number of interconnected devices.

7) PRIVACY/SECURITY

Privacy is a big concern when it comes to IoT. As we proceed to embed these interconnected machines and a more extensive assortment of wireless machines, the threats may penetrate enterprise infrastructures. The Intricacy of security threats presented by IoT devices can have severe consequences. All the information is encrypted between IoT devices to achieve confidentiality. However, this could affect the computational cost of IoT devices [120].

C. IoT FEATURES

IoT has infinite features that are not limited to an IoT device being smart to act and communicate with other IoT devices to inform us of what happens nearby. In this section, we will discuss a few of the IoT features [29]:

1) COMPATIBILITY

IoT platform should connect with any machine and sensor over the interconnected network and provide feasibility and flexibility to deploy the required services, but some IoT devices may require extra hardware to make it compatible.

2) INDEPENDENCE

The IoT platform should not be dependent on any vendor or third party and should be open to any device that needs to join the network.

3) IMPLEMENTATION

The devices should be able to connect in much less time and should be an easy-to-use on-demand interface available at any time.

4) DISTRIBUTED ARCHITECTURE

The IoT platform should be able to manage the edge applications, where they can be analyzed in a central place, then distribute them where they are needed.

D. IoT SECURITY REQUIREMENTS

DARPA (Defense Advanced Research Projects Agency) has perceived the security shield for the internet of things as one of the four endeavors with a potential to impact security broader than the internet itself [30]. Four principles (Authentication, Confidentiality, Integrity, and Availability) are required to guarantee the security between different devices. Implementation of security should involve during the development lifecycle of all the IoT devices [31], [32].

1) AUTHENTICATION

Networks can be the powerless connection in the current computing world. They are among a generally vulnerable and effectively hijacked area of the whole arrangement. Every device in the IoT network must have the option to identify any device attempting to make an association. The acknowledgment procedure is verified, recognized, and approved by the device's certification to decide whether the client is authentic to utilize the resources. IoT clients choose to go for a straightforward or complex approach and use considerably more secure confirmation as two-way authentication, computerized certificate, or biometrics authentications dependent on IoT client needs. IoT confirmation uses an alternate mindset for the validation process where does not require human interaction for verification purposes since it is between sensors and machine-to-machine associations in IoT. However, it is very challenging to achieve authentication due to the IoT's nature, where many nodes are connected to the network (e.g., devices, humans, services, processing units, and service providers) [33]. In 2015, Rizzardi *et al.* published a research paper: ''Security, privacy and trust in Internet of things: The road ahead'' [34], to reveal the opinion of considering a set of IoT devices communicating to achieve a common target where their vision considered that IoT deployments involve different technologies, architectures and implementations to build a successful and secure communication. They divided their work into three different areas: security requirements (authentication, access control, and confidentiality), trust, and privacy.

2) CONFIDENTIALITY

Confidentiality and privacy are terms that are used conversely in our lives. They differ from each other where confidentiality is a user sharing information to another user that a third person cannot divulge unless an authorization was given to access the required information. Privacy refers to safety from the interference of others into a user's information. Confidentiality is critical to avoid the transfer of confidential data to the wrong node in the network. Cryptography, strong passwords, and encryption techniques are vital in maintaining confidentiality. For example, confidentiality requires sensors to ensure that data is sent to the correct node [35], [36].

3) INTEGRITY

Integrity requires that data is not changed or damaged in an unauthorized manner [38]. IoT devices' essential purpose is to share data with other IoT devices, so it is incredibly critical to ensure the data's integrity, consistency, and accuracy. Which guarantees that data reaches the destination without being tampered with during transit or affected by collision (e.g., breach of confidentiality) [39]. Firewalls and protocols usually manage data integrity, but due to IoT's constraint on low computing capacity, Integrity is not guaranteed [40].

4) AVAILABILITY

Despite hardware issues and security threats, to achieve the IoT approach, IoT devices and services should be available at any time and from anywhere [41], [42]. There is a necessity to identify possible threats to IoT systems and pick the correct defenses based on the type of data and its sensitivity. It is also necessary to incorporate security in the design phase and define the specific security requirements based on risk assessment. A more research focus should be in the design phase to study the intruder behavior to gain access and compromise the system.

E. IoT DEVICES REQUIREMENTS

IoT device requirements can be divided into three different categories. These categories are:

1) LOW RESOURCE CONSUMPTION

A significant challenge facing IoT devices is minimizing the power consumption. IoT is estimated to generate 100s of Zettabytes (trillions of Gigabytes). This requires minimizing power consumption starting from the design phase so as to increase the lifetime of the device and to maximize the capacity and life of on-board batteries. Battery failure is critical and cannot be taken as an option in wearable medical devices like a pacemaker, and so it is crucial to be aware of the pattern of power consumption and track the battery life of these devices. A notable example of a low power requiring devices may be that of battery powered wireless sensors required to function for an extended period which may span to months or years [43], [44].

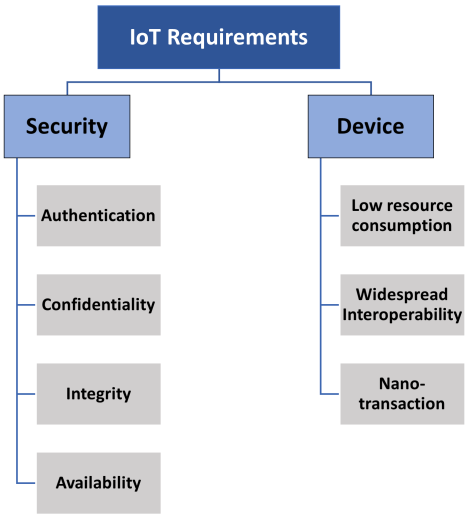


FIGURE 3. Summary for IoT Requirements.

2) WIDESPREAD INTEROPERABILITY

Interoperability appeals to a technology industry that routinely churns through new buzzwords. IoT is an amazingly diverse space, including an enormous assortment of hardware structure components and programming systems. All technologies are interactive inside the IoT, from smartwatches, cameras, indoor regulators, and drones. Billions of IoT devices, sensors, actuators, and smart machines are associated with the web for gathering information through interfacing and correspondence arranged in a heterogeneous manner. Interoperability is the ability to make all devices associated with an organization communicate and accomplish a particular task [45], [46].

3) NANO-TRANSACTIONS

Billions of Nano-transactions are generated by IoT devices. All transactions are generated and maintained over the internet, which mandates an efficient mechanism to manage this tremendous number of transactions without sacrificing any requirement from security to performance of the process [47].

As shown in Figure (3) The life system of IoT devices operates by sending data frequently, which is the major motive for creating a standardized shared communication model for which the above discussed requirements should be considered, if any application should be part of the IoT network. The blockchain model is the primary solution to the problem, which will is discussed in section V.

III. TYPES OF COMMUNICATION SYSTEMS

A. CENTRALIZED SYSTEMS

Transactions, the archetype of organizational activities, need tracking, validation, and regulation where a ledger system serves the purpose of maintaining integrity and validity. This type forms a centralized ledger system where a single entity controls the ledger, regulating and validating transactions. In a centralized system, the single point of authority maintaining the transactions can delegate the internal and external data. However, this system has its downfalls. A failure in the central authority will bring down the whole system. In addition to that, there are no restrictions to modifying the ledger, which can cause frauds and other misrepresentations of transactions [48]. This system is also prone to failure due to its centralized nature, as it can bring down the whole network at a single point of failure.

B. DISTRIBUTED SYSTEMS

Distributed Ledger System: To overcome the limitations of a centralized ledger system that is easily prone to disparity, discrepancies, and modification, a distributed ledger technology(DLT), which is immutable, tamper-proof, and self-maintaining, was proposed [49]. Centralized control is not present, and the authority is distributed to maintain the ledger and validate the transaction [50]. This approach led to the formulation of cryptocurrencies used in trading currencies through the distributed framework and record of the transaction is stored in the DLT. In other words, a distributed ledger can be defined as a type of decentralized database. This decentralized network maintains a copy of the whole database where it is replicated and synchronized. Transactions are recorded in the ledger, which is time-stamped, and non-amendable [51].

IV. BLOCKCHAIN MODEL

A. BLOCKCHAIN

Blockchain technology is a fully distributed and trusted ledger cryptocurrency technology that maintains a tamper-proof record of transactional data resulting in transparency, integrity, and verifiability of these transactions [52]–[55]. Satoshi Nakamoto has founded blockchain in 2009, commonly known as Bitcoin [56].

Blockchain removes the need for central authorization between network devices as it maintains a decentralized public ledger. It is a form of a device to device (D2D) network [57], [58]. The network participants, also known as nodes, share the public ledger. Blockchain is tamper-proof, where the transactions are permanently recorded once verified and added to the blockchain, which is then unmodifiable, and in-erasable [59]. Nodes form a distributed network; A copy of the public ledger is stored in all nodes and updated simultaneously in order to prevent loss of data which could occur due to any single point of failure [60].

B. HOW BLOCKCHAIN WORKS

In a blockchain process, as shown in Figure (4), a block in the shared ledger represents a new transaction being issued; once issued, a broadcast is sent to all participants. The majority of the nodes execute algorithms to confirm and validate the new individual block [61]. To ensure the security and privacy of the content of the distributed ledger content, public-key encryption is used [62]. Usually, the first block, "genesis block," is created at the beginning of the

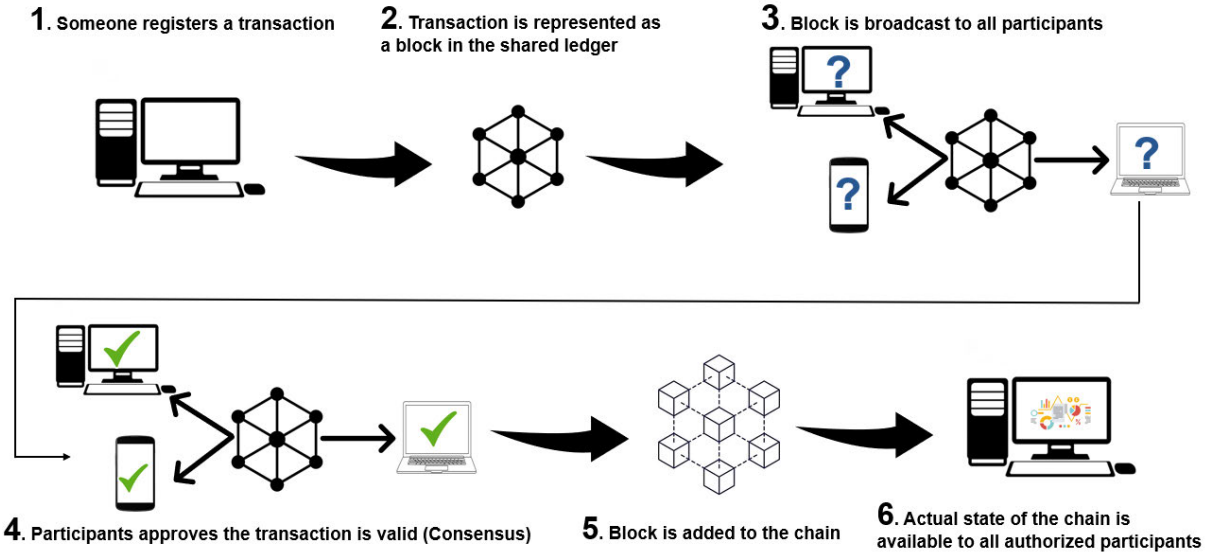


FIGURE 4. Blockchain Process.

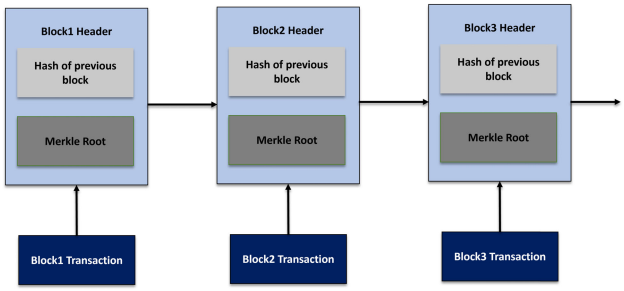


FIGURE 5. Blockchain from the inside.

blockchain, containing the header of the block and a data transaction. Hash algorithms are used to create the block's timestamp (e.g., SHA256 [63] as seen in Figure 7); the consequent transactions go into the blockchain and calculate the current hash from the previous block hash. The network participants are required to execute algorithms to confirm and validate any new transactions. This process is called consensus, illustrated in Figure (5) Blockchain from Inside [64], [65]. As shown in Figure (6) Blockchains are classified into two types of platforms, public blockchain or private blockchain [66], [67]. A public blockchain allows any network participant to issue a transaction and participate in the consensus [68]. Well-known examples of permission-less platforms are Bitcoin [56], Zerocash [69] and Ethereum [70]. Alternatively, in the private blockchains [71], every network participant can conduct transactions restricted to a limited number of approved participants. An example of permission blockchains is multi-chain [72].

C. VALIDATION ALGORITHMS

The advancement of decentralized design and edge computing stays a significant issue that should be addressed [14]. Goiri and LopezdeIpina [73] examined how to utilize web protocols to effectively actualize IoT using a semantic procedure to help exchange the data in a distributed way, where nodes are situated at various locations and can communicate effectively with one another. Liu [74] additionally depicts the framework (U2IoT) comprising of two sections, the IoT unit and the ubiquitous IoT, which organizes the correspondence between several nodes. It is worth noting that the blockchain framework to be chosen is the most critical component of the consensus algorithm [75]. The main standard blockchain protocols used for achieving the consensus are shown in Table (1) and listed as [76]:

1) PROOF OF WORK (PoW) ALGORITHM

Satoshi Nakamoto's model's main characteristic is utilized to address the issue of double-spending (spending the same Bitcoin in two other transitions [56]). PoW permits the system nodes to accomplish specific tasks that will limit the work for the system. A puzzle "guess the zeros" is created by the system to be solved at a particular time. This puzzle is required to be resolved to get the block accepted by the participants who are called miners. The miners who do not solve the puzzle will attempt to guess the new puzzle [77]. PoW is generally frequently used on the public frameworks since it takes much power but remains the most straightforward algorithm to verify [78].

2) PROOF OF STAKE (PoS) ALGORITHM

This algorithm uses another strategy to reach a consensus. Rather than solving the PoW puzzles, the producer of a different block is chosen in a deterministic way. There is no block reward; it relies upon the number of stakes a miner has [79]. The miners take the transaction fees; this technique permits the block producers to build a trusted and distributed framework with a high-stake node (loyal node) [80], [81].

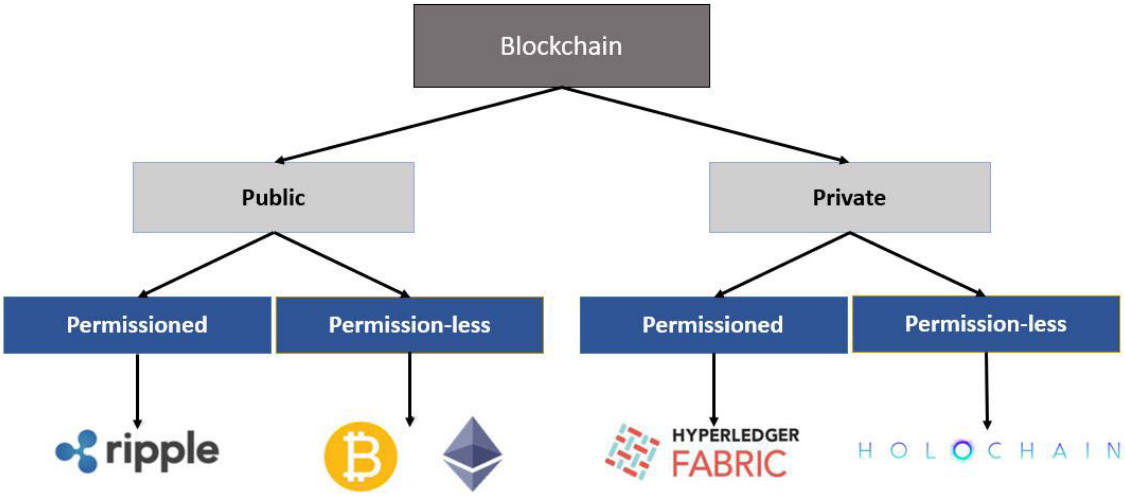


FIGURE 6. Types of Blockchain.

3) PRACTICAL BYZANTINE FAULT TOLERANCE ALGORITHM (PBFT)

PBFT uses the replication method for fault tolerance [82]. It tolerates 1/3 of the byzantine reproduction attacks depending on the agreement set up in the blockchain system. All network participants should agree on an amount of fault tolerance. Compared to other methods, this method requires the least effort [83]. The blockchain systems that rely on PBFT for consensus are Hyperledger [84], Stellar [85] and Ripple [86].

4) DELEGATED PROOF OF STAKE ALGORITHM (DPoS)

This algorithm uses a reputation system to choose the nodes as witnesses ranking them to achieve consensus. Non-trusted nodes are prevented from participating using the same system. The trusted nodes can create blocks but cannot change the transaction details [82]. Besides, they can prevent non-trusted nodes from being included in the next block [87], [88].

Smart contracts, first proposed in the 1990s by Nick Szabo, is a computer program that automatically executes when predefined conditions are met. It is a method used to form agreements in a blockchain. This system eliminates the need for a trusted third party or a central authority, resulting in extra cost and long execution time [89]. Smart contracts are embedded in the blockchain, stored, replicated, and automatically updated enabling transaction cost and service cost to be reduced [89]. The contract's execution is an immutable transaction in the blockchain providing access control and secure enforcement of the contract. Having a smart contract ensures better security for the transaction. Third-party costs are not required, and so no administration and service costs are needed for this purpose, so the business process becomes more efficient [90].

D. SMART CONTRACT PROCESS

A typical smart contract is a computer program with a computational logic of an if-then condition deployed on the blockchain. After a smart contract is set up, it is triggered by addressing a transaction to it. The triggering transaction data determines the mode of execution of the smart contract, which usually carries out the procedure automatically in a predefined manner on every node in the network. Here the blockchain network can be considered a distributed virtual machine where the smart contract is run on [90]. Once the smart contract is deployed, it becomes immutable where even the smart contract's programmer cannot tamper with it. It is an automated process in each peer or node of the blockchain network called a decentralized app(Dapp). Different kinds of blockchain have their implementation of smart contracts based on the framework used. Ethereum's smart contract is programmed in solidity programming language and is paid with its currency named gas/ether [91]. Hyperledger, on the other hand, has chain code equivalent to smart contracts, which can have different codes deployed on each channel based on their restrictions. The chain code here can be used to control the access to the transactions and validate the transactions at the endorsing peer [92].

1) TYPICAL BLOCKCHAIN APPLICATIONS WITH SMART CONTRACT

The addition of smart contracts to the distributed system brings forth intelligent industries that may involve applications to enhance the digital economy, such as the internet of things, financial services, management, and health care. These tasks can be integrated into mainstream blockchain-based development platforms such as Ethereum and Hyperledger [93]. The public sector can be one of the most beneficial sectors as the smart contract functionality

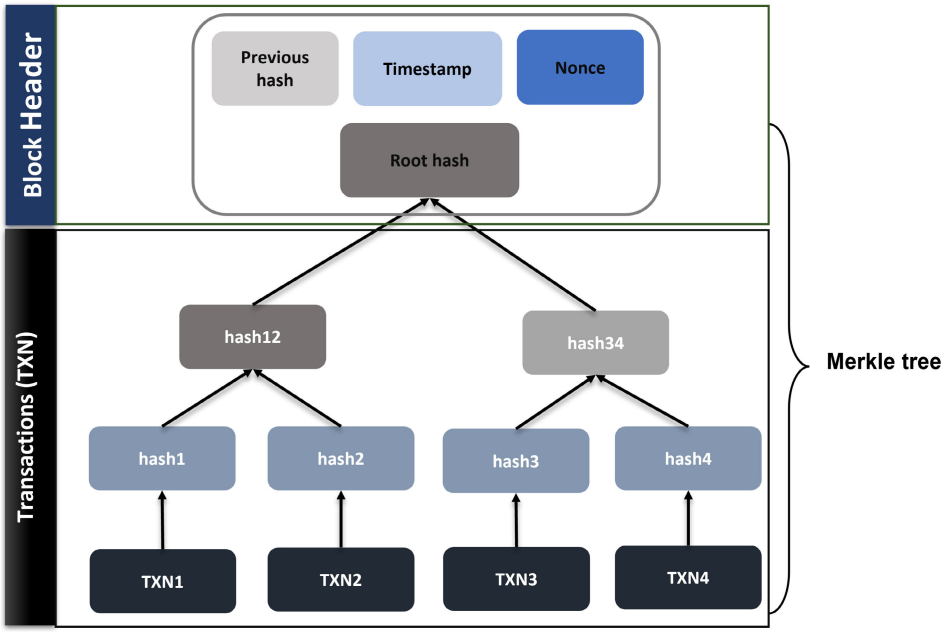


FIGURE 7. Structure of a block with SHA-256 hashing.

can be used to program restrictions and governance [94]. The multitude of applications in the public sector can include legal contracts, property registries, and public procurement, where corruption, a vulnerability enabled by the existence of third parties, can be prevented. Tax evasion scenarios can be overcome when transactions happen between two entities in different countries [94]. Data integrity can be safeguarded with this immutable network for public records and other sensitive data with tamper-proof transactions. Internet of things (IoT) platforms can rely on this for security and restricted access through blockchain transactions [95]. The supply chain is another field most influenced by smart contracts where third-party costs can be easily reduced by automation [96]. While the data may be stored off-chain for a supply chain, information on the data, authenticity, and integrity of the data can be safeguarded through blockchain [97]. At the forefront of all, smart contracts can ensure distributed systems security and efficiency and better control with automation.

E. LIMITATIONS OF BLOCKCHAIN

The critical advantage of blockchain is that it utilizes the decentralized ledger, which is shared straightforwardly among nodes with no central authority. Despite that, some researchers have discovered through research that blockchain has some real issues that should be addressed:

1) SCALABILITY

One of the most critical concerns in the blockchain is the scalability of the network due to blockchain's characteristic of having a decentralized framework, where every node in the system can exchange transactions and keep up a copy of the whole ledger [99]. An inter-node latency occurs, which exponentially increments with each extra node; the blockchain gets slower as more nodes are associated with its system [100], [101].

2) STORAGE, BANDWIDTH

As the blockchain expands, the prerequisites for storage "Cryptographic verifications make this information storage immutable", data transmission, and computational power required by the participating nodes in the network increase. Eventually, it becomes unwieldy enough that it's doable for the couple of devices that can manage the cost of the resources to process blocks, prompting the switch to centralization, which does not cost as much as for large blockchains [102].

3) FEES

Different transactions are packaged in each block, and after that, they can be checked by miners. That implies that with an increase in the number of transactions, there will be more work for miners to approve, which implies an increment of transaction charges [103], [104].

4) DATA PRIVACY

Exchanging data on the blockchain is inherently shared between every node on the system. That level of directness is not always a sufficiently secure method for data storage [105], [106].

5) NETWORK SIZE

Since blockchains need a large number of nodes and since every user is a node, that implies the more extensive the network, the better it reacts to attacks, but still, there is a

TABLE 1. Consensus algorithms in Blockchain.

Type	Main feature	Advantages	Disadvantages	Used by
PoW	Miners try to solve. a mathematical puzzle	Simplest algorithm to verify.	Consumes a lot of power.	Bitcoin
		Anti- DoS attacks.	It is costly	Ethereum
		Low impact on stakes of miner.	51% attack or majority attack	Nxt
PoS	Validates blocks . according to stakes	Low computational power.	Fake Stake attacks	Ethereum
		There's no need for powerful equipment to mine.	Tragedy of commons	Litecoin
PBFT	Reaches consensus . even with faulty nodes	Tolerant to existence of faulty nodes.	Sybil attacks.	Hyperledger
		Needs less computation.	Scaling	Zilica
		Safeguards against failures.	One-third of nodes should be non-faulty.	Ripple
DPoS	Witness node is chosen by reputation	Untrusted nodes cannot participate	Community participation defines success.	Bitshared
		Fast and efficient.	Prone to centralisation.	TRON
		Protection against double spend attack.		Tezos

chance of internal defects. In IoT devices, the size truly matters! It has a physical limitation [107], [108].

Although blockchain is improving, it faces many bottlenecks and impediments that prevent it from being utilized as a standardized platform for digital currencies over the globe. The IOTA comes as the coming age of blockchain to address this technology's downsides with a different framework [109]–[111].

V. IOTA MODEL

A. IOTA

IOTA is a distributed ledger platform, heralded as a "cryptocurrency without a blockchain" [112], created in 2015. All IOTA's currency coins have already been created; there will be no mining involved. The total number of IOTA coins is around 2.8 Peta. IOTA is marked as the top ten most significant cryptocurrencies by market cap [113]. IOTA aims to achieve its objective to provide power to transactions between IoT devices [114]. The IOTA naturally solves the drawbacks of the blockchain and offers features required to establish a peer-to-peer micropayment system. The powerful part of this technology that makes it different from other distributed ledger technologies is that it depends on a Hash Directed Acyclic Graph (DAG), also known as (Tangle) rather than blockchain, which is used for storing the transactions [112]–[114]. Instead of the miners' need to perform the computational PoW in a consensus process for validating the blocks of transactions, the network participants themselves will perform the PoW consensus process, as we will see in the next section of the research [115].

B. HOW IOTA WORKS

The tangle "DAG" is the data structure of IOTA technology, consisting of a collection of vertices (transactions) connected by edges. The tangle is created as a lightweight protocol for tiny devices, especially (IoT devices), to facilitate the billions of connected devices [116]. Tangle is a particular kind of DAG that is distributed block-less ledger used for storing transactions. Each transaction represents a vertex in the graph. Moreover, each edge represents the network participants who perform the computational proof-of-work (POW) by explaining a cryptographic puzzle repeatedly. Hash Cash was an example of a cryptographic puzzle used that hashed similar information with a bit of variety until a hash finds a certain number of driving zero bits to keep away from spam [117], [118] and Sybil attacks [119] and validating the previous transaction. When a new transaction is issued, it should approve and validate two previous transactions to be accepted in the graph [120]. For indirect approval, if there is no direct graph between the new transaction and the previous transaction, but there is an indirect path of the length of at least two, the new transaction indirectly approves the previous transaction. According to Genesis, a transaction can be approved in both ways, "directly or indirectly" [113]. This approval will issue a direct edge between the new transaction and two previous transactions.

The unapproved transactions are called "tips." Each incoming transaction should choose two tips to approve according to the Uniform Random Tip Selection strategy, which is used for choosing two tips randomly from the available tips. This method introduced a new issue as the transactions are not evenly spread out across time. The Poisson Point Process model is used to address this issue by making it more realistic and organizing the transactions' arrival. Poisson Point Process is used to analyze the location of transactions in real-time. The Poisson Point Process model achieves this by calculating the rate of incoming transactions and set it to a number (λ) to find the average. For example, if λ=3 and the number of transactions is 120, then the total simulation time will be 40-time units. One more thing to point out, if we set λ to be very small as shown in Figure (8)(a), we will get a DAG network where their transactions approve only one previous transaction because the transaction becomes slow "lazy" as there will be a single tip to approve. Conversely, with huge λ, the transaction coming will be so large that the genesis (root) tip will only be seen on DAG, as shown in Figure (8)(b). Random Un-Weighted Walk Monte Carlo (RWMC) algorithm [121], used as an advanced tip selection algorithm, places a walker on the start "genesis" transaction and starts walking till reaching the required tip [122]. The path it takes is for transactions that directly approve the one we are currently on. This algorithm aims to generate fair samples from some complex distribution [123], but it may coincide before it issues a new transaction. Weighted Random Walk algorithms are used as an alternative algorithm for tip selection with more advanced features than the previous algorithms.

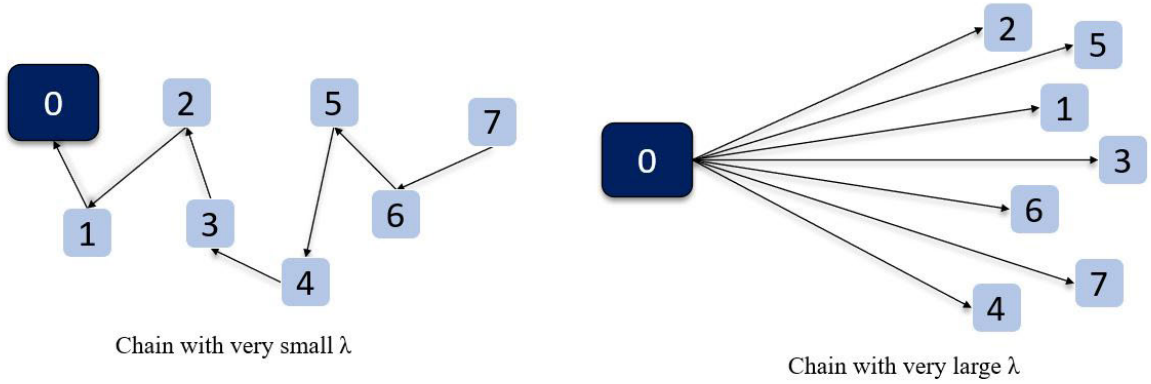


FIGURE 8. Variation in amount of λ.

The tip algorithm's main feature is its ability to avoid lazy tips ''transaction that approves old transactions than the latest transactions,'' it sends a broadcast based on not updated tangle, this will not help the tangle, since no new transactions are confirmed. To deal with the lazy tips problem, a system with cumulative weights should represent each transaction's importance better. The central concept behind the cumulative weight is adding a counter for each transaction, how many approvals they have, and adding one for the current state. The counter is also used for direct and indirect approvals [112]–[118]. If with every tip it chooses the heaviest weight transaction without any probabilities involved, we will reach a Super-Weighted Random Walk, where there are many tips spread out within the timeline, which is the main drawback of walking too much. With this method, a large percentage of the tips will never get approved. So, we need a method to define how to control the heaviest transactions regardless of their importance. The control of the heaviest transactions is defined by a new parameter called (α); if α equal to zero, it will follow the unweighted walk. If we set the α to a very high value, then we will get the super-weighted walk. Determining the best value of α is an open research topic. One more algorithm, called the Markov Chain Monte Carlo algorithm, is used to decide each step-in random walk probability.

The transactions still need extra checking if the two transactions are not conflicting [124] and do not approve conflicted transactions [112]. In case there are conflicting transactions, the nodes need to decide which transactions will be isolated by running the selection algorithm several rounds to check which two transactions are approved indirectly by the selected tip ''unconfirmed transactions'' [121]. To complete and issue a valid transaction, the node must solve a cryptographic puzzle for security reasons. To eliminate the need for mining from miners, the genesis transaction contains all the network tokens. Another notation is the site set of nodes representing transactions in a tangle graph, which is the ledger for storing the transactions [125]. In this way, tangle

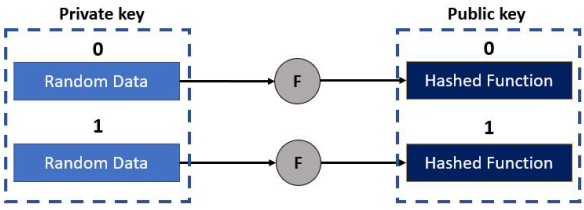


FIGURE 9. Signature is derived from private key parts.

graphs the nodes while they are issuing the transactions, also contributing to securing the network's communication. It is another idea that the tangle graph foregoes the blockchain in favor of more scalability because there are no blocks and chains, no mining, and minors. PoW in the tangle graph is much less than PoW in blockchains [113]–[115].

C. WHAT MAKES THE IOTA QUANTUM-PROOF?

IOTA does not use traditional cryptography algorithms or depend on discrete computing algorithms or factoring numbers. Instead, it uses hash-based signatures, which makes computers faster for validating the transactions. It is a robust protocol resistant against quantum computers because of the Winternitz signature, which uses both private and public keys. As shown in Figure (9), the signature is derived from private key parts. The private key signature will represent each bit of the message in '0' or '1' digit representation to generate random data for each case. The public key will represent the hashed function in each case. When we need to sign a message, the private key for each bit of data will be exposed depending on the message case, whether it is '0' or '1'. Then the hash function will be calculated and compared to the public key, where the verifier will do it. Hence, generating a second round of signatures would contain more details about the private key, which will allow the attacker to tamper further signatures.

TABLE 2. IOTA Features.

Feature	Description
Infinite Scalability	• Built upon DAG structure. • Transactions validation and transformation are run in parallel in tangle.
Lightweight Protocol	• Low energy consumption designed for IoT devices. • IOTA can be run on tiny and big devices.
Nano-payments	• No miners. • No fees. • Real-time payment streaming. • Efficient M2M communication.
Data Security	• Secure data transmission. • Ensure the data authenticity, confidentiality and integrity.
Partition Tolerant	• Clustering in IOTA tangle. • Ability to work offline in off-tangle.

Therefore, the Winternitz One-Time-Signature (OTS) was proposed in [126], [127], where the method used for constructing the digital signature focuses on applying several rounds of cryptographic function on a secret input, where the number of rounds depends on the message to be signed. For that reason, IOTA should not use the same address for sending transactions more than once because a part of the private key is revealed each time it is used for sending, which makes it vulnerable to attacks. Also, IOTA focuses on developing hardware that can handle the ternary representation instead of the binary representation to perform the cryptographic calculation quickly. IOTA uses the ternary hardware with a hash function called the CURL prototype. CURL depends on the random sponge method, where the sponge construction is a critical iterated development to assemble a hash method with a variable-length input and subjective yield length dependent on some fixed length change. The Keccack creators invent CURL, and it uses the SHA-3 algorithm for signing. However, IOTA is still in the developing phase and needs to be improved to run on the ternary hardware. However, since IOTA is still running on binary hardware, there is a need for data conversion from binary to ternary, which is achieved using a hash function called Kerl or (Keccack-348) [69].

D. IOTA FEATURES AND ADVANTAGES

IOTA's idea stands apart from other innovations. As shown in Table (2) its flexible design, which is significantly more progressed than other distributed ledger frameworks, this advanced stage will move forward, with the features given below:

1) DISTRIBUTED DATA TRANSACTION

IOTA is an open-source cryptocurrency made for IoT's environment. This IoT environment is attempting to unite a distributed ledger for the Internet of Things. It is not the same as most types of digital currencies that use blockchains to record transactions. A transmitted record is a database kept and unreservedly refreshed by every member of the expansive network in its least complex structure. The distribution process is unique, as there is no central authority to distribute the records to other nodes, yet it instead keeps them independently by every center point. Each node on the tangle approves two past transactions to guarantee that the more significant part agrees with the consensus that another distributed record has been built upon by IOTA. The IOTA's main idea is the capacity to distribute through a tangle diagram, which gives the benefit of building up secure, totally validated, and carefully designed correspondence between IoT devices and sensors [128], [129].

2) MICRO-TRANSACTIONS AND ZERO FEES

IOTA generates micro-transactions in real-time, just like an ecosystem prepared and adaptable for scaling without mining and blocks. The system's security and authorization are maintained by all the nodes connected to the system and create transactions. For the first time in tangle innovation, micro-transactions are enabled, which gives developers new business areas for their IoT device applications. In addition to exchanging money between users, IOTA enables IOTA devices to exchange transactions to demand support. To introduce this service, users will pay a limited amount of IOTA's known as ''micro-payment'' in exchange for the data. Zero fees for each exchange is another advantage that accompanies IOTA since there is no need to pay miners, which is a tangle innovation achievement [130].

3) SCALABLE DISTRIBUTED LEDGER

There is no scalability constraint because each transaction allows the sender to validate two past transactions on the tangle to connect to neighbors. Further transactions may be checked as the number of users transmitting them increases, meaning IOTA scales proportionally to the sum of transactions. IOTA mainly makes the mechanism better because of its infinite variations in the total number of transactions generated. Furthermore, IOTA will reach a high transaction throughput if more IOTA transactions are made, and the confirmation rates will improve [131].

4) MASKED AUTHENTICATION MESSAGING (MAM)

Masked authenticated messaging is a second-layer data communication protocol that fulfills all industries' critical needs from integrity, authentication, and privacy. It adds some

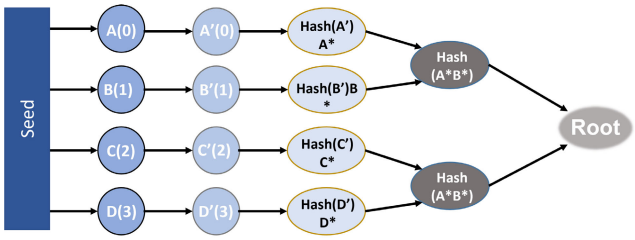


FIGURE 10. Signature is derived from private key parts.

functionalities to access the encrypted messages over the tangle. Any address ''seed'' in IOTA can send a message over a network by providing proof of work to prevent spamming. A subscriber would collect the message when it reaches the subscriber's point if the node was listening to that specific channel. One main advantage of MAM is its ability to transmit by remote control commands. MAM is also more efficient to use in some off-tangle protocols in real-time streaming. Also, because of the distributed nature of the nodes, the messages contribute to the security of the network by increasing the total hashing power (e.g., a similar example is a Radio if the frequency is correct, one can listen to the channel; otherwise, we cannot) [116], [132]. RuvviTag is an example of MAM being installed in the IoT device. It is an open-source program where it starts in advertising itself on boot until a connection is made. The program initializes the MAM protocol by sending a predefined data packet. RuvviTag parses this data and replies with a plaintext message ''INIT MAM.'' After that, the MAM encryption process is finished and split into chunks that are distributed to nodes. After the transmission process is completed, the RuvviTag goes to sleep to conserve power. MAM has used the Merkle tree signature scheme to sign the cipher block of an encrypted message in more depth. The channel's ID is used as a root of the Merkle tree signature, and the seed of IOTA will be to create the Merkle tree. Merkle tree has several parameters: The index is one of the parameters used for producing the address (Seed, Index, Security). Figure (10) shows that A, B, C, D are private keys, and their corresponding addresses A', B', C', D' are generated with indexes = 0,1,2,3. The hash(addresses) are represented as A'', B'', C'', D'', which are narrowed down by combining each pair up to the root.

In public mode, this root is utilized as the MAM address. Meanwhile, in restricted and private modes, the MAM address is hash(root). Each message is encoded with a one-time pad (OTP) that consists of the channel ID and the index of the key used to sign the message; an extra nonce might be utilized as a revocable encryption key. The subsequent figure hash is marked utilizing the private key contained in one of the leaves. The encoded payload, the signature, and the leaf's siblings are then distributed to the tangle where anybody having access to the symmetric key can discover and decrypt it. While expanding a MAM stream, the message is first confirmed by approving if the signature is contained in one of the tree's leaves. On the other hand, if the signature approval fails, the whole message is deemed invalid.

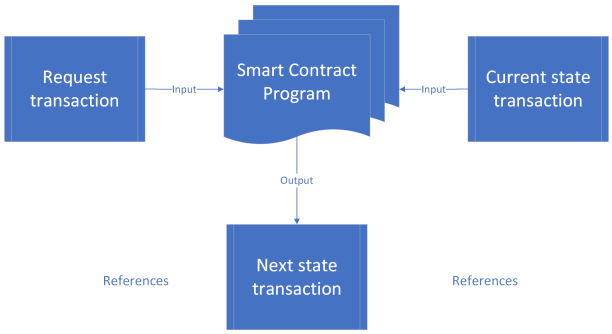


FIGURE 11. IOTA smart contract program.

5) QUANTUM COMPUTING PROTECTION

Quantum computers will have the option to play out the encryption strategies quicker than current computers, as discussed in Section IV, although it is still in the development stage and will not be available soon, and it is estimated to land in the year 2030. Nevertheless, IOTA is quantum-resistant [64, 116] as it uses the Winternitz One-Time Signature Scheme.

E. IOTA SMART CONTRACT

IOTA Smart Contracts are smart contract programs Figure (11) executed on layer two by the authorized committee (off-Tangle). The Nodes Committee collectively updates the ledger by sending signed transactions to the tangle using the threshold signature. IOTA[1] Smart Contracts are very powerful and require fewer resources than blockchain. They make use of cases that might not have been feasible, with fees being the only benefit. This is especially true in the IoT domain, where micro-contracts and micro-transactions are expected to be normal. IOTA Smart Contracts are classified as an immutable state machine:

State Machine: Every smart contract has a state linked to the Tangle. The state includes data such as account balances and input conditions. Each state update represents a state change on the Tangle.

Immutable: The state code and the smart contract program code are permanent since they are stored on the Tangle. The state can be updated incrementally by linking new transactions to the Tangle.

The tangle creates a verifiable audit trail for state transitions. It assumes that the state transitions are accurate and cannot be manipulated by malicious or incorrect nodes. IOTA Smart Contracts have a natural way to run distributed computing. Each smart contract can be executed in a localized scope without requiring the entire network to execute it. This approach also ensures that IOTA Smart Contracts would not become an obstacle to scaling up the IOTA network in the future. Every Smart Contract has its owner, who is responsible for:

[1] http://visualgenome.org/

- Build and submit a smart contract application to the network.
- Deciding how large the committee would be (number N) and picking network nodes to be part of it.
- Deciding how many committee nodes can reach a consensus on smart contract state changes. That number is called a quorum.
- Defining other general parameters for the design of the smart contract.

The smart contract owner may be a single entity, such as an organization or a person, or maybe a decentralized collection of peers, such as a consortium of organizations. For every case, the owner only controls the smart contract setup and configuration and does not participate in the operation of the smart contract. Owners may choose how to set up smart contracts, depending on their context and purpose. For example, a smart contract that handles a high-value of transactions may require a large node committee. Simultaneously, a smart contract that handles micro-transactions may require only a few nodes in the committee. There are many possible reasons for a smart contract to be created or implemented. The rewards are one of the main reasons. Although IOTA transactions are fee-less, IOTA Smart Contracts provide an opportunity for businesses to charge a fee for IOTA tokens, such as to cover operating costs. This fee is called a ''reward''. Both owners and committee nodes are eligible for smart contract rewards. It is up to the owner to negotiate a minimum acceptable reward with the committee's node operators.

- Committee nodes can receive rewards by processing a specific smart contract that provides rewards.
- Owners also have the option of creating smart contracts that give a percentage of the reward to the owner.

Another potential reason to be a member of the committee is to build a positive reputation. Smart contract owners can choose to set up committees of nodes with a positive reputation only. Such a reputation system may establish an open market for committee nodes that promotes good conduct on the network. The Smart Contract Software is an algorithm that includes instructions for a virtual machine (VM). The VM can be in any language or hard-coded in the node program. As shown in figure (12), the program takes two transactions as input: the request transaction and the current state transaction. The following state transaction often applies to the request transaction and the previous state transaction. In this way, the Smart Contract Software has a deterministic way to create a chain of state updates triggered by incoming requests. The hash program is stored in the Tangle and is thus immutable.

1) IOTA SMART CONTRACT EXECUTION

An SC is operated by a committee of fixed-size nodes (with distributed sharing of private keys) that executes a program by consensus and sends the results to the tangle. The SC's fixed size is determined by the SC's owner (issuer and operator). Hundreds are still a feasible size for threshold cryptography.

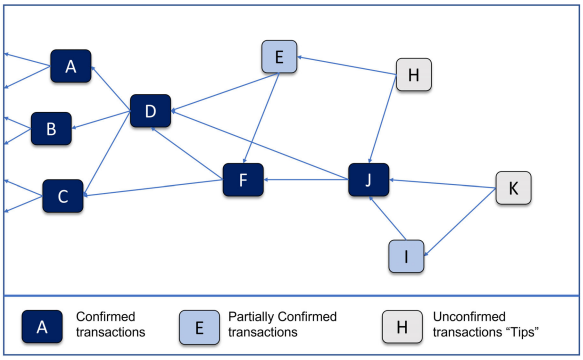


FIGURE 12. IOTA Tangle.

One node is the bare minimum, meaning that SC requests are processed by just one centralized script. Only the creator, other committee nodes, and other trusted (so-called access-) nodes know the addresses of committee nodes in the network.

Each smart contract has an owner who is in charge of the following:

- Creating and uploading the SC software to the network.
- Choosing the nodes that will be members of the committee and deciding the committee's size (number n).
- Choosing a ''quorum,'' which is the number of committee nodes that must agree on SC status updates.
- Identifying other general configuration parameters.

An owner may be a single entity, such as a company or a person, or a decentralized group of peers, such as a consortium of companies. In any case, the owner is only responsible for the SC's setup and configuration and is not involved in its operation. Depending on the context and intent, the owner may choose how SCs are set up. An SC that handles high-value transactions, for example, may need a broad committee of nodes, while an SC that handles micro-transactions may only need 20-30 nodes.

An SC program is a virtual machine instruction set in the form of an algorithm (VM). IOTA SC's primary virtual machine is WebAssembly (WASM).

2) CHAIN OF IOTA SMART CONTRACT

Contract chains, which reflect the contract state, are used to transact smart contracts. Any time a smart contract receives a request, its state is changed, and a new block is added to the contract. In one block, all of these updates are gathered and verified. As a consequence, the chain retains all previous states as well. Many Smart Contracts can be found on the chain, all of which are dependent on the chain's global state. The contract chain is, in this context, a Tangle-based blockchain. IOTA Smart Contracts are similar to ''traditional'' Smart Contracts, with the added advantage of building several parallel chains, each using the same native IOTA token and safely exchanging between them the Tangle. This ensures that various applications can securely communicate with each other.

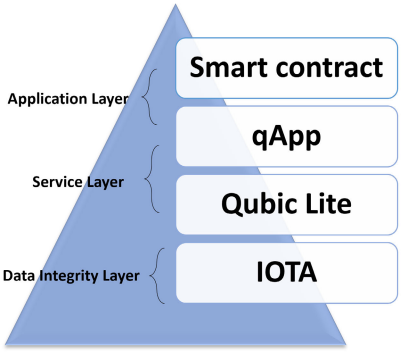


FIGURE 13. IOTA Smart Contract Layers.

3) MULTIPLE CHAIN ENVIRONMENT

A multi-chain environment has been introduced with the Alpha update, which is protected by the Tangle (base layer 1): Subnets made up of committee nodes can run multiple networks in parallel while maintaining the tangle environment that protects IOTA's digital assets. Each of these Chains, which operate similarly to an Ethereum blockchain, can host many smart contracts. The IOTA Foundation's smart contract solution differs from current architectures in that it eliminates inefficiencies such as the inability to operate smart contracts in parallel and at scale, the inability to run ''third-party'' smart contracts on various virtual machines, and the insertion of volatile and often unaffordable fees, to name a few. Developers and businesses may identify their flexible environments and the sizes of validation committees that meet their necessary or desired level of decentralization and protection with the IOTA Smart Contracts Protocol, the layers of this protocol are shown in Figure (13). They can use the IOTA Smart Contract Protocol to run a permission Smart Contract chain, for example, checked by a committee of their nodes or define a committee of nodes among consortium partners as the structure of the smart contract is shown in Figure (14). The IOTA smart contract protocol (ISCP) is a second layer built on top of the core protocol and executed by GoShimmer nodes. ISCP is also designed to be fully ''permissionless,'' meaning that a committee of validators may be selected from a pool of validators available on the open market. The inherent protection and interoperability that comes from anchoring each Smart Contract state and its outcomes on the IOTA fee-less base layer benefit all Smart Contract chains, whether open or private. As a result, IOTA Smart Contracts do not necessitate the execution of all Smart Contracts by all nodes in the network but instead allow for a more versatile, meaningful concept that meets the Smart Contract owner's needs. This would drastically reduce cost and power consumption while also increasing flexibility and ensuring that individual security specifications and the compatibility and interoperability demanded by applications that run on distributed systems that are called decentralized Applications (dApps) are met.

VI. IOTA SECURITY

Currently, security is imperative for keeping up control of your things whether it is physical or virtual. Cybersecurity is essential in keeping you secured, shielding your integrity, and staying away from unwanted information exposure. IOTA gives robust cybersecurity measures around information integrity, validation, accessibility, and confidentiality, which are the principal security necessities for IoT devices as discussed in section III, and it is even future proof against quantum attacks. While these security features are significant for using public or private key encryption, the keys themselves depend increasingly on ''human'' safety measures. This is considered the weakest point and the main issue with these. Finally, many clients have fallen victim to an attack against the IOTA people group. The attackers in that occurrence effectively distinguished this ''human component'' as the weak connection. By utilizing a well-made phishing site that seemed, by all accounts, to be a real IOTA seed generator, they had the option to gather numerous seeds over quite a while. They went after the trust of the network and invested energy cautiously improving the page to seem higher in internet searcher results, further legitimizing their trick according to unsuspecting community members. Unfortunately, this isn't the first, nor will it be the last time such a trick is executed against IOTA, or digital ledger technologies more comprehensively. There is just a single method to ''prove'' who owns a given IOTA address, and that is to spend from it. To spend from an address, one just must know the seed from which the location began. The key takeaways of these realities are: Spending IOTA tokens is confirmation of ownership and If your seed is attacked in any way, the tokens in your wallet are gone. Nevertheless, there are a few things you can do to protect yourself such as, treating your seed as though it is the main key to your safety. Whoever holds the key has direct access to the contents of the safe. IOTA is an evolutionary advancement in distributed ledger technology that can revolutionize some industrial sectors as diverse as finance, healthcare, automotive and logistics. Many new investors are realizing the potential of IOTA and it is growing in popularity. It is however very important for people to understand the personal responsibility they take on when investing in IOTA, which also applies to all other decentralized systems. The seed is intended to cover the security of IOTA and how the reader can confidently purchase and store the IOTA Token. David [83] proposed to choose between three levels of signature security, these levels are:

1) Security level 1: 81-trit or 128 -bit, which is relatively low security with very high performance and efficiency, which is fully suited for tiny IoT devices that will only transact and store a small number of values.
2) Security level 2: 162-bit or 256-bit, which is standard security with medium efficiency which is best for users who store a higher amount of data.
3) Security level 3: 243-trit or 384-bit, which is full-blown quantum-proof security that conforms all National

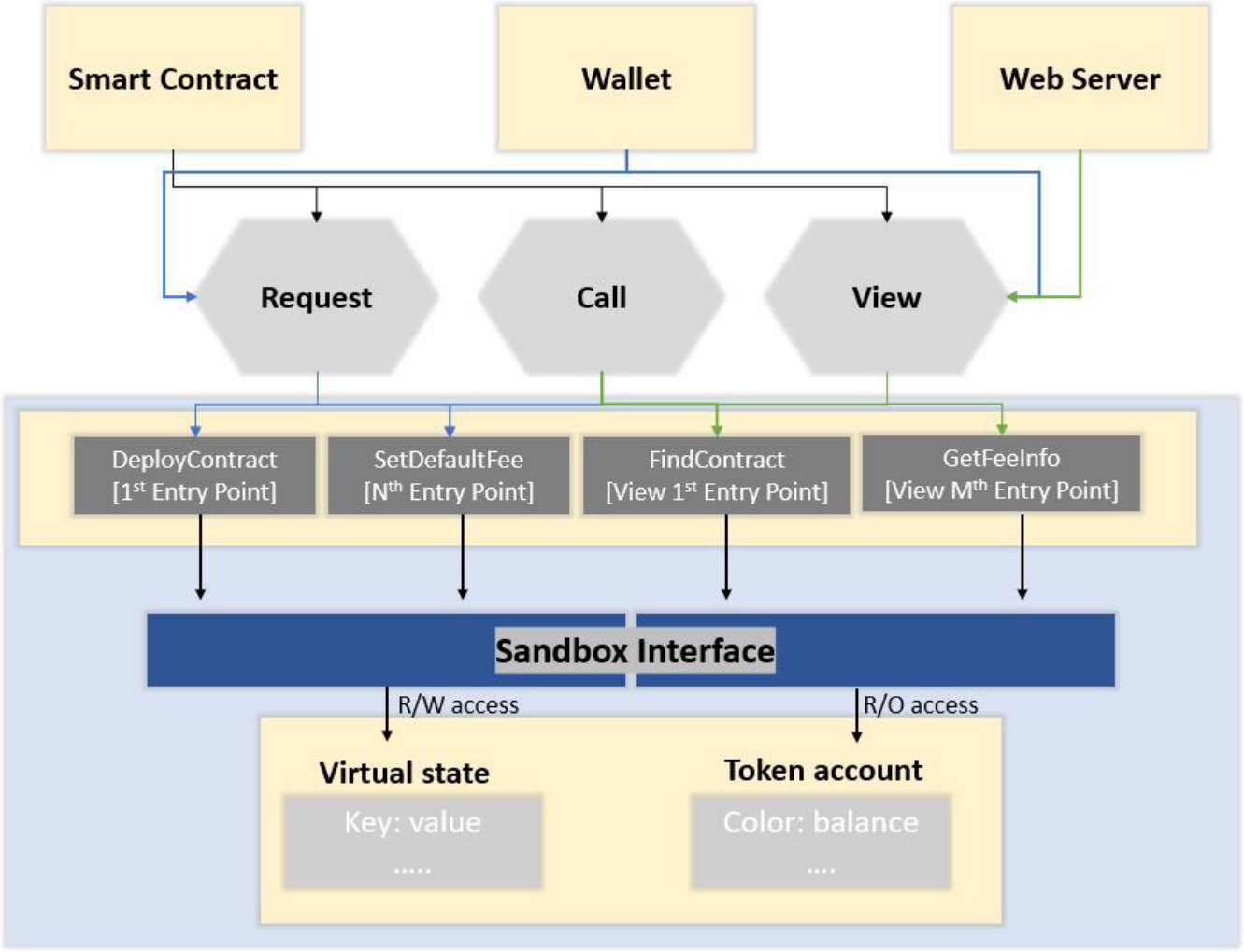


FIGURE 14. IOTA Smart Contract Structure.

Security Agency (NSA) requirements for sensitive material.

IOTA is still in the development stage and still depends on some coordinator nodes to ensure the security that checks every transaction to make sure it is legitimate. The IOTA community developers plan to be shutting off the coordinator, to make the IOTA fully decentralized. If the IOTA depends fully on users, the network will be vulnerable to attack easily if it is not big enough. If the attacker can attack more than one third of the total transactions, then the whole network can be compromised. Table (4) shows the summarizing of IOTA application in the literature.

VII. IOTA LIMITATIONS

Regarding the misconception in transaction fees, in IOTA you do not need to pay any token to validate your transaction as compared to other distributed ledger technologies. However, each transaction would still require a fee in order to secure the network. It requires a fee proportional to the amount of PoW per second, which corresponds to some computational power limited by available CPU resources. Also, ASIC processors are in binary representation which will make local Proof of Work slow. The difficulty will also be increased to maintain a high PoW cost, in this case, you will have to use a cloud ASIC farm for the PoW. The second misconception is that IOTA is viable for IoT in terms of sustainability in computational overhead, as its computational cost is high for IoT devices. The devices must do the PoW, which still requires a huge cost overhead due to the security level needed for the PoW. The tangle also requires a Proof of work for its security. This implies that transaction generators must spend money on chips and electricity. The proof of Work also requires each IoT device to have a working chip on it. However, the cryptocurrencies that rely on the Proof of stake (PoS) will increase the power consumption which translates at the end to an increased cost even by using Application Specific Integrated Circuit (ASIC) processors which are designed for special applications. The third misconception is that IOTA does not support smart contracts because the transaction order is biased to each node. Most of IOTA's use cases proposed that

smart contract is a big advantage to IOTA if it is implemented. The smart contracts are the ones that require an order of transaction which makes the computation complex due to its complex transactions.

VIII. PERFORMANCE ANALYSIS: IOTA VS. BLOCKCHAIN

''Resolved the three major issues of blockchain - fees, scaling limitations, and centralization.'' As per David Sonstebo, the co-founder of IOTA. The major benefit from the IOTA structure is that it removes the reliance on a central node with entire transaction fees-free, because of the absence of miners, so the mining fees in IOTA is not a factor in high amount transactions. However, using Bitcoin which relies on mining, creates a centralization issue, the statistics shows that over 70% of Bitcoins are currently controlled by server farms in China, which means it's under the Chinese government control and if they decide to cut off the farms, it could have disastrous effect on its value and its usability. But IOTA does not rely on a mining process or on miners to produce the transactions and is, therefore, a truly decentralized framework that protects the currency from such a similar event [113].

The transfer to blockchain requires a considerable amount of time and money. Blockchain also requires costly hardware due to the complexity of the processing logic and the blockchain ledger structure from a network participant perspective. There is as well a major concern related to its status in the long-term due to its scalability, which loomed over the Bitcoin head from the start. The scalability of cryptocurrencies is its ability to handle the growth in its values while allowing other network participants to invest in the world of digital currency. This is the main problem with blockchains in general that limit the number of requests that can be made to its ledger. While IOTA deals with the scalability issue by eventually reaching the stability point. As Bitcoin is an example of blockchain technology, IOTA is an example of tangle technology [113]. IOTA solves some problems of blockchain's structure as shown in Table 1. Other areas where IOTA beats the blockchain: First, Bitcoin has a very low transaction rate with a double-digit range which is simply not enough for many applications, however, in IOTA the transaction rate increases as more users get connected to the network. Also, the time for the confirmation of a transaction is much better in IOTA because, in blockchain, all should reach a consensus, which costs a lot of time. The second area where IOTA beats blockchain is its scalability, in IOTA the scalability increases as the number of transactions increase. The system gets faster as the number of participant nodes and transactions increases. Micro-payment is another major area where IOTA outperforms blockchain where IOTA is a real micro-payment currency. In general, what makes IOTA interesting is the low latency paired with the possibility to send transactions with free of transaction fees. While in the blockchain, with Bitcoin as a payment system, the problem is created with the mining processes. Efficiency is perhaps the main issue facing blockchain users because it is too costly in terms of power consumption and security assurance. If you use the blockchain technology for in-house work, it will be difficult to reproduce the concept of the miners to guarantee extreme security for Bitcoin, and for that more and more power is needed. Power consumption for Bitcoin Mining is currently equal to a full year electricity consumption for Argentina. IOTA is a lot smarter because you do not need the whole mining process. The security in blockchain is only achieved with high transaction rates, if we neglect the security part, the computational power will decrease. If we do increase the security to increase the transaction rate, then the blockchain is not tamper proof, and we cannot prove that the data cannot be manipulated. The blockchain technology is tamper proof only from outside the block because they don't have physical access to the actual systems. However, the administrator of the blockchain network can theoretically manipulate the new data, which is a dilemma for industries and companies, that the blockchain cannot be changed or modified over time. In IOTA this scenario does not happen.

IX. SIMULATION ANALYSIS: IOTA VS. BLOCKCHAIN

A simulator can mimic the performances of network nodes in reaching the consensus by providing behavior similar to a real system. In addition, a distributed ledger simulator usually provides a convenient way for the participants to tune the system configuration to run different settings for the sake of comparison. In this section, we will look at the role of simulation in IOTA and blockchain environments.

A. DAG SIMULATOR

Manuel *et al.* [146] introduced the DAGSim simulator, a DAG-based distributed ledger protocol for an asynchronous, continuous-time, and multi-nodes simulation framework. They model actual and semi-actual participants in the system to assess the behavior of IOTA cryptocurrency. DAGSim simulator shows that the participants with low latency and a high connection rate have a higher probability of having their transactions accepted in the network. DAGSim simulator allows the simulation of uncertain scenarios and assesses whether the implemented consensus algorithms have the desired effects in terms of resistance and security. Some research papers discusses the leverage of simulations linked with analytical decisions to handle the validation or exploration process. Seongjoon *et al.* [147] suggested and executed a general simulator based on DAG cryptocurrency using Python. The simulator was used to validate the analytical performance model by publishing a transaction to the ledger with a smaller average number of tips to increase the transaction speed. Michele in [148], introduced and released an open-source simulation environment based on DAG to analyze the network's performance. Furthermore, Bartosz Ku smierz [149] runs a continuous-time simulator to test the tip count reliability while changing the joining transaction rate. The authors perform analytical predictions on the number of choosing the tips using a uniform random tip selection algorithm, and they showed the effect of this on the growth of the Tangle.

TABLE 3. Comparison between IOTA and Blockchain [101-119, 105,117].

	Blockchain	IOTA
Concept	Digital Money	Digital Money for IoT
Market Cap	274 Billion$	10 Billion$
Fully Developed	Yes	Still-in transition
Trust-less Operation	Yes	Yes
Consensus	PoW	Currently uses a coordinator
Smart Contract	Yes	PoC
User Authentication	Digital Signature	Digital Signature
Address Format	160 bit	81 trytes
Release Date	103%	1003%
Transaction Weight-age	Low fees paid, slower to confirm	Instantly
Growth Rate	274 Billion$	10 Billion$
Structure	Block	Nodes
Scalability	Decrease over time	Increase over time
Transaction Speed	10 Minutes	2 Seconds
Miners	Has miners	No miners
Transaction per second	14	Unlimited
Quantum computer resistant	No	Yes

TABLE 4. IOTA methods description and applications.

Method	Year	Application	Description
[134]	2019	Healthcare Industry	"IOTA Viability In Healthcare Industry"
[135]	2018	Vehicular Applications	"IOTA Feasibility and Perspectives for Enabling Vehicular Applications"
[136]	2019	Smart utility meter system and a smart car transaction system	"Enhancing IoT Security and Privacy using Distributed Ledgers with IOTA and The Tangle"
[137]	2020	Mobile-Agent Distributed Intelligence Tangle-Based approach	"Enabling distributed intelligence for the Internet of Things with IOTA and mobile agents"
[138]	2018	Tango for Periodic Pulsed Entries	"A Semi-Synchronous Iota-Tangle type Distributed Ledger"
[139]	2019	Decentralized Capability-Based Access Control framework using IOTA for large scale infrastructure "smart city"	"A Decentralized Lightweight Capability Based Access Control Framework using IOTA for Internet of Things"
[140]	2019	TangoChain, utilizing a directed acyclic graph as underlying ledger data structure for smart cities	"A Lightweight Distributed Ledger for Internet of Things Devices in Smart Cities"
[141]	2019	Use Case in Blood Glucose Data	"Designing a Distributed Ledger Technology System for Interoperable and General Data Protection Regulation–Compliant Health Data Exchange"
[142]	2020	Securing the logs of a system	"Securing Logs of a System - An IoTA Tangle Use Case"
[143]	2020	Bosch XDK110 multisensor and a storage/visualization application	"IoT sensors integrated with the distributed protocol IOTA/Tangle"
[145]	2019	Manufacturing industry	"On IOTA as a potential enabler for an M2M economy in manufacturing"

B. BLOCKCHAIN SIMULATOR

Ryohei *et al.* in [150] proposed a SimBlock that can visualize participants behavior and transactions propagation. By exploring better neighbor selection policies and evaluating the effect of relay networks. SimBlock can facilitates the research fields for blockchain network. In [151], Maher *et al.* developed BlockSim, a framework for creating discrete-event dynamic system models for blockchain systems. BlockSim comprises three layers: an incentive layer, a connector layer, and a system layer. It is programmed in python and focused on modeling and simulating block generation using the Proof of Work consensus mechanism. To assist developers in better comprehending, evaluating, and planning for system performance. Santosh *et al.* created a complete open-source simulation tool for permission blockchain systems in [152]. This simulation is intended to assess system stability and transaction throughput (TPS) for private blockchain networks by simulating scenarios and then decide the best system settings for developers' needs. The findings of a comparison between this simulation and the real-world Ethereum private network using PoA consensus prove that BlockSIM can be beneficial.

A summarized table from section VII and VIII is shown in Table (3)

X. FUTURE DIRECTION

It is extensively acknowledged that IOTA innovation and its applications are still in their earliest stages. There are many open research that need to be addressed to guarantee that IOTA is a solid match for IoT devices as far as security and effectiveness. Solid understanding of industrial environment requirements is required before IOTA can be generally conveyed. Although empowering IOTA innovation is making the IoT idea increasingly possible, a huge research exertion is required.

A. INFORMATION SECURITY CHALLENGES

IoT is vulnerable toward attacks for a few reasons. To start with, because of their resource capacity limit, the greater part of the communications is wireless, which makes eavesdropping extremely easy. Second, the vast majority of IoT components are known for their low energy and processing capacities, they can't execute complex methods to enhance their security. The most serious issues were explained in section VIII which identified a set of security prerequisite

concerns in fulfilling particularly the authentication requirement, which is difficult because it requires fitting infrastructures and servers to accomplish their objective through the exchange of proper messages with different nodes. Additionally, for information integrity, solutions should ensure that an enemy can't alter information without the system recognizing the change. The issue of information integrity has been broadly considered in all conventional processing and communication systems, yet it needs to be further researched in IOTA. Nonetheless, new issues emerge when the attacker access client seeds, at that point the information can be hacked by enemies while it is stored in the node.

B. RESEARCH TRENDS

IOTA has shown its potential in industries and academic fields. We will discuss possible future research directions concerning:

1) STOP THE COORDINATION

IOTA is designed as a decentralized ledger system. Nevertheless, coordinators are centralized and the whole IOTA network relies on coordinators. Where the coordinator is a checkpoint for valid transactions, which are then validated by the entire network.

2) BIG DATA ANALYTICS

IOTA could be joined with big data. Here we generally sorted the blend into data management and data analytics. Concerning data management, IOTA could be utilized to store securely significant amount of information that is distributed. IOTA could likewise guarantee that the information is unique and tamper free. About data analytics, transactions on IOTA could be utilized for huge data analytics.

3) REPLACE THE PoW

A major disadvantage of IOTA is the PoW, where the function of PoW is like the stacking of consecutive transactions that have fixed difficulties. Since IOTA is created to run on low power devices, the difficulty is low, and it would not take much in the method for dedicated resources to weight the whole processing power of the IOTA tangle. This implies the security of the tangle straightforwardly relies upon the number of transactions being handled and that there is no real way to adjust the security level to true conditions. To solve this problem, we can replace the PoW of IOTA by the RaiBlocks currency technique, which is like IOTA, both of them use the DAG, RaiBlocks has no miners, no transaction fees, and near-instant transactions. However, it differs from IOTA that it uses a concept of block-lattice, where every node holder maintains his private blockchain with each block holding a single transaction in it. This means that each transaction requires two addresses for sending and receiveing. The PoW in RaiBlocks is accomplished by deciding on conflicting transactions. PoW stacking requires maximizing the constant system hash rate which is a cost that is inherently paid as far as power utilization by clients of the network. Since RaiBlocks doesn't depend on high system PoW to look after security, the working expense of RaiBlocks nodes is a lot lower.

XI. CONCLUSION

In this paper we presented IOTA Tangle for internet of things. We compared it to Blockchain technology. We pointed out the advantages of using IOTA tangle. In summary, the tangle graph solves the main issues in blockchains and most other cryptocurrencies, which are the scalability and the transaction fees, by eliminating the need for a mining process and depending on network participants to perform the proof of work by approving two previous transactions. Thus, removes the need for miners and ensure that the system is fully decentralized. The most interesting part of the tangle technology is that the transaction speed increases when the number of users increases which is not provided in the blockchain. IOTA will not stop at this point; many industries are working on applying the IOTA to real-world applications. This survey established an understanding of the most powerful techniques used to secure IoT devices which is the blockchain and covers the limitations of the blockchain by fitting the IOTA novel design, where the goal of IOTA is to help manage, utilize and optimize the IoT.

REFERENCES

[1] J. Pan and J. McElhannon, "Future edge cloud and edge computing for Internet of Things applications," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 439–449, Feb. 2017.
[2] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.
[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.
[4] Egham. *Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent From 2016, 2017*. Accessed: Mar. 15, 2016. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016
[5] T. Gomes, F. Salgado, S. Pinto, J. Cabral, and A. Tavares, "A 6LoWPAN accelerator for Internet of Things endpoint devices," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 337–371, Dec. 2017.
[6] H. Tsunoda and G. M. Keeni, "Feasibility of societal model for securing Internet of Things," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Madrid, Spain, Jun. 2017, pp. 541–546.
[7] J. Hu, Y. Cai, and N. Yang, "Secure transmission design with feedback compression for the Internet of Things," *IEEE Trans. Signal Process.*, vol. 66, no. 6, pp. 1580–1593, Mar. 2017.
[8] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.
[9] S. J. Johnston, M. Scott, and S. J. Cox, "Recommendations for securing Internet of Things devices using commodity hardware," in *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, Dec. 2016, pp. 307–310.
[10] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, Jul. 2017.
[11] J. Chaudhry, A. Ibrahim, and A. Bashir, "Internet of threats and context aware security: Part two," *IEEE Internet Initiative Newslett.*, May 2017.
[12] A. Batcheller, S. C. Fowler, R. Cunningham, D. Doyle, T. Jaeger, and U. Lindqvist, "Building on the success of building security in," *IEEE Secur. Privacy*, vol. 15, no. 4, pp. 85–87, Aug. 2017.
[13] *INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems, in Co-Operation With the Working Group RFID of the ETP EPOSS, Internet of Things in 2020: Roadmap for the Future*, Eur. Commission, Inf. Soc. Media, Europe, May 2008.
[14] *CERP-IoT Cluster, Visions and Challenges for Realising the Internet of Things, European Commission*, Eur. Commission, Europe, 2010.

[15] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[16] C. Doukas, "Building Internet of Things with the Arduino," CreateSpace, North Charleston, SC, USA, Tech. Rep. 1, 2012.

[17] T. Mark, "Industry 4.0 and Internet of Things tools help streamline factory automation," Control Eng., California, TX, USA, Tech. Rep., 2015, pp. M7–M10, vol. 62, no. 2.

[18] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, Jun. 2015.

[19] Y. Sun, H. Song, A. J. Jara, and R. Bie, "Internet of Things and big data analytics for smart and connected communities," *IEEE Access*, vol. 4, pp. 766–773, 2016.

[20] S. Lee, G. Tewolde, and J. Kwon, "Design and implementation of vehicle tracking system using GPS/GSM/GPRS techology and smartphone application," in *Proc. Internet Things (WF-IoT)*, 2014, pp. 353–358.

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

[22] F. Shrouf, J. Ordieres, and G. Miragliotta, "Smart factories in Industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm," in *Proc. IEEE Int. Conf. Ind. Eng. Manage.*, Dec. 2014, pp. 697–701.

[23] F. Hu, D. Xie, and S. Shen, "On the application of the Internet of Things in the field of medical and health care," in *Proc. IEEE Int. Conf. Green Comput. Commun., IEEE Internet Things IEEE Cyber, Phys. Social Comput.*, Aug. 2013, pp. 2053–2058.

[24] K. Mandula, R. Parupalli, C. H. Murty, E. Magesh, and R. Lunagariya, "Mobile based home automation using Internet of Things (IoT)," in *Proc. Int. Conf. Control, Instrum., Commun. Comput. Technol.*, 2015, pp. 340–343.

[25] L. Atzori and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, 2010.

[26] K. Hong, D. Lilethun, U. Ramachandran, B. Ottenwalder, and B. Koldehofe, "Mobile fog: A programming model for large-scale applications on the Internet of Things," in *Proc. MCC*, 2013, pp. 15–20.

[27] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[28] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.

[29] K. Zhae and L. Ge, "A survey on the Internet of Things security," in *Proc. 9th Int. Conf. Comput. Intell. Secur.*, 2013, pp. 336–341.

[30] A. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digit. Commun. Netw.*, vol. 4, no. 2, pp. 118–137, 2018.

[31] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in *Proc. Euro Med Telco Conf. (EMTC)*, Nov. 2014, pp. 1–5.

[32] R. Weber, "Internet of Things—New security and privacy challenges," *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, 2010.

[33] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.

[34] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.

[35] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 111, no. 7, pp. 1–6, Feb. 2015.

[36] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer*, vol. 44, pp. 51–58, Sep. 2011.

[37] H. Pohls, "JSON sensor signatures (JSS): End-to-end integrity protection from constrained device to IoT application," in *Proc. 9th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Brasília, Brazil, 2015, pp. 306–312.

[38] H. C. Pohls, "JSON sensor signatures (JSS): End-to-end integrity protection from constrained device to IoT application," in *Proc. 9th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.*, Brasília, Brazil, Jul. 2015, pp. 306–312.

[39] D. Airehrour and J. Gutierrez, "Ananalysis of secure MANET routing features to maintain confidentiality and integrity in IoT routing," in *Proc. Int. Conf. Inf. Resour. Manage.*, 2016, pp. 15–26.

[40] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) security: Current status, challenges and prospective measures," in *Proc. 10th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2015, pp. 336–341.

[41] M. Abdmeziem, "Data confidentiality in the Internet of Things," Ph.D. dissertation, ResearchGate, Berlin, Germany, 2016.

[42] M. T. Lazarescu, "Design of a WSN platform for long-term environmental monitoring for IoT applications," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 3, no. 1, pp. 45–54, Mar. 2013.

[43] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for Internet of Things (IoT)," in *Proc. 2nd Int. Conf. Wireless Commun., Veh. Technol., Inf. Theory Aerosp. Electron. Syst. Technol. (Wireless VITAE)*, Feb. 2011, pp. 1–5.

[44] C. Perera, P. P. Jayaraman, A. Zaslavsky, D. Georgakopoulos, and P. Christen, "MOSDEN: An Internet of Things middleware for resource constrained mobile devices," in *Proc. 47th Hawaii Int. Conf. Syst. Sci.*, Jan. 2014, pp. 1053–1062.

[45] *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*, IEEE Standard 610, 1991, pp. 1–217.

[46] M. Elkhodr, S. Shahrestani, and H. Cheung, "The Internet of Things : New interoperability, management and security challenges," *Int. J. Netw. Secur. Appl.*, vol. 8, no. 2, pp. 85–102, Mar. 2016.

[47] J. Cooper and A. James, "Challenges for database management in the Internet of Things," *IETE Tech. Rev.*, vol. 26, no. 5, pp. 320–329, 2014.

[48] G. Nair and S. Sebastian, "Blockchain technology centralised ledger to distributed ledger," *Int. Res. J. Eng. Technol.*, vol. 4, no. 3, pp. 2823–2827, 2017.

[49] D. Burkhardt, M. Werling, and H. Lasi, "Distributed ledger," in *Proc. IEEE Int. Conf. Eng., Technol. Innov. (ICE/ITMC)*, Jun. 2018, pp. 1–9.

[50] R. Maull, P. Godsiff, C. Mulligan, A. Brown, and B. Kewell, "Distributed ledger technology: Applications and implications," *Strategic Change*, vol. 26, no. 5, pp. 481–489, 2017.

[51] A. Sunyaev, "Distributed ledger technology," in *Internet Computing*. Cham, Switzerland: Springer, 2020, pp. 265–299.

[52] S. H. Shaheen, M. Yousaf, and M. Jalil, "Temper proof data distribution for universal verifiability and accuracy in electoral process using blockchain," in *Proc. 13th Int. Conf. Emerg. Technol. (ICET)*, Dec. 2017, pp. 1–6.

[53] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consum. Electron. Mag.*, vol. 7, no. 2, pp. 18–21, Mar. 2018.

[54] M. Pustisek, A. Kos, and U. Sedlar, "Blockchain based autonomous selection of electric vehicle charging station," in *Proc. Int. Conf. Identificat., Inf. Knowl. Internet Things (IIKI)*, Oct. 2016, pp. 217–222.

[55] R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," in *Proc. 11th Int. Conf. Telecommun. Syst. Services Appl.*, 2017, pp. 1–6.

[56] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Bitcoin, El Salvador, White Paper 21260, 2008.

[57] V. L. Lemieux, "A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017.

[58] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: A review," *IEEE Access*, vol. 6, pp. 10179–10188, 2018.

[59] A. Kaushik, A. Choudhary, C. Ektare, D. Thomas, and S. Akram, "Blockchain—Literature survey," in *Proc. 2nd IEEE Int. Conf. Recent Trends Electron., Inf. Commun. Technol. (RTEICT)*, May 2017, pp. 2145–2148.

[60] A. Banerjee and K. P. Joshi, "Link before you share: Managing privacy policies through blockchain," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017, pp. 4438–4447.

[61] M. Turkanovic, M. Holbl, K. Kosic, M. Hericko, and A. Kamisalic, "EduCTX: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018.

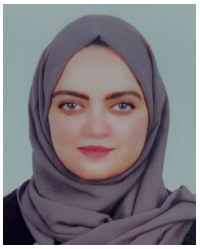
[62] Y. Desmedt and E. Miami, "Public cryptography," in *Proc. 6th Int. Workshop Pract. Theory Public Key Cryptogr.*, 2003, pp. 1–266.

[63] *Secure Hash Standard (SHS), Federal Information Processing Standards Publication*, NIST, Gaithersburg, MD, USA, 2012, vol. 37.

[64] M. D. Sleiman, A. P. Lauf, and R. Yampolskiy, "Bitcoin message: Data insertion on a proof-of-work cryptocurrency system," in *Proc. Int. Conf. Cyberworlds (CW)*, Oct. 2015, pp. 332–336.

[65] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, "OmniPHR: A distributed architecture model to integrate personal health records," *J. Biomed. Inform.*, vol. 71, pp. 70–81, Jul. 2017.
[66] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: A review," *IEEE Access*, vol. 6, pp. 10179–10188, 2018.
[67] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[68] *Eris Industries Documentation-Blockchains*, Accessed: Mar. 15, 2016. [Online]. Available: https://erisindustries.com/docs_subdomain/explainers/blockchains.html
[69] E. Ben Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, Berkeley, CA, USA, May 2014, pp. 459–474.
[70] D. Wood, "Ethereum: A secure decentralised generalised transaction ledger," EIP-150 Revision, Ethereum Project Yellow Paper, 2014, pp. 1–32, vol. 151.
[71] 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, Jan. 2017.
[72] *MultiChain-Open Source Private Blockchain Platform*. Accessed: Mar. 15, 2016. [Online]. Available: https://www.multichain.com/
[73] A. G. Goiri and D. L. de Ipina, "On the complentarity of triple spaces and the web of things," in *Proc. 2nd Int. Workshop Web Things*, New York, NY, USA, 2011, pp. 1–6.
[74] H. Ning and H. Liu, "Cyber-physical-social based security architecture for future Internet of Things," *Adv. Internet Things*, vol. 2, no. 1, pp. 1–7, 2012.
[75] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2016, pp. 467–468.
[76] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2016, pp. 2663–2668.
[77] M. Vukolic, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proc. Int. Workshop Open Problems Netw. Secur.*, 2015, pp. 112–125.
[78] Z. Zheng, S. Xie, H. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2016.
[79] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without proof of work," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, vol. 9604, 2016, pp. 142–157.
[80] M. Borge, E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, and B. Ford, "Proof-of-personhood: Redemocratizing permissionless cryptocurrencies," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS PW)*, Paris, France, Apr. 2017, pp. 23–26.
[81] A. Kiayas, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Proc. Conf.*, vol. 10401, 2017, pp. 357–388.
[82] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.
[83] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, Jul. 1982.
[84] *Hyperledger Project*, Linux Found., USA, 2015.
[85] D. Mazieres, "The stellar consensus protocol: A federated Model for internet-level Consensus," Stellar Develop. Found., San Francisco, CA, USA, Tech. Rep. 32, 2015.
[86] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," Ripple, U.K., White Paper, 2014, p. 151, vol. 5, no. 8.
[87] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Jan. 2017, pp. 1–5.
[88] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba, "A taxonomy of blockchain-based systems for architectire design," in *Proc. IEEE Int. Conf. ICSA*, 2017, pp. 243–252.
[89] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, Apr. 2020.
[90] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.
[91] M. Wohrer and U. Zdun, "Smart contracts: Security patterns in the ethereum ecosystem and solidity," in *Proc. Int. Workshop Blockchain Oriented Softw. Eng. (IWBOSE)*, Mar. 2018, pp. 2–8.
[92] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers*, vol. 310, no. 4, 2016.
[93] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.
[94] J. A. T. Casallas, J. M. Cueva-Lovelle, and J. I. R. Molano, "Smart contracts with blockchain in the public sector," *Int. J. Interact. Multimedia Artif. Intell.*, vol. 6, no. 3, p. 63, 2020.
[95] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized BlockChain for IoT," in *Proc. 2nd Int. Conf. Internet Things Design Implement.*, Apr. 2017, pp. 173–178.
[96] P. Helo and Y. Hao, "Blockchains in operations and supply chains: A model and reference implementation," *Comput. Ind. Eng.*, vol. 136, pp. 242–251, Oct. 2019.
[97] F. Longo, L. Nicoletti, A. Padovano, G. d'Atri, and M. Forte, "Blockchain-enabled supply chain: An experimental study," *Comput. Ind. Eng.*, vol. 136, pp. 57–69, Oct. 2019.
[98] M. M. Alshaikhli, "IOTA viability in healthcare industry," M.S. thesis, Dept. Comput. Eng., Qatar Univ., Doha, Qatar, 2019.
[99] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2016, pp. 1–6.
[100] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, and S. Chen, "The blockchain as a software connector," in *Proc. 13th Work. IEEE/IFIP Conf. Softw. Archit. (WICSA)*, Apr. 2016, pp. 182–191.
[101] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—A systematic review," *PLoS ONE*, vol. 11, no. 10, Oct. 2016, Art. no. e0163477.
[102] G. Zyskind and O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, May 2015, pp. 180–184.
[103] V. Buterin, "Ethereum white paper," Ethereum, USA, Ethereum White Paper 1, 2009, pp. 22–23.
[104] P. Noizat, "Blockchain electronic vote," in *Handbook of Digital Currency*. New York, NY, USA: Academic, 2015, ch. 22, pp. 453–461.
[105] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep. 2016.
[106] H. C. Pohls, V. Angelakis, S. Suppan, K. Fischer, G. Oikonomou, E. Z. Tragos, R. Diaz Rodriguez, and T. Mouroutis, "RERUM: Building a reliable IoT upon privacy- and security-enabled smart objects," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Apr. 2014, pp. 122–127.
[107] S. Feld, M. Schönfeld, and M. Werner, "Analyzing the deployment of bitcoin's P2P network under an as-level perspective," *Proc. Comput. Sci.*, vol. 32, pp. 1121–1126, Jan. 2014.
[108] G. Karame, "On the security and scalability of bitcoin's blockchain," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 1861–1862.
[109] S. Ammous, "Blockchain technology: What is it good for?" Lebanese American Univ., Beirut, Lebanon, Tech. Rep. SSRN 2832751, 2016.
[110] Q. K. Nguyen, "Blockchain—A financial technology for future sustainable development," in *Proc. 3rd Int. Conf. Green Technol. Sustain. Develop. (GTSD)*, Nov. 2016, pp. 51–54.
[111] G. Gabison, "Policy considerations for the blockchain technology public and private applications," *SMU Sci. Technol. Law Rev.*, vol. 19, p. 327, 2016.
[112] A. Gaggioli, "Blockchain technology: Living in a decentralized everything," *Cyberpsychol., Behav., Social Netw.*, vol. 21, no. 1, pp. 65–66, Jan. 2018.
[113] S. Popov. (2016). *The Tangle*. [Online]. Available: https://iota.org/IOTA Whitepaper.pdf
[114] S. Popov, O. Saa, and P. Finardi, "Equilibria in the Tangle," UNICAMO, Campinas, Brazil, Tech. Rep. 136, 2017, pp. 160–172.
[115] L. Tennant, "Improving the anonymity of the IOTA cryptocurrency," 2017.
[116] B. Ferrarini, J. A. Maupin, and M. Hinojales, "Distributed ledger technologies for developing Asia," ADBI Work. Paper 533, Dec. 2017. [Online]. Available: https://ssrn.com/abstract=3187964
[117] M. Paul, R. Amr, and S. Ralf, "BlockChain a new foundation for building trustworthy and secure distributed applications (DAPP's) of the future, ICSY - Integrated Communication Systems," Tech. Rep., 2017. Accessed: Dec. 12, 2018. [Online]. Available: http://dspace.icsy.de:12000/dspace/handle/123456789/432

[118] R. Mohammad, "Universal Digital Dollar," uddcoin.com, 2018.
[119] V. Red, "Practical comparison of distributed ledger technologies for IoT," in *Proc. SPIE, Disruptive Technol. Sensors Sensor Syst.*, 2017, Art. no. 102060G.
[120] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, "Decentralized consensus for edge-centric Internet of Things: A review, taxonomy, and research issues," *IEEE Access*, vol. 6, pp. 1513–1524, 2018.
[121] B. Kusmierz, "The first glance at the simulation of the Tangle: Discrete model," IOTA Found., Berlin, Germany, Tech. Rep., 2017.
[122] F. Wang and D. P. Landau, "Efficient, multiple-range random walk algorithm to calculate the density of states," *Phys. Rev. Lett.*, vol. 86, no. 10, pp. 2050–2053, Mar. 2001.
[123] C. Robert, "Monte Carlo methods," in *Wiley StatsRef: Statistics Refernce Online Book*. Springer, 2016.
[124] C. Cachin and M. Vukolic, "Blockchain consensus protocols in the wild," in *Proc. 31st Int. Symp. Distrib. Comput. (DISC)*, Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, Jul. 2017.
[125] J. Maupin, "Mapping the global legal landscape of blockchain and other distributed ledger technologies," *Centre Int. Governance Innov.*, no. 149, Jul. 2017.
[126] J. Buchmann, E. Dahmen, S. Ereth, A. Hulsing, and M. Ruckert, "On the security of the winternitz one-time signature scheme," Technosche Universität Damstadt, Darmstadt, Germany, Tech. Rep., 2011, pp. 363–378.
[127] *Hash Based Signatures*, ImperialViolet, Los Angeles, CA, USA, 2013.
[128] M. Atzori, "Blockchain-based architectures for the Internet of Things: A survey," Tech. Rep., 2016.
[129] J. P. Buntix, "IOTA: Internet of Things without the blockchain?" Tech. Rep., 2014. Accessed: Nov. 14, 2016. [Online]. Available: http://bitcoinist.net/iota-internet-things-without-blockchain/
[130] S. Guald, F. Ancoina, and R. Stadler, "An arbitrary scalable, energy efficient and anonymoud transaction network based on colored tangles," in *Proc. CryptoGuru PoC SIG*, 2017.
[131] B. Martin, F. Michaud, D. Banks, and A. Mosenia, "OpenFog security requirements and approaches," in *Proc. IEEE Fog World Congr. (FWC)*, 2017, pp. 1–6.
[132] D. Sonstebo, "IOTA development roadmap," Tech. Rep., 2017. [Online]. Available: https://blog.iota.org/iota-development-roadmap74741f37ed01
[133] N. Buchmann, C. Rathgeb, H. Baier, C. Busch, and M. Margraf, "Enhancing breeder document long-term security using blockchain technology," in *Proc. IEEE 41st Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2017.
[134] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, A. Bicaku, and J. Bastos, "A lightweight authentication mechanism for M2M communications in industrial IoT environment," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 288–296, Feb. 2019.
[135] M. M. Alshaikhli, "IOTA viability in healthcare industry," M.S. thesis, Dept. Comput. Eng., Qatar Univ., Doha, Qatar, 2019.
[136] P. C. Bartolomeu, E. Vieira, and J. Ferreira, "IOTA feasibility and perspectives for enabling vehicular applications," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–7.
[137] B. Shabandri and P. Maheshwari, "Enhancing IoT security and privacy using distributed ledgers with IOTA and the Tangle," in *Proc. 6th Int. Conf. Signal Process. Integr. Netw. (SPIN)*, Mar. 2019, pp. 1069–1075.
[138] T. Alsboui, Y. Qin, and R. Hill, "Enabling distributed intelligence in the Internet of Things using the IOTA Tangle architecture," in *Proc. 4th Int. Conf. Internet Things, Big Data Secur.*, 2019, pp. 392–398.
[139] B. Andriamanalimanana, C.-F. Chiang, J. Novillo, S. Sengupta, and A. Tekeoglu, "Tango: The beginning—A semi-synchronous Iota-tangle type distributed ledger with periodic pulsed entries," in *Proc. 2nd Cyber Secur. Netw. Conf. (CSNet)*, Oct. 2018, pp. 1–3.
[140] S. K. Pinjala and K. M. Sivalingam, "DCACI: A decentralized lightweight capability based access control framework using IOTA for Internet of Things," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, Apr. 2019, pp. 13–18.
[141] A. Tekeoglu and N. Ahmed, "TangoChain: A lightweight distributed ledger for Internet of Things devices in smart cities," in *Proc. IEEE Int. Smart Cities Conf. (ISC)*, Oct. 2019, pp. 18–21.
[142] D. Hawig, C. Zhou, S. Fuhrhop, A. S. Fialho, and N. Ramachandran, "Designing a distributed ledger technology system for interoperable and general data protection regulation–compliant health data exchange: A use case in blood glucose data," *J. Med. Internet Res.*, vol. 21, no. 6, Jun. 2019, Art. no. e13665.
[143] M. Bhandary, M. Parmar, and D. Ambawade, "Securing logs of a system—An IoTA Tangle use case," in *Proc. Int. Conf. Electron. Sustain. Commun. Syst. (ICESC)*, Jul. 2020, pp. 697–702.
[144] W. F. Silvano, D. De Michele, D. Trauth, and R. Marcelino, "IoT sensors integrated with the distributed protocol IOTA/Tangle: Bosch XDK110 use case," in *Proc. 10th Brazilian Symp. Comput. Syst. Eng. (SBESC)*, Nov. 2020, pp. 1–8.
[145] A. Raschendorfer, B. Mörzinger, E. Steinberger, P. Pelzmann, R. Oswald, M. Stadler, and F. Bleicher, "On IOTA as a potential enabler for an M2M economy in manufacturing," in *Proc. CIRP*, vol. 79, 2019, pp. 379–384.
[146] M. Zander, T. Waite, and D. Harz, "DAGsim: Simulation of DAG-based distributed ledger protocols," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 46, no. 3, pp. 118–121, Jan. 2019.
[147] S. Park, S. Oh, and H. Kim, "Performance analysis of DAG-based cryptocurrency," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2019, pp. 1–6.
[148] M. Bottone, F. Raimondi, and G. Primiero, "Multi-agent based simulations of block-free distributed ledgers," in *Proc. 32nd Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, May 2018, pp. 585–590.
[149] B. Kusmierz, W. Sanders, A. Penzkofer, A. Capossele, and A. Gal, "Properties of the Tangle for uniform random and random walk tip selection," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 228–236.
[150] C. Faria and M. Correia, "BlockSim: Blockchain simulator," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 439–446.
[151] M. Alharby and A. van Moorsel, "BlockSim: An extensible simulation tool for blockchain systems," *Frontiers Blockchain*, vol. 3, Jun. 2020.
[152] S. Pandey, G. Ojha, B. Shrestha, and R. Kumar, "BlockSIM: A practical simulation tool for optimal network design, stability and planning," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 133–137.



MAYS ALSHAIKHLI received the B.Sc. degree in computer science from Yarmouk University and the M.Sc. degree (Hons.) in computing from Qatar University, in 2012 and 2019, respectively, where she is currently pursuing the Ph.D. degree with the Computer Engineering Department. Her research interests include distributed systems, IOTA, blockchain, the IoT, and deep learning.

TAREK ELFOULY received the M.Sc. and Ph.D. degrees from BESANÇON University (FRANCHE-COMTÉ), in 1996 and 2000, respectively. He is currently an Associate Professor with Tennessee Technological University. He has over 16 years of experience in wireless sensor networks and computer network research. He published over 80 papers, most of them are related to wireless sensing and network security. He also has three U.S. awarded patents. He has managed to secure more than three million dollars of funds for his research in collaboration with many universities in USA, Canada, and Europe, such as Ohio State University, the New Jersey Institute of Technology, the University of British Columbia, and the Imperial College of London. He worked on topics related to network security and physical layer security. He has also worked on applications of wireless sensor networks, especially in the field of structural health monitoring and health applications. His team had implemented a sensor node that can harvest energy from vibrations while installed on infrastructures, such as bridges with an easy installation process on old infrastructures. He has a few projects under development related to machine learning and E-health. His projects won many national and regional awards in Qatar. He supervised many post graduate students and served as an examiner for many others. Beside his research, he has 20 years of teaching experience. He has taught courses in hardware, programming and networks. He has supervised more than 20 senior projects and six Theses. He served as a CE Program Coordinator at Qatar University. He is a Senior Member of the IEEE Society.

OMAR ELHARROUSS (Member, IEEE) received the master's degree from the Faculty of Sciences, Dhar El Mehraz, Fez, Morocco, in 2013, and the Ph.D. degree from the LIIAN Laboratory, USMBA-Fez University, in 2017. His research interests include artificial intelligence, pattern recognition, image processing, and computer vision. He worked on two project funded by QNRF. He currently holds a postdoctoral at Qatar University funded by Supreme Committee of delivery and legacy. He is involved in multitude of projects related to computer vision and image processing, and has published in well reputed journals.

AMR MOHAMED (Senior Member, IEEE) received the M.S. and Ph.D. degrees in electrical and computer engineering from The University of British Columbia, Vancouver, Canada, in 2001 and 2006, respectively. He has worked as an Advisory IT Specialist with the IBM Innovation Centre, Vancouver, from 1998 to 2007, taking a leadership role in systems development for vertical industries. He is currently a Professor with the College of Engineering, Qatar University. He has over 25 years of experience in IoT, edge computing, pervasive AI, and wireless networking research and industrial systems development. He holds three awards from IBM Canada for his achievements and leadership, and four best paper awards from IEEE conferences. His research interests include wireless networking, and edge computing for IoT applications. He has authored or coauthored over 200 refereed journal and conference papers, textbooks, and book chapters in reputable international journals, and conferences. He is serving as a Technical Editor for three international journals, has served as a guest editor in several special issues, and has served as a technical program committee (TPC) and the co-chair for many IEEE conferences and workshops.

NAJMATH OTTAKATH received the Bachelor of Technology degree in the field of electronics and communication engineering from the University of Calicut. She is currently pursuing the Master of Science degree in computing with Qatar University. She is also a Research Assistant for projects related to computer vision and image processing at Qatar University.