Universidad
Rey Juan Carlos

TESIS DOCTORAL

Resilience against Intentional Risk in Blockchain Implementations using Complex Networks

Autor:
Alberto Partida Rodríguez

Directores:

Regino Criado Herrero

Miguel Romance del Río

Programa de Doctorado en Ciencias
Escuela Internacional de Doctorado

2022

D. Regino Criado Herrero, PhD

Full Professor of Applied Mathematics, Materials Science and Engineering, and Electronic Technology at Universidad Rey Juan Carlos and Director of the Institute of Data Technology, Complex Networks and Cybersecurity Sciences.

D. Miguel Romance del Río, PhD

Full Professor of Applied Mathematics, Materials Science and Engineering, and Electronic Technology at Universidad Rey Juan Carlos and Deputy Director of the Institute of Data Technology, Complex Networks and Cybersecurity Sciences.

DECLARE that the present doctoral thesis, titled 'Resilience against intentional risk in blockchain implementations using complex networks', submitted by Alberto Partida Rodríguez to obtain the title of Doctor, was carried out under their supervision within the PhD programme of Sciences in the International Doctoral School at Universidad Rey Juan Carlos in Madrid, Spain.

Madrid, May 2022

Signed: Regino Criado Herrero, PhD   Miguel Romance del Río, PhD

Acknowledgements

Regino Criado, Miguel Romance, Alejandro García del Amo, Jesús Seoane, Javier Lillo, Sergio Iglesias, Santiago Moral and all colleagues from URJC.

Silvia Cruz and Ainhoa Romero from URJC Healthy University.

Claudio J. Tessone, Francesco de Collibus and Matija Piškorec from Universität Zürich.

Saki Gerassis, Javier Taboada and Eduardo Giráldez from University of Vigo.

Diego Andina from Universidad Politécnica de Madrid.

Javier Prieto from University of Salamanca.

Osvaldo Aníbal Rosso from Cocinet, Argentina.

Raquel, Javier and Marc, who believed in me.

María Jesús, Pablo y Pablo, who built my values.

Victorina and Pablo, who made me feel loved.

My full gratitude and admiration.

I will continue learning from all of you, just one "baby step" at a time.

Abstract

Background

The title of this doctoral thesis is "Resilience against intentional risk in blockchain implementations using complex networks". It is based on four pillars of knowledge:

First, the world economy depends on data stored, processed and analysed by information systems. Keeping these systems secure is of paramount importance. All computers, from servers to handheld devices, especially those that hold databases, are valuable targets to actors with malicious intentions. They aim to obtain either some illicit benefit or to provoke disruptions. The term cybersecurity refers to computer security. Intentional risk management takes care of analysing attacks on information systems [21].

Second, complex network theory is a powerful field at the crossroad of mathematics, physics, computer science, statistics and sociology, among many other disciplines. It describes systems composed of a multitude of elements that interact with each other, mostly in a non-linear way [81, 2, 9].

Third, blockchain technology implements a distributed ledger. A ledger is a database that registers transactions between accounts. A blockchain keeps the history of exchanges as a list of records replicated in multiple locations to guarantee its integrity [116, 110]. A public blockchain allows any participant to join and leave the system at any time. Private blockchains require prior authorisation to join. This doctoral thesis studies public blockchain implementations. Bitcoin (BTC) is the pioneer public blockchain implementation that inaugurated an entire new way to approach the transfer of digital value [79]. Ethereum (ETH) is a public blockchain implementation with an advanced scripting functionality [39]. Within the realm of public distributed ledger implementations focused on the "Internet of Things" [72], IOTA [63] and IoTeX [65] are front-runners that have considerable potential to grow.

Fourth, the definition of resilience in psychology refers to the capacity to confront adversity and to get out of it reinforced. In engineering, resilience in a material reveals the capacity to absorb energy when deformed and to recover when the deforming force ceases. In this doctoral thesis, I use complex network theory [81, 2, 9] to model blockchain implementations and analyse their resilience against intentional risk.

Research objectives

I identify six research drivers in this doctoral work. The first objective of this thesis is to provide an introduction to blockchain technology to understand its applicability. The second objective is to describe public blockchain implementations that stand out in their category such as Bitcoin (BTC), Ethereum (ETH) and IoTeX to land the concept of a blockchain onto real-life applications [116]. IOTA, although it is a distributed ledger based on a directed acyclic graph (DAG), completes this description. Bitcoin [79] and Ethereum [39] are pioneers in the transfer of digital value. IOTA [63] and IoTeX [65] are two outstanding distributed ledger implementations related to the Internet of Things (IoT), IOTA is based on a DAG and IoTeX on a blockchain. The third, and broad, objective is to model blockchain and DAG implementations as complex networks to further characterise these constructs. The fourth, and specific, objective consists of modeling, using complex networks, the four implementations mentioned in the second objective, i.e., three blockchains: BTC, ETH and IoTeX, and a DAG: IOTA, to understand their growth patterns. The fifth objective is to link the complex networks that we create, out of the fourth objective, with the three key components of intentional risk [21], i.e., value, anonymity and accessibility, to secure the blockchains that these networks represent. Ultimately, the sixth, final, and highly novel objective is to pose a set of practical recommendations that would increase the resilience against intentional risk of public blockchains. Table 1 summarises the objectives of this research together with an initial classification of the type of objective.

Table 1: Research objectives.

Nr.	Objective	Type
1	Present blockchain technology	Theoretical (generic)
2	Describe outstanding public blockchain implementations	Theoretical (specific)
3	Model blockchain (and DAG) as a complex network	Analytical (generic)
4	Study complex networks in BTC, ETH, IOTA and IoTeX	Analytical (specific)
5	Link these complex networks to intentional risk parameters	Multi-disciplinary
6	Recommend actions to increase resilience against intentional risk	Practical (and novel)

Methods

This thesis uses complementary methods to achieve the proposed objectives. With regard to BTC and ETH, the first method models Bitcoin plus Ethereum as an open system of systems (SoS) of public blockchains to explain how they work. This step provides insights on how to improve their resilience against intentional risk. Second, in the case of IOTA and IoTeX, this thesis models their transactions by using complex networks. The nodes in these networks are the blockchain participants and the edges represent the transactions between them. The objective of these networks is the study of Identity and Access Management (IAM) resilience against intentional risk in blockchain-based IoT platforms. It also models BTC and ETH transactions by using complex networks to compare them with the IOTA and IoTeX networks. Equally, in this case, the nodes are blockchain participants and the edges represent transactions between them. The complex networks created from the value transactions happening in each blockchain implementation, although they are limited to brief time windows, provide insightful results.

I round up this doctoral research studying the visibility graphs (VG) of the complete IOTA and IoTeX price volatility time series. I analyse the complex networks that these series create and propose an intentional risk-based strategy to introduce 5G [51], the fifth-generation technology standard for mobile communications, whose deployment started in 2019-2021, on IoT blockchain implementations. Table 2 links the methods used in this research with the blockchain implementations that are the object of study, with the set objectives and with the research articles published in a JCR journal focused on these topics, as listed in Table 5.

Table 2: Research methods, including the blockchain implementation that is the object of study, the article in which they are applied (see Table 5) and the objectives that they cover.

Blockchain	**Method**	**Objective**
Article 1		
BTC, ETH	Model public blockchains as open SoS	1-4
BTC, ETH	Use the SoS model to improve resilience against intentional risk	5,6
Article 2		
IOTA, IoTeX	Model transactions in blockchain (and DAG) using complex networks	1-4
IOTA, IoTeX	Use these complex networks models to improve IAM resilience against intentional risk	5,6
BTC, ETH	Model transactions using complex networks to compare them with IOTA and IoTeX	1-4
Article 3		
IOTA, IoTeX	Create daily price volatility VG	1-4
IOTA, IoTeX	Use VG to analyse the impact of a technology: 5G	5,6

Results

The study of the SoS of public blockchains shows how blockchain implementations create networks that grow in complexity. In the case of BTC and ETH, they complement each other within this SoS. With regard to distributed ledger implementations in the IoT world, IOTA and IoTeX transaction networks tend to display a scale-free behaviour, although weaker than in BTC and ETH transaction networks. In mathematical terms, the degree distribution of a scale-free network follows a power law function [2, 9].

The structural analysis of IOTA and IoTeX VGs produces degree distributions that resemble a power law function for a specific range of degrees. Additionally, the plot of the average clustering coefficient per degree produces a slightly better power law fit. This result reveals a fractal, more concretely, hierarchical structure in the communities created within these VG networks. Table 3 summarises the results of this doctoral research.

Table 3: Summary of the results.

Object of study	**Results**
Open SoS of public blockchains	Blockchain implementations grow in complexity
BTC, ETH	They complement each other within this SoS
IOTA, IoTeX transaction networks	Weak power law fit in degree distribution
BTC, ETH transaction networks	Stronger signs of power law fit in degree distribution
IOTA, IoTeX daily price VGs	Signs of power law fit for some ranges in degree distribution Fractality in the originating time series Possible power law fit in average clustering coefficient per degree Communities in a hierarchical structure

Conclusions

The novelty of this doctoral work resides in the link that the author proposes between the results of the research and practical measures to increase the resilience against intentional risk of blockchain implementations. First, regarding the SoS of public blockchains, we conclude that this SoS is composed of BTC, a non-inflationary money system, and ETH, a world, financial computer system. This SoS transfers digital value and it aspires to position itself as a distributed alternative to the fiat-currency based financial system. Mass adoption of this SoS depends on its resilience against intentional risk. Value, anonymity and accessibility are useful dimensions to improve this resilience.

Second, resilience against intentional risk in blockchain requires an IAM concept that transcends a single blockchain implementation. The interplay of edge and global ledgers running on edge and cloud servers can contribute to achieve data integrity. Generally, blockchain can answer some security requirements in the IoT world.

Third, the structural analysis of the VGs of IOTA and IoTeX price series shows how both distributed ledger-based IoT platforms, being IOTA direct acyclic graph-based (DAG) and IoTeX blockchain-based, are still at an initial development stage and their VGs display a hierarchical structure. The arrival of the 5G mobile technology can accelerate the development of blockchain-based IoT platforms and contribute to improve their resilience against intentional risk. Table 4 compiles the key conclusions of this doctoral work and refers to the corresponding articles published during this

Table 4: Key conclusions.

Article	Conclusions
1	BTC and ETH in the open SoS of public blockchains: a SoS to transfer digital value This SoS aspires to be an alternative to the fiat-currency based financial system Resilience against intentional risk contributes to mass adoption
2	Blockchain answers partially IoT information security requirements A resilient blockchain requires a multi-level IAM concept based on multiple local and global ledgers running on edge and cloud servers
3	Blockchain-based IoT platforms are still in early development phases IOTA and IoTeX time series display a hierarchical structure 5G can speed up IoT related blockchain development 5G can improve resilience against intentional risk

research.

Published articles

This doctoral thesis consists of a compilation of three research articles, listed in Table 5. They all use intentional risk as the common thread. During this doctoral work, the author of this thesis has published these articles as the first author in *Electronics*, a journal indexed by JCR that, in 2020, reached an impact factor of 2.397 and a 5-year impact factor of 2.408.

Table 5: Articles that I have published, as first author, during my doctoral work, in *Electronics*, a JCR-indexed journal.

Nr.	Article title
1	Modeling Bitcoin plus Ethereum as an open System of Systems of public blockchains to improve their resilience against intentional risk [87].
2	Identity and Access Management resilience against intentional risk for Blockchain-based IoT platforms [85].
3	Visibility graph analysis of IOTA and IoTeX price series: an intentional risk-based strategy to use 5G for IoT [86].

According to the Journal Citation Indicator (JCI), the rank of this peer-reviewed journal in 2020 was the following:

- Q3 (126/223) in Computer Science, Information Systems.
- Q2 (158/319) in Engineering, Electrical and Electronic.
- Q2 (73/171) in Physics, Applied.

Similarly, with regard to the Journal Impact Factor (JIF), the rank of this peer-reviewed journal in 2020 was the following:

- Q3 (93/161) in Computer Science, Information Systems.
- Q3 (145/273) in Engineering, Electrical and Electronic.
- Q3 (88/160) in Physics, Applied.

Resumen

Antecedentes

El título de esta tesis doctoral es Resiliencia frente al riesgo intencional en redes complejas implementadas con tecnología blockchain". Se fundamenta en cuatro pilares de conocimiento. Primero, la economía mundial depende de datos que son almacenados, procesados y analizados por sistemas de información. Es esencial mantener la seguridad de estos sistemas. Cualquier computador, desde un servidor a un dispositivo móvil, en especial si alberga una base de datos, es un valioso objetivo para los cibercriminales: delincuentes informáticos que intentan obtener algún beneficio ilícito o provocar una denegación de servicio. El término ciberseguridad se refiere genéricamente a la seguridad informática, mientras que la gestión del riesgo intencional analiza los ataques a los sistemas de información [21].

Segundo, la teoría de redes complejas es un área de investigación emergente que ofrece resultados muy potentes. Se encuentra en la encrucijada entre la matemática, la física, la computación, la estadística y la sociología, entre muchas otras. Es útil para describir sistemas formados por una multitud de elementos que interaccionan entre ellos, principalmente de modo no lineal [81, 2, 9].

Tercero, la tecnología de cadena de bloques, "blockchain.$^{\text{en}}$ inglés, implementa un registro distribuido de operaciones, también llamado libro mayor de contabilidad. Este libro de operaciones es una base de datos donde se registran todas las transacciones que suceden entre distintas cuentas. Una cadena de bloques registra, una a una, todas las transacciones y replica esta lista de transferencias en múltiples localizaciones para garantizar su integridad [116, 110]. Una cadena de bloques es pública si permite a cualquier participante entrar y salir del sistema en todo momento. Por el contrario, si los participantes requieren una autorización externa para unirse a la cadena, entonces se habla de cadenas de bloques privadas. Las cadenas de bloques investigadas en esta tesis doctoral son públicas. Bitcoin (BTC), la implementación pionera de una cadena de bloques pública, inauguró una nueva forma de abordar la transferencia de valor digital [79]. Ethereum (ETH) es una implementación de una cadena de bloques pública con una funcionalidad avanzada de ejecución de secuencias de comandos, "scripting.$^{\text{en}}$ inglés [39]. Por otro lado, dentro del ámbito de las implementaciones públicas de libros distribuidos de contabilidad centrados en el Ïnternet de las cosas"[72], IOTA [63] e IoTeX [65] son proyectos pioneros con un considerable potencial de crecimiento.

En cuarto lugar, la definición de resiliencia en psicología se refiere a la capacidad de afrontar la adversidad y salir reforzado de ella. En ingeniería, la resiliencia de un material revela la capacidad de absorber energía cuando se deforma y de recuperarse cuando cesa dicha fuerza. En esta tesis doctoral, utilizo la teoría de redes complejas [81, 2, 9] para modelar las implementaciones de blockchain y analizar su resiliencia frente al riesgo intencionado.

Objetivos de la investigación

Identifico seis objetivos en esta tesis de doctorado. El primer objetivo es aportar una introducción a la tecnología blockchain para entender su aplicabilided. El segundo objetivo es describir las implementaciones públicas de blockchain que destacan en su categoría como Bitcoin (BTC), Ethereum (ETH) e IoTeX, para explicar el concepto de blockchain en implementaciones reales [116]. IOTA, aunque es una implementación basada en un grafo acíclico dirigido ("Directed Acyclic Graph.^{en} inglés, abreviado: DAG) y no en una cadena de bloques, completa esta descripción. Bitcoin [79] y Ethereum [39] son pioneros en la transferencia de valor digital. IOTA [63] e IoTeX [65] son dos destacadas implementaciones de regisgtros distribuidos relacionadas con el Internet de las Cosas (Ïnternet of Things.^{en} inglés, abreviado: IoT). El tercer objetivo es genérico: modelar implementaciones de blockchain como redes complejas para poder profundizar en su construcción. El cuarto objetivo, más específico, consiste en modelar, mediante redes complejas, las cuatro implementaciones específicas mencionadas en el segundo objetivo, es decir, tres blockchains: BTC, ETH e IoTeX, y un DAG: IOTA, para tratar sus patrones de crecimiento. El quinto objetivo es vincular las redes complejas que creamos a partir del cuarto objetivo con los tres componentes clave del riesgo intencional [21], es decir, el valor, la anonimidad (Chapela et al. prefirieron esta palabra a la de .^{a}nonimato") y la accesibilidad, para asegurar las blockchains que representan estas redes. Finalmente, el sexto y novedoso objetivo es plantear un conjunto de recomendaciones prácticas que aumenten la resiliencia contra el riesgo intencional de las blockchains públicas. La Tabla 6 resume los objetivos de esta investigación junto con una primera clasificación del tipo de objetivo.

Tabla 6: Objetivos de la investigación.

No.	Objectivo	Tipo
1	Presentar la tecnología blockchain	Teórico (genérico)
2	Describir implementaciones blockchain públicas destacadas	Teórico (específico)
3	Modelar blockchain (y DAG) como una red compleja	Analítico (genérico)
4	Estudiar las redes complejas de BTC, ETH, IOTA e IoTeX	Analítico (específico)
5	Asociar estas redes complejas con los parámetros de riesgo intencional	Multi-disciplinar
6	Recomendar acciones para aumentar la resiliencia frente al riesgo intencional	Práctico y novedoso

Metodología

En esta tesis he utilizado métodos complementarios para alcanzar los objetivos propuestos. Con respecto a BTC y ETH, primero modelo Bitcoin más Ethereum como un sistema de sistemas ("system of systems.^{en} inglés, abreviado: SoS) abierto de blockchains públicas. Este paso proporciona un marco con el que mejorar su resiliencia frente al riesgo intencional. En segundo lugar, en el caso de IOTA e IoTeX, modelo sus transacciones utilizando redes complejas en las que los nodos son cada uno de los dispositivos que participan en la blockchain y las aristas representan las transacciones entre los participantes. El objetivo de crear estas redes es implementar una gestión de identidades y accesos (ïdentity and access management.^{en} inglés, abreviado: IAM) resiliente al riesgo intencional en plataformas IoT basadas en blockchain. También modelo las transacciones de BTC y ETH utilizando redes complejas para compararlas con las redes de IOTA y IoTeX. En este caso, también los nodos representan a los participantes en la blockchain y las aristas a las transacciones entre ellos. Las redes complejas creadas por las transacciones de valor que ocurren en cada implementación blockchain, aunque representan breves ventanas de tiempo, proporcionan resultados interesantes.

Concluyo esta tesis con el estudio de los grafos de visibilidad ("visibility graphs.^{en} inglés, abreviado: VG) de las series temporales completas de volatilidad de precios de IOTA e IoTeX. Analizo las redes complejas que crean estas series y propongo una estrategia, basada en la gestión del riesgo intencional, para introducir 5G [51], la quinta generación del estándar tecnológico de comunicaciones móviles, cuyo despliegue comenzó en 2019-2021, en las plataformas IoT basadas en blockchain. La Tabla 7 enlaza los métodos que utilizo en esta tesis doctoral con las implementaciones de blockchain que estudio, los objetivos planteados y los artículos de investigación publicados en una revista científica JCR enfocada en estos temas. La Tabla 10 lista dichos artículos.

Tabla 7: Métodos de investigación aplicados en esta tesis, junto a la correspondiente implementación blockchain que es objeto de estudio, el artículo en el que se aplica dicho método (ver Tabla 10) y los objetivos de la tesis con los que se asocia.

Blockchain	**Método**	**Objetivo**
Artículo 1		
BTC, ETH	Modelar blockchains públicas como SoS abiertos	1-4
BTC, ETH	Usar el modelo de SoS para mejorar la resiliencia frente al riesgo intencional	5,6
Artículo 2		
IOTA, IoTeX	Modelar las transacciones en blockchain (y DAG) usando redes complejas	1-4
IOTA, IoTeX	Usar ese modelo de redes complejas para mejorar la resiliencia de IAM frente al riesgo intencional	5,6
BTC, ETH	Modelar las transacciones en blockchain usando redes complejas y comparar con las redes complejas de IOTA e IoTeX	1-4
Artículo 3		
IOTA, IoTeX	Crear el VG de volatilidad de precios diarios	1-4
IOTA, IoTeX	Uso de VG para analizar el impacto de una tecnología como 5G	5,6

Resultados

El estudio del SoS de blockchains públicas muestra cómo las implementaciones blockchain crean redes que crecen en complejidad. En el caso de BTC y ETH, se complementan dentro de este SoS. En cuanto a las implementaciones de libros mayores distribuidos en el mundo del IoT, las redes de transacciones de IOTA e IoTeX tienden a mostrar un comportamiento de escala libre, aunque más débil que en las redes de transacciones de BTC y ETH. En términos matemáticos, una distribución de grados de una red de escala libre sigue una función de ley de potencias [2, 9].

El análisis estructural de los VG de IOTA e IoTeX produce distribuciones de grado que se asemejan a una función de ley de potencias para un rango específico de grados. Asimismo, el gráfico del coeficiente medio de clusterización por grado produce una mejor aproximación a una ley de potencias. Este resultado revela una estructura fractal, más concretamente, jerárquica, en las comunidades creadas dentro de estas redes de VG. La Tabla 8 resume los resultados de esta investigación doctoral.

Tabla 8: Resumen de los resultados.

Objecto de estudio	**Resultados**
SoS abierto de blockchains públicas	Las implementaciones de blockchain crecen en complejidad
BTC, ETH	Se complementan dentro del SoS de blockchains públicas
Redes de transacciones en IOTA e IoTeX	Débil ajuste de ley de potencias para la distribución de grado
Redes de transacciones en BTC y ETH	Mejor ajuste de ley de potencias para la distribución de grado que en el caso de IOTA e IoTeX
VGs de precios diarios de IOTA e IoTeX	Ajuste de ley de potencias para ciertos rangos de la distribución de grado Fractalidad en la serie temporal origen del grafo Ajuste a ley de potencias para la función de coeficientes de clusterización por grado Comunidades con estructura jerárquica

Conclusiones

La originalidad de esta tesis doctoral reside en cómo su autor relaciona los resultados de la investigación con medidas prácticas para aumentar la resiliencia contra el riesgo intencional en implementaciones de blockchain. Primero, con respecto al SoS de blockchains públicas, se concluye que este SoS está compuesto por BTC, un sistema monetario no inflacionario, y ETH, un sistema informático financiero y mundial. Este SoS transfiere valor digital y aspira a posicionarse como una alternativa distribuida al sistema financiero basado en moneda fiduciaria. La adopción masiva de este SoS depende de su resiliencia frente al riesgo intencional. El valor, la anonimidad y la accesibilidad son dimensiones útiles para mejorar esta resiliencia.

Tabla 9: Conclusiones clave.

Artículo	**Conclusiones**
1	BTC y ETH en el SoS abierto de blockchains: un SoS para transferir valor digital
	Este SoS aspira a ser una alternativa al sistema financiero basado en moneda fiduciaria
	La resiliencia frente al riesgo intencional contribuye a su adopción masiva
2	Blockchain responde parcialmente a los requisitos de seguridad de IoT
	Una blockchain resiliente requiere un concepto de IAM multi-nivel basado en registros locales y globales ejecutados en servidores .$^{\text{ed}}$gez en la nube
3	Las plataformas IoT basadas en blockchain están aún en fases iniciales de desarrollo
	Las series temporales de precios en IOTA e IoTeX muestran una estructura jerárquica
	5G puede acelerar el desarrollo de blockchains para IoT
	5G puede mejorar la resiliencia frente al riesgo intencional

Segundo, la resiliencia contra el riesgo intencional en blockchain requiere un concepto de gestión de identidades (IAM) que trasciende a una única implementación de blockchain. La interacción de registros de operaciones locales y globales (.$^{\text{ed}}$ge and global ledgers.$^{\text{en}}$ inglés), que se ejecutan en servidores cercanos al usuario final (.$^{\text{ed}}$ge server.$^{\text{en}}$ inglés) y en la nube, puede contribuir a conservar la integridad de los datos. En general, en el mundo del IoT, blockchain puede responder a algunos requisitos de seguridad.

Tercero, el análisis estructural de los VG de las series de precios de IOTA, que utiliza un grafo acíclico dirigido (DAG), e IoTeX, que usa una blockchain, muestra cómo ambas plataformas de IoT se encuentran aún en una fase de desarrollo inicial y muestran una estructura jerárquica. La llegada de la tecnología móvil 5G puede acelerar el desarrollo de las plataformas de IoT basadas en blockchain y contribuir a mejorar su resiliencia frente al riesgo intencionado. La Tabla 9 recopila las conclusiones clave de esta tesis doctoral y hace referencia a los artículos correspondientes publicados durante este doctorado.

Artículos publicados

Esta tesis doctoral consiste en la compilación de tres artículos, enumerados en la Tabla 10. Todo ellos tienen al riesgo intencional como hilo conductor. Durante este doctorado, estos artículos han sido publicados en *Electronics*, una revista científica indexada por JCR que, en 2020, alcanzó un factor de impacto de 2.397 y un factor medio de impacto de los últimos cinco años de 2.408. Según el indicador de citas de revistas JCI, la clasificación de *Electronics* en 2020 fue la siguiente:

- Q3 (126/223) en Computación y Sistemas de Información.
- Q2 (158/319) en Ingeniería eléctrica y electrónica.
- Q2 (73/171) en Física aplicada.

Según el indicador de impacto de revistas (JIF), la clasificación de *Electronics* en 2020 fue la siguiente:

- Q3 (93/161) Computación y Sistemas de Información.
- Q3 (145/273) en Ingeniería eléctrica y Electrónica.
- Q3 (88/160) en Física aplicada.

Tabla 10: Artículos (en inglés) que he publicado, como primer autor, durante mi doctorado, en la revista científica *Electronics*, indexada por JCR.

Nr.	**Título del artículo**
1	Modeling Bitcoin plus Ethereum as an open System of Systems of public blockchains to improve their resilience against intentional risk [87].
2	Identity and Access Management resilience against intentional risk for Blockchain-based IOT platforms [85].
3	Visibility graph analysis of IOTA and IoTeX price series: an intentional risk-based strategy to use 5G for IoT [86].

Foreword

I have worked in this doctoral thesis during the last years under the guidance of my PhD directors, Regino Criado and Miguel Romance, both Professors at the Department of Applied Mathematics in the URJC. I devoted my research to the study of public blockchain implementations by using complex network theory with the ultimate objective to provide practical recommendations on how to increase their resilience against intentional risk. For this purpose, I have compiled the results of this doctoral work in three articles that I have published in *Electronics*, a JCR-indexed journal. I first research Bitcoin (BTC) and Ethereum (ETH), the two most relevant public blockchain implementations, at least up to 2022, as complementary holons within a System of Systems (SoS). Second, I analyse the transaction networks of BTC and ETH, together with IOTA and IoTeX, two outstanding distributed ledger-based Internet of Things (IoT) platforms, to focus on Identity and Access Management (IAM) aspects. Third, I use visibility graphs (VG) to study IOTA and IoTeX price time series as complex networks and to show how 5G, the mobile technology, could contribute to their development. In all these three research paths, I link the conclusions that I obtain with the resilience against intentional risk of public blockchain implementations. This doctoral thesis is structured as follows:

Chapter 1. Introduction

This chapter explains the motivation for this doctoral thesis: how to manage intentional risk in blockchain implementations. First, it outlines its main ingredients. Second, it presents the objectives that I set for the published articles and how these pieces of research connect with each other. Third, it describes the structure of this work and it shares the collection of additional investigation activities that I have performed during this doctoral thesis. Fourth, it includes a section that deals with the origin of each of the eight main recipe ingredients that constitute my doctoral thesis.

Chapter 2. State of the art

This chapter presents a helicopter view of the current knowledge related to the eight objects of study of this doctoral thesis and how they are interlinked. They are blockchain, complex networks analysis, system of systems engineering (SoSE), identity and access management (IAM), visibility graphs (VG), internet of things (IoT), 5G and intentional risk.

Chapter 3. Methodology and implementation

The third chapter presents the methodologies used in each of the published articles and how they are implemented using real data. Additionally, it finds common patterns in the proposed methodologies and it links all of them as components of a general framework to study intentional risk in blockchain implementations by using complex networks.

Chapter 4. Modeling Bitcoin plus Ethereum as an open System of Systems of public blockchains to improve their resilience against intentional risk

This chapter reproduces verbatim the article on how to model Bitcoin plus Ethereum as an open System of Systems of public blockchains to improve their resilience against intentional risk. This article was published in January 2022 in the Special Issue on the 10^{th} Anniversary of Electronics: Advances in Networks of the peer-reviewed and JCR-indexed MDPI journal *Electronics* [87].

Chapter 5. Identity and access management resilience against intentional risk for blockchain-based IoT platforms

This chapter displays verbatim the article on identity and access management resilience against intentional risk for blockchain-based IoT platforms. This article was published in February 2021 in the Special Issue on IoT Security and Privacy through the Blockchain of the peer-reviewed and JCR-indexed MDPI journal *Electronics* [85]. After publication, the article was declared "Editor’s choice".

Chapter 6. Visibility graph analysis of IOTA and IoTeX price series: an intentional risk-based strategy to use 5G for IoT

This chapter shares verbatim the article on visibility graph analysis of IOTA and IoTeX price series: an intentional risk-based strategy to use 5G for IoT. This article was published in September 2021 in the Special Issue on Blockchain for 5G and IoT: Opportunities and Challenges the peer-reviewed and JCR-indexed MDPI journal *Electronics* [86].

Chapter 7. General discussion

This chapter consolidates all results from the published articles and links them with the stated objectives.

Chapter 8. Conclusions

This chapter presents the main conclusions of this doctoral thesis.

Chapter 9. Future research

This chapter suggests future research paths.

Chapter 10. References and bibliography

This chapter shares the list of sources referred and consulted for this research work.

Appendix A. Blockchain and information security

This appendix provides, first, a summary with the most relevant complex network features identified in stable blockchain implementations. Second, it presents a collection of information security design patterns and good practices that, if implemented, could have mitigated the impact of the security incidents analysed in the article on IAM resilience in IoT platforms [85], included in this thesis. Third, it proposes a brief questionnaire that both technologists and investors could use to create an initial "business card" for each blockchain project that they need to assess.

Appendix B. A blockchain proposal to answer five key use cases: Socioblock

This last appendix presents Socioblock: a public but permissioned blockchain implementation proposal that contributes to a decentralised society. It is based on some of the security patterns presented in Appendix A. Finally, it describes five specific use cases of Socioblock: self-sovereign identities, ad-hoc insurance, self-sovereign medical records, exchange of academic records and mortgage search.

Keywords

Blockchain, complex networks theory, intentional risk, resilience, system of systems engineering, identity and access management, Internet of Things, visibility graph, 5G, Bitcoin, Ethereum, IOTA, IoTeX.

Contents

List of Figures

List of Tables

List of Acronyms

API	Application programming interface
AI	Artificial intelligence
BCE	Before Christian Era
BIP	Bitcoin improvement proposal
BTC	Bitcoin
CA	Certification authority
CCDF	Complementary cumulative distribution function
DAG	Directed acyclic graph
DApp	Distributed application
DeFi	Decentralised finance
EIP	Ethereum improvement proposal
ERC	Ethereum request for comments
ERC20	Ethereum requests for comments Nr. 20. Technical smart contract standard in Ethereum to implement fungible tokens
ETH	Ethereum
EU	European Union
EUR	Euro
FNMT	Spanish Mint. Fábrica Nacional de Moneda y Timbre
GAN	Generative adversarial networks
Gbps	Gigabits per second
GDPR	General Data Protection Regulation
HVG	Horizontal visibility graph
IAM	Identity and access management
ILP	Interledger protocol
IOC	Indicator of compromise
IoT	Internet of things
IOTA	IoT DAG-based distributed ledger implementation
IoTeX	IoT blockchain-based implementation
IR	Intentional risk
IS	Information system
IT	Information technology
JCI	Journal citation indicator
JIF	Journal impact factor
JCR	Journal citation reports
KYC	Know your customer

LCC	Largest connected component
ML	Machine learning
NGO	Non governmental organisation
PAR	Profitability associated to the attacker
PDF	Probability density function
PKI	Public Key Infrastructure
PoW	Proof of work
RA	Registration authority
SOA	Service oriented architecture
SoS	System of systems
SoSE	System of systems engineering
SWOT	Strengths, weaknesses, opportunities and threats
URJC	Universidad Rey Juan Carlos. King Juan Carlos University
US	United States of America
USD	United States Dollar
UZH	University of Zurich
VG	Visibility graph, also called natural visibility graph
WBTC	Wrapped Bitcoin, an ERC20 token

1. Introduction

This introductory chapter explains the motivation for this research, the objectives of this doctoral thesis and the organisation of the work that I have carried out.

1.1 Motivation for this research

1.1.1 Weaving together eight study lines

This research starts off a journey towards more informed decisions to increase resilience against intentional risk in blockchain implementations with the invaluable help of complex network analysis. I propose an original way to weave together these eight lines of research: blockchain-based distributed database implementations, complex network analysis, system of systems engineering (SoSE), identity and access management (IAM), visibility graphs (VGs), Internet of Things (IoT), 5G and intentional risk management.

1.1.2 A new recipe

This research work focuses on blockchain technology and analyses blockchain implementations by using complex networks. Particular attention goes to disciplines such as SoSE, IAM, VGs and intentional risk, and to realms such as IoT and 5G, as well. Using a gastronomic image, the mission of this PhD dissertation is to create a new dish based on eight ingredients, each of them as interesting and novel as the other seven. This new dish is not designed exclusively for *haute cuisine* "information security" chefs but for curious "cybersecurity" cooks at a broad range of locations. These are the selected ingredients:

- The arrival of a new technology: blockchain. A promising distributed database construct that guarantees integrity and redundancy through decentralisation [110]. It changes the way human beings create and keep digital value [116]. It brings along the unveiling of an Internet of value that is currently powering a myriad of business cases in fields such as crypto-assets [79, 39], the Internet of Things (IoT) [63, 65] and financial technology (fintech), i.e., technology firms that leverage technology to offer novel financial value propositions.

- A powerful mathematical tool: The use of complex networks analysis to model connected information systems that show non-linear complexity [81, 2, 9]. A toolkit at the crossroad of mathematics, statistics and physics to better understand network features and dynamics.

- A complexity management instrument: SoSE. It helps describing "supersystems", i.e., complex systems comprised of elements, named holons, that are systems themselves and interact between each each other [67, 68, 7].

- A security instrument: Identity and access management is the tool to ensure that the right entities (authentication) have access to the right systems and information (authorisation). Most business models and their underlying information systems require identification, authentication and authorisation services for the user entities [82].

- An imaginative algorithm to associate time series with complex networks so that network theory properties can contribute to describing the initial time series: a visibility graph (VG) [73, 77].

- A network over the Internet: the Internet of Things (IoT) consists of a multitude of devices, mostly sensors and actuators, that act as interfaces between the physical and the digital world, plus their corresponding servers, that process related data [72].

- A mobile technology: 5G. A fifth-generation technology standard that brings a higher bandwidth and a lower latency than in previous versions to mobile networks [51].

- A novel theory, intentional risk management, on how to deal with attacks to information systems by ill-intentioned actors aiming to obtain benefit, is an increasingly relevant field [21]. The world economy and human communities depend on information systems and, ultimately, on their cybersecurity. The objective of cybersecurity is to protect those systems and hence the information stored in them from intentional attacks, making them more resilient [82].

With the combination of these eight unique elements, this thesis proposes a *modern cuisine* "cybersecurity" dish that brings light to improvements in the resilience against intentional risk in the complex networks created by blockchain implementations such as Bitcoin (BTC) [79] and Ethereum (ETH) [39] and by two IoT platforms such as IOTA [63] and IoTeX [65].

1.2 Objectives

The objectives that I set for this doctoral thesis rotate around the title of this thesis: **resilience against intentional risk in blockchain implementations by using complex networks**. The way I approach this research is from the big picture of an overall objective, that coincides with this title, to a series of more specific objectives, focused on particular blockchain implementations. I achieve each of these objectives through the publication of three peer-reviewed articles in *Electronics*, a JCR-indexed journal with an impact factor in 2020 of 2.397. Table 1.1 lists the research objectives together with the corresponding published articles.

Table 1.1: Mapping research objectives to published articles.

Nr.	Research objective	Article
1.2.1	Facilitate understanding of BTC and ETH	[87]
1.2.2	Improve IAM resilience against intentional risk in blockchain	[85]
1.2.3	Create an intentional risk-based strategy for blockchain	[86]

1.2.1 Facilitate understanding of BTC and ETH

To build the big picture, I first formulate a SoS that transfers digital value and aspires to position itself as a distributed alternative to the traditional fiat currency-based financial system. More concretely, I focus on modeling BTC and ETH as system elements in an open SoS of public blockchains. The aim is to better understand the role of public blockchains in society and how they can be resilient against intentional attacks. BTC and ETH are the most capitalised, at least until March 2022 [23], blockchain-based cryptocurrencies. The paper titled "modeling Bitcoin plus Ethereum as an open System of Systems of public blockchains to improve their resilience against intentional risk" [87], published in 2022, achieves this first objective.

1.2.2 Improve IAM resilience against intentional risk

A second, more specific, objective focuses on how identity and access management (IAM) can stand as a key security requirement to build resilience against intentional risk in blockchain. To that end, I research blockchain-based IoT platforms. Adjacent to this, I study how blockchain can answer some of the security requirements on IoT platforms. The paper titled "identity and access management resilience against intentional risk for blockchain-based IoT platforms" [85], published in 2021, meets this second objective.

1.2.3 Create an intentional risk-based strategy

The third objective is to shape a set of security recommendations within an intentional risk-based strategy. To put this strategy in context, I focus on how 5G, the new mobile telephony technology, can improve information security in the two most capitalised, at least until March 2022 [25], IoT platforms that use a distributed ledger, i.e., IOTA and IoTeX. For this, I research their price series using visibility graphs (VGs). The paper with the title "visibility graph analysis of IOTA and IoTeX price series: an intentional risk-Based strategy to use 5G for IoT" [86], published in 2021, fulfils this

third objective.
Table 1.2 maps the objectives set in the original research plan, and stated in Table 1, with the objectives that I finally undertake in this doctoral work.

Table 1.2: Mapping research plan objectives to undertaken objectives.

Resilience against Intentional Risk in Blockchain implementations using Complex Networks		
Nr.	**Research plan objective**	**Accomplished by**
1	Present blockchain technology	1.2.1
2	Describe outstanding public implementations	1.2.1, 1.2.2
3	Model blockchain as a complex network	1.2.1, 1.2.2
4	Study complex networks in BTC, ETH, IOTA and IoTeX	1.2.1, 1.2.2
5	Link these complex networks to intentional risk parameters	1.2.1, 1.2.2, 1.2.3
6	Recommend actions to increase resilience against intentional risk	1.2.1, 1.2.2, 1.2.3

1.3 Research structure

1.3.1 This doctoral thesis

This doctoral thesis leads up to the completion of my PhD research work. I structure this thesis by compilation of the articles listed in Table 1.3. The common thread in all of them is the question of how to improve resilience against intentional risk. After this introduction, Chapter 2 provides an overview of the state of the art in each of the eight ingredients that I propose in Section 1.1.2. In Chapter 3, I present the key points of the methodology that I use to achieve each of the objectives and its implementation. Subsequently, Chapters 4, 5 and 6 reproduce verbatim each of the published articles. Chapter 7 consolidates the results from the published articles as learning points while Chapter 8 summarises the key conclusions and Chapter 9 hints some future research paths. A final chapter lists the references used in this thesis. Appendix A provide additional information on blockchain and information security, including security design patterns. Finally, Appendix B suggests a public blockchain project, including four use cases.

Table 1.3: Articles that I have published as first author in *Electronics*, a JCR-indexed journal, for this thesis.

Nr.	**Article title**	**Journal**
1	"Modeling Bitcoin plus Ethereum as an open System of Systems of public blockchains to improve their resilience against intentional risk" [87].	MDPI Electronics
2	"Identity and Access Management resilience against intentional risk for Blockchain-based IoT platforms" [85].	MDPI Electronics
3	"Visibility graph analysis of IOTA and IoTeX price series: an intentional risk-based strategy to use 5G for IoT" [86].	MDPI Electronics

1.3.2 Additional research activities

In addition to the articles mentioned in Table 1.3, during this doctoral thesis, I also took active part in other research activities related to blockchain and complex networks. Table 1.4 summarises them, including the type of academic activity and date.

Table 1.4: Additional research work during this thesis.

Activity	Title	Year
Talk	"A simulation of a Bitcoin blockchain based on a pseudo-randomly selected block". 15th Experimental Chaos and Complexity conference [83].	2018
Poster	"On Identity Management in blockchain implementations". Manifesting Intelligence Conference 2020 [84].	2020
Poster	"Heterogeneous preferential attachment in Ether and key Ethereum-based tokens". International Conference on Complex Networks [30].	2021
Article	"Heterogeneous Preferential Attachment in Key Ethereum-Based Cryptoassets." Frontiers in Physics Journal [32]. Rank by JIF: Q2 in Physics, JCR impact factor in 2020: 3.560. Joint work with the Blockchain Center at University of Zurich (UZH).	2021
Chapter	"The role of smart contracts in the transaction networks of four key DeFi-collateral Ethereum-based tokens". Complex Networks & their applications X. Conference proceedings, published by Springer [31].	2022

1.4 Origin of the main objects of study

This section presents the roots for each of the eight ingredients listed in Section 1.1.2, key for the elaboration of this doctoral thesis.

1.4.1 Blockchain

Planet Earth took shape around 4.5 billion years ago [48]. The first humans that used some stone tools appeared 2.5 million years ago [48]. The oldest evidence of proto-writing, the use of ideographic and mnemonic symbols to convey information, appears in the Bronze Age (3300 BCE to 1200 BCE, i.e., Before Christian Era). There is evidence that human beings have been using writing since then. In fact, the origin of writing is economic [29]. The will to record events and transactions is a fundamental human trait. Ancient Mesopotamian pictographic tablets around 3200 BCE already recorded quantities of items on clay tablets [28], acting as primitive ledgers. A ledger is a book of transactions documenting incoming and outgoing transfers of an asset. Typical first assets were, e.g., cereal grains, and, later on, tokens and coins [29]. Throughout History, bookkeeping has been mainly a centralised activity. It is still pivotal for our economic activities. The data registered in a ledger need to be highly available for all stakeholders. A typical strategy by human beings to guarantee data availability is to keep several copies of that data. Blockchain technology achieves this availability. It consists of a growing list of records: a distributed database maintained by nodes that participate in a network [116, 110]. A high number of participant nodes keep a copy of the growing list of records. These records are mainly transactions between participants in the network. They confirm sets of transactions organised in blocks. These blocks are chained, i.e., linked together, via cryptographic means to guarantee immutability. Therefore the name *blockchain*: a decentralised way to keep a ledger. David Chaum's 1979 vault system can be considered one of the first proposals of a public distributed record-keeping system [98]. However, the seminal paper on Bitcoin by Satoshi Nakamoto brings blockchain to the spotlight, although it does not mention literally the word "blockchain" [79].

1.4.2 Complex networks

Reductionism and the modeling of non-linear phenomena using linear models have been key strategies in physics to understand many systems of interest [27, p.4]. However, there are many non-linear systems in the real world that cannot be characterised by linear approaches. They require newer and more integrating approaches such as the one that complex network analysis offers. 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). By that time, graph theory was dealing with static graphs, i.e., with a permanent structure.

The study of building graphs with a high number of nodes has led to different models. Paul Erdős and Alfréd Rényi in 1959 [36, 27, p.4] presented a model to construct random networks but assuming that the network had a fixed number of nodes, i.e, not considering growth. In a random network of N nodes (or vertices), new connections, also called edges (or links), are created with uniform probability between any pair of nodes. Random networks are characterised by a normal degree distribution [12, section 2], where the degree of a node represents the number of connections that it has. This type of network is not commonly found in natural structures, as Albert et al. concluded in 1999 [8] when they created a model to generate scale-free networks via preferential attachment, i.e., not all edges are equally likely, in network growth processes. When sociologists and physicists 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 [1].

1.4.3 System of systems engineering

Traditionally, systems engineering helps understanding systems. A system is a group of elements that act as an entity, following some principles, with a specific purpose, and interacts with the environment. When the components that constitute a system are systems themselves, then the degree of complexity is greater and "system of systems" engineering comes into play [67]. These "supersystems", also called "networks of networks", started to be objects of study in the early 2000s. The US Department of

Defence, the air transportation network and the continental power grid are examples of SoS [68]. For instance, the "supersystem" of the US Department of Defence is composed of different systems such as the Air Operations Center and the Navy Operations Center, all of them independent systems with a common purpose: defending a nation. Additionally, their interaction among them and with their environment create emergent properties.

1.4.4 Identity and access management

The concept of identity as any quality to uniquely characterise an individual or community is closely linked to private property. For a member of a community to claim ownership of an object, they would need to get the association of their identity with the right to own that object, accepted by the community. In the digital world, identities are one of the five elements to secure, i.e., networks, data, systems, applications and identities [82]. Access to specific data will be a variable depending on the identity of the user and the access rights they might have. IAM is, consequently, a key requirement to transfer and hold digital value.

1.4.5 Visibility graphs

The registration of a series of data points ordered along time creates a time series in mathematics. Time series analysis describes these data points and tries to foresee their future values. In 2008, Lacasa et al. came up with the idea to use visibility graphs (VGs) to transform a time series into a complex network [73]. They identified specific one-to-one relationships between the type of time series and the properties of complex network [73]. VGs are useful instruments to link time series with complex networks. In this way, complex network analysis helps identify particular features present in time series.

1.4.6 Internet of Things

During the 1990s, Internet users started to browse the first web servers and to send their first emails. Researchers and first-time web publishers exchanged information using Internet protocols. The growing pervasiveness of the Internet triggered, since the early 2000s, the connection of a multitude of small devices, such as sensors and actuators, with their corresponding data servers, via the Internet. Those were the early days of the Internet of Things (IoT) [85, 86]. Since then, the personal, home and industrial use of IoT devices grows non-stop, reaching the figure of 50 B connected devices already in 2018 [72].

1.4.7 5G technology

One of the social characteristics of human beings is our need to communicate. Technology has played a pivotal role in our remote communications. First, the telegraph and second, the telephone, changed the way human interactions take place. The arrival of the mobile telephony in 1980 multiplied our communication possibilities. There was no further need to be close to a fixed phone connected to a land line [51]. All successive generations of mobile telephony have introduced a better sound quality based on a broader bandwidth, a lower latency and a faster transmission speed. 5G refers to the fifth-generation cellular technology standard whose deployment started in 2019-2021. 1 Gbps transmission speed and 30 ms latency are real, achievable figures using 5G [86].

1.4.8 Intentional risk

On one hand, resource scarcity is a constant parameter that has accompanied human beings since their appearance on planet Earth. On the other hand, free will in human beings, understood as the capacity to select which action to undertake, provides a degree of freedom. The combination of these two elements creates the risk of a specific human actor to start off an activity that could give them access to more resources, however using illicit or unethical means. This is the origin of intentional risk. Those ill-intentioned actors are called adversaries. Military defence theory has studied them profoundly [82]. In 2016, Chapela et al. suggested a novel way to manage information security based on intentional risk [21].

2. State of the art

This chapter provides a helicopter view to the body of knowledge existing in each of the topics present in this doctoral work. Blockchain, complex network analysis and intentional risk are the three most relevant subjects. Systems of systems engineering, identity and access management, visibility graphs, internet of things and 5G complete the list of research fields.

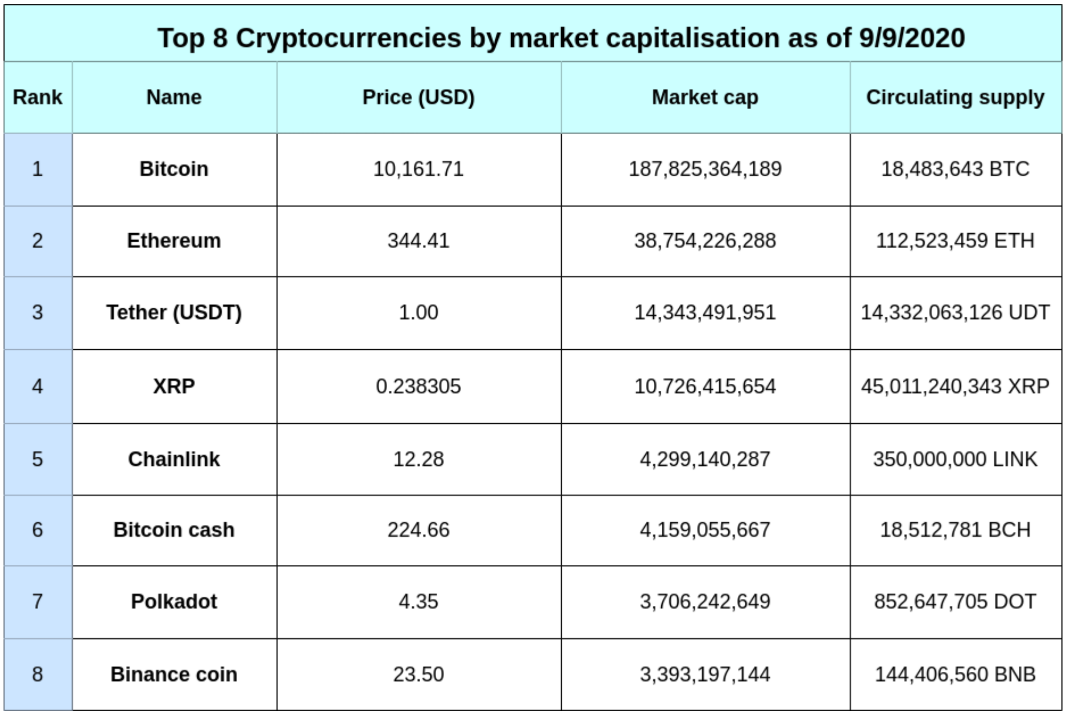
2.1 Blockchain

2.1.1 A distributed database

Blockchain finds its roots in cryptography and distributed systems [116]. It follows a simple motto, i.e., "**the longest chain wins**". It is a type of database that stores a number of records in a block [110, p.17]. Each block is unequivocally linked to the following block using cryptographic means [110, p.17]. Out of many other use cases, this technology can create a ledger, i.e., a book consisting of a chain of linked blocks with records that represent financial transactions or any other event that is worth registering permanently. Although Catalini et al. mention the cost of verification and the cost of networking as two fundamental challenges for blockchain technologies [19], their future, and even their present, is promising. Articles related to blockchain implementations are numerous. Some of them include use cases related to finance [33, 37, 89], e-government services [54], digital product, i.e., non-fungible token, distribution [22], identity management [54, 85], legal contracts [54], health data [49], land registry [10], car parts logistics [71], cybercrime and illegal marketplaces [103] and even dating [97], among many others. The list of applications grows almost daily, as there is a myriad of activities that would benefit from decentralised data integrity.

2.1.2 Bitcoin and Ethereum

Undoubtedly, the most popular and capitalised [23] blockchain implementation is the peer-to-peer electronic cash system Bitcoin (BTC), proposed by the pseudonym Satoshi Nakamoto [79]. After Bitcoin, the second cryptocurrency in terms of market capitalisation, at least until March 2022 [23], is Ethereum (ETH). Like BTC, ETH is an open-source, public, permissionless blockchain-based distributed computing plat-



Top 8 Cryptocurrencies by market capitalisation as of 9/9/2020				
Rank	**Name**	**Price (USD)**	**Market cap**	**Circulating supply**
1	**Bitcoin**	10,161.71	187,825,364,189	18,483,643 BTC
2	**Ethereum**	344.41	38,754,226,288	112,523,459 ETH
3	**Tether (USDT)**	1.00	14,343,491,951	14,332,063,126 UDT
4	**XRP**	0.238305	10,726,415,654	45,011,240,343 XRP
5	**Chainlink**	12.28	4,299,140,287	350,000,000 LINK
6	**Bitcoin cash**	224.66	4,159,055,667	18,512,781 BCH
7	**Polkadot**	4.35	3,706,242,649	852,647,705 DOT
8	**Binance coin**	23.50	3,393,197,144	144,406,560 BNB

Figure 2-1: Cryptocurrencies market capitalisation [23]. Date: 9/9/2020

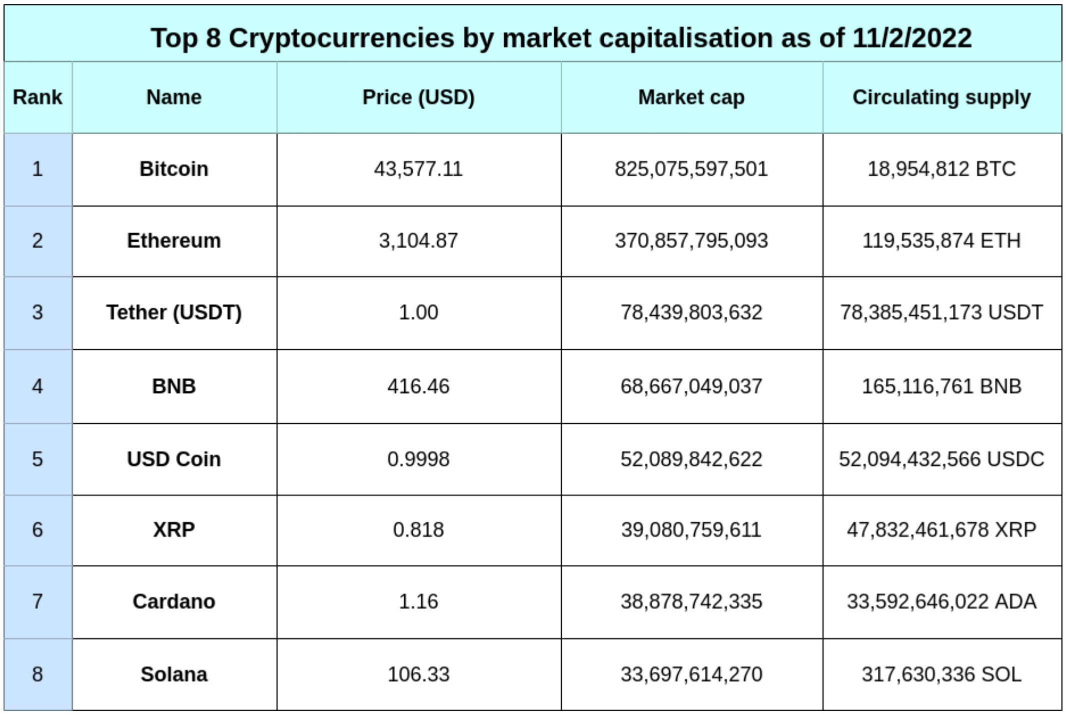
form. Additionally, it features smart contracts, i.e., scripting functionality, and it provides a decentralised Turing-complete virtual machine [39].

2.1.3 A myriad of cryptocurrencies

The list of available cryptocurrencies continues growing. The creation of a new blockchain project, together with a new token, making use of open-source software, is a real possibility, especially for seasoned code developers [115]. Equally, the inception of a new cryptocurrency as an ERC20 token on top of ETH, using open-source software, is also feasible. Being still a pretty immature market, the price of cryptocurrencies in fiat currencies, such as USD and EUR, is still highly volatile. Proof of it is that, apart from the top two cryptocurrencies, BTC and ETH, the list of the top eight most capitalised coins has changed considerably in only 17 months between September 2020 and February 2022, both in terms of coins and prices. Figures 2-1 and 2-2 display a snapshot from 9 September 2020 and 11 February 2022 of the top eight cryptocurrencies according to their market value [23].

2.1.4 The power of the blockchain nodes

The distributed nature of blockchain is funded on the existence of a multitude of nodes that keep a trustworthy copy of the database [74, part 1]. The number of nodes in widely used blockchain implementations, such as Bitcoin and Ethereum, is high [87] and they interact between each other. These numbers and in-



Top 8 Cryptocurrencies by market capitalisation as of 11/2/2022

Rank	Name	Price (USD)	Market cap	Circulating supply
1	**Bitcoin**	43,577.11	825,075,597,501	18,954,812 BTC
2	**Ethereum**	3,104.87	370,857,795,093	119,535,874 ETH
3	**Tether (USDT)**	1.00	78,439,803,632	78,385,451,173 USDT
4	**BNB**	416.46	68,667,049,037	165,116,761 BNB
5	**USD Coin**	0.9998	52,089,842,622	52,094,432,566 USDC
6	**XRP**	0.818	39,080,759,611	47,832,461,678 XRP
7	**Cardano**	1.16	38,878,742,335	33,592,646,022 ADA
8	**Solana**	106.33	33,697,614,270	317,630,336 SOL

Figure 2-2: Cryptocurrencies market capitalisation [23]. Date: 11/2/2022

teractions make the use of complex network techniques to study blockchain advisable. Typically, nodes are blockchain participants, i.e., Bitcoin and Ethereum addresses, and edges represent transactions between them [75, 69, 44, 11]. The higher the number of nodes, i.e., participants, the higher the degree of distribution and, therefore, of trust on a blockchain implementation. The common interest and, subsequently, the honesty of the majority of participants play a pivotal role in this type of distributed networks that lack a central authority. In blockchain, more than 50% of the participants would need to collide on an illegitimate intent (collusion) to compromise the network. However, the more nodes in the network, the higher the computing power (hash power) required to create (mine) blocks and, consequently, the more hash power needed to control over 50% of it. Chapela et al. propose a link between intentional risk [21, p.2] and Game Theory [21, p.5]. References such as Houy [53] suggest as well a link between mining incentives and Game Theory in large blockchain networks.

2.1.5 Data integrity and double-spending protection. Block mining

Data integrity in the blockchain database, i.e., the guarantee that transactions are not fraudulently modified, comes from the use of block content hashing and public key cryptography. Double-spending avoidance, i.e., **the absence of double entries in the blockchain comes from effective time stamping and consensus-making algorithms**. Only the first transaction reaching the chain is accepted [79, p.2]. Participant blockchain nodes need to agree on a single history of events. Hence the importance of reaching an "honest" consensus in the network. Once a block is finalised and accepted by most market participants, over 50%, it is cryptographically immutable. This is known as blockchain mining. The word mining can be misleading. The author or authors behind the pseudonym of Satoshi Nakamoto do not mention it in their original paper. In the blockchain world, the process followed by the nodes to keep the network operational can be incentivised both by transaction fees and just-created block rewards, e.g., in the form of new currency, like in the case of Bitcoin [41].

2.1.6 Bitcoin

Without mentioning the word blockchain at all, Satoshi Nakamoto in 2008 describes an ongoing chain of hash-based “proof of work” (PoW) [79, p.1]. This is the heart of a purely peer to peer version of electronic cash, widely known by the name of Bitcoin (BTC). It combines three powerful artifacts: **the blockchain technology, a distributed peer-to-peer network and a fully decentralised consensus-based approach based on “proof of work”** [112].

Financial activity on public blockchains grows year on year. Böhme et al. (2015) use also the word Bitcoin to refer to the online communication protocol that facilitates the use of the homonimous virtual currency [17, p.213]. However, investor interest is focusing not only on Bitcoin but also on other blockchain implementations [41, 95]. As a result of that, already in 2016 Q1 blockchain funding overtook Bitcoin funding [52].

Figure 2-3 shows how the daily closing price of Bitcoin in USD was a single-digit, or maximum two-digit, integer during its early years. This price first reached a three-digit integer on 1/4/2013. BTC prices started highly volatile periods in the second half of 2017 and, even more markedly, in 2021, reaching over USD 61000 on 13/3/2021 and USD 65000 on 14/11/2021. The steep increase in the price of Bitcoin and its high volatility makes it a highly speculative asset for some investors. This behaviour contrasts with its initial purpose of being just a coin to facilitate digital transactions [79].

Nonetheless, Bitcoin is anti-inflationary: the total number of coins that can be mined is limited to almost 21 million BTC. This fact makes some cryptocurrency owners consider Bitcoin storage of value, similar to precious metals such as gold, platinum or silver. Already in 2017, Bouri et al. confirmed that Bitcoin acts as a hedge against uncertainty in short investment horizons [16]. Those who keep their Bitcoins are called *"hodlers"*. They hope that Bitcoin unit value, compared with physical currencies such as USD and EUR, will continue to grow. **These investors consider Bitcoin as a digital value reserve, i.e., "the digital Gold"** [87]. In the long term, this can pose a threat to Bitcoin’s transactional value proposition: Satoshi Nakamoto’s original Bitcoin paper’s title was "a peer-to-peer electronic cash system" [79].

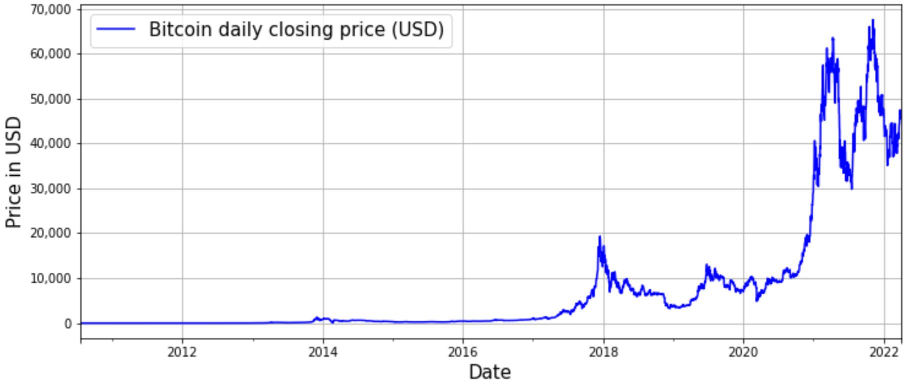


Figure 2-3: Bitcoin daily closing price in USD since early days in 2010. Price data from *investing.com* [58].

2.1.7 Bitcoin nodes

There are two types of nodes in the Bitcoin network: full nodes and lightweight nodes. Full nodes mine Bitcoins. **Mining consists of keeping the overall transaction record updated and operational** [17, p.217]. In 2017, more than 50% of mining pools were located in China [106, 45]. In 2020, this percentage was close to 80%. After China's BTC mining ban in July 2021, mining pools exited China and in August 2021 U.S reached 35.4% and Kazakhstan 18.1% BTC mining power [106]. Full nodes receive income via both transaction fees and reward Bitcoins when a new block is successfully mined [53]. The reward for mining, i.e., the number of coins generated per block, decreases geometrically, with a 50% reduction (halving), every 210000 blocks, i.e., almost every four years. There is a finite number of BTCs: it almost reaches 21 million. This amount of BTC will probably be reached around 2140. The BTC mining rate adapts to the available hash rate so that a block takes around 10 minutes to be mined. Once all coins are mined, full nodes will only receive income to pay for their computing resources via transaction fees [18]. Computing resources are devoted to creating the "proof of work" (PoW). Satoshi Nakamoto refers to it as the need "to determine representation in majority decision making" [79, p.3]. In other words, **the miners signal that they have a vested interest in mining a block by devoting computing power to it**. "Proof of work" is highly energy intensive. There are alternatives to "proof of work", e.g., Marko Vukolić proposes to replace "proof of work" with Byzantine Fault Tolerance (BFT) replication [107].

Bitcoin lightweight nodes do not mine blocks nor store the entire transaction history, however, they can verify transactions following the Simplified Payment Verification (SPV) based on Merkle trees. A hash tree or Merkle tree is a tree of hashes that links a transaction to the block in which it is timestamped [79, p.3]. Bitcoin lightweight nodes require less resources: they just need the chain of block headers to operate [56]. Lightweight nodes participate in the Bitcoin network but they do not receive incentives. Their reliance on an honest network is higher than for full Bitcoin nodes. In

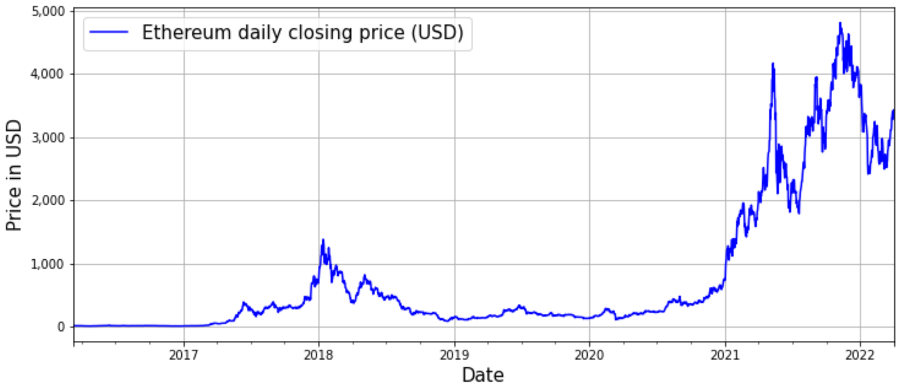


Figure 2-4: Ethereum daily closing price in USD since early days in 2016. Price data from *investing.com* [59].

March 2022, and thanks to its distributed design features, **the Bitcoin network has been permanently available since its inception in January 2009**. The forks performed in the Bitcoin blockchain so far were not due to mitigating a fraudulent use nor there has been double-spending.

2.1.8 Ethereum

Blockchain technology provides a distributed database that keeps an incontestable history of transactions or events [78, slide 2]. Industries, such as finance and insurance, are piloting blockchain-based implementations. The potential applicability of blockchain technologies transcends these two economically relevant sectors. Ethereum is possibly the clearest example of a public blockchain platform that is being used for very different use cases.

Conceived in 2013 and launched in 2015, Ethereum has implemented a blockchain-based *"Turing-complete"* machine [38]. A programming language is Touring-complete if it can simulate any Turing machine. A Turing machine is able to recognise and decide on data manipulation rule sets. In practice, a programming language with conditional branching and the ability to change an amount in memory is Touring-complete [91]. Ethereum provides a blockchain-based platform to run decentralised applications named "smart contracts" [39]. It deals with rule-based states rather than only with financial transactions. **A contract in Ethereum is a programmable autonomous agent**. Figure 2-4 shows ETH price volatility periods starting in the second half of 2017 and, especially, in 2021, similarly to BTC, as Figure 2-3 indicates.

2.1.9 Ethereum nodes

Any node participating in the Ethereum network can be a miner [38]. **On average, each 10 minutes, Bitcoin solves a block and creates a new one, whereas Ethereum produces a new block each 15 seconds**. This shorter time reduces dramatically the possibility to find double-spending in the network, as consensus is reached more quickly. Ethereum consensus model is based on ”proof of work” as BTC, although ”proof of stake” has been already announced and the plan is to move Ethereum to "proof of stake" by H2 2022 [26]. Ethereum nodes are rewarded both for successful mining but also for "uncle blocks", contrary to the lack of rewards in BTC for orphaned blocks. When two or more blocks in Ethereum are created almost simultaneously, only one of them will be mined and reach the ledger in the blockchain. The rest of the blocks are called "uncle blocks" [62]. Ethereum applies a multi-currency ecosystem: Ether and gas. Rewards are in the form of Ether. Execution fees in Ethereum are called gas. This internal currency distinction is meant to keep execution costs somehow stable even if the value of Ether increases.

2.2 Complex networks analysis

2.2.1 From graph theory to complex network theory

Section 1.4.2 mentions that Euler initiated graph theory in 1736. However, more recently, the origin of complex network theory dates back to 1999, when Réka Albert and Albert-László Barabási developed their Barabási-Albert model [8, 27, p.8] to generate random **scale-free networks, i.e., networks that display a power law function as their degree distribution**, in which few nodes display a high degree compared with the rest of the nodes. **The degree of a node corresponds to the number of edges that link it**. Albert and Barabási realised that many observed natural networks, such as protein interactions, and human-made ones, like Internet connections or social networks, did not follow the random graph model described by Paul Erdős and Alfréd Rényi in 1959 [36, 27, p.4], nor the Watts and Strogatz random small-world model, published in 1998 [111, 27, p.8]. Sections 2.2.2 and 2.2.3 deal with these two frequent and non-exclusive types of complex networks, different from the Erdős-Rényi model of random networks, presented in Section 1.4.2: small world networks and scale-free networks.

2.2.2 Small world networks

Small world networks are characterised by small average shortest path lengths between pairs of nodes and relatively high clustering coefficients [88, 27, p.4], i.e., most nodes are not linked to each other but they can be reached via few links. A small average shortest path between nodes means that they are relatively close to each other in terms of edges that one needs to traverse to link those nodes. The shortest distance between two nodes is also called the geodesic distance. **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**. In small-world networks, the number of nodes increases exponentially with the ‘diameter’ of the network [99], i.e., the length between two nodes is proportional to the logarithm of the number of nodes in the network. They are high density networks and can create communities if the nodes that act as "connectors" in the network show different connecting patterns with different gropus of nodes. A connected community is a cluster, i.e., a collection of nodes that are "more connected among them" than with the rest of the network. 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 networks [111, 12, section 2].

2.2.3 Scale-free networks

A next milestone in complex network theory is the characterisation of scale-free networks. These networks are very present as well in natural and human-made networks. Albert and Barabási studied scale-free networks in 1999 [8, 27, p.8]. They focused on growth, i.e., how the number of nodes in some networks rises over time, and on **preferential attachment, i.e., how new links, interestingly, tend to appear in more connected nodes**. On the latter, they were inspired by the seminal work of Eggenberger and Pólya in 1923 [34]. These networks contain **few large degree nodes and many small degree nodes** [12, section 2] and may show a self-similar structure [99]. They are **usually less highly clustered than small world networks, although some scale-free networks can show a small-world structure as well** [100]. The influence of the large nodes, the hubs, is greater than in small worlds. A typical example of a scale-free network is a hub-and-spoke configuration in air transportation. Later on, in 2002, Albert and Barabási studied how the topology of a network, in this case, a scale-free network influences its robustness against failures and attacks [1]. Reid and Harrigan, in 2011, studied the pseudo-anonymity of BTC using complex network analysis. By that year, they did not find much literature describing the network structure of Bitcoin [93]. They identified two complex networks in Bitcoin: the transaction network and, alternatively, the user network. Nodes in the transaction network correspond to transactions and edges to specific outputs in each transaction. Nodes in the user network represent, initially, BTC addresses, and, subsequently, users, once origin addresses in a multi-input transaction are considered belonging to the same user and, therefore, contracted to a unique user. Reid and Harrigan reached the conclusion that, at that early stage, the BTC network was not scale-free yet [93, 92]. Finally, with regard to scale-free networks, it is worth mentioning **a specific subtype of scale-free network: the hierarchical model**. While in the three previously mentioned models, i.e., Erdős-Rényi, Watts-Strogatz and Barabási-Albert, the clustering coefficient of a node does not depend on its degree k, **in hierarchical networks the clustering coefficient $C(k)$ follows a power law function** as Equation (2.1) shows, with $alpha > 0$.

$$C(k) \sim \frac{1}{k^{\alpha}}. \tag{2.1}$$

2.2.4 Degree distribution in scale-free networks

The degree distribution in random networks, i.e., the plot of the number of nodes (y axis) per degree (x axis), does not display hub nodes, i.e., highly connected nodes, but rather a distribution similar to a normal curve. This is the main reason why random networks respond similarly to a random and to a targeted attack [88]: nodes are not so distinguishable. The degree distribution in small world networks can display different topologies. Perera et al. in 2017 [88] mention that they can show a normal curve, similar to random networks. However, they could also display a fat-tailed degree distribution, such as a power law, depending on the way their nodes link, e.g., whether hubs exist, as Hartmann and Sugár in 2021 [50] show in their study on power grid networks. **The degree distribution of a scale-free network produces a power law function** [8, 88, 81], as Section 2.2.3 states. In the case of scale-free networks, they are highly sensitive to an attack targeted to one of their hubs [1]. This high attack sensitivity in hubs is a fundamental characteristic for this doctoral thesis [87, 85, 86]. The name of scale-free refers to the different value that their exponent can display [15]. Equation (2.2) presents a power law degree k distribution. Common values of α range from 2 to 3 [4, 99, 85]. σ is just a constant.

$$P(k) = \sigma \frac{1}{k^{\alpha}}. \tag{2.2}$$

2.2.5 Network related terms

A complex network G is a mathematical object, $G = (N, E)$, defined by a pair of sets, a set of nodes (also called vertices) N and a set of edges (also called links) E that link the nodes. An immediate classification for networks is whether their edges have directions and then the network would be **directed** or the edges connect nodes but there is simply a connection between the nodes with no distinction between the origin and the destination of the edge. These are **undirected** networks [27, p.5]. This doctoral research works with undirected networks.

A **walk** in a network is an alternate collection of connected edges and nodes. If the walk ends in the node where it started, then the walk is closed. A **path** is a walk in which each node is only visited once. A **cycle** is a closed walk in which no edge is repeated. The **diameter** of a network is the shortest distance between the two most distant nodes. A network is **connected** if it is possible to find a path between any pair of nodes. If it is not possible, then the network is **disconnected**. Additionally, a **weighted** network adds weights to each of the edges [27, p.5].

The degree correlation in a network shows how nodes with similar degrees are connected. A network is **assortative** if nodes with similar degrees tend to be connected. On the contrary, those networks where highly connected nodes are connected with those with very few edges are called **disassortative**. **Non-assortative** or **disassortative** networks show no correlation between connected nodes and their degrees [27, p.7].

2.2.6 Centrality measures

Centrality measures characterise the importance of any given node in a complex network. **Degree** centrality refers to the number of nodes directly connected, i.e., via one hop, to a specific node. In directed networks, one can distinguish between in-degree (the number of arrows reaching a node) and out-degree (the number of arrows going out from a node) [81, 15]. **Betweenness** centrality identifies key "bridge" nodes. It measures the number of times that a node is part of the shortest path between other pairs of nodes [81, 15]. **Closeness** centrality is defined as the multiplicative inverse of the sum of the geodesic distances, i.e., the shortest distance between that node and all other nodes. Therefore, the closer a node is to the rest of nodes, the smaller the sum of geodesic distances and the greater its closeness. Equally, the further a node is to the rest of nodes, the greater the sum of shortest distances to the rest of the nodes and, consequently, the smallest its closeness [15]. **Eigencentrality** represents the advanced version of degree centrality, since it considers not only the number of direct connections that a node has but, recursively, the number of connections that direct connections to that node have. Google's PageRank and Katz centrality measures are somehow variants of eigencentrality [21].

2.2.7 Complex network analysis of BTC and ETH

The complex networks created from the history of BTC and ETH transactions do not follow a densification law and do not show a constant average degree [75]. In these networks, nodes are addresses and edges are transactions. The recommendation to participants to use different addresses for every transaction explains the existence of many nodes with very few edges [75]. Exceptionally, some addresses survive day after day. They normally correspond to payees such as exchanges, miners and donation receivers. Once they overcome their creation phase and reach a stable stage, Liang et al. [75] and Javarone et al. [69], both in 2018, and Ferretti and D'Angelo [44], in 2019, observe that **the degree distribution of these BTC and ETH transaction networks**, with millions of nodes, i.e., addresses, **resemble a power law: a heavy-tailed distribution** with lots of nodes showing very low degrees and a small number of nodes with high degrees. Both transaction networks are disassortative, i.e., high degree nodes tend to connect to low degree nodes [75]. Originally, Baumann et al. in 2014 [11] and Liang et al. in 2018 [75], confirm the scale-free nature of the BTC transaction network. Interestingly, Baumann et al. identify a small-world network when they focus on a subgraph containing only the largest transactions [11] and Liang et al. reach a similar conclusion for BTC when they focus on a monthly snapshot of the network [75]. However, they do not conclude equally regarding small-world identification when they consider the entire BTC network given the low average clustering coefficients [75].

2.3 System of systems engineering

As Section 2.2 suggests, complex network theory is a useful instrument to treat complexity from mathematics and physics. The latest engineering attempt by Jamshidi et al. to decompose complexity brings systems engineering up to the next level and proposes system of systems engineering (SoSE) when the components of the system of study, also called holons, are complex systems themselves [67, 68]. There is managerial and operational independence in each of the holons or system components while there is **a common purpose for the system of systems (SoS)** as a whole [96].

2.3.1 Open systems

The SoS found in Nature are open. Human made SoS can be open or closed. This research focuses on open human-made SoS. They manage their entropy via open interfaces, through which they exchange energy and information with the environment. In closed systems, however, entropy grows continuously [7]. Entropy relates to the degree of disorder or randomness of a system. Firt used in thermodynamics, it is linked to the Third Law of thermodynamics, through which a system reaches a constant value of entropy, usually zero, when its temperature reaches absolute zero. In Information Theory, entropy is linked with the concept of uncertainty. **Open systems interact with the surroundings to manage their complexity, based on a set of principles**: they cooperate (synergy), organise themselves (self-organisation), create new patterns and properties (emergence) and, finally, they adapt to changes (reconfiguration) [7]. This thesis uses a related set of open systems properties, proposed by Gorod et al. [47]: autonomy, belonging, connectivity, diversity and evolutive emergence [87].

2.3.2 Network centricity

Usually, systems that compose an SoS communicate to each other via networks. This fact is known as network-centricity or net-centricity. In each of these networks, it is typical to find a service-oriented architecture (SOA). An **SOA design** includes three elements: **service providers** that offer a functionality to **network consumers** and make use of **service registries** to associate providers with consumers [67, 68].

2.3.3 A paradox as a source of innovation

Jamshidi et al. suggest that the existence of **paradoxes** in a SoS, rather that a source of confusion, is a real **source of innovation** [68]. In this research, the focus lies on how tensions between autonomy and belonging, centralisation and distribution, and, finally, diversity, develop and evolve [87].

2.4 Identity and access management

An important aspect of information security is the association of a participant in an information system with their identification and with the access that they have in the system. The name of this field is identity and access management (IAM). It is very rare that an information system does not require to distinguish among its users. Therefore, **most systems require an IAM concept** [82]. Public blockchains, as open networks that transfer digital value among participants, are no exception. However, the implementation of a resilient IAM concept against intentional attacks in blockchain implementations is challenging [85].

2.4.1 IAM in distributed systems

Distributed systems usually do not rely on centralised IAM services. They deploy a service-oriented architecture (SOA) that offers IAM services in multiple and redundant locations. A basic mechanism to manage identities is via **data integrity services**, i.e., each participant is linked to an identity and the piece of data related to that link benefits from a generic data integrity functionality [113]. Open, also called permissionless, distributed systems pose a bigger identity management challenge than systems that require future participants to obtain permission to join the network [113]. This doctoral research discusses how a **resilient IAM concept** could have contributed to **limit the impact** of most of the **reported security incidents** suffered by public blockchains [85, 86].

2.4.2 The physical dimension of a digital IAM concept

The W3 Consortium, an international standard-setting community focused on the growth of the Web, supports the creation of **self-sovereign digital identities** based on **decentralised identifiers** [108] and **verifiable credentials** [109]. Public blockchain implementations, such as cryptocurrencies and IoT platforms [42], eventually require that a digital identity is unequivocally associated with a physical identity in the brick-and-mortar world. This is especially relevant in those addresses holding high value. This thesis, through the published articles that it compiles, highlights the recommendation to apply an effective IAM strategy in public blockchains to increase their resilience against intentional risk [85, 86]. Appendixes A and B go deeper on IAM proposals for public blockchains.

2.5 Visibility graphs

The original idea from Lacasa et al. in 2008 [73] of transforming a **uni-dimensional time series** into a **connected and undirected complex network** is presented in Section 1.4.5. The algorithm that Lacasa et al. propose is uncomplicated but powerful. For each of the time points in a series, there is a node at a specific "height". This "height" corresponds to the value of the series for that point in time. There is an edge between two nodes if they "see each other", i.e., it is possible to draw a line between two specific nodes without "crossing" any of the vertical height lines that "holds" each of the nodes [73]. If the visibility lines are limited only to horizontal lines, then Lacasa et al. refer to horizontal visibility graphs (HVG). Visibility graphs that do not have this horizontal line limitation are called natural visibility graphs or, simply, visibility graphs (VG) [73]. Figure 2-5 depicts two examples of VGs and HVGs from BTC and ETH daily price time series.

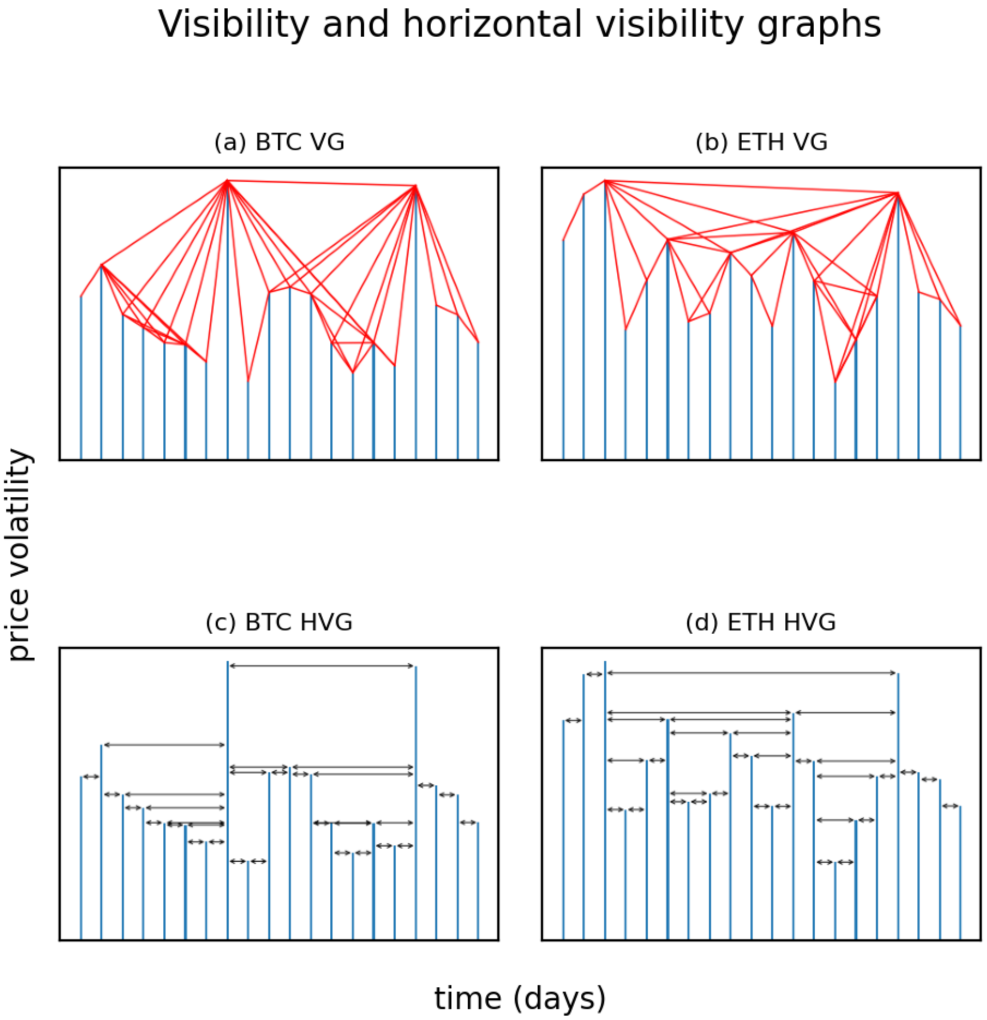


Figure 2-5: Examples of visibility graphs (VGs) in subgraphs a and b and horizontal visibility graphs (HVGs) in subgraphs c and d created from 20 daily price volatility data points from both Bitcoin (BTC) and Ethereum (ETH) daily price time series. Price data from *investing.com* [58, 59]

2.5.1 Translating data: from time series to graphs

The key contribution from Lacasa et al. is the specific conversion between a structure in a time series and a structure in a graph. More specifically, **periodic series convert into regular graphs, random series into exponential random graphs and finally, fractal series produce scale-free networks**, i.e., a visibility graph whose degree distribution is a power law function [73]. Interestingly, although Lacasa et al. confirm that the network coming from a fractal time series is scale-free, based on Song et al. [100], Lacasa et al. distinguish different resulting graphs depending on the type of fractality present in the originating time series: stochastic self-affine fractal series do not evidence repulsion between hubs and show a VG with a small-world effect, as it is the case, e.g., with the Brownian motion time series, while deterministic fractal series show a self-similar VG with hub repulsion [73]. According to how Song et al. define a self-similar fractal network, only VGs that display hub repulsion, i.e., that show disassortativity, are fractal networks [100].

2.5.2 VGs analysis in Bitcoin price series

The VG analysis performed in 2018 by Liu et al. serves as inspiration for this doctoral work [86]. In their search for patterns in the BTC price series, Liu et al. make use of VG analysis to reach the conclusion that the resulting complex networks are scale-free and, therefore, their **originating price series are fractal** [76, 73]. Additionally, they also study the average clustering coefficient per degree of the resulting VGs and identify a scale-free behaviour. This result leads them to the conclusion that the fractality of these networks display a hierarchical structure, consisting of communities created at different levels but following identical laws [76].

2.5.3 Vulnerability to intentional attacks

It is advisable to define the dual concept of vulnerability before dealing with how "hub repulsion" contributes to increasing network resilience or making networks more robust and, therefore, less vulnerable. In information security terms, a vulnerability is a weakness in a system that can be exploited to perform an intentional attack against it [82]. In network theory, the exploitation of a vulnerability leads to a structural change in the network, usually endangering its initial functionality [81]. At this point, it is key to remember the more constrained definition of a fractal network according to Song et al. [100], as mentioned by Lacasa et al. [73]. Song et al. state that a fractal network shows a strong "repulsion", i.e., disassortativity, between the hubs, i.e., the most connected nodes, on all length scales, do not connect to each other. This renders them very dispersed. Consequently, Song et al. claim that a robust modular network requires specifically this self-similar fractal topology displaying "hub repulsion", i.e., with hubs not connected between each other. Certainly, this statement confirms that when nodes are organised around dispersed hubs in self-similar nested communities with "hub repulsion", they are protected from a systemic failure and they are less vulnerable to targeted attacks because hubs are not connected to each other. Thus, a

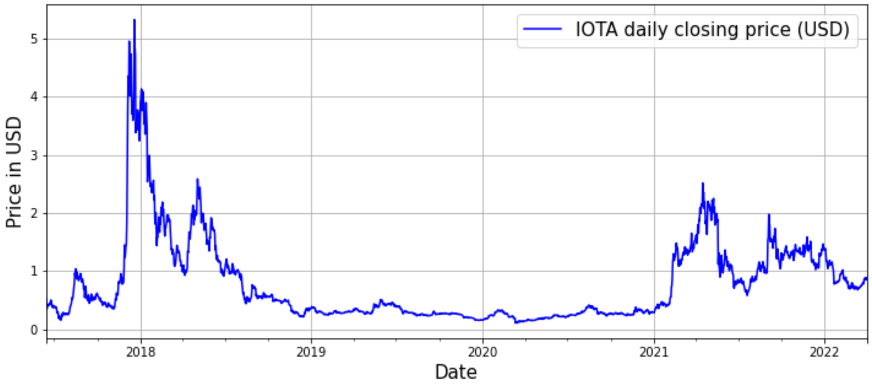


Figure 2-6: IOTA daily closing price since mid 2017 in USD. Price data from *investing.com* [60].

failure in one of those communities will not propagate easily. This is the reason why **fractal, as defined by Song et al., scale-free networks can be more resilient to attacks than non-fractal scale-free networks** [100].

2.6 Internet of things

The first public blockchain implementations, including BTC [79] and ETH [39], aim at providing a distributed way to transfer digital value from peer to peer, in the form of cryptocurrencies. However, the use cases for blockchain are broader. Similarly to transferring value, a blockchain can also transfer any other type of information in a distributed fashion. Internet of Things (IoT) related data is a relevant use case. Therefore, this thesis also studies **blockchain-based IoT platforms** [85, 86]. Data exchange through the Internet is not a human to human monopoly. In January 2021, 4.66 billion human beings were using the Internet, 92.6% of them via a mobile device [101]. In 2018, more than 50 billion IoT devices were already connected to the Internet [72], outnumbering humans. Typical IoT devices are sensors and actuators that use the Internet as their communication channel to reach the corresponding processing server and act as digital interfaces to the physical world. Examples of IoT devices are air quality monitors, thermostats, movement sensors, power switches, cameras, etc.

2.6.1 Blockchain in IoT

IoT devices' distributed location, their connection to the public Internet and their limited computing power make them ideal candidates to join a blockchain to accomplish their function [85, 86]. Additionally, certain native features of blockchain, such as its decentralisation and the redundant location of its database, justify the use of a blockchain, or, more generally, of a distributed ledger, in IoT platforms [43]. In addition, **blockchain technology answers some security requirements of IoT**

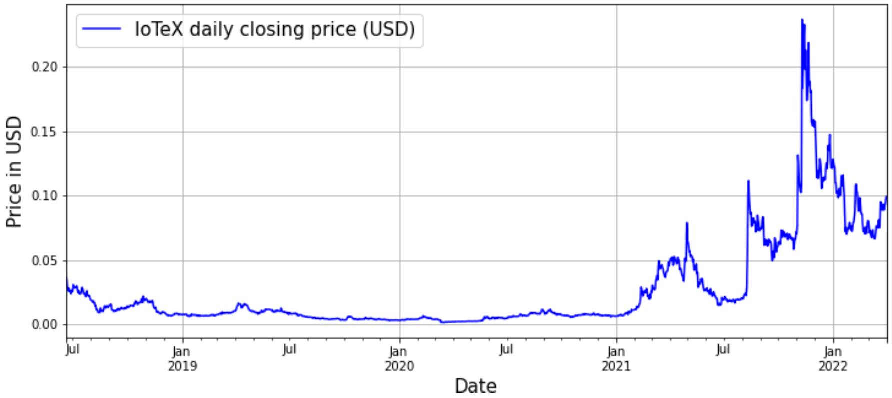


Figure 2-7: IoTeX daily closing price since mid 2018 in USD. Price data from *investing.com* [61].

platforms, especially those related to data integrity and availability [43]. This thesis focuses on the two most capitalised, at least until March 2022 [25], IoT platforms that use a distributed ledger, i.e., IOTA and IoTeX. IOTA, created in 2015, the most capitalised one, is an open-source distributed ledger, curiously, implemented in a directed acyclic graph (DAG), as an alternative to blockchain. There are no transaction fees and the IOTA token, MIOTA, is traded since 2017 [63]. Figure 2-6 shows IOTA daily closing prices since mid 2017 and its high volatility periods in 2018 and 2021. IoTeX, created in 2017, is the second most capitalised IoT platform. It is a multiblockchain IoT platform that uses permissioned and permissionless subchains. IOTX, the IoTeX token, started trading as an Ethereum ERC-20 token in 2018 [65]. Figure 2-7 displays IoTeX daily closing prices since 2018 and how the period with high volatility started in 2021.

However, IoT still poses some challenges to blockchain such as real-time communication, limited energy storage capacity per device and transaction costs and speed [85]. All in all, Fernandez et al. consider that **blockchain** can impact traditional cloud-centered IoT applications and **disrupt the IoT industry** [43]. The analysis of IAM resilience against intentional risk for blockchain-based IoT platforms [85] and the intentional risk-based strategy to use 5G for IoT [86], both included in this thesis, provide original and actionable content, in alignment with the objectives of this doctoral work.

2.7 5G technology

Linking the analysis and the conclusions of this thesis with technological challenges is essential. This way, readers can benefit from applying the discovered learning points onto real scenarios. For example, as more than 4.32 B people use mobile technology to connect to the Internet [101], it is worth focusing on the latest **mobile technology** generation, named 5G, as a powerful **lever to extend the use of DAG**

or blockchain-based IoT platforms and, at the same time, to make them more resilient against intentional risk.

2.7.1 Higher speed and lower latency

As any new mobile technology generation coming to the market, 5G provides faster data transmission rates, in the range of up to 1Gbps, and lower latency: around 30 ms [117]. This technology breakthrough **contribute undoubtedly to the growth of the IoT market** and the creation of new use cases both in domestic and industrial environments [117], especially in outdoor and remote environments where WiFi coverage is not economically feasible nor reliable.

2.8 Intentional risk

2.8.1 Security, risk, vulnerability and threat

The concept of **security** is tightly linked to human beings and their **state of being and feeling protected**. The search for protection from any agent that could harm is a constant activity throughout human history. A concept that is highly coupled with security is risk. **Risk refers to the possibility of something bad happening in the future**. Security measures aim at mitigating risk [21, 82]. A risk materialises when an agent, **a threat**, makes use of a weakness, **a vulnerability**, and causes harm [82]. The invention of computing and, with it, the processing of data, triggered the emergence of **information security**, i.e., all activities involved in protecting the data and the information systems (IS) that treat them. Using the lens of risk, information risk management focuses on mitigating the risks to information integrity, availability and, if required, confidentiality.

2.8.2 Intentional risk in information systems

Traditionally, risk management in information systems inherited **actuarial techniques**. The insurance industry use heavily these practices, based on historic data and statistics [21, 82], to quantify the impact and probability of a potential risk becoming a reality. These tools are **adequate to mitigate non-intentional, accidental risks**, present, e.g., in business continuity responses to natural events such as meteorological catastrophes. However, the benefit of applying reductionist impact and probability studies to mitigate intentional risks, i.e., those risks posed by a malicious party, is very limited. In 2015, Chapela et al. [21] coined the expression "**intentional risk management**" with a special focus on the intention that a threat agent has to harm an information system to obtain a benefit. Before the work of Chapela et al., Song et al. referred already to "intentional attacks" [100]. Chapela et al. state that **cybersecurity is the subset of information risk management that focuses on intentional risk**. Any agent that attacks an IS, leveraging on a high benefit to run risk ratio, renders the two foundational parameters in traditional risk management of impact and probability insufficient to manage risks [21, 82]. The estimations of impact and probability are highly dependant on expert judgement.

2.8.3 Profitability associated to the attacker

The security innovation that Chapela et al. bring forward is to **model information systems as complex networks** and to provide clear risk-related values to each of the nodes. They focus on three dimensions per node: **value, anonymity and accessibility** and they summarise their contribution in a simple but powerful mathematical formula [21], presented in Equation (2.3). They define the term **profitability associated to the attacker** (PAR) to quantify intentional risk. Equation (2.3) quantifies the PAR for a system S as the maximum product of the triplet $<$*value*, *accessibility*, *anonymity*/*l*$>$ for each of the nodes, i.e., each of the participant elements in the system, named p. The constant l, called legal robustness, reflects the legal consequences that an attacker could face in their corresponding jurisdiction. The PAR associated to a system is a good proxy for intentional risk.

$$\forall\, p \in S, \quad \mathrm{PAR_S} = \max\left(value_p \cdot accessibility_p \cdot \left(\frac{anonymity_p}{l} \right) \right) \tag{2.3}$$

For Chapela et al., this is their entry point to manage intentional risk in information systems in a more realistic fashion than only relying on the experience of an expert actuary. The use of complex networks analysis to manage intentional risk is applicable to any technology implementation and information system susceptible to be modelled as a complex network. In this doctoral thesis, **I analyse the complex networks** created by BTC, ETH, IOTA and IoTeX **blockchain implementations** based on network theory references such as Albert et al. [2], Boccaletti et al. [15] and Newman [81] **with the objective to increase their resilience against intentional risk** or, in other words, to **reduce their PAR**.

2.8.4 Resilience against intentional risk

Material **resilience** in engineering refers to the capacity to recover its original shape after the force causing its deformity ceases [70]. In psychology, resilience refers to the ability to **recover from adversity** [105]. Taleb goes one step further and proposes the concept of antifragility when an entity gets stronger out of a specific stress [104]. This research work suggests pragmatic **measures to improve resilience of blockchain systems against intentional risk**.

3. Methodology and implementation

This chapter presents the research methodology applied in this doctoral work. It focuses on a novel methodology, at the crossroads of SoSE, network theory, visibility graphs and intentional risk management. It also explains its implementation. The aim is to answer the question of how to improve the resilience against intentional risk in blockchain implementations with the help of complex network analysis. For that purpose, the chapter follows a bottom-up approach to explain the methodology: first, it describe the methodology applied in each of the published articles and, second, it finds the common foundations among them and propose a general framework to study intentional risk in blockchain implementations.

3.1 A three-element methodology to manage intentional risk

The first milestone of this thesis is to facilitate the understanding of public blockchains. For this, the methodology suggested in Section 3.2 models BTC and ETH, the two most relevant blockchain implementations, as a System of Systems and uses the components proposed by Chapela et al. [21] to reduce profitability associated with attackers. The second milestone is to improve identity and access management (IAM) resilience against intentional risk in blockchain implementations. The methodology presented in Section 3.3 accomplishes this task using IOTA and IoTeX as real life examples and it compares them with BTC and ETH networks. This methodology builds complex networks from public blockchain transaction data and uses, again, the parameters proposed by Chapela et al. [21] to refer to IAM. The third milestone is the creation of an intentional risk-based strategy for blockchain. Section 3.4 describes the related methodology. It introduces a new element, visibility graphs (VG), to construct complex networks from time series, and proposes a strategy to manage intentional risk with the help of the formula proposed by Chapela et al. [21] and in the realm of 5G, a mobile technology standard. In this occasion, the blockchain implementations studied are IOTA and IoTeX as well.

3.2 Methodology to understand BTC and ETH

As Sections 1.2 and 3.1 state, the first objective of this research is to facilitate the understanding of public blockchains such as BTC and ETH. For that, I model both blockchain-based cryptocurrencies as an open SoS of public blockchains. More specifically, I propose a five-step methodology to model a system composed of systems, i.e., a "supersystem", as an open SoS. This methodology is based on the references used in Section 2.3 to present the state of the art in SoSE.

3.2.1 Building a System of Sytems

In 2009, Mo Jamshidi edited the book titled "System of Systems Engineering" [68] and provided a collection of methods to disentangle the complexity present in "supersystems", i.e., systems composed of systems. The first step to frame a "supersystem" into a SoS is to identify its overall purpose, i.e., a common goal for the SoS [96]. The second step is to confirm that the system components are open and that their interaction with the environment is a way to manage their growing complexity [7]. The third step focuses on the net-centricity of the SoS. The network is the connecting element for each of the system components and for the SoS. The fourth step consists of the analysis of the SoS characteristics that propose Gorod et al. [47]: autonomy, belonging, connectivity, diversity and evolutive emergence. For each of these properties, I build a balance panel to analyse whether they tilt towards a system of highly related subsystems or towards a fully-fledged SoS. Finally, I complete this methodology with an analysis of the vulnerabilities that are present in the SoS and the threats that pose risks to the SoS. Table 3.1 summarises this methodology to analyse a "supersystem" as a SoS. This thesis uses this methodology to build the SoS of public blockchains and considers BTC and ETH as two key holons in it.

Table 3.1: 5-step methodology to build a SoS.

Step	Focus	Rationale
1	Common goal	Definition of SoS: Component systems sharing an ultimate goal
2	Open & Complex	Continuous evolution: Open systems with growing complexity
3	Network-centric	Components use networks to communicate
4	5 Characteristics	Autonomy, belonging, connectivity, diversity and evolutive emergence
5	Risk analysis	Vulnerability and threat analysis (confirmation of intentional risk)

3.2.2 Reducing the profitability associated to the attacker

Once the identification and the full description of an SoS takes place, I check the results of the fifth step mentioned in Section 3.2.1, the vulnerability and threat analysis, to confirm whether intentional risk appears as a plausible threat affecting the SoS. Table 3.1 includes this detail in step five. In general, if the second step of the methodology proposed in Section 3.2.1 validates that the system of study is open, there will be interactions with the environment and, almost undoubtedly, there will be threat agents willing to exploit a vulnerability in the system to obtain a benefit, as explained in Section 2.8.3. I then use Equation (2.3) to propose a series of generic, although practicable, measures that would increase the resilience of the system against intentional risk, i.e., reduce the PAR (profitability associated to the attacker) . Section 2.8.3 explains the concept of PAR as a proxy for the intentional risk that a system, or a SoS, is subject to. These measures target the reduction of the dimensions identified by Chapela et al. [21]: value, accessibility and anonymity. Additionally, the increase of l, the legal robustness, is a complementary measure.

Table 3.2: Strategies to reduce intentional risk.

Dimension	**Action**	**Mitigating measures**	**Stage**
Value	Reduction	Distribution across many nodes	Design and Operations
Accessibility	Reduction	Improvement of access controls	Design, development and operations
Anonymity	Reduction	Enhance IAM	Design,development, operations and governance
Legal robustness	Increase	International alignment	Operations and governance

Table 3.2 lists the portfolio of strategies that are available to reduce intentional risk. It links each dimension with an action, a high level description of possible mitigating measures and an initial indication on the most suitable lifecycle stages of the system for their implementation.

3.2.3 Implementation

Sections 3.2.1 and 3.2.2 propose a methodology that can be applied, first, to explain any complex system composed of multiple systems and, second, to identify strategies that would increase its resilience against intentional risk. The article titled "modeling Bitcoin plus Ethereum as an open System of Systems of public blockchains to improve their resilience against intentional risk" [87], published in 2022, and available in Chapter 4 of this thesis, implements this methodology, first, to understand the two most capitalised public blockchain implementations, i.e., BTC and ETH [23] and, second, to increase their resilience against attacks.

3.2.4 Data collection

The data used to model BTC and ETH as a SoS is public, very diverse and comprehensive. Table 3.3 provides examples of the main types of data sources consulted, related to BTC, ETH and other public blockchain implementations.

3.3 Methodology to improve IAM resilience against intentional risk

The second objective, as Sections 1.2 and 3.1 present, is to improve IAM resilience against intentional risk in blockchain. I study this security aspect with real data

Table 3.3: Data used to model BTC and ETH as a SoS.

Focus	Data sources (examples)
Common goal	Foundational BTC and ETH papers [79, 39, 38].
Open & Complex	Open-source development docs and fora, trading data, transaction data [14, 39, 58, 59].
Network-centric	Network APIs, similar info from other public blockchains [14, 40, 55, 64, 66].
Autonomy	BTC and ETH improvement proposals (BIP and ERC) [13, 35]
Belonging	Mining power and governance data [106, 45]
Connectivity	Wrapped BTC (WBTC) and interledger protocol (ILP) [87]
Diversity	Leadership and control structure, developer activity [87]
Evolutive emergence	BTC and ETH market analysis, fungible and non-fungible ETH tokens [87, 57, 22]
Risk analysis	Holistic SWOT, intelligence and incident analysis [82, 87]

extracted from four public blockchain implementations. As mentioned in Section 2.6, there are even more IoT devices connected to the Internet than human participants. Therefore, I research two blockchain use cases:

- implementations in which most participants are human beings: the two most capitalised blockchain-based cryptocurrencies: BTC and ETH [23].

- implementations in which most participants are IoT devices: the two most capitalised IoT platforms [25] that are based on a distributed ledger: IOTA, using a directed acyclic graph (DAG), and IoTeX, using a blockchain, as explained in Section 2.6.

This doctoral thesis considers market capitalisation as a proxy to identify the most popular, and hence used, blockchain projects. I design a methodology to characterise each of these four public blockchain implementations as a complex network. In this way, I can use network theory, a branch of knowledge that studies complex non-linear systems, whose state of the art presents Section 2.2, to learn about real blockchain implementations. This methodology consists of two stages: the creation of the complex networks out of the blockchain transaction data and the extraction of properties from those networks to propose IAM related improvements.

3.3.1 From public blockchains to complex networks

The methodology stage to create and characterise the complex network consists of three steps:

- the first step is to collect as much blockchain data as possible to create the complex network that will be the object of analysis. Public blockchain implementations usually provide, through an Internet site called *explorer*, on-chain search functionalities. These explorers filter through the entire blockchain transaction history based on parameters such as address, block number or transaction

Table 3.4: 9-step methodology to improve IAM resilience via complex networks.

Step	Focus	Rationale
	From public blockchains to complex networks	
1	Collection of blockchain data	Required input to build the complex network
2	Extract transaction data	Create an undirected and non-weighted graph
3	Characterise created networks	Calculate degree distribution and basic parameters
	From complex networks to IAM	
4	Identify hubs	Analyse degree distribution
5	Study assortativeness	Draw all connections to LCC to identify disassortative networks
6	Signs of small world	Using network density and clustering coefficients
7	Scale-free networks	Confirm the importance of highly connected nodes (hubs)
8	Heavy-tail distributions	Identify power law fits
9	Link with IAM improvements	Translate network properties into IAM actions

identifier. The most advanced ones publish even an application programming interface (API). Blockchain explorers and related APIs are not standardised: they offer different functionalities and require a specific syntax. The challenge in this step is to download sufficient on-chain data as possible using these explorers and their APIs to reach relevant conclusions.

- the second step is to extract, out of the transaction data, the sender and destination addresses of each downloaded transaction. These addresses are the keystone to build the network: every node represents an address and an edge between two nodes represents a transaction between two addresses. The resulting complex network is the most basic construct possible: an undirected and non-weighted graph. At this point, it is worth highlighting the challenge of having a different syntax in each analysed blockchain implementation. This fact requires the writing of an ad-hoc piece of code for each blockchain at stake.

- the third step is to calculate basic complex network parameters such as average degree, average clustering coefficient, density, graph connectivity, graph components and, finally, degree distribution. This analysis constitutes the bedrock for the reached conclusions on IAM resilience against intentional risk. The challenge in this case is the available computational capacity.

3.3.2 From complex networks to IAM

The methodology stage to connect the complex network analysis with IAM consists of six steps:

- identification of highly connected addresses: the collection of origin and destination addresses, extracted out of the available transaction data, gives shape to the transaction network. The next step of the methodology is to identify, via the degree distribution, whether there are many nodes, i.e., addresses, with low degrees and a small number of nodes with high degrees. The existence of highly connected addresses is an element to consider in IAM recommendations as attacks to highly connected nodes, i.e. hubs, impact the network [9, 85, 86]. Consequently, at least those nodes require strong IAM measures.

- study of assortativeness: the plot of the largest connected component (LCC) in the resulting transaction network and all nodes connected to it through one or two edges simplifies the task to identify disassortativity, i.e., when low degree nodes tend to connect with high degree nodes.

- search for small world networks: as Section 2.2.2 explains, small world networks show a small average shortest path length between pairs of nodes and a relatively high clustering coefficient. This methodology uses three parameters to identify this structure: first, connection or non-connection of the resulting network, as small worlds happen in connected networks. Second, it calculates the network density instead of the average shortest path length, as the latter is computationally intensive. Third, the average clustering coefficient finally determines whether the resulting network is a small world network.

- search for scale-free networks: Section 2.2.3 mentions that scale-free networks show lower clustering coefficients than small world networks and confirms that the influence of large nodes in scale-free networks is greater than in small worlds. This last point is key for a set of IAM actions. Section 2.2.3 highlights as well that some scale-free networks can also display a small-world structure.

- analysis of heavy-tailed distributions: the identification of power law fits just based on the graphical appearance of a degree distribution on log-log axes is not accurate [4]. Therefore, this methodology not only plots the degree distribution but it also checks PDF and CCDF and their fits to understand and to assess the goodness of fit of power law functions.

- link with IAM improvements: finally, identified network properties trigger a set of IAM related recommendations.

Table 3.4 summarises the methodology proposed to improve IAM resilience against intentional risk in complex networks created from blockchain implementations.

3.3.3 Implementation

Sections 3.3.1 and 3.3.2 put forward a methodology that, first, allows the study of transactions occurring in a blockchain implementation through an undirected and non-weighted network. Second, it looks for signs of highly connected nodes and studies whether the network adopts the shape of a small world or, alternatively, it resembles a scale-free network or, even, displays both structures simultaneously. The article titled "identity and access management resilience against intentional risk for blockchain-based IoT platforms" [85], published in 2021, and reproduced in Chapter 5 of this thesis, follows this methodology. First, it characterises IOTA and IoTeX as complex networks and, second, it sheds light on IAM resilience against intentional risk in blockchains, in this case, related to IoT. The article also briefly analyses BTC and ETH network degree distributions to compare them with the ones obtained for IOTA and IoTeX.

Table 3.5: Transaction data downloaded from IOTA, IoTeX, BTC and ETH public blockchain explorers. An epoch in IoTeX is 8640 blocks.

Token	Time window	Duration	Addresses	Transactions
IOTA	23 December 2020	24 hours	1068	22960
IOTA	25 December 2020	24 hours	1068	23225
IoTeX	epoch 13910 (December 2020)	24 hours	3190	10222
IoTeX	epoch 14000 (December 2020)	24 hours	3709	13935
BTC	21-23 December 2020 (278 blocks)	46 hours	1241548	1385212
ETH	26 December 2020 (11 blocks)	3 min	1677	1363

3.3.4 Data collection

I use the BTC [14], ETH [40, 55], IOTA [64] and IoTeX [66] explorers and APIs to download transaction data. Each consulted explorer and API is different and requires customised pieces of code to create and analyse the resulting complex networks. In the case of IOTA and IoTeX, the downloaded transaction data involves the 100 and the 500 richest addresses respectively. However, in the case of BTC and ETH, transaction data come from specific time windows. The reason to use the richest addresses as entry points to download transaction data in IOTA and IoTeX is twofold: first, it is a simple way to assess assortativity in the transaction network, i.e., if rich addresses would transact between each other, the graphical representation of the largest connected component (LLC) would show assortativity, and second, their APIs facilitate this data extraction. I use version 3.6 of the Python programming language, including open source packages such as *networkx* [80] and the *powerlaw* library by Alstott et al. [4] to code the required download and analysis snippets. It is worth mentioning the challenge to balance the need to obtain sufficient data for this analysis with the computing power available to the author: the windows of time to download transaction data are limited compared with the complete timeline of the blockchain, as Table 3.5 shows. Nevertheless, the results obtained reach insightful conclusions.

3.4 Methodology to create an intentional risk-based strategy

The third objective, as Section 1.2 and 3.1 present, is to create an intentional risk-based strategy for blockchain implementations. I explore this goal within the context of the two most market capitalised IoT platforms, i.e., IOTA and IoTeX [25]. The methodology includes four elements:

- the use of a complementary and more accessible data set related to public blockchains: their daily market price.
- the transformation of a time series into a complex network via visibility graphs.
- the study of the impact of 5G, a mobile technology standard, on these IoT platforms.
- the application of intentional risk as a lever to understand the mentioned impact of 5G on IoT.

This methodology expands into three stages: first, the transformation of a time series into a complex network, second, the structural analysis of the resulting complex network and, third, the creation of an intentional-risk strategy that, in the context of a specific technology, would protect from ill-intentioned actors aiming to extract value out of the network.

3.4.1 From time series to complex networks

The first stage in this novel methodology is to obtain the required blockchain-related input data. The challenge to retrieve sufficient transaction data from public blockchain explorers, as explained in Section 3.3.1, plus its intrinsic computational complexity encourage this author to use alternative input data sets: daily market prices are easily available and less voluminous than transaction data and they provide insights on how these IoT-related token markets behave. I therefore create a daily price volatility time series based on market data using Equation (3.1).

$$price\ volatility = \log\left(\frac{price_{max}}{price_{min}}\right). \tag{3.1}$$

As the main research tool of this doctoral thesis is complex network analysis, I use visibility graphs (VG), the original instrument proposed by Lacasa et al. [73], to transform uni-dimensional time series into connected and undirected complex networks. This imaginative approach from Lacasa et al. facilitates the analysis of a time series using network analysis techniques, as Section 2.5.1 states. Although there are other methods to map a time series to a complex network, such as the conversion into nodes of periods extracted from aperiodic time series [76], the most visual and straightforward way is the one by Lacasa et al. Therefore, I construct both the natural visibility graph (VG) [73] and the horizontal visibility graph (HVG) [77].

3.4.2 Structural analysis of the resulting complex network

Once the complex network is ready, the second stage of this methodology follows a four-step analysis process:

- description of the network via the degree distribution and basic network features such as number of nodes and edges, average density and transitivity. The number of nodes and edges informs about the size of the network. The density hints at the re-usability of the nodes and the transitivity is a first approximation towards the existence of communities.

- study of the heterogeneity of the network by comparing their degree distribution with a power law function. The comparison is not only graph-based but also founded on the use of non-linear least squares to fit a power law function and, additionally, on the PDF and CCDF as proposed by [4].

- fractality analysis via the average of clustering coefficients per degree $C(k)$. If they display a power law behaviour, this means that the network shows a fractal behaviour and forms communities at different scales in a similar way, i.e., the network is hierarchical [76].

- description of the number and location of communities present in the network.

3.4.3 An intentional risk-based strategy

The final stage in this methodology is the production of a strategy to manage intentional risk in the analysed blockchain implementations and it is based on three elements:

- the analysis performed in Section 3.4.2 on the network defined by a crypto-token market.

- the functionality that a specific technology can provide to blockchain implementations (in this case, 5G).

- the intentional risk parameters proposed by Chapela et al. [21].

Table 3.6 summarises this methodology to create a strategy to mitigate intentional risk in blockchain implementations with the help of complex network analysis.

3.4.4 Implementation

The methodology described in Sections 3.4.1, 3.4.2 and 3.4.3 provides guidance to come up with an intentional risk-based strategy in a complex system such as a public IoT blockchain and contributes to understand the impact that a specific technology, such as, in this case, 5G, can bring to this scenario. The article titled "visibility graph analysis of IOTA and IoTeX price series: an intentional risk-based strategy to use 5G for IoT" [86], published in 2021, and included in Chapter 6 of this thesis, implements this methodology, achieving the third objective of this doctoral work: the creation of an intentional risk-based strategy, in this case, focused on IOTA and IoTeX as IoT platforms that can leverage the use of 5G, a mobile technology standard.

Table 3.6: 9-step methodology to build an intentional risk-based strategy for blockchain implementations using complex networks.

Step	Description
	From time series to complex networks
1	Obtain daily price time series of the blockchain token, e.g., IOTA and IoTeX
2	Transform the time series into two complex networks via VG and HVG [73, 77]
3	Analyse the resulting network calculating degree distribution plus basic parameters
	Structural analysis of the complex network
4	Compare degree distribution with a power law to explain their linking behaviour
5	Study fractality via average clustering coefficient per degree $C(k)$
6	Compare $C(k)$ with a power law to confirm a hierarchical structure
7	Identify and locate communities in the VG and HVG networks
	Creation of an intentional risk-based strategy for a specific technology
8	Analyse how features of a technology impact these blockchain platforms
9	Produce an intentional risk-based strategy for this scenario

Table 3.7: Software used to implement the methodology presented in Section 3.4.

Step	Software	Purpose
1	web browser	Download price time series from data provider [57]
2	*visibility_graph* [46]	Create visibility graph (VG)
2	*visibility_algorithms* [114]	Create horizontal visibility graph (HVG)
3	*metaknowledge* [94]	Basic complex network analysis
3&5	*networkx* [80]	Network analysis & degree distribution & clustering coefficient
4&6	*curve_fit* [24]	Goodness of fit of power law function
4&6	*powerlaw* [3]	PDF and CCDF goodness of fit of power law
7	*community_api* [5]	Community identification
7	*cylovain* [6]	Community identification

3.4.5 Data collection

IOTA and IoTeX market price data comes from *investing.com*, an Internet-based stock market data provider [57]. The data analysis setup that implements this methodology includes the software elements presented in Section 3.3.4 plus additional Python modules. Table 3.7 lists these relevant software and Python code modules, together with the methodology step in which they are employed:

3.5 The resilience triangle

To complete this chapter on methodology and implementation, I propose the "resilience triangle" model. The methodologies presented in Sections 3.2, 3.3 and 3.4 do not play in isolation. All three pieces are indispensable and interconnected components to solve a greater academic puzzle. A puzzle that provides insight into how to model blockchain implementations using complex networks to manage, and ultimately, to improve, their resilience against intentional risk, which is the main objective of this doctoral thesis, as Section 1.2 states. Furthermore, this three-element methodology, the "resilience triangle", can be applied to manage intentional risk, not only in blockchain, but also in other informational constructs. For that purpose, the work of Chapela et al. [21] on intentional risk management acts as the guiding thread throughout the three methodologies presented in this chapter. Their simple but far-reaching intentional risk formula, represented by Equation (2.3), remains the keystone of this doctoral thesis.

Figure 3-1 suggests that the set of methodologies proposed in this thesis constitutes a complete toolkit to answer the research question.

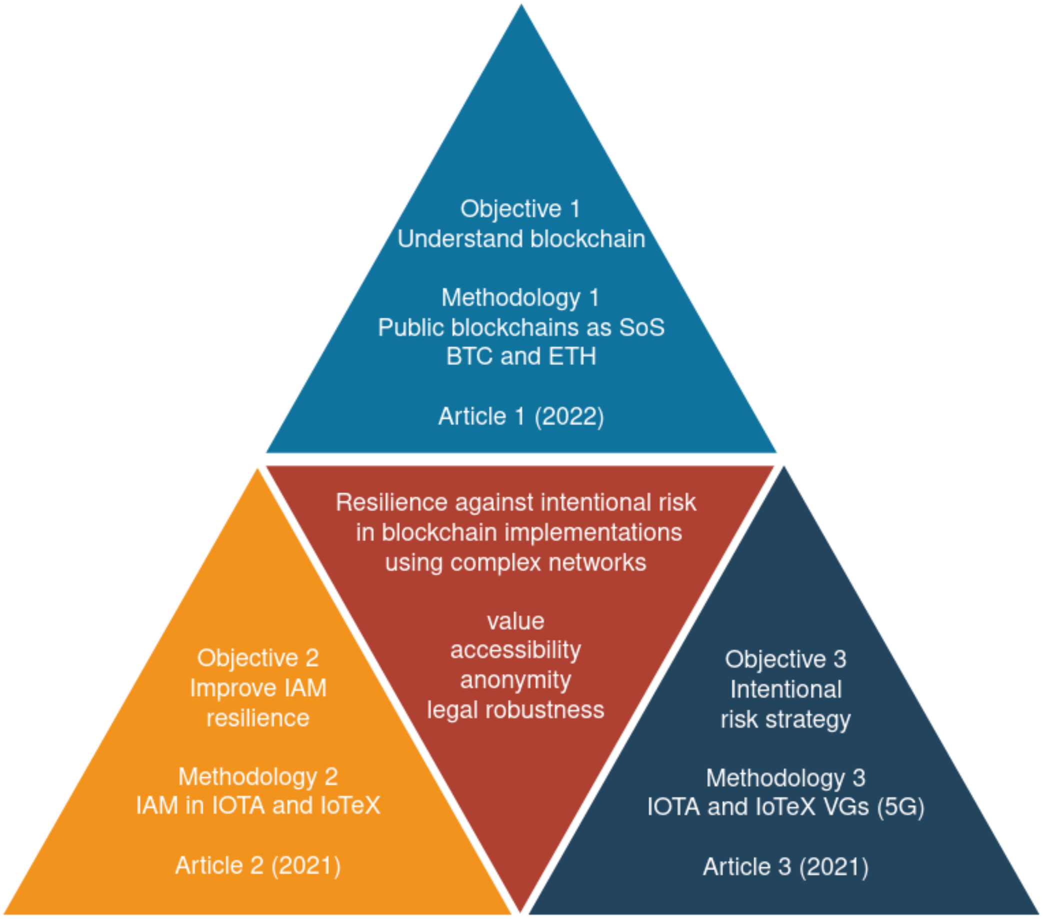


Figure 3-1: Visualisation of the methodologies proposed in this doctoral thesis, the objectives of this research and the published articles as listed in Table 1.3.

4. Modeling Bitcoin plus Ethereum as an open System of Systems of public blockchains to improve their resilience against intentional risk

electronics

MDPI

Article

Modeling Bitcoin plus Ethereum as an Open System of Systems of Public Blockchains to Improve Their Resilience against Intentional Risk

Alberto Partida [1,*], Saki Gerassis [2], Regino Criado [3], Miguel Romance [3], Eduardo Giráldez [4] and Javier Taboada [4]

[1] International Doctoral School, Móstoles Campus, Rey Juan Carlos University, 28933 Madrid, Spain
[2] GESSMin Research Group, Department of Natural Resources and Environmental Engineering, University of Vigo, Lagoas Marcosende, 36310 Vigo, Spain; sakis@uvigo.es
[3] Department of Applied Mathematics, Móstoles Campus, Rey Juan Carlos University, 28933 Madrid, Spain; regino.criado@urjc.es (R.C.); miguel.romance@urjc.es (M.R.)
[4] Department of Natural Resources and Environmental Engineering, University of Vigo, Lagoas Marcosende, 36310 Vigo, Spain; egiraldez@uvigo.es (E.G.); jtaboada@uvigo.es (J.T.)
* Correspondence: apartidar@gmail.com or a.partidar@alumnos.urjc.es

Abstract: In this article, we model the two most market-capitalised public, open and permissionless blockchain implementations, Bitcoin (BTC) and Ethereum (ETH), as a System of Systems (SoS) of public blockchains. We study the concepts of blockchain, BTC, ETH, complex networks, SoS Engineering and intentional risk. We analyse BTC and ETH from an open SoS perspective through the main properties that seminal System of Systems Engineering (SoSE) references propose. This article demonstrates that these public blockchain implementations create networks that grow in complexity and connect with each other. We propose a methodology based on a complexity management lever such as SoSE to better understand public blockchains such as BTC and ETH and manage their evolution. Our ultimate objective is to improve the resilience of public blockchains against intentional risk: a key requirement for their mass adoption. We conclude with specific measures, based on this novel systems engineering approach, to effectively improve the resilience against intentional risk of the open SoS of public blockchains, composed of a non-inflationary money system, "sound money", such as BTC, and of a world financial computer system, "a financial conduit", such as ETH. The goal of this paper is to formulate a SoS that transfers digital value and aspires to position itself as a distributed alternative to the fiat currency-based financial system.

Keywords: blockchain; Bitcoin; Ethereum; System of Systems; System of Systems Engineering; complexity; complex networks; emergence; intentional risk

check for updates

Citation: Partida, A.; Gerassis, S.; Criado, R.; Romance, M.; Giráldez, E.; Taboada, J. Modeling Bitcoin plus Ethereum as an Open System of Systems of Public Blockchains to Improve Their Resilience against Intentional Risk. *Electronics* **2022**, *11*, 241. https://doi.org/10.3390/electronics11020241

Academic Editors: Dongkyun Kim, Qinghe Du, Mehdi Sookhak, Lei Shu, Nurul I. Sarkar, Jemal H. Abawajy and Francisco Falcone

Received: 6 December 2021
Accepted: 5 January 2022
Published: 12 January 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

1.1. Epigraph

The quest to manage complexity has been present in human beings since early days. Equally, the need to register value transfer and ownership. Throughout History, we have created and taken part in complex systems with non-linear relations between their components. First, we focus on public blockchains, a technology that creates a "supersystem", also called a "network of networks" or a "system of systems", that registers the transfer of digital value, even with a potential link to physical value. We use complex network analysis and Systems of Systems Engineering to "digest" its complexity. We identify how public blockchains, such as Bitcoin and Ethereum, complement each other and emerge as an alternative to the traditional fiat currencies. Second, we propose a set of multi-disciplinary measures that, based on recent advances in intentional risk management, hint at how to improve resilience in this System of Systems of public blockchains.

1.2. Blockchain

We first explain the concept of blockchain. A blockchain finds its roots in cryptography and distributed systems [1]. It has a simple motto, i.e., "the longest chain wins". It is a type of distributed database that stores records in a linked collection of blocks [2] showing 3 key properties. First, each block is unequivocally linked to the following block by hash-function cryptography [2]. A hash is a mathematical function that provides data integrity by transforming an input into a unique encrypted output of a fixed length, i.e., validated blocks cannot be tampered with. Second, all transactions in a blockchain are accessible, i.e., they can be read by all users. In every transaction, a participant uses a unique private key to sign it. Third, the complete register of blocks is kept in all connected full nodes. This provides a high degree of availability. Sections 1.3 and 1.4 present the two most market-capitalised, public, open and permissionless blockchain implementations, Bitcoin (BTC) and Ethereum (ETH) [3].

1.3. Bitcoin

Bitcoin (BTC) is the pioneer of the current public, open and permissionless blockchain implementations. It is a crypto-currency that was launched in January 2009 following the seminal paper by Satoshi Nakamoto [4]. This author, or group of authors, decided to remain anonymous. Nakamoto's nine-page seed paper talks about a "peer-to-peer electronic cash system" [4]. It is an open-source and distributed transaction system that acts as an electronic analogue of cash located in the online world [5]. Its main feature is decentralisation, since there is no central authority responsible for issuing bitcoins and it is not necessary to involve a third party to make online transfers. In blockchain terms, a node (or peer) refers to any machine connected to the blockchain that keeps a full copy of its distributed ledger. Slowly but surely, Bitcoin is becoming a global digital value reserve, initially outside the traditional financial system. However, a growing number of players belonging to the mainstream financial system have started to accept BTC and include it in their investment portfolio. This digital store of value could replace the gold standard and become, in the future, the global digital reserve currency [6].

1.4. Ethereum

Ethereum (ETH) is an example of a public blockchain implementation that was created after BTC. ETH is a public, open and permissionless blockchain platform that runs code, i.e., smart contracts [7]. It is a shared global infrastructure that transports digital value. Ether is its native crypto-currency. The project started in 2014. Vitalik Buterim was one of its creators [8]. The ETH blockchain provides a decentralised Turing-complete virtual machine, called the "world computer", with more advanced scripting functionality than the pioneer BTC. Programming languages that use conditional branching and arbitrary memory-stored variables are Turing-complete. ETH and BTC do not compete with each other. They have different purposes and applications. While BTC plays the role of a digital reserve asset, ETH acts as the blockchain engine for an ample ecosystem of business cases. All of them benefit from the properties of a public blockchain with Turing-complete computing power. Examples are decentralised finance (DeFi), as mentioned in Section 4, Internet of Things (IoT)-related tokens [9,10] and an extensive variety of other fungible and non-fungible tokens (NFTs). Fungible tokens are exchangeable, i.e., similar to traditional coins, while non-fungible tokens are unique and distinguishable.

These complementary use cases for BTC and ETH lead us to research scientific methods that can jointly study their complexity. We use complex network theory and SoSE to understand how we can improve their resilience against intentional risk. Keeping BTC and ETH secure is pivotal for their mass adoption. We assume that these public blockchains will continue growing: BTC as a global digital store of value and ETH as an engine for decentralised applications. After introducing the blockchain technology and two of their most relevant public implementations, we move our focus, in Sections 1.5 and 1.6, to the tools we use to "digest" the complexity that we find in public blockchains.

1.5. Complex Networks

Complex networks is a field of study at the crossroad between mathematics, statistics, physics and sociology. It focuses on networks: systems composed of many interconnected dynamical units. Networks are composed of nodes, also called vertices (not to confuse this meaning of node with the one related to a computer that holds a copy of a blockchain, as explained in Section 4.2), and edges, also called links and arches. Network theory aims to capture the global properties of such systems by modeling them as graphs whose nodes represent the dynamical units, and whose links show the interactions between them [11]. Anchored in graph theory, it uses statistical analysis to describe networks with many nodes and edges between them. It is especially useful to describe systems with non-linear relations. The degree of a node is the number of edges connected to it. Complex network theory studies statistical properties of large-scale graphs such as degree distributions to model the structure and behaviour of these networks [12]. We study the complex networks that BTC and ETH spawn to understand their behaviour. We consider each of these complex networks a system within the "supersystem of public blockchains". This provides us with the opportunity to use SoSE as a novel approach to model public blockchains such as BTC and ETH.

1.6. System of Systems Engineering

The meta-definition of SoS used by [13] is a "supersystem" comprised of components that themselves are independent complex operational systems and interact with each other to achieve a common goal. Jamshidi specifies the following characteristics for SoS [13]: they are large-scale integrated systems; heterogeneous systems that can operate independently; they are networked together for a common goal. Typical real-life examples of Systems of Systems are the health care SoS, the communication and navigation SoS and the US Department of Defence SoS [13]. A very common way for these systems to interact and exchange information is through a network [13]. Notably, if these networks of networks are interdependent, they become significantly more vulnerable to random failures and targeted attacks than single networks. Single networks usually exhibit cascading failures that can rapidly provoke a system collapse. Understanding the system characteristics of BTC and ETH that could lead to a failure that propagates is a fundamental step in ensuring that public blockchains could be granted the level of trust required to effectively become widely recognised assets in the global economy [14]. Once we have identified how we study complexity in public blockchains, Section 1.7 presents intentional risk management with the objective of improving resilience in the System of Systems of public blockchains.

1.7. Intentional Risk Management

Risks proceed from accidental (non-intentional) and intentional sources. While non-intentional risks have been thoroughly studied [15] by traditional risk management methodologies, intentional risk management requires a different management approach as actuarial information does not provide sufficient insight on potential attacks. An attacker will target a specific asset depending on the value of the asset for the attacker, the risk they run to launch the attack and the cost they incur to execute it [16]. The most attractive assets to attack are those with a high value for the attacker. Among these, assets that are highly accessible for the attacker and tend to keep the attacker's anonymity will be the most targeted [16]. Both BTC and ETH fulfil these characteristics and are already becoming a prime target for cyber-attackers, in particular through crypto-currency exchanges [17]. Intentional risk managers need to identify which assets are the most coveted objectives for the attackers so that they can protect them more effectively. In this article, we apply the concept of intentional risk management to BTC and ETH to increase the resilience of this "supersystem".

1.8. Structure of the Paper

We have introduced the concepts upon which we anchor our hypothesis to model public blockchains such as BTC and ETH as complex networks that create a SoS of public blockchains to better understand and manage their complexity and, more specifically, their resilience against intentional risk. The rest of the article is organised as follows. Section 2 describes the state-of-the-art with regard first to blockchain, BTC and ETH as complex networks, second to SoSE and third to intentional risk management. Section 3 presents our methodology to model BTC and ETH as SoS. This section enumerates the SoS characteristics that we study in BTC and ETH. Section 4 describes the results of our analysis. Section 5 draws conclusions on the utility of SoSE to understand public blockchains and on how to improve resilience in a SoS devoted to transferring digital value and composed of BTC, a stable non-inflationary money, and ETH, a world financial computer system. Finally, Section 6 suggests future lines of work.

2. Related Works

2.1. Blockchain: When Technology Changes Society

Blockchain can be used, among many other use cases, to create a ledger, i.e., a chain of blocks with records representing financial transactions. Some digital ledgers are not based on chaining blocks but on directed acyclic graphs (DAG), Suciu et al. [18] compare both design options.

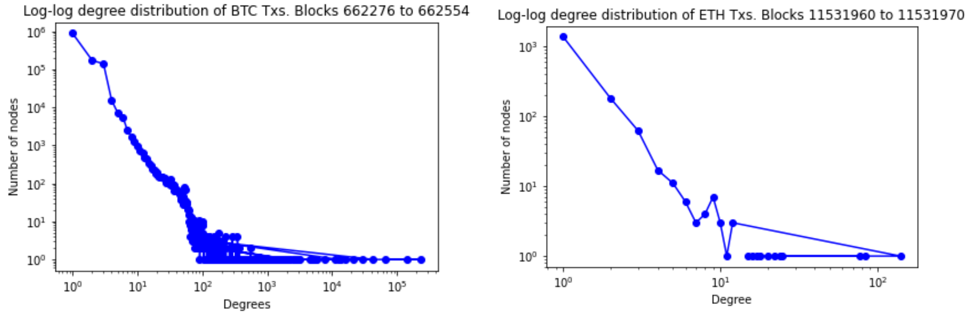
This is the case of IOTA, a public Internet of Things (IoT)-focused distributed ledger. Different digital ledgers can interact between each other, e.g., Thomas et al. [19] propose a protocol for interledger payments. Ripple uses the Interledger protocol (ILP) to connect bank systems across borders. The Ripple token (XRP) provides a standardised settlement layer across different digital asset ledgers [20]. The potential impact of blockchains in our society is immense. Blockchain is a politically non-neutral technology close to the social contract ideas of Hobbes and Rousseau [21]. There are many blockchain use cases in finance [22–25], governmental processes [2], supply chain management [26], identity management [9], legal contracts [27], health data [28], land registry [29], transport systems [30] and even cybercrime trading [31], among many others. Blockchains transcend the field of technology. Reijers et al. [21] mention that blockchain has implications on sociology and philosophy and Malone [32] introduces the idea of a potential end to central banking with the shift from fiat currencies to crypto-currencies. Understanding public blockchains better and explaining their potential in an unbiased manner to society would lead to broader adoption [33].

2.2. BTC and ETH: Public Blockchains as Complex Networks

In our quest to model BTC and ETH as a SoS, we first provide a collection of references that study both BTC and ETH using complex network theory to describe the behaviour of these networks. A comprehensive taxonomy is an optimal entry point for a systematic approach to blockchain implementations [34,35]. The existing literature on complex network theory addressing BTC is a valid sign of the complexity of the BTC network. One of the first complex network analyses of BTC transaction and user networks dates already from 2011 [5]. Reid and Harrigan [5] treat two networks, one in which BTC transactions are nodes and links are coin flows, and another one in which users, i.e., a collection of addresses, are nodes and links are coin flows as well. In the mentioned paper, the objective was to study anonymity in the BTC network. Later on, in 2014 and 2018, respectively, a new complex network analysis of BTC focused on preferential attachment confirmed that "the rich get richer" in BTC [36,37]. From a purely computational standpoint, a big data analysis framework facilitates the study of the BTC network [38]. The links of BTC with society in general and with financial markets in particular [39–41] indicate, as well, a degree of complexity that transcends traditional systems engineering.

In 2018, the degree distribution, degree assortativity, clustering coefficient and largest connected nodes in both BTC and ETH were both objects of study from a complex network viewpoint [42]. These network properties display evolutionary characteristics, i.e., they vary throughout time: their transaction networks are constantly changing with relatively low node and edge repetition ratios. According to [42], unlike typical growing networks, BTC and ETH networks do not always densify over time. This fact confirms the complexity of both BTC and ETH as systems. Complex networks analysis focused on ETH, similarly to those rotating around BTC, shows, as well, the system complexity that the ETH network entails. In 2018, Somin et al. [43] identify power law properties in both in and out degree distributions of the ETH transaction network. Guo et al. [44] reach similar conclusions in 2019. In 2020, Lin et al., Ferretti and D'Angelo and Somin et al. [45–47] continue this line of work regarding power law functions in degree distributions in both ETH and ERC20, i.e., ETH-based token networks. Collibus et al. [48] confirm this fact in 2021 and conclude that their transaction networks present super-linear preferential attachment.

A power law behaviour in a degree distribution reveals that there is a low number of nodes, in this case BTC and ETH addresses, receiving and starting a high number of edges, in this case BTC and ETH transactions, respectively, and a very high number of nodes with a very low number of edges. A typical "rich get richer" phenomenon. Figure 1a,b, inspired by [9] and produced with our own Python code [49], shows two examples of this degree distribution behaviour for BTC and ETH, present even in very short windows of time. Table 1, a simulation parameters table, shows the details of these time slots.



(**a**) (**b**)

Figure 1. Typical power-law transaction degree distributions. (**a**) BTC degree distribution. (**b**) ETH degree distribution.

Table 1. Simulation parameters related to BTC and ETH degree distributions.

Blockchain Name	Window Duration	Date	Number of Blocks	Average Number of Transactions per Block
BTC	48 h	21 December 2020	278	2000
ETH	2 min	26 December 2020	10	144

2.3. Approaching Systems Engineering: Open vs. Closed Systems

The study of complexity in Engineering has been a challenge for the last centuries. Already in 1956, Schlager [50] qualified The Bell Telephone Laboratories as the first organisation to use the term systems engineering: "when satisfactory components do not necessarily combine to produce a satisfactory system", systems engineering comes into play. In 2008, Jamshidi [13] edits a collection of articles focused on complex systems whose elements are complex as well. This new field is called System of Systems (SoS) and the discipline to design, integrate and manage these systems is System of Systems Engineering (SoSE).

Traditionally, Systems Engineering (SE) distinguishes between open and closed systems. SoSE follows a similar approach. We find the first SoS in Nature [51]. Natural SoS are continuously developing and evolving. They are self-organised and self-regulated and respond to evolving needs [51]. These properties are known as open systems characteristics. Examples of these are open interfaces, modular design principles and reconfigurable architectures. Closed immutable architecture strategies create SoS that are not available to outsiders or at a very high license cost [51]. Contrary to man-made SoS, there are no closed natural SoS. Open systems display self-governance principles such as self-control via "feedforward" and "feedback" mechanisms, self-regulation (homeostasis) to maintain their operation and self-organisation to allow for growth and complexity management [51]. Openness and evolution capacity are important anchors for our analysis as well.

2.4. Open Systems Principles

Entropy grows continuously in systems with closed interfaces. In contrast, open interfaces contribute to effectively handling complexity [51] and, consequently, entropy as well. Open systems use open interfaces to exchange energy, material and information with the outside world [51], i.e., they interact cooperatively (*synergy* principle) and they govern themselves (*self-government* principle). As a consequence, this self-organisation brings new structures, patterns and properties that do not exist in each of the components *per se* (*emergence* principle). One of these properties, paradoxically, can be a higher degree of freedom within the system. In addition, natural open systems aim to conserve energy by reducing waste as much as possible, blurring the line between waste and resources. Human-engineered systems still struggle with this *conservation* principle and with the *reconfiguration* principle as well, the latter being the possibility to adapt to changes in the environment. Finally, the *symbiosis* principle requires that all component systems, i.e., holons, benefit from participating in the system and the *modularity* principle focus on the boundaries of each component and on its level of specialisation, independence and variety of use. In an attempt to describe SoS based on their context, Gorod et al. [52] suggest using autonomy, belonging, connectivity, diversity and evolutive emergence. These properties facilitate the distinction between traditional systems and SoS [13].

2.5. Network-Centricity in Systems of Systems

Systems in a SoS interact with each other, exchanging information through a communications network. Network-centricity [13], or net-centricity [53], usually brings along the possibility for new holons to join the network and, hence, the SoS [13]. A service-oriented architecture (SOA) consisting of information service providers, service consumers and service registries is a typical design option for network-centric engineered SoS. The integrity and availability, and sometimes the confidentiality as well, of the information flows within and between network-centric SoS is paramount for their resilience [9]. At the time of writing, no published scientific study addresses the behaviour of complementary public blockchain implementations such as BTC and ETH from a network-centric SoS perspective. Federalism is an alternative way to analyse complex constructs through the political and managerial lens. Federations of systems usually present a strong sociopolitical dimension and a geographical dispersion [54].

2.6. Paradoxes in SoS Management

The existence of a paradox in a SoS is an expression of tension and complexity. SoS engineers see a paradox as a source of innovation rather than as a source of confusion [13]. We find paradoxes in the boundaries, the control and the characteristics of a SoS. In Section 4, we present a collection of paradoxes present in both BTC and ETH. They are clear expressions of tension and complexity but, ultimately, signs of innovation and new ways of thinking brought by these public open blockchain implementations.

2.7. Blockchain as a System of Systems

At the time of writing, few articles study a specific public blockchain implementation as a SoS; however, they do not suggest that a set of blockchain implementations could create a SoS. Roth [55], in 2015, performs a functional analysis of BTC as a SoS using the Systems Modeling Language (SysML) and considers BTC as a component system within the "traditional" financial SoS, as the current "sovereign money-based" financial system works as a SoS as well [55]. Reference to other potential blockchain-based holons is limited to how alternative coins could make that SoS more robust by adding redundancy to the SoS [55]. There is no mention of complementary use cases as we suggest it happens with BTC and ETH. More generally, Mylrea [56], in 2019, refers to how a blockchain-based distributed energy organisation can contribute to modernising, in an autonomous manner, a SoS such as the US power grid. The cases that Jamshidi presents as SoS [13], such as the airline industry, critical infrastructures, wireless sensors, service provision, space exploration, navigation and transportation networks, motivate our hypothesis to model public blockchains such as BTC and ETH as a SoS as well.

2.8. Intentional Risk

Given the current rise in public blockchain implementations, it becomes crucial to understand their characteristics and how we can better secure them, i.e., make them more resilient. Traditionally, information risk management has been based on an actuarial approach, using the typical impact vs. probability graphs. A specific risk was quantified as the product of the probability for that event to happen times the impact of that event happening [57], anchoring the probability on the frequency of past events. In 2015, a proposal to break down cybersecurity risks into intentional and non-intentional, the latter also named accidental, introduced an important element: the existence of ill-intentioned actors [57] who target information systems to extract value out of them, considering intentionality as the backbone for cyber-risk management [16].

Intentional risk can be static or dynamic, depending on whether the attacker has authorised access to the target system or not [16]. Static risk-based attackers make use of authorised paths to access their objective and dynamic risk-based attackers make use of any possible but unauthorised path to carry out their plan. The three parameters that Chapela et al. [16] use in their model to manage intentional risk are value, accessibility and anonymity. They propose a model to manage intentional risk in non-linear systems based on complex network analysis [16]. Using network theory, introduced in Section 1.5, the more connected a node is, i.e., the more accessibility a computer system has, the greater the risk is for it to be compromised. The study of identity management resilience against intentional risk in blockchain-based Internet of Things (IoT) platforms is an example of this [9]. Typical intentional risks against blockchain are the 51% vulnerability, double spending, private key compromises and smart contract exploitation [58].

Table 2 summarises our research on the current state of art: the description of the blockchain technology, the complex network analysis of BTC and ETH, the concepts of SE and SoSE and intentional risk management. Our contribution focuses on modelling public blockchain implementations as a SoS to better manage their resilience against intentional risk.

Table 2. The role that related works play to build our contribution.

Topic	Study	Main Takeaway	References
Blockchain technology	Many use cases	A driver for change	[18–21]
		Impacting many sectors	[21–25,28–33]
Key implementations: BTC & ETH	As complex networks	Power law degrees	[5,34–41]
		"Rich get richer"	[9,42–48]
Systems Engineering	Complexity	Open vs. close systems	[51]
SoSE	Supersystems	5 SoS properties	[13,52]
	Network-centricity	Info exchange	[9,13,53]
Blockchain as SoS	Only focus on BTC	No complementary roles	[13,55,56]
Intentional risk	Attacks	Static vs. dynamic risk	[16,57,58]
	Parameters	Value, accessibility and anonymity	[16,57]
Our contribution			
Public blockchains	Modelled as a SoS	To improve resilience against intentional risk	[55,56]

3. Methodology and Implementation

3.1. Research Methodology

Our research question focuses on how to model BTC and ETH as an open SoS of public blockchains in which they are component systems. This is a novel approach, hardly explored so far, with the objective of better understanding the role that public blockchains play and will play in society and how they can be protected from ill-intentioned attacks, i.e., their resilience against intentional risk.

Generally speaking, we propose a five-step methodology to model a set of systems as an open SoS. In this particular case, we introduce the hypothesis that the two most market-capitalised crypto-currencies by the end of 2021 [3], BTC and ETH, can be modelled as components of an open SoS.

First, following the definition of SoS used in Section 1.6, we identify a common goal for the SoS of public blockchains. Second, we confirm that BTC and ETH are open systems with growing complexity. Third, we study net-centricity in BTC and ETH. Fourth, we use the characteristics proposed by Gorod et al. [52], i.e., autonomy, belonging, connectivity, diversity and emergence, to model BTC and ETH as a SoS and analyse them based in the balance panel proposed in [13]. Fifth, out of a vulnerability and threat analysis, we propose ways to improve the resilience of this particular SoS case study against intentional risk based on the parameters of value, accessibility and anonymity proposed by Chapela et al. [16]. Table 3 depicts our methodology.

Table 3. SoSE-based methodology to manage complex "supersystems".

Step	Label	Description	Why?
1	Common goal	Component systems share an ultimate goal	Definition of SoS
2	Open & Complex	Open systems with growing complexity?	Continuous evolution
3	Network-centric	Components use networks to communicate	Information exchange
4	Characteristics	Autonomy, Belonging Connectivity, Diversity Evolutive emergence	SoS Balance panel
5	Risk analysis	Vulnerabilities and threats Resilience against intentional risk	Future evolution

3.2. Methodological Implementation

- Step 1: Identification of a SoS.
  A System of Systems (SoS) exists when its components are independent complex systems that interact with each other to accomplish a common goal [13]. We postulate

that BTC and ETH are the two most prominent components of the SoS of public blockchains. They are two different systems, both with the goal of offering a digital distributed network of value;

- Step 2: Open systems with growing complexity.
  Once we identify a SoS of public blockchains, our second step is to determine whether BTC and ETH are open systems. As we have seen in Section 2.4, openness facilitates the inclusion of new components into a SoS. Under these premises, Section 4.2 analyses BTC and ETH as open systems with growing complexity;
- Step 3: Network centricity.
  The rapid development of information networks such as the Internet has facilitated interactions among SoS via network services up to the point that we talk about net-centric SoS. The existence of a service-oriented arquitecture (SOA) on top of a data network is a key characteristic for net-centric or network-centric SoS, also named net-centric enterprise systems [53]. Section 4.3 explores a service-oriented architecture (SOA) in BTC and ETH. More holistically, elements such as people, organisations, cultures, activities and interrelationships enable both systems to interact [13];
- Step 4: SoS characteristics.
  We characterise a SoS based on its properties as a more optimal way to comprehend its complexity instead of just framing it with a definition [52]. Chapter eight in [13] presents the SoS context based on five characteristics: autonomy, belonging, connectivity, diversity and evolutive emergence. In Section 4, we analyse these five characteristics for both BTC and ETH, and use the balance panel for each of them:

  (a) Autonomy.
  Autonomous systems operate independently [13]. We analyse BTC and ETH governance models, based on informal consensus. They are both independent. We describe key stakeholders such as their development and support communities and how they reach design decisions and try to avoid software forks while maintaining project legitimacy;

  (b) Belonging.
  The property of belonging to a system relates to its vision [13]. We explore BTC and ETH visions and identify opt in and opt out possibilities within the system and the balance that they strike between centralisation and decentralisation in mining power, community support, number of users and contributing developers;

  (c) Connectivity.
  We study how BTC and ETH interact between one another [13], especially in a scripted manner, and determine their common underlying technical foundation. We also determine whether the identified network-centricity is growing and examine the price correlation that both currencies show. From the platform viewpoint, we focus on their mining reward and supply models;

  (d) Diversity.
  A SoS achieves diversity if its holons are different to each other. We refer to leadership structure, range of business cases to answer, appetite for change and potential reasons to join these networks as proxies to understand the diversity present in this SoS;

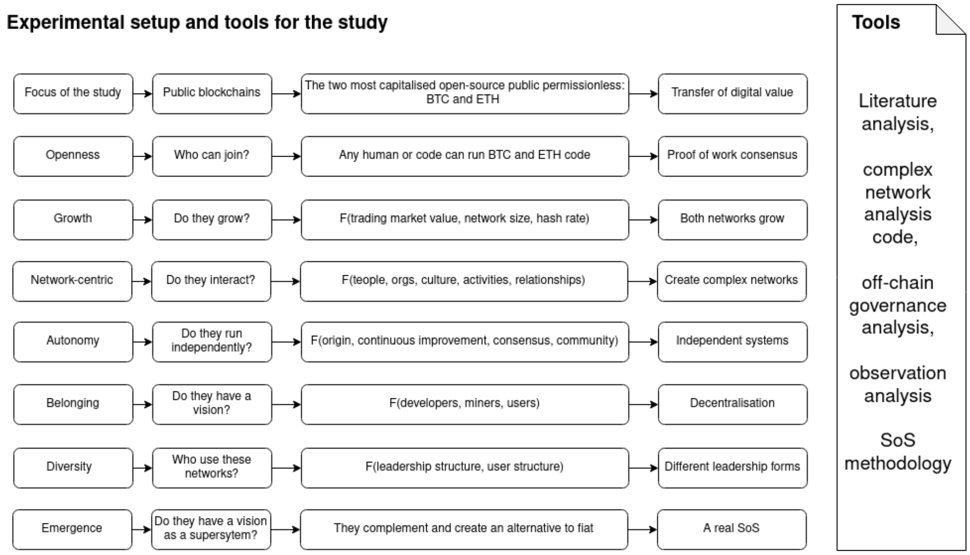
  (e) Emergence.
  A pivotal feature of any SoS is the appearance of both intended and unintended properties that are not detectable in the specific component systems, i.e., holons. Emergence concentrates the added value of using SoSE. We compare the initial vision of the SoS of public blockchains [4,8] with its current use in two different levels, i.e., SoS-wide and holon-specific, and we identify properties that emerge from considering BTC and ETH as part of a more comprehensive system. We analyse the geopolitical consequences of this new financial SoS;

- Step 5: Vulnerabilities and threats. Resilience against intentional risk.
  We complete this analysis with the vulnerabilities we identify in the SoS and the threats it is exposed to. We use one of the identified threats, related to intentional risk, to come up with a series of security measures that would increase resilience against intentional risk. For this, we use the parameters proposed by Chapela et al. [16], i.e., value, accessibility and anonymity.

4. Analysis and Results

4.1. The System of Systems of Public Blockchains

We apply the methodology proposed in this article to understand and better manage the complexity of public blockchains. We consider that BTC and ETH are the two most prominent components of the SoS of public blockchains. They are two different open-source code implementations. They attract a very diverse community of users and proponents, however, they both share the common goal of transferring digital value. Figure 2 explains, step by step, how we conduct our methodology with keywords focused on purpose (first column), brief explanation (second column), main elements analysed (third column) and eventual conclusions (fourth column). We also add a fifth column to list the main tools that we use for our analysis. With regard to our complex network analysis code, implemented in Python, we make it available via github [49].


Experimental setup and tools for the study
Tools
Literature analysis,
complex network analysis code,
off-chain governance analysis,
observation analysis
SoS methodology

Focus of the study	Public blockchains	The two most capitalised open-source public permissionless: BTC and ETH	Transfer of digital value
Openness	Who can join?	Any human or code can run BTC and ETH code	Proof of work consensus
Growth	Do they grow?	F(trading market value, network size, hash rate)	Both networks grow
Network-centric	Do they interact?	F(teople, orgs, culture, activities, relationships)	Create complex networks
Autonomy	Do they run independently?	F(origin, continuous improvement, consensus, community)	Independent systems
Belonging	Do they have a vision?	F(developers, miners, users)	Decentralisation
Diversity	Who use these networks?	F(leadership structure, user structure)	Different leadership forms
Emergence	Do they have a vision as a supersytem?	They complement and create an alternative to fiat	A real SoS

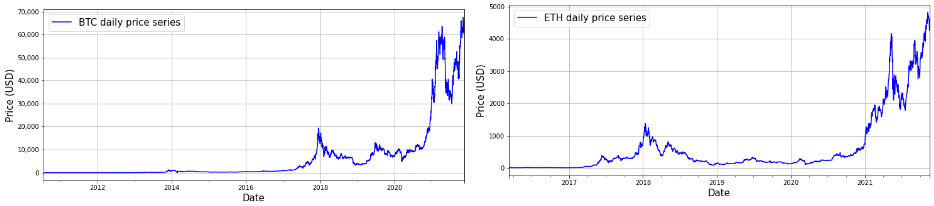
Figure 2. Experimental setup and tools for the study.

4.2. Openness and Growth

BTC and ETH are two independent public blockchain implementations. Public blockchain implementations are permissionless, i.e., they pose no obstacle to joining their network and sending transactions as a user or validating them as a node. Any code-based artifact using BTC or ETH open-source code, driven by a human being or by a script, with access to a private cryptographic key, does not require any third-party approval to participate in the network. In other words, any individual or human-made device with the possibility of running a BTC or ETH wallet or node can join these networks and perform transactions. Equally, they can also join the mining community and create new bitcoins or ether, their corresponding crypto-currencies, while verifying transactions, as long as they commit to "demonstrate commitment to the system" using proof of work-based consensus. Alternatively, some blockchain implementations propose the use of proof of stake [7]. In addition, BTC and ETH show a distinctive feature of open systems: they exchange energy and information with the outside world [51]. They exchange information with social, financial and human environments, and they display mechanisms to adapt to those environments and evolve accordingly. We use three dimensions to confirm this point: their trading market, the network size and their hash rate:

(a) Trading market: It is possible to buy and sell BTC and ETH coins. Both BTC and ETH are two public blockchain implementations that have attracted growing attention in the financial markets. Although their daily market price and their hash rate fluctuate considerably, both dimensions, price and total hash rate, have grown relentlessly for the last five years.
Figure 3a depicts the daily BTC market price since its start. The upward trend is patent. BTC market capitalisation as a cryptoasset is growing. Equally, Figure 3b depicts the daily ETH market price since its start. An upward trend is patent as well. These steep climbing prices attract new users, both retail and institutional, generating more transactions. In July 2020, BTC market capitalisation reached USD 170 B; less than a year later, in April 2021, the figure topped USD 1099 B, going up to USD 1142 B in November 2021 [3], paving the way for an incessant growth during this decade. The Ethereum cryptoasset had a market capitalisation of USD 26 B in July 2020. In April 2021, this figure was of USD 222 B. In November 2021, the market value of ETH led to a capitalisation of USD 505 B [3];

(b) Network size: As price and network size are positively correlated in both BTC [59] and ETH [48], their networks grow. According to bitnodes [60], there were around 10,540 full active BTC nodes in July 2020 while, surprisingly, there were around 9610 nodes in April 2021. A node is a BTC server that keeps a copy of the entire blockchain and validates transactions. A miner node is a node that validates blocks. In November 2021, the number of active BTC nodes reached 13,898. The trend in ETH is the opposite: according to ethernodes [61], there were close to 7900 active ETH nodes in July 2020 and over 4250 in April 2021. In November 2021, ref. [62] counted 3238 nodes. Table 4 summarises the BTC and ETH figures mentioned.



(**a**) (**b**)

Figure 3. Daily market price (source: investing.com, accessed on 16 November 2021). (**a**) Bitcoin (BTC). (**b**) Ethereum (ETH).

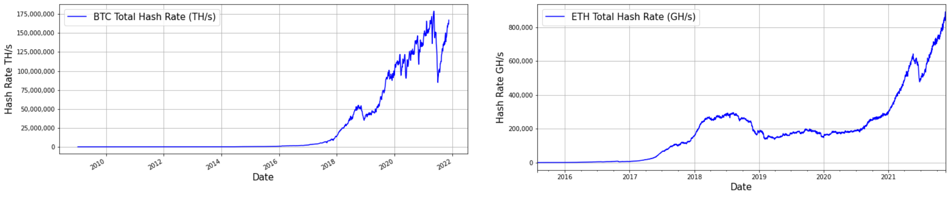
Table 4. Key Bitcoin and Ethereum figures.

Blockchain	Start	Active Nodes			Market Cap (USD B)		
Name	Date	7/2020	4/2021	11/2021	7/2020	4/2021	11/2021
BTC	2009	10,540	9610	13,898	170	1099	1142
ETH	2014	7900	4250	3238	26	222	505

Network growth is visible in the address space. A node in each of these networks is an address (see Section 2.2). By design, based on the recommendation not to re-use addresses in transactions, address spaces continue growing in BTC and ETH since their inception. This continuous growth contributes to their distributed nature and to their complexity as addresses do not expire. Equally, block validation, i.e., mining, generates new coins as well, bitcoins and ether, respectively, increasing the number of coins circulating in the systems;

(c) Hash rate: Third, hash rate measures the computing power, i.e., calculation complexity, required to mine BTC and ETH blocks. Figure 4a,b shows how, especially since

2020, hash rates also increase. Both dimensions, market price and hash rate, indicate that the complexity of these systems, consequently, grow with time. They find themselves in a *causality dilemma*, and this is an inherent signal of complexity [63].



(**a**) (**b**)

Figure 4. Total Hash Rate. (**a**) Bitcoin (TH/s) (source: blockchain.com, accessed on 18 November 2021). (**b**) Ethereum (GH/s) (source: etherscan.io, accessed on 18 November 2021).

We can broaden our focus and infer that a SoS of public blockchains is therefore an open system that can potentially grow in complexity.

4.3. Network Centricity

BTC and ETH are network-based protocols. Network participants exchange information via open-source application programming interfaces (APIs). Typical actions are, e.g., creating an address, sending an amount to an address, validating a transaction and requesting information on a transaction or on a block. Examples of these APIs are the BTC remote procedure call (RPC) and the ETH javascript (js) APIs [64,65]. Functionality is then bundled into services provided by nodes and consumed by clients. These APIs are examples of a basic distributed service-oriented architecture (SOA). They confirm the network-centricity of BTC and ETH. Table 5 summarises the network-centricity of the SoS itself using the elements suggested by Jamshidi [13] together with a forecast on how their relevance will change in the near future:

Table 5. Network-centricity in public blockchain SoS.

Interaction via	Description	Relevance
People	Holders of crypto keep BTC and ETH in their portfolio	Increasing
Organisations	Crypto exchanges offer swaps between BTC and ETH and other coins	Increasing
Culture	BTC and ETH share decentralised principles	Stable
Activities	Coin wrapping, e.g., WBTC: an ERC20 token in ETH	Increasing
Relationships	Both subject to additional financial regulation	Increasing

We find similar interactions between other public blockchains running on their own platforms, i.e., mainnets, present in this SoS. Solana (SOL) and Algorand (ALGO) are two examples, the 5th and 20th most capitalised crypto-currencies in November 2021 [3]. In general, they interact with each other via common users, crypto-exchanges, basic design principles and wrapping techniques. Coin wrapping enables cryptoassets to be used on another blockchain, different to the native one. For example, wrapped BTC (WBTC) is an ERC20 (ETH-based) token that represents BTC 1:1 in the ETH network. Finally, as all of them are public blockchains, they are subject to any financial regulation that might potentially impact all public blockchain implementations.

4.4. Autonomy

BTC and ETH operate independently. They both run a separate off-chain governance model based on informal consensus. The role of Lead System Integrator [66] is crowd-sourced to a reduced number of developers supported by a large community. The seminal BTC paper by Nakamoto [4] defines, at a high level, the first BTC design decisions. The first open-source BTC client was made public on 9 January 2009. Once Nakamoto left the project in 2011, the so-called "Bitcoin core developers", Gavin Andresen, Pieter Wuille, Wladimir van der Laan, Gregory Maxwell and Jeff Garzik, took over the BTC protocol development and software maintenance. The number of developers able to commit code to "Bitcoin core" remains stable: 37 in April 2021 and 39 in November 2021 [67]. Changes to BTC require ample consensus [68]. Anyone in the community can launch a BTC improvement proposal (BIP) [69]. The search for consensus among key stakeholders, i.e., developers, miners (node operators) and users, is a top priority. Their aim is to avoid the threat of forking the protocol [68], either in a soft or hard way. Soft forks guarantee backward compatibility and hard forks do not. A software fork introduces changes in the code from a specific point in time. Similarly, the ETH protocol [70] works with Ethereum Requests for Comments (ERC). They eventually translate into Ethereum Improvement Proposals (EIPs) that need to reach sufficient consensus [71]. The number of ETH developers who can commit code is growing slightly: from 69 in April 2021 to 81 in November 2021 [72], as Table 6 displays. On independence, every BTC and ETH stakeholder can decide independently from each other. Ultimately, anyone in BTC or ETH could fork the protocols and start a new project. It would be up to their ability to entice users to use the new forked code. A key concept in both BTC and ETH is legitimacy, or a pattern of higher-order acceptance [73]. Already, through the study of autonomy in public blockchains, we distinguish at least two of the three typical paradoxes identified in chapter eight of [13], i.e., control and team paradoxes. There is tension present regarding where decision power resides and the balance between individuality or autonomy and team membership or belonging. Broadening our focus to a SoS of public blockchains, and based on these results, we infer that it consists of independent blockchain implementations.

4.5. Belonging

The original vision of BTC is the creation of a "purely peer-to-peer version of electronic cash" [4]. BTC and ETH are digital assets with no intrinsic value and no centralised issuer [8]. The vision of ETH is to build "a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralised applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions" [8]. In both blockchains, the three main related communities, i.e., developers, miners and users, can opt in and out of the SoS at any moment. This is a sign of an open system. The first paradox mentioned in chapter eight of [13], i.e. the boundary paradox, or the need to keep some things in the systems and some things out of the system simultaneously, is patent as well in public blockchains, e.g., in the on-chain vs. off-chain information storage dilemma.

On centralisation, the three main sources of critiques are: the very reduced number of developers with commit privileges in both blockchains, see Section 4.4, the location of most of the BTC mining power and the location of most of the BTC nodes. With regard to miners, China hosted over 65% of BTC mining power until October 2020. The main reason was the electricity oversupply and corresponding reduced prices of hydroelectricity in areas such as Sichuan. The price of electricity is a key driver for miners to interact [74]. After the nation-wide ban in July 2021, China abandoned BTC mining [75]. In November 2021, the USA (35.1%), Russia (11.9%) and Kazakhstan (13.8%) account for the top three mining countries. With regard to full active BTC nodes, the USA and Germany host close to 13% of them, although this figure is less than the 20% of nodes that each of these two countries had in April 2021 [60]. Regarding ETH, 34% of active nodes resided in the USA and 22% in Germany on April 2021, while, in November 2021, the US hosted 35% and Germany decreased to 15% [61]. See Table 6.

Regarding decentralisation, the Ethereum foundation ethereum.org (accessed on 1 December 2021) organises most of the support to the ETH community. A similar foundation project exists for BTC bitcoin.org (accessed on 1 December 2021). However, none of these foundations own the ETH or the BTC networks. Both networks are public like the Internet. With over 13,000 active BTC nodes and over 3200 active ETH nodes (see Table 4), the degree of active node decentralisation is higher in BTC than in ETH, where we identify that the number of active nodes is reducing. The decrease in ETH nodes is a worrying trend, particularly given the big drop in September 2021 [76]. Estimations in February 2021 set the number of BTC users over 71 million and the number of ETH users over 14 million, with 25% of them owning both crypto-currencies [77]. Both the BTC and ETH user communities are growing. Although the number of core developers for both BTC and ETH is rather limited, see Section 4.4, the number of active contributing developers has reached close to 500 members in BTC and more than 1000 in ETH [78]. Based on these figures, we still see more evidence tilting the *belonging* feature towards decentralisation than to centralisation in the SoS of public blockchains.

Table 6. BTC and ETH autonomy and belonging related figures.

Blockchain	Users	Contrib.	Core Developers		Active Node Location (%)	
Name	**(M)**	**Devs.**	**4/2021**	**11/2021**	**4/2021**	**11/2021**
BTC	71	500	37	39	CN (65)	US (35), KZ (14), RU (12)
ETH	14	1000	69	81	US (34), DE (22)	US (35), DE (15)

4.6. Connectivity

All BTC and ETH active nodes and clients can enjoy the same power of connectivity. Both BTC and ETH networks are permissionless, i.e., provided that they run the corresponding committed open-source protocol, any compatible running code can join both networks. The study of the connectivity property confirms the network-centricity of the SoS of public blockchains [13,53]. BTC and ETH active nodes are connected to the BTC and ETH networks, respectively. Both networks run on top of the public Internet. Table 5 lists the means through which they are interconnected. We focus on the scripted interaction, i.e., coin wrapping. In November 2021, around 249,000 BTC [79], out of the 18.8 million BTC already mined by end November 2021, are tokenised in ETH via wrapped BTC (WBTC), an ERC20 token [80]. They are mostly deployed in ETH-based Decentralised Finance (DeFi) projects. This figure is growing. On July 2020, there were only 15,000 tokenised BTC [81] and, on April 2021, there were 141,000 BTC. In terms of price, BTC–ETH correlation has been permanently positive since 2018, close to 0.8 during 2019 and 2020. During November 2021, BTC–ETH price correlation was over 0.75 [82].

From the platform-centric viewpoint, BTC and ETH miners verify transactions and receive a reward for it. These transactions fill up a BTC block. Miners receive newly created bitcoins and ether, respectively, when they finalise a block, i.e., they “mine” a block. In the case of BTC, this block mining reward is halved after 210,000 blocks. The current reward of 6.25 BTC started on 11 May 2020. Those miners with a higher hash rate, i.e., computing power, enjoy a higher probability of mining a block. Once all 21 million BTCs are mined, and this will happen around the year 2140, the question of whether transaction verification income, based only on transaction fees, will be still profitable for miners remains open. Taproot, the latest BTC upgrade, performed in November 2021, aims to scale up the number of transactions that the network can cope with and to increase privacy by complicating the identification of participants in a transaction [83]. With regard to their monetary policy, while BTC supply is deflationary, i.e., limited to 21 million, ETH supply is inflationary, i.e., there is a maximum yearly new supply of 18 million ETH. Both networks show an increased connectivity. However, they have been criticised for demanding high transaction fees during times of heavy use and overall network growth. BTC aims to solve this challenge with BTC Lightning Network (BLN) and ETH with ETH 2.0. BLN collects transactions first off-chain and uses scripting to guarantee integrity [84]. ETH 2.0 promises scalability based on a multi-chain concept (sharding) [85].

In general, interledger communications such as Interledger Protocol (ILP) enable the possibility of connecting different public blockchain implementations through code-based connectors, between BTC and ETH as well. This means that a BTC transfer can end up as an ETH sum via an ILP connector in an ETH address.

4.7. Diversity

First, we identify basic differences between BTC and ETH that make them even more complementary: BTC appears as a leaderless public blockchain with a broad user population and decentralised governance. Although its degree distribution approximates a power law function [36,37], its control structure is highly decentralised. ETH degree distribution resembles a power law function [48] and its leadership structure is more precise. ETH attracts more experimentation and innovation and it is more multi-faceted than BTC. Second, we focus on the diversity existing in the three main stakeholder communities for BTC and ETH: miners, developers and users, to understand the current balance between homogeneity and heterogeneity. Mining pools are groups of miners that share computing power, i.e., hash rate. None of them reaches 51% of the total BTC hash rate [86]. Only if the five biggest BTC pools would collude, they could opt to attempt a 51% blockchain control attack to modify a transaction. A similar situation applies to ETH [87]. Regarding development, there is more activity in ETH than in BTC: there are more than 300 BIPs [69] but more than 3300 EIPs [88]. As mentioned in Section 4.4, the number of core developers in both networks is reduced, although ETH attracts more developers than BTC. From the user perspective, the increase in users is initially a good proxy for heterogeneity growth. Early adopters of BTC were libertarians and techno-anarchists [89]. In 2021, many other profiles join both networks, partially disgruntled by the highly expansionary monetary policies followed by key central banks.

4.8. Emergence

We first refer to the intended emergent properties and second to the unintended ones. Table 7 provides a summary of the emergent properties that we identify in this SoS and its components.

Table 7. Intended and unintended emergent properties.

Realm	Emergent Property	Intended
SoS	Decentralised network of digital value	Yes
SoS	Alternative to fiat-based financial system	No
BTC	Peer to peer electronic cash system	Yes
BTC	Digital global reserve asset (“digital gold”)	No
ETH	The world distributed computer	Yes
ETH	Main DeFi platform (“alternative financial conduit”)	No
ETH	Platform to transfer “unique” digital value	No

4.8.1. Intended Emergent Properties

The intended emergent property of the SoS of public blockchains is to provide a decentralised network to transfer value: in the case of BTC, via a digital asset that has no intrinsic value in itself. In the case of ETH, via a Turing-complete protocol able to implement decentralised applications. Public blockchain implementations use a digital asset with no intrinsic value. This digital asset represents digital private property in three different ways: as native crypto-currencies, such as bitcoin and ether, and, in the case of ETH, as fungible tokens (ERC20 tokens) and as non-fungible tokens (ERC721 and ERC1155 tokens). Public blockchains offer a channel through which to transfer digital private property, i.e., digital value.

4.8.2. High-Level Unintended Emergent Property

Considering our analysis of the SoS of public blockchains, we estimate that the high-level unintended emergent property of a SoS of public blockchains is to stand as an alternative to the financial system based on fiat currencies, established in 1971 with the cancellation of the direct convertibility of the USD into gold. We find two competing and distinct SoS, the traditional centralised financial SoS and the open SoS of public blockchains. Neither BTC nor ETH included this key property of aspiring to become an alternative financial system in their seminal white papers [4,8]. Figure 5 depicts the results of our SoS characteristics-based analysis [13].

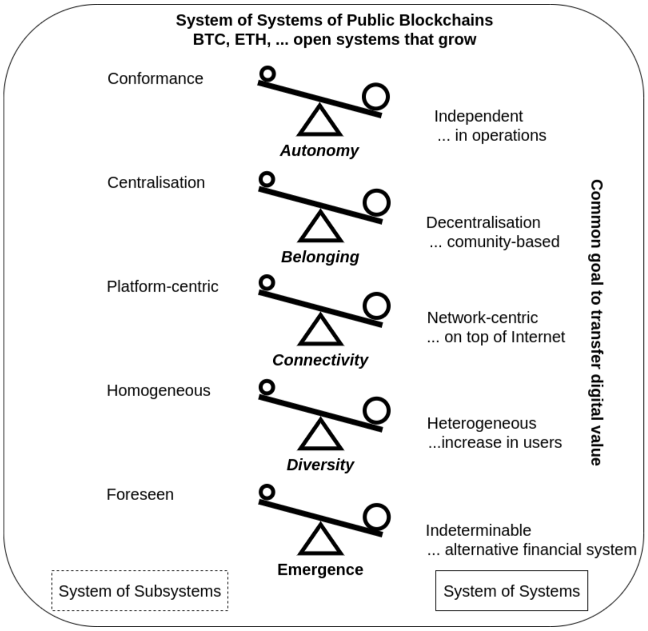


Figure 5. Public blockchains. SoS characteristics balance panel.

4.8.3. Holon-Specific Unintended Emergent Properties

More specifically, BTCs unintended emergent property is to become a global reserve asset, i.e., the "digital gold". The expanding fiat currency monetary policy since 2008, plus the performance difficulty for BTC to achieve high transaction speeds, in contrast to other blockchain implementations [90], transforms BTC into a digital value reserve more than into an instant peer to peer payment system. However, initiatives such as BLN [84] and the taproot upgrade [83] aim to increase transaction rate. An initially unintended emergent property of ETH is to act as main underlying blockchain implementation for Decentralised Finance (DeFi). DeFi translates, via smart contracts, most of the financial activities present in the traditional centralised financial system such as lending, borrowing, trading, using derivatives and depositing funds. We define it as the "alternative financial conduit" system. ETH's "distributed world computer" is the distributed platform in which an entire financial system, based on fungible tokens, is beginning to run. Stablecoins constitute the means of settlement in this distributed financial system. The total capitalisation of stablecoins in November 2021 is USD 145 B, from USD 60 B on April 2021 [91]. A stablecoin is a crypto-currency whose value is pegged to either a fiat currency, mostly the USD, or to a basket of assets.

Traditionally, the US dollar (USD) plays a dominant role in the world financial system [92]. The fundamental role that the USD plays in finance provides a geopolitical advantage to the US and leverage to apply economic sanctions to other non-allied countries. The arrival of the public blockchain-based SoS impacts this USD dominance. The fact that the most capitalised stablecoins are pegged to the USD [91] confirms the growing geopolitical importance of this new SoS. Other competing geopolitical powers such as China entered the digital coin scenario via their "digital yuan". Central banks around the globe are piloting central bank digital currencies (CBDCs) in an attempt to preserve the "status quo".

With regard to non-fungible tokens, the unintended emergent property of ETH is to act as a platform to transfer "unique" digital private property. NFTs offer a distributed and non-intermediated creativity market. Examples are "Cryptokitties" and "Mutant Apes" [93].

Additionally, a myriad of public permissionless blockchain implementations have launched their own networks, i.e., mainnets, to compete with ETH and to save ETH transaction fees. The appearance of multiple blockchain implementations to answer specific business cases [22] complements the roles of BTC and ETH within this overarching SoS of public blockchains. All these sidechains are also components, holons, in this SoS. Table 8 lists four of the top market capitalised projects in November 2021 according to coinmarketcap [3].

Table 8. Public blockchain projects within the SoS.

Project	**Origin**	**Business Case**	**Market Cap (B USD)**	**Consensus**
Binance Coin (BNB)	2017	Biggest crypto exchange's blockchain	111	Proof of authority
Solana (SOL)	2020	DeFi solution with short processing times	61	Proof of history
Cardano (ADA)	2017	Decentralised app engine	54	Proof of stake
Polkadot (DOT)	2017	Multi-chain focused on cross-chain transfers	37	Nominated proof of stake

We have modelled BTC and ETH as holons of the open SoS of public blockchains and we have identified the emergent property that creates a new distributed "supersystem" of digital private property, i.e., digital value. We present now the result of a threat and vulnerability analysis. One of the threats we identify is precisely intentional risk.

4.8.4. Vulnerabilities and Threats of the SoS of Public Blockchains

We complement the previous results with a vulnerability and threat analysis of the public blokchain SoS. We identify five vulnerabilities:

- Adoption requires understanding.
  The knowledge-based barrier to entry is considerable. Participants in this public blockchain-based SoS require understanding of the underlying mathematical, cryptographic and economic concepts upon which both BTC and ETH are built. There is hardly any abstraction layer between users and the internal complex functioning of these blockchains;
- Adoption requires hiding complexity. The user-friendliness of the software tools that interface with this SoS is still very low;
- Early stage of evolution. Even with high rates of adoption and rising market capitalisation, public blockchains are still at a very early development phase. The industry is flourishing and growing fast; however, it has not yet reached any consolidation phase;
- Signs of centralisation. Complex network theory-based literature identifies linear and super-linear preferential attachment in BTC and ETH in their transaction networks [36,37,48,59]. This reveals the higher degree of dependence on specific super-hub nodes in these networks. An additional sign of initial centralisation is the decrease in the number of active ETH nodes [76].
- Governance exclusively dependent on code. The smart exploitation of any programming error in the code that implements elements such as mining rewards, smart contracts and distributed autonomous organisations (DAO, a distributed governance engine) can siphon out funds and make any public blockchain project fail. A real example of this already happened in Ethereum in 2016 [94].

Equally, we observe five threats:

- Regulation. The overall impact that financial regulation will have on the future of this SoS is still unknown. Taxation, legal jurisdiction, cross-border implications and know

your customer requirements are just some examples of key regulatory aspects that are still not fully defined for the distributed SoS of public blockchains;
- Privacy vs. Traceability Trade off. One of the first business cases for the use of BTC was the online black market "Silk Road" [95]. Identities behind BTC addresses were not known. However, anonymity is not a design feature in BTC but, rather, pseudo-anonymity [5]. Ethereum does not offer transaction anonymity either. The lack of auditable and regulated know your customer procedures could hamper the mass growth of public blockchains;
- Future developments in encryption. Bitcoin uses SHA-256 as its hashing algorithm [96] and the Elliptic Curve Digital Signature Algorithm (ECDSA) with the elliptic curve secp256k1 to sign transactions [97]. The taproot BTC upgrade introduces Schnorr signatures [83]. Ethereum uses Keccak-256 [98] to hash transactions and ECDSA to sign them [99]. Future developments in quantum computing [100] could render current cryptographic algorithms used in public blockchains insecure. Should this happen, then the core development communities mentioned in Section 4.4 should react quickly with the corresponding cryptographic upgrade by proposing new key lengths or, alternatively, new algorithms;
- Missing co-operation. The permanent interaction between the SoS of traditional finance with the SoS of public blockchains is not yet defined. The governance frameworks in both systems need to find a common ground to allow for future-proof interactions between both financial proposals;
- Intentional risk. The economic value locked in the SoS of public blockchains is growing. Consequently, the interest of ill-intentioned actors to extract value out of it is also increasing [101]. The future of this SoS will depend on its resilience against intentional risk.

These vulnerabilities and threats pose the risk of impeding mass adoption of this SoS.

4.9. Resilience against Intentional Risk

We start from the definition of profitability associated to the attacker (PAR) proposed by Chapela et al. [16] to quantify intentional risk (Equation (1)). The level of intentional risk *IntRisk* to which a system *SoS* is exposed to corresponds to the maximum product of the <*value*, *accessibility*, *anonymity*/*k*> triplets of their *participant elements e*, being *k* a standard constant we name *legal robustness*, related to the legal consequences that an attacker could face. We propose to optimise as many factors as possible in Equation (1) to reduce the intentional risk that the SoS of public blockchains is exposed to. The reduction in the exposure to intentional risk increases the resilience of the system against it.

$$PAR = \max\left(value_e \cdot accessibility_e \cdot \left(\frac{anonymity_e}{k}\right)\right) \tag{1}$$

As *participant element* in Equation (1), we select the most fine-grained possible component of the open public blockchains we study, i.e., an address. An address in a public blockchain consists of a unique identifier that refers to a public–private cryptographic key pair involved in a transaction either as the origin or destination. We use complex network notation to mathematically state our analysis: for each of the blockchain implementations present in the SoS of public blockchains b_i, we consider a transaction network T_{b_i} in which every address N_{b_i} used is a node and every transaction between addresses is an edge T_{b_i} denoted by $T_{b_i} = (N_{b_i}, E_{b_i})$ being its nodes N_{b_i} and E_{b_i} its edges. We identify three attributes for each N_{b_i}:

- $Va(N_{b_i})$: the *value* as the quantity of cryptocurrency or fungible tokens held by the address N_{b_i}. By design, this is public information. As an example, in the case of NFTs, this attribute simply refers to the *value* assigned by the market to it;
- $Ac(N_{b_i})$: the *accessibility* of N_{b_i}. This is a function of the *accessibility* to its private cryptographic key. Having access to the private key gives the possibility to claim

ownership of $Va(N_{b_i})$. A high $Ac(N_{b_i})$ implies poor protection measures to keep the private key secure;

- $An(N_{b_i})$: the *anonymity* of N_{b_i}. This measures the degree of uncertainty to link N_{b_i} with a screened identity in the physical world. A high $An(N_{b_i})$ implies that N_{b_i} cannot be associated to a confirmed physical identity. Attackers of a public blockchain implementation b_i use a collection of N_{b_i} with a high $An(N_{b_i})$ as consecutive destinations of their fraudulent transactions to make tracking unfeasible.

Regarding the legal robustness k constant, its value indicates how dissuasive legal measures are for attackers to embark on plans to compromise public blockchains.

We increase the resilience of the SoS of public blockchains by minimising the intentional risk that each participating address runs as Equation (2) defines:

$$\forall\, b_i \in SoS, \quad IntRisk_{SoS} = \max\left(Va(N_{b_i}) \cdot Ac(N_{b_i}) \cdot \left(\frac{An(N_{b_i})}{k} \right) \right) \tag{2}$$

Table 9 lists our proposed security measures to increase this SoS's resilience against intentional risk. Their implementation requires a multidisciplinary, i.e., technical, procedural and cultural approach, especially during design, development and operations of the holons of this SoS. The scope of these proposals corresponds to the SoS of public blockchains. Only a SoS-overarching approach, or, at least, a specific focus on BTC and ETH as the two main public blockchain implementations, can increase the resilience of a SoS whose main emergent property is to become a real distributed alternative to the traditional finance system. If we would only focus on one holon, then, following Equation (1), the overall resilience of the SoS would not improve and its adoption would not increase.

Table 9. Measures to increase intentional risk resilience.

Action	Principle	Phase
Reduce asset value	Distribute value across many addresses	Design/Operations
	Avoid very rich hubs	Operations
Decrease accessibility	Maintain the use of strong crypto	Design
	Improve code security	Development
	Simplify interfaces	Development
	Improve private key security	Design/Dev/Operations
	Extend use of cold storage	Operations
	Enhance security awareness in users	Communications
Decrease anonymity	Improve identity management	Operations
	Link with physical identities	Governance
	Achieve global legal coverage	Governance
	Extend blockchain monitoring	Operations
Increase legal measures	Extend know your customer processes	Operations

5. Conclusions

We conclude that:

(a) Our proposed methodology, based on SoSE, is a valid and replicable tool to understand and to manage complex "supersystems" or "networks of networks".
We apply this methodology to the complexity present in public blockchains: we model BTC and ETH, two public open and permissionless blockchain implementations, as holons that complement each other within a SoS of public blockchains. Public blockchains enable the transfer of digital private property with a link, or not, to physical private property. Thanks to the use of SoSE, we identify that BTC aspires to become "sound money", i.e., stable non-inflationary money, a digital global reserve asset. ETH, the "distributed world computer", aims to become the "alternative financial conduit" system to run decentralised finance;

(b) The unintended emergent property of the SoS of public blockchains is to stand as an alternative to the traditional centralised financial system based on fiat currencies.

This emergent property only appears when we focus on BTC and ETH, and, more generally, on public blockchain implementations, as a unique "supersystem". This SoS transfers digital value and competes with the traditional financial system as a potentially future-proof and disruptive alternative to the way the world conducts finance, especially since the Nixon shock in 1971 [102] with the cancellation of the direct convertibility of the USD into gold;

(c) One of the threats to the future of the SoS of public blockchains is its exposure to intentional risk. The materialisation of this risk could impact its mass adoption;

(d) The parameters proposed by Chapela et al. [16] in their intentional risk equation, i.e., value, accessibility and anonymity, are useful to suggest a series of security measures that would increase the resilience against intentional risk of the SoS of public blockchains.
These measures apply to the governance, design, development, operation and communication phases present in the implementation of this SoS;

(e) The optimisation of these intentional risk parameters, i.e., value, accessibility and anonymity, in the SoS of public blockchains, will impact positively on the evolution of the emergent property of this SoS.

6. Future Work

We suggest four paths to further research on the use of SoSE in the study of public blockchains and to improve the resilience against intentional risk of the SoS of public blockchains:

(a) To analyse how the SoS of public blockchains links with the SoS of traditional centralised fiat currency-based finance;

(b) To explore whether the modeling of the Decentralised Finance (DeFi) ecosystem is a SoS in itself;

(c) To build a complete application programming interface (API) that would facilitate the implementation of security measures in public blockchains with the objective of increasing their resilience against intentional risk;

(d) To explore the potential applications of machine learning and artificial intelligence (ML/AI) techniques, as described by Xu et al. [103], in the prevention, detection and mitigation of intentional risks against public blockchains.

Author Contributions: Conceptualization, A.P. and S.G.; methodology, A.P. and S.G.; software, A.P.; validation, A.P., S.G., R.C., M.R., E.G. and J.T.; formal analysis, A.P. and S.G.; investigation, A.P. and S.G.; resources, A.P., S.G., R.C., M.R., E.G. and J.T.; data curation, A.P.; writing—original draft preparation, A.P. and S.G.; writing—review and editing, A.P., S.G., R.C., M.R., E.G. and J.T.; visualization, A.P.; supervision, R.C., M.R., E.G. and J.T.; project administration, A.P., S.G., R.C., M.R., E.G. and J.T.; funding acquisition, A.P., S.G., R.C., M.R., E.G. and J.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: We used BTC and ETH data from publicly available datasets provided by coinmarketcap.com, bitnodes.io, ethernodes.org, etherscan.io, stats.buybitcoinworldwide.com and coinmarketcap.com (all af them last accessed on 1 December 2021). We make our Python-based complex network analysis code available via github. The References Section provides details on each specific Internet address.

Acknowledgments: The authors would like to acknowledge Diego Andina. Head of Group for Automation in Signals and Communications. ETSIT. Universidad Politécnica de Madrid. He inspired A.P. to write this paper and provided initial guidance on System of Systems Engineering.

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

References

1. Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where Is Current Research on Blockchain Technology? A Systematic Review. *PLoS ONE* **2016**, *11*, e0163477. [CrossRef]
2. Walport, M. Distributed Ledger Technology: Beyond Block Chain. UK Government Chief Scientific Adviser. 2015. Available online: https://bit.ly/3yzbq34 (accessed on 16 November 2021).
3. Coinmarketcap. Cryptocurrencies Market Capitalisation in Real Time. Available online: https://coinmarketcap.com/all/views/all/ (accessed on 25 November 2021).
4. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Nakamotoinstitute.org, October 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 16 November 2021).
5. 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]
6. Weber, W.E. A Bitcoin Standard: Lessons from the Gold Standard; No. 2016-14; Bank of Canada Staff Working Paper. 2016. Available online: http://hdl.handle.net/10419/148121 (accessed on 1 December 2021).
7. Ethereum. ETH Corporate Site. Available online: https://www.ethereum.org/ (accessed on 16 November 2021).
8. Ethereum.org. Ethereum Whitepaper. Available online: https://ethereum.org/en/whitepaper/ (accessed on 16 November 2021).
9. Partida, A.; Criado, R.; Romance, M. Identity and Access Management Resilience against Intentional Risk for Blockchain-Based IOT Platforms. *Electronics* **2021**, *10*, 378. [CrossRef]
10. Partida, A.; Criado, R.; Romance, M. Visibility Graph Analysis of IOTA and IoTeX Price Series: An Intentional Risk-Based Strategy to Use 5G for IoT. *Electronics* **2021**, *10*, 2282. [CrossRef]
11. Boccaletti, S.; Latora, V.; Moreno, Y.; Chavez, M.; Hwang, D.-U. Complex networks: Structure and dynamics. *Phys. Rep.* **2006**, *424*, 175–308. [CrossRef]
12. Newman, M.E.J. The structure and function of complex networks. *SIAM Rev.* **2003**, *45*, 167–256. [CrossRef]
13. Jamshidi, M. *System of Systems Engineering: Innovations for the 21st Century*; First Published: 21 April 2008; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2009; ISBN 9780470195901/9780470403501. [CrossRef]
14. Liu, X.; Peng, H.; Gao, J. Vulnerability and controllability of networks of networks. *Chaos Solitons Fractals* **2015**, *80*, 125–138. [CrossRef]
15. Partida, A. *Secure IT Up! Cyber Insurance Due Diligence*; CreateSpace Independent Publishing Platform: Scotts Valley, CA, USA, 2012; ISBN 9781478314752.
16. Chapela, V.; Criado, R.; Moral, S.; Romance, M. *Intentional Risk Management through Complex Networks Analysis*; Springer Briefs in Optimization; Springer: Berlin/Heidelberg, Germany, 2015.
17. Marella, V.; Kokabha, M.R.; Merikivi, J.; Tuunainen, V. Rebuilding Trust in Cryptocurrency Exchanges after Cyber-attacks. In Proceedings of the 54th Hawaii International Conference on System Sciences, Maui, HI, USA, 5–8 January 2021; pp. 5636–5646.
18. Suciu, G.; Nădrag, C.; Istrate, C.; Vulpe, A.; Ditu, M.; Subea, O. Comparative analysis of distributed ledger technologies. In Proceedings of the 2018 Global Wireless Summit (GWS), Chiang Rai, Thailand, 25–28 November 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 370–373. [CrossRef]
19. Thomas, S.; Schwartz, E. A Protocol for Interledger Payments. Hyperledger Working Group. Interledger.org. 2016. Available online: https://interledger.org/interledger.pdf (accessed on 16 November 2021).
20. Frankenfield, J. Interledger Protocol. investopedia.com. Available online: https://www.investopedia.com/terms/i/interledger-protocol.asp (accessed on 19 November 2021).
21. Reijers, W.; O'Brolcháin, F.; Haynes, P. Governance in Blockchain Technologies & Social Contract Theories. *Ledger J.* **2016**, *1*, 134–151. [CrossRef]
22. Catalini, C.; Gans, J.S. *Some Simple Economics of the Blockchain*; Working Paper 22952; National Bureau of Economic Research: Cambridge, MA, USA, 2016. [CrossRef]
23. ECB. Distributed Ledger Technology. In Focus, Issue 1, European Central Bank. 2016. Available online: https://bit.ly/3fHcOYS (accessed on 16 November 2021).
24. ESMA. *The Distributed Ledger Technology Applied to Securities Markets*; Report ESMA50-1121423017-285, Discussion Paper; European Securities and Markets Authority: Paris, France, 2017. Available online: https://bit.ly/344omjI (accessed on 16 November 2021).
25. Pinna, A.; Ruttenberg, W. Distributed Ledger Technologies in Securities Post Trading: Revolution or Evolution. Available online: https://bit.ly/3oHEMaY (accessed on 16 November 2021).
26. Longo, F.; Nicoletti, L.; Padovano, A.; d'Atri, G.; Forte, M. Blockchain-enabled supply chain: An experimental study. *Comput. Ind. Eng.* **2019**, *136*, 57–69. [CrossRef]
27. Filippi, P.D.; Hassan, S. Blockchain technology as a regulatory technology: From code is law to law is code. *arXiv* **2018**, arXiv:1801.02507. [CrossRef]
28. Hölbl, M.; Kompara, M.; Kamišalić, A.; Zlatolas, L.N. A Systematic Review of the Use of Blockchain in Healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]
29. Peiró, N.N.; García, E.J.M. Blockchain and land registration systems. *Eur. Prop. Law J.* **2017**, *6*, 296–320. [CrossRef]
30. Vasiliy, E.; Spirkina, A.; Buinevich, M.; Vladyko, A. Technological Aspects of Blockchain Application for Vehicle-to-Network. *Information* **2020**, *11*, 465. [CrossRef]

31. Stroukal, D.; Nedvedova, B. Bitcoin and other cryptocurrencies as an instrument of crime in cyberspace. In Proceedings of the 4th Business & Management Conference, Istanbul (IISES), Istanbul, Turkey, 12–14 October 2016. Available online: https://bit.ly/3fgyNap (accessed on 16 November 2021).
32. Malone, J.A. *Bitcoin and Other Virtual Currencies for the 21st Century*; CreateSpace Independent Publishing Platform: Scotts Valley, CA, USA, 1861. Available online: https://amzn.to/3oFn73I (accessed on 16 November 2021).
33. Srivastava, G.; Dhar, S.; Dwivedi, A.D.; Crichigno, J. Blockchain education. In Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, 5 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–5. [CrossRef]
34. Tasca, P.; Tessone, C.J. A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. *Ledger J.* **2019**, *4*. [CrossRef]
35. Dinh, T.T.A.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.C.; Wang, J. Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 1366–1385. [CrossRef]
36. Kondor, D.; Pósfai, M.; Csabai, I.; Vattay, G. Do the Rich Get Richer? An Empirical Analysis of the Bitcoin Transaction Network. *PLoS ONE* **2014**, *9*, e86197. [CrossRef]
37. Maesa, D.D.F.; Marino, A.; Ricci, L. Data-driven analysis of Bitcoin properties: Exploiting the users graph. *Int. J. Data Sci. Anal. Nat. Res.* **2018**, *6*, 63–80. [CrossRef]
38. Sommer, D. Processing Bitcoin Blockchain Data Using a Big Data-Specific Framework. Available online: https://files.ifi.uzh.ch/CSG/staff/scheid/extern/theses/BA-D-Sommer.pdf (accessed on 16 November 2021).
39. Wheatley, S.; Sornette, D.; Huber, T.; Reppen, M.; Gantner, R.N. Are Bitcoin bubbles predictable? Combining a generalized Metcalfe's Law and the Log-Periodic Power Law Singularity model. *R. Soc. Open Sci.* **2019**, *6*, 180538. Available online: https://royalsocietypublishing.org/doi/abs/10.1098/rsos.180538 (accessed on 1 December 2021). [CrossRef]
40. Bovet, A.; Campajola, C.; Mottes, F.; Restocchi, V.; Vallarano, N.; Squartini, T.; Tessone, C.J. The evolving liaisons between the transaction networks of Bitcoin and its price dynamics. *arXiv* **2019**, arXiv:1907.03577.
41. Garcia, D.; Tessone, C.J.; Mavrodiev, P.; Perony, N. The digital traces of bubbles: Feedback cycles between socio-economic signals in the Bitcoin economy. *J. R. Soc. Interface* **2014**, *11*, 20140623. Available online: https://royalsocietypublishing.org/doi/abs/10.1098/rsif.2014.0623 (accessed on 1 December 2021). [CrossRef] [PubMed]
42. Liang, J.; Li, L.; Zeng, D. Evolutionary dynamics of cryptocurrency transaction networks: An empirical study. *PLoS ONE* **2018**, *13*, e0202202. [CrossRef]
43. Somin, S.; Gordon, G.; Altshule, Y. Social Signals in the Ethereum Trading Network. *arXiv* **2018**, arXiv:1805.12097.
44. Guo, D.; Dong, J.; Wang, K. Graph structure and statistical properties of Ethereum transaction relationships. *Inf. Sci.* **2019**, *492*, 58–71. [CrossRef]
45. Lin, D.; Wu, J.; Yuan, Q.; Zheng, Z. Modeling and Understanding Ethereum Transaction Records via a Complex Network Approach. *IEEE Trans. Circuits Syst. II Express Briefs* **2020**, *67*, 2737–2741. [CrossRef]
46. Ferretti, S.; D'Angelo, G. On the Ethereum blockchain structure: A complex networks theory perspective. *Concurr. Comput. Pract. Exp.* **2020**, *32*, e5493. [CrossRef]
47. Somin, S.; Gordon, G.; Pentland, A.; Shmueli, E.; Altshuler, Y. ERC20 Transactions over Ethereum Blockchain: Network Analysis and Predictions. *arXiv* **2020**, arXiv:2004.08201.
48. Collibus, F.M.D.; Partida, A.; Piškorec, M.; Tessone, C.J. Heterogeneous Preferential Attachment in Key Ethereum-Based Cryptoassets. *Front. Phys.* **2021**, 568. [CrossRef]
49. Github. Public Python Repository to Plot BTC and ETH Transactions Degree Distributions in Block Slices. Available online: https://github.com/acoxonante/sos (accessed on 26 December 2021).
50. Schlager, K.J. Systems engineering-key to modern development. *IRE Trans. Eng. Manag.* **1956**, *3*, 64–66. [CrossRef]
51. Azani, C.H. System of systems architecting via natural development principles. In Proceedings of the 2008 IEEE International Conference on System of Systems Engineering, Monterey, CA, USA, 2–4 June 2008; pp. 1–6. [CrossRef]
52. Gorod, A.; Sauser, B.; Boardman, J. System-of-Systems Engineering Management: A Review of Modern History and a Path Forward. *IEEE Syst. J.* **2008**, *2*, 484–499. [CrossRef]
53. Dahmann, J.; Baldwin, K.; Rebovich, G. Systems of Systems and Net-Centric Enterprise Systems. In Proceedings of the 7th Annual Conference on Systems Engineering Research (CSER 2009), Loughborough, UK, 20–23 April 2009. Available online: https://www.researchgate.net/publication/228990763_Systems_of_Systems_and_Net-Centric_Enterprise_Systems (accessed on 1 December 2021).
54. Handy, C. Balancing Corporate Power: A New Federalist Paper. Harvard Business Reviw, November–December 2009 Issue, Leadership. Available online: https://hbr.org/1992/11/balancing-corporate-power-a-new-federalist-paper (accessed on 1 December 2021).
55. Roth, N. An Architectural Assessment of Bitcoin: Using the Systems Modeling Language. *Procedia Comput. Sci.* **2015**, *44*, 527–536. [CrossRef]
56. Mylrea, M. Distributed Autonomous Energy Organizations: Next-Generation Blockchain Applications for Energy Infrastructure. In *Artificial Intelligence for the Internet of Everything*; Lawless, W., Mittu, R., Sofge, D., Moskowitz, I.S., Russell, S., Eds.; Chapter 12; Academic Press: Cambridge, MA, USA, 2019; pp. 217–239. ISBN 9780128176368. [CrossRef]

57. Andina, D.; Partida, A. *IT Security Management: IT Securiteers—Setting up an IT Security Function*; Lecture Notes in Electrical Engineering, Book 61; Springer: Berlin/Heidelberg, Germany, 2010; ISBN 9789048188819.
58. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2020**, *107*, 841–853. [CrossRef]
59. Vallarano, N.; Tessone, C.J.; Squartini, T. Bitcoin Transaction Networks: An overview of recent results. *Front. Phys.* **2020**, *8*, 286. [CrossRef]
60. Bitcoin. BTC Reachable Nodes. Available online: https://bitnodes.earn.com/ (accessed on 16 December 2021).
61. Ethernodes Dashboard. Available online: https://www.ethernodes.org/network/1 (accessed on 21 November 2021).
62. Ethernodes Dashboard. Available online: https://etherscan.io/nodetracker (accessed on 16 November 2021).
63. Bitcoin Network Hashrate VS Price Explained. Available online: https://stats.buybitcoinworldwide.com/hashrate-vs-price/ (accessed on 3 December 2021).
64. Bitcoin Developer. Bitcoin API. RPC API Reference. Available online: https://developer.bitcoin.org/reference/rpc/index.html (accessed on 21 November 2021).
65. Ethereum API. Ethers.js Library. Available online: https://docs.ethers.io/v5/api/ (accessed on 21 November 2021).
66. Gansler, J.S.; Lucyshyn, W.; Spiers, A. The Role of Lead System Integrator. Available online: https://dair.nps.edu/handle/123456789/2424 (accessed on 1 December 2021).
67. Github. Bitcoin Core Contributors. Available online: https://github.com/bitcoin/bitcoin/blob/master/CONTRIBUTING.md (accessed on 16 November 2021).
68. Nabilou, H. Bitcoin Governance as a Decentralized Financial Market Infrastructure. SSRN. 16 March 2020. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3555042 (accessed on 1 December 2021).
69. Github. Bitcoin Improvement Proposal (BIP). Submission Workflow. Available online: https://github.com/bitcoin/bips#readme (accessed on 16 November 2021).
70. Github. Ethereum Project Management Repository. Available online: https://github.com/ethereum/pm (accessed on 16 November 2021).
71. Github. Ethereum Improvement Proposals. Available online: https://github.com/ethereum/eips/issues (accessed on 16 November 2021).
72. Github. Ethereum Code Repository. Available online: https://github.com/ethereum (accessed on 16 November 2021).
73. Buterin, V. The Most Important Scarce Resource is Legitimacy. March 2021. Available online: https://vitalik.ca/general/2021/03/23/legitimacy.html (accessed on 16 November 2021).
74. Singh, R.; Dwivedi, A.D.; Srivastava, G.; Wiszniewska-Matyszkiel, A.; Cheng, X. A game theoretic analysis of resource mining in blockchain. *Clust. Comput.* **2020**, *23*, 2035–2046. [CrossRef]
75. Cambridge Center for Alternative Finance. Bitcoin Mining Map. Evolution of Country Share. November 2021. Available online: https://ccaf.io/cbeci/mining_map (accessed on 23 November 2021).
76. Conway, L. Thestreet.com. Ethereum Has Lost over 6500 Nodes in the Last Two Weeks. 2021 . https://www.thestreet.com/crypto/ethereum/ethereum-is-still-missing-huge-amount-of-nodes-after-unintentional-hard-fork (accessed on 3 December 2021).
77. Crypto.com. Measuring Global Crypto Users. February 2021. Available online: https://bit.ly/2OujUq9 (accessed on 16 November 2021).
78. Electric Capital. Blockchain Developer Analysis Report. August 2019. Available online: https://bit.ly/328lcdT (accessed on 16 November 2021).
79. Coinmarketcap. Wrapped BTC Market Capitalisation in Real Time. Available online: https://coinmarketcap.com/currencies/wrapped-bitcoin/ (accessed on 16 November 2021).
80. Bitcoin.com. Side-Chaining $3 Billion in Value: There's More Than 141,000 Tokenized Bitcoins Issued on Ethereum. 2020. Available online: https://bit.ly/3rZ1iwe (accessed on 16 November 2021).
81. Binance.com. Tokenized Bitcoin on Ethereum Explained. April 2021. Available online: https://academy.binance.com/en/articles/tokenized-bitcoin-on-ethereum-explained (accessed on 16 November 2021).
82. Coinmetrics.com. BTC ETH Price Correlation. November 2021. Available online: https://charts.coinmetrics.io/correlations (accessed on 4 August 2021).
83. Investopedia.com. Bitcoin's Taproot Upgrade: What You Should Know. Available online: https://www.investopedia.com/bitcoin-taproot-upgrade-5210039 (accessed on 4 December 2021).
84. Bitcoin Lightning Network. Available online: https://lightning.network/ (accessed on 3 December 2021).
85. Ethereum 2.0. Available online: https://ethereum.org/en/eth2/ (accessed on 3 December 2021).
86. Blockchain.com. An Estimation of Hashrate Distribution amongst the Largest Mining Pools. April 2021. Available online: https://www.blockchain.com/charts/pools (accessed on 16 November 2021).
87. Blockchain.com. Top 25 Miners by Block. Available online: https://etherscan.io/stat/miner?range=7&blocktype=blocks (accessed on 16 November 2021).
88. Ethereum.org. Ethereum Improvement Proposals. Available online: https://eips.ethereum.org/all (accessed on 16 November 2021).
89. Oliver Wyman. Crypto-Assets: Their Future and Regulation. Available online: https://owy.mn/2OC6jgE (accessed on 16 November 2021).

90. Miyamae, T.; Honda, T.; Tamura, M.; Kawaba, M. Performance improvement of the consortium blockchain for financial business applications. *J. Digit. Bank.* **2018**, *2*, 369–378.
91. Coincodex.com. Stablecoins by Market Cap and Volume. Available online: https://coincodex.com/cryptocurrencies/sector/stablecoins/ (accessed on 16 November 2021).
92. Greenwald, M.B. The Future of the United States Dollar: Weaponizing the US Financial System. Available online: https://bit.ly/3fZwglF (accessed on 4 December 2021).
93. Finder.com. The Top 50 NFT Collections You Should Know about. Available online: https://www.finder.com/cryptocurrency/nft-collections (accessed on 4 December 2021).
94. Cryptopedia. Gemini.com. What Was the DAO? 2021. Available online: https://www.investopedia.com/tech/what-dao/ (accessed on 3 December 2021).
95. Christin, N. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In Proceedings of the 22nd International Conference on World Wide Web, Rio de Janeiro, Brazil, 13–17 May 2013; pp. 213–224. [CrossRef]
96. Bitcoin.it. Hash. Available online: https://en.bitcoinwiki.org/wiki/Hash (accessed on 4 December 2021).
97. Bitcoin.it. Elliptic Curve Digital Signature Algorithm. Available online: https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm (accessed on 4 December 2021).
98. Ethereum Wiki. Ethash. Available online: https://eth.wiki/en/concepts/ethash/ethash (accessed on 4 December 2021).
99. Github.com. Ethereum Cryptography. Available online: https://github.com/ethereum/js-ethereum-cryptography (accessed on 4 December 2021).
100. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
101. Damianou, A.; Khan, M.A.; Angelopoulos, C.M.; Katos, V. Threat Modelling of IoT Systems Using Distributed Ledger Technologies and IOTA. In Proceedings of the 2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS), Pafos, Cyprus, 14 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 404–413. [CrossRef]
102. Irwin, D.A. The Nixon shock after forty years: The import surcharge revisited. *World Trade Rev.* **2013**, 12, 29–56. [CrossRef]
103. Xu, Y.; Liu, X.; Cao, X.; Huang, C.; Liu, E.; Qian, S.; Liu, X.; Wu, Y.; Dong, F.; Qiu, C.-W.; et al. Artificial intelligence: A powerful paradigm for scientific research. *Innovation* **2021**, *2*, 100179. [CrossRef]

5. Identity and Access Management resilience against intentional risk for Blockchain-based IoT platforms

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

check for updates

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

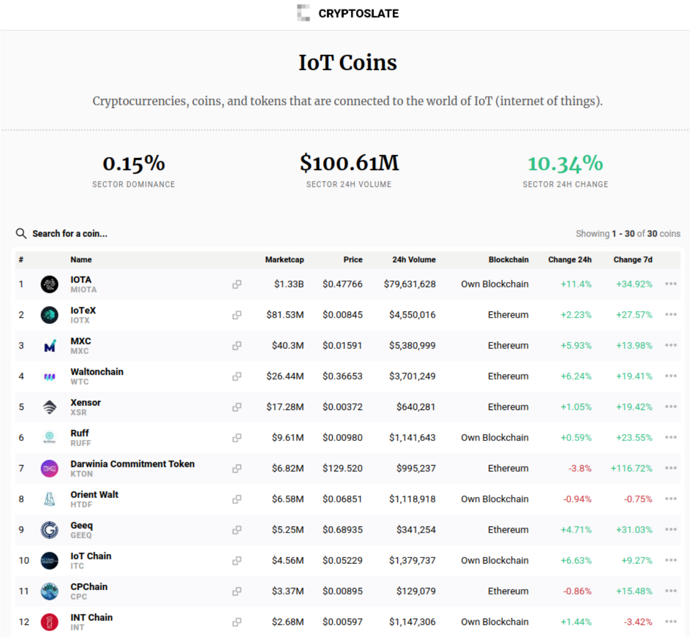
When something is highly valuable it needs to be wholeheartedly protected. An ancient strategy is to distribute it, as we infer from [11]. The Internet was born in the 1960s out of the United States Department of Defence with the aim of avoiding centralised governance. This innate approach was embraced 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 transactions, 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.



CRYPTOSLATE

IoT Coins

Cryptocurrencies, coins, and tokens that are connected to the world of IoT (internet of things).

0.15%
SECTOR DOMINANCE

$100.61M
SECTOR 24H VOLUME

10.34%
SECTOR 24H CHANGE

Search for a coin...

Showing 1 - 30 of 30 coins

#	Name	Marketcap	Price	24h Volume	Blockchain	Change 24h	Change 7d
1	IOTA MIOTA	$1.33B	$0.47766	$79,631,628	Own Blockchain	+11.4%	+34.92%
2	IoTeX IOTX	$81.53M	$0.00845	$4,550,016	Ethereum	+2.23%	+27.57%
3	MXC MXC	$40.3M	$0.01591	$5,380,999	Ethereum	+5.93%	+13.98%
4	Waltonchain WTC	$26.44M	$0.36653	$3,701,249	Ethereum	+6.24%	+19.41%
5	Xensor XSR	$17.28M	$0.00372	$640,281	Ethereum	+1.05%	+19.42%
6	Ruff RUFF	$9.61M	$0.00980	$1,141,643	Own Blockchain	+0.59%	+23.55%
7	Darwinia Commitment Token KTON	$6.82M	$129.520	$995,237	Ethereum	-3.8%	+116.72%
8	Orient Walt HTDF	$6.58M	$0.06851	$1,118,918	Own Blockchain	-0.94%	-0.75%
9	Geeq GEEQ	$5.25M	$0.68935	$341,254	Ethereum	+4.71%	+31.03%
10	IoT Chain ITC	$4.56M	$0.05229	$1,379,737	Own Blockchain	+6.63%	+9.27%
11	CPChain CPC	$3.37M	$0.00895	$129,079	Ethereum	-0.86%	+15.48%
12	INT Chain INT	$2.68M	$0.00597	$1,147,306	Own Blockchain	+1.44%	-3.42%

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].

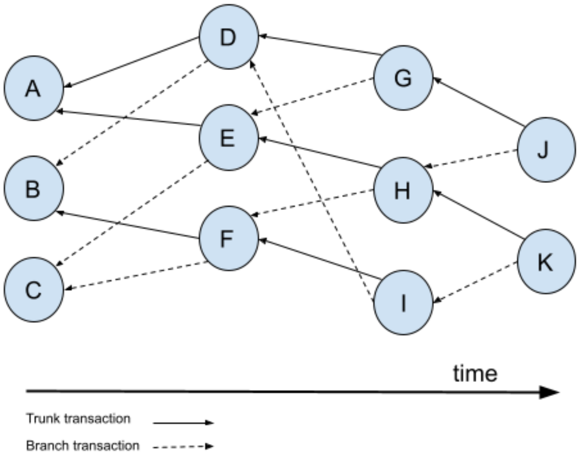


Figure 2. Ideal IOTA tangle representation.

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:

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

where

$$Acc_e = Accessibility_{element}, \tag{2}$$

$$Value_e = Value_{element}, \tag{3}$$

$$Anon_e = Anonymity_{element}, \tag{4}$$

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

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

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

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

$$Dynamic\ Risk_e = Value_e \cdot Accessibility_e. \tag{7}$$

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

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

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

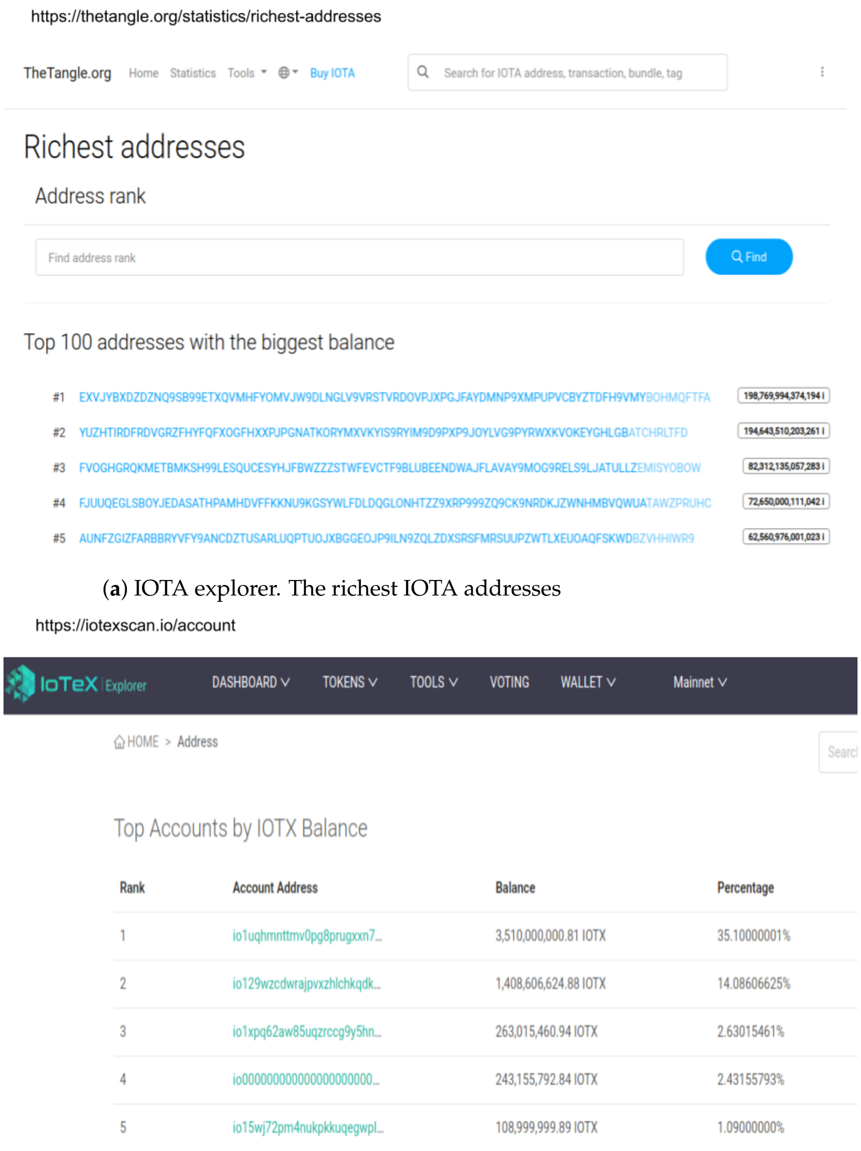
First, we have highlighted the main IoT security challenges and corresponding requirements [4–6,16,18]. Second, we have introduced current works on IoT implementations that use distributed ledgers such as those related to IOTA [31,35,38,43–46] and IoTex [51,52,54,55]. Third, we have presented complex 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



https://thetangle.org/statistics/richest-addresses

Richest addresses

Address rank

Top 100 addresses with the biggest balance

#1	EXVJYBXDZDZNQ9SB99ETXQVMHFYOMVJW9DLNGLV9VRSTVRDOVPJXPGJFAYDMNP9XMPUPVCBYZTDFH9VMYBOHMQFTFA	198,769,994,374,194 i
#2	YUZHTIRDFRDVGRZFHYFQFXOGFHXXPJPGNATKORYMXVKYIS9RYIM9D9PXP9JOYLVG9PYRWXKVOKEYGHLGBATCHRLTFD	194,643,510,203,261 i
#3	FVOGHGRQKMETBMKSH99LESQUCESYHJFBWZZZSTWFEVCTF9BLUBEENDWAJFLAVAY9MOG9RELS9LJATULLZEMISYOBOW	82,312,135,057,283 i
#4	FJUUQEGLSBOYJEDASATHPAMHDVFFKKNU9KGSYWLFDLDQGLONHTZZ9XRP999ZQ9CK9NRDKJZWNHMBVQWUATAWZPRUHC	72,650,000,111,042 i
#5	AUNFZGIZFARBBRYVFY9ANCDZTUSARLUQPTUOJXBGGEOJP9ILN9ZQLZDXSRSFMRSUUPZWTLXEUOAQFSKWDBZVHHIWR9	62,560,976,001,023 i

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

https://iotexscan.io/account

Top Accounts by IOTX Balance

Rank	Account Address	Balance	Percentage
1	io1uqhmnttmv0pg8prugxxn7...	3,510,000,000.81 IOTX	35.10000001%
2	io129wzcdwrajpvxzhlchkqdk...	1,408,606,624.88 IOTX	14.08606625%
3	io1xpq62aw85uqzrccg9y5hn...	263,015,460.94 IOTX	2.63015461%
4	io000000000000000000000...	243,155,792.84 IOTX	2.43155793%
5	io15wj72pm4nukpkkuqegwpl...	108,999,999.89 IOTX	1.09000000%

(**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

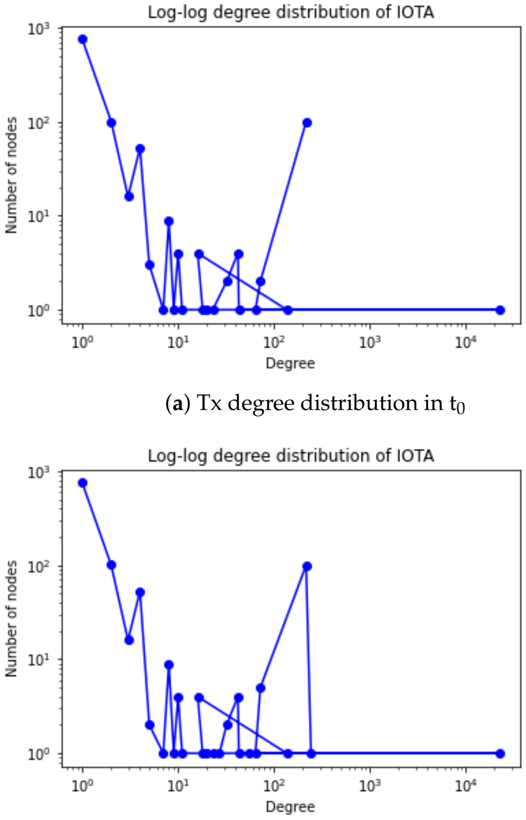
3.2. Transaction Data Preparation: Sender, Destination Pairs

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.

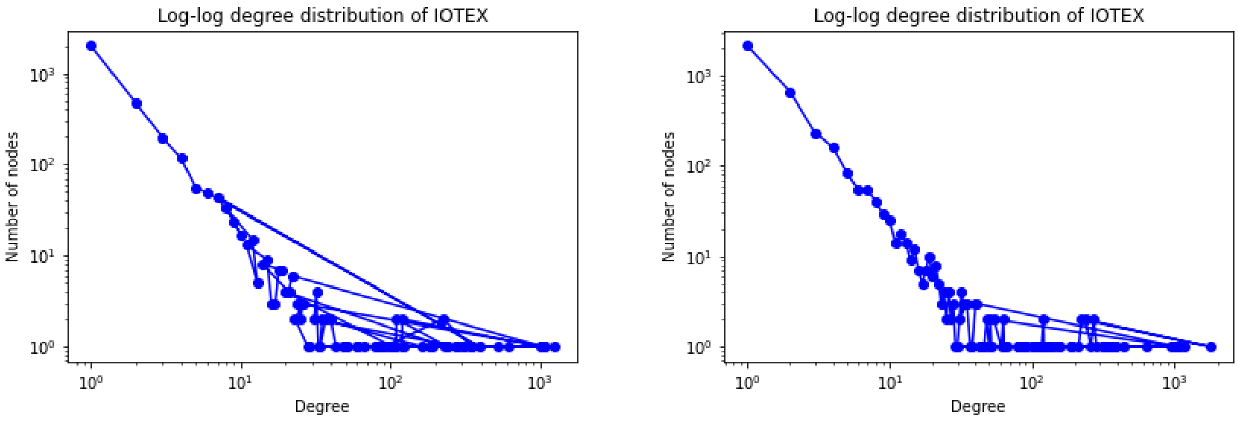
We carry out this computational analysis in a dual-processor Intel Xeon CPU @ 2.30 GHz with 13 GB RAM memory. Figure 7 summarises the methodology followed to describe IOTA and IoTeX as complex networks.



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

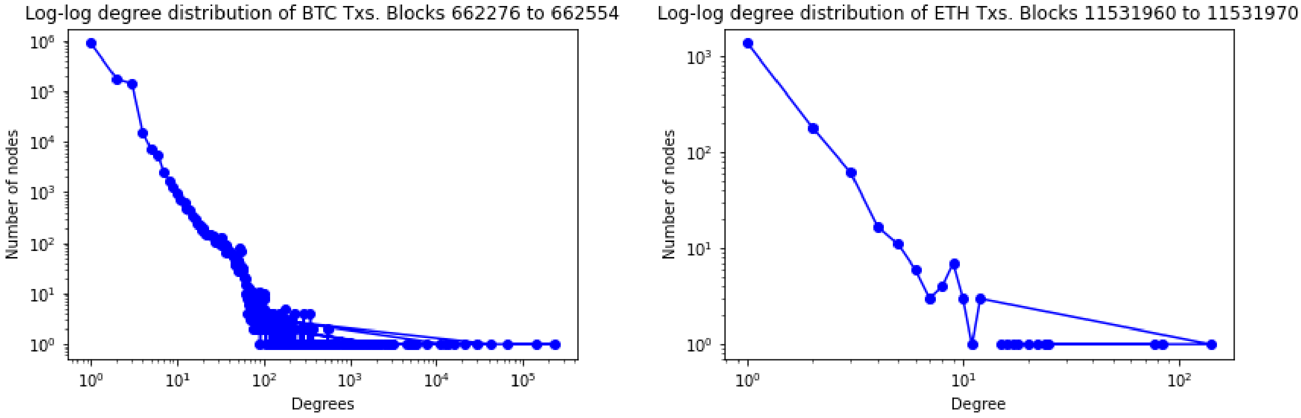
(**b**) Tx degree distribution in t_0 + 48 h

Figure 4. Degree distribution of 1068 IOTA addresses.



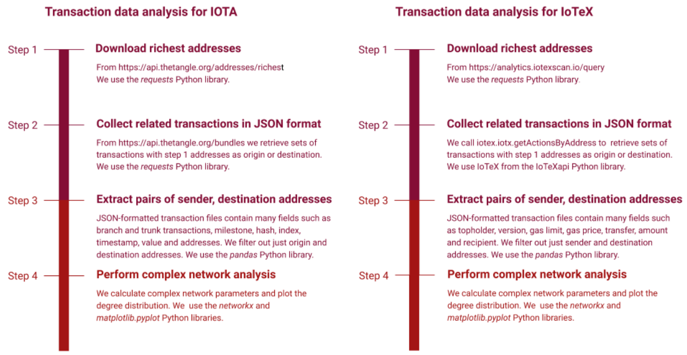
(**a**) Tx degree distribution with top 500 addr. Epoch 13,910 (**b**) Tx degree distribution with top 500 addr. Epoch 14,000

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.


Transaction data analysis for IOTA

Step 1 — **Download richest addresses**
From https://api.thetangle.org/addresses/richest
We use the *requests* Python library.

Step 2 — **Collect related transactions in JSON format**
From https://api.thetangle.org/bundles we retrieve sets of transactions with step 1 addresses as origin or destination. We use the *requests* Python library.

Step 3 — **Extract pairs of sender, destination addresses**
JSON-formatted transaction files contain many fields such as branch and trunk transactions, milestone, hash, index, timestamp, value and addresses. We filter out just origin and destination addresses. We use the *pandas* Python library.

Step 4 — **Perform complex network analysis**
We calculate complex network parameters and plot the degree distribution. We use the *networkx* and *matplotlib.pyplot* Python libraries.

Transaction data analysis for IoTeX

Step 1 — **Download richest addresses**
From https://analytics.iotexscan.io/query
We use the *requests* Python library.

Step 2 — **Collect related transactions in JSON format**
We call iotex.iotx.getActionsByAddress to retrieve sets of transactions with step 1 addresses as origin or destination. We use IoTeX from the IoTeXapi Python library.

Step 3 — **Extract pairs of sender, destination addresses**
JSON-formatted transaction files contain many fields such as topholder, version, gas limit, gas price, transfer, amount and recipient. We filter out just sender and destination addresses. We use the *pandas* Python library.

Step 4 — **Perform complex network analysis**
We calculate complex network parameters and plot the degree distribution. We use the *networkx* and *matplotlib.pyplot* Python libraries.

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

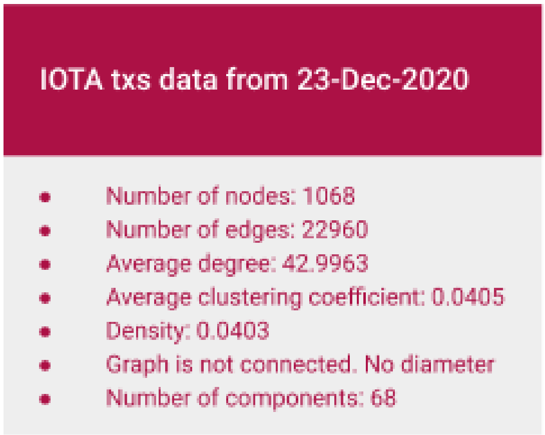
4. Analysis and Results

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.

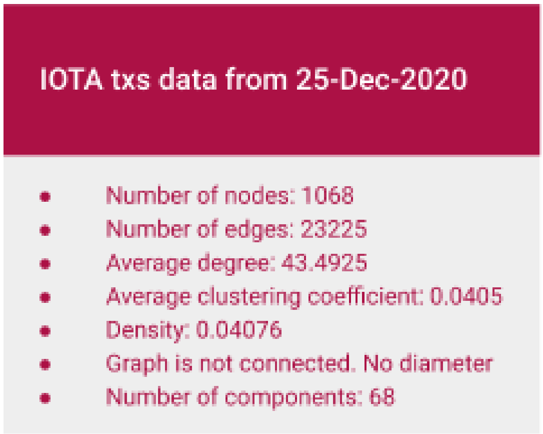
The empirical in-degree distributions of IOTA mainnet snapshots calculated by ([48] p. 5, Figure 4b) show a power-law distribution in contrast with the Poisson degree distribution extracted from simulated tangles ([48] p. 5). Compared to our dataset, Guo et al. [48] use a 13 month-long IOTA tangle dataset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



IOTA txs data from 23-Dec-2020

- Number of nodes: 1068
- Number of edges: 22960
- Average degree: 42.9963
- Average clustering coefficient: 0.0405
- Density: 0.0403
- Graph is not connected. No diameter
- Number of components: 68

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



IOTA txs data from 25-Dec-2020

- Number of nodes: 1068
- Number of edges: 23225
- Average degree: 43.4925
- Average clustering coefficient: 0.0405
- Density: 0.04076
- Graph is not connected. No diameter
- Number of components: 68

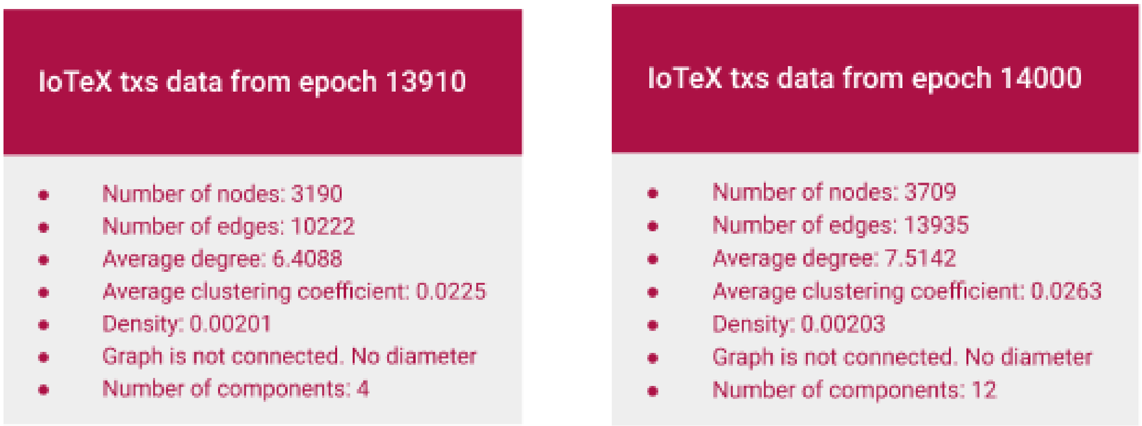
(**b**) IOTA transaction network. Sample 2

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.



IoTeX txs data from epoch 13910

- Number of nodes: 3190
- Number of edges: 10222
- Average degree: 6.4088
- Average clustering coefficient: 0.0225
- Density: 0.00201
- Graph is not connected. No diameter
- Number of components: 4

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

IoTeX txs data from epoch 14000

- Number of nodes: 3709
- Number of edges: 13935
- Average degree: 7.5142
- Average clustering coefficient: 0.0263
- Density: 0.00203
- Graph is not connected. No diameter
- Number of components: 12

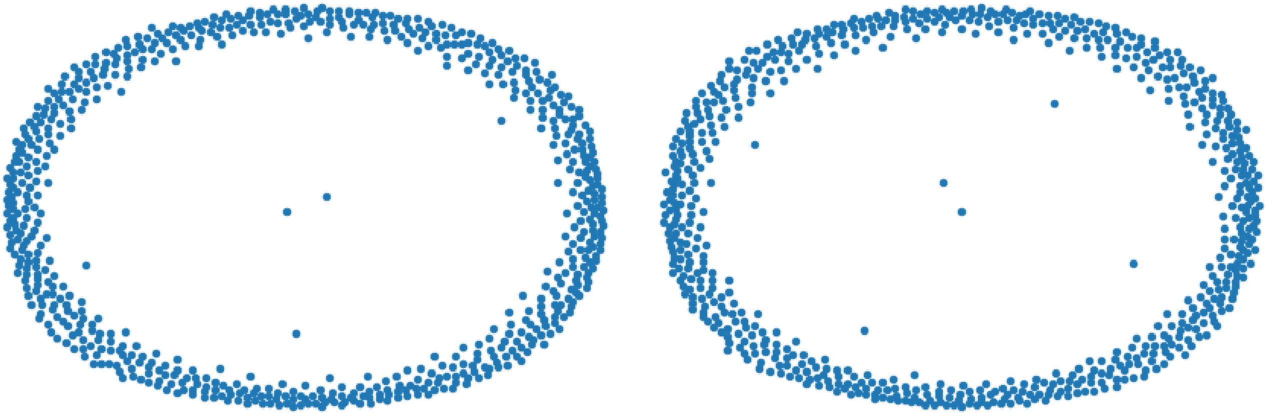
(**b**) IoTeX transaction network. Sample 2

Figure 9. Complex network analysis for IoTeX transactions.

4.3. Largest Connected Components in IOTA and IoTeX

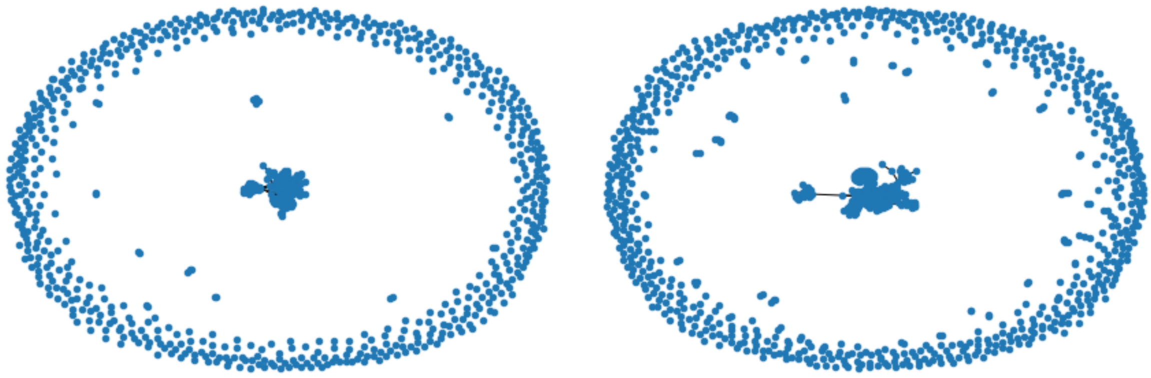
We identify the largest connected component (LCC) in both transaction networks and we draw all nodes connected to it without displaying the edges between those nodes and the LCC to ease interpretation. The appearances of the graphs showing nodes connected to the LCC in IOTA and IoTeX are similar. Figures 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.

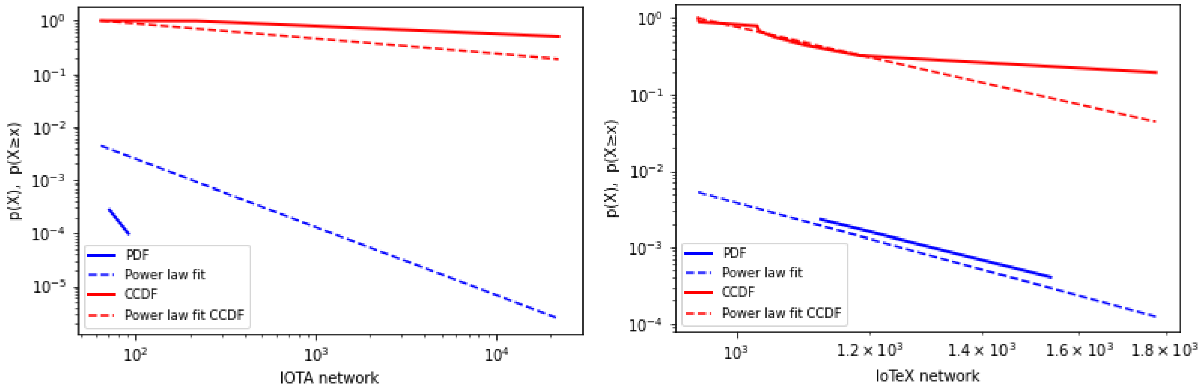
We identify power-law degree distributions as well. See Figure 6. This indicates that the transaction networks of these two public blockchain implementations display scale-free characteristics. We also obtain clustering coefficients very close to 0 indicating that neither BTC nor ETH display small-world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

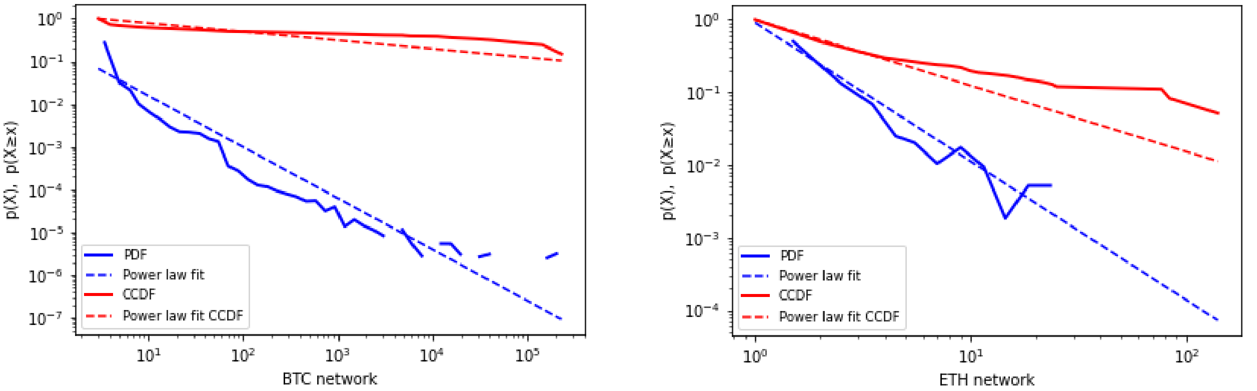


(**a**) IOTA power-law fit

(**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]

6. Visibility graph analysis of IOTA and IoTeX price series: an intentional risk-based strategy to use 5G for IoT

Errata: Section 4.4 in this published article contains two errata:

- Instead of "the values of α are very close to 2 for both HVGs", it should say "the values of α are **below** 2 for both HVGs".
- Instead of "the fit observe with *curve_fit* shows a less heavy-tailed distribution than in the degree graphs", it should say "the fit observe with *curve_fit* shows a **more** heavy-tailed distribution than in the degree graphs".

electronics

MDPI

Article

Visibility Graph Analysis of IOTA and IoTeX Price Series: An Intentional Risk-Based Strategy to Use 5G for IoT

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

[1] International Doctoral School, Rey Juan Carlos University, 28933 Madrid, Spain
[2] Department of Applied Mathematics, Rey Juan Carlos University, 28933 Madrid, Spain; regino.criado@urjc.es (R.C.); miguel.romance@urjc.es (M.R.)
* Correspondence: apartidar@gmail.com
† Current address: Móstoles Campus, Rey Juan Carlos University, 28933 Madrid, Spain.

Abstract: The transformation of time series into complex networks through visibility graphs is an innovative way to study time-based events. In this work, we use visibility graphs to transform IOTA and IoTeX price volatility time series into complex networks. Our aim is twofold: first, to better understand the markets of the two most capitalised Internet of Things (IoT) platforms at the time of writing. IOTA runs on a public directed acyclic graph (DAG) and IoTeX on a blockchain. Second, to suggest how 5G can improve information security in these two key IoT platforms. The analysis of the networks created by the natural and horizontal visibility graphs shows, first, that both IOTA and IoTeX are still at their infancy in their development, with IoTex seemingly developing faster. Second, both IoT tokens form communities in a hierarchical structure, and third, 5G can accelerate their development. We use intentional risk management as a lever to understand the impact of 5G on IOTA and IoTeX. Our results lead us to provide a set of design recommendations that contribute to improving information security in future 5G-based IoT implementations.

Keywords: IoT; IOTA; IoTeX; blockchain; decentralised ledger; cryptocurrencies; complex networks; visibility graph; powerlaw; data integrity; intentional risk; resilience

check for updates

Citation: Partida, A.; Criado, R.; Romance, M. Visibility Graph Analysis of IOTA and IoTeX Price Series: An Intentional Risk-Based Strategy to Use 5G for IoT. *Electronics* **2021**, *10*, 2282. https://doi.org/10.3390/electronics10182282

Academic Editor: Avishek Nag

Received: 31 July 2021
Accepted: 4 September 2021
Published: 17 September 2021

1. Introduction

1.1. Foundations of This Study: From Time Series to Complex Networks

In mathematics, a time series is a succession of events ordered by time. Time series analysis aims to describe the statistical characteristics of the data. Time series forecasting aims to use a model to predict future values [1]. Network science is a scientific discipline at the crossroad of mathematics, statistics and physics [2]. It characterises systems composed of a collection of nodes and edges between them. They constitute a network. The nodes represent the members of the system and the edges certain relations or transfers between them. When the number of nodes and edges is high, i.e., thousands to millions, these systems create a complex network. Complex network analysis provides insights into how these systems grow, evolve and interact with their members. It is possible to transform a time series into a complex network thanks to an easy-to-implement algorithm, i.e., a visibility graph [3]. This conversion facilitates the study of the system whose events create a time series with the powerful analysis toolkit that complex network science provides. In our case, we transform the time series created from the daily prices of the two most capitalised Internet of Things (IoT) tokens into their corresponding complex networks. These visibility networks help us understand how these two IoT platforms behave and grow: IOTA and IoTeX, the former implemented on a directed acyclic graph (DAG) and the latter on a blockchain. We apply our findings to a real life scenario, i.e., the deployment of 5G mobile networks, and we use concepts stemming from intentional risk management to suggest specific 5G design choices that can potentially improve the resilience against intentional risk of both IoT platforms.

1.2. The Value Proposition of 5G

1.2.1. Mobile Networks

Mobile networks answer the need human beings have to communicate remotely while not being at home or anywhere close to a wireless local area network (LAN) access point (Wi-Fi). Since their first release in 1980 [4] until now, a series of consecutive generations has provided continuous technology improvements. Table 1 summarises data transmission (Tx) speed, technologies and some details of each generation [5] (refer to [5–7] on protocol acronyms used in Table 1):

1.2.2. 5G: Higher Speed and Lower Latency

Speeds displayed in Table 1 are only approximate. However, they show a continuous drive towards providing customers with faster speed rates. The mobile network generation that is currently being deployed is 5G, although there are still many GSM (2nd Generation) networks in production with a switch-off date beyond 2024 [8]. The 3rd Generation Partnership Project (3GPP) industry consortium [9] develops the communication protocol specifications for 5G. Telecommunication providers have measured in real life a 5G data transmission speed of 3 Gbps (3000 million bits per second) with a 3 milliseconds (ms) air latency. More habitual figures are in the range of 500 Mbps and 30 ms latency (including both air and edge server connection time gaps). As an example, the reaction time for the human brain on an image perceived by the eye is around 10 ms [10]. 5G providers expect to improve these figures in the coming years.

Table 1. Mobile networks history in generations.

Generation	Tx Speed	Technology	Period	Details
1	14.4 kbps	Analog Tx	1970–1990	Voice only
2	up to 14.4 kbps	CDMA/TDMA	1990–2000	Digital Tx, SMS, GSM Standard
2.5	20–170 kbps	GPRS	2000–2003	First basic Internet browsing
2.75	up to 236 kbps	EDGE	2003	×3 GSM data capacity
3	144 kbps–3 Mbps	UMTS, CDMA2000	2004–2005	First streamings
3.5	1–10 Mbps	HSPA	2006–2010	Higher speed over UMTS
4	144 kbps–100 Mbps	LTE	2010–2020	First streamings
5	1 Gbps	3GPP Standards	2021–	Starting deployment

1.3. Internet of Things

The pervasiveness of Internet among human beings reaches already more than 50% of the world population, i.e., almost 4 billion people [11]. A total of 90% of those Internet users access it via mobile phones [12]. The connection of things with other things and people via Internet, known as the Internet of Things (IoT), is also growing in economic importance (USD 17 billion in 2021 [13]). The number of IoT connected devices reached the 20 billion mark in 2018 [14]. The forecast is that this figure will reach USD 30 billion by 2030 [15]. An IoT device has at least one transducer (sensor or actuator) to interact directly with the physical world and at least one network interface (e.g., 5G, Ethernet, Wi-Fi, Bluetooth) to interface with the digital world [16]. They bridge the physical with the digital world. Oracles play a similar role in distributed blockchains.

5G and Internet of Things

Already in 2016, the 3GPP consortium agreed to further develop IoT protocols like NarrowBand Internet of Things (NB-IoT) and Long Term Evolution Machine Type Communication (LTE-M). 4G mobile networks already use them within the suite of standardised low power, wide area (LPWA) technologies [17,18]. These two IoT protocols aim to meet low-cost, low-current, wide coverage and high capacity requirements. 5G is also being deployed in private networks, e.g., in industrial IoT [19]. Market analysts forecast a USD 3.6 trillion value generated in massive IoT developments up to 2035 [20].

1.4. Blockchain

The publication of the seminal Bitcoin (BTC) paper in 2008 by the pseudonym Satoshi Nakamoto [21] brought the spotlight on the blockchain, a distributed database that stores records in blocks. Each block is permanently linked to the chain of blocks by cryptographic means. The community accepts the longest chain of blocks. This technology provides data integrity as validated blocks cannot be tampered with. It also provides transparency as the chain of validated records is accessible to all participants and, finally, availability, as validators keep a copy of the blockchain [4]. Blockchain is a useful technology to register events requiring integrity, transparency and availability such as financial transactions [22–25].

Blockchain for IoT

IoT networks can benefit from the blockchain technology to answer their integrity, availability and, if required, transparency requirements [4,26]. The distributed nature of blockchain is an optimal design component for IoT implementations. As of September 2021, the market capitalisation of four IoT projects based on blockchains or directed acyclic graphs (DAG) exceeds USD 70 million: IOTA, IoTeX, MXC and Waltonchain [27]. In July 2021, their value surpassed USD 40 million.

1.5. Structure of the Paper

This paper is structured as follows. First, we introduce the foundations of our research and summarise the opportunities that 5G brings to blockchain-based IoT implementations. Second, we describe the current state-of-the-art with regard to 5G, IoT platforms and blockchain. Third, we present complex network analysis and the proxy role of price volatility. Fourth, we explain how visibility graphs bridge between time series and complex network analysis, and we briefly refer to power law functions and to intentional risk. Fifth, we share the methodology that we have followed to study IOTA and IoTeX price volatility, its implementation and the corresponding results of the analysis. Sixth, we draw several conclusions related to visibility graphs, IOTA and IoTeX markets and 5G using intentional risk concepts. Seventh, we suggest design options for 5G to improve information security in IOTA and IoTeX. Finally, we present our future work proposals.

2. Related Works

2.1. 5G Services and Their Economic Value

The International Telecommunication Union (ITU) Radio-communication sector defines the minimum standards for 5G within three main services, i.e., enhanced Mobile BroadBand (eMBB), massive Machine Type Communication (mMTC) and URLLC (Ultra Reliable and Low Latency Communications) [4]. The most deployed service continues to be eMBB [28], focused on improving data transmission rates for smartphone users. Although in 2021 5G enabled smartphones already constitute 43% of new shipped units worldwide [29], they still represent a tiny segment within the current deployed stock of smartphones. The other two services, mMTC and URLLC, are yet in their infancy. The economic value that 5G is expected to provide to the world economy is in the order of USD 12 trillion [30]. Table 2 introduces the technologies that 5G uses [4,31,32]:

Table 2. Technologies used in 5G mobile networks.

Name	Acronym	Function
Network Slicing	NS	Virtual networks in parallel to answer different speed and latency requirements.
Software-Defined Networking	SDN	Centralised programmatical network configuration. It decouples forwarding and routing.
Multi-Access Edge Computing	MEC	Cloud computing at the network edge to tap into data with local access conditions.
Network Function Virtualisation	NFV	Router as SW in off-the-shelf hardware. Key for Network Slicing.
Millimeter Wave communications	mmWC	Higher data rates than microwaves. Key for bandwidth increase.
Massive MIMO	MIMO	Wireless access technology. Multiple Input Multiple Output enabled by mmWaves.
Device to device connectivity	D2D	User equipment (UE) communicates with UE. It leads to micro clouds in base stations.

2.1.1. 5G as Optimal Communication Channel for IoT

5G mobile technology will enable new value chains in many economic sectors. Those using machine-to-machine communications are among them [4]. 5G networks will provide performance enhancements, a high degree of reliability and very low latency communications [33]. The IoT segment with the heaviest economic weight is Smart Home Technologies with a projected market volume of USD 17 billion in 2021 [13]. Smart Home IoT devices are mostly connected to the Internet via Wi-Fi connections with mobile as a redundant backup communication channel. However, IoT devices in remote places and in places with no Wi-Fi coverage make use of mobile links to exchange data with their edge and cloud servers. The arrival of 5G, although at a later stage than, e.g., person-to-person mobile communications [20], will bring better energy efficiency, reliability and performance.

2.2. Blockchain or Directed Acyclic Graph-Based IoT Platforms

The two most capitalised IoT implementations based on distributed databases, i.e., distributed ledgers, are IOTA and IoTeX [27]. IOTA's market capitalisation in July 2021 reached values such as USD 1.93 and USD 2.42 billion and IoTeX USD 181 and 188 million. In September 2021 they exceeded USD 4.3 billion and USD 633 million respectively [27]. We consider market capitalisation as a proxy for potential future economic value that these two IoT platforms can produce in IoT projects aimed to solve specific business cases, e.g., in healthcare [34] and transportation [35]. A relevant set of those projects will be using 5G mobile networks to allow for remote non-WiFi communications between sensors and edge and cloud servers.

2.2.1. IOTA

Created in 2015, IOTA is by far the most capitalised IoT platform [27]. It is an innovative solution based on a directed acyclic graph (DAG): Every participant launching a transaction in IOTA needs to validate two prior transactions, replacing the need for blocks and miners. It is a public, permissionless, open-source, and feeless distributed ledger. It enables the exchange of value between humans and machines [26]. IOTA is currently testing improvements to achieve a greater degree of decentralisation as it still requires the participation of a coordinator to validate transactions [26]. Energy, industrial communications and mobility are some of the fields where there are IOTA-based projects [36]. The IOTA token is tradeable since 2017.

2.2.2. IoTeX

Created in 2017, IoTeX allows for the use of multiple blockchains. It claims that no unique blockchain can satisfy all IoT requirements. The rootchain is a public permissionless blockchain that uses a randomised delegated proof of stake (Roll-DPoS). There are different permissioned and permissionless subchains according to their functionality [26,37]. Home domotics [38] and mobile payments [39] are two areas with promising IoTeX projects. The IoTex token started trading as an Ethereum-based token (ERC-20 IOTX token) in 2018. Table 3 presents a quick introductory summary of both IoT platforms:

Table 3. IOTA and IoTeX.

	IOTA	**IoTeX**
Start year	2015	2017
Distributed	Yes	Yes
Ledger type	DAG	Blockchain
Public	Yes	Yes
Permissionless	Yes	Yes
Multiblockchain	No	Yes
Fees	No	Low

2.2.3. Blockchain as Additional Security Value in 5G-Enabled IoT Networks

Blockchain technology brings additional security properties to the very high data transmission speed and the ultra low latency that 5G adds to IoT implementations, i.e., data integrity and non-repudiation [4,26,40]. Many blockchain-based IoT implementations can benefit from a reliable and fast 5G network, such as the use of IOTA in electric vehicle charging facilities [41] and IoTex in smart cities [42]. Nevertheless, a single blockchain implementation with no additional tools to manage the complexity of an IoT implementation, e.g., in edge and cloud computing, cannot provide all security requirements [26].

2.3. Complex Networks

Network analysis describes systems composed of many elements that interact with each other. Their relations create a graph. Nodes, also called vertices, connect between them via edges, also called links [2] (p. 2). The complexity appears when the number of nodes and links is high, and we need advanced mathematical and statistical tools to characterise those systems [43–45]. Complex network analysis is a useful tool to understand non-linear interactions [46], some of them dynamic [47] (p. 177), between network nodes. They provide a plausible behavioural model to real world examples such as social networks, contagious diseases, transportation networks and crypto-token networks [48,49] (p. 179). In our case, we use visibility graphs to transform the daily price volatility time series of IOTA and IoTeX tokens into complex networks. The study of these networks helps us understand IOTA and IoTeX markets and how 5G technology can have an impact on them.

2.4. Volatility as a Proxy Measure

The study of the relation between asset price volatility and asset trading volume is a common proposal to study markets [50]. Similarly, in crypto-currencies, the correlation coefficient between the volatility and volume is positive and statistically significant [51]. Yamak et al., studying bitcoin (BTC) from 2013 to 2019, found a bidirectional causal relationship between price volatility and trading volume being the one from volume to price volatility the strongest [51]. Equally, the number of addresses in BTC has a significant impact on the BTC price with variations over time [52], i.e., crypto-token markets relate to their networks. In Section 3, we explain how we study price volatility as a proxy to understand both IOTA and IoTex cryptocurrency markets and, ultimately, their networks and their link to a potential 5G deployment.

2.5. Visibility Graphs

Lacasa et al. propose two fast computational methods to convert a time series into a graph, the natural (in 2008, [3]) and the horizontal (in 2009, [53]) visibility graphs. The resulting graphs inherit and display structural properties of the time series. Complex network analysis helps identifying some of those properties [54]. Table 4 summarises the links between time series and visibility graphs (VG) [3]:

Table 4. Correspondence between time series and complex networks.

Time Series Type	Complex Network Type
Periodic	Regular
Random	Random (exponential degree function)
Fractal	Scale-free (power law degree function)

Visibility Graph of Bitcoin

In 2019, Liu et al. perform a visibility graph analysis of Bitcoin (BTC), Ethereum (ETH) and Litecoin (LTC) price volatility series to understand their markets [54]. They confirm that the three VGs are scale-free and they display a hierarchical structure, i.e., they cluster similarly at different levels. A power law behaviour in the function of the average clustering coefficient of each node with a specific degree confirms that each community clusters into sub-communities. These results, based on 5 years of daily prices (from April 2013 to May 2018), facilitate the construction of dynamic models of BTC, ETH and LTC markets and, in general, of any rare item market. With only 5 years of daily data, results for these three cryptocurrencies reproduce the price volatility series of the gold market throughout hundreds of years.

2.6. Power Laws

When the right tail of a probability distribution still contains a considerable amount of probability, its study is pivotal to understand that specific distribution. This is the case for power law functions. Mathematically, they behave as Equation (1):

$$p(x) = \sigma \frac{1}{x^{\alpha}}. \tag{1}$$

If $\alpha < 3$, the standard deviation of the distribution is not defined. If $\alpha < 2$, the mean of the distribution is not defined. A scale-free, i.e., all values can occur, network has a power law function as a degree distribution, at least asymptotically. The value of α for easy to identify power law functions goes goes from 2 to 3. Alstott et al. in 2014 provided a Python library to facilitate the study of the fit of empirical data with power law functions [55]. They use three typical functions to show potential power law fits, as Table 5 shows:

Table 5. Functions to study heavy-tailed distribution functions.

Function	*X* Axis	*Y* Axis
Probability density function (PDF)	Variable x	Probability $p(X = x)$
Cumulative distribution function (CDF)	Variable x	Probability $p(X < x)$
Complementary cumulative distribution (CCDF)	Variable x	Probability $p(X \geq x)$

2.7. Intentional Risk

Traditional risk management deals with system failures and environmental disasters [56]. Intentional risk management is a security innovation proposed by Chapela et al. [46]. They perform a complex network analysis on information systems using value, anonymity and accessibility as the three key dimensions to manage attacks to the system by actors in search of a benefit. They distinguish between static and dynamic risk. The former relates to actors with access to the system and the latter to actors with no initial legitimate access to the system, i.e., with a maximum possible level of anonymity. We use for our analysis the concept of dynamic risk of an element e presented in Equation (2):

$$Dynamic\ Risk_e = Value_e \cdot Accessibility_e. \tag{2}$$

We link the concept of value with the daily price of the tokens we study and the concept of accessibility with the potential functionalities that 5G can provide to these IoT networks, as we explain in Section 3.

3. Methodology and Implementation

3.1. A Complex Network from a Visibility Graph

The first future work path mentioned in [26] is the transformation of the time series created by IOTA and IoTeX transactions, i.e., the value transacted at each point of time, into complex networks using the visibility graph technique proposed by Lacasa et al. [3]. The ultimate objective is to further analyse both IoT implementations. The number of transactions taking place in both networks since their inception render this proposal unrealistic if we consider a time series indexed per second as a time unit. A look at the IOTA explorer (Mainnet feed Section) [57] reveals time slots with several transactions, with zero and non-zero value IOTA token transfers, per second. Equally, in IoTeX explorer (right hand side column in its interface) [58], we see how there is a new block, including a handful of actions with zero and non-zero IoTeX token transfers, every few seconds. Alternatively, in this study, we analyse the visibility graphs created from IOTA and IoTeX tokens' daily price volatility information since day one of trading. Daily token price information is accessible and regularly and accurately registered. It acts as a valid proxy to describe how these two IoT markets behave. We analyse the complex network stemming from the volatility visibility graphs. Our conclusions carry several implications for blockchain-based IoT implementations using 5G mobile networks.

3.2. Price Volatility Data Collection

We base our analysis on daily maximum and minimum prices for both IOTA and IoTeX tokens obtained from investing.com [59,60] (accessed on 24 July 2021). Investing.com (accessed on 24 July 2021) is a stock market quote and financial news provider. We calculate daily volatility values using Equation (3):

$$price\ volatility = ln\left(\frac{price_{max}}{price_{min}}\right). \tag{3}$$

Table 6 presents the data items we use in our analysis, i.e., 4 years of daily volatility data for IOTA and 3 years of daily volatility data for IoTeX.

Table 6. Data points analysed in this study.

Token	Data Items	Frequency	From	To	# Datapoints
IOTA	Highest and lowest price	Daily	14 June 2017	15 July 2021	1493
IoTeX	Highest and lowest price	Daily	20 June 2018	15 July 2021	1122

Figure 1 displays the lowest and highest daily price time series and the resulting price volatility time series.

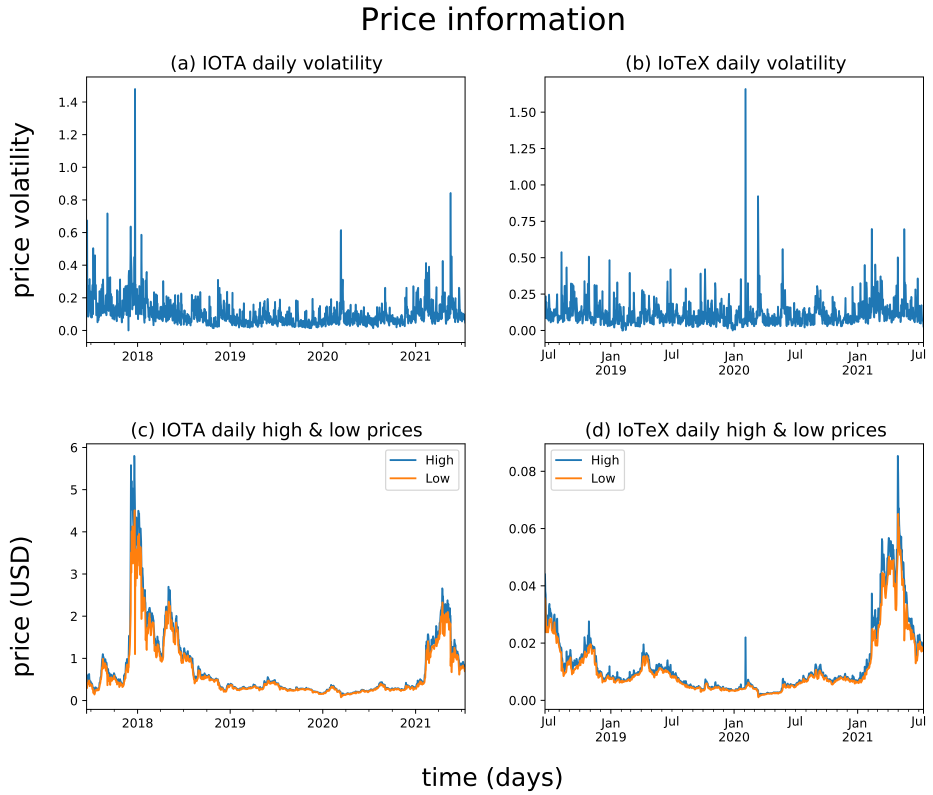


Figure 1. Daily price volatility data for IOTA and IoTeX. Subplots (**a**,**b**) display the daily volatility time series for IOTA and IoTeX, respectively. Subplots (**c**,**d**) display their components: highest and lowest prices in USD per day for IOTA and IoTeX.

3.3. Creation of the Natural Visibility Graph

Visibility_graph [61] is a Python module that implements the visibility graph proposed by Lacasa et al. [3]. We run this code to create the complex network. As input, we deploy the time series introduced in Section 3.2. The nodes correspond to each daily volatility measure, and the edges link those nodes that are "visible" to each other.

3.4. Creation of the Horizontal Visibility Graph

Visibility_algorithms [62] is a Python piece of code that implements the original proposal to create horizontal visibility graphs in Fortran 90/94 by Lacasa. Equally, we use as input the volatility time series presented in Section 3.2. The nodes correspond to each daily volatility measure, and the edges link those nodes that are "horizontally visible" to each other.

Figure 2 shows the appearance of the natural visibility graph (VG) and the horizontal visibility graph (HVG) for the 20 most recent days in our data collection.

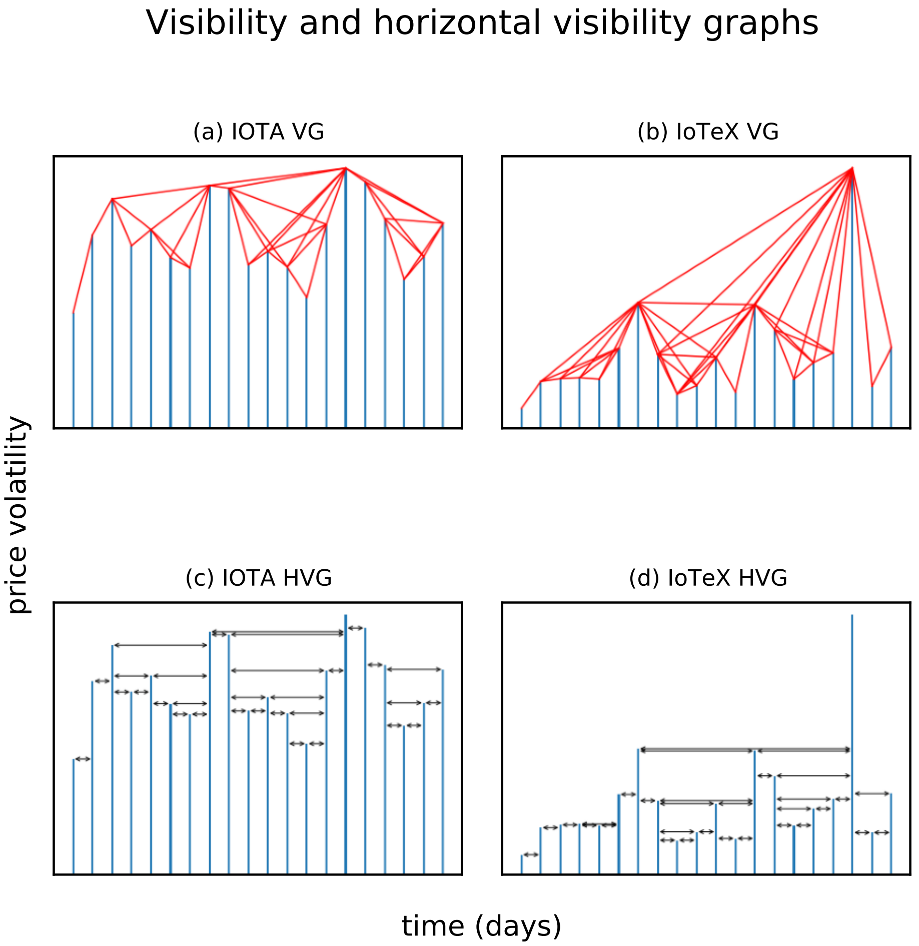


Figure 2. Visibility and horizontal visibility graphs for IOTA and IoTeX price volatility. Subplots (**a**,**b**) display the visibility graph derived from the daily volatility time series for IOTA and IoTeX, respectively (last 20 days of the dataset). Subplots (**c**,**d**) display the horizontal visibility graph derived from the daily volatility time series for IOTA and IoTeX, respectively (last 20 days of the dataset). The depiction of these graphs is the outcome of our own Python code.

3.5. Complex Network Analysis of the IOTA and IoTeX VG and HVG

Once we have these four complex networks at our disposal, i.e., the VGs and HVGs for both IOTA and IoTeX price volatilities, first, we obtain the degree for each node using the Python module *networkx* [63] and the basic network features, i.e., number of nodes and edges, number of isolated elements and self loops, average density and transitivity using the Python module *metaknowledge* [64]. Second, we proceed to measure the heterogeneity of the networks by plotting their degree functions and comparing them with potential power law fits using two methods:

3.5.1. *Curve_Fit*

First, we use the traditional *curve_fit* Python module from *scipy.optimize* [65]. It uses non-linear least squares to fit a function, in our case a power law, to the degree function of our IOTA and IoTeX volatility visibility graph-based complex network.

3.5.2. Power Law Fit Using the *Powerlaw* Module by Alstott et al.

Second, we assess the fit of the mentioned degree functions to a power law using the *powerlaw* Python module developed by Alstott et al. [55] and explained in Section 2.6.

Following [55], we plot the probability density function (PDF) and the complementary cumulative distribution function (CCDF) for each of the four degree functions in our analysis.

3.6. Average of Clustering Coefficients per Degree and Fit

Inspired by [54], we study the linking possibility between neighbouring nodes by calculating the clustering coefficient of every node in these four networks. We plot the average of the clustering coefficients per degree. After that, we assess their fit with a power law function with the *curve_fit* Python module.

3.7. Communities in the Network

Understanding the community structure of a network contributes to describing the heterogeneity of a network. We complete our study by calculating the number and location of communities in the analysed IOTA and IoTeX networks. We use the *community API* for community detection in *networkx* [66]. An alternative will be the use of the *cylovain* code [67]. We run both pieces of code, and the resulting number of communities are very similar (see Table 7):

Table 7. Community searching Python modules.

Module Name	Implemented Algorithm	IOTA Communities (VG and HVG)	IoTeX Communities (VG and HVG)
Community API	Louvain	19 and 29	15 and 23
Cylouvain	Louvain	18 and 30	15 and 23

3.8. Link with Intentional Risk and Application to 5G

First, the results we obtain in terms of how close degree functions and average clustering coefficients per degree are to a power law provide insights on the heterogeneity of the network stemming from the daily price volatility visibility graph. We link our results with the two dimensions that compose dynamic risk, i.e., value and accessibility. Second, the arrival of 5G to both IoT platforms can play an important role in increasing their accessibility and in broadening the services that both IOTA and IoTeX can provide, e.g., in terms of lower-cost, lower-energy, wider coverage and higher capacity. Table 8 summarises the steps followed in our methodology, their main objective and the tools we use:

Table 8. Summary of the methodology with steps, objectives and tools.

Step	Main Objective	Tools Used
1	Download daily maximum and minimum prices from *investing.com*	web browser
2	Production of daily price volatility time series	logarithm
3	Creation of natural visibility graphs for IOTA and IoTeX	*visibility_graph*
4	Creation of horizontal visibility graphs for IOTA and IoTeX	*visibility_algorithms*
5	Basic characterisation of the 4 networks (VG and HVG in IOTA and IoTeX)	*metaknowledge*
6	Production of the degree functions for the 4 networks	*networkx*
7	Power law fit for degree functions	*curve_fit*
8	Power law fit for degree functions (as proposed by Alstott)	*powerlaw*
9	Average of clustering coefficients per degree (as in [54])	*networkx*
10	Power law fit for average clustering (as in [54])	*curve_fit*
11	Identification of communities	*community_api*
12	Link with dynamic risk (as defined by [46])	literature review
13	Strategy to use 5G for IoT	literature review

4. Analysis and Results

4.1. The Visibility Graph Creates Four Networks

We apply the *visibility graph* and *horizontal visibility graph* algorithms to the IOTA and IoTeX daily price volatility series and we obtain four complex networks: IOTA VG, IoTeX VG, IOTA HVG and IoTex HVG. The *metaknowledge* module provides a first approximation to the properties of these four networks (see Table 9):

Table 9. Initial description of the visibility graph-based networks.

Network	Nodes	Edges	Isolates	Self Loops	Density	Transitivity
IOTA VG	1493	5715	0	0	0.005	0.300
IoTeX VG	1122	4472	0	0	0.007	0.312
IOTA HVG	1493	2969	0	0	0.003	0.344
IoTeX HVG	1122	2225	0	0	0.004	0.354

The VG networks have a higher number of edges and, consequently, still low but higher values of density than HVGs. The four networks have a very low density and a low transitivity.

4.2. Power Law Fit Using Curve_Fit

Figure 3 shows the power law fits we obtain using *curve_fit*. We see how the fit for the IoTeX VG network provides a value of $\alpha = 2.61$ in accordance with Equation (1), hinting at the existence of a scale-free network. The IOTA VG, with an $\alpha = 1.93$ does not reach a value of two. When we focus on the HVG, we see an $\alpha = 2.03$ and 2.01 for IOTA and IoTeX networks, respectively. We can even talk of incipient scale-free networks in both HVG cases. We highlight as well how in the four subplots the power law fit has a maximum degree from which there is no power law fit.

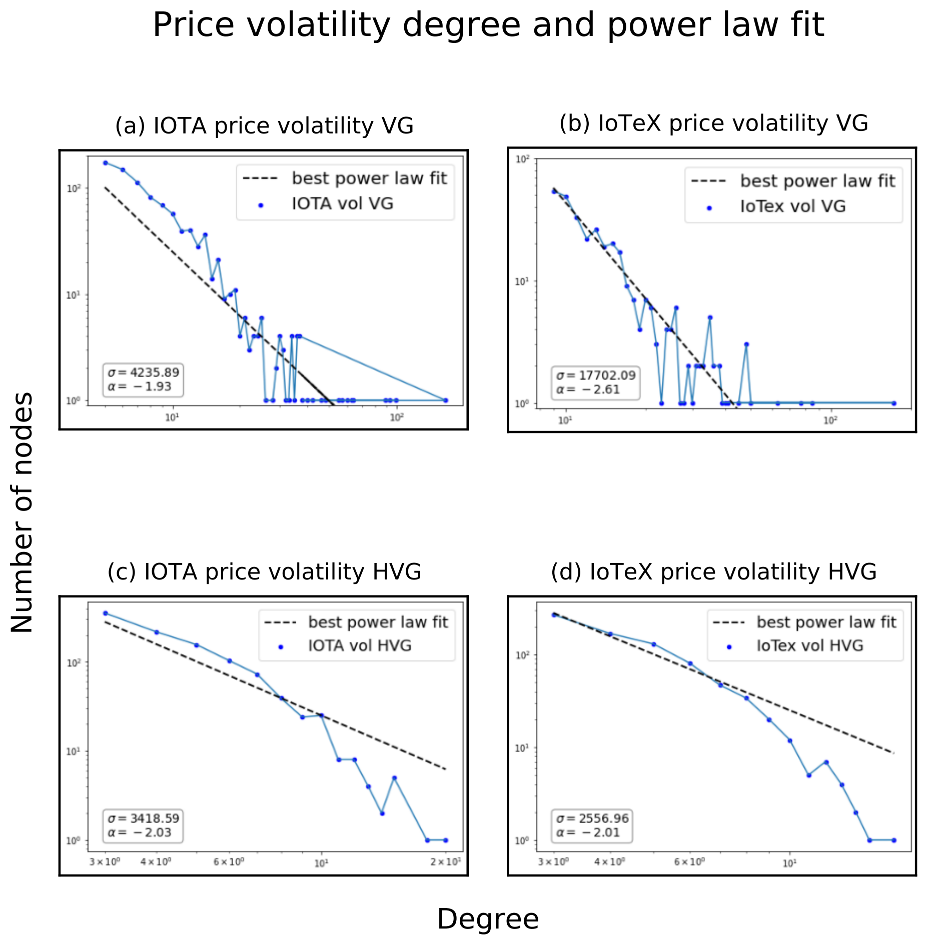


Figure 3. Number of nodes for each degree in the networks stemming from the visibility and horizontal visibility graphs for IOTA and IoTeX price volatility. Subplots (**a**,**b**) display the degree of the network stemming from the visibility graph and the best power law fit that the function *curve_fit* provides together with the corresponding best α and σ. Subplots (**c**,**d**) display the degree of the network stemming from the horizontal visibility graph and the best power law fit that the function *curve_fit* provides and the corresponding best α and σ.

4.3. Power Law Fit Using the Powerlaw Module by Alstott

We use a second, more stringent, technique to assess the power law fit of the degrees in both the *visibility graph* and *horizontal visibility graph* networks: the Python module by Alstott *powerlaw* [55]. Figure 4 shows both the empirical and the fit probability density function (PDF) and the complementary cumulative distribution (CCDF) for the four networks. We identify a good fit with the power law CCDF for the four networks. However, the PDF fit can only be partially observed in the IoTeX VG. All four values of α are well below two. In the remaining three networks, i.e., IOTA VG and IOTA and IoTeX HVG, the power law fits we obtain are quite limited in the range of degrees for IOTA VG and extremely limited for both HVGs.

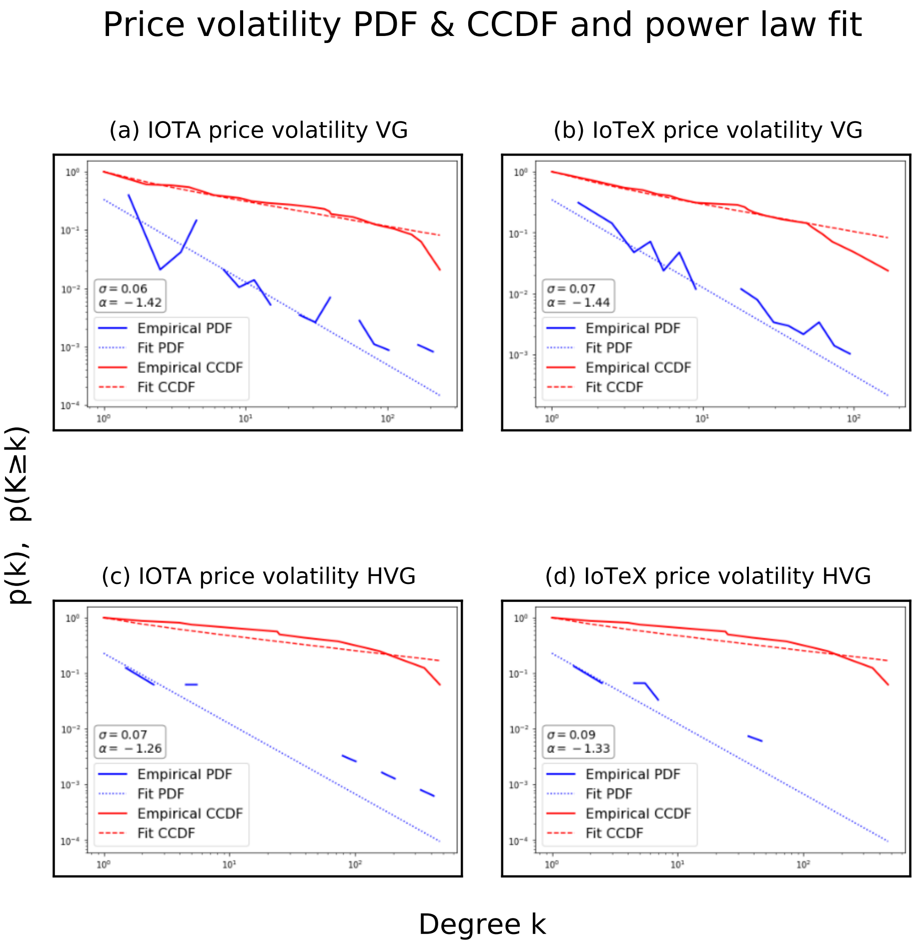


Figure 4. Both empirical and fit probability density functions (PDF) and complementary cumulative distribution functions (CCDF) using the *powerlaw* module by Alstott et al. [55].

4.4. Communities Formation Criteria within the Networks

We calculate the average of clustering coefficients per degree [54] with our own Python code. We plot this curve and fit it to a power law using *curve_fit*. We use the same scale as the degree function, although, here, the y axis' range is one order of magnitude smaller. Figure 5 reveals that the power law fit is greater than in the previous cases when we plotted the degree. This means that communities at different levels are formed according to an identical law showing a fractal behaviour, i.e., a hierarchical network [54]. The values of α are very close to 2 for both HVGs, where we identify an initial scale-free behaviour and around 1.85 for the VGs. In this case, we do not plot this fit using the *powerlaw* module by Alstott since the fit we observe with *curve_fit* shows a less heavy-tailed distribution than in the degree graphs.

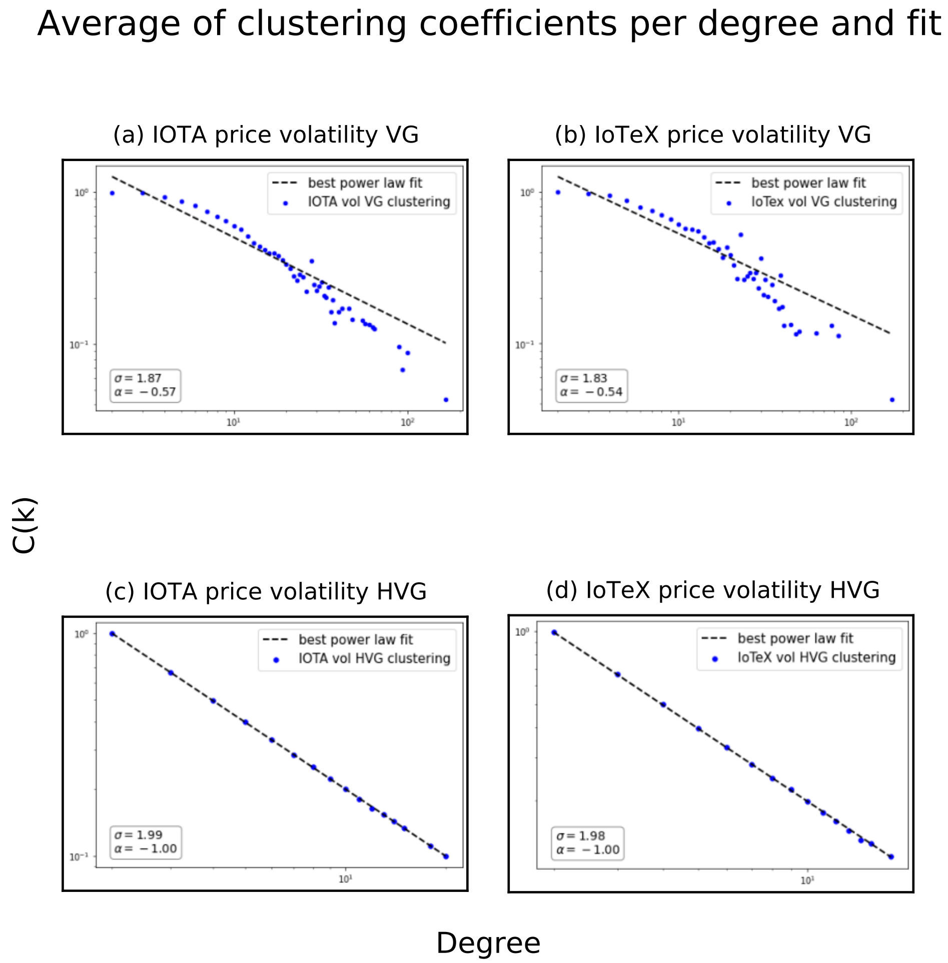


Figure 5. Best power law fit using *curve_fit* with the average of clustering coefficients per degree for (**a**) IOTA VG, (**b**) IoTeX VG, (**c**) IOTA HVG and (**d**) IoTeX HVG.

4.5. Communities Identified in the IOTA and IoTeX Networks

We obtain the existing communities in these networks using *Community API* [66], a Python module that implements the Louvain algorithm [68]. We identify a number of communities, as Table 7 shows. The presence of a community of nodes in a visibility graph is inherent to its creation. Community participant nodes tend to cluster together with a small value of the average shortest path along the timeline [54].

Figure 7 provides both volatility information as subplots in Figure 1 plus community information along IOTA and IoTeX timelines.

5. Conclusions

5.1. Visibility Graphs Are a Helpful Tool to Leverage Time Series with Network Analysis

This study confirms the usefulness of the proposal by Lacasa et al. [3] to transform time series into complex networks using visibility graphs. It is a novel way to incorporate the time dimension as an object of study within a complex network. Visibility graphs, as also confirmed by Liu et al. [54], preserve useful information present in the time series onto the resulting complex network.

5.2. IOTA and IoTeX Markets Are Still at Their Infancy in Terms of Development—IoTex Appears to Develop Faster

The number of data points studied in these networks is reduced. The history of both IoT tokens is still short. The density and transitivity figures obtained in Section 4.1 confirm this point. Similar VGs in Bitcoin, Ethereum and Litecoin [54] display stronger powerlaw fits. Their time series are 5 years long compared to the 4 and 3 year-long time series history for IOTA and IoTeX, respectively. IoTex VG, although one year younger than IOTA, seems to display a slightly better power law fit than IOTA. Figure 4 confirms this point. This could hint a faster path to maturity for IoTeX. In terms of HVG, given that the number of edges is more limited, we do not draw conclusions on maturity based on Figures 3 and 4.

5.3. IOTA and IoTeX Visibility Networks form Communities in a Hierarchical Structure

Figure 5 confirms power law fits when we plot the average of clustering coefficients per degree in the four visibility networks, i.e., IOTA VG and HVG and IoTeX VG and HVG. This leads to a hierarchical structure, similar to the findings proposed by Liu et al. in the case of Bitcoin, Ethereum and Litecoin [54]. This means that the creation of communities of nodes, as Figures 6 and 7 display, follow an identical law at different levels of time sampling.

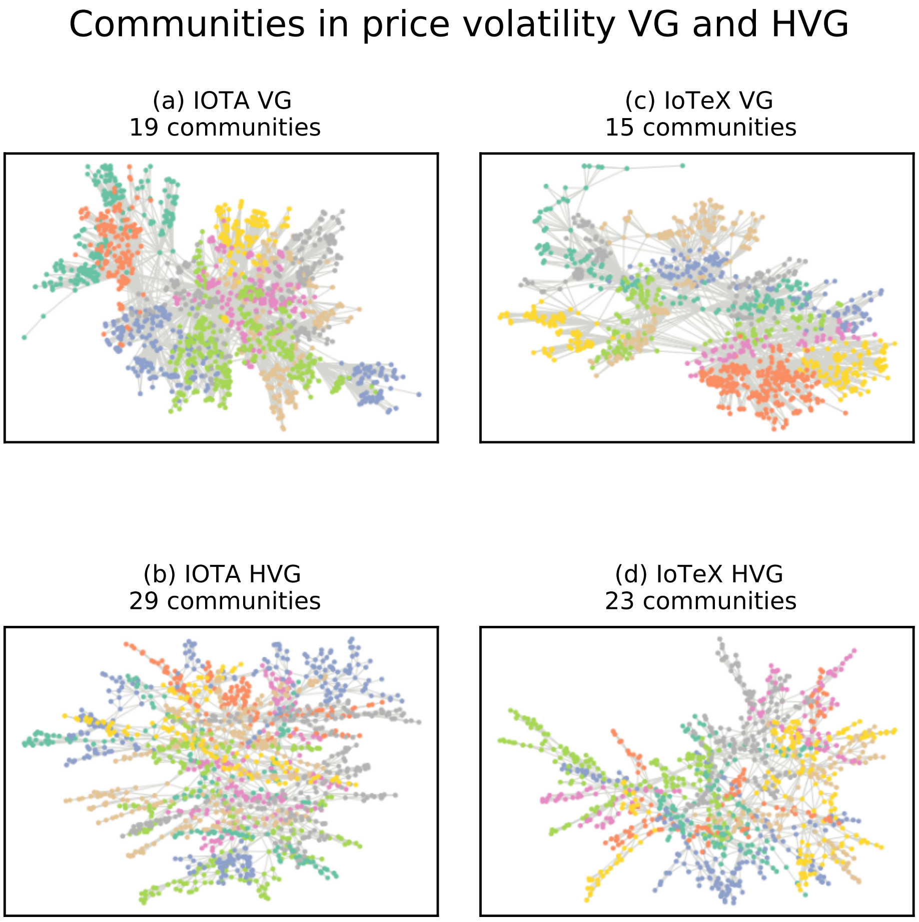


Figure 6. Communities identified by the *networkx* module *community API* in (**a**) IOTA VG, (**b**) IoTeX VG, (**c**) IOTA HVG and (**d**) IoTeX HVG throughout the timeline in network graph format.

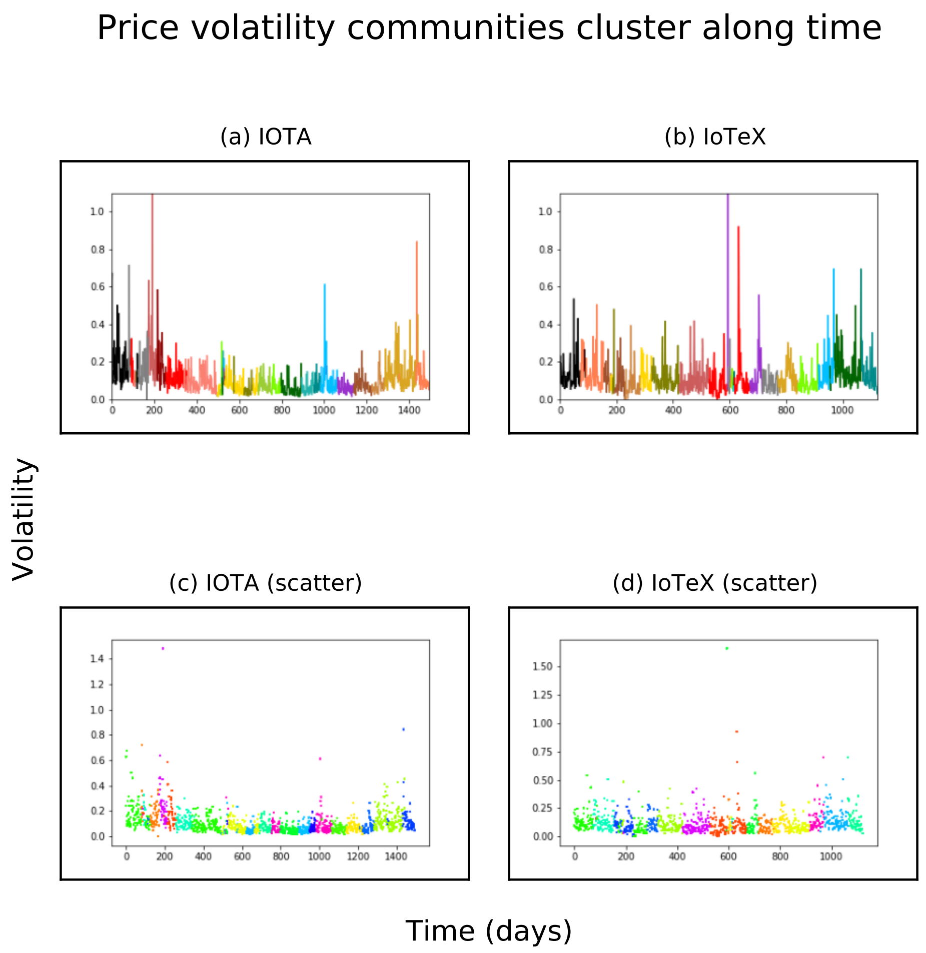


Figure 7. Communities identified by the *networkx* module *community API* in IOTA, (**a**,**c**), and IoTeX, (**b**,**d**). Graphs (**a**,**b**) use a coloured-coded continuous line and graphs (**c**,**d**) a coloured-coded scattered plot.

5.4. 5G Can Accelerate IOTA and IoTeX Development

The move into production of 5G mobile networks, with the added value explained in Section 2.1.1, will trigger the further rollout of multiple IoT implementations and increase their adoption rates. As IOTA and IoTeX are the two most capitalised platforms [27], both are optimally positioned to become worldwide references in IoT deployments.

5.5. Intentional Risk: A Lever to Understand the Impact of 5G on IOTA and IoTeX

Within intentional risk, dynamic risk measures the impact of anonymous actors on information systems [46]. Value and accessibility are the two components of dynamic risk. The use of 5G in IoT platforms such as IoTeX and IOTA can increase their dynamic risk and, consequently:

(a) The value at stake in the respective networks.
(b) The accessibility of the participants.

We suggest several strategies to mitigate the growth of these two dimensions:

(a) Distribute the new value generated across all platform participants. This will require a reduction of highly connected nodes, i.e., hubs that have a tendency to accumulate value. However, this strategy is not aligned with typical power law degree functions identified in IOTA and IoTeX. High-value hubs seem to remain and even grow in more mature crypto-networks (e.g., BTC and ETH [26]). We therefore recommend to:

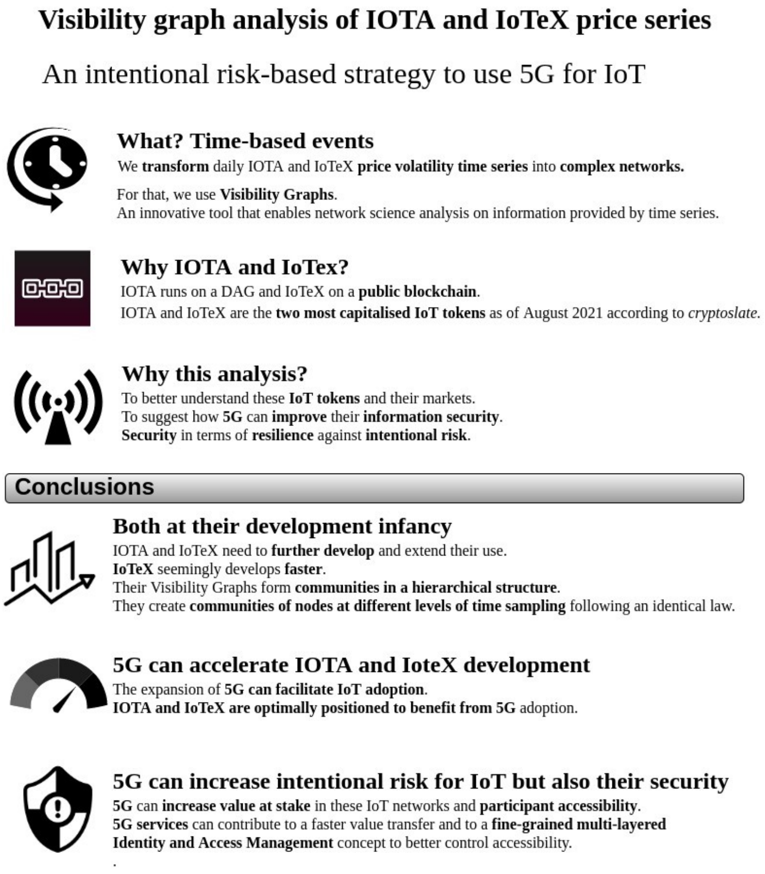
(b) Improve accessibility controls, especially to those nodes holding high value. An effective identity and access management (IAM) system, as mentioned in [26], is a potential improvement path.
(c) Apply a multi-layered IAM system at different levels of scale considering the hierarchical structure observed in IOTA and IoTeX communities.

5.6. 5G Can Improve Information Security in IOTA and IoTeX

Considering the findings of our study and our prior conclusions, we state that 5G is well positioned to contribute to the security of IOTA and IoTeX platforms. The three main 5G services, i.e., enhanced Mobile BroadBand (eMBB), massive Machine Type Communication (mMTC) and URLLC (Ultra Reliable and Low Latency Communications) can:

(a) Enable faster communications between IoT nodes so that high-value nodes can distribute their wealth more securely and quickly.
(b) Allow for the implementation of more comprehensive, more fine-grained and faster identity and access management systems that would serve IOTA and IoTeX nodes.
(c) Apply these 5G improvements not only at the edge level to tackle communications with IoT nodes but also between edge and cloud servers participating in the IoT platform, also known as "fog computing" or "fog networking", as it is the case in IoTeX [26]. This would mean that IoTeX could have the potential to quickly reap benefits from 5G given its edge and cloud design.

We use *app.diagrams.net* in Figure 8 to summarise in an infographic the main points of this study.



Visibility graph analysis of IOTA and IoTeX price series

An intentional risk-based strategy to use 5G for IoT

What? Time-based events
We **transform** daily IOTA and IoTeX **price volatility time series** into **complex networks.**
For that, we use **Visibility Graphs**.
An innovative tool that enables network science analysis on information provided by time series.

Why IOTA and IoTex?
IOTA runs on a DAG and IoTeX on a **public blockchain**.
IOTA and IoTeX are the **two most capitalised IoT tokens** as of August 2021 according to *cryptoslate.*

Why this analysis?
To better understand these **IoT tokens** and their markets.
To suggest how **5G** can **improve** their **information security**.
Security in terms of **resilience** against **intentional risk**.

Conclusions

Both at their development infancy
IOTA and IoTeX need to **further develop** and extend their use.
IoTeX seemingly develops **faster**.
Their Visibility Graphs form **communities in a hierarchical structure**.
They create **communities of nodes at different levels of time sampling** following an identical law.

5G can accelerate IOTA and IoteX development
The expansion of **5G can facilitate IoT adoption**.
IOTA and IoTeX are optimally positioned to benefit from 5G adoption.

5G can increase intentional risk for IoT but also their security
5G can **increase value at stake** in these IoT networks and **participant accessibility**.
5G services can contribute to a faster value transfer and to a **fine-grained multi-layered Identity and Access Management** concept to better control accessibility.
.

Figure 8. Infographic summary of "Visibility graph analysis of IOTA and IoTeX price series: An intentional risk-based strategy to use 5G for IoT".

6. Future Work

We suggest three paths for further research related to the role IOTA and IoTeX platforms will play in the IoT arena:

(a) Contribute to the creation of public DAG and blockchain explorers with more advanced functionalities than the currently available ones for IOTA, thetangle.org [69], and IoTeX, IoTeXscan.io [58] (both accessed on 30 July 2021). As an example, the extraction of the transactions happening in real-time from the current explorers so that they can be easily analysed is still challenging. We would also like to contribute to an academic study focused on the standardisation of blockchain explorer functionalities and on the creation of the corresponding code modules that would implement them.

(b) Once our first future work point is accomplished, we would like to perform a study similar to this one based on IOTA and IoTeX transaction data, i.e., creating the visibility graph from the transaction time series. We would complement this analysis with a time series clustering proposal that combines multiplex networks and time series attributes [1].

(c) Finally, we would like to perform a similar volatility-based visibility graph analysis on other crypto-tokens such as the three currently most capitalised ones [70], i.e., Bitcoin, ETH and USDT with their entire price time series history.

Author Contributions: Conceptualization, A.P., M.R. and R.C. methodology, A.P., M.R. and R.C.; software, A.P.; validation, A.P., M.R. and R.C.; formal analysis, A.P., M.R. and R.C.; investigation, A.P.; resources, A.P., M.R. and R.C.; data curation, A.P.; writing—original draft preparation, A.P.; writing—review and editing, A.P., M.R. and R.C.; visualization, A.P.; supervision, M.R. and R.C.; project administration, M.R. and R.C.; funding acquisition, M.R. and R.C. 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. Iglesias, P.S.; Moral-Rubio, S.; Criado, R. A new approach to combine multiplex networks and time series attributes: Building intrusion detection systems (IDS) in cybersecurity. *Chaos Solitons Fractals* **2021**, *150*, 111143. [CrossRef]
2. Newman, M.E.J. The Structure and Function of Complex Networks. *Siam Rev.* **2003**, *45*, 167–257. [CrossRef]
3. Lacasa, L.; Luque, B.; Ballesteros, F.; Luque, J.; Nuño, J.C. From time series to complex networks: The visibility graph. *Proc. Natl. Acad. Sci. USA* **2008**, *105*, 4972–4975. [CrossRef] [PubMed]
4. Hewa, T.M.; Kalla, A.; Nag, A.; Ylianttila, M.E.; Liyanage, M. Blockchain for 5G and IoT: Opportunities and Challenges. In Proceedings of the 2020 IEEE Eighth International Conference on Communications and Networking (ComNet), Hammamet, Tunisia, 27–30 October 2020; pp. 1–8. [CrossRef]
5. Meraj, M.; Kumar, S. Evolution of mobile wireless technology from 0G to 5G. *Int. J. Comput. Sci. Inf. Technol.* **2015**, *6*, 2545–2551.
6. LTE Encyclopedia. Acronyms. Available online: https://sites.google.com/site/lteencyclopedia/lte-acronyms (accessed on 22 July 2021).
7. Qualcomm. What Is 5G. Available online: https://www.qualcomm.com/5g/what-is-5g (accessed on 22 July 2021).
8. GSM Phase out Calendar. Available online: https://www.emnify.com/en/resources/global-2g-phase-out (accessed on 22 July 2021).
9. 3GPP. 3rd Generation Partnership Project (3GPP). Available online: https://www.3gpp.org/ (accessed on 22 July 2021).
10. Telekom. 5G Real Time Speed. Available online: https://www.telekom.com/en/company/details/5g-speed-is-data-transmission-in-real-time-544498 (accessed on 22 July 2021).
11. Statista. Internet Usage Worldwide—Statistics & Facts. Available online: https://www.statista.com/topics/1145/internet-usage-worldwide/ (accessed on 22 July 2021).
12. Statista. Mobile Internet Usage Worldwide—Statistics & Facts. Available online: https://www.statista.com/topics/779/mobile-internet/ (accessed on 22 July 2021).
13. Statista. Internet of Things. Revenue by Segment. Available online: https://www.statista.com/outlook/tmo/internet-of-things/worldwide (accessed on 22 July 2021).

14. 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 22 July 2021).
15. Statista. 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 22 July 2021).
16. 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 22 July 2021).
17. Ericsson. IoT Protocols in 5G. Available online: https://www.ericsson.com/en/reports-and-papers/nb-iot-and-lte-m-in-the-context-of-5g-industry-white-paper (accessed on 22 July 2021).
18. 3GPP. 3rd Generation Partnership Project (3GPP). Decisions on IoT Protocols. Available online: https://www.3gpp.org/news-events/1805-iot_r14 (accessed on 22 July 2021).
19. Qualcomm. Private Industrial Networks Offer Key Benefits for Industrial IoT. Available online: https://www.qualcomm.com/research/5g/5g-industrial-iot (accessed on 23 July 2021).
20. Qualcomm. The $12 Trillion Opportunity Ahead. Available online: https://www.qualcomm.com/media/documents/files/fierce-wireless-ebrief-5g-release-16.pdf (accessed on 22 July 2021).
21. Nakamoto, S.; Bitcoin: A Peer-to-Peer Electronic Cash System. Nakamotoinstitute.org, October 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 21 July 2021).
22. Christian, C.; Joshua, S.G. Some Simple Economics of the Blockchain, Working Paper 22952, National Bureau of Economic Research, December 2016. Available online: https://www.nber.org/papers/w22952 (accessed on 22 July 2021).
23. ECB. "Distributed Ledger Technology", In Focus, Issue 1, European Central Bank. 2016. Available online: https://bit.ly/3fHcOYS (accessed on 22 May 2021).
24. ESMA. "The Distributed Ledger Technology Applied to Securities Markets", Report ESMA50-1121423017-285, Discussion Paper, European Securities and Markets Authority, 7 February 2017. Available online: https://bit.ly/344omjI (accessed on 22 July 2021).
25. Pinna, A.; Ruttenberg, W. "Distributed Ledger Technologies in Securities Post trading: Revolution or Evolution", ECB Occasional Paper Series 172, European Central Bank, 20 April 2016. Available online: https://bit.ly/3oHEMaY (accessed on 22 July 2021).
26. Partida, A.; Criado, R.; Romance, M. Identity and Access Management Resilience against Intentional Risk for Blockchain-Based IOT Platforms. *Electronics* **2021**, *10*, 378. [CrossRef]
27. IOT Crypto Coin Market Value. Available online: https://cryptoslate.com/cryptos/iot/ (accessed on 22 July 2021).
28. Arm. Managing the Future of Cellular. Available online: https://www.arm.com/-/media/global/solutions/infrastructure/managing-the-future-of-cellular.pdf (accessed on 23 July 2021).
29. Statista. Forecast 5G-Enabled Smartphone Shipments as Share of Total Smartphone Shipments Worldwide from 2019 to 2023. Available online: https://www.statista.com/statistics/1027246/5g-smartphone-shipment-share-worldwide/ (accessed on 23 July 2021).
30. IHS Economics. The 5G Economy: How 5G Technology Will Contribute to the Global Economy. Available online: https://cdn.ihs.com/www/pdf/IHS-Technology-5G-Economic-Impact-Study.pdf (accessed on 23 July 2021).
31. Bogale, T.E.; Wang, X.; Le, L.B. mmWave communication enabling techniques for 5G wireless systems: A link level perspective. In *MmWave Massive MIMO*; Academic Press: Cambridge, MA, USA, 2017; pp. 195–225.
32. Shen, X. Device-to-device communication in 5G cellular networks. *IEEE Netw.* **2015**, *29*, 2–3. [CrossRef]
33. Khurpade, J.M.; Rao, D.; Sanghavi, P.D. A Survey on IOT and 5G Network. In Proceedings of the 2018 International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, India, 5 January 2018; pp. 1–3.
34. Fatokun, T.; Nag, A.; Sharma, S. Towards a Blockchain Assisted Patient Owned System for Electronic Health Records. *Electronics* **2021**, *10*, 580. [CrossRef]
35. Sun, H.; Hua, S.; Zhou, E.; Pi, B.; Sun, J.; Yamashita, K. Using Ethereum blockchain in Internet of Things: A solution for electric vehicle battery refueling. In *International Conference on Blockchain*; Springer: Cham, Switzerland, 2018; pp. 3–17.
36. IOTA Corporate Site. Explore IOTA Industries. Available online: https://www.iota.org/solutions/industries (accessed on 28 July 2021).
37. IoTex Team and Introduction Portal. Available online: https://iotex.io/ (accessed on 28 July 2021).
38. 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*; Park, N., Sun, K., Foresti, S., Butler, K., Saxena, N., Eds.; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer: Cham, Switzerland, 2020; Volume 336.
39. 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]
40. Mistry, I.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. *Mech. Syst. Signal Process.* **2020**, *135*, 106382. [CrossRef]
41. Florea, B.C.; Taralunga, D.D. Blockchain IoT for smart electric vehicles battery management. *Sustainability* **2020**, *12*, 3984. [CrossRef]
42. Tekeoglu, A.; Ahmed, N. TangoChain: A Lightweight Distributed Ledger for Internet of Things Devices in Smart Cities. In Proceedings of the 2019 IEEE International Smart Cities Conference (ISC2), Casablanca, Morocco, 14–17 October 2019; pp. 18–21.

43. Newman, M.E.J. The Connected World. 2011-09-15. Santa Fe Institute. Available online: https://www.youtube.com/watch?v=yAtsm5xkb5c (accessed on 21 December 2021).
44. Newman, M.E.J. Using Networks To Make Predictions. 2011-09-15. Santa Fe Institute. Available online: https://www.youtube.com/watch?v=rwA-y-XwjuU (accessed on 21 December 2021).
45. Newman, M.E.J. What Networks Can Tell Us About the World. 2011-09-15. Santa Fe Institute. Available online: https://www.youtube.com/watch?v=lETt7IcDWLI (accessed on 21 December 2021).
46. Chapela, V.; Criado, R.; Moral, M.; Romance, R. *Intentional Risk Management through Complex Networks Analysis*; Springer: Berlin/Heidelberg, Germany, 2015.
47. Boccaletti, S.; Latora, V.; Moreno, Y.; Chavez, M.; Hwang, D. Complex Networks: Structure and Dynamics. *Phys. Rep.* **2006**, 175–308. [CrossRef]
48. 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] [PubMed]
49. Guo, D.; Dong, J.; Wang, K. Graph structure and statistical properties of Ethereum transaction relationships. *Inf. Sci.* **2019**, *492*, 58–71. [CrossRef]
50. Ali, A.H.; Hassan, A.; Nasir, A.M. The relationship between trading volume, volatility and stock market returns: A test of mixed distribution hypothesis for a pre-and post crisis on Kuala Lumpur Stock Exchange. *Invest. Manag. Financ. Innov.* **2005**, *2*, 146–158.
51. Yamak, N.; Yamak, R.; Samut, S. Causal relationship between bitcoin price volatility and trading volume: Rolling window approach. *Financ. Stud.* **2019**, *23*, 6–20.
52. Guizani, S.; Nafti, I.K. The Determinants of Bitcoin Price Volatility: An Investigation with ARDL Model. *Procedia Comput. Sci.* **2019**, *164*, 233–238. [CrossRef]
53. Luque, B.; Lacasa, L.; Ballesteros, F.; Luque, J. Horizontal visibility graphs: Exact results for random time series. *Phys. Rev. E* **2009**, *80*, 046103. [CrossRef] [PubMed]
54. Liu, K.; Weng, T.; Gu, C.; Yang, H. Visibility graph analysis of Bitcoin price series. *Phys. A Stat. Mech. Its Appl.* **2020**, *538*, 122952. [CrossRef]
55. Alstott, J.; Bullmore, E.; Plenz, D. Powerlaw: A Python Package for Analysis of Heavy-Tailed Distributions. *PLoS ONE* **2014**, *9*, e85777. [CrossRef]
56. Andina, D.; Partida, A. *IT Security Management: IT Securiteers—Setting Up an IT Security Function*; Lecture Notes in Electrical Engineering; Springer: Berlin/Heidelberg, Germany, 2010.
57. IOTA Blockchain Explorer. Available online: https://explorer.iota.org/mainnet (accessed on 30 July 2021).
58. IoTeX Blockchain Explorer. Available online: https://iotexscan.io/ (accessed on 29 July 2021).
59. Investing.com IOTA Index (IOT/USD). IOT Crypto Coin Market Value. Available online: https://www.investing.com/indices/investing.com-iota-usd-historical-data (accessed on 24 July 2021).
60. Investing.com IoTeX Index (IOTX/USD). IoTeX Crypto Coin Market Value. Available online: https://www.investing.com/indices/investing.com-iotx-usd-historical-data (accessed on 24 July 2021).
61. Visibility-Graph 0.4.1 by Rodrigo Garcia. 2 February 2021. Available online: https://pypi.org/project/visibility-graph/ (accessed on 29 July 2021).
62. Visibility_Algorithms.py by Delia Fano Yela. December 2018. Available online: https://github.com/delialia/bst/blob/master/visibility_algorithms.py (accessed on 29 July 2021).
63. Networkx 2.6.2. Network Analysis in Python. Last Release in 2021. Available online: https://networkx.org/ (accessed on 30 July 2021).
64. Metaknowledge 3.4.1. Computational Research in Network Analysis. NetLab. University of Waterloo. 2020. Available online: https://pypi.org/project/metaknowledge/ (accessed on 30 July 2021).
65. Scipy.Optimize.Curve_Fit. Available online: https://docs.scipy.org/doc/scipy/reference/generated/scipy.optimize.curve_fit.html (accessed on 29 July 2021).
66. Community API. This Package Implements Community Detection. Package Name Is Community but Refer to Python-Louvain on Pypi. 2008. Available online: https://python-louvain.readthedocs.io/en/latest/api.html (accessed on 29 July 2021).
67. Cylouvain: Cython Louvain. Cylouvain is a Python Module that Provides a Fast Implementation of the Classic Louvain Algorithm for Node Clustering in Graph. 2018. Available online: https://github.com/ahollocou/cylouvain (accessed on 29 July 2021).
68. Que, X.; Checconi, F.; Petrini, F.; Gunnels, J.A. Scalable community detection with the Louvain algorithm. In Proceedings of the 2015 IEEE International Parallel and Distributed Processing Symposium, Hyderabad, India, 25–29 May 2015; pp. 28–37.
69. IOTA Tangle Explorer. Available online: https://thetangle.org/ (accessed on 30 July 2021).
70. Coinmarketcap. Cryptocurrencies Market Capitalisation in Real Time. Available online: https://coinmarketcap.com/all/views/all/ (accessed on 31 July 2021).

7. Results and discussion

This chapter presents the main results of the articles published for this doctoral work and included in Chapters 4, 5 and 6, respectively. It also includes a discussion on these results and some actionable proposals to protect these blokchain implementations from intentional risk.

7.1 On facilitating understanding of public blockchains: BTC and ETH

7.1.1 The SoS of public blockchains

BTC and ETH are the two most relevant components of the SoS of public blockchains. Both permissionless implementations transfer digital value and they are independent of each other. Besides, ETH and BTC are open to their environment, e.g., there is an open trading market, where their crypto assets can be bought and sold. More generally, they exchange value and energy with the environment outside the SoS, and, ultimately, their networks keep on growing in size and complexity. The following sections summarise the results published in Article 1 [87], available in Chapter 4 of this thesis.

7.1.2 Network centricity

BTC and ETH are network-based systems. They interact with the elements mentioned by Jamshidi et al. [68]: people, organisations, culture, e.g., they share principles on decentralisation, activities, such as coin wrapping, and relationships, as public blockchains are subject to financial regulation.

7.1.3 Autonomy, belonging, connectivity and diversity

Regarding autonomy, both public blockchain implementations are independent. BTC open source code evolves through BTC improvement proposals (BIP) and ETH, equally, via ETH improvement proposals (EIP). The search for consensus among development, user and mining communities appears as a fundamental governance principle. Regarding belonging, any participant in any of those communities can opt in and out of the SoS at any time. In these open systems, no participant in these communities owns these networks in its entirety. Therefore, consensus-driven governance is pivotal. Concerning connectivity, as the SoS of public blockchains is network-centric and both BTC and ETH are permissionless, any piece of code that implements the corresponding BTC or ETH open-source protocol can join the networks. Additionally, the connection of different public blockchain implementations via code is possible with interledger communication protocols such as the Interledger Protocol (ILP). With respect to diversity, although the transaction networks of both blockchain implementations display a power law degree distribution function, their use cases make them partners rather than competitors.

7.1.4 Emergence

This is arguably the most relevant property out of the set of properties proposed by Jamshidi et al. [68]. The intended emergent property of the SoS of public blockchains is the creation of a decentralised network to transfer digital value in the form of digital private property. More concretely, the original vision for BTC was the creation of a "purely peer-to-peer version of electronic cash" [79]. In the case of ETH, their vision is to become the "distributed world computer". This research leads to postulate that the initially unintended emergent property of this SoS is to act as an alternative to the current fiat currency based financial system. Within this alternative decentralised SoS, the unintended emergent property of BTC is to play the role of a global digital reserve asset, i.e, the "digital gold". Regarding ETH, its unintended emergent property is to facilitate decentralised finance (DeFi), i.e., to stand out as the "alternative financial conduit".

7.1.5 Vulnerability and threat analysis

The main vulnerabilities identified in BTC and ETH through this research are the knowledge-based and usability barriers to entry as a user, the early stage of evolution in terms of adoption, several signs of centralisation in terms of the prominent role that super-hubs play in their transaction networks and, finally, the exclusive dependence on code for on-chain governance. Simultaneously, the main threats identified are the uncertain regulatory scenario, the still to be decided trade off between privacy and traceability, future developments in encryption, e.g., related to quantum computing, lack of co-operation between the SoS of traditional finance and the SoS of public blockchains and, finally, the interest of diverse actors to intentionally attack this SoS to extract value out of it.

7.1.6 Resilience against intentional risk

Based on the intentional risk parameters proposed by Chapela et al. [21], there is a series of measures that can increase resilience against intentional risk, such as the distribution of value among addresses, avoidance of rich hubs, enhancement in code security, especially the off-chain pieces of code, subject to less scrutiny than the on-chain open source protocols, increase of security awareness among users, better IAM techniques, probably associating digital identities with physical ones to the detriment of privacy, better global legal coverage, extension of blockchain transaction monitoring and, finally, adoption of robust *know your customer procedures.*

7.1.7 Discussion and link with Article 2

The implementation in existing public blockchains of some of the security measures listed in Section 7.1.6 can be initiated with relative low cost and potentially high benefits. First, in-chain and off-chain code security can be improved if any piece of code added to the production environment is audited by development communities. An incentive-based security testing scheme, popularly known as a "bug bounty" programme, can trigger the interest of many stakeholders. Second, the fact that the blockchain database is publicly available makes a further development in transaction monitoring easily implementable, with a special focus on "rich hubs". Third, with regard to better IAM techniques, Article 2 in this thesis focuses on this key security concept and provides some insight on how to improve IAM resilience against intentional risk.

7.2 On improving IAM resilience against intentional risk: IOTA and IoTeX

The following sections summarise the results published in Article 2 [85], available in Chapter 5 of this thesis.

7.2.1 IOTA and IoTeX complex network analysis

The complex networks created out of IOTA and IoTeX transaction data produce non-connected graphs and display degree distributions that evoke a power law function. The very low density of edges and the very low average clustering coefficient confirm the absence of a small-world structure. These two parameters are lower in the IoTeX network than in the IOTA network. The plot of the largest connected components in both networks shows high disassortativity. This is aligned with traditional IoT architectures in which all sensors and actuators communicate with a specific server.

7.2.2 Comparison with the BTC and ETH complex networks

The complex networks built out of the BTC and ETH transaction data produce similar results. The degree distributions resemble a power law function and the low clustering coefficient and edge density values suggest that there are no signs of a small world structure. Overall, the longer the time window of the transaction data studied, the more accurate the results are and the closer the degree distribution fits a power law function.

7.2.3 Goodness of fit test of a power law function

The *powerlaw* library by Alstott et al. [4] is useful to test the goodness of fit of IOTA, IoTeX, BTC and ETH degree distributions of a power law function. BTC scores best, with ETH second, then IoTeX and finally, far from a good fit, IOTA.

7.2.4 Discussion and link with Article 3

It is interesting to highlight how two different IoT platforms in terms of architecture, balance models and use of sidechains [85] produce similar complex networks and degree distributions and how they start to resemble "older" implementations such as BTC and ETH. In addition, it is also worth noting how these networks do not show small-world structure once they reach a certain size, specially due to the very low density in their nodes. Additionally, the existence and the need to protect "rich hubs" in these networks appear again as a recommendable security measure. Considering the results of Article 2 in the context of IAM and the typical security incidents occurring in public blockchains [85], the link of digital identities with physical identities seems to be somehow required to increase resilience against intentional risk. Appendixes A and B discuss this point. Finally, while Article 2 focuses on IAM aspects, it would be advisable to zoom out, making one step further and propose a intentional risk-based protection strategy, certainly including IAM as an element of it. That is the purpose of Article 3 of this thesis. However, given the challenge to obtain transaction data from both IOTA and IoTeX, the research for Article 3 makes use of a different source of information: daily price time series.

7.3 On creating an intentional risk-based strategy: IOTA and IoTeX

The following sections summarise the results published in Article 3 [86], available in Chapter 6 of this thesis.

7.3.1 Complex networks out of visibility graphs

The complex networks that stem out of the natural visibility graphs (VG) of the IOTA and IoTeX daily price volatility time series contain almost double number of edges than the complex networks built from the horizontal visibility graphs (HVG) of the same IOTA and IoTeX time series. This fact comes from the definition of VG and HVG, as the way to draw edges in HVGs is more restricted than in VGs. Equally, due to the way visibility graphs are constructed, these networks are connected, they show low density values, their transitivity figures are close to 0.3 and lack self loops.

7.3.2 Power law fits for the degree distributions

The plot of the degree distributions for the IOTA and IoTeX natural and horizontal visibility graphs signals a fit with their corresponding power law functions, restricted to a specific maximum degree value. The PDFs and CCDFs plots complement this result. The fit with the CCDF plot, given its cumulative nature, is patent, however, the fit with the PDF plot is only existent in the IOTA and IoTeX VG networks for very specific degree ranges. Regarding the HVG networks, the fit with the PDF plot is hardly existent.

7.3.3 Communities in IOTA and IoTeX VGs and HVGs

The plot of the average clustering coefficient per degree for each of the four studied networks reveals a better power law fit than with the degree distributions, explained in Section 7.3.2. This means that the networks form communities that follow an identical law at different scales [76]. This type of fractality is known as a hierarchical structure. The rules to construct visibility graphs favour the appearance of communities in the resulting networks. Nodes participating in a community tend to cluster and connect to each other. The researched networks proceed from IOTA and IoTeX VGs and HVGs. These visibility graphs stem from a daily price volatility time series that, in the case of IOTA, ranges from 2017 to 2021, and, in the case of IoTeX, from 2018 to 2021. This research identifies 19, 15, 29 and 23 communities in IOTA and IoTeX VGs and HVGs, respectively.

7.3.4 Discussion

In tune with the discussion in Article 2, the similarity between the results obtained for both IOTA and IoTeX is remarkable. The hierarchical structure, especially in the HVG networks, first confirms the usefulness of techniques such as the visibility graphs to study time series through complex networks, and second, it seems reasonable to think that lower volatility values would produce a higher number of communities in the graph. In terms of potential security measures, the proposal to further secure "rich hubs" as an effective action to increase resilience appears as well in Article 3. In fact, the idea to reduce and, or further protect these hubs with high value, e.g., by improving accessibility controls to these nodes, is present in the three articles. Similarly, Song et al. [100] talk about "hub compartmentalisation". Ultimately, throughout these three articles, it is visible how the intentional risk parameters proposed by Chapela et al. [21] glue together, through Equation (2.3), this doctoral work.

8. Conclusions

These are the main conclusions of this doctoral thesis:

- System of Systems Engineering (SoSE) is a valid tool to increase the understanding of complex "supersystems" or "networks of networks" such as public blockchains. In the case of BTC and ETH, they are the two most revelant holons of the SoS of public blockchains. Public blockchains enable the transfer of digital value, that could potentially be linked to physical value. BTC aspires to become a "digital reserve asset" and ETH an "alternative financial conduit".

- The emergent property of the SoS of public blockchains is to become a distributed alternative to the traditional fiat currency based financial system.

- A key threat to the mass adoption of this SoS is the risk of intentional attacks that aim to extract value out of the SoS.

- Value, accessibility and anonymity, the parameters proposed by Chapela et al. [21] to manage intentional risk, are instrumental to suggest and categorise security measures that can increase the resilience against intentional risk of the SoS of public blockchains.

- The implementation of the suggested security measures impacts positively in the mentioned emergent property of the SoS of public blockchains, i.e., building a real alternative to the fiat currency based financial system.

- Blockchain fulfils some IoT security requirements. The decentralised and immutable nature of the blockchain technology, constructed as a multi-location distributed database, formed by a collection of blocks that register data and are linked together via cryptographic means, is a useful platform to provide IoT solutions with data integrity and redundancy. However, a single blockchain implementation alone cannot answer all IoT security requirements.

- An Identity and Access Management (IAM) framework based on decentralised identifiers (DIDs) and verifiable credentials (VCs) is a useful artefact to create verifiable self-sovereign digital identities on a blockchain and, consequently, to increase resilience against intentional risk.

- BTC and ETH, together with IOTA and IoTeX, display degree distributions that resemble a power law function. This means that transaction networks in these key blockchain (or DAG, in the case of IOTA) implementations contain a small set of highly connected nodes (hubs). The protection of those hubs against targeted attacks increases the resilience of those networks.

- A distributed IAM concept that would protect nodes, especially hubs, would make these blockchains more resilient against intentional risk. This IAM concept transcends a single blockchain. It requires the interplay of edge and global ledgers, that could be implemented on blockchains, running on edge and cloud servers.

- Keeping all worth-protecting value in permissioned blockchains, linked to a distributed IAM framework is an option to increase resilience.

- Visibility graphs, as proposed by Lacasa et al. [73], allow the study of unidimensional time series with the extensive toolkit that complex network theory offers. VGs are instrumental to add the time dimension within a complex network.

- The power law fits of the degree distributions in networks stemming from price volatility VGs of public blockchain implementations with a longer history, such as BTC and ETH, are better than those found in IOTA and IoTeX VGs and HVGs. Additionally, although both IOTA and IoTeX markets are still at early development stages, IoTeX appears to develop faster than IOTA.

- The deployment of 5G, the new mobile technology, can accelerate the development, rollout and adoption of IoT platforms. IOTA and IoTeX, as two relevant IoT platforms based on distributed ledgers, are optimally positioned for it.

- The use of 5G for IoT platforms, e.g., IOTA and IoTeX, can increase intentional risk parameters such as value and accessibility. A suggested intentional risk-based strategy to mitigate this growing risk consists of: first, avoiding the proliferation of rich hubs, i.e., distributing value across platform participants and, second, improving accessibility controls. This is tightly linked to multilayered IAM systems.

- The improvements provided by 5G in mobile data transmission, in areas such as speed, latency and bandwidth, can facilitate the implementation of the suggested intentional risk-based strategy. Ultimately, 5G can improve information security in IoT platforms such as IOTA and IoTeX.

9. Future research

This chapter presents worth exploring research paths that appear out of this doctoral work. Each of them is a plausible candidate to devote resources and effort. They can expand current knowledge in the field of blockchain.

9.1 On facilitating understanding of public blockchains: BTC and ETH

A system of systems (SoS) itself can be an element of a more complex system of systems. Therefore, zooming out, the joint analysis of the SoS of public blockchains and the traditional financial system, which can also be considered a SoS, together with the links between them, is a future research path: the overall SoS of value. Equally, zooming in, the decentralised finance (DeFi) ecosystem can also benefit from being modelled as a SoS. From a more operational perspective, I suggest to create an application programming interface (API) that would implement the security measures suggested in [87] for public blockchains. Finally, the study of the potential application of machine learning (ML) and artificial intelligence (AI) techniques to implement the measures proposed to increase the resilience against intentional risk in public blockcains is also a promising research topic.

9.2 On improving IAM resilience against intentional risk: IOTA and IoTeX

Given the challenge to obtain and process a complete dataset of transactions happening in a blockchain, it is worth exploring the use of visibility graphs, as proposed by Lacasa et al. [73] and Luque et al. [77], to transform the time series of the values of all performed transactions, into a complex network. This proposal would complement the study of the time series of prices, which is included in the second published article for this thesis [85]. Additionally, the role of artificial intelligence (AI) in distributed IAM concepts for blockchain is an innovative research path. Finally, the use of generative adversarial nets (GANs) to optimise proof of stake-based consensus protocols is a future research proposal as well.

9.3 On creating an intentional risk-based strategy: IOTA and IoTeX

The design and implementation of public blockchain explorers with better data search, filter and download possibilities is one future research path. Especially interesting would be the standardisation of blockchain explorer functionalities and the subsequent creation of the corresponding APIs and modules. Should this proposal to improve blockchain explorers succeed, then I would suggest to create the visibility graph for the complete IOTA and IoTeX transaction networks. Finally, I highlight the possibility to perform a similar visibility graph-related research using daily price volatility data from BTC and ETH.

10. Bibliography

[1] Réka Albert and Albert-László Barabási. Statistical mechanics of complex networks. *Rev. Mod. Phys.*, 74:47–97, Jan 2002. `https://link.aps.org/doi/10.1103/RevModPhys.74.47`.

[2] Réka Albert, Hawoong Jeong, and Albert-László Barabási. Error and attack tolerance of complex networks. *Nature*, 406:378–382, 2000. `https://doi.org/10.1038/35019019`.

[3] Jeff Alstott. Toolbox for testing if a probability distribution fits a power law. `https://pypi.org/project/powerlaw/`, 2021-08-18. Published online by pypi.org. Accessed 2022-02-27.

[4] Jeff Alstott, Ed Bullmore, and Dietmar Plenz. powerlaw: a python package for analysis of heavy-tailed distributions. *PloS one*, 9(1):e85777, 2014. `https://doi.org/10.1371/journal.pone.0085777`.

[5] Thomas Aynaud. Community detection for networkx. `https://python-louvain.readthedocs.io/en/latest/api.html`, 2009-10-04. Published online by python-louvain.readthedocs.io. Accessed 2022-02-27.

[6] Thomas Aynaud. Cylouvain: Cython louvain. `https://github.com/ahollocou/cylouvain`, 2018-04-17. Published online by github.com. Accessed 2022-02-27.

[7] Cyrus H. Azani. System of systems architecting via natural development principles. In *2008 IEEE International Conference on System of Systems Engineering*, pages 1–6. IEEE, 2008. `https://doi.org/10.1109/SYSOSE.2008.4724137`.

[8] Albert-László Barabási and Réka Albert. Emergence of scaling in random networks. *science*, 286(5439):509–512, 1999.

[9] Albert-László Barabási. Network science. `http://barabasi.com/book/network-science`, 2014-09-05. Creative Commons: CC BY-NC-SA 2.0. Online. Accessed 2022-03-31.

[10] Maurice Barbieri and Dominik Gassen. Blockchain-can this new technology really revolutionize the land registry system? In *Responsible Land Governance: Towards an Evidence Based Approach: Proceedings of*

the Annual World Bank Conference on Land and Poverty, pages 1–13, 2017. https://www.notariesofeurope.eu/wp-content/uploads/2021/09/Land-and-Poverty-Conference_Blockchain-Presentation.pdf.

[11] Annika Baumann, Benjamin Fabian, and Matthias Lischke. Exploring the Bitcoin network. In *Proceedings of the 10th International Conference on Web Information Systems and Technologies*. Institute of Information Systems, Humboldt University Berlin, 2014. https://doi.org/10.5220/0004937303690374.

[12] Laurent Beauguitte and César Ducruet. Scale-free and small-world networks in geographical research: A critical examination. In *17th European Colloquium on Theoretical and Quantitative Geography. Athènes, Greece*, pages 663–671. HAL-SHS, France, 2011-09-15. https://halshs.archives-ouvertes.fr/halshs-00623927.

[13] Bitcoin BIPs. Bitcoin improvement proposal (BIP). https://github.com/bitcoin/bips#readme. Bitcoin Improvement Proposal (BIP). Online. Accessed 2022-04-13.

[14] Blockchain.com. Bitcoin blockchain explorer. https://www.blockchain.com/explorer, 2020-12-28. Published online by blockchain.com. Accessed 2022-02-18.

[15] Stefano Boccaletti, Vito Latora, Yamir Moreno, Martín Chavez, and D-U. Hwang. Complex networks: Structure and dynamics. *Physics Reports*, 424(4-5):175–308, 2006. https://doi.org/10.1016/j.physrep.2005.10.009.

[16] Elie Bouri, Rangan Gupta, Aviral Kumar Tiwari, and David Roubaud. Does Bitcoin hedge global uncertainty? Evidence from wavelet-based quantile-in-quantile regressions. *Finance Research Letters*, 23:87–95, 2017-11. https://doi.org/10.1016/j.frl.2017.02.009.

[17] Rainer Böhme, Christin Nicolas, Benjamin Edelman, and Tyler Moore. Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, pages 213–38, 2015. https://www.aeaweb.org/articles?id=10.1257/jep.29.2.213. DOI:10.1257/jep.29.2.213.

[18] Miles Carlsten, Harry Kalodner, Arvind Narayanan, and S.Matthew Weinberg. On the instability of Bitcoin without the block reward. In *CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 154–167. ACM New York, NY, USA, 2016-10-24. https://dl.acm.org/doi/10.1145/2976749.2978408.

[19] Christian Catalini and Joshua S. Gans. Some simple economics of the blockchain. *National Bureau of Economic Research Working Paper Series Nr. 22952*, December 2016. http://www.nber.org/papers/w22952.DOI:10.3386/w22952.

[20] Gnosis chain. Welcome to Gnosis chain. Formerly the xDai chain. https://www.xdaichain.com/, 2018-10-12. Online. Accessed 2022-03-31.

[21] Víctor Chapela, Regino Criado, Santiago Moral, and Miguel Romance. *Intentional Risk Management Through Complex Networks Analysis.* Springer briefs in optimization. Springer, 2016. ISBN: 9783319264219.

[22] Usman W Chohan. Non-fungible tokens: Blockchains, scarcity, and value. *Critical Blockchain Research Initiative (CBRI) Working Papers*, 2021. https://dx.doi.org/10.2139/ssrn.3822743.

[23] Coinmarketcap. Today's Cryptocurrency prices by market cap. https://coinmarketcap.com/, 2022-02-01. Published online by Coimarketcap.com. Accessed 2022-02-04.

[24] The SciPy community. Scipy.optimize.curve_fit. https://docs.scipy.org/doc/scipy/reference/generated/scipy.optimize.curve_fit.html, 2008. Published online by scipy.org. Accessed 2022-02-27.

[25] Cryptoslate. IoT Coins. https://cryptoslate.com/cryptos/iot, 2022-02-01. Published online by Cryptoslate.com. Accessed 2022-02-04.

[26] Currency.com. ETH 2.0: What's happened so far and when is the next phase? https://currency.com/eth-2-0-what-s-happened-so-far-and-when-is-the-next-phase, 2022-01-21. Published online by Currency.com. Accessed 2022-02-11.

[27] Luciano da Fontoura Costa, Osvaldo N. Oliveira Jr., Gonzalo Travieso, Francisco Aparecido Rodrigues, Paulino Ribeiro Villas Boas, Lucas Antiqueira, Matheus Palhares Viana, and Luis Enrique Correa Rocha. Analyzing and modeling real-world phenomena with complex networks: a survey of applications. *Advances in Physics*, 60(3):329–412, 2011. https://doi.org/10.1080/00018732.2011.572452.

[28] Peter T. Daniels and William Bright. *The world's writing systems.* Oxford University Press on Demand, 1996.

[29] Professor Glyn Davies and Dr Duncan Connors. *A History of Money.* University of Wales Press, 2016.

[30] Francesco De Collibus, Alberto Partida, and Claudio Tessone. Heterogeneous preferential attachment in Ether and key Ethereum-based tokens. https://complenetlive21.weebly.com/program.html, 2021-05-24,25,26. Published online by CompleNet Live 2021. Accessed 2022-02-07. Conference info at https://complenetlive21.weebly.com/.

[31] Francesco Maria De Collibus, Alberto Partida, and Matija Piškorec. The role of smart contracts in the transaction networks of four key DeFi-collateral

Ethereum-based tokens. In Rosa Maria Benito, Chantal Cherifi, Hocine Cherifi, Esteban Moro, Luis M. Rocha, and Marta Sales-Pardo, editors, *Complex Networks & Their Applications X*, pages 792–804, Cham, 2022. Springer International Publishing. https://doi.org/10.1007/978-3-030-93409-5_65.

[32] Francesco Maria De Collibus, Alberto Partida, Matija Piškorec, and Claudio J. Tessone. Heterogeneous preferential attachment in key Ethereum-based cryptoassets. *Frontiers in Physics*, 9, 2021. https://doi.org/10.3389/fphy.2021.720708.

[33] ECB. Distributed ledger technology. In Focus. Issue 1, 2016. https://www.ecb.europa.eu/paym/pdf/infocus/20160422_infocus_dlt.pdf. Online. Accessed 2022-03-30.

[34] Florian Eggenberger and George Pólya. Über die statistik verketteter vorgänge. *ZAMM-Journal of Applied Mathematics and Mechanics/Zeitschrift für Angewandte Mathematik und Mechanik*, 3(4):279–289, 1923.

[35] Ethereum EIPs. Ethereum improvement proposal (EIP). https://github.com/ethereum/eips/issues. Ethereum Improvement Proposal (EIP). Online. Accessed 2022-04-13.

[36] Paul Erdős and Alfréd Rényi. On the evolution of random graphs. *Publ. Math. Debrecen*, 6:290–297, 1959.

[37] ESMA. The distributed ledger technology applied to securities markets. Working paper no. 2016/773, 2016-06-02. https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf. Online. Accessed 2022-03-30.

[38] Ethereum. Ethereum community. Ethereum Homestead documentation. Working paper. https://ethdocs.org/en/latest/#, 2016-03-14. Online. Accessed 2022-03-31.

[39] Ethereum. Ethereum Wiki. Ethereum white paper. A next-generation smart contract and decentralized application platform, 2016-04-13. http://github.com/ethereum/wiki/wiki/White-Paper. Published online by github.com. Accessed 2022-03-30.

[40] Etherscan.io. The ethereum blockchain explorer. https://etherscan.io/, 2020-12-28. Published online by etherscan.io. Accessed 2022-02-18.

[41] Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, and Robert Van Renesse. Bitcoin-NG: A scalable blockchain protocol. In *Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI '16)*. USENIX, 2016. https://www.usenix.org/system/files/conference/nsdi16/nsdi16-paper-eyal.pdf. DOI: 10.5220/0004937303690374.

[42] Xinxin Fan, Qi Chai, Zhefeng Li, and Tian Pan. Decentralized IoT data authorization with Pebble tracker. In *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, pages 1–2. IEEE, 2020. `https://doi.org/10.1109/WF-IoT48130.2020.9221130`.

[43] Tiago M Fernández-Caramés and Paula Fraga-Lamas. A review on the use of blockchain for the Internet of Things. *IEEE Access*, 6:32979–33001, 2018. `https://doi.org/10.1109/ACCESS.2018.2842685`.

[44] Stefano Ferretti and Gabriele D'Angelo. On the Ethereum blockchain structure: A complex networks theory perspective. *Concurrency and Computation: Practice and Experience*, 32(12), August 2019. `https://doi.org/10.1002/cpe.5493`.

[45] Cambridge Center for Alternative Finance. Bitcoin mining map. `https://ccaf.io/cbeci/mining_map`, 2020-12-28. Cambridge Center for Alternative Finance. Accessed 2022-04-10.

[46] Rodrigo Garcia. Visibility-graph 0.4.1. `https://pypi.org/project/visibility-graph/`, 2021-02-02. Published online by pypi.org. Accessed 2022-02-27.

[47] Alex Gorod, Brian Sauser, and John Boardman. System-of-systems engineering management: A review of modern history and a path forward. *IEEE Systems Journal*, 2(4):484–499, 2008. `https://doi.org/10.1109/JSYST.2008.2007163`.

[48] Yuval Noah Harari. *Sapiens: A brief history of humankind*. Random House, 2014.

[49] Taylor Hardin and David Kotz. Blockchain in health data systems: A survey. In *2019 sixth international conference on Internet of Things: Systems, management and security (IOTSMS)*, pages 490–497. IEEE, 2019. `https://doi.org/10.1109/IOTSMS48152.2019.8939174`.

[50] Bálint Hartmann and Viktória Sugár. Searching for small-world and scale-free behaviour in long-term historical data of a real-world power grid. *Scientific Reports*, 11(1):1–10, 2021.

[51] Tharaka Mawanane Hewa, Anshuman Kalla, Avishek Nag, Mika E Ylianttila, and Madhusanka Liyanage. Blockchain for 5G and IoT: Opportunities and challenges. In *2020 IEEE Eighth International Conference on Communications and Networking (ComNet)*, pages 1–8. IEEE, 2020. `https://doi.org/10.1109/ComNet47917.2020.9306082`.

[52] Garrick Hileman. State of Blockchain Q1 2016: Blockchain funding overtakes Bitcoin, 2016-05-11. `http://www.coindesk.com/state-of-blockchain-q1-2016/`. Online. Accessed 2022-03-31.

[53] Nicolas Houy. The Bitcoin mining game. *Ledger - ledgerjournal.org*, pages 53–68, 2016. https://doi.org/10.5195/ledger.2016.13.

[54] Javier W. Ibáñez and Salvatore Moccia. Designing the architecture of a blockchain platform: The case of Alastria, a national public permissioned blockchain. *International Journal of Enterprise Information Systems (IJEIS)*, 16(3):34–48, 2020. https://doi.org/10.4018/IJEIS.2020070103.

[55] Infura.io. Ethereum api. https://infura.io/, 2020-12-28. Published online by infura.io. Accessed 2022-02-18.

[56] Satoshi Nakamoto Institute. Bitcoin P2P e-cash paper. http://satoshi.nakamotoinstitute.org/emails/cryptography/2/#selection-71.17-71.70, 2008-11-03. Published online by Satoshi Nakamoto Institute. Accessed 2022-03-31.

[57] Investing.com. Internet-based financial news and stock market data provider. https://www.investing.com/, 2022-02-26. Online. Accessed 2022-02-26.

[58] Investing.com. Bitcoin historical data - investing.com. btc/usd. https://www.investing.com/crypto/bitcoin, 2022-04-01. Online. Accessed 2022-04-01.

[59] Investing.com. Ethereum historical data - investing.com, eth/usd. https://www.investing.com/crypto/ethereum, 2022-04-01. Online. Accessed 2022-04-01.

[60] Investing.com. Iota historical data - investing.com. iot/usd. https://www.investing.com/crypto/iota, 2022-04-01. Online. Accessed 2022-04-01.

[61] Investing.com. Iotex historical data. iotx/usd. https://www.investing.com/indices/investing.com-iotx-usd, 2022-04-01. Online. Accessed 2022-04-01.

[62] Investopedia.com. Uncle block (cryptocurrency). https://www.investopedia.com/terms/u/uncle-block-cryptocurrency.asp, 2022-01-21. Published online by Investopedia.com. Accessed 2022-02-11.

[63] IOTA.org. IOTA. Get started. https://www.iota.org/get-started/what-is-iota, 2016-07-11. IOTA intro pages. Online. Accessed 2022-03-31.

[64] IOTA.org. IOTA blockchain explorer. https://explorer.iota.org/mainnet, 2020-12-28. Published online by iota.org. Accessed 2022-02-18.

[65] IoTeX.io. IoTeX. Building the connected world. https://iotex.io/, 2022-02-15. IoTeX. Project presentation. Online. Accessed 2022-02-15.

[66] Iotexscan.io. IoTeX blockchain explorer. `https://iotexscan.io/`, 2020-12-28. Published online by iotexscan.io. Accessed 2022-02-18.

[67] Mo Jamshidi. System of systems engineering. new challenges for the 21st century. *IEEE Aerospace and Electronic Systems Magazine*, 23(5):4–19, 2008.

[68] Mohammad Jamshidi and Andrew P Sage. *System of systems engineering: innovations for the 21st century*, volume 58. John Wiley & Sons Incorporated, 2009.

[69] Marco Alberto Javarone and Craig Steven Wright. From Bitcoin to Bitcoin cash: a network analysis. In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, pages 77–81, 2018. `https://doi.org/10.1145/3211933.3211947`.

[70] Barbara J. Jennings, Eric D. Vugrin, and Deborah K Belasich. Resilience certification for commercial buildings: a study of stakeholder perspectives. *Environment Systems and Decisions*, 33(2):184–194, 2013.

[71] Song-Kyoo Kim, Chan Yeob Yeun, Ernesto Damiani, Yousef Al-Hammadi, and Nai-Wei Lo. New blockchain adoptation for automotive security by using systematic innovation. In *2019 IEEE Transportation Electrification Conference and Expo, Asia-Pacific (ITEC Asia-Pacific)*, pages 1–4. IEEE, 2019. `https://doi.org/10.1109/ITEC-AP.2019.8903646`.

[72] Alex Koohang, Carol Springer Sargent, Jeretta Horn Nord, and Joanna Paliszkiewicz. Internet of things (IoT): From awareness to continued use. *International Journal of Information Management*, 62:102442, 2022. `https://doi.org/10.1016/j.ijinfomgt.2021.102442`.

[73] Lucas Lacasa, Bartolo Luque, Fernando Ballesteros, Jordi Luque, and Juan Carlos Nuno. From time series to complex networks: The visibility graph. *Proceedings of the National Academy of Sciences*, 105(13):4972–4975, 2008. `https://doi.org/10.1073/pnas.0709247105`.

[74] Anthony Lewis. A gentle introduction to blockchain technology, 2015-09-09. `http://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology`. Online. Accessed 2022-03-31.

[75] Jiaqi Liang, Linjing Li, and Daniel Zeng. Evolutionary dynamics of cryptocurrency transaction networks: An empirical study. *PloS one*, 13(8):e0202202, 2018. `https://doi.org/10.1371/journal.pone.0202202`.

[76] Keshi Liu, Tongfeng Weng, Changgui Gu, and Huijie Yang. Visibility graph analysis of Bitcoin price series. *Physica A: Statistical Mechanics and its Applications*, 538:122952, 2020. `https://doi.org/10.1016/j.physa.2019.122952`.

[77] Bartolo Luque, Lucas Lacasa, Fernando Ballesteros, and Jordi Luque. Horizontal visibility graphs: Exact results for random time series. *Physical Review E*, 80(4):046103, 2009. `https://doi.org/10.1103/PhysRevE.80.046103`.

[78] McKinsey and Company. Blockchain technology in the insurance sector, 2017-01-05. `https://www.treasury.gov/initiatives/fio/Documents/McKinsey_FACI_Blockchain_in_Insurance.pdf`. Online. Accessed 2022-03-31.

[79] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. `https://bitcoin.org/bitcoin.pdf`, 2008-10-15. Published online by Nakamotoinstitute.org. Accessed 2022-03-31.

[80] Networkx.org. Network analysis in python. `https://networkx.org/`, 2022-02-23. Published online by networkx.org. Accessed 2022-02-23.

[81] M. E. J. Newman. The structure and function of complex networks. *SIAM Review*, 45(2):167–256, 2003. `https://epubs.siam.org/doi/10.1137/S003614450342480`.

[82] Alberto Partida and Diego Andina. *IT Security Management: IT Securiteers. Setting up an IT Security function*, volume 61. Springer Science & Business Media, 2010.

[83] Alberto Partida, Regino Criado, and Miguel Romance. A simulation of a Bitcoin blockchain based on a pseudo-randomly selected block. `https://tv.urjc.es/video/5b22826ad68b14cc798b45c6`, 2018-06-04. Published online by urjc.es. Accessed 2022-02-07. Conference info at `https://eventos.urjc.es/9662/accepted_abstracts/15th-experimental-chaos-and-complexity-conference.html`.

[84] Alberto Partida, Regino Criado, and Miguel Romance. On Identity Management in blockchain implementations. `https://www.manifestingintelligence.com/posters`, 2020-06-15. Published online by manifestingintelligence.com. Accessed 2022-02-07. Conference info at `https://www.manifestingintelligence.com/home1`.

[85] Alberto Partida, Regino Criado, and Miguel Romance. Identity and access management resilience against intentional risk for blockchain-based IoT platforms. *Electronics*, 10(4), 2021. `https://doi.org/10.3390/electronics10040378`.

[86] Alberto Partida, Regino Criado, and Miguel Romance. Visibility graph analysis of IOTA and IoTeX price series: An intentional risk-based strategy to use 5G for IoT. *Electronics*, 10(18), 2021. `https://doi.org/10.3390/electronics10182282`.

[87] Alberto Partida, Saki Gerassis, Regino Criado, Miguel Romance, Eduardo Giráldez, and Javier Taboada. Modeling Bitcoin plus Ethereum as an open System of Systems of public blockchains to improve their resilience against intentional risk. *Electronics*, 11(2), 2022. https://doi.org/10.3390/electronics11020241.

[88] Supun Perera, Michael GH Bell, and Michiel CJ Bliemer. Network science approach to modelling the topology and robustness of supply chain networks: a review and perspective. *Applied network science*, 2(1):1–25, 2017. https://doi.org/10.1007/s41109-017-0053-0.

[89] Andrea Pinna and Wiebe Ruttenberg. Distributed ledger technologies in securities post-trading: revolution or evolution. ECB occasional paper series 172, 2016-04-20. https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf. Online. Accessed 2022-03-31.

[90] Polygon. Bringing the world to Ethereum. https://polygon.technology/, 2017-10-12. Online. Accessed 2022-03-31.

[91] A. M. Turing. On computable numbers, with an application to the Entscheidungsproblem, 1936-11. http://www.cs.virginia.edu/~robins/Turing_Paper_1936.pdf.

[92] Fergal Reid and Martin Harrigan. An analysis of anonymity in the Bitcoin system. In *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*, pages 1318–1326, 2011. https://doi.ieeecomputersociety.org/10.1109/PASSAT/SocialCom.2011.79.

[93] Fergal Reid and Martin Harrigan. *An Analysis of Anonymity in the Bitcoin System*, pages 197–223. Security and Privacy in Social Networks. Springer, New York, NY, 7 July 2012. https://doi.org/10.1007/978-1-4614-4139-7_10.

[94] John McLevey Reid McIlroy-Young. metaknowledge 3.4.1. https://pypi.org/project/metaknowledge, 2020-11-03. Published online by pypi.org. Accessed 2022-02-27.

[95] Peter R. Rizun. Subchains: A technique to scale Bitcoin and improve the user experience. *Ledger - ledgerjournal.org*, pages 38–52, 2016. https://doi.org/10.5195/ledger.2016.40.

[96] Tariq Samad, Thomas Parisini, and AM Annaswamy. Systems of systems. *The Impact of Control Technology*, 12(1):175–183, 2011. http://ieeecss.org/sites/ieeecss/files/2019-07/IoCT-Part3-04SystemsOfSystems.pdf. No DOI available.

[97] Silvia Semenzin and Alessandro Gandini. Automating trust with the blockchain? A critical investigation of “blockchain 2.0” cultures. *Global Perspectives*, 2(1):24912, 2021. https://doi.org/10.1525/gp.2021.24912.

[98] Alan T Sherman, Farid Javani, Haibin Zhang, and Enis Golaszewski. On the origins and variations of blockchain technologies. *IEEE Security & Privacy*, 17(1):72–77, 2019. https://doi.org/10.1109/msec.2019.2893730.

[99] Chaoming Song, Shlomo Havlin, and Hernán A. Makse. Self-similarity of complex networks. *Nature*, 433(7024):392–395, 2005. https://doi.org/10.1038/nature03248.

[100] Chaoming Song, Shlomo Havlin, and Hernán A. Makse. Origins of fractality in the growth of complex networks. *Nature physics*, 2(4):275–281, 2006. https://doi.org/10.1038/nphys266.

[101] Statista. Global digital population as of January 2021. https://www.statista.com/statistics/617136/digital-population-worldwide/, 2022-02-15. How many people use the Internet? Online. Accessed 2022-02-15.

[102] Statista. Worldwide spending on blockchain solutions from 2017 to 2024. https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/, 2022-03-07. Worldwide spending on blockchain solutions from 2017 to 2024. Online. Accessed 2022-03-07.

[103] Dominik Stroukal and Barbora Nedvedova. Bitcoin and other cryptocurrency as an instrument of crime in cyberspace. In *Proceedings of the 4th Business & Management Conference, Istanbul*, 2016-10-12. http://econpapers.repec.org/paper/sekibmpro/4407036.htm. DOI: 10.20472/BMC.2016.004.018. ISBN:978-80-87927-30-4.

[104] Nassim Nicholas Taleb. *Antifragile: Things that gain from disorder.* Penguin, 2013. London. ISBN: 0141038225.

[105] Ian De Terte and Christine Stephens. *Psychological resilience of workers in high-risk occupations.* John Wiley & Sons, 2014.

[106] Visualcapitalist. After China’s Crypto ban, who leads in Bitcoin mining? https://www.visualcapitalist.com/after-chinas-crypto-ban-who-leads-in-bitcoin-mining/, 2022-02-01. Published online by Visualcapitalist.com. Accessed 2022-02-11.

[107] Marko Vukolić. *The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication*, pages 112–125. International Workshop on Open Problems in Network Security. iNetSec 2015. Lecture Notes in Computer Science, vol 9591. Camenisch J., Kesdoğan D. (eds). Springer, Cham., 1 May 2016. https://doi.org/10.1007/978-3-319-39028-4_9.

[108] W3C. Decentralized identifiers (DIDs) v1.0. `https://www.w3.org/TR/did-core/`, 2022-02-14. W3C Proposed Recommendation 03 August 2021. Online. Accessed 2022-02-14.

[109] W3C. Verifiable credentials data model v1.1. `https://www.w3.org/TR/vc-data-model/`, 2022-02-14. W3C Recommendation 09 November 2021. Online. Accessed 2022-02-14.

[110] Mark Walport. Distributed ledger technology: Beyond block chain. `https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf`, 2015-12-15. Online. Accessed 2022-03-31.

[111] Duncan J. Watts and Steven H. Strogatz. Collective dynamics of ‘small-world’ networks. *nature*, 393(6684):440–442, 1998.

[112] Jan Hendrik Witte. The blockchain: A gentle four page introduction, 2016-12-06. `https://arxiv.org/abs/1612.06244`. Online. Accessed 2022-03-31.

[113] Lei Xu, Lin Chen, Zhimin Gao, Xinxin Fan, Taeweon Suh, and Weidong Shi. Diota: Decentralized-ledger-based framework for data authenticity protection in iot systems. *IEEE Network*, 34(1):38–46, 2020. `https://doi.org/10.1109/MNET.001.1900136`.

[114] Delia Fano Yela. visibility_algorithms.py. `https://github.com/delialia/bst/blob/master/visibility_algorithms.py`, 2019-05-08. Published online by github.com. Accessed 2022-02-27.

[115] yjjnls@baidu. Awesome blockchain. `https://github.com/yjjnls/awesome-blockchain`, 2022-02-01. Published online by github.com. Accessed 2022-02-10.

[116] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. Where is current research on blockchain technology? A systematic review. *PLoS ONE*, 11(10), 2016-10-03. `https://doi.org/10.1371/journal.pone.0163477`.

[117] Heejung Yu, Howon Lee, and Hongbeom Jeon. What is 5G? Emerging 5G mobile services and network requirements. *Sustainability*, 9(10):1848, 2017. `https://doi.org/10.3390/su9101848`.

A. Blockchain and information security

A.1 Complex network features in long-standing blockchains

The following is a brief portrayal, based on Liang et al. [75] and Javarone et al. [69], of the main complex network characteristics present in the transaction networks of pioneering public blockchain implementations such as BTC and ETH:

- Densification law is not followed.
- Constant average degree assumption is not valid.
- A user is represented by many nodes, i.e., as many as transaction addresses they have.
- The lifetime of many nodes is ephemeral, as most addresses are not reused.
- Exceptionally, some nodes survive almost permanently given their function of public recipients or initiators of transactions, e.g. those used by NGOs to receive funds [92].
- The degree distribution follows a heavy-tailed distribution with a majority of nodes having low degrees and a small but not negligible number of nodes (addresses) having relatively high degrees.
- The out-degree distribution might be fitted by a power law.
- Transaction networks are disassortative, i.e., high degree nodes tend to connect with low degree nodes.
- The small-world network effect is not demonstrated. However, a largest connected component is present.

A.2 Information security design patterns for blockchain

An analysis of security incidents affecting blockchain implementations, performed to write the article on IAM resilience in IoT platforms [85], gives origin to a collection of information security design patterns and good practices for blockchain implementations, proposed in the following subsections.

A.2.1 A multi-layered approach

The construction of security properties in each of the layers connected with the transaction network, such as hardware, firmware, operating systems, middleware and distributed apps, contributes to increasing the overall level of security in a blockchain network. By contrast, the absence of security properties in each of the layers composing any information system contributes to the possibility to extract value fraudulently out of it.

A.2.2 De-constructing anonymity

Anonymity does not contribute to increasing information security. Anonymity increases the attractiveness for attackers to target blockchain implementations. Blockchain, as a powerful tool to move digital value, requires a reliable identity management component, especially in their interfaces with the physical world. Blockchain users have a unique identity in the physical world and, potentially, a set of digital identities. Section B.2.4 in Appendix B suggests a dual digital identity scheme that aspires to answer the challenge of finding the right balance between security and personal data privacy.

A.2.3 Human readable node addresses

As the incidents described in article 2 of this thesis show [85], see its title in Table 1.3, a blockchain implementation can be impacted if an entity, via a traditional web defacement, simply modifies the off-chain announcement of the address of a node that is expected to receive funds via multiple transactions. There have been multiple security incidents in which funds did not reach intended nodes as attackers smartly modified the Internet website announcing the address of the node, inserting a different address that they control. A possible way to mitigate this simple attack is the construction of an immutable and public one-to-one association between a node address and a human readable and verifiable identity. This could be implemented as a multi-layer network composed by two different layers, the transaction network and the identity network. The identity network will play a pivotal role in the security of the blockchain implementation. Similarly to a secure domain name service, it will provide identity traceability in every transaction. This identity service will be essential to create a secure blockchain implementation.

A.2.4 Security audits in on-chain code

Some blockchain implementations allow the execution of code in their nodes. This is the case of smart contracts in Ethereum. Those pieces of code need to audited, security verified and tested by different stakeholders within the network before going live. These audits should also check the way the code interacts with identities in the network. The governance, automation and distribution of these suggested code audits is a research field with a high degree of business potential.

A.2.5 Basic blockchain transaction monitoring practices

An idea worth exploring is monitoring blockchain security based on changes on degree distributions. For example, a basic event to detect would be the shift in a blockchain transaction network from being disassortative to showing recent assortative features. This event could hint that the network has been compromised and value is being quickly extracted out of the network, e.g., a high degree node starts transacting with other high degree nodes. This could potentially mean that one of those hubs is collecting value to subsequently channel it via an interface to a different network. A second example of a worth-monitoring event could be a sudden increase in the value held by a low degree node. In general, the suggestion will be to facilitate a swift incident detection with a set of indicators of compromise (IOC) based on sudden changes in the complex network parameters, such as node degree and node value, present in every blockchain implementation.

A.3 Blockchain investment questionnaire

A.3.1 Basic guidance to technologists and investors

Investment in blockchain grows year on year [102]. Already in 2016, as mentioned in Section 2.1.6, blockchain funding surpassed BTC funding. The decentralised nature of blockchain, together with its data immutability, makes this technology a promising platform to use in very different industries, as Appendix B puts forward. The following brief questionnaire could help investors building an initial coarse-grained "business card" for each blockchain-based project that they need to quickly assess before going deeper in the analysis required for investing.

- Analysis of the business process that this blokchain will answer. What is the added value expected to be provided by this blockchain?
- Number of entities participating in the blockchain and growth rate. Potential user population.
- Governance around the identity of every participant.
- Degree of openness. Will it be a permissioned or a permissionless blockchain?
- Lifetime value for every blockchain participant.

- Technology choices. Transaction speed. Will it escalate with a higher number of users?
- Possibility to apply security patterns such as the ones proposed in Section A.2.
- Development and operational resources available.
- Interfaces with related digital and physical environments.
- Political, economic, social, technology, legal and environmental analysis.

B. A blockchain proposal to answer five key use cases: Socioblock

B.1 A blockchain that contributes to a decentralised society

This appendix presents Socioblock, a blockchain project that answers five use cases: self-sovereign identities, ad-hoc insurance, self-sovereign medical records, exchange of academic records and mortgage search. The underlying technology for these five examples is a public blockchain. On top of it, decentralised applications (DApp) implement each use case. DApps run on top of a blockchain and they are based on smart contracts. This appendix serves as the high-level blueprint of Socioblock. This blockchain project inherits the learning points collected throughout this doctoral thesis with regard to resilience against intentional risk in blockchain implementations. Additionally, Socioblock also benefits from decades of experience regarding digital certificate management in public key infrastructures (PKI).

B.1.1 A key foundation: data ownership and sovereignty

Blockchain can implement the basic principle that data ownership resides on the originator of the data. Privacy legislation, such as the General Data Protection Regulation (GDPR) in the EU, aims to protect the real data owner from corporations that store and use their data. Currently, most personal data are centralised in databases owned by those big corporations and not by the originator. This data centralisation makes the implementation of GDPR dependant only on the initiative of those companies. In this proposed blockchain implementation, called Socioblock, the real owner of the data, i.e., the originator, keeps control of their data at any time. The mechanism to exert this control is simple. The data owner decides which data is shared with the different ecosystem participants.

B.1.2 A channel-enabled layer-based architecture

On top of a layer-1 blockchain such as Ethereum, there are multiple DApps that create their own layer-2 blockchains, such as Polygon [90] and xDAI [20]. Every DApp has a unique contract identifier that is included in every transaction. Socioblock implements a layer-based architecture similar to Ethereum. The underlying layer in Socioblock consists of a layer-1 public blockchain that receives services from a distributed identity provider as explained in Appendix A.2.2. This layer-1 blockchain implementation caters for the creation of different channels. Channels provide a secure way, using cryptographic means, to exchange data among subsets of participants without the rest of participants being able to read the data. The Quorum implementation in Alastria is an example [54]. On top of Socioblock, similarly to the way a Lego construction is assembled, DApps interact between them or just remain isolated, depending on the use case that they implement.

B.1.3 In-chain vs. off-chain

A usual source of confusion is the belief that a blockchain should not only register transactions, i.e., value exchanges, but also store data as if it were a traditional relational database. There are services in this blockchain that do not require any additional database to function, e.g., changes of ownership in value. This way, the blockchain is able to confirm the ownership of an asset by itself without the participation of any off-chain element. However, context data pertaining to transactions is stored off-chain due to their volume and only a reference to that data resides in-chain. While in-chain data is available to all participants, off-chain data is stored in traditional databases and it is only available via off-chain means on a "business need to know" basis. Most use cases implemented on a blockchain require both in-chain elements as well as off-chain data processing and storage. For instance, decentralised applications (DApps) require in-chain, i.e., smart contracts, and off-chain, i.e., traditional databases, capabilities.

B.2 Self-sovereign identities

The first building block in this blockchain implementation is the identity management component, a challenging element as presented in Section A.2.2 of Appendix A. This component acts as the guarantor of each participant's identity. This implies that this blockchain implementation needs to be permissioned. The identity of every ecosystem participant, be it a service provider or a service customer, needs to be confirmed. This is what Public Key Infrastructures (PKI) do with the identity of their users. Certificate Authorities (CA), since the 1990s, have collected a wealth of experience in issuing digital certificates that link a digital identity to a physical entity. A nationwide example is the PKI deployed by the Fábrica Nacional de Moneda y Timbre (FNMT) in Spain. Citizens can use FNMT certificates to interact with their national administration digitally. A more recent European example is the PKI deployed in 2020 with root CAs in all EU countries is the digital Covid certificate scheme. The issuance of a personal digital certificate only takes place after successful verification of the physical identity of the participant. Going towards a permissioned public blockchain is a key design decision and it contrasts with all public blockchain implementations studied in this thesis, which are permissionless.

B.2.1 Encryption

PKIs use cryptography to link digital with physical identities. Every entity owns an asymmetric key pair composed of a public key, published to be known by every participant, and a private key, that is kept confidential. Both keys maintain a one to one relationship. A digital certificate associates a public key to an identity. Information is usually encrypted via symmetric key encryption, much faster in processing than the asymmetric one. The information sender encrypts with the recipient's public key the symmetric key for that specific communications and sends it to the recipient. This way, only the holder of the corresponding private key, i.e., the recipient, can decrypt the symmetric key and decipher the sent data. Alternatively, if the goal is to guarantee integrity and not confidentiality, then the sender of the data signs their message using their private key and everyone with access to the sender's public key can attest the sender's identity. This decades-long used mechanism is not exclusive to blockchain implementations, however blockchain can benefit as well from this effective way to link brick and mortar identities with digital constructs. There is one initial requirement to observe: new developments in computing speed threat the unbreakability of the current encryption algorithms. Therefore, the implementation of cryptography in the blockchain should be modular: it should cater for a change in algorithms should the current ones be vulnerable, e.g., to quantum computing-based cryptoanalysis.

B.2.2 A decentralised PKI within a blockchain

Every Socioblock participant owns a unique identity. This identity is confirmed by a set of authorised CAs, aided by a set of registration authorities (RAs), as it happens in a public key infrastructure (PKI). Socioblock is a public but permissioned blockchain, i.e., everyone can join but each participant is unequivocally identified. Suggested use cases require a confirmed physical identity for each participant. Neither pseudo-anonymous nor anonymous users are allowed in the system.

B.2.3 The network of identity certification authorities

A set of nodes performs the identity confirmation function. Following the segregation of duties principle, these nodes cannot play additional services in the system. Identity, as the fundamental link between the digital and the physical world, is the cornerstone of all Socioblock use cases. The suggestion is to use CAs that are already established in the non-blockchain certificate management ecosystem. To avoid centralisation, there is a network of CAs, all cleared to issue digital certificates. Every Socioblock user obtains a digital certificate either physically visiting a local government or law enforcement facility or through an approved digital *know your customer* process. The network of CAs keeps a database off-chain, redundantly located, of all issued digital certificates. The network of CAs confirms validity of public keys upon request and they perform typical certificate renewal and revocation processes.

B.2.4 A dual digital identity scheme

There is a novel element in Socioblock, not contemplated in current non-blockchain-related PKIs: CAs issue two non-related certificates, each of them linked to a different identity:

- The digital identity that reflects their physical identity, e.g., first name and family name plus national ID number. This certificate could have additional fields. The owner of the certificate decides, at all times, what to share with whom.

- Additionally, a proxy digital identity label, consisting of a string of alpha-numeric characters, e.g. 12, that would act as their identity proxy for some blockchain transactions. Any user could have multiple randomised digital identities at any time. These "proxy identities" preserve the participant's privacy in specific use cases. Socioblock participants have the possibility to change their proxy digital identity label at any time using any of the ways described in Section B.2.3. This corresponds to a partial exercise of the right to be digitally forgotten. Only authorised CAs keep the mapping table between proxy digital identities and physical identities. This table is stored redundantly but off-chain.

This dual digital identity scheme improves personal data privacy and digital identity self-sovereignty. The participants in the system, when approaching different services, decide whether and when they will reveal their real identity to the service provider. This is not possible in most of the current Internet services: corporations collect a vast amount of personal data even if they do not really need it for their unique value proposition. Socioblock participants can use their proxy digital identity for basic services. More complex services, e.g., banking solutions, bound to comply with *know your customer* regulations, require a certificate linked to the physical identity of the customer but only on a real "need to know" basis. Initial prospective queries from customers could be performed using proxy digital identities.

B.2.5 Identity of service providers

The legal identity of companies participating in Socioblock needs to be anchored to a digital certificate and confirmed by the corresponding CA. These companies are already registered with a national tax authority. Subsequently, a legal representative requests a digital certificate to any authorised CA for the digital identity that reflects their physical identity. Service providers in Socioblock do not use a proxy digital identity.

B.2.6 Communication between identities

Communication between Socioblock participants requires that they can identify each other first. Their certificates facilitate this process. For first-time communications, the network of CAs and RAs, presented in Section B.2.2, provides a yellow-page service. Communication between participants could be between "real digital" and "digital proxy" identities. In any of these cases, communication can be encrypted, preserving end-to-end confidentiality. A strong security requirement for the network of CAs associated to the Socioblock ecosystem is to keep the integrity and confidentiality of all their root keys.

B.2.7 Open challenges

This is a high-level blueprint for a public and permissioned blockchain implementation. Several design questions remain unanswered. They require further research. I identify three main open challenges:

- Certificate management practices in a decentralised environment such as blockchain.
- Governance of a network of CAs and RAs providing their services within a blockchain ecosystem.
- Guaranteeing certificate management services availability in a blockchain implementation.

B.3 Ad-hoc insurance

The objective of this case study is to provide a blockchain-based time-based insurance scheme for physical purchases in the luxury market, e.g., a pair of highly-priced, branded sunglasses.

B.3.1 Tokenisation of a physical item

Each pair of branded sunglasses has a unique code attached to it. That code is engraved on the sunglasses' frame or physically associated to it using any other means. Each good is represented, i.e., tokenised in the blockchain. The legal company producing or distributing the good signs this token. The signed token contains the engraved code. The token acts as a lifetime digital tracker for the good. It includes ownership data: from the moment of its inception to its decommissioning. Ownership in a token is signalled by a digital signature, from the seller, of a digital file composed of the token itself and the public key of the buyer. This ownership signal can be applied recursively. Digital tokenisation is currently helping luxury brands to fight against counterfeiting.

B.3.2 Insurance acquisition

The added value of this blockchain-based insurance service is that it is fully automated and decentralised. The digital token of a good can contain smart contracts. In this case, the token includes a smart contract that contacts an insurance provider with the details of the good to ensure. This piece of code could be executed after every ownership change happening to the token. The buyer is offered the possibility to insure the good for a specific period of time and a fee. If the customer agrees, a payment from the customer's on-chain wallet to the insurer takes place. Right after that, the smart contract includes in the token the insurance details and additional contracts that would be called in case of a claim.

B.3.3 Insurance claim

During the validity period of the insurance, the insured customer can make a claim via an insurance application that interacts with the related smart contract present in the token, added when the insurance was acquired. This insurance application reads the details of the insurance from the tokenised good and process the claim. Additional steps could also be coded, e.g., the insurer could engage a surveyor service that, based on pictures, would evaluate the damage and foreseen cost of repair.

B.4 Self-sovereign medical records

This use case implements, using a blockchain, the right of every patient to own their medical records and to decide who has access to them. Currently medical providers create and store medical records of their patients in different repositories. An alternative to this is the creation of a unique medical history for every patient that would accompany them throughout their lifetime regardless of the medical providers that they would use. A self-sovereign lifetime medical record can be implemented as a collection of digital certificates that contain the medical lifetime history of a Socioblock participant. The data immutability and decentralisation that blockchain provides makes it an appropriate vehicle to transport those health-related certificates between patients and health providers.

B.4.1 Medical providers

Hospitals, clinics and any health provider with diagnostic capabilities are able to join Socioblock and its respective health-related channels. The following is a high level description of how records could be used and secured:

From the health provider to the patient:

- The health provider digitally encrypts each medical record that they produce with the corresponding public key of the patient and signs it with the health provider's private key to guarantee its authenticity.
- The patient adds this medical record to their list of medical records. As this list is encrypted with the patient's digital identity's public key, only the patient is able to decrypt it. For every new record that the patient receives, their list of medical records will grow.

From the patient to the health provider:

- The patient also signs a note of receipt with their private key to signal acceptance and ownership. This signed note goes back to the medical provider.

- The patient decides whether the medical records that remain in the centralised database of a medical service provider will be linked to the identity of the patient or whether they are the only custodians of such information. This information is present in the note of receipt mentioned in the previous step. If the patient decides to detach the record from their identity, then the health provider will keep the medical report but with no reference to any patient's identity.

- The patient decides which sections of that lifetime history shares with which providers via the blockchain by decrypting only the items they would like to share with a medical provider.

- The patient finally encrypts the medical record with the public key of the medical provider that is about to receive the record via the blockchain.

B.4.2 Ownership of medical records

This proposal guarantees that patients own their medical records. Patients can request to the medical provider the deletion of the link of the medical record with their identity. This way, medical providers can count on the information provided by that record for research purposes, but the record itself is not linked to the patient's identity. The added value of this proposal is that it can be fully automated using code in blockchain-enabled DApps. A pre-requisite for this proposal is the standardisation of the process to create and sign medical records and the participation of medical providers in this blockchain implementation.

B.5 Academic records

Blockchain can not only contribute to fight against luxury goods counterfeiting, but it can also help sharing the authenticity of academic degrees. In this case, the suggestion is to link an academic degree to a digital certificate and to use blockchain as a public communication channel.

B.5.1 Attestation process

Every student participating in this blockchain use case receives their academic results via a digital certificate. The educational institution signs digitally the degree to guarantee its authenticity, using their private signing key, similarly to what Section B.4.1 describes for medical records. The integrity of every digitally signed degree is kept via the signature checksum. The student receives the signed academic attestation and adds it to their academic records. In this case, confidentiality is not a requirement but data integrity. Socioblock participants are able to send evidence of their academic records via the blockchain. Once educational providers agree on a standard to digitalise academic degrees and join this blockchain implementation and its specific corresponding DApp channel, the possibility to forge a degree would be minimal.

B.6 Mortgage search

This case study shows how code-based contract automation in a blockchain can speed up the search of a real estate mortgage. In the brick and mortar world, searching for a mortgage can still be a cumbersome and highly paper-based process. Blockchain can bring a higher degree of transparency to it. The players at stake in this scenario are: a blockchain participant looking for a mortgage, a broker between the searching participant and mortgage providers and those financial institutions interested in offering a mortgage.

B.6.1 A set of smart contracts to match offer and demand

The logic behind this process of searching for the best mortgage can be broken down into three pieces of code within the umbrella of a decentralised blockchain-based application (DApp):

- Creation of a mortgage search: A participant looking for a mortgage interacts with the mortgage DApp by filling in a request with standardised fields that describe the desired mortgage. This mortgage request is linked to a digital identity. In a first iteration of the mortgage searching process, the requester can decide to share only the proxy digital identity, described in Section B.2.4. Later on, close to the final agreement, the selected mortgage provider requires the real digital identity linked to the physical one. The participant shares the request with a mortgage broker service that would contact mortgage providers registered in this mortgage-related DApp.

- Collection of relevant mortgage offers: A mortgage broker service gathers, via a standardised API in the blockchain, mortgage offers that match demands, from banks present in this blockchain-based ecosystem. It builds a list of all offers with their conditions. This list is available to the mortgage requester.

- Mortgage selection and signature: The mortgage requester, via the DApp, decides which of the offers, presented by the broker service, they sign. Once a specific mortgage offer is signed by the private key of the requester, the code contacts the offering bank and present to it all the required data so that the payment can be made to the real estate owner and instalments can commence.

The added value of this three-component DApp is that most of the steps are automated via smart-contracts that interact with off-chain elements such as the user interface (via an application) and the required back-end servers that produce the different mortgage offers. This reduces greatly customer friction.