electronics

MDPI

Article

Identity and Access Management Resilience against Intentional Risk for Blockchain-Based IOT Platforms

Alberto Partida [1,*,†], Regino Criado [2,†] and Miguel Romance [2,†]

[1] Department of Applied Mathematics, International Doctoral School, Rey Juan Carlos University, 28933 Móstoles, Madrid, Spain
[2] Department of Applied Mathematics, Rey Juan Carlos University, 28933 Móstoles, Madrid, Spain; regino.criado@urjc.es (R.C.); miguel.romance@urjc.es (M.R.)
* Correspondence: a.partidar@alumnos.urjc.es
† These authors contributed equally to this work.

Abstract: Some Internet of Things (IoT) platforms use blockchain to transport data. The value proposition of IoT is the connection to the Internet of a myriad of devices that provide and exchange data to improve people's lives and add value to industries. The blockchain technology transfers data and value in an immutable and decentralised fashion. Security, composed of both non-intentional and intentional risk management, is a fundamental design requirement for both IoT and blockchain. We study how blockchain answers some of the IoT security requirements with a focus on intentional risk. The review of a sample of security incidents impacting public blockchains confirm that identity and access management (IAM) is a key security requirement to build resilience against intentional risk. This fact is also applicable to IoT solutions built on a blockchain. We compare the two IoT platforms based on public permissionless distributed ledgers with the highest market capitalisation: IOTA, run on an alternative to a blockchain, which is a directed acyclic graph (DAG); and IoTeX, its contender, built on a blockchain. Our objective is to discover how we can create IAM resilience against intentional risk in these IoT platforms. For that, we turn to complex network theory: a tool to describe and compare systems with many participants. We conclude that IoTeX and possibly IOTA transaction networks are scale-free. As both platforms are vulnerable to attacks, they require resilience against intentional risk. In the case of IoTeX, DIoTA provides a resilient IAM solution. Furthermore, we suggest that resilience against intentional risk requires an IAM concept that transcends a single blockchain. Only with the interplay of edge and global ledgers can we obtain data integrity in a multi-vendor and multi-purpose IoT network.

Keywords: IoT; blockchain; decentralised ledger; complex networks; identity and access management; data authentication; data integrity; intentional risk

Citation: Partida, A.; Criado, R.; Romance, M. Identity and Access Management Resilience against Intentional Risk for Blockchain-Based IOT Platforms. *Electronics* **2021**, *10*, 378. https://doi.org/10.3390/electronics10040378

Academic Editor: Davide Brunelli
Received: 31 December 2020
Accepted: 26 January 2021
Published: 4 February 2021

1. Introduction

1.1. Internet of Things

Since the last years of the past 20th century, the Internet has contributed greatly to the connection between human beings. In October 2020, 59% of the world's population was active on the Internet, i.e., 4.66 billion people. Ninety-one percent of those Internet users do it via mobile devices [1]. The former US Vice-President Al Gore referred to the Internet as the information superhighway.

Connecting things with other things and servers via the Internet is the next big step taking place in these first decades of the 21st century. The Internet of Things (IoT) enables the connection to the Internet of a multitude of small electronic devices to facilitate their use, handling, data exchange and management. By the end of 2018, the number of IoT-connected devices surpassed the 20 billion mark [2] with a forecast of 30 billion IoT-connected devices for 2030 [3]. This information superhighway is now being extended with many additional lanes that carry information from, among many other things, sensors,

actuators, personal health devices and geolocation trackers. Reference [4] defines an IoT device as one having at least one transducer (sensor or actuator) to interact directly with the physical world and at least one network interface (Ethernet, Wi-Fi, Bluetooth) to interface with the digital world.

1.2. Blockchain Can Contribute to a Secure IoT World

Some IoT projects use a blockchain to transport data. We study how blockchain can add security to the IoT world. A blockchain is a type of distributed ledger. The blockchain technology can answer a considerable subset of the cybersecurity requirements for IoT mentioned by ETSI [5] and NIST [6] (see Section 2.1), i.e., integrity, secure communication and resilience. Simultaneously, a blockchain could add additional security properties such as availability and accessibility together with a reliable micropayment functionality. Given the large number of things connected via the Internet, the blockchain implementation that could fit the needs of the IoT would need to have no or very low transaction fees, real growth possibilities and a scalable identity management process. Blockchain technology transfers data and value in an immutable and decentralised fashion. These two properties are valuable for implementing resilient IoT platforms. However, blockchain does not answer all IoT security requirements: confidentiality and protection of personal data would require encryption on top of the blockchain.

1.3. Complex Networks Analysis: A Useful Tool to Feature Systems

The analysis of systems with many participant nodes via complex networks can provide useful information to better understand the system and draw useful conclusions. Newman (2009) ([7] p. 2) defines a network (also named a graph) as a set of vertices (or nodes) and connections (or edges) between them. The complexity comes when the number of elements in the network is high and the use of advanced mathematical and statistical tools enters into play [8–10]. The value of this multidisciplinary field comes from the possibility to describe complex interactions [11], some of them dynamic ([12] p. 177), happening in the real world (social networks, disease spreading, traffic control, etc.) with models based on complex networks ([13] p. 179). We study two blockchain-based IoT networks with complex network theory. This complex network analysis provides us with their network profiles.

1.4. Intentional Risk Management Via Complex Networks Analysis

Intentional risk management is one of the two effective pillars in cybersecurity according to Chapela et al. (2016) ([11] pp. 2–3). The other pillar is non-intentional (traditional, mostly accidental) risk management. Non-intentional risk has already been the subject of thorough study ([14] pp. 27–36). Typically, risk management methodologies were focused on non-intentional risks and were based on an actuarial approach, using the well-known equation *risk = probability x impact*. The probability is based on observation of the frequency of past events.

Intentional risks are effected by an active agent—a threat agent ([15] p. 2) that is looking for a specific profit ([11] p. 2) while running a limited risk. Chapela et al. (2016) ([11] p. 11) stated that complex-network-based intentional risk management can be applied to any information system if it can be modelled as a complex network, especially when the relations among their nodes are not linear ([11] p. 11). Once we obtain the network profiles of the two IoT platforms we study, we apply the equations proposed by [11] to increase their resilience against intentional risk.

1.4.1. Intentional Risk Management in IoT

The deployment of IoT devices is taking off exponentially: logistics, health, leisure, mobility and supply chains are just a few use cases where the exchange of sensor and actuator data brings value to society. This value can only materialise long term with a sufficient degree of data security in IoT. Simultaneously, blockchain technology is continuously

improving and it can be an appropriate platform to provide data integrity, immutability and scalability to IoT implementations. The high number of IoT devices and related information technology (IT) elements (e.g., edge and cloud servers) compose a complex system subject to be studied as a complex network, where the nodes are IoT devices and other IT elements and the edges the communications between them. This complex-network-based characterisation contributes to explaining the resilience of different IoT implementations against intentional risk and possible improvement paths.

1.4.2. Structure of the Paper

This paper is structured as follows. We first present the current developments on security requirements for IoT devices. Second, we describe how blockchain can answer some of those IoT security requirements. Third, we explain IOTA (a distributed ledger-based IoT implementation) with its present and future design decisions together with its main known security incidents. Fourth, we introduce IoTeX (a blockchain based IoT solution) and a collection of security incidents in public blockchains. Fifth, we link identity and access management (IAM) in IoT with edge and cloud computing and we analyse a data authenticity protection framework for IoT systems. Sixth, we highlight how complex network analysis can contribute to intentional risk management; and finally, we complete this paper with empirical results based on complex network analysis and provide conclusions on how to improve IAM resilience against intentional risk in IoT platforms.

2. Related Works

2.1. Security Requirements for IoT

The communication of data to and from a digital gadget via the public Internet facilitates remote management and real-time data transfer, both frequent user requirements in many use cases within different industries. One of the challenges for IoT is how to satisfy these requirements in a secure manner. The global standards development organisation ETSI has released a security baseline for Internet-connected consumer products [5] that provides a basis for future IoT certification schemes [16]. A large number of IoT devices do not display a minimum set of security features, endangering consumers' privacy and rendering these connected products as a formidable platform from where to launch massive distributed denial of services attacks, like the Mirai botnet already in 2016 [17]. Table 1 summarises the key requirements of this baseline.

Table 1. ETSI technical specifications. Cybersecurity for consumer IoT.

Provision	Key Topic
1	No universal default passwords
2	Report vulnerabilities
3	Keep software updated
4	Securely store credentials and security-sensitive data
5	Communicate securely
6	Minimised exposed attack surfaces
7	Ensure software integrity
8	Protect personal data
9	Make systems resilient to outages
10	Examine system telemetry data
11	Make deletion of personal data easy
12	Facilitate installation and maintenance
13	Validate input data

The National Institute of Standards and Technology from the U.S. Department of Commerce (NIST) acknowledges the evolution of IoT technology and its integration into US federal information systems [18], and the requirement to add security at the device-level

to cope with the increasing scale, heterogeneity and pace of IoT deployment [18]. NIST proposed a list of device cybersecurity capabilities [6]. See Table 2.

Table 2. Device cybersecurity capabilities. NIST-IR 8259D.

Capability	Key Abilities
Device identity	Unique physical and digital device identifier
Device configuration	Display and device configuration control
Data protection	Cryptographic capabilities and secure storage
Logical access to interfaces	Authentication, authentication, use and interface control
Software update	Possibility to update code
Cybersecurity state awareness	Event logging and monitoring, audit trail protection
Device security	Secure operation and communication

In addition to the technical capabilities, NIST [6] also proposed non-technical supporting capabilities for IoT. See Table 3.

Table 3. Non-technical supporting capabilities for IoT providers. NIST-IR 8259D.

Capability	Key Abilities
Documentation	Device acquisition and maintenance description during device lifetime
Information and query reception	Cybersecurity reports and queries
Information dissemination	Software maintenance and cybersecurity alerts
Education and awareness	Device and cybersecurity awareness

2.2. Blockchain. The Internet of Value Applied to IoT

When something is highly valuable it needs to be wholeheartedly protected. An ancient strategy is to distribute it, as we infer from [11]. The Internet was born in the 1960s out of the United States Department of Defence with the aim of avoiding centralised governance. This innate approach was embraced by the cyberpunk community in the early Internet days. The absence of a centralised entity that would orchestrate the governance of the network was also highly appreciated by this pioneer community as being close to their egalitarian and libertarian identity. Blockchain in essence is a distributed system as well. The interplay of many nodes, each with a trustworthy copy of the database, makes it a distributed system ([19] part 1). Sharing transactions of data and value in a common distributed database (a common ledger in a blockchain), agreed by consensus (i.e., "the longest block wins") and replicated multiple times across participating nodes without a central governance element acting as a trust provider is an attractive concept with many potential use cases. Public blockchains constitute the Internet of value. Bitcoin [20] and Ethereum [21] are by far the two most popular public permissionless blockchain implementations in terms of market capitalisation [22].

Proposed IoT implementations based on Ethereum using smart contracts yet present some challenges: incurred costs [23,24] and transaction confirmation delays [23] are still obstacles for their industry-wide implementation. Currently, the number of transactions per second (tps) that public permissionless blockchain implementations cope with cannot compete with traditional centralised payment solutions. Transaction figures are controversial and highly dependant on the source: [25] mentions that Visa averaged 5000 transactions per second during 2H2018. Bitcoin executes on average 3 to 4 tps with pikes of 7 tps [26]. Ethereum copes with an average of 12 tps [27]. On *blocktivity.info*, EOS, a public permissionless blockchain that aspires to compete with Ethereum, leads the tps ranking with over 61 million operations (equivalent to over 36 tps) [28]. The EOS web site itself has even reported a new record of 9656 tps in its jungle testnet [29]. Regardless of the precise figures, it is a fact that the current centralised payment systems process numbers of transactions that are two orders of magnitude higher (see Table 4). In addition to the number of transac-

tions, both Bitcoin and Ethereum carry fees per transaction, which renders their use for IoT devices questionable, as a high number of communications per device would increase operational costs considerably.

Table 4. Typical transactions per second (tps).

Processor	Architecture	Tps
Visa	Centralised	5000
Bitcoin	Distributed	3 to 4, pikes of 7
Ethereum	Distributed	12 on average
IOTA	Distributed	below 10
IoTeX	Distributed	f(chain)
EOS	Distributed	36

We select the two most capitalised IOT related blockchain implementations: IOTA and IoTeX. See Figure 1. We use market capitalisation as a proxy for potential user adoption and future growth. In January 2021, the market capitalisation of MIOTA, IOTA's coin, surpassed USD 1.3 B with a 24 h trading volume of USD 179 M, and the market value of IOTX, IoTeX's coin, reached USD 81 M with a 24 h trading volume of USD 4.5 M [22,30]. In December 2020, MIOTA had a market capitalisation of USD 800 M with a 24 h trading volume of USD 34 M, and the market value of IOTX reached USD 37 M with a 24 h trading volume of USD 6 M. The gap in both capitalisation and daily trading volume between both IoT coins is considerable but they rank in position 1 and 2 considering these two parameters as the ranking criteria.

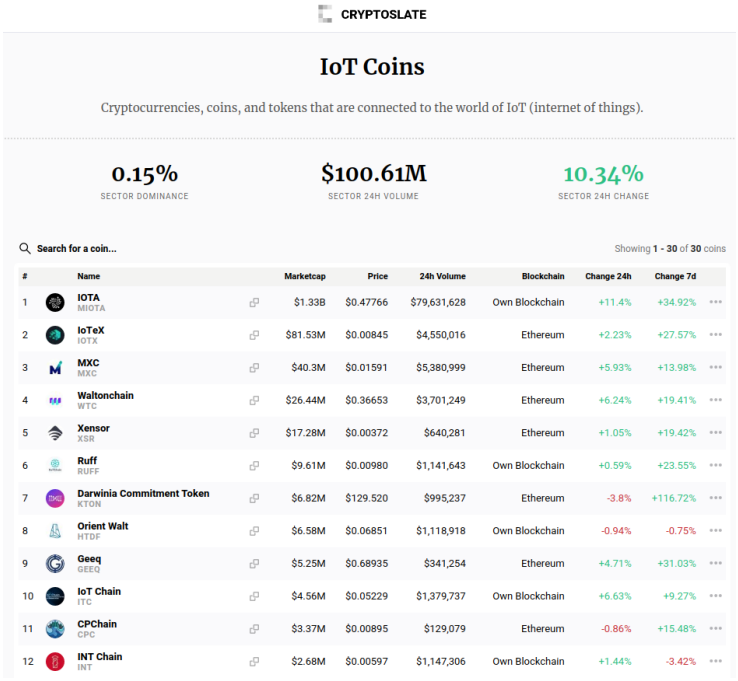


Figure 1. Market capitalisation of IoT coins on 18 January 2021.

2.3. IOTA

IOTA was created in 2015 by David Sønstebø, Dominik Schiener, Sergey Ivancheglo and Serguei Popov. It is a public, permissionless, open-source distributed ledger with no transaction fees that exchanges value between humans and machines [31]. There are no blocks nor miners, and the creators claim that it requires very low resources. It uses a directed acyclic graph (DAG) instead of a blockchain. Every participant needs to validate two other transactions when they send an IOTA transaction. Nodes in IOTA use the balance model, in contrast with the unspent transaction output (UTXO); i.e., the balance of a user is

simply a list of unspent transactions in different addresses. The balance model, i.e., keeping track of the account balance as a unique global state, is simpler and more efficient but prone to double-spending attacks [32]. The average number of transactions per second is below 10 tps most of the time [33]. There are around 291 active public IOTA nodes [34], many of them in servers located in Germany.

2.3.1. IOTA DAG. The Tangle

IOTA designers decided not to use a chain of blocks to guarantee scalability but a directed acyclic graph (DAG) called the tangle, allowing for a theoretically infinite throughput as the network grows. Every participant that issues a transaction needs to approve two previous transactions (a trunk transaction and a branch transaction, as depicted in Figure 2), thereby contributing to the integrity of the tangle. A bundle is a collection of transactions validated simultaneously. A typical transfer in IOTA is a bundle consisting of four transactions. The genesis transaction consists of an address containing all the tokens existing in IOTA and sending them to other founder addresses [35]. Most of the attacks on the tangle foreseen in its white paper [35] are related to identity; e.g., an attacker could have a myriad of Sybil identities. In a Sybil attack, the attacker tries to subvert a reputation system creating multiple identities [36]. To prevent that, reference [35] suggests using statistical Markov chain Monte Carlo (MCMC) algorithms for the nodes to create "random walks" through non-confirmed transactions (called "tips") and to provide weights to each of those tips. These weights are related to the numbers of direct and indirect approvers a transaction has. The preference for using MCMC compared to uniform random tip selection (URTS) has been confirmed in a computer simulation of the tangle [37].

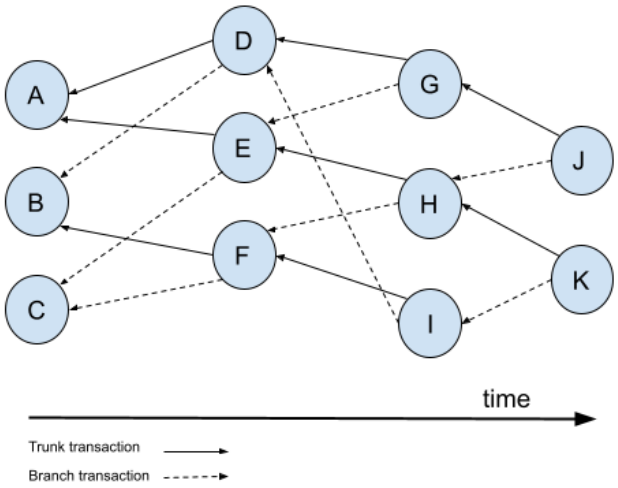


Figure 2. Ideal IOTA tangle representation.

2.3.2. The Coordinator of the Tangle

The theoretical mathematical foundation laid in [35] has a lot of potential in a sufficiently meshed and sized network; however, the tangle still makes use of a "bootstrapping" security measure to avoid attacks: a confirmed transaction needs to be referenced, directly or indirectly, by a signed transaction issued by a unique node: the coordinator (Coo). Those signed transactions are called milestones. This Coo constitutes an element of centralisation [38] that allows IOTA to create a consensus on accepting transactions. The IOTA design team confirmed that this is a temporary measure. Since its inception, IOTA has embarked on a continuous algorithm and protocol improvement effort [39–41]. They are working on eliminating the figure of the coordinator in a project called "Coordicide."

2.3.3. The Coordicide Preparing IOTA Consolidation

This complex project consists of technical workstreams [38], most of them rotating around the concept of identity management:

1. Global node identities: Using off-tangle non-post-quantum public key cryptography to identify nodes. Every node would then add its public key to every signed message.
2. Sybil attack protection via a reputation system: Providing a reputation value (called *mana*) to every node, equivalent to the total number of funds transferred by that node. This is a specific kind of proof of ownership. They distinguish between *pending mana* (based on the tokens the node holds) and *mana* (spent tokens by that node in its transactions). Both *pending mana* and *mana* decay at a rate proportional to the stake they hold.
3. Autopeering: Nodes in IOTA keep a copy of the ledger state, i.e., the tangle. Nodes share information on transactions with the neighbour nodes. This is called peering. This process is currently done manually by the node operator, and hence, could be subject to an ill-intentioned actor controlling all peering neighbours of a node. This is called the eclipse attack. IOTA designers propose the use of public-key-based cryptography to automate this node information exchange process (called autopeering). In order to do that, a regular transfer of nodes' public keys will be required.
4. Rate control: Many blockchain implementations, Bitcoin and Ethereum included, use proof of work. Proof of work is a consensus mechanism that act as a built-in network congestion limitation mechanism and deters attacks to a network by requiring the execution of a computationally demanding process for a network participant to get the service it requests confirmed. In the case of blockchains, the service is mainly transaction confirmation. A proof of work consensus mechanism favours the blockchain that has taken the most energy to be built (chainwork), in other words, "the longest chain wins." This is measured by the number of hashes required to produce the current chain [42]. For a blockchain to be trustful, honest participants in the network need to control the majority of the network's hashing power. The challenge of proof of work in IOTA is the limited computing capacity of most of their participants since IOTA positions itself as the distributed ledger for IoT devices. IOTA designers of Coordicide are studying adaptive (to the computing power of the device) proof of work (POW) algorithms.
5. Decoupling of conflict resolution and transaction validation: These are the two hardest actions to solve. Regarding the consensus mechanism, the Coordicide proposes the use of a *mana*-based fast probabilistic consensus (FPC) [39–41] or "cellular automata" (CA, also known as majority dynamics). On tip selection, the initial biased random walk used to select transactions to validate transforms into an "almost" uniformly random tip selection among non-lazy, i.e., active nodes.

2.3.4. The Path to Coordicide

This architectural re-design is complex and requires changes in the node software, the wallets, the infrastructure and most libraries. The IOTA design team planned a transitional step to drive IOTA 1.0 (with a coordinator) to the new IOTA 2.0 (with no coordinator): IOTA 1.5 (also known as Chrysalis). One of the changes included in Chrysalis is the formal introduction of reusable addresses, facilitating the integration into new exchanges, wallets and payments [43].

2.3.5. Reuse or Not of Addresses

The initial architectural decision of IOTA designers to build the tangle quantum computing proof required the use of post-quantum computing encryption to sign transactions [44]. This meant that the use of the same paying address was not secure anymore, so the remainder needs to be sent to a new address of the payee. IOTA designers advise users not to spend from the same address more than once [45]. Chrysalis includes the logical detachment of the address from the public key used to sign the transaction. It also enables the change of the public key linked to an address for every purchase. Consequently, IOTA will be in a position to offer reusable addresses to their users [46]. Having reusable addresses facilitates the implementation of a more robust identity management concept.

2.3.6. IOTA Use Cases

There are currently initiatives to use IOTA in seven sectors: mobility and automotive, global trade and supply chains, industrial IoT, ehealth, smart cities, customs and border management and digital identity [47]. Companies such as Bosch and Jaguar Land Rover have piloted projects using IOTA. Transaction confirmation delays in the IOTA production network are still challenging [48]. Most transactions take around 10 min, and 5% of transactions experience longer confirmation times ([48] p. 1). This is one of the reasons why the IOTA project has come up with a very ambitious improvement roadmap [38].

2.4. Security Incidents in IOTA

In January 2018 IOTA users lost close to USD 4 million via an attack that blended social engineering with a design possibility related to identity management. The identity of any user in a blockchain is generated via a private–public key pair. This key pair resides in a cryptocurrency wallet. To facilitate the creation and recovery of the private key, since the arrival of Bitcoin and Ethereum, it is common to use a seed to create the master private key of the cryptowallet. Seeds in Bitcoin are 12 word phrases. Seeds in Ethereum consist of 24 words. Seeds in IOTA contain 81 trytes (i.e., a capital letter or a base-three number). Hackers published or owned websites that facilitated the task to create IOTA seeds. They just needed to wait until they gathered a sufficient number of operational seeds and later they syphoned out their balances. Strictly speaking, this compromise did not exploit a design flaw in IOTA but an insecure user practice to create seeds via ad hoc sites on the Internet [49].

In February 2020 IOTA stopped the tangle in production after identifying a theft of seeds in their Trinity wallet up to a sum higher than USD 2 million. The Trinity wallet is the official mobile and desktop wallet for MIOTA tokens. Hackers compromised the code delivery network of a third party that had access to the code of the Trinity wallet since November 2019 [50]. In this case, the flaw was a human error, i.e., allowing to a third party access to the core code of the wallet without performing the required continuous security due diligence [14].

2.5. IoTeX

IoTeX was built from scratch in 2017 and launched its coin IOTX in February 2018. Raullen Chai, Qevan Guo and Jing Sun founded this project. Xinxin Fan is the head of cryptography [51]. It is a decentralised network for IoT based on a privacy-centric blockchain [52]. It uses different blockchains, permissioned or permissionless, within blockchains; it provides privacy on blockchain; and it uses fast consensus with instant finality. The IoTeX team summarised the ways blockchain benefits IoT with Table 5 ([52] p. 9):

Table 5. How blockchain benefits IoT.

Blockchain Property	IoT Requirement
Decentralization	Scalability, privacy
Byzantine fault tolerance	Availability, security
Transparency & Immutability	Trust
Programmability	Extensibility

IoTeX considers that no unique blockchain implementation can answer all their IoT requirements ([52] p. 12). Following the principle of separation of duties, specific types of blockchains will interact with specific types of IoT devices. A certain degree of complexity in IoT can only be handled by a blockchain with the corresponding degree of complexity [53].

2.5.1. IoTeX Rootchain and Subchains Fast Consensus with Instant Finality

IoTeX runs a public permissionless rootchain and multiple subchains. Subchains support smart contracts and they can be permissioned or permissionless blockchains. The IoTeX rootchain uses the UTXO model to facilitate transaction ordering. It also provides privacy and orchestrates subchains. IoTex rootchain consensus achieves instant block immutability ([52,54] p. 16). Public blockchains such as Bitcoin provide only probabilistic assurance via proof of work that a transaction has been confirmed. IoTeX rootchain uses Roll-DPoS (a randomised delegated proof of stake): Token holders vote for their delegates; these delegates are rank-ordered by the number of votes they receive. The top voted delegates are the "consensus delegates" for the current epoch (a specific length of time). From there, a sub-committee is randomly selected by a randomization algorithm to maintain consensus and produce new blocks for every new epoch [55]. The achievement of block finality is key for IoTeX cross-blockchain communications. These communications rely on simplified payment verification (SPV) [20], a technique to allow a lightweight node to verify a transaction via a Merkle tree using block headers without downloading the entire blockchain. To enable the transferral of tokens to and from subchains, IoTeX uses a two-way pegging (TWP) ([52] p. 16).

2.5.2. Privacy in IoTeX Rootchain

IoTeX preserves privacy in three focus areas: sender privacy, receiver privacy and transaction privacy.

(a) The relayable payment code (on top of the stealth address technique) uses hashed timelock contracts (HTLCs) to offer receiver privacy [56].
(b) The use of a secure multi-party computation protocol (SMCP) among bootstrapping blockchain nodes facilitates the use of a ring signature to preserve sender privacy [51].
(c) The use of Pedersen cryptographic commitments provides transaction value privacy [51].

2.5.3. IoTeX Use Cases

The IoTeX team has released a proposal for an end-to-end secure blockchain-based home IP camera system [57] that could be implemented on top of IoTex. This project includes data integrity, live streaming video sharing and blockchain-based device ownership management.

In the mobile payments arena, Xinxin Fan et al. have published a proposal for cryptocurrency mobile payments, including a solution to meet know your customer (KYC) anti-money laundering (AML) requirements [58].

These two examples already show how the IoT blockchain is an element within a broader technical construct that includes cloud servers (both edge and core) and peer to peer networks.

2.5.4. IOTA vs. IoTeX

This concludes a comprehensive review of two promising IoT platforms. They are the two biggest IoT projects in terms of market capitalisation and they are both open source initiatives backed by relevant industry players. All in all, the multichain proposal of IoTeX, while being more complex both in terms of design and implementation than IOTA, provides more versatility and adaptability, and potentially more speed thanks to its consensus design and smart contracts, especially in environments with IoT devices with very limited computing capacity. IOTA, however, without fees and mining nodes and with its DAG design, is a less sophisticated solution that benefits from the first-mover advantage. Table 6 compares IOTA against IoTeX in terms of design choices and summary figures. Finally, no known security incidents have impacted IoTex so far.

Table 6. IOTA vs IoTeX.

Criteria	IOTA	IoTeX
Year of creation	2015	2017
Market cap (USD)	1.3 B	81 M
Technology	public permissionless DAG	public permissionless root blockchain
Subchains	No	Yes (permissioned possible)
Balance model	UTXO	Balance
Transaction fees	No	Low
Consensus protocol	Proof of work	Proof of stake
Privacy	Not in the DAG	Possible in the rootchain
Known security incidents	2	0

2.6. Security Incidents in Public Blockchains

Table 7 presents the known root cause of several security incidents affecting public blockchain (BLK) implementations (Bitcoin, BTC; Ethereum, ETH) leading to loss of funds [59]. The main conclusion is that attackers took advantage of security flaws in layers different from the architecture of the blockchain implementation. In most cases a better identity management solution could have prevented the real loss of funds before they were converted into real-world fiat money.

Table 7. Security incidents affecting public blockchains.

Date	BLK	Incident	Root Cause
2011	BTC	Mt.Gox exchange hack1	Admin laptop compromised
2014	BTC	Mt.Gox exchange hack2	Leak in hot wallet and no security monitoring
2016	ETH	In a DAO. One Distributed Autonomous Organisation	Code errors in smart contract
2016	BTC	Bitfinex exchange	Flaw in multi-signature accounts and Bitgo wallet
2017	ETH	CoinDash Initial Coin Offering	Website hacked (ICO address changed)
2017	ETH	Parity wallet breach 1 and 2	Vulnerable contract code
2017	ETH	Enigma project scam	Website, slack channel and mailing list compromised
2017	ETH and BTC	Tether tokens stolen	Vulnerable wallet
2018	NEM	Coincheck exchange hacked	Vulnerable hot non-multi signature wallet

In all these incidents, hackers deviated funds in the form of tokens to addresses they controlled. From those addresses, their next step was to convert it into fiat money to use those funds as they pleased. The addresses, in Bitcoin, Ethereum and IOTA, to which these funds were transferred are known, as they appear in the respective public blockchain (or DAG ledger in the case of IOTA). The key will be to identify the owners of those addresses without building any centralised element in the blockchain architecture. This calls for the use of permissioned blockchains and resilient identity management applied at least to addresses holding considerable value.

2.7. Identity and Access Management in IoT

2.7.1. A Set of Technologies to Solve a Complex Security Problem: Cloud and Edge Computing

The need for a resilient IAM framework to avoid intentional risks, i.e., security incidents in blockchains, as stated in Section 2.6, is of paramount importance in IoT as well. In the IoT blockchain world, these requirements are even more challenging to satisfy due to the high number of IoT devices to manage [2,3] and the limited computing resources available in those devices (mostly digital sensors).

The solution to this problem does not lie in specific and unique technology but in a smart combination of current available technologies, such as blockchain, edge computing, cloud computing and cryptography.

Cloud servers provide on-demand storage and computing power over the Internet. In those scenarios where bandwidth is scarce and quick response times are essential, cloud computing is complemented by edge computing. Edge computing places computation and storage closer to the end user, mostly via mobile networks and optical fibre lines. IoT devices are heavy users of this dual cloud/edge computing Internet architecture. For example, secure storage management in IoT networks typically requires both cloud and edge computing [60]. The concept of mobile edge computing (MEC) refers to the provision of cloud computing capabilities at the edge of a cellular network. These MEC nodes can be used to offload computing tasks from IoT devices. Reference [61] proposes a noncooperative game-theoretic strategy selection to distribute work among MEC nodes.

Blockchain and edge computing architectures find applications in smart energy environments as well [62]. It is normal to find a three-layered architecture—i.e., IoT devices (mainly sensors) in layer 1, edge nodes as layer 2 and cloud services as layer 3. This type of architecture allows for the use of decentralised identifiers (DIDs) and verifiable credentials (VCs): useful artefacts to create verifiable self-sovereign digital identities for people, organisations and IoTs [63]. DIoTA, the data integrity framework proposed by Xinxin Fan et al. [64] is a representative example.

To round up this complex ecosystem, the role of smart contracts is also indispensable. They tap into the processing power provided by edge computing to implement, e.g., authentication methods in blockchain-based IoT networks via whitelisting and security scoring [65,66].

Computational intelligence (CI) models can also contribute to solving complex security problems such as identity management. The use of deep fully conventional neural networks (DFCNN), as proposed by [67], to assess the risk of embedded motion sensor-based private information inference in IoT devices could contribute to detecting fraudulent transaction initiators.

We can use additional technologies and models to improve security in IoT networks. For example, in mobile sensor IoT platforms, the use of private car trajectory data to study the aggregation effects [68] and the use of a range-free cooperative localization algorithm [69] or positioning schemes [70] could help with detecting anomalous traffic patterns in fraudulent IoT network participants.

2.7.2. DIoTA: A Decentralised Ledger-Based Framework for Data Authenticity Protection in IoT Systems

Xinxin Fan et al. [64] in 2020 proposed a way to maintain data integrity, including identity related data for IoT systems, which requires very little computing resources and just one public–private key pair per IoT device. The system is comprised of a collection of decentralised ledgers: as many edge ledgers as required and a global ledger. These ledgers run on a system of cloud and edge computing servers.

The DIoTA framework rotates around a collection of key points for this article [64]:

(a) The ledgers in DIoTA are permissioned and decentralised. Reading data could be granted to the public, but any node running ledgers supporting IoT data-producing

devices need to hold a public key certificate from a trusted public key infrastructure (PKI).

(b) Device authentication is a prerequisite for data authenticity protection.

(c) The edge ledger maintains the data authenticity protection schema rather than the IoT devices.

(d) The IoT device only needs to store a private key, crypto parameters such as a certificate and a list of edge ledger nodes.

(e) IoT data authenticity protection is based on a number of cryptographic keys. Those keys are stored in blocks within a blockchain, a distributed edge or global ledger, which runs on top of the corresponding edge or cloud servers.

(f) Reading blockchain data to look for keys and certificates is not resource-intensive. Low energy consumption in IoT devices is a functional requirement. Proposals on caching and scheduling policies to reduce transmission delays and power consumption, such as [71] and a dynamic routing algorithm based on energy-efficient relay selection [72], confirm the need to keep computing operations in the IoT device lightweight.

Xinxin Fan et al. ([64] p. 45) compared DIoTA to other data integrity solutions that could also be used to manage identities in IoT blockchains. Scalability appears as the main competitive advantage for DIoTA.

2.8. Complex Network Analysis: From Graphs to Networks

Reductionism and modelling non-linear phenomena using linear models has been a key strategy in physics to understand many systems of interest ([73] p. 4). However, many non-linear systems in the real world cannot be characterised by linear models. They require newer and more integrated approaches such as the one offered by complex networks. Coming traditionally from mathematics, complex networks received the name of graphs. Graph theory was born with the paper written by Leonhard Euler on the Seven Bridges of Königsberg (published in 1736). Graph theory in the 18th century dealt with static graphs, i.e., those with a permanent structure.

The addition of dynamism to graphs to create dynamic networks was first addressed by Paul Erdős and Alfred Rényi in 1959 ([73] p. 4) with their random networks. In a random network of N nodes (or vertices), new connections (or edges) are created with uniform probability between any pair of nodes. Random networks are characterised by a normal degree distribution ([74] Section 2). This type of network is not commonly found in natural structures. The degree of a node represents the number of connections it has. When sociologists started to use graph theory to represent social relations, the concepts of small-world and scale-free networks started to be frequently used. They both present a relatively small average shortest path length.

Small-world networks are characterised by small average shortest path lengths between pairs of nodes and relatively high clustering coefficients ([73] p. 4). A small average shortest path between nodes means that they are relatively close to each other in terms of edges that are required to traverse to link those nodes. The clustering coefficient indicates the number of edges that exist between a set of nodes connected to a specific node divided by the maximum number of edges that can exist between any of them. They are high density networks, creating communities. A connected community is a cluster. It is based on the idea of a clique. Small-world networks are frequent in social networks. Watts and Strogatz (1998) studied this type of network ([74] Section 2).

A next milestone in complex network theory was the characterisation of scale-free networks. These networks are very present as well in natural and human-made networks. Barabási and Albert studied scale-free networks in 1999. These networks contain a few large degree nodes and many small degree nodes ([74] Section 2). They are less highly clustered than small-world networks. The influence of the large nodes is greater than in small-world networks. Scale-free networks prove to be surprisingly resistant to failures but shockingly sensitive to attacks [75]. A typical example of a scale-free network is a

hub-and-spoke configuration in air transport. In that case, a targeted attack to the most connected node, the hub, could be catastrophic.

2.9. Intentional Risk Management

2.9.1. Static Risk and Dynamic Risk

The proposal to model information systems as nodes (the systems) and edges (their communication lines between them) to manage intentional risk ([11] p. 75) is a security innovation. Using complex network theory, the more connected a node is (or the more accessibility a computer system has), the greater the risk for it to be compromised. The calculation of risk scores of source and destination hosts based on the risk scores of network flows [76] is also an example of using graph theory in security risk management. The three key dimensions proposed to model the complex information system network are value, anonymity and accessibility ([11] pp. 6–7). Reference [11] considers intentionality as the backbone for cyber-risk management and close to game theory, specifically to the stability analysis of John Nash's equilibrium.

An intentional risk materialises when a threat exploits a vulnerability and produces an undesired effect ([15] p. 2) that brings a benefit to the threat actor. System failures and environmental disasters are not events falling within the scope of intentional risk. Chapela et al. (2016) [11] distinguish between static and dynamic risks in intentional risk. They state that static risk measures the "probability for a user who has authorised access to a specific application to choose to abuse his access for personal gain" ([11] p. 7). They also add a different type of risk, dynamic risk, that measures the probability that an attacker (it does not need to be a registered user) tries to get the most valuable node (of a complex network) via the least number of hops through both authorised or unauthorised but possible accesses ([11] p. 7). In dynamic risk, anonymity does not play any role as a variable to manage risk: when a threat actor exploits a vulnerability in a system, they always do it with the maximum possible level of anonymity [11].

Chapela et al. ([11] p. 99) propose the following formula for static risk:

$$Static\ Risk_e = Value_e \cdot (Acc_e) \cdot (\frac{Anon_e}{k}) \quad (1)$$

where

$$Acc_e = Accessibility_{element}, \quad (2)$$

$$Value_e = Value_{element}, \quad (3)$$

$$Anon_e = Anonymity_{element}, \quad (4)$$

$$k = standard\ constant\ related\ to\ the\ (legal)\ consequences\ the\ attacker\ could\ face. \quad (5)$$

In a network G, the static risk is defined as:

$$Static\ Risk_G = \max(\{Static\ Risk_e | e \in G\}). \quad (6)$$

Equally, for dynamic risk ([11] p. 102):

$$Dynamic\ Risk_e = Value_e \cdot Accessibility_e. \quad (7)$$

The dynamic risk of a network G is defined as the maximum of the dynamic risk of its elements, i.e.,

$$Dynamic\ Risk_G = \max(\{(Dynamic\ Risk)_e | e \in G\}). \quad (8)$$

A user that attempts to double-spend their cryptocurrency is an example of static risk. In public blockchains such as Bitcoin and Ethereum, static risk is supposedly contained by design. The "proof of work" consensus proposed by Satoshi Nakamoto ([20] p. 3) prevents by design double-spends from propagating. A typical user approaches the network via a ready-to-use wallet. The code within those wallets does not allow double-spends. A user attempting to create a double-spend would need to code their own wallet.

An ill-intentioned actor that exploits a vulnerability in a crypto wallet and siphons out funds from it is an example of dynamic risk. This actor makes use of an anonymous non-authorised unknown path in the system to extract value from it.

2.9.2. Attackers' Expected Profit

Intentional risk management differs from traditional risk management in its main focus of attention: the attacker's function of profit [11]. It depends on these three elements:

- Expected income, i.e., the value for them.
- The expenses they run (depending on the accessibility).
- Risk to the attacker (related to the degree of anonymity they can have and applicable deterrent legal, economic and social consequences). Calculated risk values should be intrinsic to the attributes of the network and require no expert estimates.

3. Methodology

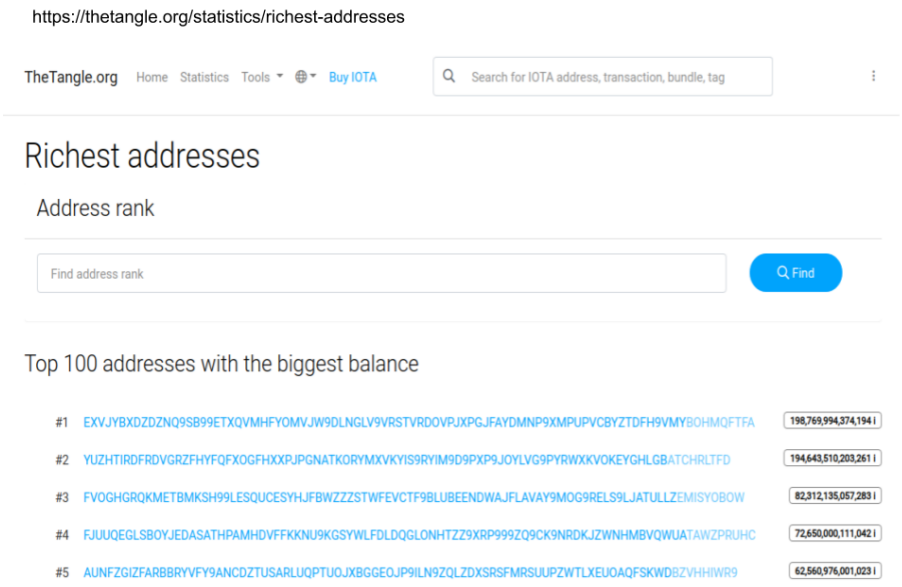
First, we have highlighted the main IoT security challenges and corresponding requirements [4–6,16,18]. Second, we have introduced current works on IoT implementations that use distributed ledgers such as those related to IOTA [31,35,38,43–46] and IoTex [51,52,54,55]. Third, we have presented complex networks as a means to describe complex non-linear systems [7–10,12,13,73] and even to manage intentional risk [11,76]. Now we describe both IOTA and IoTeX transactions as complex networks as a required step to make their IAM more resilient.

3.1. Transaction Data Collection

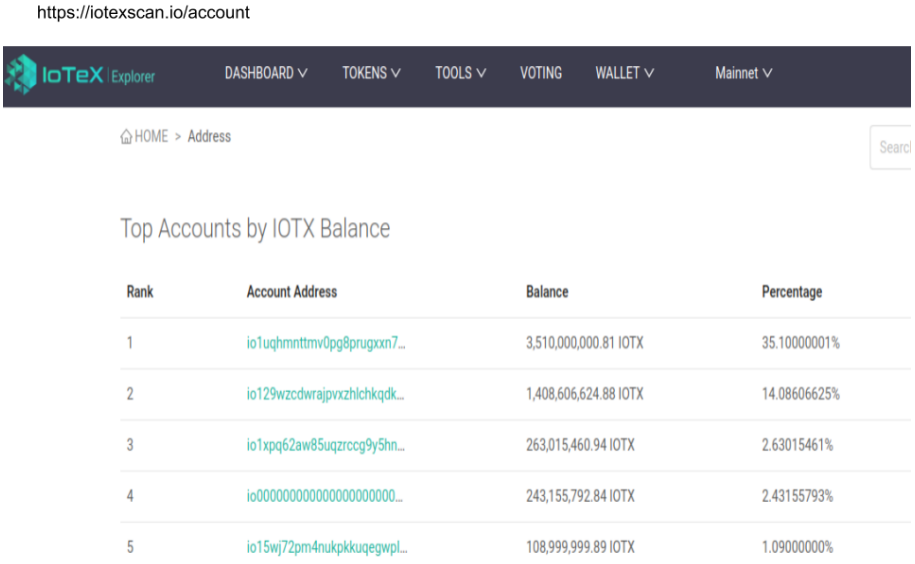
Most public blockchain implementations make block explorers available via the Internet. A block explorer is a web tool that queries blocks, addresses, transactions and hashes in a blockchain. There are explorers for Bitcoin [77] and Ethereum [78] but also for IOTA [79] and IoTeX [80]. These explorer sites publish an open application programming interface (API) to facilitate data collection. Instead of running simulations to collect data, we use these four block explorers to obtain real transaction data. We code a set of Python scripts to extract data from the IOTA and IoTeX public explorers [79,80]. See Figure 3. First, we download the list of addresses holding the highest amounts of MIOTA and IoTeX tokens respectively: the top 100 richest addresses in the case of IOTA and 500 addresses for IoTeX. Second, we use the mentioned APIs to collect transactions linked to those addresses for the longest computationally feasible time window and within the API public usage limits. Calls to these public APIs are usually data and computational-intensive. Explorers consequently limit public queries in the form of data volume caps per API call and per time unit to avoid misuse. As each API has different calls, we write a Python script for each token using the *requests* Python library. Table 8 details the transaction data we download per token and per time window.

Table 8. Transaction data downloaded for IOTA and IoTeX complex network analysis.

Token	Time Window	Addresses	Transactions	#Rich Addresses
IOTA	23-December-2020	1068	22,960	100
IOTA	25-December-2020	1068	23,225	100
IoTeX	endepoch = 13,910 (in December-2020)	3190	10,222	500
IoTeX	endepoch = 14,000 (in December-2020)	3709	13,935	500



(**a**) IOTA explorer. The richest IOTA addresses



(**b**) IoTeX explorer. The richest IoTeX addresses

Figure 3. IOTA and IoTeX ledger explorers.

We perform a similar data collection exercise with the Bitcoin and Ethereum explorers [77,78] to compare their transaction networks with those coming from IOTA and IoTeX. We use public APIs both for BTC [77] and ETH [81]. In this case, we collect all transaction data within specific time slots in December 2020. Table 9 describes the downloaded data.

Table 9. Transaction data downloaded for BTC and ETH complex network analysis.

Token	Time Window	Blocks (Number)	Addresses	Transactions
BTC	21–23-December-2020	662,276–662,554 (278)	1,241,548	1,385,212
ETH	26-December-2020	11,531,960–11,531,970 (11)	1677	1363

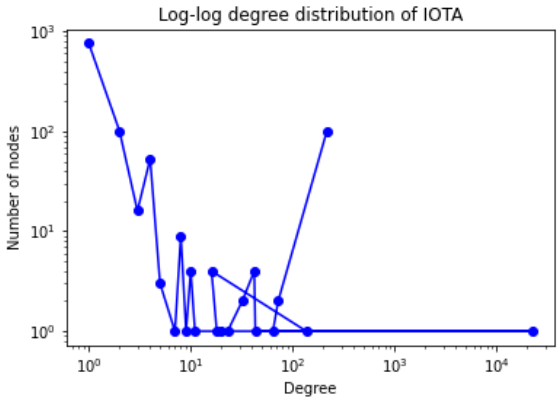
3.2. Transaction Data Preparation: Sender, Destination Pairs

Once we collect the transaction data, we extract the sender and destination fields from the JSON-formatted transaction files. The challenge in this phase is that every analysed ledger has a different structure. We therefore need to parse different JSON schemas for MIOTA, IOTX, Bitcoin and Ethereum. We use the *pandas* Python library to create a text file with a pair of addresses, sender and destination, per line. This file is the input for our complex network analysis.

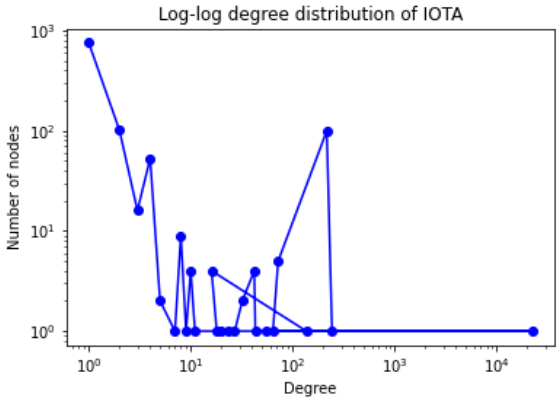
3.3. Complex Network Analysis

Each address in the input file constitutes a node, and each pair of sender and destination creates an edge of an undirected complex network of transactions per token, i.e., IOTA, IoTeX, BTC and ETH. We use the *networkx* Python library to calculate the average degree, the average clustering coefficient, the density, the connectivity, the number of components present in the network and finally the degree distribution. We conclude by plotting the degree distribution using a logarithmic axis with the *matplotlib* Python library. Figures 4–6 show the corresponding degree distributions. The outcome of this complex network analysis provides us with the network profiles for IOTA and IoTeX. The network profile of a system shows how its elements connect. This profile will be pivotal to conclude on their IAM resilience against intentional risk.

We carry out this computational analysis in a dual-processor Intel Xeon CPU @ 2.30 GHz with 13 GB RAM memory. Figure 7 summarises the methodology followed to describe IOTA and IoTeX as complex networks.

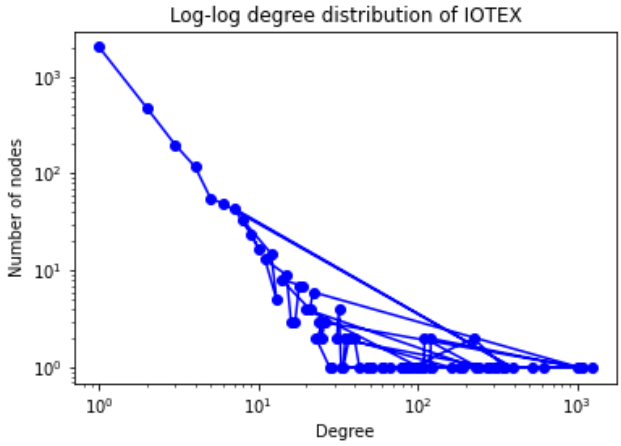


(**a**) Tx degree distribution in t_0

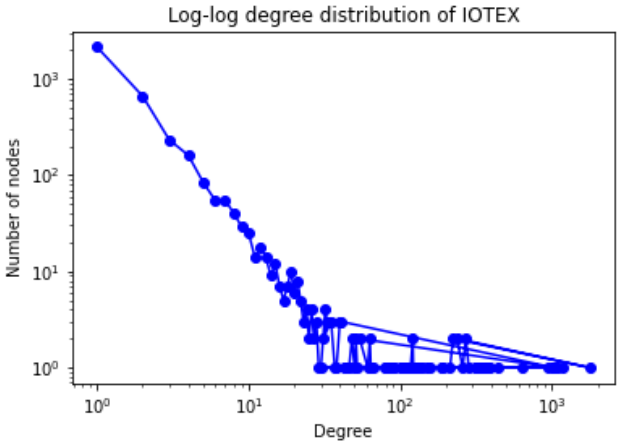


(**b**) Tx degree distribution in t_0 + 48 h

Figure 4. Degree distribution of 1068 IOTA addresses.

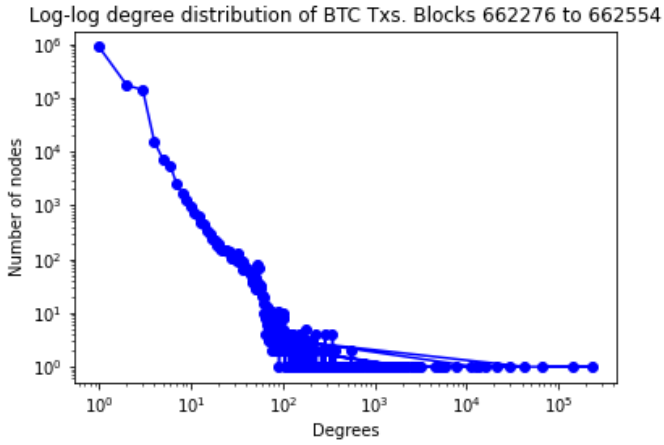


(**a**) Tx degree distribution with top 500 addr. Epoch 13,910

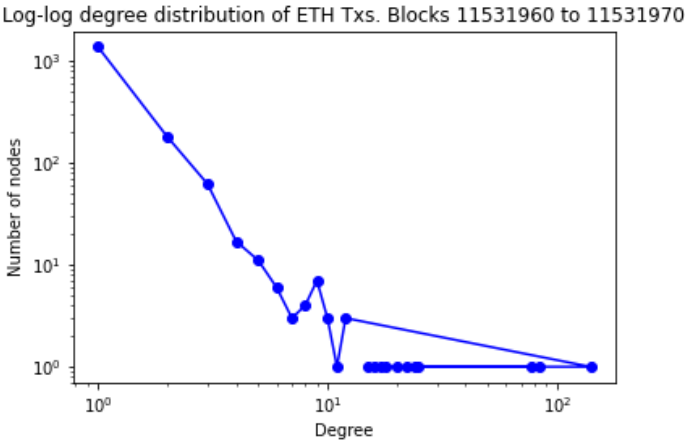


(**b**) Tx degree distribution with top 500 addr. Epoch 14,000

Figure 5. Degree distribution of IoTeX addresses in December 2020.



(**a**) BTC Tx degree distribution



(**b**) ETH Tx degree distribution

Figure 6. Tx degree distribution in BTC and ETH.

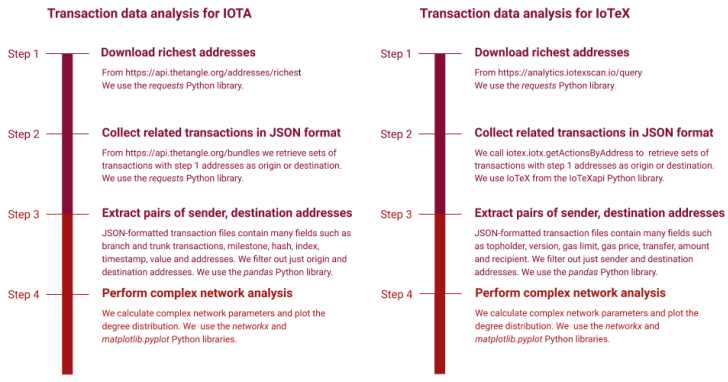


Figure 7. Steps taken to perform the IOTA and IoTeX transaction network analysis.

4. Analysis and Results

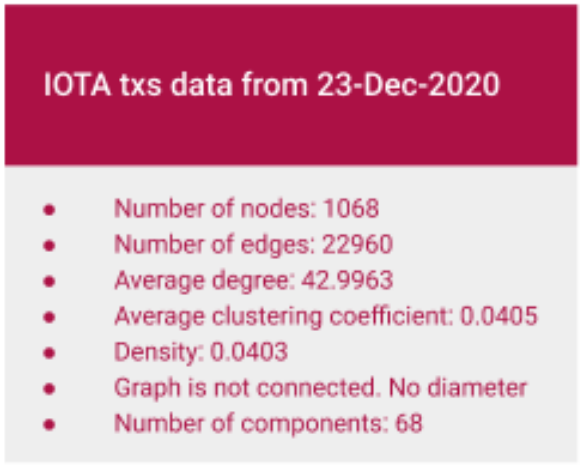
4.1. IOTA Complex Network Analysis

We follow the methodology explained in Figure 7 with the IOTA transaction data presented in Table 8 to generate a complex network. We depict the degree distribution in two-time slots in December 2020 and can see a similar pattern: a weak similarity with a power-law distribution. Although the IOTA dataset used is not sufficient to draw further

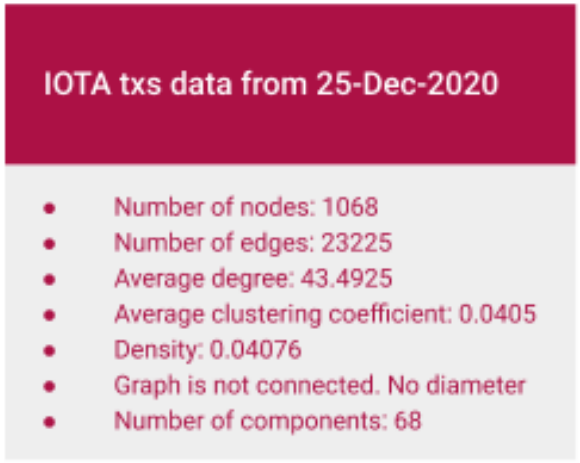
conclusions, a majority of nodes have low degrees and a small number of nodes (addresses) show high degrees. See Figure 4. Coincidentally, we detect an interesting anomaly looking in both graphs: there are around 100 addresses with a degree also close to 100. The fact that we use the list of the 100 richest addresses to extract transaction data could be a potential explanation for this anomaly.

The very low density and average clustering coefficient in these non-connected graphs described in Figure 8 provide no sign of small-world properties (see Section 2.8). These results are in line with the fact that every IOTA address with a positive balance initiating a transaction requires a new address to keep the remainder. As mentioned in Section 2.3.5, addresses sending a transaction are only used once for security reasons. Consequently, most of the highly connected (high degree) reused addresses are only transaction destinations. Those addresses can remain active for a long time. If we could verify the real-life identities behind those destination addresses holding large amounts of MIOTAs, we could increase the resilience against intentional risk in this IoT platform.

The empirical in-degree distributions of IOTA mainnet snapshots calculated by ([48] p. 5, Figure 4b) show a power-law distribution in contrast with the Poisson degree distribution extracted from simulated tangles ([48] p. 5). Compared to our dataset, Guo et al. [48] use a 13 month-long IOTA tangle dataset ranging from November 2016 to April 2019. Unfortunately, the IOTA Foundation has not published mainnet tangle datasets since April 2019.



(**a**) IOTA transaction network. Sample 1



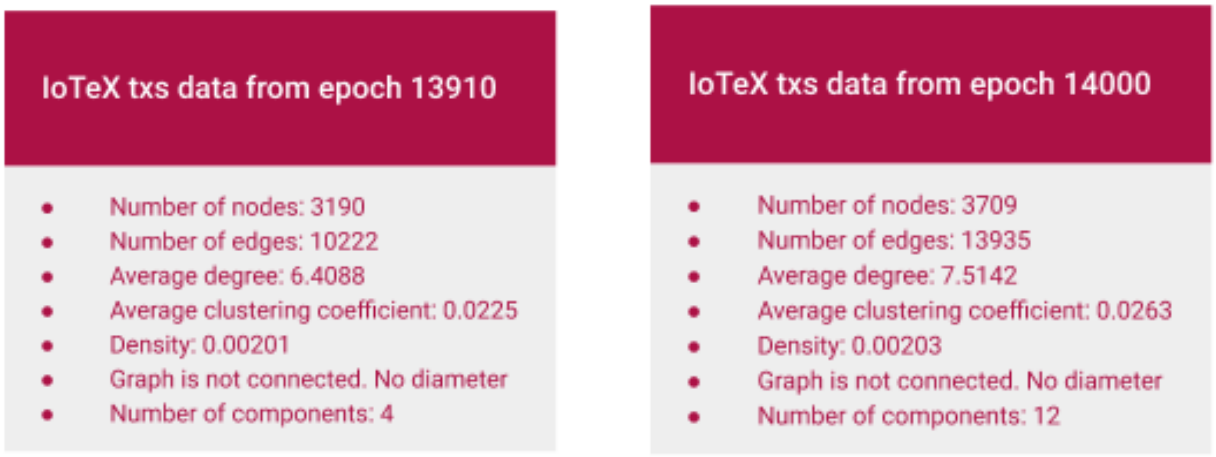
(**b**) IOTA transaction network. Sample 2

Figure 8. Complex network analysis for IOTA transactions.

4.2. IoTeX Complex Network Analysis

Equally, we follow the methodology explained in Figure 7 with the IoTeX transaction data presented in Table 8 to generate a complex network. We select two time-slots: epoch 13,910 and epoch 14,000 happening in December 2020. An epoch in IoTeX in 2020 tended to last less than 30 min. For both epochs we start with the top 500 richest addresses. Once we collect those addresses we gather up to 1000 transactions per address (as per the limit of the public IoTeX explorer API [80]).

Figure 5 shows the degree distribution of IoTeX addresses present in the analysed transactions. It resembles a power-law function. There is a very high number of addresses with a very low number of connections, and conversely, a very low number of addresses with a very high number of transactions. This is an indication of a scale-free network. The network is composed of non-connected graphs with lesser numbers of components than in the case of IOTA and a lower average degree. This indicates that rich addresses in IoTeX are more connected with other nodes than rich IOTA addresses. Similarly to IOTA, if we could verify the real-life identities behind those high-degree addresses, potentially holding high amounts of IOTXs, we could increase the resilience against intentional risk in this IoT platform. As in IOTA, with such a low average clustering coefficient, we find no sign of small-world network properties based on the data displayed in Figure 9.



(**a**) IoTeX transaction network. Sample 1

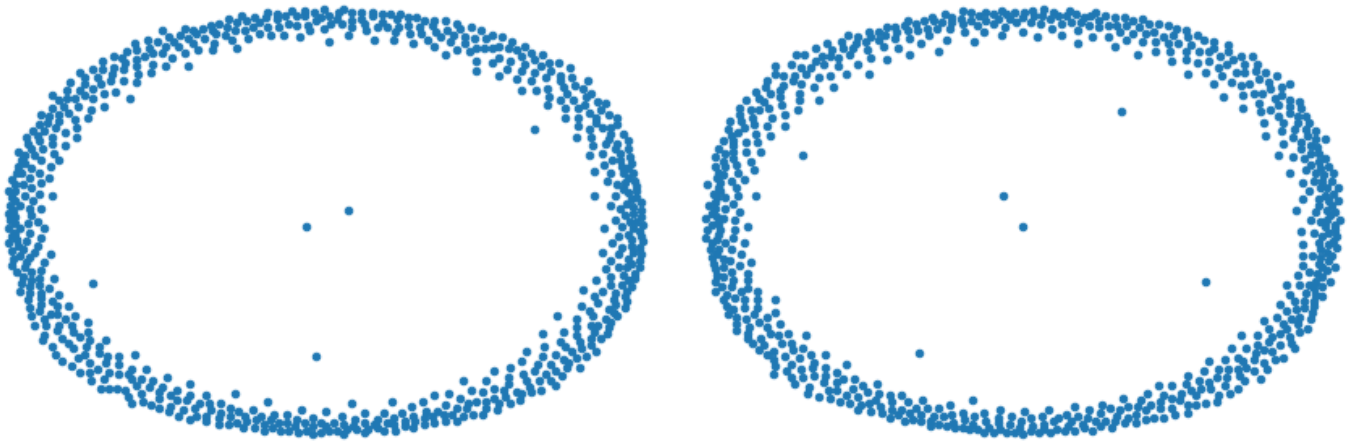
(**b**) IoTeX transaction network. Sample 2

Figure 9. Complex network analysis for IoTeX transactions.

4.3. Largest Connected Components in IOTA and IoTeX

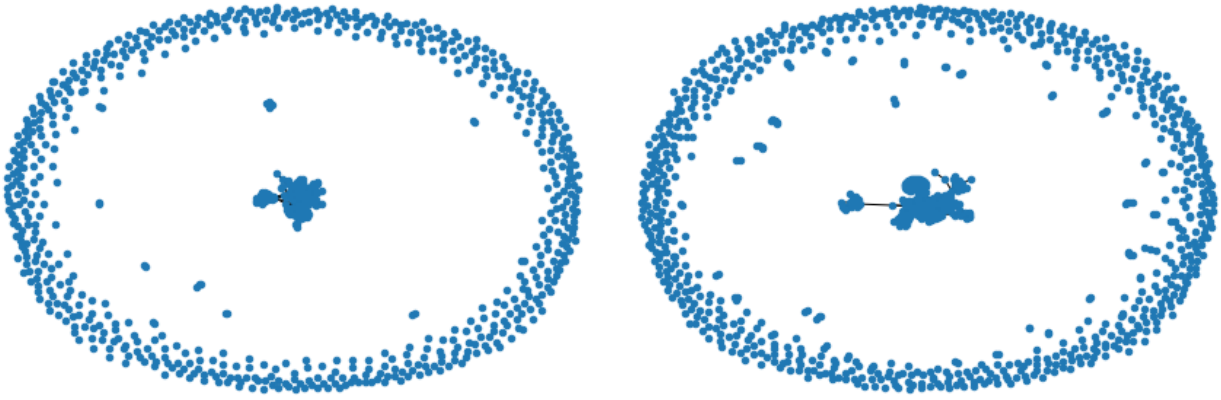
We identify the largest connected component (LCC) in both transaction networks and we draw all nodes connected to it without displaying the edges between those nodes and the LCC to ease interpretation. The appearances of the graphs showing nodes connected to the LCC in IOTA and IoTeX are similar. Figures 10 and 11 show that the disassortativity is patent; i.e., nodes do not tend to link with nodes of a similar level. On the contrary, low degree nodes tend to connect with very high degree nodes.

Figures 10 and 11 represent all nodes connected to the largest one in the network with a distance equal to or less than 3. Nodes (addresses) connected to high degree nodes do not tend to connect with each other. If we consider that most of those nodes in the IoT world are sensors or any other IoT devices, it is a plausible scenario that they connect with their assigned data collecting server. Sensors do not tend to transact with each other.



(**a**) IOTA nodes connected to LCC in t_0 (**b**) IOTA nodes connected to LCC in t_0 + 48 h

Figure 10. Nodes connected to IOTA LCC. Edges to LCC not displayed.



(**a**) Nodes connected to IoTeX LCC up to epoch 13,910 (**b**) Nodes connected to IoTeX LCC up to epoch 14,000

Figure 11. Nodes connected to IoTeX LCC. Edges to LCC not displayed.

4.4. Comparison with Bitcoin and Ethereum Complex Network Analysis

As mentioned in Section 3.1, we also collect transaction data from Bitcoin and Ethereum to build the degree distributions of their transaction networks and compare them with those obtained with IOTA and IoTeX networks. We use public APIs both for BTC [77] and ETH [81] and we follow a methodology similar to Figure 7 with the BTC and ETH transaction data presented in Table 9 to generate a complex network.

We identify power-law degree distributions as well. See Figure 6. This indicates that the transaction networks of these two public blockchain implementations display scale-free characteristics. We also obtain clustering coefficients very close to 0 indicating that neither BTC nor ETH display small-world properties. Reference [82] reaches a similar conclusion.

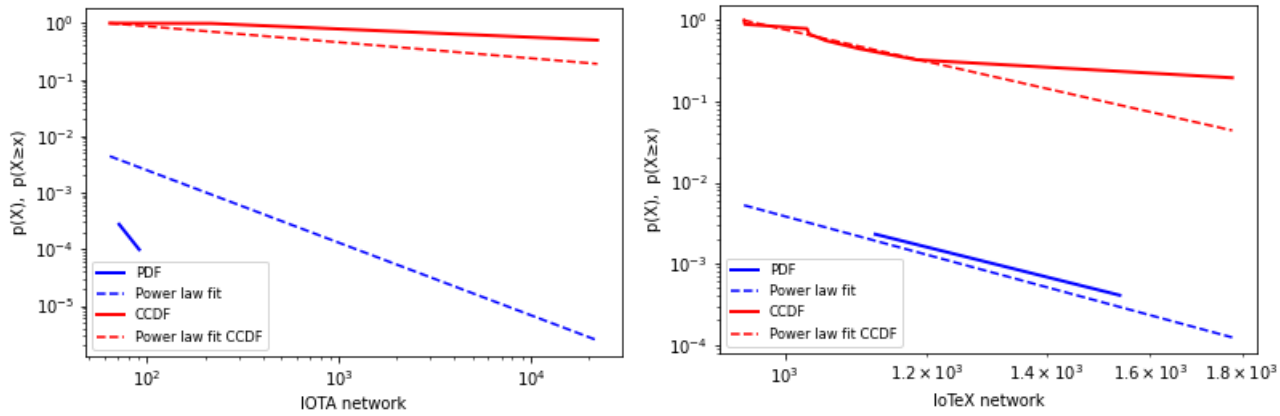
Reference [82] suggests that successful cryptocurrencies, such as Bitcoin and Ethereum, once they pass their creation phase and reach a stable stage with millions of transaction addresses, show a power-law degree distribution. References [83,84] reaches a similar conclusion: the Bitcoin network out-degree distribution might be fitted by a power-law. Our empirical results are aligned. Reference [85], however, does not reach the same power-law fit as they analyse BTC data during the early days of the BTC network, i.e., from January 2009 up to July 2011.

We also observe a very low density in these two networks. This is due to the very short periods of time observed; i.e., not many addresses are reused within adjacent blocks. Our extracted data for BTC (2 days) covers a longer time than the extracted data for ETH

(some minutes). This is the reason why the power-law degree distributions are clearer to identify in the BTC graph than in the ETH graph.

4.5. Analysis of Heavy-Tailed Distributions

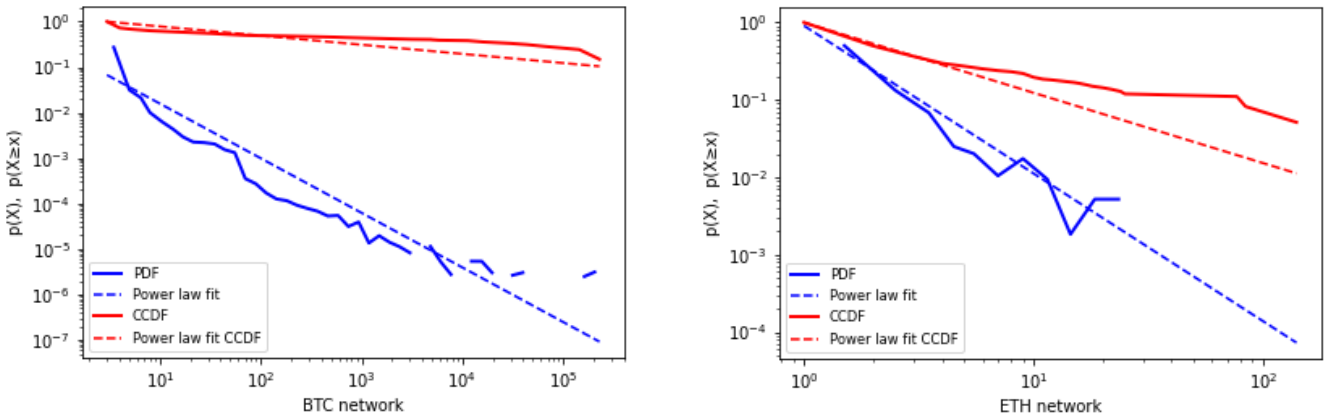
The identification of power-law fits on a log–log axis and only graphically is biased and inaccurate [86]. We use the *powerlaw* Python library developed by Alstott et al. [87] with our IOTA degree distribution dataset to assess our results. The plot from the IOTA network shows a good fit by the power-law to the complementary cumulative distribution function (CCDF). See Figure 12a. The probability density function (PDF) is, however, limited and far from a power-law fit. This is in line with our previous IOTA results presented in Section 4.1; i.e., the power-law fit is questionable. In our IoTeX degree distribution dataset, the network displays a good fit by the power-law to the PDF, with a limited range of possible degrees starting at x = 949 though. See Figure 12b. The power-law fit with the CCDF still shows a very heavy tail deviating from the power-law fit, probably due to it being young. This is in line with our previous IoTeX results presented in Section 4.2; i.e., the power-law fit is more present in IoTeX than in IOTA.



(**a**) IOTA power-law fit (**b**) IoTeX power-law fit

Figure 12. Power-law fit using Python powerlaw library by Alstott et al. IOTA and IoTeX datasets.

We also use this *powerlaw* library by Alstott et al. [87] with our BTC and ETH degree distribution datasets to confirm our results and the references mentioned in Section 4.4, i.e., [82] for both BTC and ETH and ([83,84] pp. 23–26) for BTC. The power-law fits in Figure 13a,b are evident, although with a bigger gap in ETH due to the shorter period of analysis.



(**a**) BTC power-law fit (**b**) ETH power-law fit

Figure 13. Power-law fit using Python powerlaw library by Alstott et al. BTC and ETH datasets.

5. Conclusions

5.1. Blockchain Answers a Subset of IoT Security Requirements

The blockchain technology can implement a number of IoT cybersecurity requirements based on its distributed and immutable nature. However, a single blockchain implementation with no additional means to manage complexity, such as smart contracts, edge and cloud computing, cannot fulfil all security requirements that IoT platforms need to implement. See Section 2.7.

5.2. Identity and Access Management is a Key Security Requirement to Build Resilience against Intentional Risk

Intentional risk focuses on attacks performed by actors with a defined intention to obtain a benefit (value). Intentional risks can be static and dynamic. Using the static and dynamic risk formulas proposed by Chapela et al. and presented in Section 2.9, we conclude that in IoT implementations with nodes holding large amounts of value, we can only reduce both static and dynamic risk if we control access to those nodes (mostly IoT devices and IT components). In distributed environments such as IoT, an IAM framework that uses decentralised identifiers (DIDs) and verifiable credentials (VCs), as presented in Section 2.7, can control the accessibility to those devices. DIoTA uses artefacts of this type.

5.3. IoTeX and Possibly IOTA Networks Are Scale-Free. They Require Resilience against Intentional Risk

IOTA and IoTeX are two examples of IoT platforms built on distributed ledgers. They are both in production and they both are actively improving their scalability and security. The IoTeX network displays a power-law degree distribution as scale-free networks do. Our IOTA dataset could not confirm it for the IOTA network as Guo et al. did [48], possibly due to the limited time slot analysed. In both networks there is a small set of highly connected-nodes. As mentioned in Section 2.8, in scale-free networks the influence of the large nodes is greater than in small-world networks. Scale-free networks prove to be surprisingly resistant to failures but shockingly sensitive to targeted attacks. A way to make these IoT networks less sensitive to attacks, or in other words, a way to improve their resilience against intentional risk is to implement a distributed IAM concept.

5.4. DIoTA Provides IoTex with Resilient Identity and Access Management

DIoTA, the decentralised ledger-based framework for data authenticity protection in IoT systems proposed by Xinxin Fan et al. in 2020 (see Section 2.7.2) is well-positioned to bring IoTeX into the front line of IoT blockchain-based implementations that manage intentional risk effectively. Both IOTA and IoTeX projects are immersed in promising design improvements. We consider IoTeX a more complex platform, but at the same time, better positioned to implement resilient IAM frameworks such as DIoTA. A key requirement for IoTex to achieve this aspiration is to hold all worth-protecting value in permissioned blockchains.

5.5. Resilience against Intentional Risk Requires an IAM Concept That Transcends a Single Blockchain

Based on our results for IOTA and IoTeX, we conclude that resilience against intentional risk requires an IAM concept that transcends the possibilities of a single blockchain implementation. Only with the interplay of edge and global ledgers running on edge and cloud servers we can obtain data integrity in a multi-vendor and multi-purpose IoT network.

6. Future Work

We see three main lines of future work stemming from this paper:

(a) Transforming the time series created by IOTA and IoTeX transactions into complex networks to go deeper into their analysis using the visibility graph proposed by Lacasa et al. [88].
(b) Studying whether DIoTA can be further extended using any of the artificial intelligence (AI) solutions to secure IoT services in edge computing surveyed by Xu et al. [89].
(c) Assessing the possibility of applying generative adversarial nets (GANs) to improve the speed and accuracy in consensus protocols based on proof-of-stake (PoS), such as the one used by IoTeX [90,91].

Author Contributions: These authors (A.P., R.C. and M.R.) contributed equally to this work. All authors have read and agreed to the published version of the manuscript.

Funding: Regino Criado and Miguel Romance have been partially supported by projects PGC2018-101625-B-I00 (Spanish Science and Innovation Ministry, AEI/FEDER, UE) and M1967 (URJC grant).

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

References

1. Number of Internet of Things (IoT) Connected Devices Worldwide in 2018, 2025 and 2030. Available online: https://www.statista.com/statistics/617136/digital-population-worldwide/ (accessed on 21 December 2020).
2. Sallaba, M.; Siegel, D.; Becker, S. Deloitte Blockchain Institute. IoT Powered by Blockchain. How Blockchains Facilitate the Application of Digital Twins in IoT. May 2018. Available online: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/IoT-powered-by-Blockchain-Deloitte.pdf (accessed on 21 December 2020).
3. Number of Internet of Things (IoT) Connected Devices Worldwide in 2018, 2025 and 2030. Available online: https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/ (accessed on 21 December 2020).
4. NIST. Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline. NIST Interagency or Internal Report 8259C. December 2020. Available online: https://doi.org/10.6028/NIST.IR.8259C-draft (accessed on 21 December 2020).
5. ETSI. Technical Specification. Cyber Security for Consumer Internet of Things. ETSI TS 103 645 V1.1.1 (2019-02). February 2019. Available online: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (accessed on 21 December 2020).
6. NIST. Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government. NIST Interagency or Internal Report 8259D. December 2020. Available online: https://doi.org/10.6028/NIST.IR.8259D-draft (accessed on 21 December 2020).
7. Newman, M.E.J. The Structure and Function of Complex Networks. *SIAM Rev.* **2003**, *45*, 167–257. [CrossRef]
8. Newman, M.E.J. The Connected World. 2011. Santa Fe Institute. Available online: https://www.youtube.com/watch?v=yAtsm5xkb5c (accessed on 21 December 2020).
9. Newman, M.E.J. Using Networks to Make Predictions. Santa Fe Institute. 2011. Available online: https://www.youtube.com/watch?v=rwA-y-XwjuU (accessed on 21 December 2020).
10. Newman, M.E.J. What Networks Can Tell Us about the World. Santa Fe Institute. 2011. Available online: https://www.youtube.com/watch?v=lETt7IcDWLI (accessed on 21 December 2020).
11. Chapela, V.; Criado, R.; Moral, S.; Romance, M. *Intentional Risk Management through Complex Networks Analysis*; Springer: Berlin/Heidelberg, Germany, 2015.
12. Boccaletti, S.; Latora, V.; Moreno, Y.; Chavez, M.; Hwang, D. Complex Networks: Structure and Dynamics. *Phys. Rep.* **2006**, 175–308. [CrossRef]
13. Boccaletti, S.; Buldú, J.; Criado, R.; Flores, J.; Latora, V.; Pello, J.; Romance, M. Multiscale Vulnerability of Complex Networks. *Chaos Interdiscip. J. Nonlinear Sci.* **2007**, 175–308. [CrossRef]
14. Alberto, P. Secure IT Up! In *Cyber Insurance Due Diligence*; Kroll Inc.: New York, NY, USA, 2012; pp. 6–7. ISBN 9781478314752.
15. Andina, D.; Partida, A. IT Security Management: IT Securiteers—Setting up an IT Security Function. In *Lecture Notes in Electrical Engineering*; Springer: Berlin/Heidelberg, Germany, 2010; ISBN 9789048188819.
16. ETSI. ETSI Releases First Globally Applicable Standard for Consumer IoT Security. February 2019. Available online: https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security (accessed on 21 December 2020).
17. Fruhlinger, J. CSO Online. The Mirai Botnet Explained: How Teen Scammers and CCTV Cameras Almost Brought Down the Internet. 2018. Available online: https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html (accessed on 21 December 2020).
18. NIST. IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements. Draft NIST Special Publication 800-213. December 2020. Available online: https://doi.org/10.6028/NIST.SP.800-213-draft (accessed on 21 December 2020).

19. Anthony, L. A Gentle Introduction to Blockchain Technology. Bitsonblocks.com. 2015. Available online: http://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology (accessed on 21 December 2020).
20. Satoshi, N. Bitcoin: A Peer-to-Peer Electronic Cash System. Nakamotoinstitute.org. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 21 December 2020).
21. ETH Corporate Site. Available online: https://www.ethereum.org/ (accessed on 21 December 2020).
22. Coinmarketcap. Cryptocurrencies Market Capitalisation in Real Time. Available online: https://coinmarketcap.com/all/views/all/ (accessed on 21 December 2020).
23. Papadodimas, G.; Palaiokrasas, G.; Litke, A.; Varvarigou, T. Implementation of Smart Contracts for Blockchain Based IoT Applications. Electrical and Computer Engineering Department National Technical University of Athens. November 2018. Available online: http://bloomen.io/wp-content/uploads/2018/11/ICCS-nof2018.pdf (accessed on 21 December 2020).
24. Kurt Peker, Y.; Rodriguez, X.; Ericsson, Y.; Lee, S.; Perez, A. A Cost Analysis of Internet of Things Sensor Data Storage on Blockchain via Smart Contracts. *Electronics* **2020**, *9*, 244. [CrossRef]
25. Zvi, S. k-Root-n: An Efficient Algorithm for Avoiding Short Term Double-Spending Alongside Distributed Ledger Technologies such as Blockchain. *Information* **2020**, *11*, 90.
26. Blockchain.com. Transactions Per Second. Available online: https://www.blockchain.com/charts/transactions-per-second (accessed on 21 December 2020).
27. Transactions Per Second. Available online: https://etherscan.io/ (accessed on 21 December 2020).
28. Transactions Per Second in Blockchains. Available online: https://blocktivity.info/ (accessed on 21 December 2020).
29. EOSIO Reaches a New Transaction Per Second Record: 9656. Available online: https://www.eosgo.io/news/eosio-reaches-new-transaction-per-second-record (accessed on 21 December 2020).
30. IOT Crypto Coin Market Value. Available online: https://cryptoslate.com/cryptos/iot/ (accessed on 24 December 2020).
31. IOTA. Introduction. Available online: https://www.iota.org/get-started/what-is-iota (accessed on 21 December 2020).
32. Sun, F. UTXO vs Account/Balance Model. Available online: https://medium.com/@sunflora98/utxo-vs-account-balance-model-5e6470f4e0cf (accessed on 25 December 2020).
33. IOTA Tangle Explorer. Available online: https://thetangle.org/ (accessed on 24 December 2020).
34. IOTA Tangle Explorer. Available online: https://thetangle.org/nodes (accessed on 24 December 2020).
35. Serguei, P. The Tangle. White Paper. Version 1.4.3; 2018. Available online: https://bit.ly/3e2edXo (accessed on 24 December 2020).
36. Trifa, Z.; Khemakhem, M. Sybil Nodes as a Mitigation Strategy Against Sybil Attack. *Procedia Comput. Sci.* **2014**, *32*, 1135–1140. [CrossRef]
37. Kusmierz, B.; Staupe, P.; Gal, A. Extracting Tangle Properties in Continuous Time via Large-Scale Simulations. 2018. Available online: https://tinyurl.com/yclxej5h (accessed on 26 December 2020).
38. Popov, S.; Moog, H.; Camargo, D.; Capossele, A.; Dimitrov, V.; Gal, A.; Greve, A.; Kusmierz, B.; Mueller, S.; Penzkofer, A.; et al. The Coordicide. IOTA Foundation. 2020. Available online: https://files.iota.org/papers/20200120_Coordicide_WP.pdf (accessed on 24 December 2020).
39. Capossele, A.; Mueller, S.; Penzkofer, A. Robustness and Efficiency of Leaderless Probabilistic Consensus Protocols within Byzantine Infrastructures. 2019. Available online: https://arxiv.org/abs/1911.08787 (accessed on 25 December 2020).
40. Müller, S.; Penzkofer, A.; Kuśmierz, B.; Camargo, D.; Buchanan, W.J. Fast Probabilistic Consensus with Weighted Votes. In Proceedings of the Future Technologies Conference (FTC), Vancouver, BC, Canada, 5–6 November 2020; Arai, K., Kapoor, S., Bhatia, R., Eds.; Springer: Cham, Switzerland, 2020; Volume 1289. [CrossRef]
41. Popov, S.; Buchanan, W.J. FPC-BI: Fast Probabilistic Consensus within Byzantine Infrastructures. *J. Parallel Distrib. Comput.* **2021**, *147*, 77–86. ISSN 0743-7315. [CrossRef]
42. Chain, L. Learn Me a Bitcoin. Available online: https://bit.ly/38uPTw0 (accessed on 24 December 2020).
43. Release Strategy for Chrysalis. IOTA 1.5. Available online: https://blog.iota.org/release-strategy-for-chrysalis-iota-1-5-4ea8741ea3a1 (accessed on 24 December 2020).
44. A Proposal for Reusable Addresses (Part 1). IOTA Blog. Available online: https://blog.iota.org/a-proposal-for-reusable-addresses-part1-bc6dbca84cbf (accessed on 7 July 2020).
45. A Proposal for Reusable Addresses (Part 2). IOTA Blog. Available online: https://blog.iota.org/a-proposal-for-reusable-addresses-part-2-d83d328ff1b3 (accessed on 7 July 2020).
46. A Proposal for Reusable Addresses (Part 3). IOTA Blog. Available online: https://blog.iota.org/a-proposal-for-reusable-addresses-part-3-9ec6fa1929d7 (accessed on 7 July 2020).
47. IOTA Corporate Site. Explore IOTA Industries. Available online: https://www.iota.org/solutions/industries (accessed on 25 December 2020).
48. Guo, F.; Xiao, X.; Hecker, A.; Dustdar, S. Characterizing IOTA Tangle with Empirical Data. 2020 IEEE Global Communications Conference. Taiwan Communications for Human and Machine Intelligence. Available online: https://globecom2020.ieee-globecom.org/program/symposia-tuesday (accessed on 26 December 2020).
49. PSA. Do Not Use Online Seed Generators. Reddit. Available online: https://www.reddit.com/r/Iota/comments/7rmc55/psa_do_not_use_online_seed_generators/ (accessed on 28 December 2020).

50. IOTA Foundation Suspends Network, Probes Fund Theft in Trinitytrinity Wallet. Coindesk. Available online: https://www.coindesk.com/iota-foundation-suspends-network-probes-fund-theft-in-trinity-wallet (accessed on 28 December 2020).
51. IoTex Team and Introduction Portal. Available online: https://v1.iotex.io/ (accessed on 24 December 2020).
52. IoTeX Team. IoTeX. A Decentralised Network for Internet of Things Powered by a Privacy-Centric Blockchain. White Paper. Version 1.5. 12 July 2018. Available online: https://v1.iotex.io/white-paper (accessed on 24 December 2020).
53. Stafford, B. *Decision and Control*; Wiley: London, UK, 1966.
54. Fan, X. Scalable Practical Byzantine Fault Tolerance with Short-Lived Signature Schemes. In Proceedings of the 28th Annual International Conference on Computer Science and Software Engineering, Markham, ON, Canada, 29–31 October 2018; pp. 245–256. [CrossRef]
55. Fan, X.; Chai, Q. Roll-DPoS: A Randomized Delegated Proof of Stake Scheme for Scalable Blockchain-Based Internet of Things Systems. In Proceedings of the MobiQuitous'18: Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, New York City, NY, USA, 5–7 November 2018; pp. 482–484. [CrossRef]
56. Fan, X. Faster Dual-Key Stealth Address for Blockchain-Based Internet of Things Systems. 2018. Available online: https://link.springer.com/chapter/10.1007/978-3-319-94478-4_9 (accessed on 29 December 2020).
57. Fan, X.; Zhong, Z.; Chai, Q.; Guo, D. Ucam: A User-Centric, Blockchain-Based and End-to-End Secure Home IP Camera System. In *Security and Privacy in Communication Networks, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*; Park, N., Sun, K., Foresti, S., Butler, K., Saxena, N., Eds.; Springer: Cham, Switzerland, 2020; Volume 336. [CrossRef]
58. Xu, L.; Chen, L.; Gao, Z.; Carranco, L.; Fan, X.; Shah, N.; Diallo, N.; Shi, W. Supporting Blockchain-Based Cryptocurrency Mobile Payment With Smart Devices. *IEEE Consum. Electron. Mag.* **2020**, *9*, 26–33. [CrossRef]
59. Blockchain News Site. Information Related to Incidents. Available online: https://www.coindesk.com (accessed on 28 December 2020).
60. Nyamtiga, B.W.; Sicato, J.C.S.; Rathore, S.; Sung, Y.; Park, J.H. Blockchain-Based Secure Storage Management with Edge Computing for IoT. *Electronics* **2019**, *8*, 828. [CrossRef]
61. Xiao, Z.; Dai, X.; Jiang, H.; Wang, D.; Chen, H.; Yang, L.; Zeng, F. Vehicular Task Offloading via Heat-Aware MEC Cooperation Using Game-Theoretic Method. *IEEE Internet Things J.* **2020**, *7*, 2038–2052. [CrossRef]
62. Sittón-Candanedo, I.; Alonso, R.S.; García, Ó.; Gil, A.B.; Rodríguez-González, S. A Review on Edge Computing in Smart Energy by means of a Systematic Mapping Study. *Electronics* **2020**, *9*, 48. [CrossRef]
63. Fan, X.; Chai, Q.; Li, Z.; Pan, T. Decentralized IoT Data Authorization with Pebble Tracker. In Proceedings of the 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2–16 June 2020. [CrossRef]
64. Xu, L.; Chen, L.; Gao, Z.; Fan, X.; Suh, T.; Shi, W. DIoTA: Decentralized-Ledger-Based Framework for Data Authenticity Protection in IoT Systems. *IEEE Netw.* **2020**, *34*, 38–46. [CrossRef]
65. Choi, Y.-J.; Kang, H.-J.; Lee, I.-G. Scalable and Secure Internet of Things Connectivity. *Electronics* **2019**, *8*, 752. [CrossRef]
66. Putra, G.D.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Trust Management in Decentralized IoT Access Control System. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 4–7 May 2020; pp. 1–9. [CrossRef]
67. Huang, Y.; Guan, X.; Chen, H.; Liang, Y.; Yuan, S.; Ohtsuki, T. Risk Assessment of Private Information Inference for Motion Sensor Embedded IoT Devices. *IEEE Trans. Emerg. Top. Comput. Intell.* **2020**, *4*, 265–275. [CrossRef]
68. Wang, D.; Fan, J.; Xiao, Z.; Jiang, H.; Chen, H.; Zeng, F.; Li, K. Stop-and-Wait: Discover Aggregation Effect Based on Private Car Trajectory Data. *IEEE Trans. Intell. Transp. Syst.* **2019**, *20*, 3623–3633. [CrossRef]
69. Chen, H.; Gao, F.; Martins, M.H.T.; Huang, P.; Liang, J. Accurate and Efficient Node Localization for Mobile Sensor Networks. *Mob. Netw. Appl.* **2013**, *18*, 141–147. [CrossRef]
70. Chen, H.; Liu, B.; Huang, P.; Liang, J.; Gu, Y. Mobility-Assisted Node Localization Based on TOA Measurements without Time Synchronization in Wireless Sensor Networks. *Mob. Netw. Appl.* **2012**, *17*, 90–99. [CrossRef]
71. Zhang, Z.; Chen, Z.; Hua, M.; Li, C.; Huang, Y.; Yang, L. Double Coded Caching in Ultra Dense Networks: Caching and Multicast Scheduling via Deep Reinforcement Learning. *IEEE Trans. Commun.* **2020**, *68*, 1071–1086. [CrossRef]
72. Ding, Z.; Shen, L.; Chen, H.; Yan, F.; Ansari, N. Energy-Efficient Relay-Selection-Based Dynamic Routing Algorithm for IoT-Oriented Software-Defined WSNs. *IEEE Internet Things J.* **2020**, *7*, 9050–9065. [CrossRef]
73. da Fontoura Costa, L.; Oliveira, O.N., Jr.; Travieso, G.; Aparecido Rodrigues, F.; Ribeiro Villas Boas, P.; Antiqueira, L.; Palhares Viana, M.; Correa Rocha, L.E. Analyzing and modeling real-world phenomena with complex networks: A survey of applications. *Adv. Phys.* **2011**, *60*, 329–412. [CrossRef]
74. Beauguitte, L.; Ducruet, C. Scale-free and small-world networks in geographical research: A critical examination. In Proceedings of the 17th European Colloquium on Theoretical and Quantitative Geography, Athènes, Greece, 15 September 2019; pp. 663–671. Available online: https://halshs.archives-ouvertes.fr/halshs-00623927 (accessed on 21 December 2020).
75. Barabási, A. Network Science. 2014. Creative Commons: CC BY-NC-SA 2.0. Available online: http://barabasi.com/book/network-science (accessed on 29 December 2020).
76. Chapela, M.; Sekulic, V.; Ignjatovic, A.; Bertino, E.; Jha, S. Interdependent Security Risk Analysis of Hosts and Flows. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2325–2339. [CrossRef]
77. Bitcoin Blockchain Explorer. Available online: https://www.blockchain.com/explorer (accessed on 28 December 2020).

78. Ethereum Blockchain Explorer. Available online: https://etherscan.io/ (accessed on 28 December 2020).
79. IOTA Blockchain Explorer. Available online: https://explorer.iota.org/mainnet (accessed on 28 December 2020).
80. IoTeX Blockchain Explorer. Available online: https://iotexscan.io/ (accessed on 28 December 2020).
81. Ethereum Blockchain Explorer API. Available online: https://infura.io/ (accessed on 28 December 2020).
82. Liang, J.; Li, L.; Zeng, D. Evolutionary dynamics of cryptocurrency transaction networks: An empirical study. *PLoS ONE* **2018**, *13*, e0202202. [CrossRef]
83. Javarone, M.A.; Wright, C.S. From Bitcoin to Bitcoin Cash: A network analysis. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Munich, Germany, 15 June 2018; pp. 77–81. [CrossRef]
84. Lischke, M.; Fabian, B. Analyzing the Bitcoin Network: The First Four Years. *Future Internet* **2016**, *8*, 7. [CrossRef]
85. Goldstein, M.L.; Morris, S.A.; Yen, G. Problems with Fitting to the Power-Law Distribution. *Phys. Condens. Matter* **2004**, *41*. [CrossRef]
86. Alstott, J.; Bullmore, E.; Plenz, D. Powerlaw: A Python Package for Analysis of Heavy-Tailed Distributions. *PLoS ONE* **2014**, *9*, e85777. [CrossRef]
87. Lacasa, L.; Luque, B.; Ballesteros, F.; Luque, J.; Nuño, J. From time series to complex networks: The visibility graph. *Proc. Natl. Acad. Sci. USA* **2008**, *105*, 4972–4975. [CrossRef] [PubMed]
88. Xu, Z.; Liu, W.; Huang, J.; Yang, C.; Lu, J.; Tan, H. Artificial Intelligence for Securing IoT Services in Edge Computing: A Survey. Hindawi. *Secur. Commun. Netw. J.* **2020**, 8872586. [CrossRef]
89. Wang, K.; Gou, C.; Duan, Y.; Lin, Y.; Zheng, X.; Wang, F. Generative adversarial networks: Introduction and outlook. *IEEE/CAA J. Autom. Sin.* **2017**, *4*, 588–598. [CrossRef]
90. Wang, Y. A Mathematical Introduction to Generative Adversarial Nets (GAN). Available online: https://arxiv.org/abs/2009.00169 (accessed on 30 December 2020).
91. Reid, F.; Harrigan, M. An Analysis of Anonymity in the Bitcoin System. In Proceedings of the IEEE Third International Conference on Privacy, Security, Risk and Trust, Boston, MA, USA, 9–11 October 2011; pp. 1318–1326. [CrossRef]