UNIVERSIDADE ABERTA

UNIVERSIDADE DE TRÁS-OS-MONTES E ALTO DOURO

MODELO DE *SMART PLACES* CONFIÁVEL

António José Morim Brandão

Doutoramento em Ciência e Tecnologia Web

2020

UNIVERSIDADE ABERTA

UNIVERSIDADE DE TRÁS-OS-MONTES E ALTO DOURO

MODELO DE *SMART PLACES* CONFIÁVEL

António José Morim Brandão

Doutoramento em Ciência e Tecnologia Web

Tese de Doutoramento Orientada pelo Professor Doutor José Henrique Pereira São Mamede e Coorientada pelo Professor Doutor Ramiro Manuel Ramos Moreira Gonçalves

2020

Resumo

Os *smart places*, como a desmaterialização dos diversos ecossistemas naturais, envolvem diversos ecossistemas autónomos que se interligam e promovem a integração da informação e a convergência de funções e atividades, necessariamente seguras, que dependem de dados confiáveis e fontes confiáveis. O problema da gestão de dados, da sua qualidade e da sua governação agrava-se com a quantidade de dados gerados, a multiplicidade de dispositivos, espaços, infraestruturas, utilizadores e entidades ligados, sendo um desafio tecnológico e de gestão. Os diversos riscos cibernéticos podem provocar o comprometimento dos dados, a exploração das fragilidades, a infeção dos sistemas, condicionando o funcionamento da cidade e, no limite, desligar ou mesmo destruir a infraestrutura física ao ponto de os cidadãos terem as suas vidas ameaçadas.

A metodologia de investigação escolhida para este trabalho é a metodologia *Design Science Research (DSR)*, na abordagem centrada no problema, onde se pretende construir um artefacto, que permita avaliar alternativas viáveis de utilização da tecnologia confiável, baseada em *blockchain.*

A proposta centra-se num modelo genérico de dados a aplicar aos *smart places*, no contexto das *smart cities*, focando a sua revisão e estruturação nos aspetos de gestão de dados e da sua governação. O modelo proposto adota as tecnologias *blockchain* e aplica às diferentes características da cidade, na governança eletrónica, na contratação de produtos e serviços e na recolha de dados. Os múltiplos objetos *IoT* e as múltiplas redes, juntamente com a tecnologia *blockchain*, podem resultar em espaços e cidades mais seguras e eficientes. Este trabalho aprofunda o conceito de *smart cities*, no ecossistema de mobilidade e transportes, utilizando a tecnologia *blockchain* como plataforma de segurança e confiabilidade dos dados, aplicado no artefacto do subsistema de bilhética e de tráfego, para a confiabilidade e controlo dos *logs* gerados pelos inúmeros dispositivos.

Com este artefacto pretende-se a generalização do modelo a aplicar a diferentes subsistemas permitido que os modelos de dados genéricos, sejam integrados e automatizados, com dados de qualidade e informações confiáveis. O controlo dos fluxos dos dados, a gestão do ciclo de vida dos dados e da informação permitirá um processo de gestão de dados e de gestão da informação e da sua governança, mais confiável.

Palavras-chave: *Smart Places*; *Smart Cities*; *Blockchain*; Segurança dos dados; Dados *IoT*

Abstract

Smart places, such as the dematerialization of diverse natural ecosystems, involve several autonomous ecosystems that interconnect and promote the integration of information and the convergence of necessarily secure functions and activities that depend on reliable data and reliable sources. The problem of data management, its quality, and its governance is aggravated by the amount of data generated, the multiplicity of devices, spaces, infrastructures, users and connected entities, being a technological and management challenge. The various cyber risks can lead to data compromise, exploitation of weaknesses, infiltration of systems, conditioning the functioning of the city and, in the limit, disengaging or even destroying the physical infrastructure to the point where citizens have their lives threatened.

The research methodology chosen for this work is the Design Science Research (DSR) methodology, in the problem-centered approach, where we intend to construct an artifact, which allows us to evaluate viable alternatives for using reliable, blockchain-based technology.

The proposal focuses on a generic data model to be applied to smart places in the context of smart cities, focusing on their revision and structuring in data management aspects and their governance. The proposed model adopts the blockchain technologies and applies to the different characteristics of the city, in the electronic governance, in the contracting of products and services and the collection of data. Various IoT objects and multiple networks, along with blockchain technology, can result in safer and more efficient spaces and cities. This work explores the concept of smart cities in the mobility and transport ecosystem, using blockchain technology as a platform for data security and reliability, applied in the ticketing subsystem and traffic subsystem, for the safety and control of the logs generated by the numerous devices.

With this artifact it is intended the generalization of the model to be applied to different subsystems allowed that generic data models, be integrated and automated, with quality data and reliable information. Controlling data flows, managing the data and information lifecycle will enable a more reliable data management, information management, and governance process.

Keywords: Smart Places; Smart Cities; Blockchain; Data security; IoT Data

Dedicatória

Dedico este trabalho à minha mulher e aos meus filhos,

ao meu pai e à minha mãe.

Agradecimentos

Os primeiros agradecimentos vão para o meu Orientador, o Prof. Henrique São Mamede, e para o meu Coorientador, o Prof. Ramiro Gonçalves, pela forma objetiva, planeada e desafiante que me conduziram neste percurso.

Às Universidades, Universidade Aberta e Universidade de Trás-os-Montes e Alto Douro, pelo exigente e excelente Programa Doutoral do Curso de Ciência e Tecnologia Web, multidisciplinar que permitiu um enriquecimento muito para além do curso propriamente dito.

O meu agradecimento aos meus amigos, aos meus colegas de trabalho e à minha empresa.

Aos meus colegas que começaram este percurso e se propuseram na sua primeira edição.

A todos o meu profundo agradecimento.

Nota Prévia

Este trabalho de investigação obedece às Normas de Apresentação das Dissertações de Mestrado e das Teses de Doutoramento da Universidade Aberta, de dezembro de 2014 e à Norma bibliográfica da *American Psychological Association* (APA), 6ª edição.

Índice Geral

Índice de Tabelas

Índice de Figuras

Lista de Abreviaturas, Siglas e Acrónimos

ADR - Action Design Research

AES - Advanced Encryption Standard

AHP - Analytical Hierarchy Process

AI - Artificial Intelligence

AMQP - Advanced Message Queuing Protocol

API´s - Application Program Interfaces

ASICs - Application Specific Integrated Circuits

ATC - Automatic Train Control

ATO - Automatic Train Operation

ATP - Automatic Train Protection

ATR - Automatic Train Regulation

ATS - Automatic Train Supervision

BCS - *Blockchain* Structures

BFT - Byzantine Fault-Tolerant

BI - Business Intelligence

BIM - Building Information Model

BL - *Blockchain* Local

BMS - Building Management Systems

BREEAM - Building Research Establishment Environmental Assessment Method

BTM - Balise transmission module

C-ITS - Cooperative Intelligent Transport Systems

CBIS - Compute-based information systems

CBTC - Communications-Based Train Control

CCM - Cipher Block Chaining-Message Authentication Code

CDIM - City District Information Model

CI - Computer Inter-locking

CIM - City Information Modeling

CityGML - City Geography Markup Language

CLIs - Comand-Line Interfaces

CoAP - Constrained Application Protocol

CoT - Cloud of Thing

CSSP - Cloud Storage Provider

CVIM - Common Vehicle Information Model

DAG - Directed Acyclic Graph

DAOs - Decentralized Autonomous Organization

DDS - Data Distribution Service

DHT - Distributed *Hash*-Table

DLT - Distributed Ledger Techno*log*y

dPoS - Delegated Proof of Stake,

DR - Demand Response

DRL - Deep Reinforcement Learning

DRU - Data Recording Unit

DS - Design Science

DSM - Demand Side Management

DSR - Design Science Research

DSRIS - Design Science Research in Information Systems

DSRM - Design Science Research Methodo*log*y

DSRPM - DSR Process Model

DTLS - Datagram Transport Layer Security

E2E - End-to-End

ECC - Elliptic Curve Cryptosystems

ECDH - Elliptic-curve Diffie-Hellman

ECDSA - Elliptic Curve Digital Signature Algorithm

ECMV - Elliptic Curve Menezes Vanstone

ERP - Enterprise Resource Planning

ESP - Encapsulation Security Payload

ETCS - European Train Control System

EVM - Ethereum Virtual Machine

FI - Future of Internet

GHOST - Greedy Heaviest-Observed Sub-Tree

GIS - Geographic Information Systems

GoA - Grades of Automation

GPG - GNU Privacy Guard

GPS - Global Positioning System

HLF - Hyperledger Fabric

HMAC - *hash* message authentication code

IBIS - Integrated On-board Information System

ICD - Implantable Cardioverter Defibrillator

IFC - Industry Foundation Classes

IMDs - Implantable Medical Devices

IoT - Internet of Things

IoV - Internet of Vehicles

IPFS - Inter Planetary File System

IPLD - InterPlanetary Linked Data

IPNS - InterPlanetary Naming System

IPRS - InterPlanetary Record System

IPU - Interlocking Processing Unit

ISD - Information Systems Development

ISDT - Information Systems Design Theory

ISM - Interpretative Structural Modeling

ITS - Intelligent Transport Systems

KMS - Key Management System

KPIs - Key Performance Indicator

KSI - Keyless Signature Infrastructure

LRV - Light Rail Vehicles

M2M - Machine to Machine

MC - Material Circulante

MDM - Master Data Management

Merkle - Merkle tree root *hash*

ML - Machine Learning

MPC - Multi-Party Computation

MQTT - Message Queue Telemetry Transport

MQTT-SN - MQTT for Sensor networks

MV - Máquinas Virtuais

NGTC - Next Generation Train Control

NIS - Network and Information Security Directive

NN - Nearest Neighbor

OBC - On-Board Computer

OCS - Object Controller System

OPC UA - Open Platform Communications Unified Architecture

PADR - Participatory Action Design Research

PBFT - Practical Byzantine Fault Tolerance

PDD - Protocol Driven Development

PIS - Passenger Information System

PLS - Physical Layer Security

PN - Passagens de Nível

PoS - Proof of Stake

PoW - Proof of Work

PKI - Public Key Infrastructure

PUF - Physical Unclonable Functions

QFD - Quality Function Deployment

QoS - Quality of Service

QR - Quick Response

RDF - Resource Description Framework

RE-CAWAR - Requirement Engineering Context Awareness

REST - Representational State Transfer

RFID - Radio-Frequency IDentification

Ripple - Ripple Protocol Consensus Algorithm

ROS - Robot Operating System

SCADA - Supervisory Control and Data Acquisition

SCALE - *Smart city* Application Ecosystem

SCP - Stellar Consensus Protocol

SDE - Secure Data Exchange

SDN - Software Defined Network

SDRM - Systems Development Research Methodo*log*y

SDS - Soft Design Science

SDSM - Soft Design Science Methodology

SI - Sistemas de Informação

SIEM - Security Information and Event Management

SIG - Signalling System

SIP - Sistema de Informação ao Público

SLA - Service Level Agreement

SOA - Service Oriented Architecture

SPV - Simplified Payment Verification

TIC - Tecnologias de Informação e Comunicação

TLS - Transport Layer Security

TMS - Traffic Management System

UCC - Urban Carrying Capacity

UIC - International Union of Railways

URT - Urban Rail Transit

URTs - Unidade Remota Terminal

UTO - Unattended Train Operation

VA - Valor Acrescentado

VANETs - Veiculares Adhoc Networks

VM - Virtual Machine

VTCU - Vehicle Train Control Unit

WSNs - Wireless Sensor Network

XML - Extensible Markup Language

XMPP - Extensible Messaging and Presence Protocol

ZC - Zone Controller

I. INTRODUÇÃO

I. INTRODUÇÃO

Este trabalho de investigação orienta-se para apresentar um modelo de *smart places* baseados em tecnologias seguras que permitam garantir a confiança dos dados gerados, que suportam o seu funcionamento, a geração de informação, de conhecimento e a tomada de decisões.

O modelo será avaliado com o recurso a provas de conceito através de artefactos que permitirão validar o modelo na componente de alarmística e dos sistemas de monitorização existentes numa *smart city.* O sistema escolhido foi o sistema de bilhética pertencente ao ecossistema de mobilidade e transportes.

Esta modelização procura responder às inúmeras questões que percorrem os diversos domínios envolvidos num *smart place*, onde as aplicações se integram para garantir a confiança nos dados e nas informações.

O *smart place* deste estudo será baseado nos conceitos e nos modelos de *smart city*.

A tecnologia em análise e avaliação deverá ser suportada na tecnologia *blockchain* como forma de garantir e controlar os fluxos de dados e desta forma a confiança dos dados, da informação e das transações.

Nesta perspetiva procura-se rever vários conceitos que serão detalhados ao longo deste trabalho, que passam por definir os conceitos de *smart place* e de *smart city*, os modelos de *smart city*, as caraterísticas do *blockchain,* as aplicações da tecnologia *blockchain*, os desafios e as limitações, e o sistema de informação de apoio aos sistemas de transporte ferroviários urbanos, aprofundando o sistema de gestão de tráfego e o sistema de bilhética.

O trabalho científico será consolidado através do desenvolvimento de artefactos para a aplicação deste modelo num aspeto específico do funcionamento da *smart city*, neste caso no sistema de mobilidade e transportes e na gestão dos eventos de bilhética do sistema de metro ligeiro, através da aplicação da metodologia DSR (*Design Science Research*), baseada na abordagem centrada no problema (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007).

A *smart city*, no conceito aqui apresentado, é uma cidade não apenas física, mas também digital e virtual, que apresenta várias dimensões, como a sua governança, as instituições, as empresas, as políticas de sustentabilidade ecológica, social e económica, as políticas de mobilidade e de transportes, a participação cívica dos diferentes agentes económicos

e sociais, as políticas de inovação, as TICs (Tecnologias de Informação e Comunicação) e os SI (Sistemas de Informação) que confluem para estratégias comuns (Brandão et al., 2018a).

Estas estratégias devem obedecer a *frameworks* de integração, de relação, de interação, de participação, de acesso à informação, que implicam infraestruturas de conectividade robustas, de redes de fibra ótica, de redes sem fio e de integração de redes, que poderão suportar as necessidades crescentes dos diversos serviços e aplicações, de monitorização, de controlo, de sensorização e dispositivos *IoT*, com a multiplicação de sensores, atuadores de aplicações, com arquiteturas mais adaptativas, base de dados que crescem vertiginosamente, com o tratamento de enormes quantidades de dados, através de conceitos de *big data*, de *data mining* e de visualização da informação (*InfoVis*) para poder extrair informação relevante, que reoriente as estratégias, as políticas, a criação de ecossistemas potenciadores de negócios e de novos modelos de negócio.

Em síntese, esta tese explora as seguintes áreas: os *smart places* em ambiente Web, centrando-se nas *smart cities* como contexto de aplicação, com o tema base orientado para a gestão dos dados, principalmente da governança e da segurança dos dados, e com a possibilidade de utilização da tecnologia de suporte *blockchain* como tecnologia confiável para garantir a integridade da informação e o não comprometimento dos dados.

A *smart city* é entendida em duas dimensões essenciais, numa dimensão mais material, associada aos aspetos físicos e naturais de uma cidade e na sua otimização, e numa dimensão intangível, associada aos aspetos de bem-estar das pessoas, mobilidade, educação, saúde, inovação, inclusão social e na sua governação. Esta cidade, este espaço urbano, é vulnerável ao comprometimento de dados (Popescul & Radu, 2016) e à falsa injeção de dados (K. Zhang et al., 2017). O crescente volume de dados, o grande número de dispositivos, espaços, infraestruturas e utilizadores ligados, estendem os riscos e podem provocar o comprometimento dos sistemas, com a utilização de fragilidades que podem ser transmitidas ou exploradas entre os sistemas. Este problema central pode em situações limite permitir a exploração das fragilidades ou a possibilidade de infeção que poderá comprometer o funcionamento da própria cidade e desligar ou mesmo destruir a infraestrutura física ao ponto de os cidadãos terem as suas vidas ameaçadas. (Popescul & Radu, 2016)

A gestão de dados e a governação da crescente quantidade de dados é um desafio técnico e de gestão, particularmente à medida que os dados e a informação resultante se

desenvolvem como recursos estratégicos com características que tornam difíceis de governar. O controlo dos fluxos dos dados, a gestão do ciclo de vida dos dados e da informação tornou-se num ponto crítico no processo de gestão de dados e de gestão da informação e da sua governança.

Numa primeira breve introdução refere-se à utilização de aplicações de *blockchain* em diversos domínios, descritos em alguns artigos referidos a seguir:

- O artigo de Yli-Huumo, Ko, Choi, Park, & Smolander (2016) apresenta como exemplos os protótipos de aplicações desenvolvidas e sugeridas para o uso de *blockchain* noutros ambientes, como o *IoT*, os *smart contracts*, a propriedade "inteligente", a distribuição de conteúdo digital, o *botnet* e os protocolos de transmissão P2P, usados em ambiente descentralizado.
- O artigo de Dorri, Kanhere, Jurdak, & Gauravaram (2017) descreve os componentes principais duma *smart home*, com os dispositivos *IoT*, o armazenamento local, o mineiro (*miner*) e o BL (*Blockchain* Local) e discute as várias transações e procedimentos associados a ela, com uma análise sobre segurança e privacidade. A simulação *smart home* demonstra que os custos gerais incorridos pelo método descrito são baixos e geríveis para dispositivos *IoT* de baixos recursos e são aceitáveis dados os benefícios de segurança e privacidade oferecidos.

Esta breve descrição da aplicação da tecnologia *blockchain* orienta para alguns dos aspetos críticos dos dispositivos *IoT*, como as preocupações de segurança e de privacidade dos dados.

Os *smart places* concentram diversos aspetos comuns às Organizações, como espaços de colaboração e de "inteligência" competitiva, com capacidades dinâmicas e processos de informação, com quadros de controlo, métricas e avaliações. As *smart cities* são necessariamente Organizações dinâmicas, com modelos comuns e indicadores que devem conduzir ao processo de formulação de politicas, com dados confiáveis e que suportam os processos informacionais e de negócio.

A "inteligência" competitiva e o desenvolvimento de capacidades dinâmicas nas Organizações têm como objetivo verificar se os estágios do ciclo de inteligência competitiva podem constituir elementos estimulantes para as capacidades dinâmicas das Organizações (Garcia, 2017). A "inteligência" competitiva promove a perceção da

mudança e fornece a "inteligência" necessária para a aquisição do conhecimento que será a base da ação, contribuindo para a contínua reinvenção do negócio (detetar, apreender e transformar). A "inteligência" não dever ser apresentada apenas para facilitar e melhorar a compreensão como uma capacidade única e imutável, mas por múltiplas formas e modificáveis (Schelini, 2006).

O desenvolvimento sustentável integral apresenta um quadro prático (Brown, 2005) que integra o panorama conceitual e operacional do desenvolvimento sustentável e permite identificar a série completa de necessidades e capacidades dos indivíduos e grupos, e adequar a resposta de desenvolvimento específico que se encaixa em cada situação única. O quadro mapeia e integra a consciência humana e o comportamento, a cultura, os sistemas e o ambiente físico, numa abordagem abrangente e precisa para enfrentar os nossos desafios sociais, ambientais e económicos.

A conceptualização de uma *smart city* apresenta várias dimensões, de tecnologia, de pessoas e de instituições (Nam & Pardo, 2011). Os princípios estratégicos devem ser alinhados com as três dimensões principais que passam pela integração das infraestruturas e serviços de mediação tecnológica, a aprendizagem social para o fortalecimento da base humana e a governança para a melhoria institucional e o envolvimento dos cidadãos.

Um modelo "inteligente" (Lazaroiu & Roscia, 2012) pode ser o suporte para calcular os índices e as métricas para avaliar uma *smart city*. Estes indicadores, como não são homogéneos, têm de ser ponderados para o processo de formulação de políticas e como ponto de discussão entre as partes interessadas, bem como com os cidadãos, para uma decisão final das medidas a adotar e da avaliação das melhores opções.

Os modelos de referência de uma *smart city* podem ser suportados nas características de inovação de ecossistemas "inteligentes", com a estruturação das noções de *smart city* em ecossistemas orientados a critérios verdes, interligados, instrumentados, abertos, integrados e inovadores, que podem compor um quadro de planeamento (Zygiaris, 2013).

Santos (2015) refere as cidades do futuro associadas ao talento, à inovação e à colaboração, perspetivando que a *smart city* potencia a geração de Valor acrescentado.

A cidade é apresentada como um cliente, "*city as a customer*" (Amarnath, 2011), em que a urbanização pode criar inúmeras implicações e oportunidades setoriais. As megatendências, como as alterações climáticas, as mudanças demográficas, a globalização e a urbanização, são forças transformadoras globais que definem o mundo

futuro, com impacto nos negócios, nas sociedades, economias, culturas e vidas, e com implicações na energia (redes "inteligentes", energias renováveis e energia como um serviço), na saúde, na industria, nas infraestruturas e nas cidades (sistemas de transporte, mobilidade e logística, e tecnologias de ecoconstrução).

A necessidade de um quadro de informações (Jin et al., 2014) pode abranger o sistema de informação urbana completo, o nível de sensorização e de *networking*, a estrutura de suporte de gestão de dados e o acesso *cloud*, com a integração dos sistemas e serviços.

A exploração dos dados, suportadas em plataformas, é em si um desafio pelo conjunto diverso, heterogéneo e com a interligação de dados, para construir uma vista unificada de dados (Sadoghi, 2017). O modelo de dados apresenta dificuldades ao nível da forma e dos metadados de cada fonte, para oferecer a consolidação contínua de dados sob a incerteza para fazer o modelo de dados inerentemente adaptável. O Valor que se pode atribui aos dados pode vir de diferentes serviços e formas, do processamento e da análise de dados brutos, para a apresentação de contextos que podem acionar a construção de novos serviços e negócios (Brandão et al., 2019),

Neste domínio, a dificuldade em obter dados fiáveis, pode condicionar a gestão da informação, comprometer a mobilidade sustentável e pode revelar-se um problema nas plataformas modulares. Estas plataformas pretendem integrar os dados para gerir as informações, por exemplo de trânsito e para obter uma mobilidade "inteligente" (Teixeira et al., 2017), embora com a recolha de dados dinâmica, esta é ainda limitada para avaliar como seria possível ler e prever os níveis de congestionamento de tráfego e emissões em tempo real.

A perspetiva centrada nos dados descreve as técnicas de gestão de dados para garantir consistência, granularidade, interoperabilidade e reutilização dos dados. Esta perspetiva centrada no ciclo de vida de dados duma *smart city* fica interdependente da gestão de dados nas camadas de segurança de dados e privacidade, e da infraestrutura de apoio (Gharaibeh et al., 2017).

A pesquisa sobre plataformas de software revela que para facilitar o desenvolvimento, a integração e a implantação de aplicações nas *smart city*, as tecnologias mais capacitadoras mais citadas são a *Internet of Things* (*IoT*), a computação em nuvem (*cloud*), o *big data* e os sistemas ciberfísicos (Santana et al., 2016).

As cidades que pretende ser *smart cities* baseiam-se na monitorização e na computação ubíqua e orientam a economia e a governança para a inovação, criatividade e empreendedorismo, suportada em pessoas capacitadas. Estas cidades, instrumentadas com dispositivos digitais e infraestrutura que produzem *big data*, permitem a análise em tempo real da vida da cidade, novas formas de governação urbana, e a base para idealizar cidades mais sustentáveis, competitivas, abertas, transparentes, eficientes e produtivas. (Kitchin, 2014)

Os estudos sobre diversas aplicações nas *smart cities* são inúmeros e revelam o elevado interesse e importância deste tipo de *smart place* e do impacto no desenvolvimento sustentável, participativo e inclusivo, que orientam os projetos e os desenvolvimentos neste domínio.

Neste texto introdutório revela-se a seguir alguns exemplos desta orientação.

- O estudo de caso da plataforma experimental *SmartSantander* pretendeu produzir os seguintes objetivos: o modelo de referência de arquitetura para a *IoT* de experimentação; uma instalação experimental, larga, escalável, heterogénea e confiável; um conjunto representativo de casos de uso implementados para a instalação experimental; e um grande conjunto de futuros experimentos para a Internet (Sanchez et al., 2011). O aspeto chave foi a disponibilização de um grande conjunto de aplicações com base no seu elevado potencial e impacto sobre os cidadãos, a fim de atrair o maior interesse e permitir demonstrar a utilidade da plataforma experimental.
- Uma *smart city* suportada em *Cloud of Things* (*CoT*) pode oferecer uma abordagem comum e global dos sensores na nuvem e de serviços inovadores para realizar a agregação de recursos heterogéneos, definido no paradigma *Cloud of Things* (Petrolo et al., 2012).
- O modelo de *smart cities* assistidas ou de apoio, através da aplicação da computação ubíqua na acessibilidade, fornece soluções para apoiar as pessoas com deficiência (Telles, 2017).

Este trabalho, que se pretende desenvolver no contexto das *smart cities*, no enquadramento teórico, estuda os modelos, a incorporação do *IoT* na cidade, a utilização do *big data* como ferramenta de análise e descoberta de padrões, fornece o detalhe sobre a utilização da tecnologia *blockchain* em diversos domínios, as suas caraterísticas,

estrutura de bloco, assinatura digital, protocolos/algoritmos de consenso, processo de otimização da verificação através das árvores de Merkel, analisa as plataformas de *blockchain*, perspetiva e contextualiza os mercados de dados e apresenta no ecossistema de mobilidade, os sistemas de informação de apoio aos transportes ferroviários urbanos e com maior detalhe o sistema de bilhética.

O estudo empírico descreve a metodologia, apresenta os resultados da pesquisa, com o modelo genérico de dados, a arquitetura, a aplicação da metodologia, a conceção e desenvolvimento dos artefactos, em duas iterações que se complementam, a avaliação dos artefactos e a comunicação dos resultados da investigação. Na discussão dos resultados analisam-se os fluxos de dados objeto da pesquisa e reflete sobre os caminhos que propiciariam o controlo global dos fluxos de dados e das restantes aplicações de *blockchain* numa *smart city*. Neste ponto também são revistos alguns trabalhos que se relacionam com o trabalho que se desenvolveu.

As considerações finais sintetizam as principais conclusões do trabalho e apresentam o conjunto de limitações que ainda subsistem e que podem conduzir a outras investigações, ao aprofundamento de alguns aspetos do modelo genérico de dados e ao controlo de outras fases do fluxo de dados.

1. Problema da Pesquisa

Com esta pesquisa, pretende-se esclarecer aspetos importantes da conceção, desenvolvimento e gestão de dados nas *smart cities*, principalmente sobre a confiança nos dados, com o objetivo de responder à seguinte questão:

Será possível desenvolver uma plataforma de gestão de dados e de informação, no contexto de uma *smart city*, baseada em tecnologia confiável, que evite o comprometimento dos dados e da respetiva origem*?*

2. Objetivos

A definição de objetivos revela a necessidade de centrar o tema e focar o trabalho nos aspetos considerados essenciais para que permita por um lado demonstrar através do método científico baseado na metodologia mais adequada a resposta proposta para o problema e por outro tentar generalizar a solução encontrada.

2.1. Objetivo Geral

O objetivo geral do projeto passa por aplicar um modelo de dados genérico, a propor, de suporte ao conceito de *smart city*, por forma a sistematizar as suas ações e o controlo dos fluxos de dados e da qualidade dos dados, que permitam gerir os dados e a informação, de forma confiável e segura.

2.2. Objetivos Específicos

Em síntese e de seguida definem-se os seguintes três objetivos específicos que se pretendem atingir com a concretização do trabalho a desenvolver.

1. Estruturar um modelo de dados genérico de suporte ao conceito de *smart city* que conduza e permita o alinhamento da aplicação dos ecossistemas de dados com os ecossistemas naturais.
2. Estruturar as relações entre os ecossistemas, os participantes e os dados que facilite a utilização da tecnologia *blockchain* na gestão dos dados.
3. Assegurar mecanismos de confiabilidade na gestão dos dados e das fontes dos dados.

3. Justificação

O futuro do mundo estará orientado por dados, mantendo-se ligado, monitorizado e auditável, ouvindo, vendo e a aprender.

As estatísticas da internet em 2019[1] indicam cerca de 4,38 mil milhões de utilizadores na Internet, em 31 de março de 2019, correspondendo a 56,8% da população, com um crescimento de 1.114% entre 2000 e 2019, com 50,1% concentrados na Ásia.

Na oferta e pedido de armazenamento de dados estima-se o fornecimento de 24.800 exabytes para pedidos de 42.700 exabytes em 2020[2].

[1] Internet Statistics - https://www.internetworldstats.com/stats.htm, acedido em 21-06-2019
[2] Statista - https://www.statista.com/statistics/751749/worldwide-data-storage-capacity-and-demand/, acedido em 21-06-2019

No artigo da NetworkWorld[3], a IDC[4] estima, em 2025, cerca de 175 zettabytes (ZB) de dados, dos quais 90 ZB de dados serão criados em dispositivos *IoT* e 49% dos dados serão armazenados em ambientes de nuvem pública e 30% dos dados gerados serão consumidos em tempo real. Os equipamentos *IoT* instalados nas *smart cities* em 2018[5] foram de 463,5 milhões (mais 22% do que em 2017).

Dada a importância dos dados nos *smart places*, o projeto proposto pretende centrar a investigação na confiança dos dados e na proposta de um modelo de dados genérico em que a sua avaliação será através do desenvolvimento de artefactos, baseados em provas de conceito, para responder às questões de controlo dos fluxos de dados, da gestão dos dados e da informação, e da sua governança, propondo a utilização da tecnologia *blockchain* para garantir a eficácia do modelo e a confiança nos dados e nos fluxos dos dados.

4. Estrutura da tese

Introdução

Neste capitulo pretende-se enquadrar os principais elementos que suportam os trabalhos de investigação, definindo o problema da pesquisa, os objetivos, seja o objetivo geral, sejam os objetivos específicos, o propósito e a justificação dos trabalhos de investigação e a revelação da estrutura da tese.

Parte I - Enquadramento teórico.

Nesta parte apresenta-se a revisão da literatura que percorre o estado da arte orientada aos assuntos tratados neste trabalho de investigação, o conceito mais genérico dos *smart places*, as *smart cities*, a tecnologia *blockchain* e as suas diversas aplicações, o *IoT*, e de forma mais especifica no ecossistema de mobilidade e transportes, no transporte ferroviário, os sistemas de gestão de bilhética e gestão de tráfego.

A gestão dos dados mantem-se central nesta revisão, quer na sua conceptualização, quer na sua governação.

---

[3] Networkworld - https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html, acedido em 21-06-2019

[4] Seagate e IDC Data- https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf, acedido em 21-06-2019

[5] Statista SC IoT - https://www.statista.com/statistics/423063/smart-cities-connected-things-installed-base-utilities-sector/, acedido em 21-06-2019

O primeiro ponto apresenta os *smart places* e o cenário de implementação nas *smart cities.* Define os conceitos dos *smart places* e revê os modelos que permitem aos conceitos de *smart cities* estruturar os ecossistemas naturais através dos ecossistemas de dados.

O segundo ponto centra-se na tecnologia *blockchain*, desde as suas caraterísticas, a estrutura de bloco, a assinatura digital, as principais características do *blockchain*, os mecanismos de consenso como o *PoW* (*Proof of Work*), *PoS* (*Proof of Stake*), *PBFT* (*Practical Byzantine Fault Tolerance*), *dPoS* (*Delegated Proof of Stake*), *Ripple* (*Ripple Protocol Consensus Algorithm*), *Tendermint*, outros algoritmos de consenso e os seus principais desafios. Também se revê os aspetos de aplicação na segurança, as plataformas de *blockchain*, as arquiteturas e a taxonomia, a utilização das árvores de Merkel e do *IPFS* (*Inter Planetary File System*), como formas de potenciar e otimizar a utilização da tecnologia *blockchain.*

Para a adoção da tecnologia *blockchain* é revista a forma como a tecnologia *blockchain* pode ser usada como base para garantir a confiança nos dados, o controlo dos fluxos dos dados e suportar a integridade da informação.

O terceiro ponto revê os aspetos principais das plataformas de suporte aos mercados de dados. Os mercados de dados são analisados no contexto dos *smart cities* e revendo a importância da confiança dos dados disponibilizados, na sua qualidade e na sua origem. O quarto ponto revê o sistema de mobilidade e transportes que será objeto de artefactos baseados em provas de conceitos.

A partir dos *smart places* e dos modelos de *smart cities* centramo-nos no ecossistema de mobilidade e transportes, com os sistemas de transportes públicos ferroviários, as tecnologias de informação nas redes de transportes públicos, com os sistemas de informação de apoio ao controlo e gestão, à exploração, à gestão de tráfego ferroviário e ao material circulante e especificamente o sistema de bilhética objeto central da conceção e desenvolvimento.

Parte II - Estudo empírico.

O primeiro ponto da parte II dedica-se à metodologia, com a definição do método, as etapas previstas, o problema, o desenvolvimento pretendido, como avaliar e a conclusão. Neste ponto pretende-se estruturar a metodologia de investigação, com a descrição e caracterização da investigação e dos fundamentos para a opção metodológica e a contextualização geral dos *smart places* e em particular da *smart city* em análise.

No segundo ponto apresentam-se os resultados da pesquisa, com o modelo genérico, a arquitetura de sistema e os resultados práticos. Neste capitulo pretende-se criar a contextualização, operacionalização e análise da *smart city* e do caso específico em análise, aplicado ao sistema de mobilidade e transportes, no domínio aplicacional do sistema de eventos de bilhética.

No terceiro ponto analisam-se e discutem-se os resultados. Neste capítulo pretende-se a sistematização, desenvolvimento e avaliação do modelo proposto de forma a ser generalizado. A análise e construção do modelo a adotar deve permitir a operacionalização e a avaliação da gestão de dados, a sua governança e controlo de fluxos, representando um contributo de Valor para a *smart city* e de forma genérica para os *smart places*.

Parte III - Considerações Finais.

Nesta parte apresentam-se as conclusões e limitações, onde se descrevem os aspetos conclusivos do trabalho, dando ênfase aos contributos que este trabalho fornece no âmbito da gestão e controlo dos fluxos de dados e as limitações que podem condicionar a aplicação do modelo proposto.

II. ENQUADRAMENTO TEÓRICO

II. ENQUADRAMENTO TEÓRICO

Após o Capítulo I, introdutório, aparece neste capítulo o referencial teórico onde se pretende rever e apresentar as informações obtidas através da consulta e análise criteriosa da revisão da literatura com as evidências científicas consideradas relevantes para a compreensão dos temas e que possam fornecer a informação que suportam cientificamente as questões propostas.

Esta revisão de literatura e do estado da arte pretende consolidar o referencial teórico que deve apoiar os principais aspetos desta investigação. Aspetos teóricos e conceitos relacionados com o modelo de análise são aprofundados para permitir o entendimento e a explicação do problema com a compreensão da prática pretendida para o trabalho empírico.

O estado da arte apresenta assim os vários conceitos envolvidos e as aplicações documentadas, as estratégias, as metodologias e as técnicas que facilitam a organização, a informação e o desenvolvimento das atividades da parte empírica.

1. *Smart places*

Neste ponto analisam-se as diversas perspetivas dos *smart places*, como espaços físicos, de geometria variável, com modelos de organização subjacentes e com a sua tradução virtual e digital, que adicionam outras valências e caraterísticas de modelação, de simulação, de monitorização, de participação e colaboração, de gestão e governança, que potenciam a adoção mais eficaz e eficiente de novas politicas, medíveis e controláveis.

O conceito de *smart place* redefine a dimensão espacial e desmaterializa os ecossistemas naturais em ecossistemas digitais, permitindo estabelecer relações, integrando e permitindo a interoperabilidade. A dimensão espacial dos *smart places* é variável, dependendo da geografia e dos modelos Organizacionais subjacentes. Neste conceito encontram-se as Entidades com uma expressão física e que são Organizações que contêm as dimensões, pessoas, governança e tecnologia.

Morandi, Rolando, & Di Vita (2016) redefinem as referências espaciais e conceituais. O conceito de *smart city* evolui para o conceito de região "inteligente" com características específicas e potenciais para a inovação. A transição das *IoT* para a Internet de Lugares permite a integração de serviços físicos e digitais, explorando o contexto espacial da região "inteligente" através da adoção das funções urbanas importantes para a inovação

da região metropolitana. O conceito de nó urbano evolui para o conceito de nó urbano digital que apoia o desenvolvimento da Internet de Lugares no conceito da escala de funções urbanas, com uma escala espacial mais ampla e com diferentes categorias de utilizadores como os moradores, os estudantes e as cidades-utilizadoras.

O modo, como as Organizações, as cidades, as vilas e os bairros vão responder às mudanças que o *smart* se traduz, será essencial para a necessidade de gerir os seus ambientes físicos e para o que o s*mart* significa, com os atributos físicos que se possam dar aos seus equivalentes virtuais na criação de lugares memoráveis, prósperos, sustentáveis e verdadeiros (Walters, 2011).

Na dimensão das pessoas, no estudo de Glaeser (2006) os empreendedores altamente qualificados vão inovando de forma que empregam pessoas com competências semelhantes. Nesta medida se os indivíduos qualificados aumentam, os salários dos trabalhadores à sua volta aumentam e teremos os indivíduos qualificados a concentrarem-se nas cidades "inteligentes", com tendência para maiores concentrações de riqueza. O que resulta, que as políticas locais e regionais têm interesse em garantir que as suas comunidades e regiões se tornem "inteligentes" e permaneçam "inteligentes". Para tal será necessário e essencial investir na educação e na segurança, com o objetivo de contribuir para o afluxo de trabalhadores altamente qualificados, que valorizam as ruas seguras.

Neste trabalho de investigação o *smart place* tratado será o caso específico das *smart cities*, que se detalha no ponto seguinte.

1.1. *Smart city*

Neste ponto a *smart city*, como o *smart place* objeto deste trabalho, introduz diversas visões, definições e modelos deste espaço "inteligente" formado por inúmeras dimensões e fatores que se procuram apresentar e rever com base na revisão da literatura.

No artigo (Brandão et al., 2018a) desenvolvido no âmbito desta tese considera-se que a adoção de tecnologias *blockchain*, como uma plataforma para a governança e para a segurança e confiabilidade dos dados, adaptadas às diferentes características da cidade e que passam por combinar objetos de *IoT*, várias redes, vários ecossistemas que se interligam, pode resultar em cidades mais seguras e eficientes.

As cidades passam a desenvolver-se em *smart cities* mais devido a necessidades corporativas com campanhas de marketing do que pela "inteligência" social (Deakin & Al Waer, 2011). A "inteligência" social para se desenvolver depende da qualidade e da riqueza da informação e da comunicação dessa transição. As comunidades "inteligentes" representam nas cidades um papel crítico para a criação de redes de inovação, de parcerias criativas e de aprendizagem, e na transferência de conhecimentos e na capacitação.

O processo de digitalização e a infraestrutura eletrónica subjacente ao setor de serviços permite a redução dos custos e a melhoria das relações entre compradores e fornecedores que se multiplicam e vêm facilitar as negociações e as transações (Scuotto et al., 2017). Com a partilha de conhecimentos e da interligação dos mercados eletrónicos, mais globais, as cidades ou os espaços regionais têm que se alavancar em quatro pilares; recursos humanos especializados em TICs, atividades de partilha de conhecimento, relações comprador-fornecedor e a adoção de mercados eletrónicos para potenciar os produtos e serviços regionais.

Os conceitos da cidade "inteligente" e da sociedade espacialmente habilitada apresentados por Roche, Nabian, Kloeckl, & Ratti (2012) são dois campos diferentes embora relacionados da cidade. A infraestrutura e a comunidade de dados impulsionam o primeiro conceito, enquanto os profissionais e os investigadores nomeadamente em planeamento urbano, estudos urbanos e desenho urbano estão mais preocupados com o último.

Wolisz, Böse, Harb, Streblow, & Müller (2014) apresentam o modelo de informação da cidade/região (*CDIM-City District Information Model*) como conceito de gestão de dados integrada para bairros da cidade, para simular diferentes qualidades de dados de entrada, mostrando que pequenos desvios das normas de construção ou das dimensões de construção afeta consideravelmente a exigência de energia e dos custos.

Spiekermann & Cranor (2009) apresentam os requisitos de privacidade para as *smart cities*, baseados nas perspetivas históricas e contemporâneas, através de um modelo com três níveis de preocupações, com a privacidade dos utilizadores relacionados, com as operações do sistema que passam pela transferência de dados, armazenamento e processamento e com a análise do comportamento do utilizador para desenvolver diretrizes para a construção de sistemas "*privacy by design*".

Deakin (2011) sugere que a "inteligência" embutida nas *smart cities* torna possível que se possa ativar a criatividade das comunidades virtuais emergentes e de natureza inclusiva digital, com capacidades analíticas e sintéticas para criar comunidades virtuais, através do uso da memória coletiva, *wikis* e *blogs* de serviços aprimorados eletronicamente como meio de superar as divisões sociais.

Beyer, Elisei, Popovich, Schrenk, & Zeile (2015) apresentam uma governança urbana sustentável através do processo interativo e participativo do cidadão e não apenas de utilizadores, no paradigma da mobilidade "inteligente", com o envolvimento aberto e ativo das pessoas e das partes interessadas, nas áreas da tecnologia, transporte, uso da terra, questões urbanas, meio ambiente, saúde pública, ecologia, engenharia, modos verdes e transportes públicos.

Prehofer et al. (2010) demonstraram a viabilidade de fornecer serviços "inteligentes" de *smart space* e implementando um protótipo de espaço "inteligente", ao propor um quadro baseado na *Web* como um estilo de arquitetura de software para serviços web (*REST-Representational State Transfer*) para permitir espaços "inteligentes" e para suportar aplicações difundidas em vários dispositivos.

Sánchez, Elicegui, Cuesta, Muñoz, & Lanza (2013) apresentam uma arquitetura explorando os principais conceitos do paradigma da Internet do Futuro (*FI-Future of Internet*) para criar cidades mais "inteligentes". A arquitetura é suportada nas infraestruturas de comunicações críticas existentes, na propriedade dos serviços públicos que permitam a integração de serviços atuais da cidade vertical e para a eficiência e sustentabilidade das nossas cidades. O protótipo foi implantado num parque da cidade de Santander para os serviços de adaptação da iluminação pública autónoma.

Mohammadi, Al-Fuqaha, Guizani, & Oh (2018) aprofundam a aprendizagem por reforço (*DRL-Deep Reinforcement Learning*) de apoio ao *IoT* e aos serviços "inteligentes", onde a "inteligência" dos serviços é obtida e melhorada através dos dados sensoriais, com o reconhecimento de contexto, conseguindo-se que dados não rotulados o sejam e fornecendo *feedback* dos utilizadores que permite a aprendizagem e a escolha entre ações alternativas.

Walters (2011) argumenta que se as políticas e as ferramentas de implementação do *design* urbano forem incorporadas e codificadas dentro da estrutura de governança

eletrónica de uma comunidade, poderá ser alcançado um equilíbrio quando os domínios físico e virtual melhorarem o caráter único de locais específicos.

Rey-Robert (2009) refere que temos a capacidade de medir e ver a exata condição de qualquer coisa que esteja a ser instrumentada: cadeias de fornecimento, redes de saúde, cidades e sistemas naturais. A interligação de pessoas, sistemas e objetos permitem comunicar e interagir uns com os outros e de novas formas que podem responder às mudanças com rapidez e precisão, e obter melhores resultados com a previsão e otimização para eventos futuros.

Trindade et al. (2017) examinam os termos, *smart city* e sustentabilidade, orientados para o desenvolvimento sustentável das cidades. Também apresenta uma base teórica para entender a relação entre os conceitos de desenvolvimento urbano sustentável e cidades "inteligentes", como desafio de tornar as cidades mais atraentes para as pessoas.

S. Li, Yang, & Gao (2015) estudam como as *smart cities* foram desenvolvidas na China, principalmente os papéis e relacionamentos de diversos atores, incluindo o governo, o mercado e a sociedade no desenvolvimento da *smart city*.

De Jong, Joss, Schraven, Zhan, & Weijnen (2015) investigam as doze categorias mais usadas de cidades dominantes: cidade sustentável, ecocidade, cidade de baixa emissão de carbono, cidade habitável, cidade verde, *smart city*, cidade digital, cidade *ubiquitous*, cidade "inteligente", cidade da informação, cidade do conhecimento e cidade resiliente, as suas diferenças conceituais e as inter-relações entre as doze categorias. A variedade de categorias de cidades mistura-se com o objetivo de criar a sustentabilidade social, económica e ambiental ou a regeneração.

Schaffers et al. (2011) exploram o conceito de *smart city* como ambiente de inovação aberto e orientado pelo utilizador para experimentar e validar novos serviços. O projeto, no domínio dos Laboratórios Vivos, orienta-se para recursos comuns de investigação e inovação, com a finalidade de estabelecer ecossistemas de inovação urbanos e regionais através de parcerias e estratégias de cooperação sustentável entre os principais partes interessadas.

Alawadhi & Scholl (2016) apresentam o estudo que documenta os modelos de governança que surgiram em quatro iniciativas *smart city* (Seattle / EUA, eCityGov Alliance / EUA, Munique / Alemanha, e Turim / Itália) em que se verifica que a governança depende de uma série de fatores diferentes, caso a caso, mas em que o

envolvimento das partes interessadas na governança foi considerado fundamental em todos os casos.

Kitchin (2014) centra-se em como as cidades estão a ser instrumentadas, com dispositivos digitais e infraestrutura, que produzem *big data*. Os dados da *smart city* permitem a análise em tempo real da "vida" da cidade, de formas de governação urbana, e fornece a base para antever e promover a cidade mais sustentável, aberta, transparente, competitiva e eficiente.

Khatoun & Zeadally (2016) refletem na importância dos conceitos, arquiteturas e oportunidades de pesquisa nas *smart cities* dada a previsível melhoria da qualidade de vida dos seus cidadãos. Perspetiva a focalização em aspetos como a gestão da *IoT*, a gestão de dados, a avaliação da *smart city*, a segurança e as tecnologias renováveis, com desafios que exigem soluções pró-ativas na segurança e na privacidade.

Albino, Berardi, & Dangelico (2015) procuram esclarecer o significado da palavra "inteligente" no contexto das cidades e identificar as principais dimensões e elementos que caracterizam uma cidade "inteligente", com a revisão das diferentes métricas de "inteligência" urbana na definição comum de *smart city* e das suas características.

Braem et al. (2016) apresentam num ambiente de testes da *City of Things*, na cidade de Antuérpia, Bélgica, através da infraestrutura de rede de multi-tecnologia, com a capacidade de testar novos dados e validá-los.

Streitz et al. (2005) apresentam o trabalho que projeta artefactos "inteligentes" em ambientes "inteligentes" para melhorar as relações entre os participantes em grupos de trabalho distribuídos. Os participantes mantêm a sua mobilidade pessoal, adicionando possibilidades de colaboração, de comunicação informal e de consciência social que possam contribuir para a partilha e a coesão.

Schleicher, Vogler, Dustdar, & Inzinger (2016) discutem os desafios significativos através de uma visão geral da *SCALE* (*Smart city Application Ecosystem*), suportado num *middleware*, como o sistema operativo da *smart city*. O ecossistema de aplicação da *smart city* pretende a integração das partes interessadas e os recursos para construir de forma eficiente, implantar e operar as aplicações mais importantes da *smart city*. Também revela o ciclo da cidade "inteligente" ideal através de um modelo conceptual para um sistema reativo que aborda os desafios atuais das aplicações da *smart city*.

F. Li, Nucciarelli, Roden, & Graham (2016) apresentam um *framework* que ilustra novos modelos de negócios e como as *smart cities* redefinem a escalabilidade, a analítica e a conectividade. As *smart cities* podem assim transformar modelos operacionais e verificar a sua viabilidade, vulnerabilidade e aceitabilidade de cada nova operação.

Nam & Pardo (2011) apresentam a conceptualização da *smart city* nas dimensões de tecnologia, pessoas e instituições, através dos princípios estratégicos como a integração das infraestruturas e serviços de mediação tecnológica, a aprendizagem social para a consolidação da infraestrutura humana, a governança para a melhoria institucional e o envolvimento dos cidadãos.

Benevolo, Dameri, & D'Auria (2016) analisam as iniciativas de mobilidade "inteligente" como parte da *smart city*, e investigam o papel das TICs no apoio a ações de mobilidade "inteligentes", o impacto na qualidade de vida dos cidadãos e o Valor criado para a cidade como um todo.

Grave (2016) refere o papel essencial do comprometimento das partes interessadas nos diversos projetos de *smart cities*. O compromisso baseia-se em explorar dados e informações como conhecimento, em adotar tecnologia e inovação como vantagem competitiva, em incorporar o planeamento e a metodologia de projeto, através da responsabilização transorganizacional, em ter a abordagem de liderança coletiva e reforçar a mudança individual, em promover a relação transinformacional, em usar a educação para a inclusão e em orientar a sustentabilidade na melhoria da qualidade de vida.

Dameri (2012) procura uma proposta abrangente para a definição de *smart city* dado que o significado atribuído a esta expressão parte ainda da experiência empírica e não de estudos teóricos sistémicos para a implementação efetiva da *smart city*, capaz de criar Valor público, bem-estar para os cidadãos e sustentabilidade ambiental. O conceito de cidade "inteligente" é usado para identificar um amplo espectro de soluções heterogéneas e programas municipais, envolvendo diferentes tipos de tecnologias e visando alcançar um conjunto muito grande de objetivos diferentes e não bem definidos. Estes termos são usados de forma diferente para definir projetos e soluções semelhantes, atribuídas à ideia de uma *smart city*.

A definição de *smart city* será baseada no espaço físico, cidadãos, tecnologia e governança, através do digital, da sustentabilidade, da inclusão e da democracia, com

limites e dimensões diversas, com objetivos bem definidos e mensuráveis de sustentabilidade ambiental, de criação de capital intelectual inteligente, da participação dos cidadãos e do bem-estar.

Nesta perspetiva de Dameri apresenta-se a seguinte definição de *smart city*:

> "Uma *smart city* é uma área geográfica bem definida, na qual tecnologias, como TICs, *log*ística, produção de energia e assim por diante, cooperam para criar benefícios para os cidadãos em termos de bem-estar, inclusão e participação, qualidade ambiental, desenvolvimento "inteligente", e é governada por um conjunto bem definido de sujeitos, capaz de definir as regras e políticas para o governo e o desenvolvimento da cidade."
>
> (Dameri, 2012)

Revendo as diversas perspetivas do conceito de *smart city*, podemos definir, em resumo, a *smart city* como um espaço multidimensional e multifuncional, visto como um ecossistema global e "inteligente", sensorizado em *IoT* e organizado em ecossistemas funcionais que agrupam domínios aplicacionais, que se relacionam e integram, como uma ampliação dos espaços e das comunidades, que envolve todo o espaço físico e digital, focado no cidadão, envolvendo a participação e o *feedback,* para compatibilizar as necessidades do cidadão com as politicas publicas sustentáveis.

1.2. Modelos de *smart city*

Como resultado de processos de sistematização e modelização das *smart cities* surgem diversos trabalhos que procuram responder a este desafio de definir modelos para as *smart cities.*

Dustdar, Nastic, & Scekic (2016) apresentam uma visão da cidade cibernética "inteligente", baseada na arquitetura de valores, que caracterizam as atividades coordenadas complexas que envolvem os serviços da cidade, as partes interessadas e os dispositivos "inteligentes", centrado nos cidadãos, que promove a participação e não a passividade. Nesta visão define um conjunto de capacitadores-chave como: as atividades coordenadas complexas, os incentivos como mecanismos de controlo flexível e do abastecimento, e a governança com base na infraestrutura de serviços públicos. Além de definir princípios e requisitos de *design* para cidades do futuro e como realizar uma plataforma abrangente.

Colding & Barthel (2017), usando uma perspetiva de ecologia urbana, refletem sobre os modelos de *smart city* com o objetivo de aumentar a sustentabilidade urbana, a

sustentabilidade social, de saúde, de resiliência e segurança cibernética, que podem afetar a autonomia da governança urbana, a integridade pessoal e a resiliência das infraestruturas que fornecem aos habitantes as necessidades básicas, e como os desenvolvimentos das *smart cities* podem mudar as relações do homem com a natureza.

Amorim (2016) apresenta a modelação da informação da cidade (*CIM-City Information Modeling*) onde lista os fatores essenciais para a implementação do *CIM* análogo ao paradigma *BIM* (*Building Information Modeling*) e complementar ao conceito de *smart city*. Os recursos utilizados pelas ferramentas *GIS* (*Geographic Information Systems*), o padrão *CityGML* (*City Geography Markup Language*) e o padrão *IFC* (*Industry Foundation Classes*) que permitem a identificação, a projeção, a simulação, a monitorização e a gestão urbana. Este modelo *CIM* deve considerar os conceitos de planeamento, projeto, construção, operação e manutenção. O modelo de informação conceptual deve mapear objetos e processos, e a implementação com a codificação de estruturas de dados que deve ser capaz de representar os diferentes tipos de objetos, as suas geometrias, propriedades, relações e estados, através da partilha, interoperabilidade, confiabilidade e segurança.

Rathore, Ahmad, Paul, & Rho (2016), no âmbito do planeamento urbano e construção de *smart cities* baseados em *IoT* e análise de *big data*, propõem uma arquitetura de 4 camadas: Camada 1 - Camada inferior: responsável pelas fontes de *IoT*, geração de dados e coleções; Camada 2 - Camada intermedia I: responsável para todos os tipos de comunicação entre os sensores, relés, estações de base, Internet, etc.; Camada 3 - Camada intermedia II: responsável pela gestão de dados e processamento usando estrutura *Hadoop*[6] ; e Camada 4 - Camada superior: responsável pela aplicação e uso da análise de dados e dos resultados obtidos. O sistema consiste na geração de dados, a recolha, a agregação, a filtração, a classificação, o pré-processamento, a computação e a tomada de decisão.

Ghannem, Hamdi, Abdelmoez, & Ammar (2015) apresentam um processo de desenvolvimento e uma abordagem de modelação para a construção do modelo de contexto ambiental através da metodologia *RE-CAWAR* (*Requirement Engineering*

[6] Hadoop - https://hadoop.apache.org, acedido em 21-05-2019

Context Awareness), orientada pelo modelo de contexto ambiental, onde a dimensão ambiental é a dimensão com o maior impacto nas mudanças num contexto dinâmico.

Abella, Ortiz-de-Urbina-Criado, & De-Pablos-Heredero (2017) apresentam um modelo para a análise da inovação baseada em dados e na geração de Valor nos ecossistemas das *smart cities.* O modelo trabalha em três etapas: ajusta a divulgação de dados pela *smart city* com dimensões que construem dados atraentes e reutilizáveis, analisa os mecanismos para criar produtos e serviços inovadores e explica como esses produtos e serviços podem afetar a sociedade.

Ceballos & Larios (2016) propõem um modelo para aumentar a participação dos cidadãos e apoiar o desenvolvimento do plano principal da *smart city*, adaptando o modelo de Kano (Kano et al., 1984) com base nos *KPIs* (*Key Performance Indicator)* (Cohen, 2013) e a norma ISO 37120 (ISO 37120, 2014) para sentir a perceção dos cidadãos. A Tabela II.1, adaptado da tabela 1, de Ceballos & Larios (2016), apresenta a comparação entre estes dois modelos de métricas das *smart cities*. O modelo de circulo das *smart cities* de Boyd Cohen reconhece seis KPIs para classificar uma *smart city* e a ISO 37120 inclui 17 medidas-chave:

Tabela II.1 - Comparação de dois modelos de métricas das *smart cities*

Circulo das *smart cities*	ISO 37120
Economia "inteligente" - *Smart Economy*	Economia
	Finança
Ambiente "inteligente" - *Smart Environment*	Energia
	Meio Ambiente
	Lixo sólido
	Águas residuais
	Água e Sanitários
Viver "inteligente" *Smart Living*	Resposta de Incêndio e Emergência
	Saúde
	Segurança
	Abrigo/habitação
Mobilidade "inteligente" - *Smart Mobility*	Telecomunicações e Inovação
	Transporte
	Planeamento urbano
Pessoas "inteligentes" - *Smart People*	Educação
	Lazer
Governo "inteligente" - *Smart Government*	Governança

Adaptada da tabela 1, de Ceballos & Larios (2016)

Wei, Huang, Li, & Xie (2016) apresentam um modelo de avaliação de Capacidade de Carga Urbano (*UCC-Urban Carrying Capacity*) como base para melhorar a sustentabilidade urbana. O quadro integrado analítico de *UCC*, Tabela II.2, adaptado da tabela 5 de Wei, Huang, Li, & Xie (2016), de 30 indicadores representativos da literatura, é apresentado de seguida e foi aplicado a megacidades na China, com as ponderações indicadas (Peso1, Peso2 e Peso3):

Tabela II.2 - Sistema de indicadores por sistema e área de avaliação, ponderado

Setor	**Peso1**	**Áreas de avaliação**	**Peso2**	**Indicadores**	**Peso3**
Económica	17,60%	Emprego	3,40%	X1 Urbana taxa de desemprego registado (%)	3,40%
		Afluência	7,00%	X2-Rendimento disponível das famílias urbanas per capita	3,70%
				X3-Receita Fiscal per capita (Euro)	3,30%
		Escala Económica	3,80%	X4-PIB per capita (Euro)	3,80%
		Crescimento	3,40%	X5-Taxa de crescimento do PIB anual	3,40%
Recursos	17,90%	Água	7,40%	X6-Abastecimento de água per capita (ton)	3,00%
				X7-Consumo doméstico de água diária per capita (litros)	4,40%
		Terra	3,70%	X8-Terra construtiva per capita (m2)	3,70%
		Energia	6,80%	X9-Fornecimento de gás per capita (m3)	3,10%
				X10-Consumo nacional de energia elétrica per capita(kWh)	3,70%
Ambiental	25,80%	Poluição	6,80%	X11-Descarregada de águas residuais industriais por 10 mil Euros do PIB (tonelada)	3,90%
				X12-Emissões industriais de CO2 por 10 mil Euros do PIB (kg)	2,90%
		Tratamento	13,30%	X13-A proporção de resíduos industriais sólidos que é utilizado de forma abrangente	4,00%
				X14- A proporção de águas residuais tratadas (%)	3,40%
				X15-Taxa de tratamento de lixo urbano	2,90%
				X16-O número de dias com a qualidade do ar acima da classe 2-padrão por ano	3,00%
		Espaço Verde	5,70%	X17-Área verde per capita (m2)	2,50%
				X18-Taxa de cobertura verde das áreas edificadas urbanas (%)	3,20%
Infraestrutura	38,60%	Saúde	2,90%	X19-Número de leitos hospitalares por 10.000 pessoas	2,90%
		Habitação	3,40%	X20-Espaço per capita de moradores urbanos (m2)	3,40%
		Serviços de utilidade pública	10,40%	X21-A densidade do tubo de drenagem em áreas urbanas (km / km2)	2,90%
				X22-T+I6axa de acesso à água (%)+I21	3,70%
				X23-Taxa de acesso ao gás (%)	3,80%
		Comunicação	9,20%	X24-Número de Internet por 10.000 pessoas (utilizador)	3,00%
				X25-Número de utilizadores de telemóveis por 10.000 pessoas (utilizador)	2,70%
				X26-Número de utilizadores de telefonia fixa por 10.000 pessoas (utilizador)	3,50%
		Transporte	12,70%	X27-Número de barramento por 10.000 pessoas (unidade)	3,10%
				X28-Número de carros particulares por 10.000 pessoas (unidade)	3,10%
				X29-Áreas de estradas urbanas per capita (m2)	3,60%
				X30-Densidade de estradas (km / km2)	2,90%

Adaptada da tabela 5, de Wei, Huang, Li, & Xie (2016)

Chilipirea, Petre, Groza, Dobre, & Pop (2017) apresentam uma arquitetura integrada orientada ao fluxo de dados, desde a origem ao utilizador final, para as *smart cities*, com etapas de processamento de dados, com a recolha de fontes heterogéneas, a normalização, a intermediação, o armazenamento, análise, visualização e a entrega aos serviços ou a aplicações ou a sistemas de apoio à decisão.

Lee, Phaal, & Lee (2013) apresentam um roteiro (*roadmap*), aplicando o método *QFD* (*Quality Function Deployment*), para estabelecer interligações entre serviços e dispositivos, e entre os dispositivos e tecnologias, integrando serviços, dispositivos e tecnologias capazes de implementar um projeto "inteligente" de desenvolvimento da cidade. A Tabela II.3, adaptada da tabela 8, Lee, Phaal, & Lee (2013) sugere as categorias de deteção, processamento rede, interface e segurança.

Tabela II.3 - *Smart city* padrão de classificação de tecnologia

Categoria	Definição
Deteção	Monitorar qualquer mudança externa do estado e transmitir os dados recolhidos para processar e responder a sinais de sensores
Processamento	Tratar os dados de processo a partir de sensores de acordo com uma análise, conduzindo a uma decisão racional
Rede	Ligar cada dispositivo e utilizador para apoiar a comunicação eficiente
Interface	Converter a informação que flui entre dispositivos ou entre utilizadores e aparelhos para uma forma mais inteligível (gráfica, estrutural)
Segurança	Controlar o acesso ilegal a informações de utilizadores ou instalações ao longo de todo o ambiente "inteligente" e proteger a privacidade pessoal

Adaptada da tabela 8, de Lee, Phaal, & Lee (2013)

Badii et al. (2017) concluíram que as soluções de smart cities tendem a transformar os dados em serviços, para os utilizadores e operadores da cidade, através da exploração de soluções de dados e da análise de dados cujos serviços integram dados abertos e privados, dados estáticos e em tempo real de entidades públicas e de operadores privados. As API´s (*Application Program Interfaces*) da *smart city*, dependendo das soluções de arquitetura escolhidas, para passar de dados a serviços, permitem diferentes funcionalidades, como a exploração de dados agregados e tratados por algoritmos, para a produção de serviços.

A Tabela II.4, resumida da tabela 1, de Badii et al. (2017), para diferentes soluções "inteligentes" da cidade, para passar de dados para serviços, pode ser aplicada aos casos do integrador de informações, do agregador de dados e metadados e do agregador semântico e raciocinador, limitada à interoperabilidade de dados entre as entidades da

cidade, em: tempo, espaço, vários domínios (semântica interoperável), estruturas, serviços e relacionamentos.

Tabela II.4 - Soluções "inteligentes" da cidade para passar de dados para serviços.

Soluções de *smart cities* para passar de dados para serviços
Endereçando dados abertos (*open data*)
Endereçando dados privados
Endereçando dados em tempo real
Endereçando serviços interoperáveis
Recolha de dados empurrando (*Push*)
Recolha de dados puxando (*Pull*)
Fornecendo pesquisa de dados
Fornecendo pesquisa de metadados
Fornecendo raciocínio espacial
Fornecendo raciocínio de tempo
Fornecendo acesso autenticado integrado aos dados
Fornecendo dados / serviços interoperáveis sintáticos
Fornecendo dados / serviços interoperáveis semânticos
Independente de *API* das alterações no modelo de dados
Fornecendo *API REST* nos dados
Fornecendo *API SPARQL* em dados
Fornecendo suporte de inferência em dados
Fornecendo visualização de dados (*business intelligence*, *dashboarding*)
Fornecendo suporte à tomada de decisões

Adaptada da tabela 1, de Badii et al. (2017)

A Tabela II.5, resumida da tabela 3, de Badii et al. (2017) apresenta os domínios de *front-ends* de *APIs* de *smart cities* para fornecer serviços para aplicações "inteligentes" da gestão da cidade, e para aplicações *web* e móveis (*mobile*).

Tabela II.5 - Soluções de APIs de *smart city*

Domínios de *front-ends* de APIs de *smart city*
API: Serviço de Pesquisa
(*GPS API*) pesquisa de texto completo
(*API GPS*) Pesquisa em torno de um ponto de *GPS*
(*GPS API*) Obter a localização de *GPS*
(*Location API*) Pesquisar ao longo de uma linha, um polígono
(*Location API*) Pesquisar numa área, uma forma fechada
(*Location API*) Pesquise rua, região, município, etc.
API: Mobilidade
Obter Transporte Público, pontos de autocarro, linhas, e cronograma
Obter atraso de tempo real de autocarros públicos oi de outros modos de transporte
Obter o estado do tráfego fluido
Obter o estado do estacionamento
Obter estado dos preços nos postos de combustível
Obter local e a rota do veículo (Atual: Latitude, Longitude | *POI*; Destino: Latitude, Longitude | *POI*)
Obter um encaminhamento intermodal

Domínios de *front-ends* de APIs de *smart city*
Obter uma bilhética integrada
Obter uma rota para uma boa entrega (planeamento multi-paragem)
API: Meio Ambiente, sensores e atuadores, *IoT*, saúde
Obter estruturas de saúde (hospitais, médicos, etc.)
Obter o estado de primeiros socorros
Obter Previsão
Obter Sensor / Valor do Atuador / Estado
Obter a poluição, a temperatura, a polinização, etc.
API: A participação do utilizador e consciencialização
Obtenha informações sobre a monitorização de *social media*
Salvar os comentários fornecidos pela multidão (*crowd sourcing*) por serviço
Salvar os votos e o média fornecidos pela multidão (*crowd sourcing*) por serviço
Obter / Definir estado do painel de mensagem variável por local
(EVENTO *API*) Obter eventos da cidade / área (hoje em dia, semana e mês)
API: Assistente pessoal (compromisso + recomendação)
Salvar Perfil do utilizador
Obter sugestões à medida (*on demand*)
Obter informações sonoras, informações, compromissos
Receba as notícias de proteção civil (*in push*)
Salvar o estado dos sensores móveis
API: Domínios de Serviços Georreferenciados
API: Tipo de Chamada (JSON e / ou HTML)
Consulta SPARQL (*SPARQL Query*)
Consulta SPARQL com inferência (SPARQL *Query with Inference*)
REST
Consulta ID (*Query* ID)
API para recursos não funcionais
Autenticação direta da *API*
Autenticação de *API* via social média
Controlo de licenciamento de dados

Adaptada da tabela 3, de Badii et al. (2017)

Bellini, Nesi, & Pantaleo (2015) relataram um estudo comparativo de aferição de repositórios das *frameworks* de modelação e descrição de informação (*RDF-Resource Description Framework*) para os serviços das *smart cities* com base em suas principais características do SPARQL[7]. O *RDF*[8] é uma *framework* para modelação e descrição de informação, rotulado e direcionado para representar informações na Web. As *RDF store*[9] analisados foram as seguintes: Virtuoso[10], GraphDB[11], Blazegraph[12], CumulusRDF[13], Stardog[14] e o Strabon[15]. A proposta de referência da *smart city RDF* [16] teve por base a

[7] SPARQL - http://www.w3.org/TR/sparql11-query/ , acedido em 12-03-2019
[8] RDF - https://www.w3.org/RDF/ , acedido em 12-03-2019
[9] *RDF store* - https://db-engines.com/en/article/RDF+Stores , acedido em 12-03-2019
[10] Virtuoso - https://virtuoso.openlinksw.com/rdf-quad-store/ , acedido em 13-03-2019
[11] GraphDB - http://graphdb.ontotext.com/, acedido em 13-03-2019
[12] Blazegraph - https://www.blazegraph.com/, acedido em 13-03-2019
[13] CumulusRDF - https://www.w3.org/2001/sw/wiki/CumulusRDF, acedido em 13-03-2019
[14] Stardog - https://www.stardog.com/, acedido em 13-03-2019
[15] Strabon - http://www.strabon.di.uoa.gr/, acedido em 13-03-2019
[16] *smart city RDF* - http://www.disit.org/smartcityrdfbenchmark, acedido em 14-03-2019

Florença smart city acessível como Km4City[17]. O modelo de avaliação pretendeu validar se as *RDF stores* são adequados para a modelação da *smart city* e a sua aplicação. As *RDF stores* podem ser usadas para integrar os dados de várias origens e as aplicações utilizam esses dados para fornecer novos serviços aos cidadãos e à gestão publica.

Anthopoulos, Janssen, & Weerakkody (2015) compararam *smart cities* com diferentes modelos, através da sistematização dos métodos de modelação e de *benchmarking*. Estabeleceram quais as dimensões comuns, as pessoas, o governo, a economia, a mobilidade, o ambiente e a vivência.

A Tabela II.6, adaptada de tabela 1 de Anthopoulos, Janssen, & Weerakkody (2015) apresenta as diferentes abordagens de modelação das *smart cities*:

Tabela II.6 - Abordagens de modelação das *smart cities*

Fonte	Modelo	Descrição
(Söderström et al., 2014)	Modelos de nove pilares Equação da *smart city* que combina instrumentação, interconexão e "inteligência".	Planeamento, serviços de gestão de serviços de infraestrutura e serviços humanos Instrumentação (a transformação de fenómenos urbanos em dados) + interconexão (de dados) + "inteligência" (trazida pelo software)
(ITU-T, 2014)	*Smart city*: Indicadores Chave de Desempenho e Sustentabilidade	Sustentabilidade ambiental, produtividade, qualidade de vida, equidade e inclusão social e o desenvolvimento de infraestruturas
(UN-Habitat, 2013)	Dimensões da Prosperidade da Cidade	Produtividade e prosperidade das cidades, infraestrutura urbana: alicerce da prosperidade, qualidade de vida e prosperidade urbana, equidade e prosperidade das cidades, sustentabilidade ambiental e da prosperidade das cidades
(Anthopoulos, 2015)	Dimensões da *smart city*	Recursos, transporte, infraestrutura urbana, bem estar, governo, economia e coerência
(ISO 37120, 2014)	ISO 37120 desenvolvimento sustentável das comunidades, indicadores de serviços da cidade e qualidade de vida	Economia, educação, energia, meio ambiente, finanças, resposta ao incêndio e emergência, governança, saúde, lazer, segurança, habitação, resíduos sólidos, telecomunicações e inovação, transporte, planeamento urbano, águas residuais, água e saneamento.
(Neirotti et al., 2014)	Domínios da *smart city*	Recursos naturais e energia, transportes e mobilidade, edifícios, bem-estar, governo, economia e pessoas
BID [18]	Iniciativa Cidades Emergentes e sustentáveis (ICES) Aplicação do filtro económico para a priorização das áreas de ação	Método de decisão qualitativa de impacto económico. *Urban Dashboard* [19] - Painel Urbano que permite explorar e comparar mais de 150 indicadores quantitativos
(Lee et al., 2014)	Quadro de análises da *smart city*	Abertura urbano, inovação de serviços, parcerias, formação, pro-atividade urbana, integração de infraestrutura "inteligente" na cidade, governança da cidade "inteligente"

Adaptada de tabela 1, de Anthopoulos, Janssen, & Weerakkody (2015)

[17] Km4City - https://www.km4city.org/?devTools , acedido em 20-02-2019
[18] BID - https://www.iadb.org/es/desarrollo-urbano-y-vivienda/programa-ciudades-emergentes-y-sostenibles
[19] Urban Dashboard - http://www.urbandashboard.org/iadb/index.html , acedido em 4-04-2019

A Tabela II.7, adaptada da tabela 2 de Anthopoulos, Janssen, & Weerakkody (2015), apresenta algumas das ferramentas de avaliação das *smart cities*.

Tabela II.7 - Ferramentas de *benchmarking* da *smart city*

Fonte	Ferramenta de avaliação comparativa	Descrição
(Moreno Pires et al., 2014)	Indicadores de Desenvolvimento Sustentável Local	21 ECOXXI indicadores, agrupados nos seguintes sectores: sustentável, educação desenvolvimento, mar e costa, instituições de meio ambiente, conservação da natureza e da biodiversidade, planeamento florestal, ar, água, resíduos, energia, transportes, ruido, agricultura e turismo
(Kourtit et al., 2014)	*Global City*: Índices de medição de desempenho	Economia, pesquisa e desenvolvimento, interação cultural, qualidade de vida, meio ambiente e acessibilidade
(Desouza & Flanery, 2013)	Avaliação da Resiliência da Cidade e Quadro de Implementação	Componentes da Cidade: Recursos e processos (físico) pessoas, instituições e atividades (social)
(Cruz & Marques, 2014)	*Scorecard*: Governo Local Sustentável	Critérios sociais, económicos, ambientais e governamentais
(Singhal et al., 2013)	Parâmetros de competitividade	Ambiente físico, capital social, finanças, desenvolvimento, investimento, potencial do utilizador
UN Habitat (UGI, 2004)	Indicadores de governança urbanas	Eficácia, equidade, participação, responsabilização e segurança
(Lazaroiu & Roscia, 2012)	Modelo para calcular índices de *smart city*	Economia, mobilidade, meio ambiente, pessoas, bem-estar, governança
(Duarte et al., 2014)	Quadro de Avaliação de Cidade Digital	Conectividade, acessibilidade e comunicabilidade

Adaptada da tabela 2 de Anthopoulos, Janssen, & Weerakkody (2015)

As diversas abordagens de modelação e as ferramentas de avaliação das *smart cities* levantam várias questões quando se pretende sistematizar e identificar os testes padrão repetíveis e em que dados devem ser suportados. Quais as análises que fornecem Valor? Quais são os dados mais adequados? Como identificar as prioridades? Como maximizar o Valor para a cidade? Como alavancar as melhores práticas na cidade? Como implantar tecnologia ajustada à sua dimensão? As cidades mais "inteligentes" deverão ser cidades que antecipam os problemas para os resolver de forma proactiva e coordenada e que aproveitam as informações mais ajustadas para obter melhores decisões, com o objetivo de estimularem o crescimento económico sustentável (McNamee, 2009).

Os conceitos fundamentais do projeto de uma cidade "inteligente" encontra-se extensamente revistos e com inúmeras iniciativas. As vulnerabilidades de segurança, as questões de privacidade no contexto das *smart cities* e dos seus serviços mantêm a necessidade de aprofundamento e investigação. As TICs e a infraestrutura das cidades potenciam o objetivo de a cidade melhorar a qualidade dos serviços que presta aos cidadãos e melhorar a sua qualidade de vida (Khatoun & Zeadally, 2016). A Tabela II.8,

adaptada da tabela 2, de Khatoun & Zeadally (2016) descreve as caraterísticas de segurança cibernética orientada para os riscos do ambiente construído.

Tabela II.8 - Standards e normas de segurança e recomendações para a segurança cibernética de *smart places*

Característica	Descrição	Normas e recomendações
Organizacional	Desenvolver um plano de salvaguarda e recuperação (*backup & recover*)	Cinco Melhores Práticas para Melhorar os Sistemas de Gestão de Edifícios, Schneider Electric (Strass & Williamson, 2014)
	Gerir utilizadores e senhas	Standards IET: - Riscos de segurança cibernética no ambiente construído - Padrões, competências e aprendizagem (Boyes, 2016) - Edifícios "Inteligentes": Entendendo e gerindo os riscos de segurança (IET, 2012)
	Abrir sessões de *feedback*	Cibersegurança em edifícios "inteligentes", (*Cybersecurity in Smart Buildings*, 2015)
	Definir os *standards*, ferramentas, procedimentos de segurança e regras para a comunidade	Roteiro da Ciência de Medição para Edifícios de Energia Net-Zero (Pellegrino et al., 2010) Entendendo o risco e o investimento em infraestrutura resiliente (Gallego-Lopez & Essex, 2016)
	Desenvolver políticas relacionadas a gestão de senhas e configurações	Centros de Partilha e Análise de Informação (ISACs) - Modelos cooperativos (ENISA, 2017) Modelo do conceito padrão da *smart city* (ISO 30182: 2017) Standard sobre as diretrizes e abordagens existentes sobre desenvolvimento sustentável e resiliência nas cidades (ISO 37121: 2017)
Técnico	Fornecer segurança física para os equipamentos, cabos de rede e servidores Tráfego de rede e criptografar com algoritmos simétricos robustas, como AES e *Blowfish* [20]	ANSI / TIA-862, Edifício, Sistemas de Automação Cabeamento Padrão Guia GSA Especificação interoperável Edifício Automação e Controlo de Sistemas usando o ANSI / ASHRAE 135-1995, BACnet
	Uso de ligação segura, como uma VPN para acessos remotos	• Requisitos de segurança de edifícios "inteligentes" baseados em Internet das coisas usando serviços Web RESTful (Niemeyer et al., 2014)
	Segurar a rede sem fio com protocolo WPA2 *IDS Deploy* na construção Usar autenticação através de servidor centralizado autorização e contabilidade (AAA) como um servidor RADIUS Implantar uma *firewall* em cada ponto de transição	• Agência Federal BSI[21] de Segurança da Informação

[20] Blowfish- https://www.schneier.com/academic/blowfish/ , acedido em 5-04-2019
[21] BSI - https://www.bsi.bund.de/EN/Home/home_node.html , acedido em 5-04-2019

Característica	Descrição	Normas e recomendações
	Implantar uma *firewall* em cada ponto de transição Implantar uma *firewall* em cada ponto de transição Usar métodos de autenticação fortes, tais como cartões biométricos ou "inteligentes"	
Recursos Humanos	Programa de formação abrangente para programadores e administradores de sistemas. Informar e sensibilizar para as questões de segurança Utilizadores chave de alerta e aconselhamento onde há ameaças Planos de continuidade para garantir a recuperação de desastres	Framework ISO 27001 Cidadão Ciberseguro[22] Recomendação de deteção de intrusões UC *Berkeley security policy-guideline*[23]) ISO 22301 - *Business continuity*
Legal	Respeitar aspetos jurídicos da segurança Usar as normas de segurança e recomendações da cibersegurança nacional, de agências e de atores de segurança de TI para acompanhamento Boas práticas de utilização das TIC Controlo e performance Proteção de dados pessoais	Lei n.º 46/2018, de 13 de agosto - Regime Jurídico de Segurança do Ciberespaço ISO/IEC 27001 - Standard para sistema de gestão da segurança da informação Diretiva NIS *(Network and Information Security Directive*) relativa à segurança das redes e da informação (EU) 2016/1148 ITIL - Melhores práticas (Alter, 2015) COBIT - Objetivos de Controlo de Informações e Tecnologias Relacionadas Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, Regulamento Geral sobre a Proteção de Dados (RGPD)

Adaptada da tabela 2, de Khatoun & Zeadally (2016)

As *smart cities*, como grandes consumidores e produtores de dados, apresentam desafios de segurança de dados. A conectividade transforma as *smart cities* em ambientes complexos em que a análise de segurança tradicional não é suficiente sendo necessário adicionar requisitos de segurança de dados específicos e novas soluções. O quadro de quatro camadas apresentado por Popescul & Radu (2016) elenca os elementos críticos para o funcionamento da *smart city*: coisas "inteligentes", espaços "inteligentes", sistemas "inteligentes" e cidadãos "inteligentes".

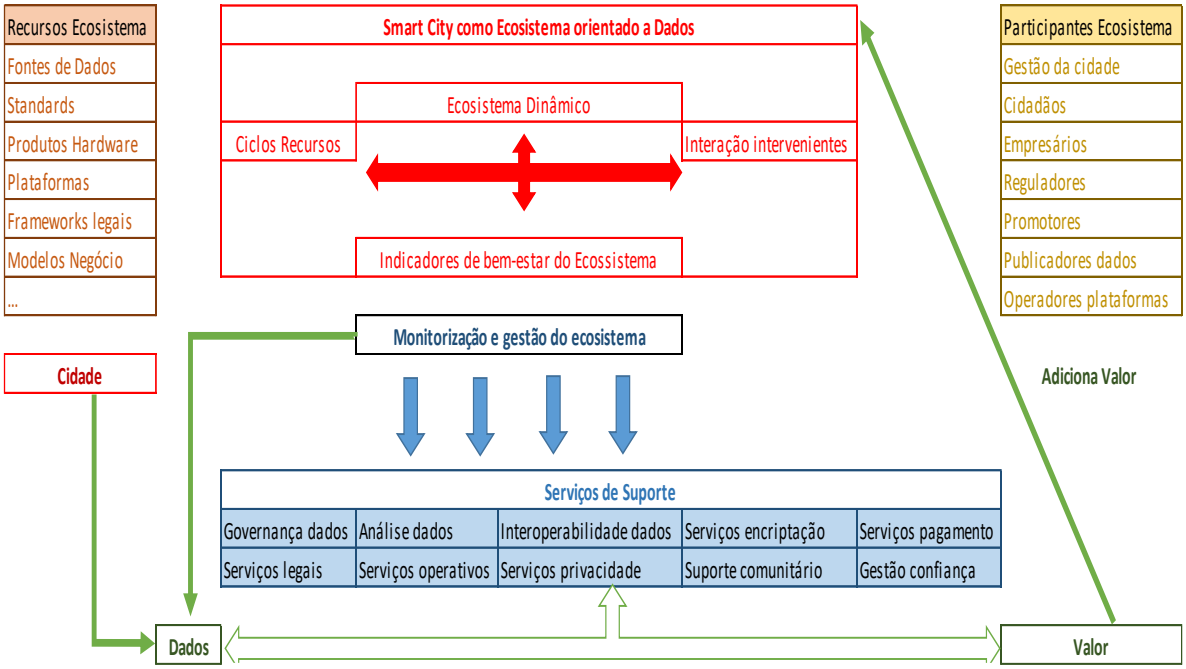
Os ecossistemas orientados aos dados suportados em *IoT* necessitam de recolha de dados confiável como resultado da comunicação e da interação dos ecossistemas naturais. As análises são um pré-requisito fundamental para a "inteligência" urbana. A *smart city*

[22] CNCS - https://lms.nau.edu.pt/courses/course-v1:CNCS+CC101+2018_T1/about , acedido em 5-07-2019
[23] UC Berkeley security policy - https://security.berkeley.edu/intrusion-detection-guideline , acedido em 5-04-2019

depende da capacidade de traduzir os dados da *IoT* em serviços úteis e inovadores. (Dhungana et al., 2016).

A Figura II.1, adaptada da figura 1, de Dhungana et al. (2016), traduz a *smart city* como ecossistemas dinâmicos orientados aos dados.

Figura II.1 - Visão global do Ecossistema orientado por Dados e seus componentes



Adaptada da figura 1, de Dhungana et al. (2016)

Esta figura sintetiza os recursos, os participantes, os serviços de suporte ao ecossistema da *smart city* orientado aos dados. A monitorização e gestão do ecossistema permite que a cidade, através dos dados, adicione Valor, que "alimenta" os ciclos de recursos e a interação dos intervenientes da *smart city*, de forma dinâmica e medível através dos indicadores de bem-estar do ecossistema.

As cidades consomem 75% da produção mundial de energia e geram 80% das emissões de CO2. O modelo para calcular os índices da "*smart city*" revelam que os indicadores escolhidos não são homogéneos e têm pesos diferentes. Os indicadores são os considerados na Tabela II.9, adaptado da tabela 1, de Lazaroiu & Roscia (2012), para uma compreensão mais alargada e de uso simples, para o processo de formulação de políticas e medidas de adoção e a sua avaliação. (Lazaroiu & Roscia, 2012)

Tabela II.9 - Indicadores da *smart city*

Lista de Indicadores
1. Poluição.
2. Capacidades inovadoras

Lista de Indicadores
3. CO2
4. Governação transparente
5. Gestão sustentável de recursos
6. Separação de lixos
7. Instalações educativas
8. Condições de saúde.
9. Transporte público sustentável, inovador e seguro
10. Áreas pedonais
11. Ciclovias
12. Áreas verdes
13. Produção de resíduos sólidos urbanos
14. GWh doméstico
15. Combustíveis
16. Estratégias políticas e perspetivas
17. Disponibilidade das infraestruturas TIC
18. A flexibilidade do mercado de trabalho

Adaptado da tabela 1, de Lazaroiu & Roscia (2012)

Esta tabela permite identificar a lista de indicadores quantificáveis que poderão fornecer a evolução histórica e quantificar o impacto das intervenções realizadas neste espaço, como as alterações de politicas, de investimento público, de regulamentação ambiental e social, de entre outras.

A dinâmica económica das *smart cities* encontra-se desenvolvida num modelo da dinâmica de sistemas de uma cidade, como um complexo e adaptativo sistema de sistemas unificando as abordagens para o Produto Interno Bruto da Cidade, através de um "pensamento de sistema" para os decisores políticos. (Hennessy et al., 2011)

O uso de algoritmos, projetados para explorar o conhecimento dos agentes combinados, que precisam cooperar e integrar as suas informações, para fornecer serviços avançados para os utilizadores da *smart city* e para garantir a interoperabilidade dos diferentes agentes, necessitam de consolidar diferentes e heterogéneas ontologias que se unificam através de técnicas de ontologia correspondentes, para melhorar os resultados e fornecer os resultados mais precisos possíveis. (Otero-Cerdeira et al., 2014)

O papel da academia, como *smart place* inserido nas *smart cities*, também é destacado no trabalho de Coccoli, Maresca, Stanganelli, & Guercio (2015) que apresentam um modelo de universidade, mais "inteligente" e baseado num modelo de *smart city*, através de um estudo de caso de colaboração entre a indústria e a universidade, com soluções "inteligentes" para melhorar a eficácia do ensino superior.

Em síntese, os modelos de *smart city* multiplicam-se e complementam-se tendo como aspetos comuns a necessidade de subdividir a *smart city* em ecossistemas que se

interagem e se integram, de implementar indicadores de avaliação ponderados e de considerar como principais dimensões as pessoas, as instituições e a tecnologia.

Esta perspetiva dos ecossistemas orientados aos dados, que agrupam funções e domínios aplicacionais, refletem o entendimento resultante desta pesquisa, sobre a visão dos *smart places*, as *smart cities*, como espaços físicos que se desmaterializam em ecossistemas de dados, agrupando domínios aplicacionais com caraterísticas de interdependência e de grupos de dados semelhantes, submetidos à governança de uma Organização, que gere, controla e define as politicas centradas no bem-estar do cidadão e na sustentabilidade ambiental, social e económica.

1.3. *Smart cities* e a *IoT* (*Internet of Things)*

A *IoT* é central no desenvolvimento das *smart cities*, podendo mesmo dizer-se que sem a *IoT* não existiria uma cidade que se "conhece", que "aprende", que se "controla" e que permite sustentadamente alterar as suas politicas ajustando as suas práticas, a colaboração, a participação para obter melhor qualidade de vidas, mais desenvolvimento e socialmente integradora.

Os benefícios de combinar o *blockchain* com *IoT* é apresentado por Marr (2018), a partir da ideia de construir máquinas "inteligentes" capazes de comunicar e operar através de *blockchain,* pode resolver quatro questões: a supervisão, o uso de criptografia e armazenamento distribuído, as facilidades do *smart contract* e a segurança geral do ambiente de *IoT*.

A *smart city* através da *IoT* permite consolidar o governança imaginada, urbana e universal, e áreas urbanas "inteligentes", procurando integrar redes sociais com soluções *IoT*, inovar com tecnologias *IoT* verdes e soluções de *middleware IoT* com conhecimento de contexto, e utilizar técnicas de inteligência artificial para recriar e combinar *IoT* com *cloud computing*. (Mali & Kanwade, 2016)

Harrison & Donnelly (2011) referem que a instrumentação das *smart cities* é um aspeto chave nas novas teorias sobre as cidades, o que permite considerar quadros teóricos ao nível de ações individuais e não depender de abstrações estatísticas para a compreensão do que está a acontecer. Esta visão é multidisciplinar e contribuí para a arquitetura, o planeamento, a engenharia, a construção, a operação e a governança das cidades, que "torna o invisível visível".

A crescente implantação e em grande escala de tecnologias da *IoT* na *smart city* procura obter operações monitorizadas para tornar a cidade mais eficiente e melhorar a qualidade de vida dos habitantes da cidade. Este objetivo deve basear-se numa arquitetura de *IoT* segura para evitar ataques cibernéticos que podem comprometer as principais funções da cidade, aceder indevidamente aos dados pessoais e provocar graves danos. A arquitetura apresentada por Chakrabarty & Engels (2016) contem quatro blocos básicos de *IoT*: a rede negra (*Black Networks*) que criptografa a carga útil e os metadados dentro de uma comunicação da camada de *link* do protocolo *IoT*, controladores *Trusted SDN* (*Software Defined Networking*) que gerem e orquestram o fluxo de comunicação entre os nós *IoT* e a restante infraestrutura de rede; o registo unificado para consolidar as tecnologias heterogéneas; e os sistema de gestão de chaves (*KMS-Key Management System*) para gerar, distribuir, armazenar, revogar, alterar e usar chaves.

Petrolo, Loscrì, & Mitton (2017) apresentam a visão da *smart city* como nuvem de coisas (*CoT-Cloud of Things*) através dos sensores em nuvem como ponte para as *IoT*. As coisas são os principias requisitos para a integração de diferentes ecossistemas de *IoT* dentro da Nuvem.

Chowdhary & Deep Kaur (2016) caraterizam os modelos de mobilidade *IoV* (*Internet of Vehicles*), como parte da *IoT*, numa *smart city*. Para tal simula a *VANETs* (*Veiculares Adhoc Networks*), com diversos parâmetros de configuração, criando vários cenários próximos dos movimentos reais dos nós, sob vários modelos de mobilidade heterogéneos.

Noutra perspetiva, é analisada uma *smart home* que se pode multiplicar no ambiente urbano, em que que a *IoT*, com as suas aplicações no ambiente muito próximo e individual de vida das pessoas e das famílias, analisa uma casa conectada que interliga os dispositivos digitais entre si e através da internet, com as comunicações ativadas por diferentes protocolos, sendo necessário orientar para standards de conectividade na rede da casa "inteligente". (Samuel, 2016)

Nitti, Pilloni, Giusto, & Popescu (2017) apresentam uma arquitetura *IoT* para uma aplicação de turismo sustentável numa cidade de ambiente "inteligente", em que o *IoT* é a chave tecnológica para o desenvolvimento de ambientes urbanos "inteligentes" com a utilização de dados agregados, integrados numa única plataforma de decisão. A arquitetura pretende otimizar o movimento de navios de cruzeiro de turistas na cidade de

Cagliari, Itália, utilizando informações de transporte, de fila de tempos de espera, de pontos de interesse, de dados de transporte real e um algoritmo de otimização.

A arquiteturas *IoT* são de serviço preferencialmente centralizado e começam a estar centradas no utilizador, com os dispositivos móveis. As arquiteturas centradas no utilizador, para os utilizadores finais, tornam a cidade num "corpo inteligente" suportada na Internet para fornecer serviços, onde as questões da privacidade do utilizador e de segurança são centrais. (Shaikh et al., 2016)

A abordagem da *smart city*, com sensores e atuadores sobre uma infraestrutura de comunicação dinâmica e *performance*, que envolve a integração e correlação de dados e informações vindas de diferentes fontes e áreas, pode otimizar a gestão ativa com a utilização de uma rede heterogénea, com várias tecnologias, suportada numa plataforma modular e para diferentes fluxos de dados. (Rinaldi et al., 2017)

A utilização de duma infraestrutura *IoT* para criar um "laboratório vivo" pode promover a poupança de energia e a sustentabilidade ambiental e revela desafios e oportunidades para o desenvolvimento de edifícios e cidades "inteligentes", em conformidade, com as expectativas de saúde e segurança ou com as normas e as políticas organizacionais. (Bates & Friday, 2017)

Psomakelis et al. (2016) apresentam uma arquitetura orientada a serviços *SOA* (*Service Oriented Architecture*), na plataforma RADICAL, para a recuperação e análise de grandes conjuntos de dados provenientes de sites de redes sociais e *IoT*, recolhidos por aplicações da *smart city* e por serviços de agregação de dados, através de uma infraestrutura de *smart city* inovadora, que agrega e combina de forma uniforme o *big data* social e a *IoT*, para permitir a eficiência de técnicas de análise de "sentimento", para reduzir o tempo de registo, recuperação, atualização e processamento e utilizar técnicas de armazenamento para a representação da frequência, no contexto da análise de sentimento em *big data* e para a melhor abordagem algorítmica do mapeamento dimensional.

O objetivo da *smart city* baseada em *IoT* é projetar e implantar soluções "inteligentes" da cidade, replicáveis, escaláveis e sustentáveis, e a adoção de um quadro de consenso. Outro objetivo dos projetos de *smart cities* do futuro será o de ter uma rede de comunicações *IoT* distribuída, como uma infraestrutura para a implantação de soluções partilháveis e replicáveis das *smart cities*. (Rhee, 2016)

Latre et al. (2016) apresentam para a cidade das coisas (*City of Things*) um laboratório de testes integrados e de tecnologia múltipla, que permite a configuração e validação de novas experiências a nível da tecnologia e do utilizador. A cidade das coisas trata-se de uma abordagem integrada, permitindo a experimentação em três camadas diferentes: redes, dados e laboratório vivo suportado numa infraestrutura de rede de tecnologia múltipla sem fios.

A cidade tente a ser mais "inteligente" e procura ser segura e preceptiva, para otimizar os recursos e melhorar a qualidade de vida do cidadão. A ligação do mundo virtual ao físico tende a levar os serviços em tempo real, baseadas na tecnologia *IoT*, a modificarem as respostas a situações reais. (Sonawane & Shaikh, 2017)

A crescente quantidade de dados gerados nas *smart cities* traz a necessidade de novas práticas e técnicas para a gestão de dados eficaz e análise, e para gerar informações que podem ajudar na utilização dos recursos de forma "inteligente" e eficaz. Rao & Syamala (2017) apresentam alguns dos serviços personalizados num ambiente de *smart city* através da modelação semântica (Uceda-Sosa et al., 2011) e a teoria Dempster-Shafer. A teoria Dempster-Shafer é uma teoria de decisão fundindo várias evidências e fontes (Luo et al., 2018)

As atividades mais estimulantes passam principalmente por integrar os serviços de *IoT* e processar de forma eficiente o *big data* para a tomada de decisões. Neste domínio o trabalho de Rathore, Paul, Ahmad, & Jeon (2017) apresenta um sistema completo, com vários tipos de sistemas "inteligentes", casa "inteligente", redes veiculares, sistema de água, estacionamento "inteligente", e objetos de vigilância, baseado em *IoT*, para o planeamento da futura *super city*, utilizando *big data analytics*. A arquitetura de suporte inclui quatro camadas e utiliza o ecossistema Hadoop[24], com programação MapReduce, em que a transferência e a computação é distribuída confiável e escalável.

A pesquisa realizada por Arasteh et al. (2016) descreve as tecnologias da *IoT* para cidades "inteligentes", os componentes principais e as características de uma *smart city* e revela que a plataforma *IoT* com outros sistemas autónomos e "inteligentes" pode fornecer aplicações "inteligentes" e de ampla disseminação e difundidos, que será uma das tendências futuras. Também apresenta os principias desafios que passam pela segurança

[24] Hadoop - https://hadoop.apache.org/ , acedido em 20-04-2019

e privacidade, a heterogeneidade, a confiabilidade, a grande escala, os aspetos legais e sociais, o *big data*, as redes de sensores e as barreiras de resposta aos pedidos (*DR-Demand Response*).

Na *Internet of Things* (*IoT*), as "coisas" ligadas à Internet fornecem uma entrada de dados e recursos que oferecem a possibilidade ilimitada de aplicações e serviços. sistemas da *smart city* suportada em *IoT* (Giang et al., 2016), também exploraram o processo de desenvolvimento de aplicações num perspetiva baseada na coordenação através de um modelo de coordenação distribuída, que supervisiona os componentes distribuídos para a construção das aplicações da *smart city* baseada em *IoT*.

Bharadwaj, Rego, & Chowdhury (2016) apresentam um sistema de gestão de resíduos sólidos da cidade de Bengaluru, Índia, como solução arquitetónica baseada em *IoT* para a automatização eficiente do processo de monitorização, recolha e gestão de resíduos sólidos. Os sensores recolhem dados dos caixotes do lixo enviados para a nuvem através da Internet utilizando o protocolo MQTT (*Message Queue Telemetry Transport*).

1.3.1. Protocolos de comunicação em *IoT*

Os protocolos standards revistos neste ponto são usados no *IoT* e na industria 4.0, e passam pelos protocolos OPC UA[25], ROS[26], DDS[27], MQTT[28] (Profanter et al., 2019), MQTT-SN[29] (Stanford-Clark & Truong, 1999), AMQP[30] e CoAP[31] (Corak et al., 2018).

O protocolos analisados são apresentados a seguir com as suas principais caraterísticas e de forma comparativa na Tabela II.10.

O OPC UA é um protocolo de comunicação *M2M* (*Machine to Machine*) para automação industrial, o ROS é um *middleware* de robótica com um conjunto de *frameworks* de software para desenvolvimento, o DDS é um protocolo de *middleware* e um padrão de *API* para conectividade de dados, o MQTT oferece flexibilidade nos padrões de comunicação e funciona como um canal para dados binários, o MQTT-SN, próximo do

[25] OPC UA - https://opcfoundation.org/about/opc-technologies/opc-ua/ , acedido em 13-05-2019.
[26] ROS - http://www.openrobotics.org/ , acedido em 13-05-2019.
[27] DDS - https://www.dds-foundation.org/ , acedido em 13-05-2019.
[28] MQTT - http://mqtt.org/ , acedido em 14-05-2019.
[29] MQTT-SN - http://www.mqtt.org/new/wp-content/uploads/2009/06/MQTT-SN_spec_v1.2.pdf , acedido em 14-05-2019.
[30] AMQP - https://www.amqp.org/ , acedido em 10-05-2019.
[31] CoAP - https://tools.ietf.org/html/rfc7252 , acedido em 10-05-2019.

MQTT, é adaptado a dispositivos com recursos limitados e com baixa largura de banda, o AMQP orienta-se à mensagem e ao encaminhamento com confiabilidade e segurança e o CoAP é projetado para a interoperabilidade com a web e projetado para aplicações M2M.

A Tabela II.10, adaptada da tabela 1, de Profanter, Tekat, Dorofeev, & Rickert (2019) resume algumas das caraterísticas dos protocolos standards usados no *IoT* e industria 4.0. Além dos protocolos analisados ainda se utilizam o XMPP[32] (*Extensible Messaging and Presence Protocol*) que se trata de um protocolo aberto, extensível, baseado em XML (*Extensible Markup Language*) através de *gateways* e o WebSocket[33] (IETF - RFC 8441) que permite a interação entre um navegador da Web e um servidor da Web com baixa carga (Corak et al., 2018).

Tabela II.10 - Comparação dos protocolos standards usados no *IoT* e industria 4.0

Protocolo	**OPC UA**	**ROS**	**DDS**	**MQTT**	**MQTT-SN**	**AMQP**	**CoAP**
Descritivo	*Open Platform Communications Unified Architecture*	*Robot Operating System*	*Data Distribution Service*	*Message Queuing Telemetry Transport*	*MQTT for Sensor networks*	*Advanced Message Queuing Protocol*	*Constrained Application Protocol*
Comunicação	TCP/IP, UDP	TCP/IP, UDP	TCP/IP, UDP	TCP/IP	UDP, não IP	TCP/IP	UDP
Padrões	RPC, Pub/Sub	RPC, Pub/Sub	(RPC), Pub/Sub	Pub/Sub	(RPC), Pub/Sub	Pub/Sub	Pub/Sub
Qualidade de Serviço	Não	Não	Sim	Sim	Não	Sim	Não
Autenticação	*User*, PKI	(Mac)	PKI	User, PKI	PKI	*User*, PKI	PKI
SSL/TLS	Sim	Não	Sim	Sim	Não	Sim	Não
Std API	Não	Não	Sim	Não	Não	Sim	Não
Standards				ISO/IEC 20922:2016 (MQTT) v3.1.1	ISO/IEC 19464 (AMQP) v1.0 OASIS (AMQP) V1.0		IETF - RFC7252
Software	open62541	ROS Melodic Morenia	eProsima Fast RTPS Opendds	Eclipse Paho. Eclipse Mosquitto, HiveMQ CE. Rabbit MQ		Rabbit MQ	coap.me contiki-os

Adaptada da tabela 1, de Profanter, Tekat, Dorofeev, & Rickert (2019)

[32] XMPP - https://xmpp.org/ acedido em 10-05-2019.
[33] WebSocket - https://tools.ietf.org/html/rfc8441 , acedido em 13-05-2019.

Esta tabela resume também algumas das plataformas mais utilizadas para permitir a comunicação multiprotocolo em ambientes *IoT*, como é o caso de Rabbit MQ[34], *broker* de mensagens, que suporta protocolos de mensagens múltiplas, confirmação de entrega, encaminhamento flexível para *queues* e trocas múltiplas.

1.4. *Big data*

O *big data* e os dados abertos criam novas oportunidades e novas ideias sobre como os cidadãos percebem a sua cidade "inteligente".

A *smart city* revela-se também com a proliferação de vários aspetos *smarts* da cidade, s*mart lighting*, *smart waste management*, *smart parking*, *smart traffic management*, *smart energy-efficient buildings* e com o aparecimento dos *smart devices* e da *smart technology*, principalmente de conectividade e comunicação.

Estes conceitos orientam-se para o aumento da eficiência e o aperfeiçoamento dos serviços, que através de *IoT* recriam aplicações para as cidades "inteligentes". Os dados gerados exigem plataformas para processar, agregar e interpretar os dados produzidos pelos dispositivos e pelas tecnologias "inteligentes".

A utilização de uma plataforma de *big data* para edifícios "inteligentes", com sistemas avançados de gestão de edifícios (*BMS-Building Management Systems*), interligados a diversos sensores e atuadores e com redes dedicadas, permite potenciar a análise de dados e o desenvolvimento de aplicações, flexibilizando a capacidade de redimensionar-se o comportamento do edifício "inteligente", atendendo aos requisitos de escalabilidade, processamento de dados, flexibilidade, interoperabilidade e privacidade. Esta perspetiva permite aplicar regras de automatização para preservar ou aumentar o conforto e economizar energia. (Linder et al., 2017)

O processo de auto-arranque (*bootstrapping*) das *smart cities*, através de um modelo autossustentável, é baseado em fluxos de dados em *big data* e no procedimento base para explorar grande quantidade de dados por meio do conceito *store API*. O objetivo é dissociar o elemento político, da manutenção tecnológica da cidade, e que de forma coerente se desenvolva um *rollout* pela cidade, por fases, em que na fase inicial, a

[34] RabbitMQ - https://www.rabbitmq.com/ , acedido em 13-05-2019.

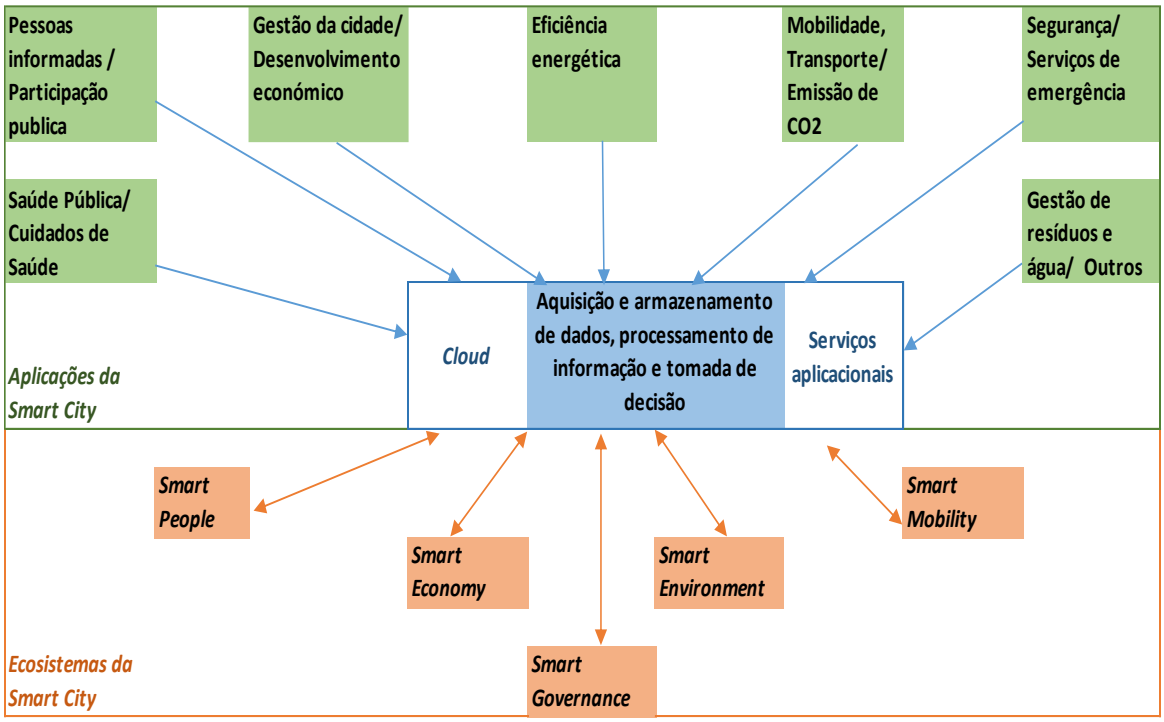
utilidade e as receitas sejam geradas, e nas fases seguintes só o serviço de utilidade é suportado e na ultima fase surja a dimensão diversão / lazer (Vilajosana et al., 2013).

Moreno et al. (2017) apresentam dois cenários de aplicabilidade das técnicas de *big data* para *smart cities* onde mostram o potencial da aplicabilidade deste tipo de técnicas para fornecer serviços rentáveis, como a gestão do consumo de energia e conforto em edifícios "inteligentes" e a deteção de perfis de viagem no transporte "inteligente".

Al Nuaimi, Al Neyadi, Mohamed, & Al-Jaroodi (2015) reveem as aplicações de *big data* para apoiar as *smart cities* e exploram as oportunidades, desafios e benefícios da incorporação de aplicações. Também tentam identificar os requisitos que suportam a implementação de aplicações de *big data* nos serviços.

A Figura II.2, adaptada da figura 1, de Khan, Anjum, & Kiani (2013), apresenta o contexto da gestão e análise de dados num ambiente *Cloud*.

Figura II.2 - Contexto de gestão e análise de dados duma *smart city*, ambiente Cloud



Adaptada da figura 1, de Khan, Anjum, & Kiani (2013)

Esta figura identifica os cinco ecossistemas da *smart city*: o *smart people*, a *smart economy*, o *smart governance*, o *smart environment* e o *smart mobility*. Estes ecossistemas agrupam aplicações ou serviços aplicacionais em *cloud*, para a aquisição e armazenamento de dados, processamento de informação e tomada de decisão. O contexto

da gestão e análise de dados em *big data* privilegiará as necessidades aplicacionais subjacentes às politicas aplicadas.

A plataforma de *analytics big data* combina técnicas de processamento de dados em lote e em tempo real e requer a utilização de algoritmos de aprendizagem sobre conjuntos de dados que são caracterizados por natureza grande, dinâmica e rápida. Na aplicação, em *smart grid*, os requisitos exigem um *framework* com poder computacional MapReduce, Stream e Iterative, utilizando o Apache Spark como plataforma integrada que combina os requisitos de processamento de dados em lote, em tempo real e iterativo, o que permite fornecer metodologias avançadas de análise e aprendizagem automática para a rede elétrica (Shyam R. et al., 2015).

A gestão de energia "inteligente" tem por base grandes quantidades de dados, com um modelo de dados, uma infraestrutura de TIC, para a recolha de dados e sua governança, para a integração de dados e a sua partilha, processamento e análise, com segurança e privacidade (Zhou et al., 2016). Esta gestão tem em consideração quatro aspetos principais: a gestão da geração de energia, a gestão de micro-redes e energia renovável, a gestão de ativos e operação colaborativa, e a gestão do lado da procura (*DSM - Demand Side Management*).

As recomendações e as práticas a serem usadas na rede "inteligente", principalmente a confiabilidade e a baixa latência, são dois objetivos em que um ambiente altamente distribuído permite gerir as grandes quantidades de dados gerados por sensores e medidores para o processamento aplicacional. (Jaradat et al., 2015)

A solução de armazenamento em nuvem dever ser capaz de armazenar grande quantidade de dados heterogéneos e fornecê-los de forma uniforme (Fazio et al., 2015). Subjacente a esta solução, apresentam uma arquitetura hibrida que combina estratégias orientadas a documentos e a objetos para otimizar o armazenamento, a consulta e a recuperação de dados.

Os desafios, da combinação da *IoT* e do *big data*, trazem negócios e tecnologias que permitem às cidades concretizar a visão, os princípios, e os requisitos das aplicações de *smart cities.* O *big data* pode permitir obter as informações valiosas e de Valor que auxiliem na tomada de decisão. (*Hash*em et al., 2016)

A aprendizagem automática (*ML-Machine Learning*) e a inteligência artificial (AI-*Artificial Intelligence*) podem alavancar a *Internet of Things* (*IoT*) e o *Big data (BD)* para

desenvolver serviços personalizados nas *smart cities*. Chin, Callaghan, & Lam (2017) avaliaram, em termos de precisão, confiabilidade e velocidade, quatro algoritmos de classificação *ML*: rede *Bayes (BN- Bayes Network)*, Naïve Bayesian (NB), o algoritmo J48 da árvore de decisão, e de vizinho mais próximo (*NN - Nearest Neighbor*), na plataforma na WEKA ML[35], correlacionando os efeitos dos dados meteorológicos (principalmente precipitação e temperatura) com as viagens curtas realizadas por ciclistas em Londres.

O Valor dos dados em grandes infraestruturas permite um planeamento urbano inteligente, sustentável e resiliente, através de uma gestão de dados mestres (*MDM-Master Data Management*). Os sistemas MDM baseiam-se em padrões de *smart cities*, modelos de conceito de *smart city*, *frameworks* de infraestrutura de comunidades "inteligentes" e tecnologias de semântica web. O objetivo será o de facilitar o intercâmbio de dados de infraestrutura para o planeamento urbano inteligente, sustentável e resiliente (Ng et al., 2017).

2. Blockchain

No âmbito deste trabalho foi realizado uma revisão sistemática da literatura, na investigação sobre a tecnologia *blockchain*, como suporte à proposta de modelo de confiança aplicado a *smart places*, apresentado em conferência (Brandão et al., 2018b). A revisão procurou respostas para as seguintes questões de pesquisa:

- Q1: Qual a evolução ao longo dos anos no número de publicações sobre *blockchain*?
- Q2: Quais as caraterísticas principais de pesquisa analisadas na pesquisa sobre *blockchain*?
- Q3: Quais as áreas de aplicação da tecnologia *blockchain*?
- Q4: Quais são as limitações na pesquisa atual na pesquisa *blockchain*?
- Q5: Quais são as futuras tendências e desafios de pesquisa para *blockchain*?

O trabalho de revisão e do estudo de ontologias adotadas permitiu em resumo obter as seguintes respostas:

[35] WEKA - https://www.cs.waikato.ac.nz/ml/weka/ , acedido em 2-04-2019

- Na seleção de documentos dos catálogos bibliográficos disponíveis foram selecionados 190 documentos para revisão, que revelam o crescente interesse do tema da tecnologia *blockchain* com a evolução de cerca de 14 documentos em 2014 para cerca de 100 já em 2017.
- Nestes documentos, verifica-se também que surgem novas aplicações em áreas embrionárias que não eram relevantes nos documentos primários. Verifica-se a predominância do sistema bitcoin com 38%, o aparecimento de outras criptomoedas com 12%, a *IoT* com 28%, o setor financeiro com 14%, a governança eletrónica com 12%, os *smart contracts* com 10%, as *smart cities* e os negócios, ambos com 9% e a saúde com 5%.
- Os temas centrais revelados passam pelas questões da segurança com cerca de 32%, confiança com cerca de 23%, privacidade e anonimato com cerca de 18% cada e a escalabilidade com cerca de 7%.

No decurso do trabalho os documentos para revisão foram sendo atualizados ao longo da elaboração de tese, com base na sua relevância para o tema da tese e tendo em consideração a ontologia definida.

A rede de *blockchain* é revelada como uma *framework* para processamento de dados descentralizada, com as características de imutabilidade e de auto-organização (W. Wang et al., 2018).

A revisão sistemática da literatura de aplicações (Casino et al., 2018) baseadas em *blockchain* identificou limitações da tecnologia *blockchain* e direções futuras a explorar em vários setores, como a cadeia de fornecimento, negócios, saúde, *IoT*, privacidade e gestão de dados. Esta tecnologia emergente apresenta problemas e desafios que passam pela adequação do *blockchain,* as questões de latência e escalabilidade (com base em atributos: confiança, contexto, desempenho e consenso), os desafios da sustentabilidade do protocolo *blockchain,* a resiliência quântica, a adoção de *blockchain* e interoperabilidade, a gestão de dados e soluções de privacidade e segurança, a aplicação conjunta com o *big data* e a inteligência artificial.

Risius & Spohrer (2017) adaptam um quadro de investigação criada para estruturar o conhecimento atual sobre tecnologia *blockchain,* com três grupos de atividades: *design* e recursos, medição e valor, e gestão e organização, com quatro níveis de análise: utilizadores e sociedade, intermediários, plataformas, empresas e indústria. Concluindo

que a investigação se tem orientado para as questões tecnológicas, *design* e funcionalidades e não para a governança e criação de valor.

A *smart city* utiliza tecnologia da informação e comunicação para integrar e gerir infraestruturas físicas e de negócios sociais para obter melhores serviços aos seus cidadãos, otimizando os recursos disponíveis. A possibilidade de interrupção digital coloca desafios importantes de segurança e de privacidade. Uma estrutura de segurança que integra a tecnologia *blockchain* com dispositivos "inteligentes" pode fornecer uma plataforma de comunicação segura numa *smart city*. (Biswas & Muthukkumarasamy, 2016)

Zheng, Xie, Dai, Chen, & Wang (2017) apresentam uma visão abrangente sobre a tecnologia *blockchain* em que os principais desafios se centram nos problemas de escalabilidade e segurança. Comparam alguns algoritmos de consenso típicos, utilizados em diferentes *blockchains* conforme os desafios técnicos. Vários dos conceitos e normas apresentados podem ajudar na consolidação destes conceitos. Como a ISO TC 307[36] que estabeleceu os seguintes grupos de trabalho sobre: arquitetura de referência, taxonomia e ontologia (SG 1); casos de uso (SG 2); segurança e privacidade (SG 3): identidade (SG 4); e contratos "inteligentes" (SG 5). (Anjum et al., 2017)

A tecnologia *blockchain* tem evoluído nas suas caraterísticas e versões, desde o *blockchain* da versão 1.0 subjacente à moeda *bitcoin* para a versão 2.0 subjacente aos *smart contracts* 2.0 e, mais recentemente, para a 3.0 com a introdução de novas arquiteturas e da sua combinação que pretende ultrapassar algumas das limitações do *blockchain* como o aumento do número de transações por minuto, a possibilidade de combinar vários tipos de registos e a troca nativa com outros tipos de moeda. (Brandão et al., 2018b)

2.1. Caraterísticas

Este ponto pretende apresentar as principais caraterísticas do *blockchain* que passam pela estrutura de bloco, assinatura digital e protocolos de consenso.

As caraterísticas principais do *blockchain* orientam-se para: a descentralização, em que o não é necessário um terceiro para validar, mas através de algoritmos de consenso para

[36] ISO TC 307 - https://www.iso.org/committee/6266604.html , acedido em 8-04-2019

manter a consistência de dados da rede distribuída; a persistência, em que as transações inválidas são detetadas e depois de incluídas no *blockchain* não podem ser excluídas ou revertidas; o anonimato, em que a iteração realiza-se através de um endereço gerado, que pode não revelar a identidade real do utilizador; e a auditoria das transações, em que podem ser facilmente verificadas e rastreadas. (Z. Zheng et al., 2017a)

2.1.1. Estrutura de Bloco

Um bloco genérico consiste num cabeçalho e num corpo do bloco. O cabeçalho do bloco inclui:

- A versão do bloco, que indica qual o conjunto de regras de validação do bloco seguir.
- A *hash* da árvore Merkle *(Merkle tree root hash)*, que expõe o valor *hash* de todas as transações no bloco.
- O registo de data e hora, que indica data e a hora atual em segundos no horário universal desde 1 de janeiro de 1970.
- O campo *nBits*, que indica o limite de destino de um *hash* de bloco válido.
- O campo *Nonce*, que se trata de um campo de 4 bytes, que normalmente começa com 0 e aumenta para cada cálculo de *hash*.
- O ponteiro de dados inviolável é o apontador *hash (Pointer Hash)* que indica um valor de *hash* de 256 bits que aponta para o bloco anterior.

O corpo do bloco é composto por um contador de transações e transações (dados).

O número máximo de transações que um bloco pode conter depende do tamanho do bloco e do tamanho de cada transação.

A estrutura de dados vinculada e inviolável é um bloco, a lista-vinculada inviolável de blocos trata-se de *blockchain* (como abstração estrutural será uma lista de objetos) e a árvore binária inviolável é a árvore Merkle (como abstração estrutural será um conjunto de objetos). (Gupta, 2017)

2.1.2. Assinatura Digital

O *blockchain* utiliza um mecanismo de criptografia assimétrica para validar a autenticação de transações. A assinatura digital é baseada em criptografia assimétrica e é usada principalmente em ambientes não confiáveis. A assinatura digital apresenta-se

como um conjunto de três algoritmos: do algoritmo para a assinar através da função *sign (sk, m),* do algoritmo de geração de chaves *keygen (n)* que resultam as chaves privada *sk* e pública *pk* e do algoritmo de verificação através da função *verify (pk, m, sign (sk, m))*. (Gupta, 2017)

A sua aplicação passa por publicar o *pk* da chave pública como a sua identidade e usar a chave secreta *sk* para provar a sua identidade. Assim cada utilizador tem um par de chaves, chave privada *sk* e chave pública *pk*. A chave privada deve ser reservada e servir para assinar as transações. As transações assinadas digitais são transmitidas em toda a rede. A assinatura digital normalmente envolve duas fases: a fase de assinatura e a fase de verificação.

O envio de uma mensagem do utilizador X para o utilizador Y passa pela fase de assinatura em que o utilizador X criptografa os seus dados com sua chave privada e envia para utilizador Y o resultado criptografado com os dados originais. Na fase de verificação, o utilizador Y valida o valor com a chave pública do utilizador X, desta forma, o utilizador Y verifica se os dados foram adulterados ou não. A construção da assinatura digital normalmente usada no *blockchain* é o *ECDSA* (*Elliptic Curve Digital Signature Algorithm*) (D. Johnson et al., 2001).

2.1.3. Protocolos de Consenso

O consenso num ambiente distribuído, na rede *blockchain* distribuída, torna-se um dos principais desafios. No *blockchain,* não existe um nó central que garanta que os diários (*ledgers*) nos nós distribuídos sejam iguais. O protocolo de consenso é o mecanismo central de uma rede *blockchain* que mantém a confiança nos nós distribuídos a partir de possíveis ataques. Os seguintes protocolos de consenso procuram garantir que os diários em nós diferentes sejam consistentes (Z. Zheng et al., 2017a):

- Prova de Trabalho - *PoW* (*Proof of Work*)
- Prova de Participação - *PoS* (*Proof of Stake*)
- Tolerância a Falhas Bizantinas Práticas - *PBFT* (*Practical Byzantine Fault Tolerance*)
- Prova de Participação Delegada - *dPoS* (*Delegated Proof of Stake*)
- Tolerância a Falhas Bizantina Delegada - *dBFT* (*Delegated Byzantine Fault Tolerance*)

- Prova de Importância - *PoI* (*Proof of Importance*)
- *Ripple*
- Protocolo de Consenso Estrelar - *SCP* (*Stellar Consensus Protocol*)
- *Tendermint*

A Figura II.11. adapta a tabela II, baseada em Zheng, Xie, Dai, Chen, & Wang (2017) e a tabela III (Bach et al., 2018), junta-as numa única tabela com as características dos protocolos de consenso analisados, através da poupança de energia e do poder de tolerância à adversidade.

Tabela II.11 - Caraterísticas dos algoritmos de consenso

Propriedades	**Algoritmos**								
	PoW	***PoS***	***PBFT***	***DPoS***	***DBFT***	***PoI***	***Ripple***	***SCP***	***Tendermint***
Poupança de Energia	Não	Parcial	Sim	Parcial	Sim	Sim	Sim	Sim	Sim
Poder de tolerância à adversidade	< 25% Potência Computação	<51% Participação	< 33.3% Réplicas	< 51% Validadores	< 33.3% Réplicas	<50% Importância	<20% Nós defeituosos	Variável	Não requer mineiros

Adapta a tabela II, baseada em Zheng, Xie, Dai, Chen, & Wang (2017) e a tabela III (Bach et al., 2018)

Os protocolos PBFT, DBFT, PoI, *Ripple*, SCP e *Tendermint* apresentam poupança de energia. Os protocolos de consenso, PoS, dPoS e PoI, apresentam maior poder de tolerância à adversidade (~<51%), embora com mecanismos específicos de validação (participação, validadores e importância).

Nos pontos seguintes procura-se rever as caraterísticas de cada um destes protocolos de consenso.

2.1.3.1. PoW (Proof of Work)

O protocolo PoW (Prova de Trabalho) apresenta uma estratégia de consenso usada na rede Bitcoin (Nakamoto, 2008).

Numa rede descentralizada é necessário selecionar nós para registrar as transações. Uma forma simples é a seleção aleatória, mas a seleção aleatória pode ser vulnerável a ataques. Assim se um nó quiser publicar as transações num bloco terá de provar que o nó não é capaz de atacar a rede. Esta prova traduz-se em significativos cálculos através de computação. No algoritmo PoW, cada nó da rede calcula um valor de *hash* do cabeçalho do bloco, que contém um *nonce* e os mineradores mudam o *nonce* com frequência para

obter valores *hash* diferentes. O consenso no PoW necessita que o valor calculado seja igual ou menor do que um determinado dado valor. Quando um nó atinge o valor de destino, ele difundirá o bloco para outros nós e todos os outros nós devem confirmar mutuamente a exatidão do valor de *hash*. Se o bloco for validado, os outros mineiros anexam esse novo bloco aos seus próprios *blockchains*.

Os mineiros são os nós que calculam os valores *hash*. Em caso de simultaneidade na validação dos blocos, a cadeia que se torna mais longa depois é reputada como a autêntica. Ou seja, se dois nós criam blocos validados simultaneamente, os mineradores continuam a minerar blocos até que um ramo fique mais longo e seja considerado o autêntico.

Foram desenvolvidos vários protocolos alternativos tendo por base o PoW, como é exemplo o numero primo de prova de trabalho (*Prime Number Proof-of-Work*) apresentado por King (2013) que procura cadeias especiais de números primos que possam ser usadas através de três tipos de cadeias primárias conhecidas como cadeia Cunningham (Forbes, 1999) do primeiro tipo, cadeia Cunningham de segunda tipo e a cadeia bigémea (*bi-twin*) que são qualificadas como prova de trabalho. A cadeia principal está ligada ao bloqueio de *hash* para preservar a propriedade de segurança do Bitcoin (Nakamoto, 2008), enquanto uma síntese de avaliação contínua da dificuldade é projetada para permitir que a cadeia principal atue como prova de dificuldade ajustável.

Outras abordagens tentam otimizar através de projetos de circuitos integrados específicos de aplicação (*ASICs - Application Specific Integrated Circuits*) projetados especialmente para computação PoW para a operação de consenso *blockchain,* para permitirem a mineração de *blockchain*, ao obter uma quantidade significativa de computação para encontrar um novo bloco válido (H. Cho, 2018).

2.1.3.2. PoS (Proof of Stake)

O protocolo PoS (prova de participação) é uma alternativa económica em termos energéticos ao PoW. Os mineiros neste protocolo têm que provar a propriedade do valor. Parte do principio que quem tem mais valores ou mais moedas têm menor probabilidade de atacar a rede. Esta escolha é baseada no saldo da conta, dado que quem tem mais valores torna-se dominante na rede. Surgem outras propostas que combinam o tamanho da participação com outros critérios para decidir qual delas deve moldar o próximo bloco. Vasin (2014) apresenta a randomização para prever o próximo gerador através duma fórmula que procura o menor valor de *hash* combinado com o tamanho da participação

aplicada à cripto moeda *BlackCoin*. King & Nadal (2012) privilegia a escolha baseada na idade dos valores. Os mais antigos e os maiores têm maior probabilidade de minerar o próximo bloco. O PoS economiza mais energia e é mais eficaz do que o PoW. Várias redes e plataformas *blockchain* adotaram inicialmente o PoW e passaram para o PoS como é o caso do Ethereum (Wood, 2019) e (Zamfir, 2015)

2.1.3.3. PBFT (Practical Byzantine Fault Tolerance)

O protocolo de tolerância prática a falhas bizantinas PBFT (*Practical Byzantine Fault Tolerance*) baseia-se num algoritmo de replicação para tolerar falhas bizantinas (Castro & Liskov, 1999) em que podem permitir que os sistemas continuem a funcionar corretamente mesmo quando houver erros, embora nem todos os erros sejam admissíveis, nomeadamente quando ocorrem em todos os nós.

O projeto *Hyperledger Project*[37] utiliza o PBFT como seu algoritmo de consenso, já que o PBFT pode manipular até um terço de réplicas bizantinas maliciosas. Um novo bloco é determinado numa rotação. Em cada rotação, um primário será selecionado de acordo com algumas regras e fica responsável por recomendar a transação. Todo o processo poderá ser dividido em três fases: pré-preparado, preparado e comprometido. Em cada fase, um nó entrará na próxima fase se receber votações de mais de dois terços de todos os nós. O que implica que no protocolo PBFT cada nó seja conhecido pela rede.

2.1.3.4. *dBFT* (*Delegated Byzantine Fault Tolerance*)

O dBFT (tolerância a falhas bizantina delegada), descrito no *Neo whitepaper*[38]. baseia-se em nós profissionais que são recomendados para registrar as transações. O mecanismo de consenso dBFT utiliza o consenso tolerante a falhas bizantinas através de voto por procuração. O portador do *token Neo*[39] pode escolher o contador que suporta e o grupo selecionado de contadores chega a um consenso e gera novos blocos. A votação na rede *Neo* continua em tempo real e não com um prazo fixo. Os clientes são de dois tipos: contadores e nós comuns em que os nós comuns não participam no consenso, apenas votam no nó do contador que desejam suportar (delegando o voto) e os nós do contador escolhidos com sucesso ficam incluídos no processo de consenso. Se pelo menos dois

[37] Hyperledger Project - https://www.hyperledger.org/ , acedido em 18-04-2019
[38] Neo Whitepaper - https://docs.neo.org/en-us/whitepaper.html , acedido em 18-04-2019
[39] Nós Neo - https://neo-ngd.github.io/reference/How-To-Become-NEO-Consensus-Node.html , acedido em 18-04-2019

terços dos contadores acordarem que a transação é válida, esta permanece consolidada no *blockchain* e na seguinte rotação de consenso será iniciada através de outro contador selecionado aleatoriamente. (Bach et al., 2018)

2.1.3.5. *dPoS (Delegated Proof of Stake)*

O dPoS (prova delegada de participação) apresenta como principal diferença o tipo de democracia em que o PoS é uma democracia direta, enquanto o dPoS é uma democracia representativa. As partes interessadas elegem os representantes para gerar e validar os blocos. Como são muito menos nós para validar o bloco, o bloco pode ser confirmado com mais rapidez, levando à rápida confirmação das transações. Os parâmetros da rede, como tamanho de bloco e intervalos de bloco, poderiam ser ajustados pelos delegados. Os utilizadores não precisam de se preocupar com os delegados desonestos, pois podem ser eliminados facilmente. O ecossistema de BitShares[40] utiliza o dPoS para encontrar as soluções mais eficientes para obter o consenso distribuído.

2.1.3.6. *PoI* (*Proof of Importance*)

Uma conta pode ser elegível para um "Cálculo da Importância", se ela contiver pelo menos 10.000 XEMs investidos. Dada a elegibilidade, a Importância é calculada com base na quantidade de XEM adquirido, a classificação da conta dentro da rede (encontrada usando o algoritmo NCDawareRank), um fator de ponderação baseado na localização topológica da conta e duas constantes adequadas determinadas pela rede NEM[41].

2.1.3.7. Ripple (Ripple Protocol Consensus Algorithm)

Ripple (Schwartz et al., 2014) é um algoritmo de consenso que utiliza sub-redes confiáveis coletivamente dentro da rede maior. Na rede, os nós são divididos em dois tipos: servidor para participar do processo de consenso e cliente para transferir apenas fundos. Cada servidor tem uma lista de nós exclusivos (UNL). O UNL é importante para o servidor. Ao determinar colocar uma transação no livro razão (*ledger*), o servidor consultaria os nós no UNL e se os contratos recebidos atingissem 80%, a transação seria registada no livro razão (*ledger*). Para um nó, o *ledger* permanecerá correto contando que a percentagem de nós defeituosos no UNL seja menor que 20%.

[40] Bitshares - https://bitshares.org/ , acedido em 18-04-2019
[41] NEM - https://nem.io/ , acedido em 18-06-2019

2.1.3.8. *SCP (Stellar Consensus Protocol*)

O Protocolo de Consenso Estelar (SCP) (Mazières, 2015) é um protocolo de acordo bizantino que deriva do PBFT. No PBFT, cada nó tem que consultar outros nós, enquanto o SCP dá aos participantes o direito de escolher em qual conjunto de outros participantes acreditar.

2.1.3.9. *Tendermint*[42]

O *Tendermint* (Kwon, 2014) é um algoritmo de consenso bizantino. Um novo bloco é determinado numa rotação. Um proponente seria selecionado para transmitir um bloco não confirmado nesta rotação. O processo pode ser dividido em três etapas: previsão do passo, em que os validadores escolhem se devem transmitir uma previsão para o bloco proposto; passo de recomendação, em que se o nó tiver recebido mais de dois terços do bloco proposto, ele transmitirá um pré-aviso para aquele bloco e se o nó recebeu mais de dois terços dos pré-compromissos, ele entra na etapa de confirmação; confirmar passo, em que o nó valida o bloco e transmite uma confirmação para esse bloco, se o nó recebeu dois terços das confirmações, aceita o bloco e em contraste ao PBFT, os nós precisam bloquear as suas moedas para se tornarem validadores e se um validador é considerado desonesto, seria punido.

2.1.3.10. Outros algoritmos de consenso

Um algoritmo de consenso deve ser eficiente, seguro e conveniente. (Z. Zheng et al., 2017b)

Novos algoritmos de consenso estão a ser desenvolvidos para tentar resolver problemas específicos de novas aplicações *Blockchain*.

O PeerCensus (Decker et al., 2014) tem como propósito o desassociar a criação de blocos e a confirmação de transações para que a velocidade de consenso possa ser aumentada.

De outra forma, Kraft (2016), para resolver o problema do comprometimento da segurança do *bitcoin* devido à alta taxa de geração de blocos, apresenta um método de consenso para garantir que um bloco seja gerado a velocidade estável. Então, a regra de seleção de cadeias GHOST *(Greedy Heaviest-Observed Sub-Tree)* (Sompolinsky & Zohar, 2013) é proposta para resolver este problema. Em vez do maior esquema de

[42] Tendermint - https://tendermint.com/ , acedido em 12-06-2019

ramificação, o GHOST pondera os ramos e mineiros que poderiam escolher o melhor a seguir.

Chepurnoy, Larangeira, & Ojiganov (2016) apresentaram outro algoritmo de consenso para sistemas *blockchain peer-to-peer* onde qualquer um que forneça provas não-interativas de recuperabilidade, para os instantâneos do estado passado, concorda em gerar o bloco. Neste protocolo, os mineradores só precisam armazenar cabeçalhos de blocos antigos em vez de blocos inteiros.

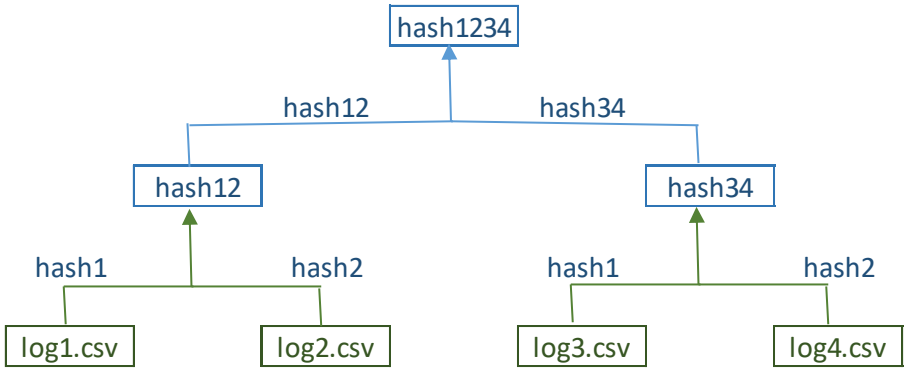
A pesquisa realizada por Wang et al. (2018), sobre os mecanismos de consenso e a gestão da mineração em redes de *blockchain,* examinou os protocolos de consenso *blockchain* em três perspetivas: os implementadores de redes de *blockchain*, os participantes de consenso e os utilizadores de redes *blockchain*. Conclui, que nas redes *blockchain*, as falhas bizantinas originam que nós defeituosos exibam comportamentos arbitrários, incluindo ataques mal-intencionados, erros de nós e erros de conexão.

2.2. Merkle *Tree*

Uma árvore Merkle, também conhecido como um *hash* de árvore binária, é uma estrutura de dados usada para resumir e aumentar a eficiência para verificar a integridade de grandes conjuntos de dados, permitindo uma visão de mais alto nível. (Merkle, 1988)

A construção da árvore Merkle passa pela utilização de funções hash MD5. SHA-3, e SHA-256, que originam valores exclusivos, que também reproduzem entradas com o estado atual de uma determinada entrada. As árvores binárias Merkle vão projetando à medida que nova informação surge na estrutura de dados e em cada nó tem no máximo dois filhos, que combina duas entradas em conjunto para obter uma única saída. A partir de vários pares de entradas (por exemplo de ficheiros de log.csv) a estrutura de árvore desenvolve-se de acordo com a Figura II.3 apresentada a seguir:

Figura II.3 - Árvore de Merkel



As árvores Merkle permitem verificar se um dado de entrada foi incluído num conjunto de dados e em que ordem. Podem também permitir compactar grandes conjuntos de dados através da remoção dos ramos supérfluos, mantendo apenas os que são necessários para a prova.

A camada de dados fornece os blocos de dados relacionados, utilizando técnicas como a criptografia assimétrica, carimbo de data / hora (*timestamp*), algoritmos *hash* e árvores Merkle e outras otimizações. No sistema *blockchain*, cada nó de computação que vencer a competição de consenso terá o poder de criar um novo bloco, juntando todos os dados relacionados e gerados dentro de um período de tempo específico e estruturado na árvore Merkle. (Yuan & Wang, 2016)

Com a utilização das árvores de Merkel passamos a ter a capacidade para verificar se uma transação está incluída num bloco, sem ser necessário aceder a toda a cadeia, e com a possibilidade das criptomoedas da verificação de pagamento simplificado (SPV-*Simplified Payment Verification*). Os nós não mantêm o *blockchain* completo e através dos nós SPV usam os caminhos de Merkle para verificar as transações. Os nós SPV usam apenas o cabeçalho do bloco, sem conhecerem as transações, apenas verificam as transações e vinculam essa cadeia específica à transação de interesse, estabelecendo um *link* entre a transação e o bloco que a contém, usando um caminho Merkle. (Kim et al., 2017)

Cho, Park, & Lee (2017) propõem o voto cego, em que que cada nó é independente, entre os nós, usando um *hash* de bloco e uma árvore de Merkle, onde um grande número de decisões ocorrem dinamicamente, sem saber qual o nó a selecionar. Os nós armazenam as transações transferidas numa *pool* de transações de acordo com determinado número par. A árvore de Merkle é criada dinamicamente de cada vez, portanto, é um método para eliminar a rastreabilidade, para bloquear o gerador e recolher um grande número de decisões.

As caraterísticas principais das árvores Merkel são as seguintes:

- Verifica-se que se os nós tiverem a mesma transação usando o recurso de árvore Merkel, o valor da raiz da árvore do Merkel será o mesmo para todos os nós. Se a transação for comprometida o valor de *hash* da raiz de árvore de Merkle estará incorreto.

- A utilização das árvores de Merkle permite maior eficiência, desempenho global e escalabilidade.
- As árvores de Merkle passam a ser uma componente importante da tecnologia *blockchain* com os desafios de escalabilidade e de capacidade de processamento.
- A forma mais comum e simples de árvore Merkle é a árvore Merkle binária através do mecanismo de provas de Merkle. A prova de Merkle consiste em obter o *hash* raiz da árvore e os ramos consistem nos nós com os *hash* que vão subindo ao longo do trajeto do nó até à raiz. A prova verifica que o *hashing* é consistente com todo o caminho da árvore.
- Todas as transações no bloco são combinadas na raiz da árvore de Merkle. A raiz da árvore Merkle garante a integridade das transações, pois a alteração nas transações causa um valor totalmente diferente do valor da raiz da árvore Merkle. (Lei et al., 2017)

Como exemplo de aplicação, as provas de Merkle na plataforma Ethereum tem em cada cabeçalho do bloco três árvores para três tipos de objetos, transações, recibos e o estado, para obter respostas verificáveis para vários tipos de consultas e questões.

As árvores utilizadas na Ethereum são mais complexas utilizando a árvore Merkle-Patrícia. As árvores binárias Merkle são estruturas de dados para preferencialmente autenticar informação no formato de lista, com uma série de blocos seguidos, ou para árvores de transação onde não importa quanto tempo leva para editar uma árvore depois de criada é imutável. As árvores de estado tornam-se mais complexas. No Ethereum a árvore de estados consiste resumidamente num mapa de valores-chave, em que as chaves são os endereços e os valores são "declarações", catalogando as contas de balanço/os saldos, o *nonce*, o código e o armazenamento para cada conta (o armazenamento é em si uma árvore). O estado do contrato é armazenado num mapeamento de saldos que associa o endereço de utilizadores a um saldo. (Wohrer & Zdun, 2018)

A estrutura de dados desejada deve poder calcular rapidamente a nova raiz de árvore após uma inserção, atualização, editação ou exclusão da operação, sem ter de recalcular toda a árvore através de duas propriedades secundárias: a limitação da profundidade da árvore evitando ataque de negação de serviço (*DoS*) e a raiz da árvore depende somente dos dados e não na ordem das atualizações.

A árvore Merkel Patrícia[43] pretende alcançar estas propriedades simultaneamente. Cada nó tem 16 filhos e o caminho em cada nó é determinado pela codificação hexadecimal, a partir da raiz, para descer a 6, em seguida, o quarto, e assim por diante até chegar ao fim. A raiz de armazenamento é o *hash* de 256 bits do nó raiz de uma árvore Merkle Patrícia que representa o conteúdo da conta. As árvores Merkle Patrícia são usadas para armazenar todas as ligações (chave, valor) na plataforma Ethereum. O cabeçalho do bloco contém as três raízes, de três formas de representação: do estado, das transações e dos recibos. (Vujicic et al., 2018)

2.3. Plataformas *Blockchain*

As diferentes abordagens da tecnologia *blockchain* encontram-se associadas a diversas plataformas. A Tabela II.1, adotada da figura 1 de Anjum, Sporny, & Sill (2017), apresenta e compara os diversos tipos de *blockchains* através dos principais princípios da segurança da informação e que passam pela confidencialidade, a disponibilidade da informação, a integridade, o não repúdio, a proveniência/origem, a pseudonimização e a comunicação seletiva. As cores das letras verde, amarelo e vermelho representam o sistema de semaforização da avaliação com o respetivo o grau de cumprimento considerados (verde - cumpre, amarelo - disponível, vermelho - não cumpre).

Tabela II.12 - Análise de segurança da informação *blockchain*

	Características de segurança de *blockchains*					
Princípio	**Bitcoin**	**Ethereum**	**Stellar**	**IPFS**	**Blockstack**	***Hash*graph**
Confidencialidade	**Não**	**Não**	**Não**	**Endereços de conteúdo baseado em *hash***	**Não**	**Não**
Disponibilidade de informações	**Bloco de espelhamento**	**Bloco de espelhamento**	***Ledger* espelhamento**	**Gráfico e ficheiro de espelhamento**	**Bloco de espelhamento / DHT espelhamento**	***Hash*graph / espelhamento; Opcional histórico eventos**
Integridade	**Múltiplas verificações de bloco**	**Múltiplas verificações de bloco**	**Verificação bloco mais recente**	**Conteúdo de endereçamento baseado em *hash***	**Múltiplas verificações de bloco**	**Consenso com probabilidade um**
Não repúdio	**Assinaturas digitais**	**Assinaturas digitais**	**Assinaturas digitais**	**Assinaturas digitais**	**Assinaturas digitais**	**Assinaturas digitais**
Proveniência	**Entradas / saídas de transação**	**Funções Ethereum máquina de estado e transição**	**Assinado digitalmente instruções de transição razão**	**Assinaturas digitais e versionamento**	**Entradas de transação e saídas e referências cadeia virtuais**	***Hash*graph / espelhamento; Opcional histórico eventos**
Pseudonimização	**As chaves públicas**	**As chaves públicas e endereços contrato**	**As chaves públicas**	**As chaves públicas**	**Chaves públicas, mas estimulo de**	**Não suportado; poderia ser em camadas**

[43] Árvore Merkel Patrícia - https://github.com/ethereum/wiki/wiki/Patricia-Tree , acedido em10-05-2019

	Características de segurança de *blockchains*					
Princípio	**Bitcoin**	**Ethereum**	**Stellar**	**IPFS**	**Blockstack**	***Hash*graph**
					informação pública	
Comunicação seletiva	**Não**	**Não**	**Não**	**Não**	**O acesso seletivo ao armazenamento cifrado**	**Não suportado; poderia ser em camadas**

Adaptada da figura 1, de Anjum, Sporny, & Sill (2017)

Nesta tabela verifica-se que as plataformas em análise apresentam pelo menos um item de análise a vermelho, que não cumpre, de comunicação seletiva ou de confidencialidade.

A Tabela II.13, adotada da figura 2 de Anjum, Sporny, & Sill (2017), apresenta e compara as principais características de desempenho dos vários tipos de *blockchains*, através das principais caraterísticas associadas à tecnologia *blockchain* que passam pela consistência, a disponibilidade do sistema, a tolerância a falhas, a escalabilidade, a latência, a auditabilidade, a resiliência, a resistência à negação de serviço (*DoS*) e a complexidade do sistema. As cores das letras verde, amarelo e vermelho representam o sistema de semaforização da avaliação com o respetivo o grau de cumprimento considerados (verde - cumpre, amarelo - disponível, vermelho - não cumpre). Estes tipos de *blockchain* e respetivas plataformas não se esgotam nos tipos apresentados, sendo claro que vão sendo crescentemente adicionadas novas de tecnologias especializadas de contabilidade distribuída (*DLT- Distributed Ledger Technology*) e em novos domínios de aplicação.

Tabela II.13 - Análise de características de desempenho de *blockchain*

	Características de desempenho de *blockchains*					
Princípio	**Bitcoin**	**Ethereum**	**Stellar**	**IPFS**	**Blockstack**	***Hash*graph**
Consistência	**Verificações de Blocos. 30 a 60 minutos**	**Verificações de Blocos. 20 a 60 minutos**	**Verificação de bloco único Menos de 1 minuto**	**Espelhamento P2P. Limitado principalmente pela rede E/S. Vários segundos para ficheiros com menos de 128 KB.**	**Verificações de Blocos. 30 a 60 minutos**	**Consenso com probabilidade um; Acordo bizantino, mas os atacantes devem controlar menos de um terço**
Disponibilidade do sistema	**Verificações de Blocos. 30 a 60 minutos**	**Verificações de Blocos. 20 a 60 minutos**	**Verificação de bloco único Menos de 1 minuto**	**Resposta de solicitação de armazenamento único. Vários segundos para ficheiros com menos de 128 KB.**	**Verificações de Blocos. 30 a 60 minutos**	**Votação virtual; DoS resistente sem prova de trabalho, conversa rápida**
Tolerância a falhas	**Cadeia mais longa, ganha**	**Cadeia mais longa, ganha**	**Último bloco de votação sempre tem consenso.**	**Endereço de conteúdo *hash*. Altamente resiliente contra o particionamento de rede.**	**Cadeia mais longa, ganha**	**Votação virtual. DoS resistente sem prova de trabalho, fofoca rápida**
Escalabilidade	**Tamanho do bloco. 7 transações por segundo**	**Tamanho do bloco. 7-20 transações por segundo**	**Milhares a dezenas de milhares de transações por segundo.**	**Milhares a dezenas de milhares de transações por segundo. Escala linearmente conforme os nós são adicionados.**	**Tamanho do bloco. 7 transações por segundo**	**Milhares a dezenas de milhares de transações por segundo. Limitado apenas pela largura de banda**

	Características de desempenho de *blockchains*					
Princípio	**Bitcoin**	**Ethereum**	**Stellar**	**IPFS**	**Blockstack**	***Hash*graph**
Latência	**Verificações de Blocos. 30 a 60 minutos**	**Verificações de Blocos. 20 a 60 minutos**	**Verificação de bloco único Menos de 1 minuto.**	**Resposta de solicitação de armazenamento único. Vários segundos para ficheiros com menos de 128 KB.**	**Verificações de Blocos. 30 a 60 minutos**	**Votação virtual; limitado apenas pelo protocolo gossip, exponencialmente rápido**
Auditabilidade	**Total**	**Total**	**Total**	**Dificuldade**	**Total**	**Configurável**
Resiliência	**Total**	**Total**	**Total**	**Falha se os nós que armazenam dados falharem**	**Total**	**Total**
Resistência à negação de serviço	**Gastar Bitcoins**	**Gastar Ether**	**Gastar Stellar**	**Os ficheiros são apenas espelhados se solicitados**	**Gastar Bitcoins**	**Estado Assinado / Prova de Participação / <1/3 atacantes**
Complexidade do Sistema	**Médio**	**Alto**	**Médio**	**Médio**	**Médio**	**Baixo, mas em todo o sistema**

Adaptada da figura 2, de Anjum, Sporny, & Sill (2017)

Nos subpontos seguintes serão detalhadas algumas das principais plataformas analisadas, Hyperledger Fabric, Stellar, Ethereum e *InterPlanetary File System* que poderão suportar os tipos de *blockchain*, o Ethereum, o Stellar e o IPFS. No entanto, as plataformas e os tipos não se esgotam nas plataformas analisadas a seguir e no Anexo I - Quadro comparativo de plataformas *blockchain*, onde se apresenta uma lista de plataformas com as suas principais caraterísticas.

2.3.1. Hyperledger Fabric (HLF)

O projeto Hyperledger[44] teve na sua base vários requisitos que passam por: transações privadas e contratos confidenciais para garantir a confidencialidade e a privacidade; a identidade e auditabilidade para suportar a troca de identidades e auditoria, através da possibilidade da anonimidade da identidade; a interoperabilidade, através de componentes independentes, pela interação quando a informação é trocada e utilizada por esses componentes; a portabilidade em ambientes computacionais heterogéneos, ao abstrair-se das interfaces dos componentes, separando-os dos ambientes; a arquitetura baseada em quatro categorias, que são disponibilizadas como, serviços de identidade, de política, de *blockchains* e de *smart contracts*.

O HLF apresenta um consenso que é alcançado quando a ordem e os resultados das operações de um bloco tenham cumprido os critérios explícitos, que passam por: a consulta e atualização contabilística, usando pesquisas baseadas na chave, consultas de

[44] Hyperledger Fabric - https://github.com/hyperledger/fabric , acedido em10-03-2019

intervalo, e consultas de chave composta; a leitura somente de consultas do histórico; as operações que contêm as assinaturas de todos os pares a endossar e que são submetidos ao serviço de encomendas, pela validação de transações que cumpra as políticas de nomeadamente de contribuição; a contabilidade de um canal que contém um bloco de configuração com a definição de políticas, listas de controlo de acesso, e outras informações pertinentes; e pelo canal que permite a criptografia de diferentes autoridades de certificação.

As principais funções passam por: *blockchains* permissivos com finalidade imediata; ambientes para a execução de contratos "inteligentes"; módulos de consenso baseados no PBFT (Castro & Liskov, 2002), em No-op (consenso ignorado) para tratar no modo padrão, enquanto o código está na versão de pré-lançamento, para depurar (*debug*) e o protótipo SIEVE (para executar operações, comparar as saídas em cópias e procurar disparidades) como solução modular para replicar aplicações não determinísticas num sistema BFT (Cachin et al., 2016); uma *framework* de eventos que suporta eventos predefinidos e customizados; o cliente SDK (Node.js) para interagir com a rede *blockchain*; e o suporte para APIs REST (*Representational State Transfer*) básicas e CLIs (*comand-line interfaces*) (Cachin, 2016).

A investigação realizada por Sousa, Bessani, & Vukolić (2017) na plataforma HLF (*Hyperledger Fabric*) permite uma extensibilidade e suporte a vários serviços de encomenda para a construção do *blockchain*. A implementação e avaliação do serviço de encomendas BFT (*Byzantine Fault-Tolerant*) para HLF permitiu atingir até dez mil transações por segundo e escrever uma transação de forma irrevogável no *blockchain* em meio segundo.

2.3.2. Stellar

A plataforma utiliza o mecanismo de consensos Stella. O projeto Stellar[45] é um projeto *open-source*, com a infraestrutura de pagamentos distribuída, que interliga bancos, sistemas de pagamento e as pessoas. A plataforma Stellar permite a construção de carteiras móveis, ferramentas bancárias, dispositivos "inteligentes" e fornece servidores HTTP API RESTful chamados Horizon, que ligam a Stellar Core à rede Stellar.

[45] Stellar - https://www.stellar.org , acedido em 11-03-2019

Um lúmen (XLM) é o ativo nativo da rede Stellar, uma unidade de moeda digital, como um bitcoin.

2.3.3. Ethereum

A plataforma Ethereum[46] é descentralizada, com capacidade para executar *smart contracts* e aplicações descentralizadas suportadas em tecnologia *blockchain*.

As principais caraterísticas passam por: as aplicações que funcionam de acordo com a forma como foram programadas, através do contrato que é imutável, sem censura, fraude e interferência de terceiros; tem uma máquina virtual descentralizada, a máquina virtual Ethereum (*EVM - Ethereum Virtual Machine*), para executar scripts nos nós públicos; e com o protocolo Casper (Baliga, 2017) a rede do Ethereum passou de *Proof-of-Work* (PoW) para *Proof-of-Stake* (PoS).

O protocolo Casper[47], lançado na versão *Serenity* da plataforma Ethereum, utiliza o conceito de depósitos e apostas de segurança para obter consenso. Neste protocolo os nós ligados ao sistema Ethereum fazem depósitos de segurança significativos definidos pelo protocolo, passando a serem nós validadores ligados e que demonstram comprometimento e interesse em avançar na rede *blockchain* Ethereum, apostando os seus depósitos de segurança.

Esta lista inicial de validadores é vinculada através do contrato Casper, que pode evoluir com base em novos nós e os nos nós mais antigos deixam o sistema. Cada validador é selecionado pseudo-aleatoriamente para produzir um bloco do conjunto do validador ativo, com a probabilidade da seleção linearmente ponderada pelo depósito de cada validador. Se um validador estiver *offline*, um validador diferente será selecionado e esse processo será repetido até que um validador *on-line* seja localizado e crie um bloco. Se um validador produz um bloco que é incluído na cadeia, ele recebe uma recompensa de bloco igual ao total de Ether no conjunto do validador ativo. Se o validador produz um bloco que não é incluído na cadeia, o protocolo funciona de tal forma que o validador perde o depósito de segurança igual à recompensa do bloco. Este mecanismo propõe

[46] Ethereum - https://www.ethereum.org/ , acedido em 20-02-2019

[47] Ethereum Casper Protocol - https://blockgeeks.com/guides/ethereum-casper/, acedido em 20-07-2019

resolver o problema *Nothing-at-Stake*, que impede que os nós produzam blocos que não serão incluídos na cadeia principal (Baliga, 2017).

A plataforma Ethereum permite que: se facilite a segurança dos cripto-ativos, a escrita, a implementação e a utilização de *smart contracts*; se criem cripto-moedas; se criem organizações autónomas democráticas (*DAOs - Decentralized Autonomous Organization*); e se utilizem ferramentas de desenvolvimento em Go, C ++, Python, Java, etc. Um Ether (ETH) é o ativo nativo da rede Ethereum, uma unidade de moeda digital.

2.3.4. InterPlanetary File System (IPFS)

O *InterPlanetary File System*[48] (IPFS) (Benet, 2014) é uma plataforma para suportar um sistema de ficheiros distribuído *peer-to-peer* que procura interligar os dispositivos ao mesmo sistema de ficheiros. O IPFS pode ser visto como um único local de BitTorrent, que troca objetos dentro de um repositório Git. A sua organização passa por um Merkle DAG (*Directed Acyclic Graph*) generalizado (estrutura de dados semelhante a uma árvore Merkle, menos rigorosa dado que o DAG pode não ser balanceado e seus nós podem conter dados), sobre a qual é possível construir sistemas de ficheiros com versão, *blockchains* e até uma Web permanente. O IPFS combina uma tabela *hash* distribuída, com troca de blocos e um *namespace* autocertificado, tende a não ter pontos de falha (com as novas versões, as melhorias de performance e o aumento de nós) e os nós não precisam confiar uns nos outros.

Nas especificações técnicas dos protocolos IPFS[49] são apresentados os protocolo IPFS, a camada de rede (libp2p que cobre a rede e o encaminhamento), os registos, o *naming* e os sistemas de registo (*IPRS-InterPlanetary Record System* e *IPNS - InterPlanetary Naming System)*, as estruturas de dados e formatos (*IPLD-InterPlanetary Linked Data*, unixfs e multiformatos), os ficheiros/sistema de ficheiros mutável (interface do *Virtual File System*, no *linux* e no topo do *MerkleDAG*), a troca de blocos (*bitswap* inspirada em BitTorrent), componentes internos específicos (blocos e bloqueio de serviço, serviço DAG e DAG, importação de dados, especificação do repositório local do nó do IPFS), APIs públicas (*Core API* principal, API HTTP e CLI), a gestão de chaves (KeyStore,

[48] IPFS - https://ipfs.io/ , acedido em 10-04-2019

[49] SPEC IPFS - https://github.com/ipfs/specs , acedido em 10-03-2019

KeyChain) e o desenvolvimento orientado por protocolo (*PDD-Protocol Driven Development*).

Em resumo os principais componentes do IPFS passam por: a tabela de *hash* distribuída cujos os nós podem armazenar e partilhar dados sem coordenação central; o IPNS (*InterPlanetary Naming System)* que permite que os dados trocados sejam instantaneamente pré-autenticados e verificados usando criptografia de chave pública; o Merkle DAG que permite que os dados sejam exclusivamente identificados, invioláveis e permanentemente armazenados; e permite aceder a versões anteriores de dados editados através do Sistema de Controle de Versão (Git). (Benet, 2014)

Zheng, Li, Chen, & Dong (2018) propõem um modelo de armazenamento de dados *blockchain* que mostra como usar redes IPFS para reduzir o armazenamento de dados *blockchain,* através de uma prova de conceito para os mineradores poderem armazenar menos dados de *blockchain* em cenário real e como novos nós podem sincronizar rapidamente com a rede. Como resultados calcularam a taxa de compressão face ao bitcoin (pode atingir 0,0817) e verificaram melhores características do esquema, no espaço de armazenamento, segurança e velocidade de sincronização de nós.

2.4. Comparação do *blockchain* com outras tecnologias em ambiente *IoT*

Hankerson, Vanstone, & Menezes (2003) revelam os cinco objetivos fundamentais para comunicações seguras: a confidencialidade, para manter os dados em segredo de todos, exceto daqueles autorizados a ver; integridade dos dados, para assegurar que os dados não tenham sido alterados por meios não autorizados; a autenticação de origem de dados, corroborar a fonte de dados; a autenticação de entidade, para corroborar a identidade de uma entidade; e não-repúdio, para impedir uma entidade de negar compromissos ou ações anteriores.

As camadas de *IoT*, para soluções *smart*, estão representadas na Tabela II.14, adaptada de Yang, Wu, Yin, Li, & Zhao (2017), com as soluções existentes.

Tabela II.14 - Análise em camadas de *IoT*

Camadas	Soluções
Camada de aplicação	*Smart places*, *smart city*, s*mart home*, sistema de saúde, gestão de energia, monitorização ambiental, internet industrial, veículos conectados
Camada de transporte	*Transport Layer Security* (TLS), *Datagram Transport Layer Security* (DTLS)
Camada de rede	*Low power Wireless Personal Area Networks* (6LoWPAN), 6LoWPAN/IPSec, IPSec, IPSec's *Authentication Header* (AH), *Encapsulation Security Payload* (ESP), *End-to-End* (E2E), IEEE 802.15.4, IPv6

Camadas	Soluções
Camada de perceção	*Wireless Sensor Networks* (WSNs), *Implantable Medical Devices* (IMDs), *Implantable Cardioverter Defibrillator* (ICD), *Radio-Frequency Identification* (RFID), *Global Positioning System* (GPS).

Adaptada de Yang, Wu, Yin, Li, & Zhao (2017)

A Tabela II.15, adaptada da tabela 3, de Mohamad Noor & Hassan (2019) procura sintetizar os principais desafios da segurança de *IoT* e as possíveis medidas de mitigação.

Tabela II.15 - Desafios atuais na segurança de *IoT* e medidas de mitigação

Camada	Desafios de Segurança	Mitigação
Perceção	Deteção do nó do sensor anormal Os algoritmos de criptografia de escolha e o mecanismo de gestão de chaves a serem usados	Algoritmo de deteção de falhas, sistema descentralizado de deteção de intrusão
		Criptografia de chave pública devido à rede de grande escala
		Protocolo de reserva de *slots*
		Controlo de acesso, mitigação de ataques DoS
Aplicação de rede	Dados e anonimato do remetente Vulnerabilidades do dispositivo Ativando a Comunicação IPSec com Nós IPv6 Sistemas de computador embutidos e configuráveis.	Pesquisa na adequação do IPv6 e IPSec para comunicação segura.

Adaptada da tabela 3, de Mohamad Noor & Hassan (2019)

As soluções de criptografia de chave pública implicam uma adequada gestão de chaves que inclui geração, distribuição, armazenamento, atualização e destruição de chaves secretas. Os algoritmos de criptografia de chave pública de baixa potência aplicados em *IoT* e para redes de sensores sem fio passam por algoritmos como: o Rabin's Scheme[50], o NtruEncrypt[51] e a Criptografia de Curva Elíptica (ECC - *Elliptic Curve Cryptosystems*) (Gaubatz et al., 2005). O ECC define o conjunto de protocolos de intercâmbio e de concordância de chave criptográfica assimétricos diferentes, como o ECDH (*Elliptic-curve Diffie-Hellman*), o ECDSA (*Elliptic Curve Digital Signature Algorithm*) e o ECMV (*Elliptic Curve Menezes Vanstone*). A distribuição de chaves pode divide-se em quatro grupos: distribuição de chave de transmissão, distribuição de chaves de grupo, pré-distribuição da chave mestra e distribuição de chaves em pares.

Suarez-Albela, Fernandez-Carames, Fraga-Lamas, & Castedo (2018) compararam o desempenho dos conjuntos de cifras ECDSA e RSA (Rivest et al., 1978), e avaliaram o impacto das diferentes curvas ECC e tamanhos de chaves RSA usando nós de *IoT* com recursos restritos. Nos cenários selecionados a ECDSA (D. Johnson et al., 2001) é uma

[50] Rabin, ponto 8.3 - http://cacr.uwaterloo.ca/hac/about/chap8.pdf , acedido em 10-06-2019

[51] Ntru Encrypt - https://www.onboardsecurity.com/products/ntru-crypto/ntru-resources , acedido em 10-06-2019

alternativa melhor do que o RSA para proteger dispositivos de *IoT* com recursos limitados.

Os problemas de segurança de soluções *IoT* podem afetar a implantação e a adoção, implicando novas pesquisas em segurança nas tecnologias *IoT*, para tentar resolver os desafios e os riscos, em detetar fragilidades para minimizar as vulnerabilidades, através de tecnologias confiáveis e a possibilidade de integração de mecanismos de segurança. As áreas de segurança da *IoT*, que começaram por adaptar protocolos e algoritmos existentes ao contexto da *IoT*, passam por: a análise forense, a engenharia da segurança, a deteção de intrusão, a resiliência, a privacidade, a confiança na *IoT* social, a confiança, a autocorreção, as políticas de segurança, as arquiteturas, o controlo de acesso, a autenticação, a identidade, as comunicações, os sistemas operativos, a cifragem, as funções físicas não clonáveis (*PUF-Physical Unclonable Functions*), a segurança física da camada (*PLS- Physical Layer Security*) e a segurança de hardware. A tecnologias DLT (*Distributed Ledger Technology*), no caso o *blockchain,* fornecem operações confiáveis e descentralizadas, nomeadamente de troca de *tokens*, de armazenamento de metadados e da execução de programas e outros serviços, que a serem usadas em *IoT*, podem rastrear elementos físicos e digitais, a criação de metadados *IoT*, serviços de gestão descentralizada do controlo de acesso, a atualização descentralizada e confiável de *firmware*. (Roman-Castro et al., 2018)

Os dois tipos de novas tecnologias passam pelo SDN (*Software Defined Network)* e pelo *blockchain* que convergem com as soluções de segurança *IoT*. O SDN separa o controlo de rede e o controlo de dados, permitindo o controlo centralizado e a gestão dinâmica da rede para a alocação de recursos aos dispositivos de *IoT*. O trabalho de Shaghaghi, Kaafar, Buyya, & Jha (2018) estabelece um conjunto de requisitos para uma solução de segurança *IoT* e analisa as soluções existentes em relação a esses requisitos. O *blockchain* pode resolver os problemas de confiabilidade, segurança, escalabilidade e QoS (*Quality of Service*). O *blockchain* aplicado ao *IoT* permite a descentralização, pseudoanonimato e transações seguras. (Mohamad Noor & Hassan, 2019)

A tecnologia *blockchain* aplicada a sistemas *IoT* em larga escala permite que: os dados sejam à prova de adulteração; se confie menos embora se estabeleça a possibilidade de troca de mensagens, mais robusta e mais confiável; os dados sejam mais privados; se registe as ações históricas e os dados de transações antigas dos dispositivos "inteligentes"; se partilhe os ficheiros distribuídos; se elimine a autoridade única de controlo; se reduzam

os custos no desenvolvimento da infraestrutura; se aumente a confiança; e se acelere as transações. (Kumar & Mallick, 2018)

A atividade essencial de uma rede *blockchain* é de garantir que os nós confiáveis da rede cheguem a acordo de um único registo de transações, à prova de adulteração. A rede deve tolerar que uma parte dos nós que se desviam desse registo canónico. A rede *blockchain* pode ser resumida em quatro níveis de implementação: os protocolos de organização de dados e rede, os protocolos de consenso distribuído, a estrutura de organização autónoma baseada em máquinas virtuais (MV) distribuídas e a implementação de aplicações com interfaces homem-máquina (W. Wang et al., 2018)

Em síntese, as questões e os desafios que passam pelo o recurso de tecnologias *blockchain,* passam por serviços mais confiáveis e convenientes, mas em que as questões de segurança se mantêm na necessidade de sermos cautelosos na escolha das soluções a adotar. (Lin & Liao, 2017)

A tecnologia *blockchain* poderá dar melhor segurança, especialmente para dados confidenciais e em aplicações de *blockchain* em que seja necessário promover a transparência e imutabilidade. (Stephen & Alex, 2018)

2.5. Arquiteturas e Taxonomia

A taxonomia proposta por Xu et al. (2017) revela as principais características arquitetónicas de *blockchains* e o impacto nas suas principais decisões de design. A decisão de *design* como projeto de *blockchain* carateriza-se por a estrutura de dados, o protocolo de consenso, a configuração de protocolo e o novo *blockchain,* orientada a uma segurança refletida e a uma escalabilidade prudente. Estas opções em detalhe são classificadas com o respetivo impacto, através de propriedades fundamentais, como a eficiência de custos, o desempenho e a flexibilidade.

A taxonomia pode mostrar o impacto de diferentes opções de *design* sobre os atributos de qualidade e permite que a análise de atributos de qualidade forneça uma base para a comparação.

O desenho de novas formas de arquiteturas de software distribuídas passa por definir onde o acordo e a partilha podem ser estabelecidos sem confiar num ponto de integração central. O *blockchain* considera-se como uma peça de software de ligação com uma complexa estrutura interna, de várias configurações e diferentes variáveis, o que implica

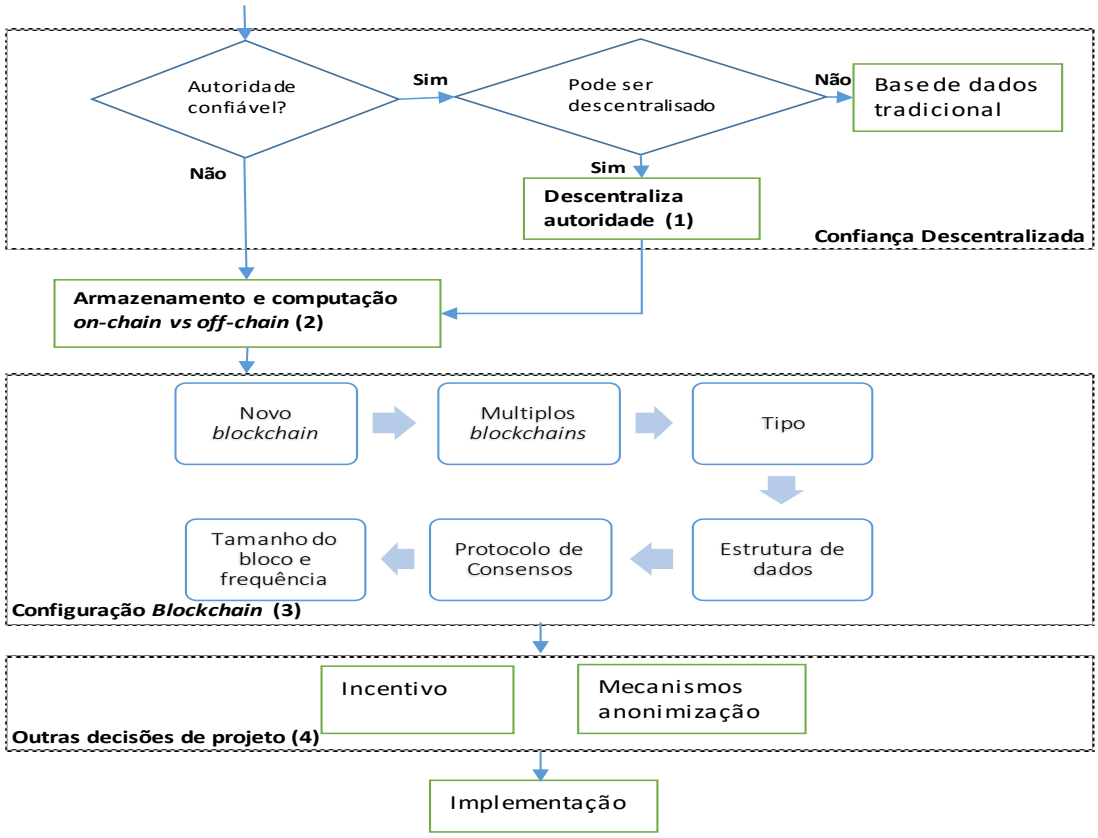
definir uma taxonomia para classificar, comparar e avaliar o impacto sobre as arquiteturas de software.

A Figura II.4, adaptada da figura 1 de Xu et al. (2017), apresenta o processo de projeto para sistemas suportados em *blockchain* e carateriza as seguintes quatro etapas de *design:*

1. O *design* arquitetural quanto à descentralização, em que a descentralização incide na responsabilidade e capacidade de um local central ou autoridade, onde existe um gama de possibilidades entre a descentralização e a centralização, com as duas opções para a descentralização parcial: a permissão e a verificação.
    a. A permissão, em vez de participação pública anónima, num *blockchain* pode ser permitida que uma ou mais autoridades possam agir como uma entrada para a participação.
    b. A verificação, em que o ambiente de execução dum *blockchain* é autossuficiente e só pode aceder à informação presente numa transação ou no histórico de transações do *blockchain,* e aos estados de sistemas externos não são diretamente acessíveis.
2. O *design* arquitetural em relação ao armazenamento e à computação, em que os *blockchains* proporcionam propriedades únicas, quanto à quantidade de poder computacional e ao espaço de armazenamento de dados, verificando-se que ainda são limitados. A eficiência de custos, o desempenho e a flexibilidade são as principais decisões de *design* para o uso de *blockchain,* o que incluí a escolha de quais os dados e a computação que deve ser colocado em cadeia e o que deve ser mantido fora da cadeia.
    a. Os dados do item tratam um procedimento comum para a gestão de dados em sistemas baseados em *blockchain* para armazenar dados brutos fora de cadeia, e de armazenar em cadeia apenas metadados, pequenos dados críticos, e *hash* dos dados brutos.
    b. A coleção do item trata do conceito de recolha de dados comum em *blockchains*, quando se utiliza *blockchains* como um registo.
3. O *design* arquitetural em relação à configuração de *blockchain,* onde se consideram várias opções de configuração para usar *blockchain,* como decisão de projeto pretende-se ter um objetivo para usar um *blockchain* público, consórcio / *blockchain* comunidade ou *blockchain* privado.

4. Nos outros projetos arquitetónicos e de implantação, as outras opções de *design* passam pela preocupação de anonimato e incentivos, e o impacto da implantação.
    a. O anonimato refere-se às diferentes técnicas que têm sido propostas para preservar o anonimato no *blockchain*.
    b. O incentivo permite para os *blockchains* e suas aplicações, principalmente para os *blockchains* públicos, introduzir incentivos financeiros ou mecanismos de reputação e classificação, para conseguir a adesão de mineiros à rede, para validar transações e gerar blocos corretamente.
    c. A implantação de *blockchain* também tem impacto sobre os atributos de qualidade do sistema.

Figura II.4 - Processo de projeto para sistemas suportados em *blockchain*



Adaptada da figura 1, de Xu et al. (2017)

A tecnologia blockchain é usada em cenários onde nenhuma autoridade confiável única é necessária e a autoridade confiável pode ser descentralizada ou parcialmente descentralizada. Os projetos de blockchain relacionados com decisões de design em relação à (des)centralização são ponderados com o seu impacto (1 - menos favorável, 2 - neutral e 3 - mais favorável) sobre as propriedades de qualidade (propriedades

fundamentais, eficiência de custos, atuação e flexibilidade) são discutidos na Tabela II.6, adaptada da tabela I de Xu et al. (2017). As limitações de blockchains são a próxima decisão sobre a divisão da computação e o armazenamento de dados entre as cadeias *on* e *off*.

Tabela II.16 - Projeto de *blockchain* relacionados com decisões de *design*

Decisão	**Opção**	**Impacto**			
		Propriedades fundamentais	**Eficiência de custos**	**Atuação**	**Pontos Falha**
Totalmente centralizado	Serviços com um único fornecedor (exemplo, governos, tribunais)	1	3	3	1
	Serviços com prestadores alternativos (por exemplo, serviços bancários, pagamentos online, serviços de *Cloud*)				
Parcialmente centralizado e Parcialmente descentralizada	*Blockchain* com permissão com permissões para operações refinadas sobre o nível de transação (por exemplo, a permissão para criar ativos)	2	2	2	-
	Com permissão *blockchain* com os mineiros com permissão (escrever), mas nós normais de menor permissão (ler)				
Totalmente descentralizada	*Blockchain* com menos permissão	3	1	1	Maioria (nós, poder, participação)
Verificador	Verificador único de confiança dos sinais de rede (verificador externo transações válidas; verificador interno utiliza o estado externo previamente injetado)	2	2	2	1
	M-de-N verificador de confiança pela rede	3	1	1	M
	Verificador de confiança ad hoc por parte dos participantes envolvidos	1	3	2	1 (escolha per ad hoc)

Adaptada da tabela I de Xu et al. (2017)

As decisões de design relacionados com decisões de conceção de projetos de blockchain em relação ao armazenamento e cálculo são analisadas através do seu impacto (1 - pouco favorável, 2 - menos favorável, 3 - mais favorável e 4 - muito favorável) relativo sobre as propriedades de qualidade (propriedades fundamentais, eficiência de custos, atuação e flexibilidade) e são discutidos na Tabela II.17, adaptada da tabela II de Xu et al. (2017). Depois disso, um conjunto de decisões de *design*, sobre a necessidade de configuração blockchain, tem de ser feito, tais como, o tipo de *blockchain*, o protocolo de consenso, o tamanho do bloco e a frequência.

Tabela II.17 - Projeto de *blockchain* relacionados com decisões de conceção.

Decisão		**Opção**	**Impacto**			
			Propriedades fundamentais	**Eficiência de custos**	**Atuação**	**Flexibilidade**
Dados do item	Na cadeia	Embutido na operação (Bitcoin)	4	1	1	2
		Embutido na operação (Ethereum Pública)		4	1	3
		Contrato "inteligente" variável (Ethereum Público)		2	3	1
		Contrato "inteligente" de *evento log* (Ethereum Público)		3	2	2
	Cadeia *off*	Privado / nuvem de terceiros	1	^ Kb Insignificante	4	4

Decisão		Opção	Impacto			
			Propriedades fundamentais	**Eficiência de custos**	**Atuação**	**Flexibilidade**
		Sistema *Peer-to-Peer*		4	3	3
Coleção de itens	Na cadeia	Contrato inteligente	4	4 (público)	4	1
		Cadeia separada		1 (público)	1	4
Computação	Na cadeia	Restrições de transação	4	1	1	1
		Contrato inteligente				
	Cadeia *off*	Privado / nuvem de terceiros	1	4	4	4

Adaptada da tabela II de Xu et al. (2017)

As decisões de conceção sobre configuração *blockchain* são discutidos na Tabela II.18, adaptada da tabela III de Xu et al. (2017), com a avaliação qualitativa (1 - menos favorável, 2 - neutral e 3 - mais favorável) das propriedades de qualidade.

Tabela II.18 - Projetos *blockchain* relacionados com decisões de projeto sobre a configuração *blockchain*.

Decisão		Opção	Impacto			
			Propriedades fundamentais	**Eficiência de custos**	**Atuação**	**Flexibilidade**
Âmbito *Blockchain*		*Blockchain* público	3	1	1	1
		Blockchain comunidade/consórcio	2	2	2	2
		Blockchain privado	1	3	3	3
Estrutura de dados		*Blockchain*	3	1	1	1
		GHOST	2	2	2	1
		BlockDAG	1	3	3	3
		Testemunha segregada	3	2	1	1
Protocolo de consenso	Abordagem Segurança	Prova-de-obra	3	1	1	1
		Prova de recuperabilidade	3	1	1	1
		Prova-de-jogo	2	2	2	3
		BFT (tolerância a falhas bizantinas)	1	3	3	1
	Abordagem Escalabilidade	Bitcoin-NG	3	1	1	1
		Protocolo da operação de cadeia Off	1	3	2	3
		Mini-*blockchain*	2	2	1	2
Protocolo configuração	Abordagem Segurança	Confirmação X-bloco	1	1	1	3
		Ponto de verificação *(checkpointing)*	3	3	3	1
	Abordagem Escalabilidade	Tamanho do bloco original e frequência	3	**n/d**	1	**n/d**
		Tempo de mineração tamanho do aumento / diminuição bloco	1	**n/d**	3	**n/d**
Novo *blockchain*	Abordagem Segurança	Mineração incorporada	3	2	1	1
		Blockchain popular de gancho ao nível de transação	2	1	2	3
		Prova de "queimadura" (*Proof-of-burn*)	1	1	3	2
	Abordagem Escalabilidade	Correntes laterais	3	1	1	1
		Vários *blockchains* privados	1	3	3	3

Adaptada da tabela III de Xu et al. (2017)

A taxonomia poderá servir para comparar *blockchains*, definir corretamente o projeto e permitir a avaliação de arquiteturas de software suportadas na tecnologia *blockchain*, através das características dos *blockchains* e o seu impacto para diferentes cenários de decisão a partir de atributos de desempenho e de qualidade, nomeadamente de disponibilidade, segurança e desempenho.

2.6. Aplicações da tecnologia *blockchain*

As aplicações do *blockchain* começam a ser globais e principalmente nos domínios das aplicações *smarts*. De seguida revê-se vários artigos, alguns já referidos, que analisam projetos de aplicação da tecnologia *blockchain*, principalmente no domínio dos *smart places* suportados por *IoT*.

Dorri, Kanhere, Jurdak, & Gauravaram (2017) descrevem os componentes principais duma *smart home* (dispositivos *IoT*, armazenamento local, o mineiro (*miner*) e o BC local) e analisa as várias transações e procedimentos associados a ela, com a preocupação sobre segurança e privacidade. A simulação da *smart home* demonstra que os custos gerais incorridos pelo método descrito são baixos e geríveis para dispositivos *IoT* de baixo recurso e são aceitáveis, dados os benefícios de segurança e privacidade oferecidos.

Ra & Lee (2018) apresentam uma solução baseada em *blockchain* que promove a confidencialidade através de uma chave do grupo e através da gestão de chaves com base na cadeia, num ambiente *smart home*, usando a árvore Merkle Estendida e a autenticação e comunicação baseadas em KSI (*Keyless Signature Infrastructure*).

Yli-Huumo, Ko, Choi, Park, & Smolander (2016) apresentam como exemplos os protótipos de aplicativos desenvolvidos e sugeridos para o uso do *blockchain* noutros ambientes, como o *IoT*, os contratos "inteligentes", a propriedade inteligente, a distribuição de conteúdo digital, o *botnet* e os protocolos de transmissão P2P, usados em ambiente descentralizado. Isso mostra que a tecnologia *blockchain* não está limitada a aplicações em criptografia.

Hammi, Hammi, Bellot, & Serhrouchni (2018) apresentam uma solução em tecnologia *blockchain* para definir zonas virtuais seguras onde os equipamento *IoT* se podem identificar e confiar uns nos outros.

Jabbari & Kaminsky (2018) argumentam que o *blockchain* tem potencial para promover as cadeias de abastecimento, mas continuam a ser necessárias novas pesquisa e que identificam quatro categorias de questões: Como podem os produtos físicos ser ligados ao *ledger* digital? Como podem as redes ativadas por *blockchain* ser ligadas a outros mercados externos? Como pode ser melhorada a estrutura do *blockchain* para permitir as estruturas da cadeia de fornecimentos mais complexas? Como pode ser reservado espaço suficiente para armazenar a quantidade de informação exigida pelas cadeias de fornecimento? Estas questões podem vir a ser revistas no contexto dos mercados de dados

suportados em *blockchain* e com o recurso a *smart contracts* para interligar as diversas plataformas de fornecimento.

Qu, Tao, Zhang, Hong, & Yuan (2018) apresentam as formas de estruturas *blockchain* (*BCS-Blockchain Structures*) projetados para estabelecer a relação entre *blockchain* e *IoT*.

Os dipositivos *IoT* são analisados em quatro perspetivas: a exploração das limitações mais importantes dos dispositivos *IoT* e quais as soluções; a classificação dos ataques de *IoT*; os mecanismos e as arquiteturas de autenticação e de controlo de acesso; e os problemas de segurança nas diferentes camadas. (Yang et al., 2017)

Gaetani et al. (2016) apresentam uma base de dados baseada em *blockchain* para garantir a integridade dos dados em ambientes de *cloud computing* em que se pretende resolver as ameaças à integridade de dados e a adulteração de dados, que pode afetar de forma maliciosa decisões criticas. Nos ambientes de computação em nuvem, os proprietários de dados não conseguem controlar aspetos importantes, o armazenamento e o controlo de acessos. A utilização do *blockchain*, para minimizar as ameaças de integridade de dados embora pareça ser uma escolha natural, ainda apresenta várias limitações como o baixo rendimento, a alta latência e alguma instabilidade.

A tecnologia *blockchain* pode ser usada para melhorar a robustez e segurança da rede elétrica (Liang et al., 2018) através de um *framework* distribuído baseado em *blockchain* para a proteção dos dados e para aumentar a capacidade autodefensiva dos sistemas elétricos de energia contra ataques cibernéticos. As caraterísticas do *blockchain* no *framework* proposto passa por uma rede privada, o iniciador de transação deve ser completamente automático, o conteúdo da transação deve ser a recolha de medições, as transações são independentes e não relacionadas, a verificação de blocos históricos antes do processo de votação é desnecessária, a velocidade de conexão da cadeia muito mais rápida que a clássica de 7 transações por segundo (bitcoin), não existe recompensa para o nó, não existe o ataque de duplo gasto, e é difícil o ataque de 51% dado que o limite é ajustável. O caso de estudo baseou-se no sistema de *benchmarking* IEEE-118 que é composto por 54 geradores, 118 nós e 186 ramos, usado como base de cenários de ataque cibernético entre o método existente e a estrutura proposta, representados em dois cenários. O trabalho mostra que o *blockchain* pode ser considerado uma solução promissora na segurança de dados nos sistemas de energia.

3. Mercado de Dados

Neste ponto destaca-se a aplicação da tecnologia *blockchain* para os *data marketplaces*. Este destaque traduz a importância destes mercados de dados no contexto das *smart cities*, principalmente dos dados abertos e na necessidade de se fornecer dados de fornecedores confiáveis, de fontes confiáveis e com dados confiáveis.

Os mercados de dados, no contexto dos *smart places*, com as enormes quantidades de dados, principalmente de *IoT*, revelam diversas abordagens centralizadas e descentralizadas. No artigo (Brandão et al., 2019) desenvolvido no âmbito deste trabalho de investigação são analisados os mercados de dados descentralizados suportados na tecnologia *blockchain* como forma de garantir a confiança na cadeia de fornecimento dos dados, aos atores que intervêm no mercado e às fontes de dados, através da contratualização através dos *smart contracts*, o fornecimento dos dados pelos produtores de dados, o controlo dos fluxos dos dados e o acesso aos dados.

Os mercados de dados podem estar baseados numa arquitetura centralizada ou descentralizada e em três modelos de abertura: abertos, fechados ou mistos.

Os dados baseiam-se em dados dinâmicos, conjuntos de dados estáticos, através de fluxos dinâmicos e estáticos. O acesso aos dados realiza-se através de APIs externas ou internas, de *download* ou plataformas de *blockchain*, com o objetivo de obter dados e informação de qualidade, utilizando o *feedback* do utilizador, a integridade dos dados e a proveniência dos dados.

As características mais importantes para os participantes nos mercados de dados passam por: um catálogo de dados com funções de pesquisa; o controlo de acesso; ferramentas para criar acordos adequados; monetizações adequadas para as transações; monitorização do cumprimento dos *SLAs* e resolução de disputas; e ferramentas para avaliar a qualidade e a confiabilidade dos dados e dos seus fornecedores.

A confiança é central para avaliar a qualidade e a fiabilidade dos dados e dos seus fornecedores. A segurança, com a gestão, autenticação e autorização de identidades, é integrada nas soluções de mercado.

O papel dos mercados de dados é crucial na economia da informação e do conhecimento, o que torna os dados confiáveis fundamentais para a automação de regras na interação máquina a máquina, na aprendizagem automática, na aplicação de algoritmos de IA

(Inteligência Artificial), na tomada de decisões e para criar novas oportunidades de negócios.

O Valor dos dados será condicionado por fragilidades e por possíveis violações cibernéticas, que aumentam as perdas financeiras, envolvendo apólices de seguro sobre os dados, para proteção comercial. Os mercados de dados promoverão a terceirização cruzada com vários produtores de dados, envolvendo diferentes formatos de dados, nomeadamente de dados da *IoT* e de *crowdsourcing*.

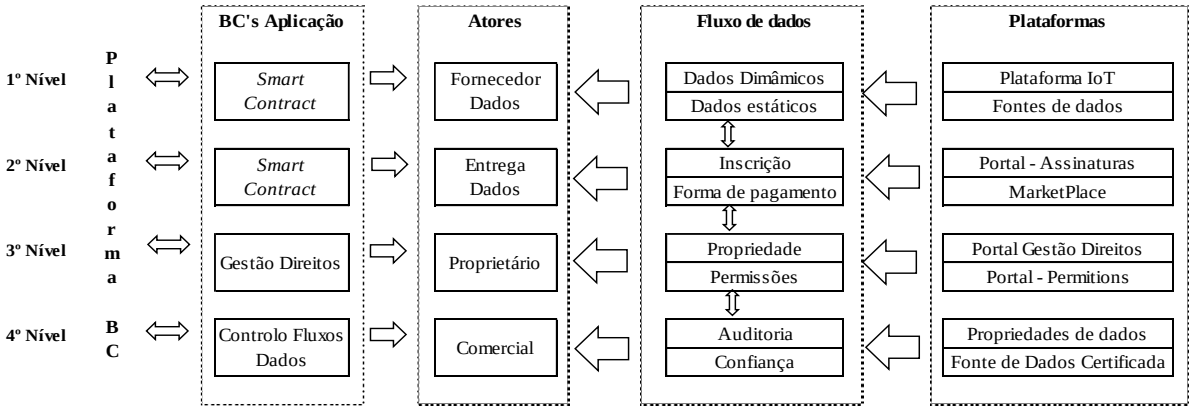
O controlo da cadeia de fornecimento de dados começa na fonte confiável, continua no processo de tratamento e criação de Valor e termina com a satisfação da entrega. Para garantir segurança e confiabilidade, propõem-se quatro níveis de aplicação, adicionando funcionalidades específicas, suportadas na tecnologia *blockchain*.

O problema de confiança na origem dos dados pode ser resolvido por um modelo e uma arquitetura suportado em *blockchain* que abordam os quatro níveis desse problema:

- O fornecimento de dados;
- A entrega de dados;
- A gestão de direitos e permissões de acesso;
- O produtor de dados.

Este modelo pretende garantir a origem dos dados base e a confiança em todo o processo. A Figura II.5, adaptada da figura 3, de (Brandão et al., 2018a) apresenta os atores, fluxos de dados, plataformas e formas de aplicação de *blockchain*.

Figura II.5 - Mercado de dados baseado em *blockchain*



Adaptada da figura 3, de Brandão et al. (2019)

Ivanschitz, Lampoltshammer, Mireles, Revenko, & Schlarb (2018) apresentam um mercado de dados com base em múltiplos repositórios de dados descentralizadas,

permitindo o acesso através de um portal central, apoiado em metadados normalizados e semanticamente melhorados, confiáveis e consistentes, para funcionalidades eficientes de pesquisa e recomendação apoiadas por um catálogo central. Nestes repositórios descentralizados cada nó participante implementa o conjunto definido de serviços e interfaces como um rastreador de dados, um mapeador de metadados, um nó de *blockchain* e componentes de gestão e armazenamento de dados, e um modelo conceitual comum para permitir interfaces padrão que facilitem a interoperabilidade e a utilização de conjuntos de dados.

O trabalho Sterling (Hynes et al., 2018) apresenta um mercado de dados descentralizado de dados privados, com a distribuição e preservação da privacidade dos dados através de *smart contracts* suportados em *blockchain*. Os *smart contracts,* imutáveis e irrevogáveis, dos fornecedores de dados para os consumidores, representam os interesses dos seus criadores ao avaliar automaticamente os dados, através de mecanismos para que os fornecedores dos dados possam controlar a utilização dos seus dados, através da verificação automática dos contratos de consumo de dados e manifestar restrições, como os preços e a privacidade diferencial. Este mercado de dados permite que a economia resultante confirme que os interesses de todas as partes estão alinhados.

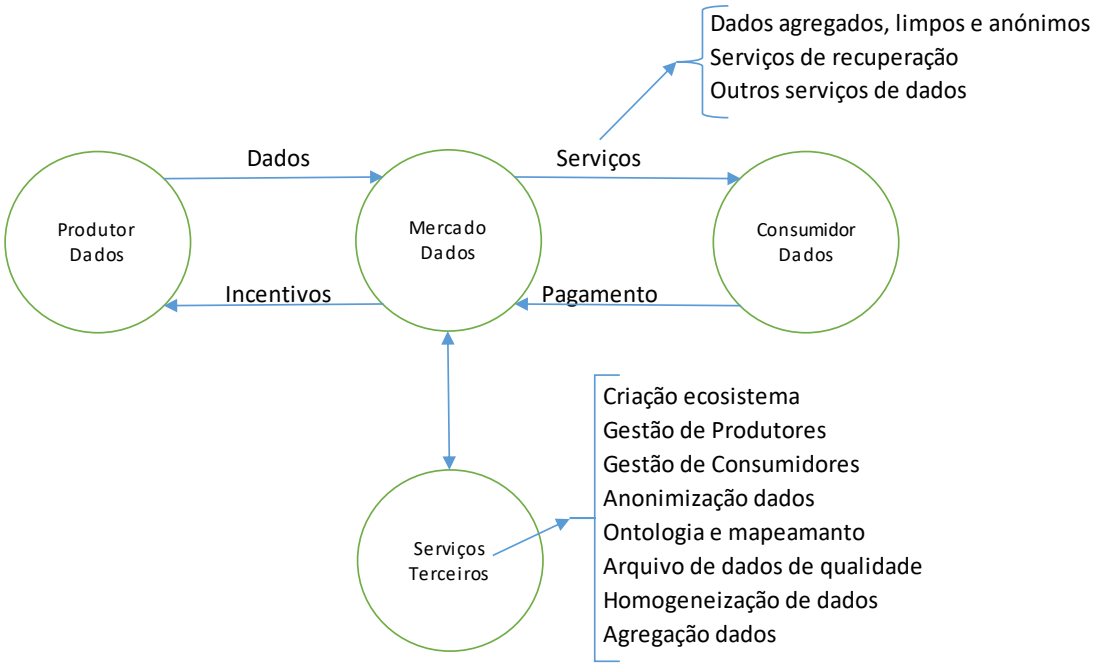
No mercado de dados apresentado por Agarwal, Dahleh, & Sarkar (2018) é considerada uma solução algorítmica para criar o mercado de dados, com um mecanismo em tempo real de correspondência robusta para comprar de forma eficiente e vender dados de testes para tarefas de aprendizagem automática. Nesta solução é considerada a monetização de dados e modelos pré-testes para fixar o preço de dados de testes entre compradores e vendedores. Estes dados são livremente replicáveis, o seu Valor dependente da correlação com outros dados, das tarefas de previsão, da precisão e da utilidade dos dados.

Chakrabarti & Chaudhuri (2017) discutem como a tecnologia *blockchain* pode ser usada no mercado de dados associados aos processos de negócio no setor do retalho para beneficiar os clientes e os retalhistas, com a transparência sobre a origem dos produtos, o combate à falsificação, a gestão mais eficiente da cadeia de fornecimento e melhorar a gestão de fidelidade com o aperfeiçoando do perfil dos clientes.

A proposta de utilização do modelo de serviço de mercado de dados para resolver a partilha de dados científicos é apresentada por Ghosh (2018), como plataforma para a partilha de dados para a comunidade científica, analisando os desafios motivacionais e as

práticas para a troca de dados científicos. Os desafios na partilha de dados passam por motivar a colaboração, as múltiplas estruturas e formatos dos dados, evitar a incompletude, duplicação e inconsistência de dados, diversos contextos, diferente organização de dados, a dinâmica de dados, a gestão da propriedade dos dados, a criação de uma comunidade de produtores de dados e consumidores formando um ecossistema de dados criado para garantir a qualidade dos dados e com preços adequados. A Figura II.6, adaptada da figura 1 de Ghosh (2018), apresenta um possível modelo geral para um *marketplace* de dados.

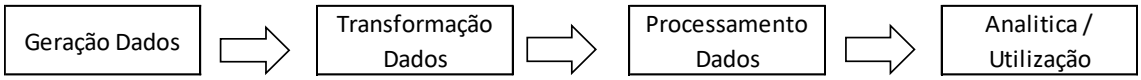
Figura II.6 - Modelo geral do marketplace de dados



Adaptada da figura 1, de Ghosh (2018)

A cadeia de fornecimento de dados é apresentada de forma simplificada na Figura II.7, adaptada da figura 1 de (Brandão et al., 2019), em que os fornecedores que entregam os dados brutos dos produtores (geração de dados), que convertem os dados em produtos para "armazéns" de dados (transformação de dados), que armazenam dados em centros de distribuição ao proporcionarem aos retalhistas dados tratados (processamento de dados) que os filtram, agregam e formatam permitindo diversas visualizações e personalizações para os entregar ao utilizador (analítica/ utilização).

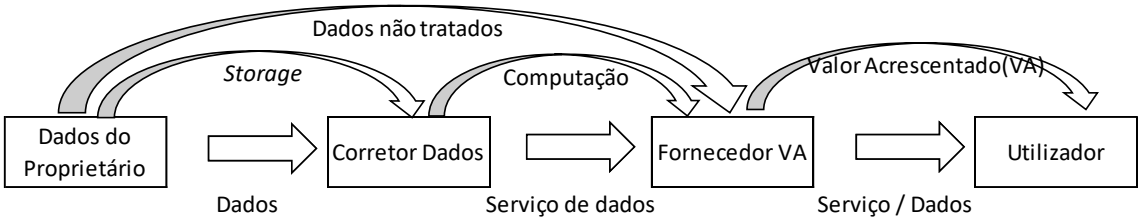
Figura II.7 - Modelo simplificado do marketplace de dados



Adaptada da figura 1 de Brandão, Mamede, & Gonçalves (2019)

A Figura II.8, adaptada da figura 2 de Brandão, Mamede, & Gonçalves (2019), apresenta um modelo associado de mercado de dados, com os atores desse mercado: o proprietário dos dados, o corretor de dados, o fornecedor de serviços de Valor acrescentado (VA) e o utilizador final.

Figura II.8 - Modelo do mercado de dados e os atores



Adaptada da figura 2 de Brandão, Mamede, & Gonçalves (2019)

Dao, Alistarh, Musat, & Zhang (2018) apresentam o projeto DataBrigh no âmbito da aprendizagem automática para a troca global descentralizada de dados, de gestão da propriedade e de computação confiável. Este projeto procura responder à questão: como promover o intercâmbio global de dados, que todos podem contribuir com computação e dados para treino de aplicativos de aprendizagem automática? O sistema DataBright trata-se de um mercado de dados e um mercado de computação confiável, que transforma a criação de exemplos de treino e de partilha de computação num mecanismo de investimento, em que quem contribui torna-se acionista do conjunto de dados que eles criaram.

Draskovic & Saleh (2017) apresentam um mercado de dados, *Datapace*, para dados de sensores *IoT*. Este mercado de dados é descentralizado e baseado em *blockchain.* Consideram que existem dados cuja utilização está em serem consumidos imediatamente, senão perdem valor, e dados duradouros. Mas quem recolhe os dados quer obter um lucro adicional a partir desses dados, além do propósito base dos dados. O sistema *Datapace* ativa a tokenização de valor e a economia de *token*, garante a integridade dos dados

através da guarda dos *hash* de dados, ativa os recursos de *smart contract* e fornece segurança de rede através das caraterísticas de consenso e imutabilidade do PBFT.

Smith, Ofe, & Sandberg (2016) exploram a proposta de Valor de um mercado de dados abertos, como inovação em serviços digitais, procurando ultrapassar as barreiras de adoção de dados abertos, através de um estudo de caso exploratório, considerando os cinco valores percebidos mais valorizados e que passam por: a menor complexidade da tarefa, o maior acesso ao conhecimento, as maiores possibilidades de influenciar, o menor risco e a maior visibilidade. Neste trabalho verificou-se que para os utilizadores de dados abertos o Valor está no portal central que fornece o melhor acesso a dados abertos e aos serviços de suporte associados, e poder aceder aos fornecedores de dados abertos nas atividades de partilha de conhecimento, permitindo a transferência de conhecimento dentro dos ecossistemas.

A plataforma Enigma (Zyskind et al., 2015) de computação descentralizada pretende garantir a privacidade de diferentes partes que podem armazenar dados conjuntamente e executar cálculos sobre os dados e simultaneamente manter os dados privados. O modelo computacional da Enigma baseia-se numa versão otimizada de computação multipartidária segura, garantida por um regime de partilha secreta verificável. A Enigma tem uma tabela de *hash* distribuída (*DHT-Distributed Hash-Table*) fora da cadeia (*off-chain*) que é acessível através do *blockchain,* que armazena apenas as referências dos dados. Os dados privados devem ser criptografados antes do armazenamento e do controlo de acesso serem programados no *blockchain*.

O mercado de dados MARSA (Cao et al., 2016) apresenta um mercado dinâmico baseado em nuvem de dados de sensorização humana quase em tempo real para que diferentes partes interessadas possam vender e comprar esse tipo de dados. Esta projeto apresenta técnicas para selecionar que tipos de dados e como gerir os contratos de dados com base em diferentes modelos de custos, qualidade dos dados, e os direitos sobre os dados. A plataforma considera soluções para diferentes transferências de dados para possibilitar um mecanismo de comunicação aberta e escalável entre vendedores (fornecedores de dados) e compradores (consumidores de dados).

O novo modelo comum de informação do veículo *(CVIM - Common Vehicle Information Model)* (Pillmann et al., 2017) pode potenciar a criação de mercados de *big data* com os dados dos veículos automóveis. O projeto europeu AutoMat pretende desenvolver um

mercado aberto fornecendo um único ponto de acesso para dados do veículo independente da marca. O trabalho apresenta uma arquitetura para este mercado de dados como facilitador de serviços de dados transversal ao setor do veículo automóvel. O modelo de dados é aberto e harmonizado, que permite a agregação de dados e conjuntos de dados genéricos independente da marca. Aplicaram os conceitos AutoMat e o protótipo a casos de uso de previsão de tempo e qualidade da estrada a aplicações não automóveis.

A troca segura de dados (*SDE-Secure Data Exchange*) (Gilad-Bachrach et al., 2017) pretende garantir o intercâmbio de dados entre diversas plataformas do mercado em nuvem. O sistema deve respeitar os requisitos de: aproveitar a infraestrutura de armazenamento em nuvem existente; alinhar aos incentivos existentes para serviços em nuvem; e usar modelos de confiança que refletem a realidade atual dos serviços em nuvem. O mercado de nuvem (*cloud),* dos prestadores de confiança, necessita de uma solução geral de criptografia para os proprietários de vários dados armazenados nas diferentes *clouds,* permitindo que os dados privados criptografados estejam disponíveis numa *cloud* sem conluio e de forma honesta, através de um avaliador que se pretende envolver numa avaliação da segurança dos dados pertencentes a um subconjunto dos proprietários dos dados nas diversas plataformas. O resultado do trabalho passa por um protocolo prático e eficiente para permitir o SDE usar computação segura multiparte *(MPC-secure Multi-Party Computation),* numa nova adaptação do ambiente auxiliado por servidor.

Jang, Park, Lee, & Hahn (2018) propõem três níveis hierárquicos do mercado *big data* de várias fontes de dados de *IoT,* através de um modelo de mercado *big data* competitivo, várias fontes de dados, um fornecedor de serviços e clientes. Começa com o fornecedor de serviços que reúne os dados de múltiplas fontes e fornece informações importantes de dados apurados como um serviço para os clientes, que determina a aquisição de dados ideal a partir de múltiplas fontes de dados, com a restrição orçamental definida. As múltiplas fontes de dados seguem a ação do fornecedor de serviços, de forma independente, através de preços de licitação. Os resultados analíticos demonstraram que a abordagem proposta garante um ponto de equilíbrio único que maximiza o retorno para todos os participantes do mercado, podendo através da tecnologia *blockchain* ser aplicada para projetar uma estrutura totalmente descentralizada, onde todos os componentes são produtores ou consumidores.

O mercado descentralizado Wibson (Travizano et al., 2018) pretende capacitar os indivíduos para rentabilizar com segurança os seus dados pessoais. Este mercado baseado em *blockchain* proporciona aos indivíduos uma forma de vender de forma segura e anonimamente as informações num ambiente confiável. A combinação dos *smart contracts* e do *blockchain* permite aos vendedores e compradores de dados transacionar diretamente, mantendo os indivíduos a capacidade de manter o anonimato.

4. Ecossistema de Mobilidade

O ecossistema de mobilidade, numa *smart city*, passa pela gestão da procura através de uma capacidade seletiva da oferta, adotando uma estratégia de eficiência do sistema, no sentido da redução da necessidade de deslocações, com a eficiência da deslocação, procurando melhorar ou manter o meio ambientalmente sustentável, com a eficiência dos transportes e a melhoria da eficiência energética.

Os elementos centrais da mobilidade passam por *smart cities* inclusivas, novos modelos de negócio, de inovação, de tecnologia e de dados, com infraestrutura e conectividade, novos veículos e veículos mais autónomos, através de eficientes cadeias de abastecimento, suportados na eficiência energética, na otimização de carregamento, e em formas crescentes de mobilidade ativa.

Os seis principais objetivos da mobilidade "inteligente" são agrupados nas seguintes categorias: reduzir a poluição, reduzir o congestionamento do tráfego, aumentar a segurança das pessoas, reduzir a poluição sonora, melhorar a velocidade de transferência e reduzir os custos de transferência. Os quatro grupos principais de iniciativas são classificados por: as empresas e as organizações de transporte público; as empresas privadas e os cidadãos; os órgãos públicos e os governos locais; e a combinação dos atores que realizam iniciativas integradas. (Benevolo et al., 2016)

As políticas públicas revelam-se adequadas se "alimentadas" pelos dados e informação do funcionamento da cidade, o conhecimento das relações e interdependências dos diversos ecossistemas e atores, e a participação e o envolvimento dos cidadãos.

A criação das infraestruturas deverá orientar-se para as populações, ser suportadas na economia partilhada, nas energias hipocarbónicas, nas novas tecnologias, com passagens intermodais mais eficientes e com sistemas de bilhética e pagamento seguros, confiáveis, escaláveis, flexíveis, eficientes e integráveis com os produtos e serviços da cidade.

Neste contexto, os transportes devem adaptar-se às alterações para suportar as necessidades de mobilidade de pessoas e bens. Os sistemas de informação procuram mais eficiência da operação através da automatização, da segurança e da redundância.

A segurança tenta minimizar as fragilidades dos sistemas contra os ataques físicos (*security*), lógicos (cibersegurança), e contra acidentes e ações não intencionais (*safety*). Os métodos passam essencialmente pela identificação de perigos, a avaliação de riscos e controlo de danos.

As infraestruturas e os serviços da cidade estão mais interconectados, permitindo a monitorização, o controlo e a automação. Os sistemas de transporte público e privado integram-se e acedem a dados de localização, de tempo e de tráfego, melhorando a sua eficiência na intermodalidade, na segurança pública e na recuperação de desastres. A ponderação, entre os benefícios de uma cidade eficiente e uma cidade mais observada e escutada e os riscos, tem um elemento central, a garantia de que os direitos e as liberdades são protegidos. (Elmaghraby & Losavio, 2014)

Os aspetos de usabilidade das aplicações permitem aos utilizadores encontrarem informações sobre os serviços oferecidos. As métricas e os métodos utilizados para avaliar a usabilidade das aplicações relacionadas com sistemas de transporte público indicam que a satisfação, eficácia e eficiência são as métricas de usabilidade mais utilizadas. A pesquisa parece ser o método de usabilidade mais utilizado entre os investigadores, seguido por testes de campo e entrevista no desenvolvimento de sistemas de transporte público utilizáveis. (Hussain et al., 2017)

4.1. Sistemas nos transportes ferroviários de passageiros

No ecossistema de mobilidade, nas *smart cities*, os transportes públicos ferroviários de passageiros têm um papel aglutinador e estruturante no desenho dos fluxos de transportes e na grande capacidade de movimentar pessoas no espaço urbano. O trânsito ferroviário urbano nas cidades, sobretudo nas regiões, nas metrópoles e nas megacidades, desempenha um papel central nas viagens diárias e com os fluxos de passageiros sempre crescentes.

O futuro das oportunidades ferroviárias para energia e meio ambiente [52] indica que quase 200 cidades em todo o mundo possuem sistemas de metro, o comprimento combinado excede 32.000 quilómetros, em que os sistemas de metropolitano ligeiro acrescentam 21 000 quilómetros de comprimento em mais 220 cidades. Este estudo apresenta várias tendências no transporte ferroviário que passam por:

- O transporte ferroviário ser um dos pilares da mobilidade de passageiros e transporte de mercadorias.
- A ferrovia é um dos modos de transporte mais eficientes e de menor emissão, com forte dependência da eletricidade.
- A maioria das redes ferroviárias está localizada na Índia, na China, no Japão, na Europa, na América do Norte e na Federação Russa e as redes de metro e metro ligeiro operam nas principais cidades do mundo.
- O futuro do transporte ferroviário depende da resposta à crescente procura de transporte e à crescente pressão dos modos de transporte concorrentes.
- O investimento anual em infraestruturas ferroviárias aumenta para US $ 315 mil milhões em 2050, com base em projetos atuais e em vários estágios de construção e planeamento e prevê um forte crescimento nas redes ferroviárias de alta velocidade.
- O uso global da eletricidade ferroviária chegará a quase 700 TWh em 2050.
- As duas categorias, a ferrovia urbana e a de alta velocidade preveem grandes benefícios globais.

Os *drivers* para o transporte urbano (*LRV- Light Rail Vehicles*) [53] até 2021 são apresentadas na tabela seguinte:

Tabela II.19- Tendências de aquisição de metros ligeiros

***Drivers* para o transporte urbano**	**Tendência até 2021**
Urbanização e mudanças demográficas	Fortemente aumentando
Seleção de sistemas de transportes públicos	Aumentando
Novos de desenvolvimento e atualização da infraestrutura	Aumentando
Aquisições de substituição	Constante
Fundos de investimento	Fortemente aumentando

[52] The Future of Rail - https://www.aktuellhallbarhet.se/wp-content/uploads/2019/01/the-future-of-rail.pdf, acedido em 30-04-2019.
[53] LRV - https://www.sci.de/fileadmin/user_upload/MC_Studien_Flyer/Flyer_MC_LRV.pdf, acedido em 30-04-2019

O relatório da UNIFE [54] indica que o setor ferroviário continuará o seu crescimento impulsionado pela procura, inovação e legislação, e que:

- Esta indústria continuará a crescer.
- Todos continentes e todos os segmentos de produtos continuarão a crescer.
- As megatendências continuam a impulsionar a procura pelo transporte ferroviário.
- A digitalização é uma nova oportunidade.

O relatório de 2019 da UIC (*International Union of Railways*) [55] apresenta o futuro do sistema de transporte ferroviário na europa que será focado no cliente, numa visão partilhada, com o sistema de mobilidade integrado, no melhor Valor em termos de qualidade e custos, os clientes finais a receberem um serviço de qualidade, o transporte a responder de forma flexível às mudanças de procura e às condições de operação, sendo um modo seguro, confortável e sustentável em termos energéticos. Esta industria continuará a atrair o talento e a inovação.

O relatório da RSSB [56] recomenda a aplicação do método BREEAM (*Building Research Establishment Environmental Assessment Method*) para a avaliação sustentável para todos os novos desenvolvimentos de estação, parque de veículos e para grandes reformas para minimizar o carbono no ciclo de vida. A infraestrutura tem ciclos de vida longos e são fortemente controlados para fins de segurança, desempenho e satisfação do cliente, dai que se devam utilizar as oportunidades para reduções precoces de carbono nos novos projetos. Esta ferramenta é útil para avaliar o desempenho ambiental do desenvolvimento, embora não aborde as amplas questões do desenvolvimento sustentável, de adequação do local geográfico de soluções e de pegada ambiental de longo prazo. (Sewell & Fraser, 2019)

Nestes sistemas, as estações e as transferências com outros modos são pontos críticos para a perturbação da rede ferroviária. Lu & Lin (2019) propõem a aplicação de uma abordagem única de acessibilidade baseada na localização para a análise de vulnerabilidades da rede de trânsito ferroviário urbano. O método de acessibilidade que

[54] UNIFE - https://www.rolandberger.com/publications/publication_pdf/roland_berger_world_rail_market_presentation_final.pdf, acedido em 30-04-2019.
[55] UIC - https://uic.org/europe/IMG/pdf/2019_uic_railway_technical_strategy_europe.pdf, acedido em 20-04-2019
[56] RSSB - https://www.rssb.co.uk/Library/improving-industry-performance/Rail-Industry-Decarbonisation-Task-Force-Initial-Report-to-the-Rail-Minister-January%202019.pdf, acedido em 30-04-2019.

analisa a vulnerabilidade da rede rodoviária é medido pelas interrupções de estação, pelas falhas de ligação e de linha, com base na combinação do método de acessibilidade e da abordagem da teoria dos grafos. Como resultados explicam-se as características de fluxo de passageiros ferroviários, as mudanças nos custos de viagens, os modos alternativos de trânsito, a medição das consequências na rede ferroviária e as implicações para a tomada de decisões nas perturbações na rede ferroviária.

A falta de desempenho da engenharia de manutenção é uma das principais causas da má prestação de serviços e no desempenho dos negócios (Fourie & Chimusoro, 2018). O desempenho da engenharia de manutenção é medido usando vários parâmetros, que incluem a capacidade da organização para atualizar e substituir a frota, a disponibilidade de peças de reposição, a disponibilidade de competências, o fluxo de informação e a tecnologia da informação.

A manutenção é um aspeto crítico na oferta de um sistema de transporte urbano de passageiros. O processo de manutenção deve ser integrado e combinado com o método de decisão de manutenção "inteligente", baseado numa estratégia de indução de árvore de decisão para identificar a classe de equipamentos e regras que levaram a falhas semelhantes. Esta "chave" define-se como a prioridade para a reparação, a prevenção, ao prever possíveis avarias, de modo a estabelecer o programa de manutenção e de tomada de decisão. (M. Zhang, 2017)

Liu & Sun (2018) analisam as aplicações de *BIM* (*Building Information Model*) na construção do sistema ferroviário. O espaço local é limitado, a alocação de recursos é complexa e normalmente com um calendário curto, e são vários os problemas complexos de engenharia nas intervenções subterrâneas. A tecnologia BIM permite a visualização tridimensional, a parametrização, a simulação virtual, a informação (custos, opções técnicas, dimensionamento, compatibilidade, etc.) que acompanha todo o processo de projeto, revisão, construção e manutenção. A construção da plataforma de metro deve ser baseada em BIM e tecnologia em *Cloud*, com o uso de câmaras e sensores para alcançar a integração eletrónica, o controlo dinâmico da operação e a manutenção de instalações e espaços subterrâneas, para melhorar a operação e a manutenção.

A segurança é outro dos aspetos críticos a considerar no projeto de construção, manutenção e operação de um sistema urbano de transporte ferroviário. Os processos de gestão de riscos de segurança no URT (*Urban Rail Transit*), desde a fase de projeto,

apresentam fatores de risco indiretos da segurança, como os defeitos de gestão, os fatores de risco de segurança direta e dos participantes. O modelo proposto, através do método de pesquisa orientada de texto (J. Li et al., 2018), refere que para cada acidente é realizada uma descrição padronizada das informações do acidente correspondente, que permite a acumulação de dados e análise de risco. Os métodos de análise e avaliação de riscos contêm as informações de risco de segurança integradas no modelo descritivo do acidente usando pontos de acidentes, para serem geridos e controlados.

De forma geral os sistemas URT representam desafios para entender as ameaças cibernéticas e o seu impacto, de modo a priorizarem os investimentos e os esforços de robustez.

O exemplo do projeto SECUR-ED [57] apresenta uma orientação para as organizações de segurança encarregadas do transporte público, em especial os operadores, nas operações diárias, nos procedimentos otimizados e na visão dos futuros sistemas de segurança.

Song, Li, List, Deng, & Lu (2017) apresentam um método para estudar os fatores de vulnerabilidade de um sistema URT (*Urban Rail Transit*), baseado no processo de hierarquia analítica (*AHP-Analytical Hierarchy Process*) e de modelação estrutural interpretativa (*ISM-Interpretative Structural Modeling*) cujos resultados fornece informações para a tomada de decisão, com estratégias pró-ativas e políticas de reforço da segurança e a promoção do desenvolvimento sustentável do espaço urbano. Na figura seguinte, adaptada da tabela 1 de Song, Li, List, Deng, & Lu (2017) apresenta-se as 6 dimensões que agrupam os 21 fatores de vulnerabilidade.

Tabela II.20 - Fatores de Vulnerabilidade no URT

Dimensão	**Fatores**
Individual (B1)	Capacidade técnica individual (C1)
	Conscientização da segurança individual (C2)
	Disciplina individual (C3)
	Carga de trabalho individual e *stress* (C4)
	Estado físico e fisiológico individual (C5)
Equipamento / instalações (B2)	Condição do equipamento / instalação (C6)
	Desempenho de equipamentos / instalações (C7)
	Proteção de equipamentos / instalações (C8)

[57] SECUR-ED Project - http://www.secur-ed.eu/wp-content/uploads/2014/12/SECUR-ED_White_Paper_Final.pdf , acedido em 30-04-2019.

Dimensão	Fatores
Meio Ambiente (B3)	Ambiente natural (C9)
	Meio social (C10)
	Ambiente operacional (C11)
Gestão (B4)	Investimento em segurança (C12)
	Educação e formação (C13)
	Regras e regulamentos (C14)
	Estrutura Organizacional (C15)
Estrutura (B5)	Layout da estação (C16)
	Topologia de rede (C17)
	Interdependência de equipamento / instalação (C18)
Emergência (B6)	Plano de gestão de emergência (C19)
	Execução de resposta de emergência (C20)
	Configuração do sistema de suporte de emergência (C21)

Adaptada da tabela 1 de Song, Li, List, Deng, & Lu (2017)

Os recursos humanos constituem-se como a peça fundamental nestes sistemas. A avaliação das cargas de trabalho conduz a práticas mais colaborativas e sustentáveis que podem minimizar os riscos de sobrecarga e de falhas. A abordagem de sistemas para prever e medir a carga de trabalho dos sistemas de gestão do tráfego ferroviário, através do projeto In2Rail (Evans, 2017), explora diversas questões sobre as principais princípios de carga de trabalho, através do aumento de estilos de trabalho colaborativo e responsabilidades partilhadas, com maior flexibilidade, mais configurável para suportar os requisitos de informação para cada função específica e apoiar cada função durante diferentes cenários. O conjunto de ferramentas In2Rail pretendeu fazer previsões de carga de trabalho de sistemas de gestão de tráfego com um nível mais alto de confiança, que as técnicas existentes de medição da carga de trabalho, para apoiar o desenvolvimento contínuo de pessoas, processos e tecnologia.

4.2. Tecnologias de informação nos sistemas de transportes públicos

As tecnologias de informação têm suportado os operadores de transportes públicos na melhoria da segurança e da qualidade do serviço prestado aos seus clientes. A segurança das infraestruturas orienta-se para a promoção de metodologias de gestão de risco com a avaliação das vulnerabilidades do sistema e o desenho de procedimentos, boas práticas e tecnologias de proteção contra ciberataques. A avaliação torna-se permanente e coloca os sistemas em monitorização contínua, adensada pela infraestrutura tecnológica mais complexa e interdependente.

O sistema de informação de um sistema de transporte urbano de passageiros pode ser subdividido em quatro sistemas de informação de apoio, de:

- Controlo e Gestão;
- Exploração;
- Gestão do Tráfego Ferroviário;
- Material Circulante.

Nos pontos seguintes será detalhado o conjunto de sistemas que podem constituir cada um dos sistemas de informação de apoio.

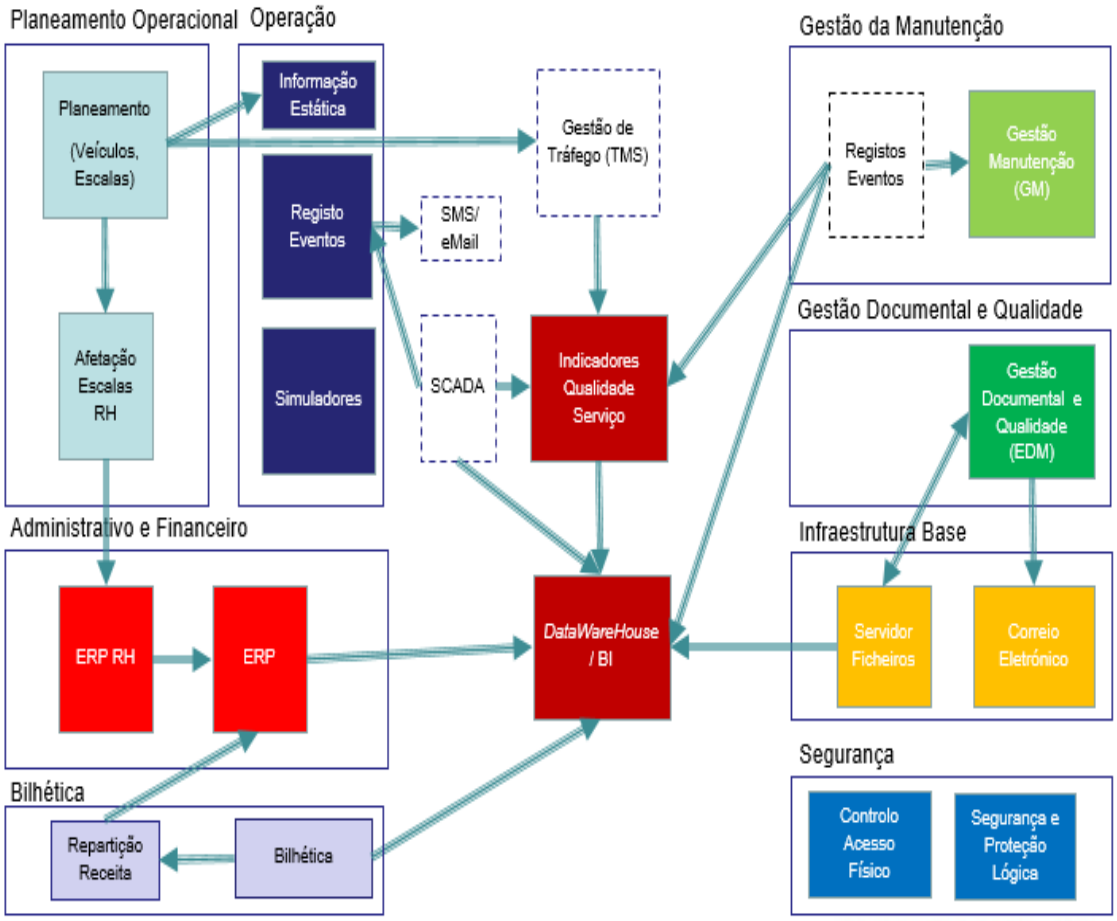
4.2.1. Sistema de Informação de Apoio ao Controlo e Gestão

Este sistema abrange o conjunto de aplicações de *backoffice*, de gestão, controlo e planeamento que permitem dotar as empresas de transportes com as funções base para responder às obrigações legais, fiscais, de reporte, de análise e avaliação.

Neste domínio surgem as aplicações de gestão (*ERP-Enterprise Resource Planning*), de gestão de recursos humanos, de planeamento operacional (oferta teórica programada), de afetação de veículos e escalas, de gestão de eventos/incidentes, de gestão da manutenção, de gestão documental e qualidade, a infraestrutura base, a segurança física e lógica, os indicadores de qualidade serviço a partir da *datawarehouse* e ferramentas de BI (*Business Intelligence*).

Estas aplicações e fluxos de dados encontram-se descritos na figura seguinte.

Figura II.9 - Sistema de Informação de Apoio ao Planeamento e Gestão



O planeamento operacional, referente aos serviços de veículos e escalas de recursos humanos, apresenta a graficagem da circulação, os serviços teóricos e a resolução de incompatibilidades, e a afetação a escalas teóricas de recursos humanos. A informação estática fica disponibilizada pela aplicação de geração/formatação de horários.

A aplicação ERP pode incluir a contabilidade, as compras, o comercial, o financeiro e a logística. Do sistema de bilhética é recebido o valor da repartição de receita num sistema intermodal. A aplicação de recursos humanos permite o processamento de vencimentos, nomeadamente com a afetação das escalas.

Na operação, através do registo de eventos, são geridos os incidentes e as ações de manutenção corretiva. Também são disponibilizados simuladores de condução por tipo de veiculo e simuladores de manutenção.

A aplicação de gestão da manutenção permite planear a manutenção preventiva, a gestão dos recursos de manutenção, gerir as obras de manutenção corretiva, gestão de stocks e a gestão de rotáveis.

A gestão documental e da qualidade permite controlar o ciclo de vida dos documentos e os processos de certificação da qualidade.

A infraestrutura base apresenta os inúmeros servidores para a gestão do domínio, da rede, de partilha de ficheiros, de correio eletrónico, de telefones, de *networking*, de *dns* e muitos outros necessários para as funções base nomeadamente de segurança física e lógica.

Os indicadores qualidade de serviço são o resultado do conjunto de opções tomadas nos diversos domínios. O seu cálculo tem por base os dados dos diversos sistemas e procedimentos de medição disponibilizados na *datawarehouse* e utilizando ferramentas de cálculo BI.

Tyrinopoulos & Aifadopoulou (2008) apresentam uma metodologia para o controlo de qualidade dos serviços prestados aos passageiros do transporte público, que passam pelas características como a segurança, o desempenho, a pontualidade, a acessibilidade e a eficiência. A metodologia proposta tem sete categorias principais: segurança, conforto e limpeza; informação e comunicação com os passageiros; acessibilidade; terminais e desempenho dos pontos de paragem; desempenho das linhas/rotas; elementos gerais do sistema de transporte público, nomeadamente o sistema de tarifário e emissão de bilhetes, horários; e indicadores compostos como resultado dos indicadores das cinco categorias anteriores, para um quadro consolidado do desempenho ou da satisfação / insatisfação.

As perceções de qualidade de serviço e lealdade influência a satisfação do utilizador dos utilizadores do transporte publico. (van Lierop & El-Geneidy, 2016) A Tabela II.21, baseada na tabela 6 de van Lierop & El-Geneidy (2016), apresenta um resumo da eficácia da implementação de estratégias e o impacto nos três grupos que usam o sistema: utilizadores cativos, utilizadores por escolha e utilizadores cativos por escolha.

Tabela II.21 - Resumo da eficácia das estratégias

Estratégias	Cativo	Escolha	Cativo pela escolha
Qualidade de serviço de autocarro	forte impacto	impacto médio	impacto médio
Qualidade de serviço do metro	impacto médio	forte impacto	impacto médio
Confiabilidade	forte impacto	impacto médio	forte impacto
Segurança	forte impacto	impacto médio	impacto médio
Em formação	impacto médio	forte impacto	forte impacto
Limpeza	impacto médio	impacto médio	forte impacto

Adaptada da tabela 6, de van Lierop & El-Geneidy (2016)

Estas estratégias revelam a necessidade de intervir em todas elas dado o seu forte impacto em pelo menos um dos grupos de utilizadores.

4.2.2. Sistema de Informação de Apoio à Exploração

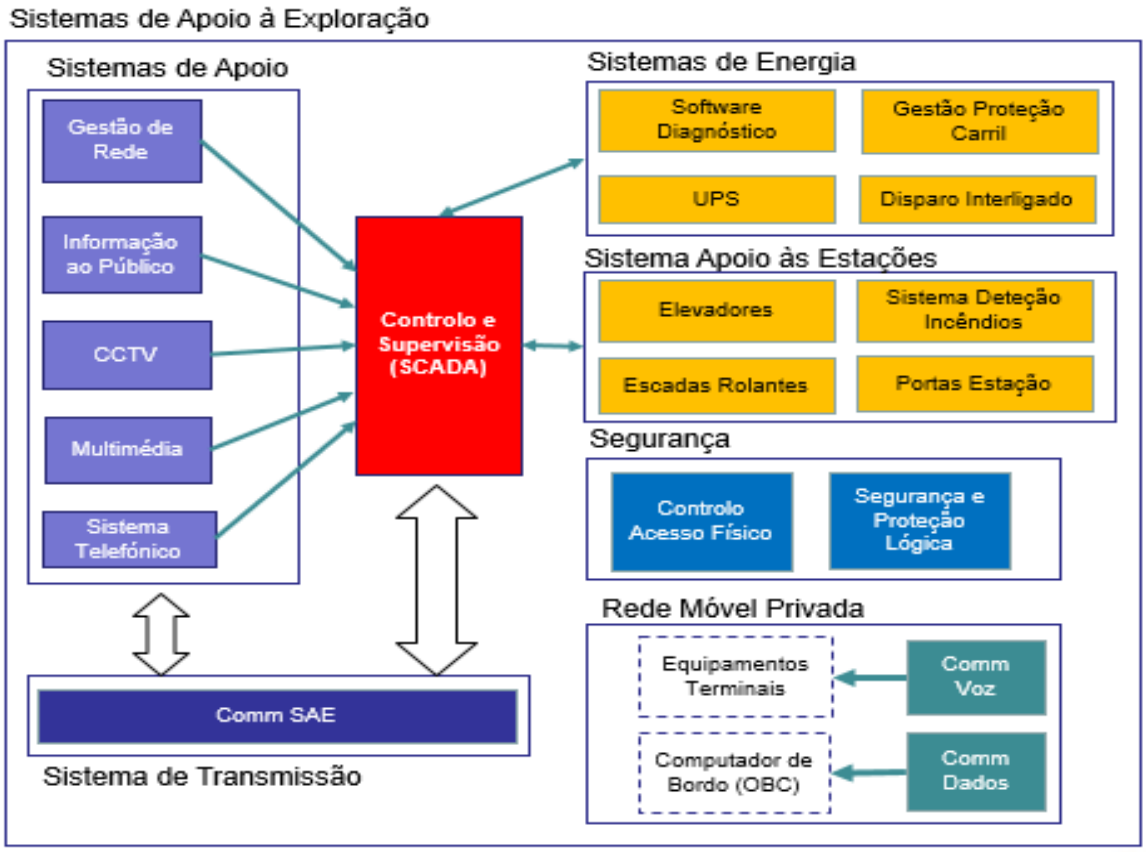
Estes sistemas encontram-se concentrados nas estações, nos parques de viaturas e nos percursos intermédios. As estações têm sistemas com o objetivo de apoiar os passageiros no acesso aos transportes de forma fácil, rápida e confortável.

Estes sistemas suportam um conjunto vastos de funções que passam por: o sistema de gestão da estação que permite gerir os elevadores, as escadas rolantes, o sistema de deteção e supressão de incêndios, a bombagem, a desenfumagem, a abertura e fecho portas, a iluminação, a energia e as comunicações; o sistema de informação ao publico (SIP) que permite orientar os passageiros para os respetivos cais com a informação dos serviços, destinos e tempos de espera e em caso de perturbação ou emergência orientar a sua movimentação nas estações; o sistema de multimédia permite a emissão de canais corporativos com a possibilidade de inserir o SIP; o sistema de videovigilância permite registar e monitorizar as imagens de apoio à exploração e à segurança de pessoas e bens, com o recurso a processamento de imagens e analítica para detetar diversos eventos de segurança; o sistema de gestão de energia permite gerir a rede elétrica de tração, de suporte aos restantes sistemas, de comutação, de redundância e da energia socorrida.

Estes sistemas e os sistemas de gestão de tráfego encontram-se normalmente centralizados num centro de controlo de operações das diversas linhas.

A Figura II.10 apresenta o Sistema de Informação de Apoio à Exploração com as diversas relações e os fluxos de dados que se estabelecem entre as várias aplicações.

Figura II.10 - Sistema de Informação de Apoio à Exploração



O sistema de transmissão integra o conjunto dos sistemas de telecomunicações e módulos de suporte necessários à operação dos serviços disponibilizados sobre redes de telecomunicações, nomeadamente, a aplicação de gestão de rede e suporte aos sistemas de apoio à exploração.

O sistema SCADA (*Supervisory Control and Data Acquisition*), para o controlo de supervisão e aquisição de dados, de uma infraestrutura pública apresenta risco de segurança, com sistemas complexos, interconectados e frequentemente antigos (Temple et al., 2017). Este sistema comporta duas funções principais, a função de controlo e monitorização e a função de supervisão e atuação. Nestas funções encontram-se os sistema de gestão da catenária, da rede de energia (baixa tensão, média tensão e, se aplicável, a de alta tensão), da iluminação, das escadas mecânicas, dos elevadores, da ventilação, da desenfumagem, da bombagem, da deteção e supressão de incêndios, dos sistemas de alimentação socorrida, dos carregadores industriais de baterias, do controlo da temperatura, da velocidade do sistema de ventilação, das medidas (tensão e amperagem), das URT's, das passagens de nível (PN), dos alarmes e eventos e dos diversos serviços auxiliares.

A gestão da energia comporta os sistemas de proteção de média tensão, o *software* de diagnóstico e configuração de relés, o controlo por URTs (Unidade Remota Terminal), os sistemas de proteção, comando e controlo suportado pelo sistema SCADA, a gestão da proteção do carril e o sistema de disparo interligado através de autómatos programáveis para comutação de rede e de redundância.

4.2.3. Sistema de Informação de Apoio à Gestão do Tráfego Ferroviário

A segurança e a precisão destes sistemas relacionam-se com a segurança e a eficiência da operação de trânsito ferroviário e com a segurança da vida dos passageiros. O certificado de segurança do sistema de sinalização de metro tem de ser obtido para se poder realizar a operação de transporte de passageiros, respeitando ensaios, normas, procedimentos, formação e verificações exaustivas da sua conformidade.

Os modelos dinâmicos e algoritmos para a gestão de tráfego ferroviário permitem otimizar os horários ferroviários tornando as operações mais robustas e resistentes a desvios. O plano diário pode ser ajustado tentando manter as operações viáveis e evitar a propagação do atraso. Os problemas de reescalonamento *on-line* de tráfego ferroviário têm aspetos dinâmicos e não deterministas. O escalonamento estático inicial contem a oferta teórica com a probabilidade teórica dos problemas de escalonamento, o reescalonamento dinâmico do tráfego ferroviário permite minimizar a incerteza para os estados futuros (Corman & Meng, 2015).

Os agentes de computação permitem o desenvolvimento de sistemas em larga escala distribuídos num ambiente dinâmico. Os sistemas de gestão de tráfego gerem sistemas de transporte geograficamente distribuídos. As técnicas e os métodos dos sistemas de agentes e multiagentes são aplicados neste domínio na modelação e simulação, no encaminhamento dinâmico, na gestão de congestionamentos, no controlo dinâmico do tráfego, procurando resolver questões críticas como a interoperabilidade, a flexibilidade e a extensibilidade. (Bo Chen & Cheng, 2010)

Mazzarello & Ottaviani (2007) apresentam uma arquitetura para implantação de um sistema avançado de Gestão do Tráfego (*TMS-Traffic Management System*), em tempo real, capaz de otimizar a confluência do tráfego em redes ferroviárias com diferentes sistemas de sinalização procurando resolver o aumento da intensidade de tráfego e a complexidade do sistema ferroviário.

Também Li, Yang, & Gao (2015) procuram soluções para o controlo coordenado da circulação dos comboios com base num modelo multiagentes. O movimento de um conjunto ordenado veículos que funcionam numa linha férrea é modelado por um sistema multiagentes, em que cada veículo comunica com os veículos adjacentes para ajustar a velocidade e pode acompanhar a velocidade desejada, as distâncias entre veículos são estabilizadas dentro duma área de segurança.

A ferrovia é orientada pelos serviços das comunicações móveis, que evolui para uma infraestrutura em que os veículos, os passageiros, as viajantes e mercadorias estão mais interligados e podem fornecer mobilidade mais fina, conforto e maior segurança. A conectividade sem fios e de alta velocidade de dados evolui para serviços com alta taxa de dados, alta definição permitindo novos serviços ao passageiro, de segurança e de vigilância (Ai et al., 2015).

A "inteligência" preditiva para um sistema de gestão de tráfego ferroviário (Roberts et al., 2017) deve prever o aumento de procura dos sistemas de transporte traduzida em maior eficiência e mobilidade mais "inteligente", em meios de transporte autónomos que permitirão a evolução da tecnologia do sistema de transporte "inteligente" (*ITS-Intelligent Transport Systems*) e do ITS cooperativo (*C-ITS- Cooperative Intelligent Transport Systems*[58],). O ITS cooperativo permite mais os benefícios nos serviços e aplicações de ITS, que comunica e partilha informações dos pontos ITS, para melhorar a eficiência, o conforto, a sustentabilidade e a segurança

A Tabela II.22 baseada na figura 1 do resumo da UITP59 sobre as tendências de automação, apresenta os quatro graus de automação. Existem vários graus de automação (GoA-Grades of Automation). Estes são definidos de acordo com as funções básicas da operação de veículos que são da responsabilidade do pessoal e da responsabilidade do próprio sistema. Por exemplo, um Grau de Automação 0 corresponderia à operação no local e à vista. O grau de automação 4 refere-se a um sistema no qual os veículos são executados de forma totalmente automática sem qualquer equipa operacional a bordo.

[58] CITS - https://www.itsstandards.eu/cits, acedido em 10-07-2019
[59] UITP - Metro Automation - https://www.uitp.org/sites/default/files/Metro%20automation%20-%20facts%20and%20figures.pdf, acedido em 09-07-2019.

Tabela II.22 - Graus de Automação

Grau de Automação	Tipo de operação de veículos	Configurando o veiculo em movimento	Paragem do veiculo	Fecho da porta	Operação em caso de interrupção
GoA 1	ATP com Condutor	Condutor	Condutor	Condutor	Condutor
GoA 2	ATP e ATO com Condutor	Automático	Automático	Condutor	Condutor
GoA 3	Sem condutor	Automático	Automático	Apoio ao veiculo	Apoio ao veiculo
GoA 4	UTO	Automático	Automático	Automático	Automático

A proteção automática de veículos (*ATP-Automatic Train Protection*) é o sistema responsável pela segurança básica, ao evitar colisões entre veículos, passagens de sinal vermelho e ultrapassagem dos limites de velocidade.

A operação automática de veículos (*ATO-Automatic Train Operation*) permite a condução automática ou parcial do veiculo e funcionalidades sem condutor, ao executar funções de condução embora não fecha as portas.

O controlo automático de veículos (*ATC-Automatic Train Control*) executa automaticamente as operações normais de sinalização, como a configuração de rotas e a regulamentação de veículos. Os sistemas ATO e ATC trabalham em conjunto para manter um veiculo dentro da tolerância definida no seu cronograma. O sistema combinado ajusta parâmetros operacionais de forma marginal.

A implementação de sistemas de operação de veículos sem supervisão (*UTO-Unattended Train Operation*) permite aos operadores otimizarem o tempo de operação dos veículos, aumentando a velocidade média do sistema.

Esta crescente automatização reflete-se na maior flexibilidade na operação, numa maior segurança operacional, com o aumento na qualidade de serviço e a melhoria das condições de viabilidade financeira.

O programa de Controlo de Veículos de Próxima Geração (*NGTC-Next Generation Train Control*) estuda as semelhanças e diferenças entre o Sistema Europeu de Controlo Ferroviário (*ETCS- European Train Control System*[60]) e o sistemas de controlo de

[60] ERTMS/ETCS - http://www.railwaysignalling.eu/wp-content/uploads/2016/09/ERTMS_ETCS_signalling_system_revF.pdf , acedido em 13-07-2019.

veículos baseado em comunicação CBTC (*Communications-Based Train Control*[61]*)* (Gurník, 2016). O ETCS trata-se de um sistema de controlo de veículos desenvolvido para as principais linhas ferroviárias europeias, enquanto os sistemas CBTC foi desenvolvido separadamente para sistemas de controlo de veículos ferroviários urbanos. O ETCS procura promover a interoperabilidade entre linhas. O sistema de sinalização ERTMS / ETCS (ou apenas ETCS) L2 fornece as informações para uma condução segura, em relação aos efeitos das ações, às alterações das condições da linha e à ativação da travagem de emergência, se a velocidade excede o máximo permitido.

Os sistemas de controlo de veículos baseados em comunicações (CBTC) são plataformas de sinalização de metro, que coordenam e protegem os movimentos de veículos dentro dos carris de uma estação e entre diferentes estações. Nestas plataformas CBTC, a função principal, é executado pelo sistema (*ATS-Automatic Train Supervision*), que automaticamente escolhe e direciona os veículos na rede, e evita situações de impasse (*deadlock*). (Mazzanti & Ferrari, 2018)

O sistema CBTC é um sistema distribuído complexo num ambiente aberto e dinâmico. O principal fator que restringe o desempenho do sistema e o grau de aperfeiçoamento é a sua complexidade. Analisaram principalmente a complexidade do sistema a partir de dois aspetos de implementação de estrutura e de função (T. Chen et al., 2018). A figura seguinte é adaptada da tabela 2 de Chen et al. (2018) que descreve as principais funções do sistema.

Tabela II.23 - Principais funções do CBTC

Tipo de equipamento	**Nome do equipamento**	**Nome da função**
A bordo	ATP de bordo (*On-board*)	Localização do Veiculo / determinação da velocidade do veiculo
		Sobre a proteção da velocidade
	ATO de bordo	Condução de veículos automático
Lado do caminho	Controlador de Zona (*ZC-Zone Controller*)	Gestão de veículos
		Cálculo das Autoridades de Movimento (MA)
	Computador de Interbloqueio (*CI-Computer Inter-locking*)	Interbloqueio da rota
	Sistema de Supervisão Automática de Veiculos (*ATS-Automatic Train Supervision System*)	Supervisão e regulação automáticas de veículos

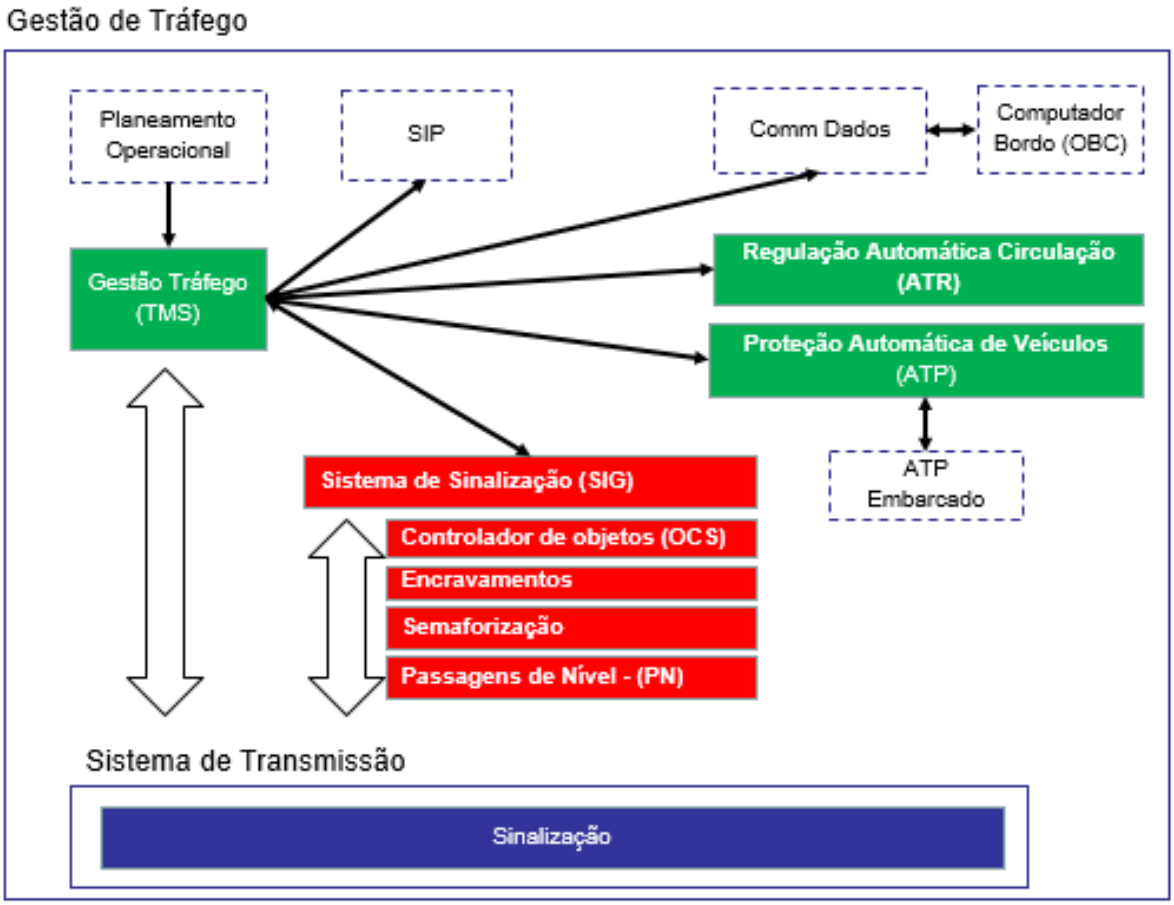
O sistema de transporte urbano ferroviário pode ser descrito como um espaço métrico em que os espaços topológicos são introduzidos para formar a autoridade de movimento e a

[61] IEEE. (2004). IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements. https://ieeexplore.ieee.org/document/1405808

trajetória (ocupação da via). As regras de segurança são verificadas executando uma série de cálculos de verificação tendo por base a topologia. (Haifeng Wang et al., 2018)

A Figura II.11 apresenta um esquema de um sistema de tráfego tradicional, envolvendo o ATP e o ATR como sistemas de proteção e regulação.

Figura II.11 - Sistema de Informação de Apoio à Gestão de Tráfego genérico



O sistema de sinalização (*SIG - Signalling System*) é composto genericamente por: o sistema de encravamento vital baseado em computador e na unidade de processamento do encravamento (*IPU - Interlocking Processing Unit*); o sistema de controlador de objetos (*OCS - Object Controller System*); a semaforização, no caso dos sistemas que interagem com a circulação automóvel e os peões; o sistema de gestão de tráfego (*TMS-Traffic Management System*); a regulação automática de circulação *(ATR - Automatic Train Regulation*); e o computador de bordo (*OBC - On-Board Computer*). Além de outros dos sistemas de proteção adotados (ATP, ATO ou UTO).

Os sistemas de sinalização utilizam as balizas na via tratando-se de um dispositivo passivo que é energizado quando um veiculo passa e que comunica com o módulo de transmissão da baliza (*BTM - Balise Transmission Module*) ligado ao veiculo através de mensagens

de telegrama. Este equipamento é crítico e a sua interface que pode ser explorada para alterar ou manipular informações sobre telegramas. Os mecanismos de segurança e integridade devem ser reforçados com a proteção de segurança para as mensagens de telegrama com abordagens de AES-CCM (*AES-Advanced Encryption Standard, CCM - Cipher Block Chaining-Message Authentication Code*) (Dworkin, 2007) e HMAC (*Hash Message Authentication Code*) que adicionam a proteção e a verificação de integridade de dados para mensagens de telegramas recebidas pelo BTM a partir de balizas. (Guo et al., 2018)

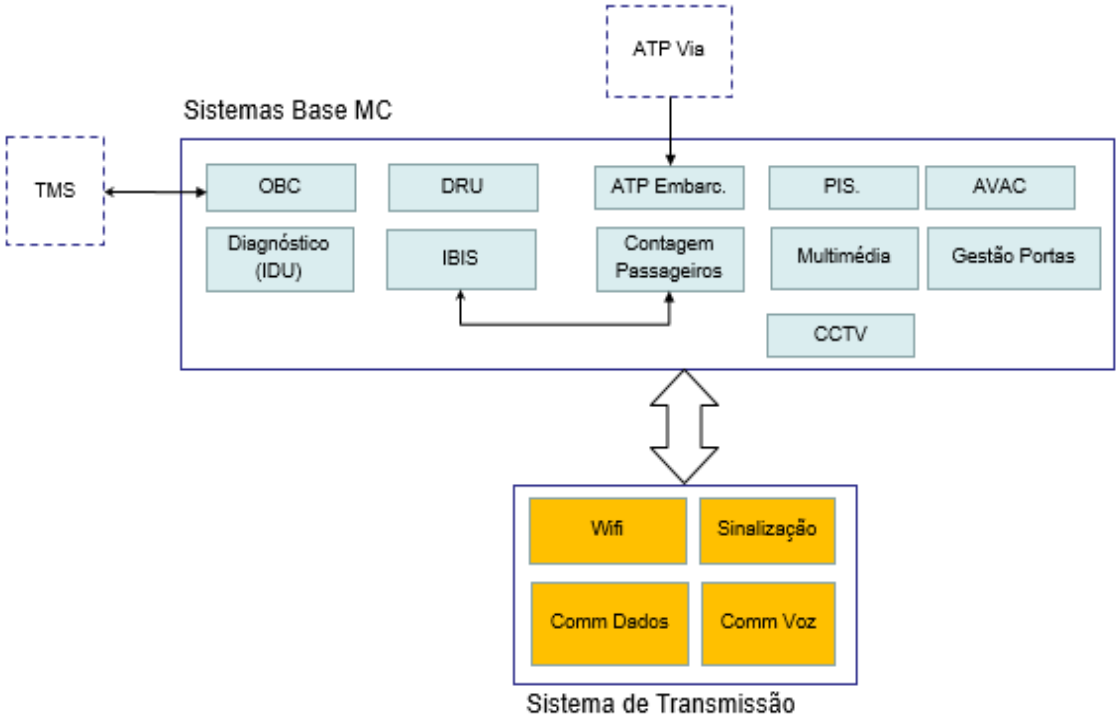
O modelo de integração de gestão de segurança e do sistema de sinalização, adequada para o controlo da comunicação base com o veiculo (*CBTC-Communication-Based Train Control)*, de acordo com as normas CENELEC [62], pretende garantir a segurança e a avaliação baseada na verificação de segurança e no processo de validação. O método foi aplicado em todas as fases do ciclo de vida de desenvolvimento do sistema CBTC, para monitorizar e controlar cada atividade no ciclo de vida e a avaliar cada documento no processo de desenvolvimento do sistema e assegurar a rastreabilidade dos documentos relevantes e testar todas as funções do sistema (Yan et al., 2017).

4.2.4. Sistema de Informação de Apoio ao Material Circulante

Os sistemas de suporte ao material circulante permitem gerir, controlar e operar os diversos subsistemas instalados nos veículos e que se relacionam com o seu movimento. As funcionalidades passam pela gestão e controlo do veículo, as comunicações de dados e voz, a gestão da energia de tração, da iluminação, do AVAC, das portas, a informação aos passageiros (SIP), o sistema de videovigilância, a contagem de passageiros, os sistemas de multimédia, os sistemas de proteção e segurança, de entre outros sistemas. A figura seguinte descreve os principias subsistemas de controlo e comando do veiculo.

[62] IEC 62278-2002 Aplicações ferroviárias - especificação e demonstração de confiabilidade, disponibilidade, facilidade de manutenção e segurança (RAMS)
IEC 62279-2002 Aplicações ferroviárias - sistemas de comunicação, sinalização e processamento - software para sistemas de controlo e proteção ferroviária
IEC62425-2007 Aplicações ferroviárias - sistemas de comunicação, sinalização e processamento - sistemas eletrónicos relacionados à segurança para sinalização

Figura II.12 - Sistema de Informação de Apoio ao Material Circulante (MC)



Os sistemas de informação de apoio ao material circulante são genericamente compostos por: o computador a bordo (*OBC - On Board Computer*); o sistema de informação embarcado (*IBIS - Integrated On-board Information System*); a unidade de gravação de eventos (*DRU - Data Recording Unit*); o sistema de ar condicionado AVAC; o sistema de multimédia; o sistema de comunicações de voz; o sistema de comunicação de dados que permite a ligação ao TMS; o sistema de informação ao passageiro (*PIS - Passenger Information System*); o computador central (*VTCU - Vehicle Train Control Unit*); a unidade de controlo de tração; barramento principal do veículo; e o monitor de diagnóstico.

4.3. Sistema de Bilhética

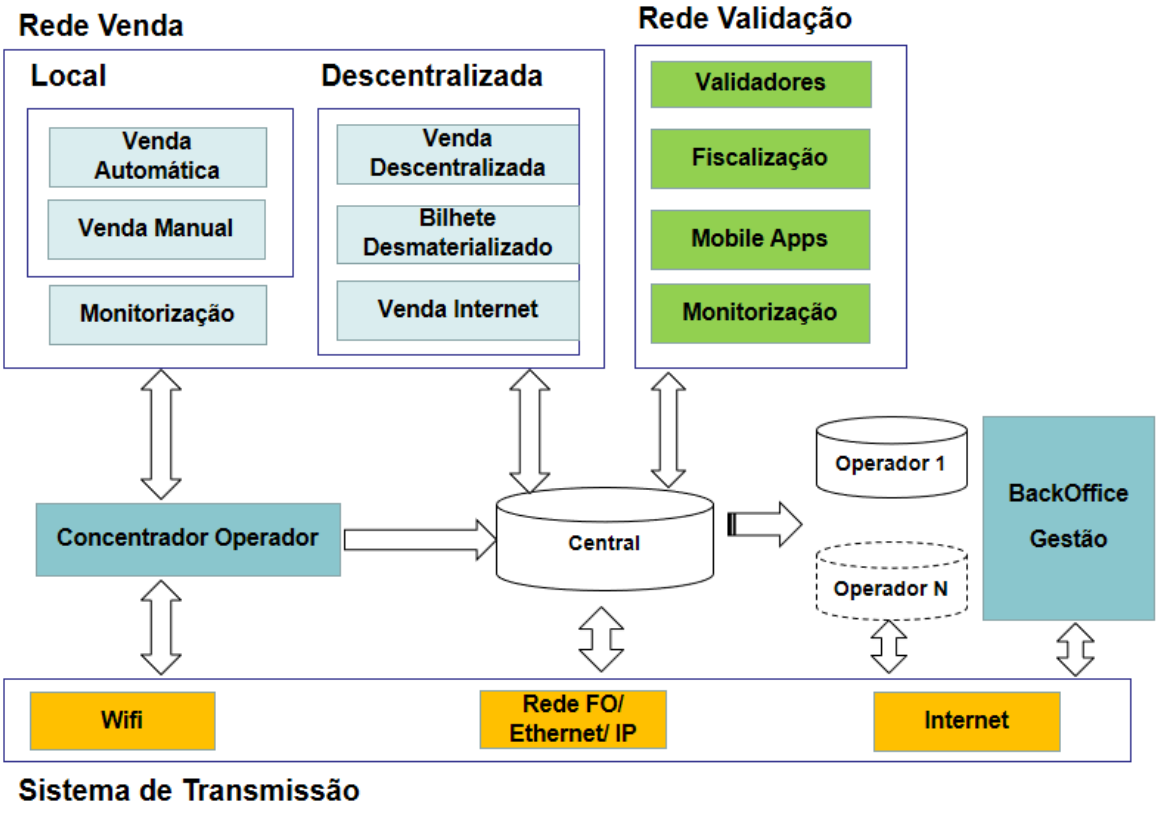
Este sistema é tratado com maior detalhe dado que será sobre ele que os trabalhos de prova de conceito, no âmbito da tese, serão realizados e que se pretende que possa validar o modelo proposto nas componentes de alarmística e controlo do fluxo de dados.

O sistema de bilhética genericamente é composto por uma rede de venda (local e descentralizada), uma rede de validação e uma base central que centraliza todos os dados de venda, validação e monitorização, e que os replica para cada um dos operadores. De forma mais detalhada teremos os seguintes módulos ou blocos funcionais:

- Os equipamentos de bilhética que podem incluir os equipamentos de venda e carregamento automática, de validação, equipamentos de fiscalização ou venda e equipamentos controladores locais e controladores de operador. Também existem formas descentralizadas de venda, de validação e de bilhetes eletrónicos.
- A aplicação de *backoffice* permite a gestão de todas as funções de bilhética e cada um dos operadores dos seus dados de bilhética monomodal. As principais funções passam pela gestão comercial de venda e carregamento, controlo da receita, incorporação na contabilidade, cálculo da matriz origem/destino, registo de validações, dados de fiscalização e dados de sensores e alarmes.

A figura seguinte sintetiza a arquitetura geral do sistema de bilhética.

Figura II.13 - Arquitetura Geral do Sistema Bilhética



A arquitetura base apresentada na figura anterior permite vários fluxos de dados para registo transacional embora consolidada numa base de dados central. As novas soluções de desmaterialização também estão presentes e funcionam de forma descentralizada,

Ferreira, Nóvoa, Dias, & Cunha (2014) propõem uma solução de *e-ticketing* no transporte público com a utilização de dispositivos móveis para minimizar o custo de investimento das operadores de transporte publico e maximizar a aceitação pelo cliente.

No mesmo sentido, Mallat, Rossi, Tuunainen, & Öörni (2007) realizaram uma pesquisa para a adoção do serviço móvel *e-ticketing* no transporte público, que sugere a compatibilidade do serviço de mobile *ticketing* com o comportamento do cliente, a mobilidade e fatores contextuais, incluindo as restrições de orçamento, a disponibilidade de outras alternativas, e a pressão do tempo na situação de uso de serviço, que são o que determinam a sua adoção e que podem ser integrados nos modelos de adoção tradicionais.

A aceitação do cliente e os exemplos de adoção da tecnologia de mobilidade (Bongaerts et al., 2017) parte de novos desafios com: os custos crescentes de energia; a internet das coisas (*IoT*); a tecnologia *blockchain*; a mudança nos canais de comunicação; e a maior competição. Os desafios no negócio de mobilidade passam para o nível: do cliente / consumidor / utilizador devido às tendências demográficas, urbanização, partilha de carros, vivências num mundo digital, simplicidade / conveniência, soluções em tempo real e omnipresentes; do fornecedor devido aos custos crescentes de energia, a internet das coisas / *big data*, o ajuste para dispositivos móveis, a transparência e a nova competição fora do setor; e da governação devido ao aumento do custo da infraestrutura, do aquecimento global, dos cuidados de saúde e da segurança. O desenvolvimento da tecnologia *blockchain* pode resultar como um novo impulso para uma mobilidade mais conectada, sem os intermediários e com os contratos "inteligentes" entre o utilizador e o fornecedor.

A gestão de ciclo de vida do bilhete devia permitir combinar vários fornecedores de bens e serviços. A dificuldade está numa arquitetura ou numa solução tecnológica unificada para a gestão de comércio eletrónico como resultado da transação com serviços complementares conjugados com a gestão do bilhete eletrónico que se relacionam com diferentes sistemas, aplicações e interfaces do sector dos transportes e de outros serviços que se possam relacionar (Bumanis et al., 2017).

Nair, Pawar, Tidke, Pagar, & Wani (2018) propõem soluções baseadas em dispositivos móveis com os dados de localização dos transportes, *e-ticketing online*, geração de ticket por pagamento em dinheiro e validação por código QR (*Quick Response*).

Também Sheikh, Khapekar, Kumar, & Kumar (2018) apresentam uma revisão das técnicas do sistema de *e-ticketing* para a implementação do bilhete eletrónico. Esta revisão conclui que embora se use as tecnologias RFID, GPS, WIFI e o código AZTEC,

é o código QR bidimensional (comparação dos códigos [63]) de rápida resposta que se tem destacado por ser fácil de usar e versátil para o sistema de bilhete eletrónico eficiente.

Kazi, Bagasrawala, Shaikh, & Sayyed (2018) apresentam um sistema *e-ticketing* "inteligente" para o transporte público que pretende responder às necessidades como o tempo de espera indevida nas paragens, o reembolso por incumprimentos e a falta de lugares para os passageiros. O objetivo passa por uma bilhética ágil e suave que permite a afetação automática do lugar do passageiro com a reserva do bilhete digital, com o pagamento sem recurso a dinheiro, em que o utilizador verifica a disponibilidade de lugares, reserva bilhetes, obtém o lugar automaticamente através de algoritmo eficiente e de acordo com o tempo de espera esperado.

Nos sistemas de bilhética estão presentes aspetos fundamentais diretos, como a disponibilidade do serviço de bilhética e a formação do preço e indiretos, como a qualidade da prestação do serviço de transporte, a pontualidade e a regularidade, o cumprimento da oferta, a manutenção dos equipamentos e das infraestruturas, a limpeza, a informação ao publico e a comunicação com o cliente.

Neste trabalho será focado principalmente na disponibilidade do serviço, resultado da alarmística do sistema e consequentemente do cumprimento da manutenção atempada.

[63] 2D Barcode - https://www.tec-it.com/en/support/knowbase/barcode-overview/2d-barcodes/Default.aspx , acedido em 13-07-2019

III. ESTUDO EMPÍRICO

III. ESTUDO EMPÍRICO

1. Metodologia

Neste ponto procura-se obter a informação para escolher a metodologia científica mais adequada para desenvolver o trabalho proposto.

Na tabela seguinte sintetiza-se de forma cronológica as contribuições consideradas mais relevantes para o desenvolvimento da metodologia da DSR (*Design Science Research*) no domínio das SI/TICs.

Tabela III.1 - Contribuições para a metodologia DSR

Ano	Contribuição	Referências
1992	Define uma teoria do design de sistemas de informação (*ISDT-Information Systems Design Theory*) para produzir sistemas de informação mais eficazes.	(Walls, Widmeyer, & El Sawy, 1992)
2002	Define a DS (*Design Science*) em TICs com a intervenção no mundo representacional definido pela hierarquia de preocupações seguindo a semiótica. A natureza complementar dos ambientes representacional (interno) e real (externo) fornece a base para articular as bases ontológicas e epistemológicas.	(Purao, 2002)
2004	A pesquisa predominante tende a ser orientada por descrições, baseada no paradigma das "ciências explicativas", resultando na Teoria da Organização. A relevância pode ser mitigada com as pesquisas baseadas em prescrições, no paradigma das "ciências do design" e na Teoria da Gestão, em que os produtos da pesquisa seriam "regras tecnológicas testadas em campo e fundamentadas". A natureza dessas regras é discutida, assim como as estratégias de pesquisa que as produzem.	(Aken, 2004)
2006	A DS é definida e comparado com outros paradigmas de pesquisa e apresenta sete diretrizes para entender, executar e avaliar a pesquisa de *design*.	(Manson, 2006)
2006	Desenvolve um quadro de atividades para a interação da *Design Science* com pesquisas noutros paradigmas científicos.	(Venable, 2006)
2007	Define três ciclos de atividades relacionados: o ciclo de relevância, o ciclo do rigor e o ciclo de desenho central, recuperando a natureza pragmática da DS.	(Hevner, 2007).
2007	A pesquisa em DS deve atende a três objetivos: ser consistente com a literatura anterior, fornecer um modelo de processo nominal para a realização de pesquisa em DS e fornecer um modelo mental para a apresentação e avaliação da pesquisa em DS no SI. O processo da DS tem seis etapas: identificação e motivação do problema, definição dos objetivos para uma solução, projeto e desenvolvimento, demonstração, avaliação e comunicação.	(Peffers et al., 2007)
2009	A *Soft Design Science* (SDS) procura novas formas de melhorar as organizações humanas, nos aspetos sociais, com atividades de *design*, desenvolvimento, instanciação, avaliação e evolução de um artefacto tecnológico. A abordagem SDS combina o processo comum de pesquisa DS (design, construção-artefacto, avaliação) com a metodologia iterativa de *Soft Systems*, num método de pesquisa-ação orientada ao *design*.	(Baskerville et al., 2009)
2011	Apresentam um *roadmap* do DS para planear, executar e comunicar a pesquisa em DS, com outras críticas construtivas, melhorias e	(Alturki et al., 2011)

Ano	Contribuição	Referências
	extensões, e com uma ampla cobertura dos aspetos e atividades de pesquisa em DS.	
2012	Discutem a semântica da teoria do *design* a partir de uma visão epistemológica do *framework*, relacionando-o a um ciclo idealizado de pesquisa científica e procuram demonstrar o potencial da estrutura da DSRIS (*Design Science Research in Information Systems*)	(Kuechler & Vaishnavi, 2012).
2013	A DSR (*Design Science Research*) tem duas dimensões: o estado de conhecimento existente nos domínios do problema e a solução para a oportunidade de pesquisa em estudo. O esquema de comunicação DSR tem semelhanças com os padrões de publicação convencionais em que substitui a descrição do artefacto DSR na seção tradicional de resultados.	(Gregor & Hevner, 2013)
2015	Descreve uma metodologia para a realização da DSR, através de uma orientação abrangente para conduzir as pesquisas e aprofunda a teoria de DS (*Design Science*) e diferentes tipos de teoria.	(Vaishnavi et al., 2015)
2017	Comparam seis metodologias de DSR através de um *framework* de comparação das metodologias de desenvolvimento de sistemas de informação existente, para apoiar os investigadores de DS na escolha da metodologia DSR adequada e melhor-adaptada. As seis metodologias são: SDRM (*Systems Development Research Methodology*); DSRPM (*DSR Process Model*); DSRM (*Design Science Research Methodology*); ADR (*Action Design Research*); SDSM(*Soft Design Science Methodology*); e PADR (Participatory Action Design Research).	(Venable et al., 2017)

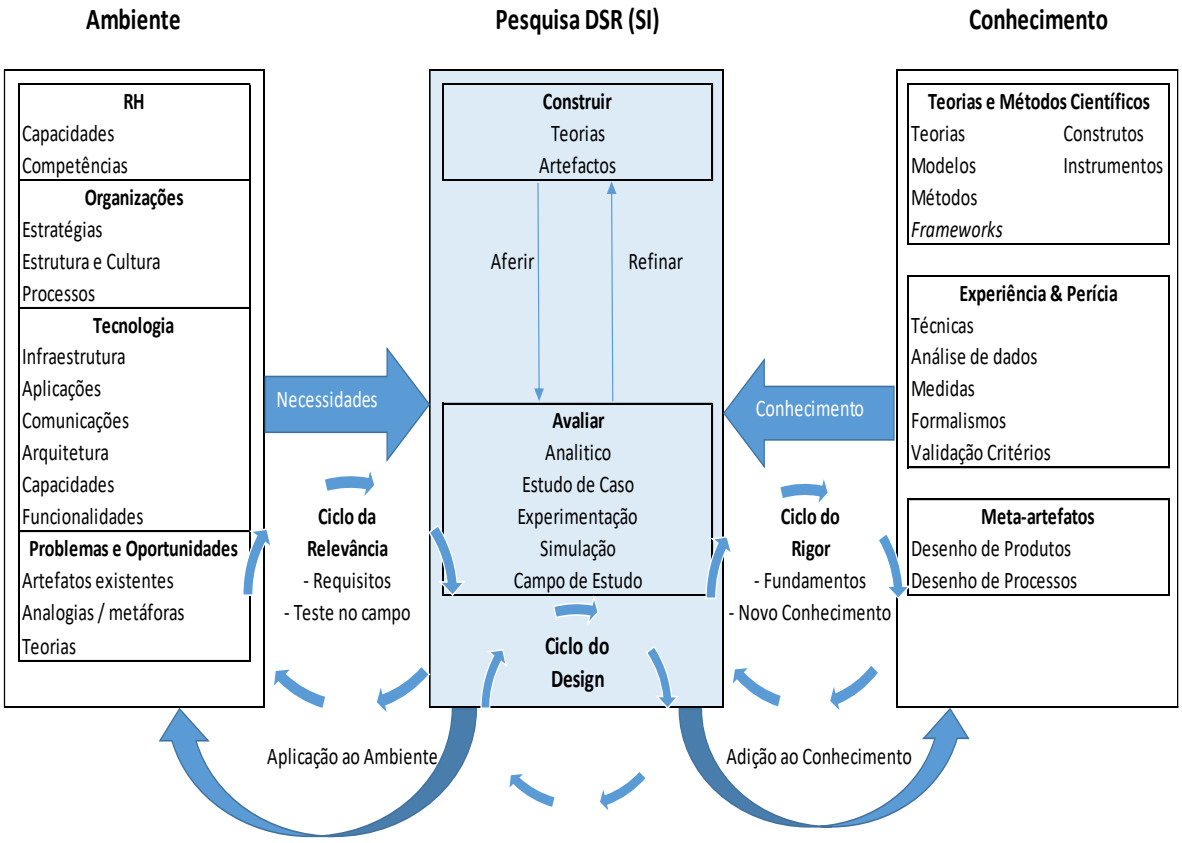
A partir do resumo das diversas contribuições consideradas, detalha-se a seguir as que serão analisadas, no sentido de poderem vir a ser a metodologia mais adequada para dar resposta aos objetivos deste trabalho.

A Teoria de Design de Sistemas de Informação (ISDT) deve ser uma teoria prescritiva integrando teorias normativas e descritivas com caminhos de *design* para produzir sistemas de informação mais eficazes (Walls et al., 1992). Esta teoria apresenta as sete características que diferenciam as teorias de *design*: devem lidar com objetivos como contingências; nunca pode envolver explicações ou previsões puras; são prescritivas; são teorias compostas que abrangem teorias da ciência natural, ciências sociais e matemática; as teorias explicativas dizem "o que é", as teorias preditivas dizem "o que será", e as teorias normativas dizem "o que deveria ser" enquanto as teorias de *design* dizem "como ou porque"; mostram como as teorias explicativas, preditivas ou normativas podem ser usadas de maneira prática; e são teorias da racionalidade processual.

A visão dos três ciclos da pesquisa em DS apresentada por Hevner (2007) está relacionada com as atividades de projeto. O ciclo de relevância tem como entradas os requisitos para a pesquisa e apresenta os artefactos da investigação em testes. O ciclo de rigor apresenta as teorias e os métodos conjuntamente com a experiência no domínio, a base do conhecimento para a pesquisa e com o novo conhecimento resultante. O ciclo de desenho suporta a atividade de investigação para a construção e avaliação de artefactos e processos

de *design*. A figura seguinte, adaptada da figura 1 de Hevner (2007), apresenta os ciclos de DSR, com maior detalhe e procurando estabelecer as dinâmicas que decorrem das possíveis interações para além dos próprios ciclos.

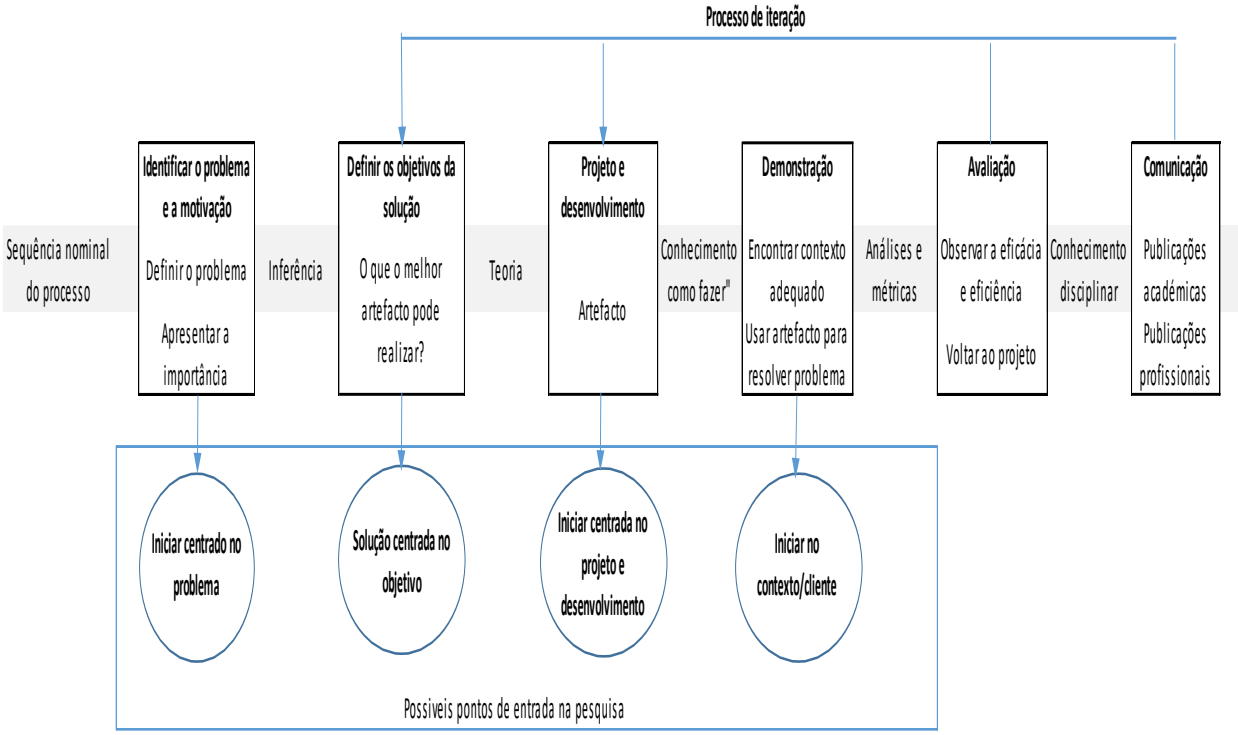
Figura III.1 - Ciclos de DSR



Adaptada da figura 1, de Hevner (2007)

Peffers, Tuunanen, Rothenberger, & Chatterjee (2007) demonstram uma metodologia para a realização de projeto de pesquisa científica (*DS-Design Science*) aplicada aos sistemas de informação. A metodologia de pesquisa (*DSRM-Design Science Research Methodology*) inclui princípios, práticas e procedimentos para realizar a investigação. Esta metodologia tem três objetivos: consistente com a literatura anterior; um modelo de processo nominal da pesquisa DS; e um modelo mental para a apresentação e avaliação da pesquisa DS. O processo é definido em seis etapas: a identificação do problema e motivação, a definição dos objetivos, o projeto e desenvolvimento, a demonstração, a avaliação e a comunicação. A figura seguinte, adaptada da figura 1 de Peffers et al. (2007), apresenta as etapas referidas e as relações estabelecidas para o processo DSRM e o processo iterativo proposto.

Figura III.2 - Modelo de Processo DSRM



Adaptada da figura 1, de Peffers et al. (2007)

A escolha da metodologia mais adequada para o DSR (*Design Science Research*) é um desafio importante e critico para os investigadores. Esta escolha pode suportar ou condicionar um trabalho de investigação e a sua sustentação cientifica.

O trabalho de Venable, Pries-Heje, & Baskerville (2017) apresenta um *framework* para comparar as seis metodologias DSR a partir da adaptação do *framework* (Avison & Fitzgerald, 2006, pp. 597-603) para comparar as metodologias de ISD (*Information Systems Development*), de acordo com a tabela seguinte, adaptada da tabela 8 de Venable, Pries-Heje, & Baskerville (2017).

Tabela III.2 - *Framework* para comparar metodologias DSR

Elemento ou subelemento do *framework*	**Descrição**
1. Filosofia	
a. Paradigma	Sistemas vs. Ciência, Objetivista vs. Ontologia Subjetivista, Positivista vs. Epistemologia Interpretativa
b. Objetivos	Possíveis metas / objetivos para metodologias de DSR incluem: aumentar a relevância; aumentar o rigor da pesquisa; melhorar (para quem - cliente? *stakeholders*? público?; de que forma? eficácia? eficácia, eficiência, ética); emancipação / perspetiva crítica; consenso das partes interessadas; resolver o problema "certo"; eficácia dos artefactos; relação com a literatura existente; significância prática; ou significância teórica.
c. Domínio	Nenhum cliente específico, Único cliente, múltiplo / grupo de clientes, cliente social
d. Alvo	Tipo de artefacto: SI / TI, CBIS (*Compute-based information systems*), método / ferramenta / técnica / metodologia ISD, produto (geralmente, não apenas em SI / TI), processo (geralmente, não apenas em SI / TI)

Elemento ou subelemento do *framework*	Descrição
2. Modelo	Qual é o mecanismo básico de abstração e representação usado? (1) verbal, (2) analítico ou matemático, (3) icónico, pictórico ou esquemático, e (4) simulação
3. Técnicas e Ferramentas	Quais ferramentas e técnicas são usadas na metodologia?
4. Objetivo (atividades de DSR)	Quais etapas / atividades do processo de DSR são cobertas? As atividades encontradas em comum entre as metodologias de DSR incluem: (a) Avaliação de problemas, (b) Projeto / enquadramento, (c) Projeto / construção, (d) Avaliação e (e) Reflexão.
5. Saídas	Quais são as entregas em cada etapa e no final? (O mesmo que para o ISD)
6. Prática	
a. Fundo	Comercial ou Académico?
b. Base de utilizadores	Números e tipos de utilizadores da metodologia DSR (usar citações como substitutos)
c. Participantes	Quais papéis participam e quais competências são necessárias? Pesquisador, Cliente, Utilizador, Outras partes interessadas
7. Produto	O que os compradores de metodologia obtêm por seu dinheiro? Programas? Treinamento? Documentação? Serviço de ajuda? Consultoria? Etc. (O mesmo que para o ISD)

Adaptado da tabela 8, de Venable, Pries-Heje, & Baskerville (2017)

Enquadrado com o nosso trabalho e em detalhe podemos responder que: os paradigmas (1a) são baseados na ciência, objetivista e positivista; tem como objetivos (1b) um novo artefacto ou melhoria de existentes e no domínio (1c) não especifico do cliente; tem como alvo (1d) o CBIS, a TI ou modelos; no âmbito das atividades de DSR (4), identifica-se o problema, define-se os objetivos da solução, pretende-se o *design* e desenvolvimento duma solução, pretende-se validar e adaptar para uso generalizado, na reflexão pretende-se realizar a comunicação com a comunidade científica; tem como saídas um artefacto; tem como prática o acesso à academia e como participantes os investigadores e os utilizadores (avaliadores), e o produto serão principalmente artigos científicos.

Estas respostas ás questões levantadas na Tabela III.2 e aplicando as respostas de acordo com a tabela 9 (Venable, Pries-Heje, & Baskerville, 2017, p. 7), verifica-se que a metodologia DSRM é a mais adequada aos objetivos deste trabalho.

No mesmo sentido e usando as comparações entre os diferentes paradigmas de pesquisa (Vaishnavi et al., 2015) verifica-se que este trabalho tem como orientação básica o *design* (baseada em projeto); a ontologia de múltiplas alternativas de estados do mundo contextualmente situadas, e possibilitadas social e tecnicamente; a axiologia baseia-se no controlo, na criação, no progresso de melhoria e aperfeiçoamento, e na compreensão, a epistemologia baseada no conhecimento pelo fazer, em que a construção é objetivamente restrita dentro de um contexto e a circunscrição iterativa descobre significados, em abordagens ou métodos de pesquisa DSR.

A teoria de projeto de sistemas de informação (ISDT) é definida como uma teoria prescritiva que integra teorias normativas e descritivas em caminhos de projeto destinados a produzir sistemas de informação mais eficazes (Walls et al., 1992). O DSRM sugere que se deve observar e medir o quanto um artefacto apoia uma solução para o problema (Peffers et al., 2007).

Um modelo conceptual (J. Johnson & Henderson, 2002) pretende ser a descrição de alto nível da forma como um sistema se organiza e se opera. O modelo deve especificar e descrever: as principais metáforas e analogias utilizadas no *design*; os conceitos do sistema dirigidos aos utilizadores, onde se inclui os objetos de dados, de domínio, de atividades que os utilizadores criam e manipulam, os atributos e as operações que podem ser executadas; as relações entre esses conceitos; e os mapeamentos dos conceitos e o domínio das atividades que o sistema foi projetado para suportar.

Os problemas reais devem ser conceptualizados e representados de forma adequada, através de técnicas apropriadas em que a solução deve ser construída, implementadas e avaliada usando critérios apropriados. (March & Smith, 1995)

No caso do modelo conceptual para um sistema interativo dever existir: uma visão idealizada de como o sistema funciona; a estrutura ontológica do sistema, com os objetos, as relações e as estruturas de controlo; e o mecanismo pelo qual os utilizadores realizam as atividades que o sistema deve suportar. (J. Johnson & Henderson, 2002)

Em resumo considera-se apropriada a pesquisa científica em design (DSR), numa abordagem centrada no problema, para a prova de conceito que valide o modelo genérico de dados proposto, suportado em *blockchain*. A metodologia DSR seguida baseia-se nas seis etapas previstas no processo DSRM de Peffers, Tuunanen, Rothenberger, & Chatterjee (2007), com o uso de metodologias de pesquisa baseadas em modelos conceituais (J. Johnson & Henderson, 2002; March & Smith, 1995) e o desenho do projeto de prototipagem (Walls et al., 1992).

1.1. Método

O método que suporta este trabalho cientifico é o DSRM, de acordo com o modelo de Peffers, Tuunanen, Rothenberger, & Chatterjee (2007), reforçado pela abordagem prevista estar centrada no problema e na dinâmica iterativa do modelo, que fortalece a forma como se pode melhorar e validar o modelo que se propõe no âmbito deste trabalho.

O modelo genérico de dados proposto pretende conceptualizar o funcionamento de um *smart place*, especificamente duma *smart city* e que se procura validar através de artefactos que concretizam provas de conceito.

A etapas seguem as 6 etapas descritas na Figura III.2 - Modelo de Processo DSRM, com o processo iterativo proposto numa abordagem Centrada no Problema. (Peffers et al., 2007)

1.2. Etapas

Neste ponto as etapas referidas na metodologia são descritas de forma sucinta a seguir.

Primeira Etapa - Identificação do problema e motivação

A gestão de dados e a governação da crescente quantidade de dados gerados por uma multiplicidade de dispositivos é um desafio tecnológico e de gestão, particularmente à medida que os dados e a informação resultante se desenvolvem como recursos estratégicos e de decisão, com características que os tornam diferentes de governar, os artefactos típicos das TIC. O controlo dos fluxos dos dados, a gestão do ciclo de vida dos dados e da informação tornou-se num ponto crítico no processo de gestão de dados e de gestão da informação e da sua governança.

Segunda Etapa - Objetivo da solução

O objetivo passa por desenvolver um modelo de dados genérico, de suporte ao conceito de *smart places*, particularmente de *smart cities*, por forma a sistematizar as suas ações sobre os dados, o controlo dos fluxos de dados e da qualidade dos dados, que permitam gerir os dados e a informação, de forma confiável e segura.

O projeto pretende testar o modelo através do desenvolvimento de um artefacto aplicacional, de conceção distribuída e adaptável para responder às questões de controlo dos fluxos de dados, da gestão dos dados e da informação e da sua governança, propondo a utilização da tecnologia *blockchain* para garantir a eficácia do modelo.

3ª Etapa - Design e desenvolvimento

O artefacto pretende testar e concretizar o seguinte:

1. Estruturar um modelo de dados genérico de suporte ao conceito de *smart place* que conduza e permita o alinhamento da aplicação dos ecossistemas de dados com os ecossistemas naturais.

2. Estruturar as relações entre os ecossistemas, os participantes e os dados que facilite a utilização da tecnologia *blockchain* na gestão dos dados, na segurança e na privacidade.

3. Assegurar mecanismos de privacidade e confiabilidade na gestão dos dados.

As provas de conceito centram-se na segurança dos dados e no controlo do fluxo de dados, no ecossistema de mobilidade, no domínio aplicacional dos transportes públicos ferroviários, no sistema de bilhética e no seu modelo de dados associado aos eventos de alarmística que condicionam as disponibilidades dos sistemas e equipamentos e o correto cálculo dos níveis de serviço contratados de suporte e manutenção, com elevado impacto no utilizador e na compra do seu bilhete.

Nesta perspetiva e tendo em consideração a análise extensiva dos diversos sistemas e a possibilidade de se obter dados reais e se conseguir demonstrar e validar o modelo com base nos artefactos de demonstração, pretendem-se controlar o fluxo de dados dos *logs* deste sistema de alarmística, garantindo a confiança da produção dos *logs* e do envio entre entidades distintas pela internet, com a utilização da tecnologia *blockchain* para a autenticidade dos *logs* e o controlo do acesso aos *logs* às entidades, utilizadores e aplicações envolvidas neste fluxo de dados.

Num processo de iteração e melhoria pretende-se numa segunda iteração resolver o problema de garantir a autenticidade no momento do registo do evento e a forma como estes registos possam ficar disponíveis nos nós aceites desta rede privada de entidades distintas.

Outras iterações seriam necessárias para atingir todo o fluxo de dados deste os dispositivos *IoT* e a sua disponibilização nos quadros de controlo da *smart city*, percorrendo todos os cinco níveis previstos no modelo de dados genérico da *smart city*, no ponto II.2.1.

4ª Etapa - Demonstração

Após o desenvolvimento pretende-se a demonstração na componente de monitorização e alarmística do sistema de bilhética, para verificar se os artefactos previstos de prova de conceito podem garantir a segurança dos dados e o controlo do fluxo de dados.

No processo iterativo previsto na metodologia o artefacto poderá ser extensivamente adaptado para melhorar a forma como podemos garantir às Organizações participantes a

confiança no bom funcionamento do sistema e principalmente minimizar o impacto nos utilizadores finais do sistema, o utente, o cidadão.

5ª Etapa - Avaliação

A avaliação decorre da demonstração e da verificação que os *logs* obtidos e transmitidos se revelam imunes à adulteração ou manipulação e se garante a entrega exclusivamente aos destinatários autorizados.

Este processo prevê a comparação entre os sistemas desenhados sem esta preocupação de segurança e estes que decorrem de uma conceção suportados em *security by design* através da implementação destes mecanismos baseados na tecnologia *blockchain*.

Nesta fase, com base na avaliação realizada equaciona-se uma segunda iteração para a etapas 3ª e 4ª deste método, reforçando os processos de autenticidade e principalmente de integridade dos dados e dos respetivos registos.

6ª Etapa - Comunicação

O processo de comunicação baseia-se na escrita de manuscritos sobre três aspetos essenciais para a elaboração deste trabalho consubstanciado nesta tese, a revisão sistemática da literatura, o modelo genérico de dados confiável de uma *smart city* e os mercados de dados. Para o efeito e no decurso do trabalho de pesquisa e investigação elaboramos três manuscritos que foram apresentados nas conferências da *World Conference on Information Systems and Technologies* (WordCIST) de 2018 e 2019 e da *International Conference on Software Process Improvement* (CIMPS) de 2018, respetivamente com os títulos "Revisão Sistemática da Literatura, Pesquisa em Tecnologia *blockchain* como Suporte ao Modelo de Confiança Proposto Aplicado a *smart places*", publicado em 28 de março de 2018, "Um modelo de *smart city* seguro por *blockchain*", publicado em 27 de setembro de 2018 e "Mercado de Dados (*Marketplace*) confiáveis", publicado em 27 de março de 2019 (Brandão et al., 2018b, 2018a, 2019). Estes manuscritos submetidos encontram-se referenciados no ponto de Publicações no final da tese. Também se elaborou um manuscrito inicial sobre a aplicação da tecnologia *blockchain* na saúde, especificamente nos registos clínicos e que se encontra ainda em revisão e em trabalho de investigação e aprofundamento baseado no modelo adaptado ao apresentado nesta tese.

A contribuição deste trabalho de investigação revela-se no modelo genérico de dados suportado em tecnologia *blockchain* aplicado a uma *smart city*. As provas de conceito

desenvolvidas orientam-se para validar o modelo e potenciar a utilização da tecnologia *blockchain* em ambientes de *IoT* nas componentes de alarmística e monitorização.

As principais limitações passam por se ter avaliado principalmente as componentes de alarmística e monitorização e não das operações ou das transações. Também foi avaliado uma parte do fluxo de dados entre os 5 níveis definidos.

No entanto a avaliação realizada com as duas iterações na metodologia do processo DSRM, permite a demonstração que o modelo proposto é validado com as provas de conceito realizadas.

Num contexto mais amplo, o modelo pode ver alargado a sua aplicação a outros *smart places*, que suportam Organizações, com outras arquiteturas e aplicações.

1.3. Problema Central

Os *smart places* são vulneráveis ao comprometimento de dados (Popescul & Radu, 2016) e à falsa injeção de dados (K. Zhang et al., 2017), que com o crescente volume de dados e com o grande número de dispositivos, espaços, infraestruturas e utilizadores ligados, estende os riscos e pode provocar o comprometimento de todo(s) o(s) sistema(s), com a utilização de fragilidades que podem ser transmitidas ou exploradas entre os sistemas. Num caso extremo, a exploração das fragilidades ou a injeção poderá comprometer o funcionamento da própria cidade e, no limite, desligar ou mesmo destruir a infraestrutura física ao ponto de ameaçar a vida dos cidadãos ou o seu bem-estar. (Popescul & Radu, 2016)

A questão a ser respondida é a seguinte: como garantir que os dados contidos nos *logs* dos sistemas de alarmística não são adulterados ou manipulados antes de serem entregues a outras entidades e sistemas?

No *log* registam-se os eventos de alarmes de equipamentos para ajudar a detetar e proteger as Organizações contra violações de segurança cibernética e melhorar os processos de manutenção. Um *log* fornece os alarmes de erros, as ações de ativação e desativação de funções ou equipamentos, os registos de auditoria dos acessos à rede, aplicação ou base de dados, de como acederam e quando tiveram o acesso. Desta forma, permite que se possa gerir a disponibilidade dos sistemas e se detetem acessos indevidos a sistemas ou a informações confidenciais que permitam a investigação de comportamentos não autorizados.

2. Resultados da Pesquisa

Tal como já foi referido na introdução, o modelo proposto deve traduzir a dinâmica de ecossistemas digitais que suportam os ecossistemas naturais, os *smart ecosystems*, que comportam respetivamente vários domínios aplicacionais, com modelos de dados e base de dados "alimentados" por dispositivos *IoT* e móveis.

O trabalho concentrou-se principalmente no controlo do fluxo de dados, tendo sido desenvolvidos artefactos, baseados em provas de conceito que testassem a garantia de autenticidade e de integridade dos dados, controlando os fluxos entre entidades e entre aplicações permitindo a conceção de um sistema baseado em *blockchain*, suportado na rede IPFS e utilizando uma rede *blockchain* para transferir a informação de controlo sobre os dados e o acesso aos ficheiros *log*, evitando a manipulação dos *logs* e numa segunda iteração dos registos, evitando que um participante consiga realizar alterações/omissões de eventos, distorcendo a informação, o cumprimentos de determinados *SLA´s* ou a própria lógica de negócio dos sistemas monitorizados.

A evolução deste sistema nas diferentes fases do fluxo de dados pode oferecer também a hipótese de utilizar este mecanismo de controlo e segurança, deste os sensores, dispositivos *IoT* ou equipamentos móveis, evitando manipulações e alterações que evitem a deteção e condicionem os dados dos sistemas monitorizados.

2.1. A escolha da tecnologia *blockchain*

A questão do porquê da escolha da tecnologia de *blockchain*, como resposta às questões da investigação, é central. Esta escolha, embora se tenha logo revelado como a tecnologia emergente com potencial para viabilizar o modelo proposto, foi analisada e verificadas as suas caraterísticas ao longo do estudo teórico e especificamente no ponto 2., do II Capitulo.

Como veremos esta escolha incide principalmente sobre as motivações Organizacionais para a adoção tecnologia *blockchain*. Entroncando noutras questões mais comuns. O que é a tecnologia *blockchain*? Como poderá a tecnologia *blockchain* ser aplicada aos diversos contextos de negócio? Que potenciais usos podem ter?

(Li et al., 2018) referem que os futuros estudos se devem focar no porquê e no quem, ao mesmo tempo, para avaliar os impactos da tecnologia *blockchain* aos diversos níveis, deixando de se considerar a tecnologia *blockchain* como uma caixa preta, analisando-a

nos contextos em que se deve utilizar e em que circunstâncias esta tecnologia funciona melhor e para quem.

Assim, neste ponto procura-se apresentar a análise comparativa com outras tecnologias, quais as suas vantagens e desvantagens, de modo a que se possa afirmar, neste contexto de investigação, que a tecnologia *blockchain* poderá ser a melhor opção.

As comparações da tecnologia *blockchain* com outras tecnologias revelam-se principalmente em duas perspetivas. Numa perspetiva de base de dados e numa perspetiva de tecnologia de segurança.

2.1.1. Perspetiva de base de dados

Na perspetiva de base de dados verifica-se que se trata de uma tecnologia que armazena os dados de forma distribuída e imutável, com as vantagens e desvantagens que estas caraterísticas representam.

A Tabela III.3 compara a tecnologia *blockchain*, com a base de dados *legacy* centralizada e a base de dados distribuída, através das principias caraterísticas das base de dados, como a disponibilidade, a integridade do registo, a tolerância ao erro, a confidencialidade, o tempo de computação e a colaboração entre nós confiáveis, em três níveis, alto, médio e baixo.

Tabela III.3 – Comparação *Blockchain* vs. Base de dados *legacy* centralizada e Base de dados distribuída

Caraterísticas	***Blockchain***	**Base de dados *legacy* centralizada**	**Base de dados distribuída**
Disponibilidade	Alto	Baixo	Médio
Integridade do Registo	Alto	Médio	Médio
Tolerância ao erro	Alto	Baixo	Alto
Confidencialidade	Baixo	Alto	Médio
Tempo de computação	Baixo	Alto	Médio
Colaboração entre nós confiáveis	Alto	Baixo	Baixo

(Anwar, 2017)

Como se verifica nesta comparação a tecnologia *blockchain* tem uma alta tolerância ao erro, ao eliminar a possibilidade de um único ponto de falha, tal como a base de dados distribuída.

A tecnologia *blockchain* apresenta uma caraterística diferenciadora como a alta colaboração entre os nós confiáveis. Cada nó da rede contém assim a mesma versão do histórico de transações, como todos os outros nós participantes. Esta caraterística conduz a alta disponibilidade e a integridade do registo das transações distribuídas pelos nós. Cada registo é processado e verificado por nós adicionais. Outra caraterística importante, já referida, é a grande tolerância a falhas, dado que existem cópias iguais do *ledger*, com a informação exata e atualizada. A natureza distribuída do sistema baseado em *blockchain* permite que os nós possam recuperar as transações perdidas após falha.

A Tabela III.4 procura comparar os nós entre *blockchains* sem permissão (públicos), com permissão (privados) e uma base de dados centralizada, através das caraterísticas de taxa de transferência, latência, número de leitores, número de escritores, número de escritores não confiáveis, mecanismo de consenso e gestão centralizada.

Tabela III.4 – Comparar os nós entre *blockchains* sem permissão, com permissão e a base de dados centralizada.

Caraterísticas	***Blockchain* sem permissão**	***Blockchain* com permissão**	**Base de dados central**
Taxa de transferência	Lento	Alto	Muito alto
Latência	Lento	Médio	Rápido
Número de leitores	Alto	Alto	Alto
Número de escritores	Alto	Baixo	Alto
Número de escritores não confiáveis	Alto	Baixo	0
Mecanismo de consenso	Principalmente PoW, alguns PoS	Protocolos BFT (por exemplo PBFT)	Nenhum
Gestão centralizada	Não	Sim	Sim

Adaptado da tabela 1, de Wust & Gervais (2018)

A troca de dados num sistema descentralizado depende da escala do sistema, com o número de escritores sem confiança mútua, a sua taxa de transferência, o numero de estados que atualiza e que pode lidar num determinado período de tempo. Ao tomar a decisão de se usar a tecnologia *blockchain* ou não, deve ter-se em consideração o balanceamento destas caraterísticas e a forma de compensação das caraterísticas mais negativas, e no caso da tecnologia *blockchain* a ponderação entre *blockchains* públicos ou privados. (Wust & Gervais, 2018)

2.1.2. Perspetiva de segurança

A perspetiva de segurança é mais vasta e enfática, e conduz principalmente à comparação com tecnologias criptográficas e com outras tecnologias de contabilidade distribuída (*DLT-Distributed Ledger Technology*), através de inúmeras possibilidades de aplicação ou de tentativas de aplicação.

As abordagens mais comumente utilizadas para garantir a segurança dos dados passam pela infraestrutura de chave pública (*PKI - Public Key Infrastructure*) e nos protocolos de criptografia, por exemplo de e-mail como o S/MIME (*Secure / Multipurpose Internet Mail Extensions*). No entanto, sobre estas tecnologias existem várias ameaças de segurança, nomeadamente o ataque MITM (*Man-In-The-Middle*) e o ataque EFAIL (falha de segurança em sistemas de e-mail em que os conteúdos podem ser transmitidos de forma criptografada).

Como solução para as limitações destas tecnologias, no caso de mensagens, Khacef & Pujolle (2019) apresentam uma proposta de utilização da tecnologia *blockchain* para tornar as comunicações mais seguras, em mensagens, mantendo o desempenho e a segurança dos dados gravados no *blockchain*, através de um contrato "inteligente" para verificar as identidades e das chaves públicas associadas, e assim validar os certificados dos utilizadores. O sistema é descentralizado e permite aos utilizadores trocar mensagens de forma segura. A caraterística de imutabilidade da tecnologia *blockchain* fornece a solução para os problemas identificados no campo da PKI centralizada.

A confiança e a rastreabilidade são duas das caraterísticas básicas da tecnologia *blockchain*. No entanto, essas características podem não ser suficientes para fornecer uma solução completa, sendo necessário adicionar fortes protocolos criptográficos. Este adicional fornece mais confiança, rastreabilidade, segurança e controlo, essenciais para soluções críticas em contextos críticos e com maiores riscos. A imutabilidade e rastreabilidade dos dados são requisitos fundamentais para qualquer sistema critico. O sistema baseado em tecnologia *blockchain* deverá garantir: a proteção de integridade de armazenamento seguro; a privacidade e propriedade dos dados; a partilha de dados; e a rastreabilidade e responsabilização dos dados. (Katuwal et al., 2018)

2.1.3. *Blockchain* – vantagens e desvantagens

Dada a crescente dependência da tecnologia, as pessoas, as empresas e os governos suportam as suas ações e decisões em sistemas de informação em cujos dados têm de confiar. A confiança nos espaços digitais conduz à relação com a confiança em dados "autorizados". Assim, as quebras de confiança, as falsificações instalam dúvidas e receios, com novos problemas de segurança e privacidade, e com a disseminação das transações desmaterializadas. (Ruta et al., 2017)

A Tabela III.5 apresenta as principiais forças e fraquezas da tecnologia *blockchain* em relação às alternativas e em certos casos.

Tabela III.5 - Pontos fortes e fraquezas da tecnologia *blockchain*

Pontos fortes	**Fraquezas**
Visibilidade	Falta de privacidade
Agregação	Falta de padronização
Validação	*Garbage in, garbage out (GIGO)*
Automação	Efeito caixa preta
Resiliência	Ineficiência

Adaptado da tabela 1, de Babich & Hilary (2019)

Os pontos fortes da tecnologia *blockchain* e as suas fraquezas refletem a necessidade de ponderação face aos objetivos dos sistemas a desenvolver ou a substituir.

A principal vantagem da tecnologia *blockchain* é que o *ledger* não pode ser modificado ou excluído após os dados terem sido aprovados pelos nós de acordo com o protocolo de consenso. Estas caraterísticas permitem à tecnologia *Blockchain* garantir a integridade dos dados e a sua segurança, razão pela qual o seu uso se estende também a outros serviços e aplicações. (Rithika et al., 2019)

A tecnologia *blockchain* fornece assim, uma plataforma que permite interligar várias entidades, com múltiplas fontes de dados e que geram informação para sustentar decisões. Evitando assim que a decisão pode ficar condicionada ou parada com informação errática ou utilizada para fins não intencionais ou em falsos registos. (Babich & Hilary, 2019)

Um dos principais problemas com outras tecnologias está na forma de verificar se a informação recebida da rede é autêntica e atualizada. A tecnologia *blockchain* tem a capacidade de resolver este problema de autenticidade sem a inclusão de intermediários confiáveis. Esta caraterística permite que qualquer interveniente possa verificar a

autenticidade dos dados de forma independente, de quem ou onde estão os dados. (Mattila, 2016)

Os principais atributos da tecnologia *blockchain* passam por eliminar a necessidade de autoridades de confiança intermediárias, devido à natureza descentralizada da rede, o aumento da transparência e a imutabilidade do *blockchain*.(Hammer, 2018)

De acordo com Lin & Liao (2017) a tecnologia *blockchain* é compostas por seis elementos-chave: descentralizada; transparente; código aberto; autonomia; imutável; e anonimato.

2.1.4. Blockchain no contexto de IoT

As questões relacionadas com as *smart cities*, que se baseiam em redes com dispositivos de *IoT*, passam pelo estrangulamento, com o aumento multiplicador dos dispositivos ligados e que criam problemas num sistema centralizado. A tecnologia *blockchain* pode ser aplicada para resolver este problema devido à sua caraterística descentralizada. Amjad & Javaid, (2019) apresentaram um trabalho que propõe uma arquitetura de rede híbrida com funções centralizadas e outras descentralizadas, para obter eficiência. O sistema baseado em *blockchain* permite fixar os dispositivos a partir de serviços não confiáveis fornecidos por servidores não confiáveis. A tecnologia *blockchain* pretende manter o sistema seguro para diferentes transações sempre que os serviços são prestados ao cliente. O cliente fica protegido, dado que os serviços são verificados no inicio. A análise mostra que o desempenho do sistema aumenta e aumenta a segurança face ao sistema existente.

O ambiente *IoT* necessita de um processo de registo e autenticação, em que a tecnologia *blockchain*, na relação com a criptografia, pode fornecer melhores formas de autenticação e no processo de registo do que com outras soluções contemporâneas. (Ghuli et al., 2017)

A tecnologia *blockchain* necessita que a maioria dos nós da rede devam participar no mecanismo de consenso para verificar os dados de origem. Os dispositivos *IoT* são equipamentos com recursos limitados, sendo por isso, necessário melhorar o esquema de *blockchain* existente para permitir incluir estes equipamentos. Chen, Wang, e Wang (2018) apresentam duas possibilidades de ultrapassar esta possível limitação, através da: seleção aleatória de nós cooperativos para resolver o enigma de *hash* para chegar a um consenso; e da verificação baseada na maioria sem necessitar de executar criptografia (cifrar/decifrar) reduzindo o cálculo de cada nó *IoT*.

O potencial da tecnologia *blockchain* para proteger a integridade dos dados em redes do *IoT* pode ser melhorado através do esquema de verificação de dados baseada em *blockchain* e ultrapassar a deficiência das abordagens centralizadas, com um ponto único de falha e congestionamento da rede. Esta proposta pode reduzir o número de nós de cooperação e confiar em nós para gerar o bloco, e os dados são retransmitidos por um número aleatório de nós de cooperação selecionadas aleatoriamente. Assim, o nível de segurança do sistema pode ser significativamente melhorado.

A Tabela III.6 resume a comparação entre PKI e o esquema de dados baseados em *blockchain* com o esquema de verificação para evitar o ataque do nó central, eliminar o congestionamento da rede e evitar o ataque das ligações.

Tabela III.6 - Comparação entre o PKI e o esquema de dados baseados em *blockchain* estocásticos com esquema de verificação

	PKI	**Dados baseados em *blockchain* com esquema de verificação**
Evitar o ataque do nó central	A certificação poderá falhar quando Autoridade de Certificação (CA) é destruído.	A certificação não poderá ser afetada por ataque a um ponto único.
Eliminar o congestionamento da rede	Apenas o CA tem autoridade para verificar.	Cada nó tem autoridade para verificar.
Evitar o ataque das ligações.	O atacante pode atacar o acesso à Autoridade de Certificação (CA), na fonte e destino	O atacante não sabe quem atacar.

Adaptado da figura 8, de Chen, Wang, e Wang (2018)

Os resultados das simulações demonstram que a segurança aumentou numa rede *IoT* em larga escala, mesmo com um pequeno número de nós cooperativos.

Cekerevac, Prigoda, e Maletic (2018) referem que a tecnologia *blockchain* pode identificar e autenticar os dispositivos *IoT* autónomos. Desta forma a tecnologia *blockchain* pode transformar as soluções *IoT*, evitando falhas na gravação dos dados e informações, ao permitir controlar sensores e os dados de medições, e os equipamentos *IoT* poderem enviar os dados diretamente. A tecnologia permite que cada participante, com base no nível de licença possa aceder a dados, nomeadamente do estado em tempo real.

2.1.5. Adoção

Os *drivers* não técnicos, nomeadamente "crenças filosóficas", efeitos de rede e incentivos económicos, poderiam explicar também a adoção da tecnologia *blockchain*. Esses *drivers* podem explicar, afinal, a razão base para a adoção da tecnologia *blockchain*.

Tabela III.7 - *Drivers* para a adoção de tecnologia *Blockchain*

Categoria	***Drivers***
Propriedades do cenário	Estado armazenamento
	Vários escritores
	Não é possível usar TTP (*Trusted Third Party*)
	Escritores desconhecidos
	Escritores não confiáveis
	Verificação pública
"Crenças filosóficas"	Não se vai usar TTP
	Necessidade de descentralização
	Reforço da privacidade
	Sistema alternativo
	Razões políticas
Efeitos de rede	Impulsionada pela comunidade
	Curiosidade
	Bom para usar
Incentivos económicos	Produto de marketing
	Equipamentos de venda de mineração
	Consultoria de venda
	Carregar para a plataforma
	Medo de perder
	Investimento alternativo

Adaptação da tabela 1, de Koens & Poll (2018)

Para além destes *drivers* é necessário ser mais objetivo e procurar resposta e resultados que permitam de forma sustentável adotar esta tecnologia.

O que começou como um código colocado por um investigador anónimo (Nakamoto, 2008), com o objetivo de criar uma nova plataforma de moeda, o bitcoin, a tecnologia *blockchain* disparou em popularidade, em quase todos os setores, das cadeias fornecimento, das finanças e da saúde, passando pela educação e pelo planeamento da cidade. Em conclusão, a tecnologia *blockchain* parece melhorar não só as tarefas em indústrias atuais, como em outros contextos que vão surgindo (Sharma & Bhuriya, 2019).

No que diz respeito às capacidades *blockchain* como o aumento do acesso de dados e da validade dos dados, a tecnologia *blockchain* aparece principalmente com os aspetos de

segurança, com a confiança na validade dos dados, donde veem e para rastrear as ações (Bauer, Zavolokina, Leisibach, e Schwabe, 2019).

De forma a testar a adoção da tecnologia *blockchain* no modelo a propor foi aplicado o modelo de maturidade para adoção de *blockchain* proposto por Wang (2016), que se descreve a seguir, com o procedimento em três fases para a adoção segura desta tecnologia.

Ponto 1: O porquê do *blockchain*? (4 das 6 questões positivas permite uma adoção segura)

- Várias partes partilham dados: os vários participantes necessitam de visualizar informações comuns;
  Aplica-se à nossa proposta? Sim. A várias entidades e/ou aplicações.
- Várias partes partilham dados atualizados: múltiplos participantes tomam ações que precisam ser registados e alteram os dados;
  Aplica-se à nossa proposta? Sim.
- A exigência de verificação: os participantes precisam de confiar na validade das ações que são registradas;
  Aplica-se à nossa proposta? Sim.
- Os intermediários adicionam custos e complexidade: a eliminação de intermediários e da "autoridade central" de registo tem o potencial de reduzir o custo e a complexidade;
  Aplica-se à nossa proposta? Sim.
- As interações são sensíveis ao tempo: reduzir os atrasos tem benefícios de negócios;
  Aplica-se à nossa proposta? Sim.
- Interação de transação: as transações criadas por diferentes participantes dependem umas das outras;
  Aplica-se à nossa proposta? Sim.

Resultado: A resposta a 6 das 6 questões são positivas. Trata-se de uma adoção segura de acordo com o modelo de maturidade para adoção de *blockchain*.

Para reforçar a sua adoção deve respeitar o ponto 2 e 3, o que vai de encontro ao modelo proposto.

Ponto 2: Desenvolvimento deve focar-se em:

- Análise de requisitos;
- *Design* arquitetónico.

Ponto 3: Operação, em que o sistema *blockchain* substituirá um sistema existente, propondo-se um procedimento de substituição progressiva:

- Manter o funcionamento do sistema existente e executar o sistema *blockchain* como o sistema de backup para um determinado período;
- Se o sistema *blockchain* está a funcionar corretamente, deixá-lo correr como o sistema operativo principal e executar o sistema existente como o sistema de backup.
- Finalmente, operar o sistema *blockchain* como o suporte.

Resultado: O nosso modelo e os artefactos desenvolvidos começam de forma progressiva procurando complementar todo o fluxo de dados.

Como se avaliou, a adoção da tecnologia *blockchain* prevista no modelo genérico de dados, no contexto dos *smart places*, suportados em *IoT*, cumpre os requisitos que podem potenciar as vantagens elencadas ao longo deste ponto, principalmente na garantia da autenticidade dos dados e da integridade dos dados, fornecendo diversas aplicações que serão complementares e estruturantes no funcionamento dos ecossistemas da *smart city*.

2.2. Modelo Genérico de Dados

O resultado do estudo teórico realizado permite estruturar as ontologias gerais que se revelam potenciadoras de um modelo genérico de dados que representa o conjunto de conceitos e o relacionamento entre estes, inferindo os principais objetos do domínio.

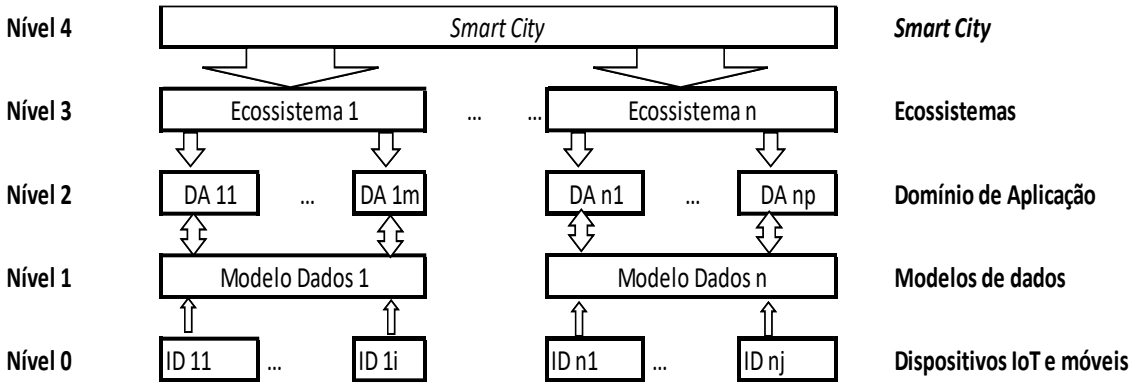
A proposta de um modelo genérico de dados de confiança representado na Figura III.3 pretende organizar uma *smart city* global, em ecossistemas (Ceballos & Larios, 2016; Dhungana et al., 2016), com os respetivos domínios de aplicação, suportado em modelos de dados genéricos, alimentados pelos inúmeros dados *IoT*.

A *smart place* é o espaço físico e lógico que se pretende estruturado. As *smart cities* são divididas em ecossistemas, *smart economy*, *smart environment*, *smart living*, *smart mobility*, *smart people* e *smart government*, baseados no circulo de Cohen (2013). Cada ecossistema possui vários domínios aplicacionais com componentes de gestão, monitorização, segurança e privacidade, que são estruturados em modelos de dados genéricos, dependendo das aplicações do domínio.

O modelo tem cinco níveis estratificados, que agregam os dados e resumem ao nível superior as informações necessárias e suficientes que garantem a gestão do nível inferior.

Este modelo reflete o desenho, como a síntese do estudo (Walls et al., 1992) realizado de forma a simplificar e refletir a perspetiva de um *smart place* (*smart city*) baseado em *IoT*.

Figura III.3 Modelo de contexto duma *smart city*



(Brandão et al., 2018a)

Neste modelo a troca de dados entre os ecossistemas são baseados em interfaces que promovem a interoperabilidade de dados que necessitam ou dependem de dados de outros ecossistemas. Trata-se de um aspeto fundamental para realizar a gestão de dados e o controlo de fluxo de dados e para se atingir dados únicos e de confiança para a dinâmica que se espera de uma *smart city*.

As características dos dados devem permitir que o fluxo de dados seja consistente e suficientemente granular em cada nível para se poder segmentar os dados partilhados com as proteções e as permissões adequadas.

Cada nível tem capacidade de processamento de dados e de armazenamento, através de computação *cloud* distribuída, a reutilização de dados *IoT* e dos dados agregados

O modelo que se pretende de confiança orienta-se para tornar o sistema centrado no cidadão, no utilizador, com uma abordagem global da gestão de dados e da governança dos dados, com o controlo das permissões, dos consentimentos face à privacidade, da visualização dos dados, dos acessos aos históricos e na reutilização dos dados para diversas finalidades.

A Tabela III.8 pretende agrupar o conjunto de aplicações do *blockchain* num *smart place* (na *smart city*), tipificando em seis tipos de aplicação de *blockchain* que agrupam as finalidades que suportam o modelo.

Num primeito tipo temos as transações seguras que se orientam para o uso da tecnologia *blockchain* para garantir as transações distribuídas de dados imutáveis, com a troca de registos de transações consistentes e incorruptíveis e se possível orientadas à monetização das transações.

Num segundo tipo temos a segurança dos dados que permite o uso da tecnologia *blockchain* para garantir o acesso autorizado aos diversos participantes ou envolvidos nos processos cumprindo as permissões padrão ou autorizadas, de forma consistente com os diversos tipos de atores e por ação do cidadão ou utilizador.

Num terceiro tipo temos o controlo do fluxo de dados que permite a utilização do *blockchain* para garantir a gestão dos dados entre Organizações e o respeito pelas regras associadas aos tipos de dados (pessoais, pessoais sensíveis, dados sensíveis, dados abertos, etc.). Esta utilização permite também o acesso do cidadão aos seus dados, aos seus consentimentos e ao histórico de acessos aos seus dados.

Num quarto tipo temos a aceitação dos dispositivos que se orienta a utilização do *blockchain* para garantir que os nós aceites tenham uma "identidade" na Organização, validada por certificação ou através de *smart contracts*.

Num quinto tipo temos o controlo de versões que orienta o uso do *blockchain* para garantir a compatibilidade das versões do sistema, dos equipamentos *IoT*, dos dispositivos móveis e de outros dispositivos.

Num sexto tipo temos a aplicação na segurança do sistema que pretende usar a tecnologia *blockchain* para garantir a confiança das configurações dos sistemas, como os servidores em *cloud*, os dispositivos *IoT* e os dispositivos móveis.

A tabela a seguir mostra estes seis tipos de aplicação da tecnologia *blockchain*.

Tabela III.8 - Tipos de Aplicação do *blockchain* (BC)

Tipo	Aplicações de *blockchain* (BC)
BC1	Transações seguras
BC2	Segurança dos dados
BC3	Controlo do fluxo de dados
BC4	Aceitação de dispositivos
BC5	Controlo de versões
BC6	Segurança dos sistemas

A Tabela III.9 relaciona os cinco níveis propostos na Figura III.3 com os seis tipos de aplicação da tecnologia *blockchain* da Tabela III.8.

Tabela III.9 - Aplicação do *blockchain* no contexto de *smart cities*

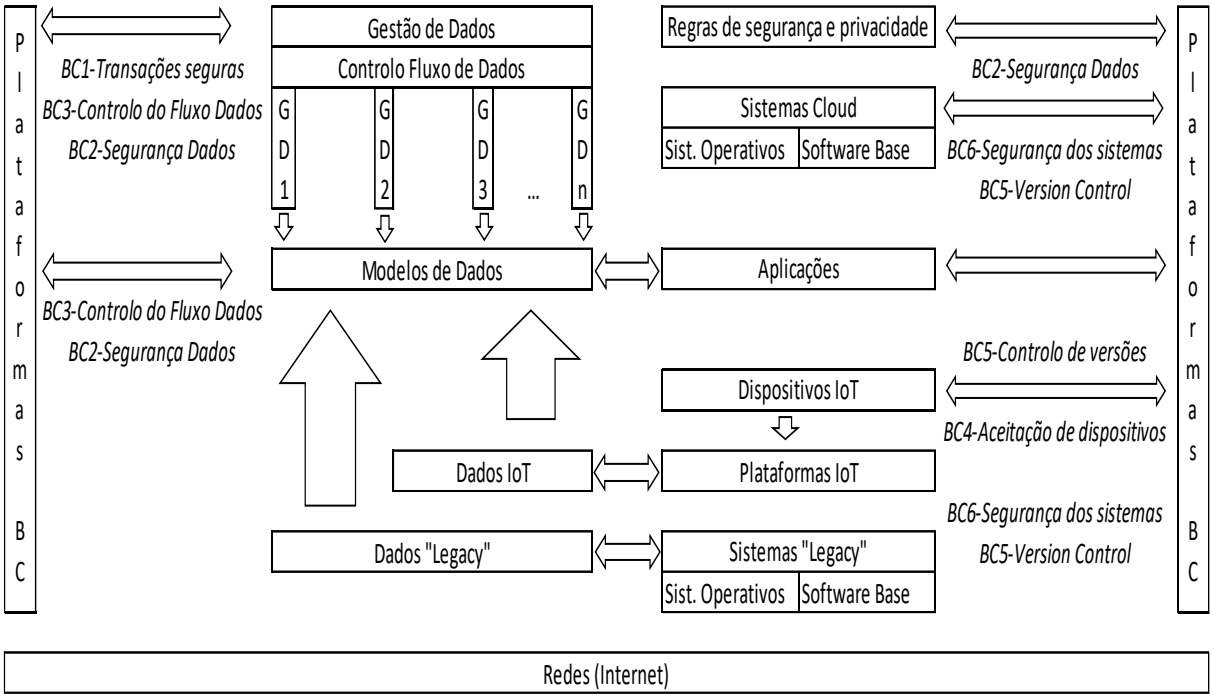
Contexto da *smart city*		**Aplicação do *blockchain***					
		BC1	**BC2**	**BC3**	**BC4**	**BC5**	**BC6**
Nível 4	*Smart city*	X	X	X			
Nível 3	Ecossistemas	X	X	X			
Nível 2	Domínio de Aplicação	X	X	X	X	X	X
Nível 1	Modelos de dados		X	X		X	X
Nível 0	Dispositivos *IoT* e móveis		X	X	X	X	X

A análise ao que se pretende em cada um dos níveis verificamos que o tipo BC2 da segurança dos dados e o BC3 do controlo de fluxo de dados se aplicam a todos os níveis no contexto da *smart city*. O tipo BC1 das transações seguras aplica-se aos três níveis superiores. Os tipos BC5 e BC6, referentes ao controlo de versões e segurança dos sistemas, aplicam-se aos 3 níveis inferiores. O tipo BC4 aplica-se ao nível 2 e 3, ao domínio de aplicação e aos dispositivos *IoT* e móveis.

2.3. Arquitetura Geral

A definição da arquitetura tem como base os fluxos de interação dos diversos níveis e tipos de aplicação *blockchain* revelados na Tabela III.9 com a utilização de plataformas de *blockchain* e plataformas *IoT*. O controlo do fluxo de dados baseia-se na necessidade de segmentar os dados em grupos com caraterísticas homogéneas e que permitam a sua gestão e controlo dos fluxos de dados, como forma de definir regras de segurança e de privacidade que permitam controlar o acesso e a alteração, subordinando à gestão de permissões e à gestão de consentimento. A Figura III.4 apresenta os principias fluxos num *smart place*, respeitando as seis aplicações da tecnologia *blockchain* previstos no modelo.

Figura III.4 - Fluxos de dados num *smart place*

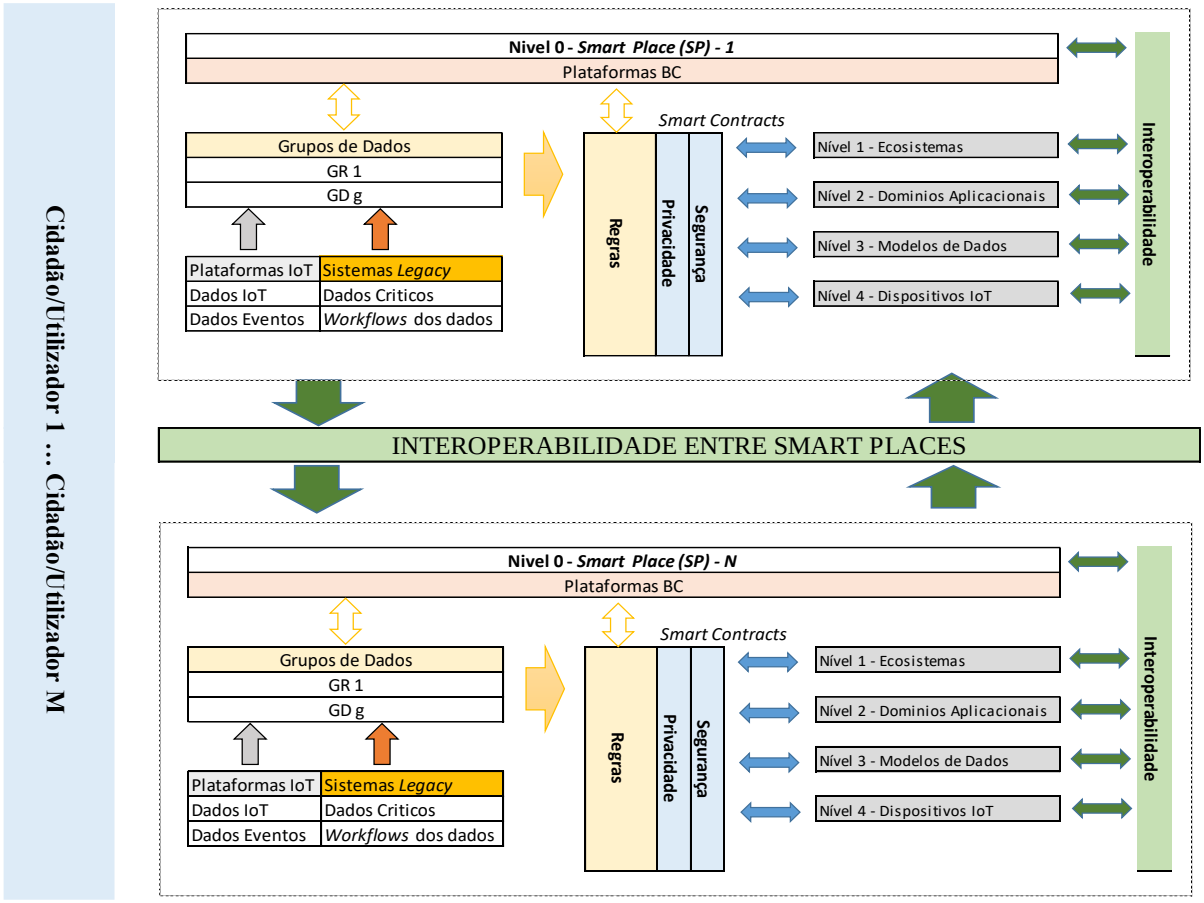


O modelo de confiança proposto apresenta como aspeto crítico a forma de estabelecer a interoperabilidade baseada nos grupos de dados (GD). Os grupos de dados respeitam as estruturas de dados, de acordo com o domínio de aplicação, para permitir definir uma granularidade sobre o conjunto de dados, para aplicar regras de privacidade e para aplicar regras de segurança padrão ou as definidas pelo cidadão/utilizador.

Os *smart places* centrados no cidadão/utilizador e numa perspetiva de mobilidade física e lógica terão de interagir entre si e comunicar os grupos de dados e as regras de segurança e privacidade que estarão disponíveis para estabelecer uma continuidade de dados e de presença do cidadão/utilizador em espaços físicos e lógicos diversos.

Esta perspetiva pode ser visualizada na Figura III.5 através dos macro fluxos intra e inter *smart places*, centrados no cidadão/utilizador, que comunicam dentro do seu espaço (intra) e entre espaços distintos (inter) através de grupos de dados e de acordo com as regras de segurança e privacidade padrão ou definidas pelos cidadãos/utilizadores.

Figura III.5 – Macro Fluxos Intra e Inter *smart places*, centrados no cidadão/utilizador



A relação que se pode vir a estabelecer entre vários *smart places* não será objeto de análise neste trabalho e de aplicação da metodologia definida, podendo em futuras investigações vir a ser concretizada.

2.4. Aplicação da metodologia

Neste ponto desenvolve-se a metodologia sumariamente descritiva no ponto deste capitulo, especificamente no ponto III.1.2. referente às etapas da metodologia.

A concretização da metodologia permitirá a validação de alguns aspetos do modelo genérico de dados baseado na tecnologia *blockchain* e da arquitetura geral descritos nos pontos anteriores.

Esta especificação conduz a uma clara e objetiva proposta para a realização dos artefactos que permitirão demonstrar e validar o modelo e a sua projeção ou extrapolação para os restantes ecossistemas, domínios aplicacionais, sistemas e modelos de dados e dispositivos *IoT* que constituem o modelo de dados genérico proposto para os *smart places* e neste caso em análise nas *smart cities*.

2.5. A escolha do ecossistema de mobilidade e a aplicação de Bilhética

No contexto das *smart cities* os problemas de autenticidade e de integridade dos dados são críticos no funcionamento e segurança dos diversos ecossistemas e das pessoas, conforme detalhadamente referimos nos ponto 1.1., do capitulo II.

O conhecimento aprofundado deste ecossistema por parte da equipa de investigação e a possibilidade de intervir, desenvolver e rever, em termos de dados, de base de dados e de aplicações permitiu consolidar vários dos aspetos a avaliar no modelo proposto.

O sistema de mobilidade, analisado no ponto 4, do capitulo II, na componente de transportes ferroviários, acresce às preocupações de segurança ferroviária, aspetos normativos adicionais, integrações com outros modos de transporte coletivo e individual, necessidades imperativas de disponibilidade, cumprimento da oferta, qualidade dos serviços prestados ao cliente e o acesso múltiplo a dados de monitorização e alarmística que permitem em tempo real a redefinição e reafectação do transporte, a autorregulação, a antecipação de problemas e a segurança em todas as componentes.

A escolha inicial incidiu sobre o sistema de gestão de trafego na sua componente de alarmística e monitorização, como sistema de elevada criticidade e risco, com incidência sobre a segurança das pessoas e do espaço publico. Nos estudos realizados foi possível verificar que se tratava de um sistema sujeito a grandes restrições de acesso, limitações de propriedade intelectual, patentes e de *software* proprietário, que condicionavam o desenvolvimento do artefacto, o conhecimento do modelo de dados da aplicação e a possibilidade de validar e testar. Embora tenha sido possível testar a autenticidade dos *logs* referente à 1ª iteração, demonstrando a universalidade do modelo e do artefacto proposto.

O sistema de bilhética surgiu como opção para validar o modelo como resposta à questão de investigação. Este sistema tem elevado impacto no cliente final, na sua perceção sobre a qualidade do sistema de mobilidade, a sustentabilidade económica e com impacto ambiental nos espaços e nas *smart cities*. A componente de monitorização e alarmística fornece dados sobre os múltiplos equipamentos de venda, de validação e de sensorização, distribuídos por várias entidades/operadores, com múltiplos fornecedores sujeitos a níveis de serviços baseados em elevada disponibilidade dos equipamentos, principalmente dos que têm elevado impacto direto no cliente final e nos locais de mais afluência.

Como se virá a verificar o sistema escolhido servirá como referência para a realização do artefacto, com as provas de conceito, podendo ser extrapolado para outros sistema que se inserem num *smart place*, nas componentes de alarmística e monitorização.

O conhecimento aprofundado destes sistemas no ecossistema de mobilidade permitiu construir as provas de conceito e validar o modelo genérico de dados proposta.

2.6. Conceção e desenvolvimento do artefacto

A conceção e desenvolvimento do artefacto suportou-se nas escolhas sustentadas pelos pontos 2.1 e 2.5 que permitiram encontrar a forma de validar o modelo proposto, através da utilização da tecnologia *blockchain* no contexto do ecossistema de mobilidade.

As etapas descritas no 1.2 e 1.3, do capitulo 3, definem o problema e a motivação.

Os *smart places* são vulneráveis ao comprometimento de dados (Popescul & Radu, 2016) e à falsa injeção de dados (K. Zhang et al., 2017), com a utilização de fragilidades que podem ser transmitidas ou exploradas entre os sistemas.

A conceção e desenvolvimento do artefacto tem como objetivo o de encontrar a solução que permita testar a aplicação do modelo de dados genérico confiável baseado na tecnologia *blockchain,* de suporte aos *smart places*, particularmente de *smart cities*.

O artefacto pretende, assim, testar e validar o modelo proposto numa componente específica, para garantir a segurança dos dados e o controlo do fluxo de dados.

O modelo de dados e os dados que servem de base ao artefacto referem-se à componente aplicacional dos eventos de monitorização e alarmística, existentes nas aplicações suportada em *IoT* e para o qual o modelo proposto se direciona.

O registo e tratamento destes eventos permitem ações continuadas de manutenção preditiva, preventiva e corretiva, a avaliação das disponibilidades dos sistemas e dos equipamentos e o cálculo dos níveis de serviço contratados de suporte e manutenção.

O *smart place* proposto para esta experimentação é uma *smart city*, o ecossistema em análise é o ecossistema de mobilidade (*smart mobility*), o domínio aplicacional é o dos transportes públicos ferroviários urbanos, o sistema e o modelo de dados que serve de base à metodologia é o do sistema de bilhética na sua componente de alarmística e monitorização de equipamentos *IoT*.

O cumprimento dos níveis de serviço, através de *SLAs* (*Service Level Agreement*) contratuais, tem um elevado impacto no utilizador final sobre a compra do seu bilhete com consequências nas possíveis multas e na satisfação ou insatisfação sobre a experiência de viajar num determinado transporte.

A manipulação dos dados pode dissimular os problemas existentes e esconder situações graves de indisponibilidade, de acessos indevidos e de alarmes graves ou críticos poderem ser omitidos, com consequências imprevisíveis.

A escolha deste sistema e do modelo de dados para testar o modelo baseou-se no elevado impacto que tem com o cliente final e na qualidade percebida que tem na formação da qualidade global sobre o sistema de transporte. Também por se tratar de uma componente aplicacional transversal ao sistemas e aplicações que estão suportados em equipamentos com sensorizações ou baseados em *IoT* e desta forma poder demonstrar e validar o modelo nesta componente de alarmística e monitorização com base nas provas de conceito que compõem o artefacto de demonstração.

Outros sistemas foram analisados e ponderados para este trabalho principalmente o sistema de gestão de tráfego, que se revelou muito difícil de aceder dado o nível de segurança e os processos de certificação de segurança a que obedece e o não acesso à estrutura e modelo de dados, muito condicionado por se tratar de um sistema proprietário e com elevada dependência do fornecedor e com restrições de propriedade intelectual, direitos de autor e patentes.

Neste artefacto evolui-se do modelo tradicional suportado num ficheiro *log* que é transferido entre entidades ou aplicações, para o modelo confiança de controlo efetivo do fluxo de dados dos *logs* do sistema de alarmística (na primeira iteração da metodologia) e na segurança no registo dos dados (na segunda iteração da metodologia).

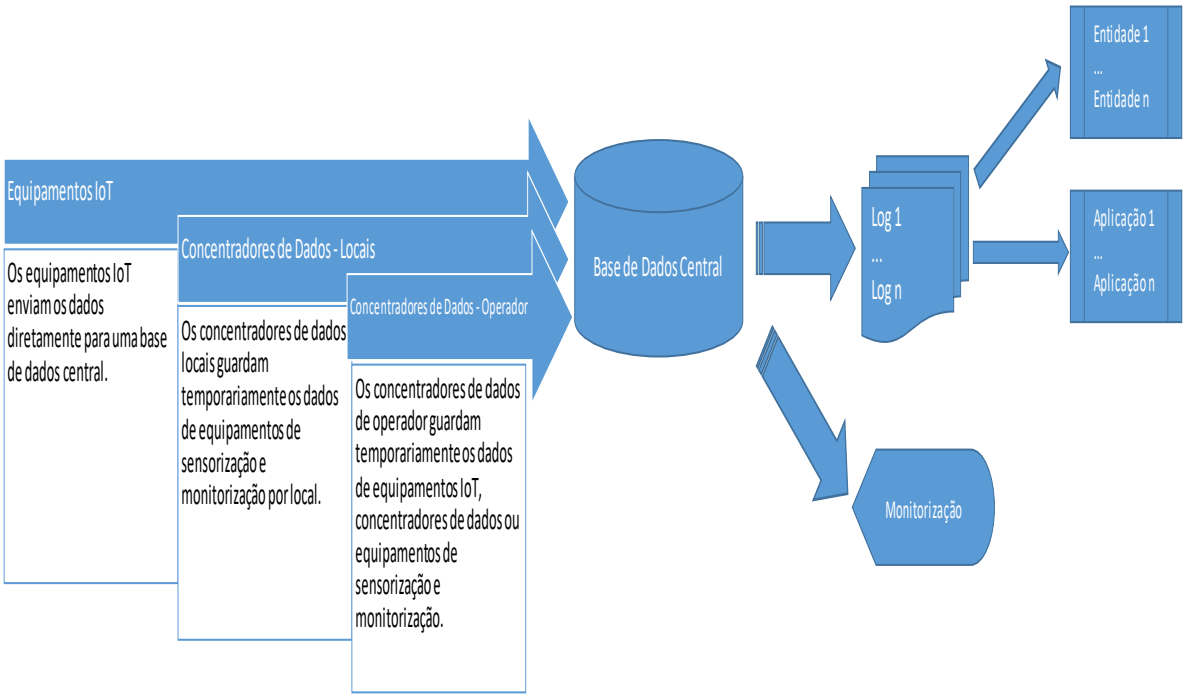
2.6.1. 1ª Iteração da metodologia proposta

O artefacto, baseado em provas de conceito, na 1ª iteração, pretende garantir a confiança na geração de ficheiros *logs*, no seu acesso e no envio entre sistemas ou entidades distintas.

O fluxo de dados global tradicional apresenta o fluxo de dados de eventos de alarmística e monitorização para a base de dados central e depois a sua disponibilização para aplicações de monitorização, para a criação de ficheiros *logs* sequenciais no tempo e a

sua transferência para outras entidades e para aplicações que consolidam esses dados em aplicações como o SIEM (*Security Information and Event Management),* a *datawarehouse,* ferramentas de cálculos de *SLA´s* com penalidades e ferramentas de BI (*Business Intelligence*).

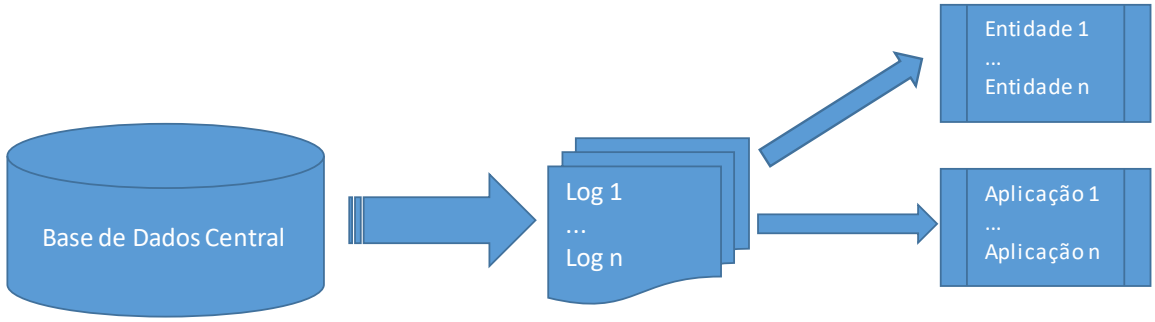
Figura III.6 - Fluxo de dados de eventos de alarmística e monitorização



A existência de concentradores de dados locais e de operador deve-se à necessidade de armazenar os dados em situações de *offline* em que diversos equipamentos não têm armazenamento próprio ou têm capacidade limitada.

A conceção do artefacto concentra-se na fase indicada na figura seguinte.

Figura III.7 - Fase do fluxo de dados objeto do artefacto



Esta primeira iteração teve como foco a resposta em como proteger os *logs* e garantir a sua autenticidade. O *log* regista os eventos e alarmes, permitindo às Organizações a

análise e a proteção contra violações de segurança cibernética. Os *logs* podem fornecer registos de auditoria dos acessos à rede, à aplicação ou à base de dados, o modo como acederam e quando tiveram acesso. Assim, permitem a deteção de acessos indevidos, a sistemas ou informações confidenciais e a investigação de comportamentos não autorizados.

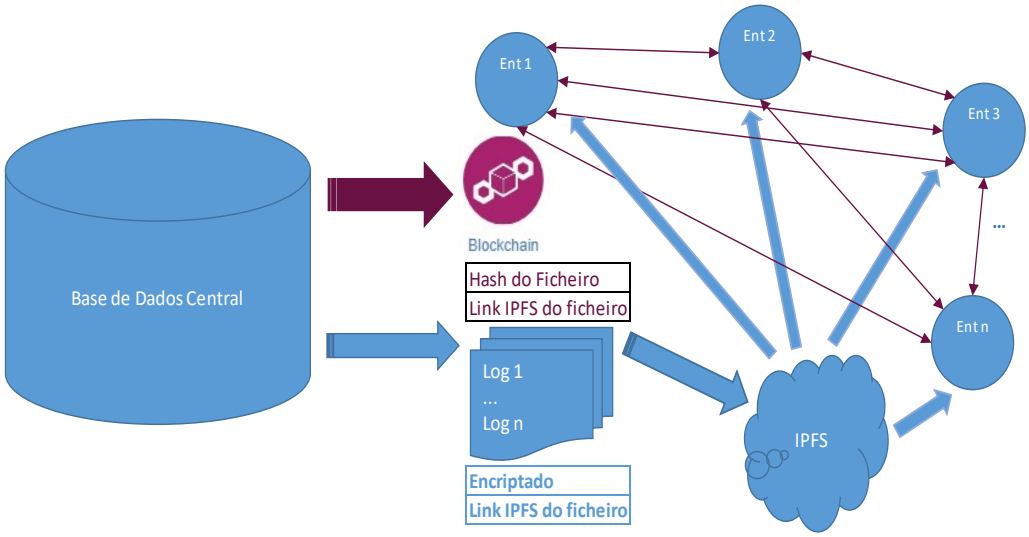
Os principias problemas passam por violações de segurança em contas com privilégios ou permissões especiais, para obter um nível de acesso que possibilite a edição dos *logs* para manipular o seu rastro e o *log* histórico.

O fluxo tradicional da Figura III.7 foi alterado para permitir dois processos descritos na Figura III.8 de controlo de fluxo, que passam por:

- A geração dos ficheiros *log* e que os disponibiliza numa rede IPFS suportada em *blockchain,* fornecendo aos diversos nós da rede privada o acesso por chave privada e pública para a cifragem/decifragem dos ficheiros disponíveis.
- Os dados com a indexação dos *links* dos ficheiros e respetivo *hash*, distribuídos por uma rede *blockchain*, fornecem aos nós das entidades envolvidas a informação para aceder aos ficheiros, em sequência e com o *hash* esperado para cada um dos ficheiros (podendo utilizar o mesmo o *hash* de acesso à rede IPFS).

A Figura III.8 apresenta assim a conceção do artefacto de desmonstração garantido a redundância dos ficheiros *log* intrínseco à rede IPFS e dos dados de acesso na rede privada de *blockchain,* a autenticidade dos ficheiros *logs* através dos mecanismos *hash* dos ficheiros e o acesso suportado em chaves para a cifragem/decifragem dos ficheiros.

Figura III.8 - Conceção do Artefacto na 1ª Iteração



A rede privada de *blockchain* necessita de um convite e deve ser validada pela entidade ou utilizador que implementou a rede obedecendo ao conjunto de regras implementadas. Esta rede configura um *blockchain* privado e uma rede autorizada que impõe restrições de participação e de transações a realizar. Desta forma, os participantes necessitam de permissão para participar, através do mecanismo de controlo de acesso utilizando uma autoridade certificadora ou com a emissão de chaves privadas e públicas da rede.

O *blockchain* privado e independente, implementado nesta prova de conceito permite que o processo de integração com outras entidades ou aplicações forneça uma verificação independente da autenticidade dos ficheiros *logs*, da integridade dos dados no ficheiro e da sequência dos ficheiros.

O ficheiro IPFS cifrado é acedido através do seu *hash* (ipfs/ <file*hash*>) contido no *blockchain* para o poder decifrar através da chave privada. A gestão de chaves e a partilha distribuída de *blockchain* permite gerir os acessos aos ficheiros *log* com os dados *IoT*. A implementação dos mecanismos de cifragem e envio para IPFS dos ficheiros *log* decorreu conforme o detalhe descrito no ponto 2.6.1.1 com a Operacionalização da 1ª Iteração.

Também se analisou a rede de *blockchain* integrada com o IPFS através da plataforma Infura[64] que fornece as API´s para aceder ao Ethereum e ao IPFS, evitando configurações específicas das infraestruturas para nós Ethereum e nós IPFS. Esta solução permite interagir com as plataformas Ethereum e IPFS através das ferramentas e das API´s disponibilizadas.

A criação deste mecanismo de replicação dos ficheiros *log* é mantida pelos *ledgers* distribuídos pelos diferentes nós da rede privada de *blockchain*, de diferentes entidades, com as propriedades de segurança, nomeadamente de imutabilidade dos dados para aceder aos ficheiros *logs* acessíveis na rede distribuída IPFS.

A 5ª Etapa, de avaliação da primeira iteração da metodologia de investigação seguida, permitiu verificar que os mecanismos implementados permitem garantir os objetivos definidos na conceção do artefacto.

[64] Infura - https://infura.io/, acedido em 10-06-2019

A avaliação, que decorreu da demonstração e da verificação, indica que os *logs* obtidos e transmitidos se revelam imunes à adulteração ou manipulação e se garante que são a entregue exclusivamente aos destinatários autorizados.

Este processo comparou os sistemas tradicionais desenhados sem esta preocupação de autenticidade e segurança, com esta prova de conceito concebida e verificou-se que através da implementação destes mecanismos baseados na tecnologia *blockchain*, se potencia a criação de soluções desenhadas de base para a segurança e a privacidade (*security by design e privacy by design*).

A avaliação permitiu confirmar que a utilização da tecnologia de *blockchain* pode tornar o acesso ao *log* descentralizado disponível em qualquer nó da rede, com os dados *hash* disponíveis nesses locais autorizados e acedidos através de mecanismos criptográficos que os protegem de acesso indevidos.

Os nós podem validar por consenso e verificar se os dados estão corretos deixando de ser possível a edição do *log* e a sua manipulação. Cada bloco no *blockchain* tem o *hash* único de cada ficheiro *log*, o que comprova a integridade da informação e a fiabilidade de todas as transações, evitando qualquer tentativa de adulterar o *log* e o seu acesso indevido pela proteção criptográfica.

A avaliação identificou uma importante fragilidade no controlo do fluxo de dados. Os dados enviados para os ficheiros *logs* e inseridos na base de dados podem nesta fase de inserção condicionar a geração dos ficheiros *log* e poderem ser manipulados pela entidade que detém a base de dados central ou por acessos indevidos.

Nesta avaliação e tendo em conta o fluxo de dados verificou-se também a necessidade de controlar a fase do processo anterior à geração dos ficheiros *logs*, existindo o risco de nesta fase se poder filtrar ou manipular os registos inseridos na base de dados. Esta constatação implicou uma 2ª iteração que se revela importante para completar mais uma fase no controlo do fluxo de dados global.

2.6.1.1. Operacionalização da 1ª Iteração

A 1ª iteração realizou-se com a implementação dos mecanismos de cifragem e envio para a rede IPFS dos ficheiros *log* e da implementação do *blockchain* em Ethereum, e realizou-se com os passos descritos e desenvolvidos para estas provas de conceito.

Adotou-se a plataforma Ethereum para a rede *blockchain* criando-se três nós e desenvolvendo a estrutura de dados, nomeadamente os *hashs* dos ficheiros *logs* e os *links* para os ficheiros na rede IPFS. Desta forma os nós desta rede privada contêm as chaves privadas e públicas que permitem o acesso à decifragem dos ficheiros *logs*.

No primeiro conjunto de testes, referentes à 1ª iteração, analisou-se o sistema num contexto de funcionamento normal embora num ambiente simulado.

Neste caso, e na primeira iteração, utilizaram-se dados reais recolhidos até 2019-04-01 às 15:46:21 pelos diversos equipamentos da rede de bilhética, inseridos numa base de dados de testes, em SQLEXPRESS versão 14.0.1., tendo por base um processo de exportação diária onde foram gerados ficheiros *logs* com os eventos filtrados pelo tipo de equipamento e com os tipos de alarmes para a avaliação do cumprimento de níveis de serviço (SLA´s) de disponibilidade.

Na tabela seguinte encontram-se os campos que são gravados no ficheiro *log*, numa base diária e que são enviados para entidades terceiras prestadoras de serviço e para aplicações especificas para o cálculo de disponibilidades e respetiva aplicação de penalidades dependendo do intervalo do indicador contratual.

Tabela III.10 - Campos exportados para o ficheiro *Log*

Campo	Descrição
Codigo	Evento ID
Equipamento	Equipamento ID
TipoEvento	Tipo de Evento
DescricaoTipoEvento	Descrição Tipo Evento
Modulo	Módulo
DataHoraOn	Data Hora online Real
DataHoraOnCorrigida	Data Hora online Corrigida ao período mensal
DataHoraOff	Data Hora offline Real
DataHoraOffCorrigida	Data Hora offline Corrigida ao período mensal
Estacao	Código da Estação
NomeEstacao	Nome da Estação
Operador	Operador de Transportes
NomeOperador	Nome do Operador

A tabela seguinte identifica os tipos de eventos considerados para esta avaliação. De notar que os tipos de eventos se centram principalmente nos que têm maior impacto no cliente, na utilização do sistema de bilhética.

Tabela III.11 - Tipo de Eventos considerados

Tipo Evento	Descrição do Tipo de Evento
124	Cofre de moedas cheio - Cofre de moedas
123	Cofre de moedas não está presente - Cofre de moedas
132	Cofre de notas cheio - Cofre de notas

Tipo Evento	Descrição do Tipo de Evento
131	Cofre de notas não está presente - Cofre de notas
164	Dispensador de cartões bloqueado - Dispensador
224	Dispensador de cartões bloqueado - Dispensador 2
121	Não há trocos (modo "quantia exata") - Depósito de trocos
126	Parado devido a encravamento - Depósito de trocos
160	Dispensador de cartões encravado - Dispensador
220	Dispensador de cartões encravado - Dispensador 2
161	Dispensador de cartões vazio - Dispensador
170	Erro de comunicação (Impressora de recibos) - Impressora de recibos
171	Sem papel - Impressora de recibos
120	Erro de comunicação (Moedas) - Moedas
122	Erro na abertura do shutter - Moedas
134	Notas encravadas no mecanismo - Notas
130	Falha de comunicação - Notas
140	Não há comunicação com o módulo OEM - OEM/SIBS
143	Não há comunicação com a SIBS - OEM/SIBS
142	Pagamento MB indisponível - OEM/SIBS
190	Erro de comunicação (Módulo *Contactless*) - Sem-Contacto
102	Fora de serviço

A perceção do funcionamento global do sistema fica refletido no cálculo de indicadores e deve conduzir a processos de reposição, conservação e manutenção mais apurados e que minimizem o seu elevado impacto nos processos de negócio. Tratam-se de processos que exigem confiança nos dados contidos nos ficheiros *log*, sendo por isso tentadoras as manipulações dos ficheiros *log*, no sentido de omitir ou corrigir determinados sinais ou as suas entradas em *ON* ou em *OFF*. Os períodos de indisponibilidade podem ser objeto de ponderação agravada (2x mais) dependendo da localização dos equipamentos face ao impacto no cliente e a simultaneidade da indisponibilidade de equipamentos num local.

Os tipos de eventos são tratados face à simultaneidade dos sinais, podendo não contar se ocorrerem no mesmo período.

A Tabela III.12 apresenta um exemplo do ficheiro log gerado, referente ao mês novembro de 2018 (de 01-11-2018 a 30-11-2018).

Tabela III.12 – Exemplo do ficheiro *log*

Codigo	Equipamento	TipoEvento	DescricaoTipoEvento	Modulo	DataHoraOn	DataHoraOnCorrigida	DataHoraOff	DataHoraOffCorrigida	Estacao	NomeEstacao	Operador	NomeOperador
49721319	1717	130	Falha de comunicação	Notas	2018-05-26 14:25	2018-11-01 00:00		2018-11-30 23:59	17	Casa da Música	2	Operador01
52479956	24912	123	Cofre de moedas não está presente	Cofre de moedas	2018-10-24 08:38	2018-11-01 00:00	2018-11-03 12:53	2018-11-03 12:53	249	Fânzeres	2	Operador01
52513980	2812	123	Cofre de moedas não está presente	Cofre de moedas	2018-10-26 12:41	2018-11-01 00:00	2018-11-02 14:51	2018-11-02 14:51	28	Vilar do Pinheiro	2	Operador01
52600364	1212	102	Fora de serviço		2018-10-31 14:25	2018-11-01 00:00	2018-11-01 09:41	2018-11-01 09:41	12	Srª da Hora	2	Operador01
52602213	5813	120	Erro de comunicação (Moedas)	Moedas	2018-10-31 17:12	2018-11-01 00:00	2018-11-01 14:58	2018-11-01 14:58	58	João de Deus	2	Operador01
52602681	24411	130	Falha de comunicação	Notas	2018-10-31 18:13	2018-11-01 00:00	2018-11-01 00:17	2018-11-01 00:17	244	Rio Tinto	2	Operador01
52602737	6111	120	Erro de comunicação (Moedas)	Moedas	2018-10-31 18:14	2018-11-01 00:00	2018-11-01 05:59	2018-11-01 05:59	61	24 de Agosto	2	Operador01
52603312	25015	131	Cofre de notas não está presente	Cofre de notas	2018-10-31 18:59	2018-11-01 00:00	2018-11-01 04:33	2018-11-01 04:33	250	Santo Ovídio	2	Operador01
52603619	5813	131	Cofre de notas não está presente	Cofre de notas	2018-10-31 19:23	2018-11-01 00:00	2018-11-01 16:28	2018-11-01 16:28	58	João de Deus	2	Operador01
52603626	5813	160	Dispensador de cartões encravado	Dispensador	2018-10-31 19:23	2018-11-01 00:00	2018-11-01 14:59	2018-11-01 14:59	58	João de Deus	2	Operador01
52603657	5813	140	Não há comunicação com o módulo OEM	OEM/SIBS	2018-10-31 19:27	2018-11-01 00:00	2018-11-01 14:55	2018-11-01 14:55	58	João de Deus	2	Operador01
52604256	1713	122	Erro na abertura do shutter	Moedas	2018-10-31 20:31	2018-11-01 00:00	2018-11-01 04:21	2018-11-01 04:21	17	Casa da Música	2	Operador01
52604416	1611	161	Dispensador de cartões vazio	Dispensador	2018-10-31 20:52	2018-11-01 00:00	2018-11-01 00:02	2018-11-01 00:02	16	Francos	2	Operador01
52604498	3412	130	Falha de comunicação	Notas	2018-10-31 21:04	2018-11-01 00:00	2018-11-01 03:20	2018-11-01 03:20	34	Fonte do Cuco - Linha P	2	Operador01
52604784	5412	140	Não há comunicação com o módulo OEM	OEM/SIBS	2018-10-31 21:36	2018-11-01 00:00	2018-11-01 08:45	2018-11-01 08:45	54	Aliados	2	Operador01
52605093	24412	140	Não há comunicação com o módulo OEM	OEM/SIBS	2018-10-31 22:19	2018-11-01 00:00	2018-11-01 03:38	2018-11-01 03:38	244	Rio Tinto	2	Operador01
52605136	5011	171	Sem papel	Impressora de recibos	2018-10-31 22:22	2018-11-01 00:00	2018-11-01 00:11	2018-11-01 00:11	50	Salgueiros	2	Operador01
52605250	2611	140	Não há comunicação com o módulo OEM	OEM/SIBS	2018-10-31 22:41	2018-11-01 00:00	2018-11-01 03:06	2018-11-01 03:06	26	Modivas Centro	2	Operador01
52605265	24612	120	Erro de comunicação (Moedas)	Moedas	2018-10-31 22:44	2018-11-01 00:00	2018-11-01 03:48	2018-11-01 03:48	246	Baguim	2	Operador01
52605469	312	130	Falha de comunicação	Notas	2018-10-31 23:13	2018-11-01 00:00	2018-11-01 10:42	2018-11-01 10:42	3	Brito Capelo	2	Operador01
52605655	6816	170	Erro de comunicação (Impressora de recibos)	Impressora de recibos	2018-10-31 23:37	2018-11-01 00:00	2018-11-01 08:54	2018-11-01 08:54	64	Estádio do Dragão	2	Operador01
52605794	812	134	Notas encravadas no mecanismo	Notas	2018-10-31 23:51	2018-11-01 00:00	2018-11-01 11:04	2018-11-01 11:04	8	H. Pedro Hispano	2	Operador01
52605983	5011	140	Não há comunicação com o módulo OEM	OEM/SIBS	2018-10-31 23:58	2018-11-01 00:00	2018-11-01 00:11	2018-11-01 00:11	50	Salgueiros	2	Operador01

A introdução de uma camada de controlo, proposta na 1ª iteração, resulta da necessidade de gerar, guardar, enviar e receber os ficheiros *log*, de e para diversas Entidades (dependendo da maior ou menor divisão das prestações de manutenção) ou aplicações de cálculo ou de análise preditiva e preventiva, que procura garantir a confiança nos dados e melhorar o funcionamento global do sistema de bilhética.

O ambiente de testes foi criado utilizando o Oracle VM Virtual Box versão 5.2.26, onde se criaram os nós com o sistema operativo Ubuntu Server 16.04.6 (BC01, BC02 e BC03) [65], instalando as ferramentas *gpg* e *ipfs*.

As provas de conceito realizadas a seguir permitiram gerar as chaves e os mecanismos de cifragem, fornecendo os dados necessários para os nós da rede *blockchain*, para o acesso aos ficheiros *log* e à forma de decifragem dos ficheiros *logs* autênticos.

Os comandos seguintes permitiram gerar o par de chaves, a chave privada que se deve manter em segurança e a chave pública que se pode partilhar com outros utilizadores a quem se pode confiar o acesso.

No nó BC01:

- *BC01>gpg --gen-key (RSA 2048, com o utilizador: dwbctest01, email: dwbctest01@gmail.com)*

[65] https://itsfoss.com/install-linux-in-virtualbox/, atualizado e acedido em 28-08-2019

Para exportar a chave pública de dwbctest01:

- *BC01>gpg --export --armor dwbctest> dwbctest01PublicKey.asc*

Para importar nos outros nós (BC02 e BC03) com outros utilizadores (dwbctest02 e dwbctest03) a chave pública:

No nó BC02:

- *BC02>gpg --import dwbctest01PublicKey.asc*
- *BC02>gpg --list-keys*

No nó BC03:

- *BC03>gpg --import dwbctest01PublicKey.asc*
- *BC03>gpg --list-keys*

Para cifrar o ficheiro *log*:

- *BC01>gpg --encrypt - dwbctest02 DWBC_BI_20181203111116_20181101_20181130.csv*

Para enviar o ficheiro *log* para o IPFS:

- *BC01>ipfs add DWBC_BI_20181203111116_20181101_20181130.csv.gpg*

A expressão Qm ...1 é o *hash* do ficheiro *log* original.

Os utilizadores dwbctest02 e dwbctest02 obtêm o ficheiro através dos comandos: seguintes:

No nó BC02:

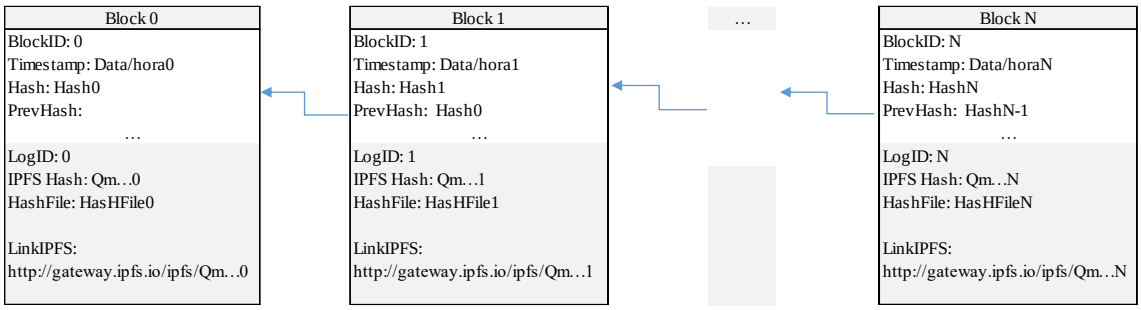
- *BC02>ipfs get Qm…1*
- *BC02> gpg --decrypt Qm…1 > DWBC_BI_20181203111116_20181101_20181130.csv*

No nó BC03:

- *BC03>ipfs get Qm…1*
- *BC02> gpg --decrypt Qm…1 > DWBC_BI_20181203111116_20181101_20181130.csv*

A Figura III.9 apresenta a forma como o *blockchain* associado ao IPFS apenas armazena o *hash* do ficheiro IPFS (e/ou o seu link), mantendo os dados exigidos no *blockchain* na sua forma mais simples, com as propriedades *peer-to-peer* distribuídas do IPFS.

Figura III.9 - *Blockchain* de controlo dos *Logs*



Os campos IPFSHash (SHA256), HashFile (se necessário um *hash* mais forte como o SHA512) e LinkIPFS, adicionados à estrutura base do bloco, permite que o *blockchain* distribuído pelos diversos nós da rede privada de *blockchain* contenha a informação necessária e suficiente para garantir a autenticidade dos ficheiros *log*, a possibilidade de verificação da sua integridade e da sua sequência, e através do acesso à chave publica nos outros nós (BC01, BC02 e BC03) para a possibilidade de decifrar.

A implementação desta rede privada de *blockchain* é baseada em 3 nós e suportados na plataforma Ethereum conforme os procedimentos [66],[67],[68],[69] e [70] adaptados.

A configuração conjunta do IPFS e do Ethereum pode ser realizada através do Infura conforme procedimentos [71] adaptados, em que os ficheiros *logs* podem ser armazenados no IPFS e o *hash* do ficheiro *log* pode ser armazenado no Ethereum, através do uso das API´s para aceder à rede Ethereum e ao IPFS.

Também foi possível realizar os testes da 1ª iteração para os *logs* gerados pelo sistema de gestão de tráfego, através dos ficheiros de *log* gerados (TT_*LOG* - 2018-12-02-0520.csv e Event_*LOG* - 19010100.csv), referentes às passagens dos veículos nas balizas fixas ao longo de toda a via, verificando-se assim a possibilidade de se garantir a autenticidade e integridade dos dados, através de uma camada de confiança.

---

[66] Install Geth - https://geth.ethereum.org/install-and-build/Installing-Geth, acedido em 28-05-2019
[67] Private Network - https://github.com/ethereum/go-ethereum/wiki/Private-network, acedido em 28-05-2019
[68] Private Network - https://medium.com/@yashwanthvenati/setup-private-ethereum-blockchain-network-with-multiple-nodes-in-5-mins-708ab89b1966, acedido em 15-06-2019
[69] Ethereum - https://medium.com/cybermiles/running-a-quick-ethereum-private-network-for-experimentation-and-testing-6b1c23605bce, a acedido em 03-08-2019
[70] Example Ethereum Privado - https://medium.com/coinmonks/private-ethereum-by-example-b77063bb634f, acedido em 24-08-2019
[71] Example Infura - https://www.freecodecamp.org/news/hands-on-get-started-with-infura-and-ipfs-on-ethereum-b63635142af0/, acedido em 04-09-2019

Este teste confirma a viabilidade desta solução para sistemas ou aplicações que gerem ficheiros *logs* com os eventos de alarmística ou monitorização.

2.6.2. 2ª Iteração na metodologia proposta

A avaliação da 1ª iteração permitiu verificar que os registos poderiam ser manipulados na geração do ficheiro *log* ou na inserção na base de dados.

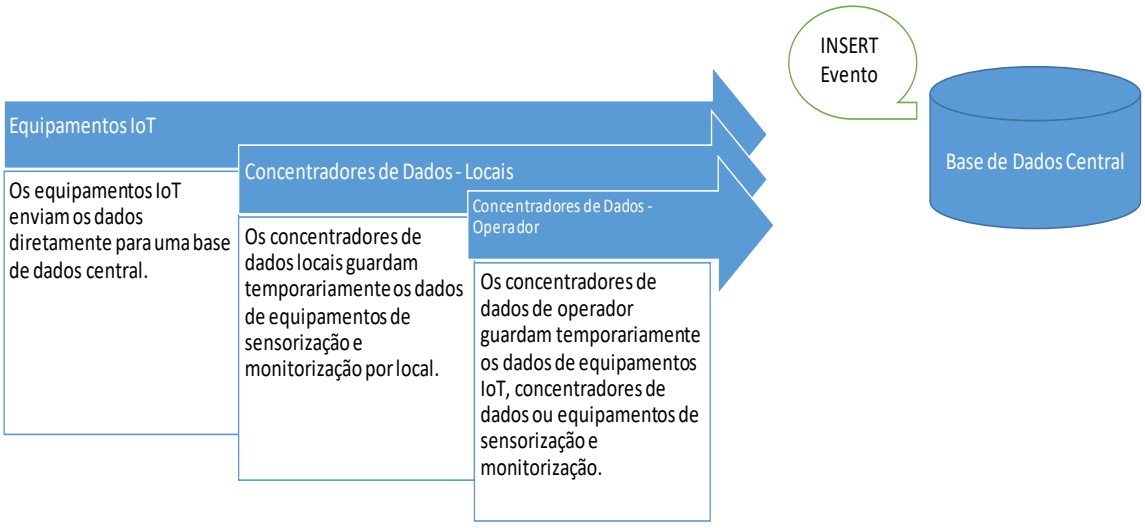
A solução proposta nesta 2ª iteração da metodologia permite melhorar a integridade dos dados, mantendo o fluxo de dados já demonstrado na primeira iteração ao garantir que os dados no momento de registo na base de dados não podem ser manipulados, através de registos seguros, registo a registo, pelo respetivo *hash* evitando ataques internos.

A segurança dos registos de dados, na 2ª iteração, pretende garantir no momento do registo do evento que os registos ficam disponíveis nos nós aceites desta rede privada de entidades distintas sem possibilidade de adulteração.

Este artefacto foca-se em evitar tentativas de intrusão ou manipulação que possam comprometer a inserção do registo e condicionar a geração do ficheiro *log* ou o acesso aos ficheiros *logs* (1ª iteração) evitando falsificar o registo completo, truncar o *log*, inventar novos registos e injetar entradas de registos no passado.

A Figura III.10 mostra qual o objeto previsto para a 2ª iteração e que respeita à fase de inserção de eventos na base de dados a partir dos equipamentos *IoT*, dos concentradores de dados locais e de operador. A inserção de eventos, apresentada a seguir, consolida os diversos fluxos de dados tendo em consideração os diversos *endpoints*.

Figura III.10 - Fase do Fluxo de Dados de Inserção na Base de Dados



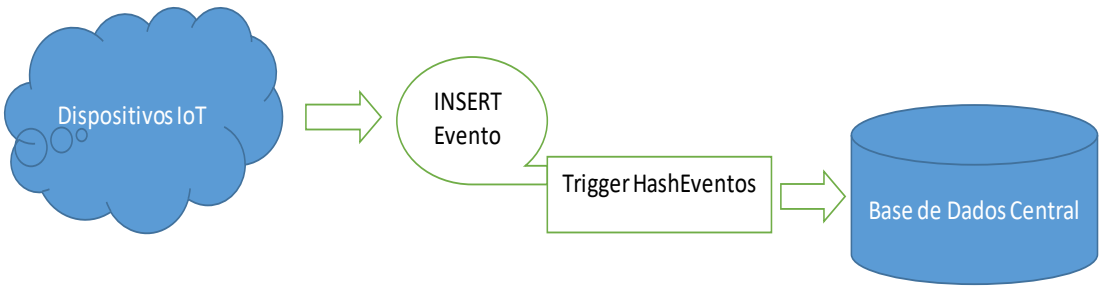
Esta fase utiliza os dados, sem tratamento, dos equipamentos e sistemas e que são integrados numa ou em várias bases de dados. Os mecanismos de comunicação podem utilizar os mecanismos de publicação e subscrição com troca de mensagens através do protocolo MQTT ou com o envio de ficheiros *xml* com estruturas e formatos pré-definidos.

As provas de conceito desenvolvidas não se concentraram na fase do fluxo de dados dos dispositivos *IoT* até à base de dados e na forma com se consegue que todos os eventos sejam sujeitos a mecanismos de verificação prévia da autenticidade dos equipamentos, aos quais se adicionariam campos de controlo.

O artefacto inicia-se na fase do processo de inserção na base de dados, dos dados com origem em equipamentos *IoT*, que a partir dai cria os blocos que contêm os dados de controlo de conjuntos de registos, utilizando a rede *blockchain* privada e as árvores de Merkel para os agrupar através de *hash* combinados.

A validação conjunta de registos permite desta forma criar uma rede de controlo sobre conjuntos de registos de eventos, otimizando os mecanismos de validação e consenso. A Figura III.11 apresenta este fluxo e a implementação de um *trigger* que adiciona a chave *hash* dos eventos a inserir na base de dados.

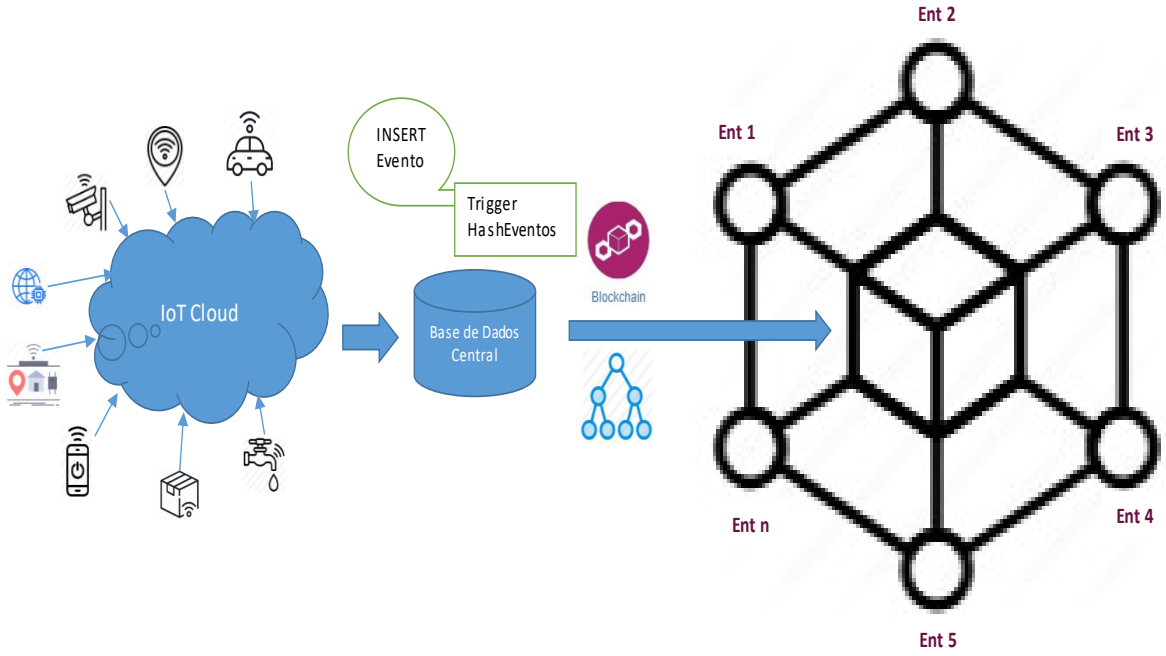
Figura III.11 - Inserção com geração de *Hash* por registo



A fase de inserção ainda se mantém concentrada num ponto central para facilitar a prova de conceito. Neste cenário optou-se por inclui um *trigger*, referido na figura anterior, que cria os dados de controlo (*hash* do registo) que servirão de base à rede *blockchain*. A utilização da árvore de Merkel permite validar grupos de registos melhorando a performance da solução. A rede *blockchain*, neste cenário, constitui-se como uma rede de controlo que valida a confiança dos dados. Tal como na 1ª iteração da metodologia a rede de *blockchain* serve principalmente para distribuir os dados de controlo e de acesso aos dados dos eventos, constituindo-se como uma camada de confiança.

Este cenário, mais detalhado no ponto 2.6.2.1 com a Operacionalização da 2ª Iteração, é apresentado na Figura III.12 onde ainda se mantém a limitação, dos dados dos eventos residirem em bases de dados centrais, que contêm os dados acedidos através dos dados de controlo dos registos de eventos, na rede *blockchain*.

Figura III.12 - Cenário de demonstração do artefacto (2ª iteração)



Esta iteração testou e validou o controlo do fluxo de dados ao nível do registo, para o tipo de aplicação *blockchain* (BC3-Controlo de fluxo de dados) prevista no modelo.

Não foi possível testar e avaliar os outros tipos de aplicação de *blockchain* (BC4-Aceitação de dispositivos, BC5-Controlo de versões e BC6-Segurança dos sistemas) previstos no modelo, para garantir a autenticidade do equipamento, a correta versão instalada e a segurança do sistema. Os equipamentos da rede de bilhética testados não permitem essa implementação, dado que não têm a funcionalidade de gestão de chaves privadas e publicas ou de certificação para a garantia da integridade dos dados e o armazenamento é limitado para guardar os dados dos nós da rede *blockchain* associado a cada equipamento e em situações de *offline*.

2.6.2.1. Operacionalização da 2ª Iteração

A 2ª Iteração implicou o acesso ao modelo de dados e a alteração da estrutura de dados do sistema ou da aplicação, sendo por isso intrusivo sobre os sistemas existentes.

Nesta simulação adicionou-se o *trigger* seguinte que na fase de inserção de registos na base de dados adiciona um campo de controlo *HashEvento* que permite garantir a integridade dos dados de cada registo e é o valor que é inserido no bloco para constituir o *blockchain* de controlo sobre os registos de eventos.

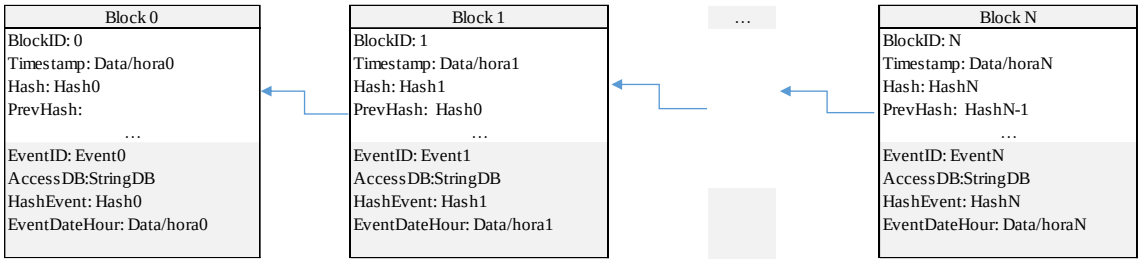
```
CREATE TRIGGER dbo.HashEventos
ON Eventos
INSTEAD OF INSERT
AS
BEGIN
  SET NOCOUNT ON;

  INSERT dbo.Eventos (campo 1, campo 2, ..-, campo n, HashEvento)
    SELECT campo 1, campo 2, ..., campo n,
              HASHBYTES('SHA2_256', CONCAT([campo 1],'|',[campo 2],'|', …,'|',[campo n]))
    FROM inserted;
END
```

Os campos 1 a n são, pelo menos, os referidos na Tabela III.10 - Campos exportados para o ficheiro *Log*.

A estrutura de dados simplificada do *blockchain* é descrita na figura seguinte:

Figura III.13 - Estrutura Dados simplificada de Blocos na 2ª Iteração



O *blockchain* nesta versão tem um bloco por cada registo, com campos que permitem o acesso aos dados EventID, AccessDB, e os campos de controlo *Hash*Event (campo de controlo do registo) e EventDateHour (data/hora do evento).

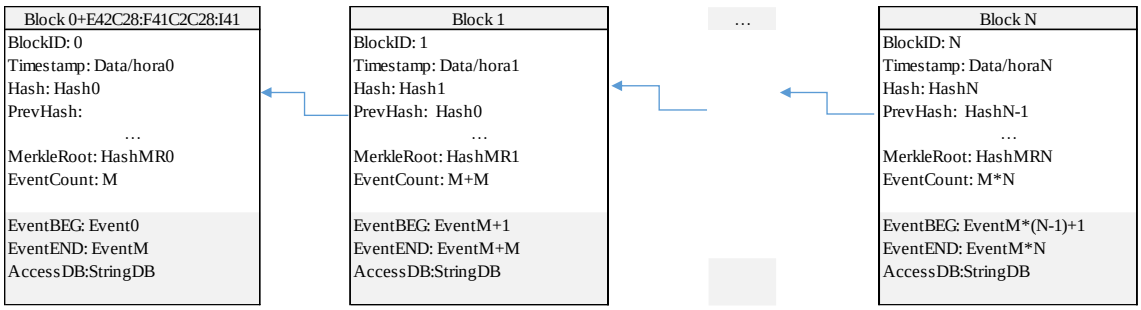
A quantidade de registos previsíveis num sistema de bilhética, multioperador e com milhares de dispositivos a enviar eventos dos inúmeros sinais, implicará a procura de soluções que permitam validar grandes quantidades de registos/transações.

O mecanismo que se propõe baseia-se nas árvores de Merkel em que cada *hash* do registo serve como entrada para a árvore de Merkle que conjuntamente com outros registos vai recalculando de forma recursiva o valor da MerkleRoot.

O valor MerkleRoot vai sendo inserido num único bloco para permitir que sejam validados os dados de forma massiva. O processo começa com a inserção do *hash* de cada registo num bloco separado que é somado com o registo seguinte, resultando num único bloco, até se obter um único bloco como saída.

A Figura III.14 apresenta a estrutura de dados com árvore Merkel e a forma como os blocos se relacionam.

Figura III.14 - Estrutura de dados com árvore Merkel



As árvores Merkle validam um conjunto de transações. Os N registos de dados são combinados numa árvore Merkle. Para verificar se um determinado elemento está incluído na árvore são necessários um máximo de 2 * *log*2 (N) de cálculos. Este algoritmo permite uma forma eficiente de verificar se uma transação está num bloco ou associada a um bloco.

A rede *blockchain* de testes manteve-se com três nós e desenvolveu-se adicionando à estrutura de dados base de *blockchain* o *hash* resultado da raiz árvore de Merkle que permite também validar os conjuntos de registos de dados.

Esta prova de conceito trata um bloco de eventos, através de um algoritmo para gerar um *hash*, que verifica a validade do conjunto de dados tendo por base os eventos originais. A função *hash* não é executada de uma única vez para o conjunto de eventos, mas resulta do *hash* de cada evento sendo depois reunidos num *hash* resultado da implementação da árvore de Merkle.

A estrutura parece-se com uma árvore, em que os nós de base contêm N eventos. Cada par de *hash* combina-se a partir da linha inferior, através de *hash* intermédios até ao *hash* no topo, que permite validar todo esse conjunto de registos.

2.7. Avaliação (5ª Etapa metodologia DSRM)

A avaliação decorre da demonstração das provas de conceito passo a passo e da verificação que os *logs* obtidos e transmitidos que se revelam imunes à adulteração ou à manipulação e que se garante a sua entrega exclusivamente aos destinatários autorizados (1ª Iteração). Os dados do *link* do ficheiro na rede IPFS e o respetivo *hash* foram inseridos na rede *blockchain,* constituindo-se uma camada de controlo sobre os dados de acesso aos ficheiros *log* garantindo a confiança dos dados e da sua integridade.

Na prova de conceito, da 2ª iteração, os dados dos eventos transmitidos por cada equipamento, em tempo real, em *off-line* ou em blocos, possibilitaram inserir os registos dos eventos, com mecanismos de autenticidade e controlo sobre os campos dos registos de dados.

Os dados de controlo permitiram o acesso aos dados e garantiram a integridade dos dados contidos nos registos validados por funções *hash* e que foram inseridos na rede *blockchain* para constituir a camada de controlo sobre os dados registados.

Este processo de avaliação começou por rever e comparar entre os sistemas desenhados sem esta preocupação de segurança e estes que decorrem da sua conceção suportados nos mecanismos baseados na tecnologia *blockchain*.

Os artefactos desenvolvidos separaram os dados dos eventos, dos dados de controlo para controlar o fluxo de dados, garantindo que os *logs* enviados para a rede IPFS ou os registos contidos nas bases de dados sejam validados pelos dados de controlo residentes na rede *blockchain*.

Esta avaliação da componente de monitorização e alarmística do sistema de bilhética, em duas iterações permitiu verificar que os artefactos previstos de prova de conceito podem garantir a segurança dos dados e o controlo do fluxo de dados.

O processo iterativo previsto na metodologia permitiu melhorar o controlo do fluxo de dados e pode ser extensivamente adaptado para melhorar a forma como podemos garantir a confiança no bom funcionamento do sistema, criando uma camada de controlo do fluxo de dados suportada em tecnologia *blockchain*, uma camada de confiança.

As limitações mais relevantes passam por se ter avaliado as componentes de alarmística e não as operações ou transações. Também foi avaliado uma parte do fluxo de dados entre os 5 níveis definidos no modelo.

Num contexto mais amplo, o modelo pode ver alargada a sua aplicação a outros *smart places*, a arquiteturas e aplicações, como um modelo que se aplica ao desenvolvimento de sistemas semelhantes.

2.8. Comunicação (6ª Etapa DSRM)

O processo de comunicação baseou-se na escrita de manuscritos sobre três aspetos essenciais para a elaboração deste trabalho consubstanciado nesta tese, a revisão sistemática da literatura, o modelo genérico de dados confiável de uma *smart city* e os mercados de dados. Para o efeito e no decurso do trabalho de pesquisa e investigação elaboramos três manuscritos que foram apresentados nas conferências da *World Conference on Information Systems and Technologies* (WordCIST) de 2018 e 2019 e *International Conference on Software Process Improvement* (CIMPS) de 2018, respetivamente com os títulos "Revisão Sistemática da Literatura, Pesquisa em Tecnologia *blockchain* como Suporte ao Modelo de Confiança Proposto Aplicado a *Smart Places*", publicado em 28 de março de 2018, "Mercado de Dados (Marketplace) confiáveis", publicado em 27 de março de 2019 e "Um modelo de *smart city* seguro por *blockchain*", publicado em 27 de setembro de 2018 (Brandão et al., 2018b, 2018a, 2018a). Estes manuscritos encontram-se referenciados no ponto específicos de Publicações no final da tese.

A contribuição deste trabalho de investigação revela-se na viabilidade do modelo genérico de dados proposto, suportado em tecnologia *blockchain* e aplicado a uma *smart city*. As provas de conceito desenvolvidas orientaram-se para validar o modelo, com a utilização da tecnologia *blockchain*, principalmente no controlo do fluxo de dados, na autenticidade dos dados (*logs* e registos) e na integridade dos dados, através de uma camada de controlo, a camada de confiança.

2.9. Resultados Práticos

Os ficheiros só podem ser acedidos pelo nome ou chave e o respetivo caminho. A escolha do IPFS (*Inter-Planetary File System*) permite a redundância dos dados, a transparência (segurança e autenticidade) e a descentralização que facilita o armazenamento de grandes quantidades de dados, evitando a limitação da utilização exclusiva do *blockchain*, em que a quantidade de dados ainda é um aspeto critico.

A gravação de *logs* do sistema ou da aplicação fornece, em modo assíncrono, a possibilidade de analisar e avaliar os eventos que ocorreram e que foram objeto de uma prévia configuração dos itens de auditoria a registar.

O uso consolidado de ficheiros *logs* (de vários sistemas ou equipamentos) permite a ferramentas como os sistemas de gestão e correlação de eventos de segurança (*SIEM-Security Information and Event Management*), com recursos robustos e com aprendizagem automática para a deteção de incidentes, a sua correlação e alerta. Também permite obter análises preditivas, notificar, diagnosticar, enviar alarmes e detetar anomalias, para a resposta do problema, evitando afetar os sistemas em exploração ou reduzir o tempo de inatividade de equipamentos críticos.

A autenticidade e a integridade dos dados são um aspeto critico e que pode condicionar as respostas e os automatismos que possam ser desencadeados, vários deles sem intervenção humana. Desta forma a garantia na confiança dos dados é muito critica para evitar manipulações, acessos indevidos aos *logs* gerados e que servem de base a várias análises e a informação de tomada de decisão muitas vezes automatizada.

Adicionalmente à escolha do sistema de ficheiros distribuído IPFS (suportado em *blockchain*) utilizou-se a tecnologia de *blockchain* para permitir controlar o fluxo de dados dos ficheiros *log* de forma distribuída, criptograficamente protegido e verificando a correção dos dados, a verificação do *log* através do bloco no *blockchain* que comprova a exatidão dos *logs*.

Para a segurança criptografia utilizamos a criptografia assimétrica através da ferramenta GPG (*GNU Privacy Guard)* que permite implementar os mecanismos de chaves (privadas e públicas), descrita no ponto 2.6.1.1.

O *blockchain,* na 1ª iteração, serve como apontador para o IPFS e para verificação do respetivo *hash*. O *hash* gerado ao adicionar o ficheiro à rede IPFS pode servir de *hash* que garante a integridade do *log* gerado, podendo, no entanto, ser adicionado o *hash* mais robusto (SHA512) que servirá de validação do respetivo bloco e permitirá:

- Obter o acesso do *log* na rede IPFS;
- E a decifragem dos ficheiros confidenciais armazenados em IPFS protegidos por chaves privadas e públicas usando GPG.

A função *hash* criptográfica tem as seguintes caraterísticas: não pode gerar o mesmo valor de *hash* para entradas diferentes; os mesmos dados geram o mesmo valor de *hash*; gera

rapidamente um *hash* para qualquer conjunto de dados; não se consegue calcular a entrada com base no valor de *hash*; e qualquer alteração nos dados de entrada altera o *hash*.

O *blockchain* neste contexto serve de camada de controlo para permitir garantir a confiança nos dados contidos nos *logs* disponíveis na rede IPFS e a sua decifragem por utilização segura entre nós da rede *blockchain*.

Neste contexto foram também simulados os *logs* do sistema de gestão de trafego (TT_Logs e Event_Logs) que são gerados automaticamente pelo sistema proprietário (TMS) e resultaram da mesma forma como controlo do fluxo de dados.

Esta abordagem verificou-se pouco intrusiva nos sistemas existentes e permitiu garantir a autenticidade dos *logs* em qualquer nó da rede e a integridade dos dados contidos nos *logs*.

A 2ª iteração adicionou uma camada de controlo implementada através da rede *blockchain* para validar os registos inseridos nas bases de dados e com eles garantir a integridade dos dados logo na chegada dos eventos, pelos diversos equipamentos, ao nível do registo.

Este artefacto conduz a um nível de confiança superior o que torna os registos inseridos invioláveis e com a utilização das árvores de Merkel otimiza a validação de blocos de registos melhorando a performance do sistema de validação dos registos.

A integração de *big data* com a tecnologia *blockchain* poderá permitir também responder e gerir a maioria das principais questões e desafios que envolvem o *big data*, principalmente na confiança nos dados que o suportam.

A tecnologia *blockchain* tem a expectativa de dar uma maior confiança na integridade dos dados, de entradas imutáveis, *timestamp,* aceitação baseada no consenso, rastreios de auditoria, e garantia sobre a origem dos dados. Estas são as áreas que poderão tornar a tecnologia *blockchain* central. Para além da integridade dos dados, a camada de dados partilhada que a tecnologia *blockchain* poderá introduzir cria um conjunto inteiramente novo de possibilidades, de capacidades e de conhecimentos para atuação da Inteligência Artificial. (Rabah, 2018)

3. Discussão dos Resultados

Analisando os resultados dos testes realizados na simulação das duas iterações é possível discutir o potencial da solução desenvolvida.

Nesta análise demonstra-se que este tipo de abordagem permite detetar adulterações nos *logs*, garantir a autenticidade dos *logs* e garantir que os registos inseridos nas bases de dados não são objeto de manipulação, reduzido as falhas por omissão ou manipulação dos dados dos registos e dos *logs* gerados.

A 1ª iteração verificou através das provas de conceito implementadas que se consegue criar uma camada de confiança através da rede *blockchain*, permitindo que os dados contidos nos *logs* se encontrem disponíveis e acessíveis na rede IPFS em qualquer nó da rede de confiança.

Estas provas de conceito também demonstram que um sistema desenvolvido e que utilize ficheiros *logs* como base para análise ou avaliações, utilizando várias aplicações ou diversas entidades, produz dados de confiança, suportado em *logs* autênticos e que se encontram disponíveis para detetar os eventos que constituíam a base para o cálculo de indisponibilidades, de erros ou problemas que permitam análises preditivas ou de desvios de padrões ou intervalos de confiança para a adequada execução dos processos e dos principais grupos de funções descritos na Figura III.15, em ambiente IoT.

Figura III.15 - Principais Grupos de Dados/Funções

A Figura III.15 revela assim as principias funções em ambiente IoT que podem ser usadas pelos diversos conjuntos de dados e que necessitam de confiar nos dados, através de uma camada de confiança suportada em *blockchain* e que são fornecidos para apresentarem a informação correta e que permita uma análise objetiva, uma gestão adequada e um correto funcionamento do mercado e a satisfação dos clientes.

Desta 1ª iteração podemos afirmar que este processo de controlo baseado em *blockchain* e IPFS pode ser utilizado em sistemas ou aplicações que gerem *logs* que serão utilizados por outras aplicações e/ou por outras entidades. A 2ª iteração adiciona este controlo para o nível do registo, aumentando a segurança dos dados.

Além das 2ª iterações realizadas no âmbito deste trabalho de investigação podemos verificar que este modelo se poderá vir a alargar às fases anteriores, dos equipamentos *IoT* diretamente para a rede *blockchain*, resolvidas as limitações dos dispositivos de sensorização e equipamentos IoT ainda em operação, verificadas ao nível dos recursos

nomeadamente processamento, transmissão, armazenamento e funcionalidades dos equipamentos IoT.

De notar que o modelo proposto foi testado nas componentes de eventos e não nas componentes transacionais que envolvam monetização.

A abordagem proposta estabelece a separação da camada de dados, da camada de controlo, sendo que esta se efetiva através da tecnologia *blockchain* adotando os campos necessários para definir os caminhos de acesso aos dados e as verificações da integridade dos dados.

Os campos vão sendo adotados conforme se analisa o fluxo de dados que se quer controlar (ver campos adotados na 1ª iteração e na 2ª iteração, no ponto 2.6.1.1 e no ponto 2.6.2.1).

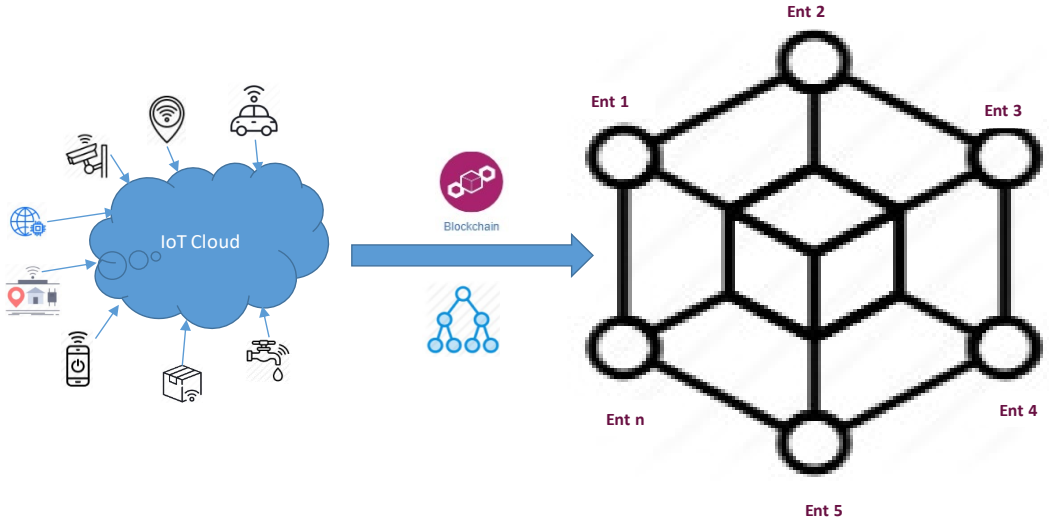
Esta camada de controlo a que chamamos camada de confiança fornece aos nós da rede privada de *blockchain*, os dados para o acesso e para a verificação da integridade dos dados.

O modelo proposto no ponto 2.2 (Modelo Genérico de Dados), do Capitulo II baseia a sua conceção nas trocas de dados principalmente através da interoperabilidade de dados entre os ecossistemas. A gestão de dados e o controlo de fluxo de dados necessita de uma camada de confiança para permitir que os dados sejam únicos e de confiança, fornecendo à *smart city* a dinâmica harmoniosa entre os seus ecossistemas, a automatização dos processos e a possibilidade de estabelecer algoritmos de inteligência artificial e análise de *big data* para promover, de forma incremental e bem testada, novas formas de tomada de decisão.

As características dos dados de controlo devem ser analisadas e estruturadas por forma a permitir que o fluxo de dados seja consistente e suficientemente granular em cada nível para se poder segmentar os dados partilhados com as proteções e as permissões adequadas.

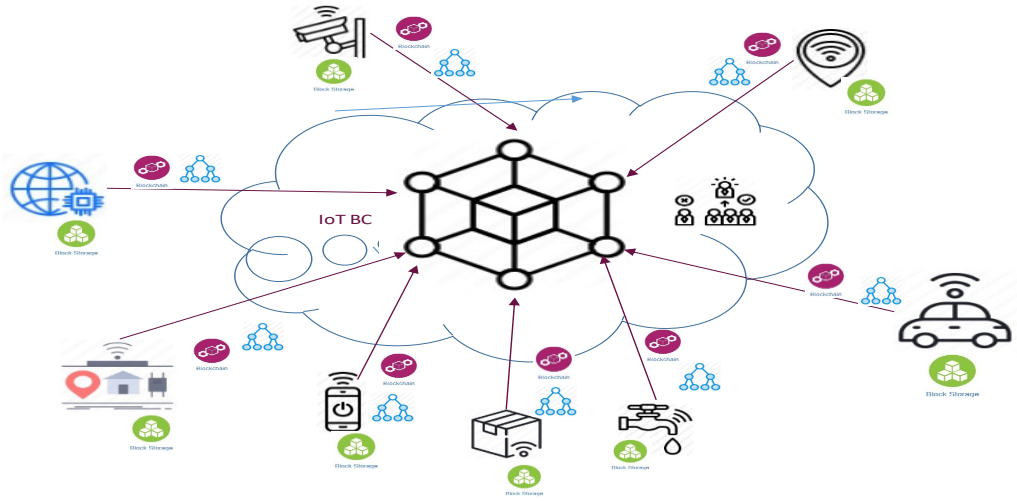
A Figura III.16 apresenta uma visão global da solução em que a rede IoT baseada em nuvem e em plataformas IoT seria controlada por uma rede *blockchain* e com ela estabelecer uma rede de controlo ou de confiança para gerir o fluxo de dados e garantir a confiança dos dados através da implementação dos tipos de aplicações de *blockchain* (da Tabela III.8) definidos no ponto 2.2, do Capitulo III, que passam pelos 6 tipos definidos: Transações seguras, Segurança dos dados, Controlo do fluxo de dados, Aceitação de dispositivos, Controlo de versões e Segurança dos sistemas.

Figura III.16 - Fluxo de Dados considerando uma rede *IoT* e uma rede *Blockchain*



A Figura III.17 apresenta o cenário objetivo em que a rede *blockchain* se integra com a rede *IoT* sendo que neste cenário as camadas de controlo e de dados *IoT* se juntam e são suportadas na rede *blockchain*. Este cenário poderá ter mecanismos de simplificação ou agrupamento que facilitem o processamento, o consenso, o armazenamento e a transmissão, conforme por exemplo a proposta de Chen, Wang, e Wang (2018).

Figura III.17 - Fluxo de Dados Integrando o *IoT* com *Blockchain*



Este cenário como vimos ainda apresenta várias limitações com a dificuldade de obter o armazenamento e a computação para tratar grandes quantidades de dados numa rede *blockchain.* Tendo constituído, nesta investigação, a principal razão por se ter adotado a tecnologia *blockchain* como camada de confiança ou de controlo, podendo no futuro incluir a camada de dados.

3.1. Trabalhos relacionados

Para os sistemas de comando e controlo utilizando protocolos de computação distribuída, foi desenvolvida uma prova de conceito usando IPFS e IPNS que permite obter comunicações mais seguras e anónimas. (de Aquino et al., 2018)

Cucurull & Puiggalí (2016) apresentaram uma solução de implementação usando a tecnologia *blockchain* com a estrutura base do *bitcoin* para aumentar a segurança dos *logs* imutáveis. O mecanismo de consenso PoW que suporta o projeto de *blockchain*, tendo por base a estrutura utilizada na rede bitcoin, que não pode ser modificado pela intervenção de menos de 50% da capacidade de mineração dos nós que validam.

Ali, Dolui, & Antonelli (2017) apresentam uma *stack* de software de *blockchain* e o sistema de ficheiros interplanetário (IPFS) *peer-to-peer* para controlar o acesso descentralizado e o *blockchain* para criar um *legder* de operações dos dados *IoT*, com várias limitações nomeadamente a dificuldade em manter um fluxo de dados através de IPFS e explorar sem *blockchain* para aumentar do tempo de processamento de blocos e economia de armazenamento nos nós validadores.

O projeto e a implementação apresentado por Hasan, Sultan, & Barbhuiya (2019) fornece uma solução descentralizada sem o controlo de preço do fornecedor de armazenamento em nuvem (*CSSP-Cloud Storage Provider)* para fornecer um serviço de armazenamento em nuvem baseados em *blockchain* e IPFS, para a validação de dados.

A arquitetura do IPFS foi melhorada (Y. Chen et al., 2017) para permitir mais rendimento dos utilizadores individuas e dos fornecedores de conteúdos, para que as informações do IPFS de cada nó possam ser salvas no blockchain e para tal combina neste esquema três formas de replicação e de armazenamento.

Zheng, Li, Chen, & Dong (2018) projetam um modelo de armazenamento baseado em IPFS para *blockchain* para vários tipos de transação, procurando melhorar o espaço de armazenamento, a segurança e a sincronização de nós.

A revisão de um mecanismo global para proteger as camadas de *IoT*, tendo em consideração a diversidade de recursos em *IoT*, foi apresentada por Khan & Salah (2018), em que a segurança de *IoT* foi analisada e categorizaram os problemas de acordo com as das camadas de *IoT* (alto nível, nível intermediário e baixo nível). Neste trabalho analisaram a utilização da tecnologia *blockchain* para alguns dos principais problemas de segurança da *IoT*. A aplicação da tecnologia *blockchain*, suportado em *smart contracts*,

permitirá a gestão, o controlo e a proteção de dispositivos *IoT*, usando s recursos intrínsecos do *blockchain* para a segurança do *IoT*, nomeadamente, espaço de endereçamento, identidade das coisas e sua governança, autenticação e integridade dos dados, autenticação, autorização e privacidade, e comunicações seguras.

Em síntese verifica-se que existem vários trabalhos que se apoiam na rede IPFS e utilizam a rede *blockchain* para resolver alguns dos problemas encontrados em termos de segurança, de autenticidade e de integridade dos dados, fortalecendo a contribuição deste trabalho no aprofundamento do conhecimento e na forma como os *smart places* se podem revelar mais confiáveis e com dados de confiança.

IV. CONSIDERAÇÕES FINAIS

IV. CONSIDERAÇÕES FINAIS

Os *smart places* e, neste caso específico, as *smart cities*, suportam o seu funcionamento num conjunto vasto de dados que monitorizam e atuam sobre os diversos ecossistemas.

A *smart city* é física, digital e virtual, enquandrando vários fatores que passam pela participação do cidadão, a participação dos agentes económicos e sociais, a governança, as políticas inovadoras, as infraestruturas tecnológicas, a sustentabilidade ecológica, energética, social e económica, e as políticas de mobilidade e de transportes, que convergem em estratégias dinâmicas e em novas abordagens.

As estratégias de participação e de interação, necessitam de robustas e resiliêntes infraestruturas de conectividade, que suportam a multiplicidade de equipamentos, de sensores e de atuadores, que geram enormes quantidades de dados, que são tratatos de forma automática para extrair informação relevante, para reorientar as estratégias, as políticas e a criação de ecossistemas potenciadores de novos modelos de negócio.

Neste contexto, a confiança nos dados assume um papel fundamental na segurança, na dinâmica e no funcionamento da *smart city*.

As redes de transportes, como infraestruturas críticas nos fluxos de pessoas e bens, são suportadas em diversos sistemas com graus diferentes de maturidade e de inovação. Os sistemas são principalmente sistemas *legacy* e com soluções proprietárias. As soluções encontradas têm de ter em consideração este cenário e a necessidade de cumprir processos morosos de testes e certificação.

A metodologia cientifica, DSRM (Peffers et al., 2007), adotada neste trabalho de investigação, revelou-se adequada e permitiu a dinâmica que serviu de base à exploração de artefactos que pudessem demonstrar e validar o modelo genérico de dados proposto.

A opção foi para um sistema transversal ao ecossistema de mobilidade e transportes como é o sistema de bilhética, na componente de alarmística e monitorização, e que não tivesse restrições no acesso ao seu modelo de dados e estrutura de dados, importante para a 2ª iteração. A abordagem seguida neste trabalho revelou-se pouco intrusiva nos sistemas e aplicações, adicionando uma camada de confiança.

O modelo proposto visou aumentar a proteção das infraestruturas, dos sistemas e aplicações, contra a adulteração dos dados e a omissão de eventos, reduzindo a possibilidade de acessos indevidos que alterem os dados inseridos.

Este trabalho permitiu, no âmbito das *smart cities,* em ambientes *IoT,* propor um modelo genérico de dados suportado em seis tipos de aplicação *blockchain* e que através dos artefactos baseados em provas de conceito se demonstrou a viabilidade de garantir a autenticidade dos ficheiros *log* e a sua integridade, e a integridade dos registos de eventos.

Ambas as iterações revelaram a possibilidade de se criar uma camada de confiança que permite garantir a integridade dos dados e a autenticidade da origem dos dados, com base na utilização da tecnologia *blockchain* e da rede IPFS suportada em *blockchain.*

Na introdução foram identificados o objetivo geral e três objetivos específicos. O trabalho de investigação permitiu atingir os objetivos, que procuramos nos parágrafos seguintes apresentar e responder com os contributos alcançados.

O objetivo geral do projeto passa por aplicar um modelo genérico de dados, a propor, de suporte ao conceito de *smart city*, por forma a sistematizar as suas ações e o controlo dos fluxos de dados e da qualidade dos dados, que permitam gerir os dados e a informação, de forma confiável e segura.

Em conclusão foi possível propor um modelo genérico de dados de suporte à *smart* city (ponto 2.2, do capitulo III) que sistematiza e permite gerir os dados e a informação, de forma confiável e segura. A avaliação da sua viabilidade resulta da validação dos artefactos confirmando o controlo do fluxo de dados no tratamento dos *logs* e na inserção de novos registos de dados.

Em síntese e de seguida definem-se os seguintes três objetivos específicos que se pretenderam atingir com a concretização do trabalho a desenvolver.

1. Estruturar um modelo de dados genérico de suporte ao conceito de *smart city* que conduza e permita o alinhamento da aplicação dos ecossistemas de dados com os ecossistemas naturais.

Este objetivo foi atingido na conceção do modelo de dados genérico, com a organização da *smart city* em ecossistemas que se relacionam e são "alimentados" por dados IoT, agrupados por domínios aplicacionais e que se suportam em 6 tipos de aplicações *blockchain*, para garantir a autenticidade e a integridade dos dados.

2. Estruturar as relações entre os ecossistemas, os participantes e os dados que facilite a utilização da tecnologia *blockchain* na gestão dos dados.

A criação de uma camada de confiança adaptada às diversas aplicações permite a gestão de dados, independente da estrutura de dados e da localização dos dados.

3. Assegurar mecanismos de confiabilidade na gestão dos dados e das fontes dos dados.

Os mecanismos de confiabilidade propostos revelam-se nos seis tipos de aplicação da tecnologia de *blockchain* que suportam o funcionamento da *smart city* e dos seus ecossistemas, fornecendo o conjunto de funcionalidades que permitem gerir e controlar os dados, a autenticidade das fontes dos dados e a origem dos equipamentos *IoT*.

1. Conclusões

Os *smart places* revelam espaços físicos, de dimensão variável e com Organizações que gerem esses espaços, que se desmaterializam em espaços digitais e virtuais, potenciando a participação do cidadão, otimizando a gestão dos recursos, melhorando a qualidade dos espaços e dos cidadãos, e fornecendo alavancas para a inovação, a inclusão social, a sustentabilidade ambiental, energética e económica.

A utilização massiva de equipamentos *IoT* e móveis, integrados em *Cloud* e de acesso através da Internet, suportados em robustas infraestruturas de conetividade, potencia a monitorização em tempo real, a avaliação dinâmica, os algoritmos de resposta e atuação, as comunicações *machine-to-machine*, a inteligência artificial, os algoritmos de *data mining*, o tratamento de *big data*, a *machine learning*, etc.

Esta realidade, que se densifica, conduz a novos problemas, com a quantidade de dados gerados e com a dificuldade em controlar os fluxos de dados, a qualidade de dados e a confiança na origem dos dados.

O problema em controlar os fluxos de dados, a qualidade de dados e a confiança na origem dos dados, nas *smart cities*, centra o trabalho de investigação que foi desenvolvido.

Em conclusão podemos verificar que os artefactos baseados em provas de conceito permitiram confirmar que a tecnologia *blockchain* pode constituir-se como uma camada de confiança sobre os dados e desta forma garantir a autenticidade dos dados e da integridade dos dados.

A 1ª iteração permitiu controlar o fluxo de ficheiros de dados, dos ficheiros de *log*, garantindo a autenticidade dos ficheiros e a integridade dos dados contidos nos ficheiros

e também permitiu o acesso controlado através do mecanismo de cifragem e decifragem, através de chaves privadas e públicas.

O objeto central do trabalho focou-se nas componentes de alarmística e monitorização dos sistemas, resultando em *logs* que extraem e guardam os eventos, onde se registam os problemas, os alarmes, os incidentes, a disponibilidade ou indisponibilidade dos equipamentos, dos serviços e dos componentes, as quebras de segurança, as tentativas de acesso, os acessos indevidos e muitos outros acontecimentos que podem implicar ações, comportamentos e análises preditivas, preventivas ou corretivas e consequentes ações de operação e manutenção.

O resultado do trabalho demonstrou que este modelo é viável e as soluções são universais para sistemas e aplicações que gerem ficheiros *logs*, comprovando no controlo do fluxo de dados da alarmística e monitorização do sistema de bilhética e do sistema de gestão de tráfego. Estes artefactos confirmaram a aplicação do modelo proposto no tipo de aplicação *blockchain* principalmente no controlo de fluxo de dados (BC3-Controlo de fluxo de dados do modelo), não sendo intrusivo nos sistemas e aplicações.

A 2ª iteração adicionou ao primeiro processo de controlo de fluxo de dados dos ficheiros *log*, o controlo dos registos de eventos inseridos na base de dados. A tecnologia *blockchain* permitiu da mesma forma constituir-se como uma camada de confiança que garante a autenticidade dos dados e a integridade dos dados, e desta forma fornece o mecanismo de acesso aos dados de forma controlada e com a garantia de não adulteração dos dados. Esta iteração pôde ser melhorada com a utilização das árvores Merkle que permitiram validar grupos de registos com o *hash* resultado da combinação dos *hashs* dos registos base, até à raiz, otimizando o processamento e o armazenando face ao tratamento do registo a registo.

Esta iteração implicou necessariamente o acesso ao modelo de dados das aplicações, sendo mais intrusiva, implicando adicionar campos de controlo e de acesso aos dados, e ativar na fase de inserção *triggers* que forneceram os mecanismos de controlo e de construção do *blockchain* de registos. Tal como na 1ª iteração, a tecnologia *blockchain* constituiu-se como uma camada de confiança dos dados, mantendo a informação de controlo através de *hashs* e de informação de acesso aos dados (*links*).

Nesta fase e com o trabalho de investigação desenvolvido podemos afirmar que a tecnologia *blockchain* garante a autenticidade dos dados e a integridade dos dados, através

de uma camada de confiança, que a liga aos dados, mas é independente da camada de dados.

O estudo realizado permite perspetivar a evolução crescente em termos investigação da tecnologia *blockchain*, suportada no enorme investimento que se realiza em diversas áreas e sobre diversos aspetos da tecnologia *blockchain*, o que conduz à espectativa que os novos modelos de negócios tenderão a usar contratos "inteligentes" dinâmicos e estruturas descentralizadas, com propostas de Valor baseadas em tecnologia *blockchain* e terão de cumprir as seguintes caraterísticas base: a imutabilidade, a criptografia, a distribuição, a tokenização e a descentralização.

A tecnologia *blockchain* tenderá a incorporar ou a ser incorporada em tecnologias complementares, como a identidade descentralizada (*SSI-Self-Sovereign Identity*), o *big data*, a *IoT* e a inteligência artificial (AI), fornecendo a camada de confiança e futuramente com as expectáveis melhorias de processamento, com consensos mais eficientes, e com maiores capacidades de armazenamento, incluirá a camada de dados.

2. Limitações e Trabalho Futuro

Este trabalho não estudou os sistemas transacionais monetizados que suportam várias atividades inerentes ao funcionamento de uma *smart city*.

O modelo proposto foi avaliado principalmente no controlo de fluxo de dados e resultou na adoção de soluções que separam a camada de dados, da camada de controlo, a que se chamou a camada de confiança. Esta limitação resulta da dificuldade em obter capacidade de armazenamento e computação distribuída para tratar grandes quantidades de dados, como é o caso, através de uma rede *blockchain* que inclua grandes volumes de dados *IoT*.

Os trabalhos futuros devem incidir sobre os sistemas transacionais e completar as restantes fases do fluxo de dados desde os equipamentos *IoT*, ao armazenamento e tratamento dos dados, com a criação de camadas de confiança, suportadas numa rede *blockchain* que fornece a segurança aos dados.

Também deverão ser realizados trabalhos para os restantes tipos de aplicações de *blockchain* definidas no modelo, nomeadamente verificar se os equipamentos *IoT* são equipamentos válidos e efetuar o controlo de versões por tipo de equipamento, e a partir dai poder verificar a segurança dos dados transmitidos, em tempo real ou em blocos, possibilitando a existência blocos de eventos de *offline* em algumas fases do envio.

Bibliografia

Abella, A., Ortiz-de-Urbina-Criado, M., & De-Pablos-Heredero, C. (2017). A model for the analysis of data-driven innovation and value generation in smart cities' ecosystems. *Cities*, *64*, 47–53. https://doi.org/10.1016/j.cities.2017.01.011

Agarwal, A., Dahleh, M., & Sarkar, T. (2018). A Marketplace for Data: An Algorithmic Solution. *ArXiv:1805.08125 [Cs]*. http://arxiv.org/abs/1805.08125

Ai, B., Guan, K., Rupp, M., Kurner, T., Cheng, X., Yin, X.-F., Wang, Q., Ma, G.-Y., Li, Y., Xiong, L., & Ding, J.-W. (2015). Future railway services-oriented mobile communications network. *IEEE Communications Magazine*, *53*(10), 78–85. https://doi.org/10.1109/MCOM.2015.7295467

Aken, J. E. van. (2004). Management Research Based on the Paradigm of the Design Sciences: The Quest for Field-Tested and Grounded Technological Rules: Paradigm of the Design Sciences. *Journal of Management Studies*, *41*(2), 219–246. https://doi.org/10.1111/j.1467-6486.2004.00430.x

Al Nuaimi, E., Al Neyadi, H., Mohamed, N., & Al-Jaroodi, J. (2015). Applications of big data to smart cities. *Journal of Internet Services and Applications*, *6*(1). https://doi.org/10.1186/s13174-015-0041-5

Alawadhi, S., & Scholl, H. J. (2016). Smart Governance: A Cross-Case Analysis of Smart City Initiatives. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2953–2963. https://doi.org/10.1109/HICSS.2016.370

Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart Cities: Definitions, Dimensions, Performance, and Initiatives. *Journal of Urban Technology*, *22*(1), 3–21. https://doi.org/10.1080/10630732.2014.942092

Ali, M. S., Dolui, K., & Antonelli, F. (2017). IoT data privacy via blockchains and IPFS. *Proceedings of the Seventh International Conference on the Internet of Things - IoT '17*, 1–7. https://doi.org/10.1145/3131542.3131563

Alter, M. (2015). *Best Practices for IT Service Management*. Introducing ITIL. https://www.nysforum.org/events/4_30_2015/Final.pdf

Alturki, A., Gable, G. G., & Bandara, W. (2011). A Design Science Research Roadmap. Em H. Jain, A. P. Sinha, & P. Vitharana (Eds.), *Service-Oriented Perspectives in Design Science Research* (Vol. 6629, pp. 107–123). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-20633-7_8

Amarnath, A. (2011). *City as a Customer Strategy: Growth Opportunities From The Cities of Tomorrow*. 31.

Amjad, S., & Javaid, N. (2019). *The Secure Service System for Clients through Service Provider by using the IoT in Blockchain*. 7.

Amorim, A. L. de. (2016). Cidades Inteligentes e City Information Modeling. *XX Congreso de la Sociedad Iberoamericana de Gráfica Digital*, 481–488. https://doi.org/10.5151/despro-sigradi2016-440

Anjum, A., Sporny, M., & Sill, A. (2017). Blockchain Standards for Compliance and Trust. *IEEE Cloud Computing*, *4*(4), 84–90.

Anthopoulos, L. G. (2015). Understanding the Smart City Domain: A Literature Review. Em A. de Janvry & R. Kanbur (Eds.), *Poverty, Inequality and Development* (Vol. 1, pp. 9–21). Springer US. https://doi.org/10.1007/978-3-319-03167-5_2

Anthopoulos, L. G., Janssen, M., & Weerakkody, V. (2015). Comparing Smart Cities with different modeling approaches. *Proceedings of the 24th International*

Conference on World Wide Web, 525–528. http://dl.acm.org/citation.cfm?id=2743920

Anwar, U. (2017). *Blockchain: Anonymisation Techniques within Distributed Ledgers*. 6.

Arasteh, H., Hosseinnezhad, V., Loia, V., Tommasetti, A., Troisi, O., Shafie-khah, M., & Siano, P. (2016). Iot-based smart cities: A survey. *Environment and Electrical Engineering (EEEIC), 2016 IEEE 16th International Conference on*, 1–6.

Avison, D., & Fitzgerald, G. (2006). *Information systems development: Methodologies, techniques and tools* (4.ª ed.). McGraw Hill.

Babich, V., & Hilary, G. (2019). *Distributed Ledgers and Operations: What Operations Management Researchers Should Know about Blockchain Technology*. 39.

Bach, L. M., Mihaljevic, B., & Zagar, M. (2018). Comparative analysis of blockchain consensus algorithms. *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1545–1550. https://doi.org/10.23919/MIPRO.2018.8400278

Badii, C., Bellini, P., Cenni, D., Difino, A., Nesi, P., & Paolucci, M. (2017). Analysis and assessment of a knowledge based smart city architecture providing service APIs. *Future Generation Computer Systems*, *75*, 14–29. https://doi.org/10.1016/j.future.2017.05.001

Baliga, D. A. (2017). *Understanding Blockchain Consensus Models*. 14.

Baskerville, R., Pries-Heje, J., & Venable, J. (2009). Soft design science methodology. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology - DESRIST '09*, 1. https://doi.org/10.1145/1555619.1555631

Bates, O., & Friday, A. (2017). Beyond Data in the Smart City: Repurposing Existing Campus IoT. *IEEE Pervasive Computing*, *16*(2), 54–60.

Bauer, I., Zavolokina, L., Leisibach, F., & Schwabe, G. (2019). *Exploring Blockchain Value Creation: The Case of the Car Ecosystem*. 10.

Bellini, P., Nesi, P., & Pantaleo, G. (2015). Benchmarking RDF Stores for Smart City Services. *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, 46–49. https://doi.org/10.1109/SmartCity.2015.45

Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System. *ArXiv:1407.3561 [Cs]*. http://arxiv.org/abs/1407.3561

Benevolo, C., Dameri, R. P., & D'Auria, B. (2016). Smart Mobility in Smart City. Em T. Torre, A. M. Braccini, & R. Spinelli (Eds.), *Empowering Organizations* (Vol. 11, pp. 13–28). Springer International Publishing. https://doi.org/10.1007/978-3-319-23784-8_2

Beyer, C., Elisei, P., Popovich, V. V., Schrenk, M., & Zeile, P. (2015). *REAL CORP 2015. Plan Together—Right Now—Overall. From Vision to Reality for Vibrant Cities and Regions Proceedings of the 20th International Conference on Urban Planning, Regional Development and Information Society*.

Bharadwaj, A. S., Rego, R., & Chowdhury, A. (2016). IoT based solid waste management system: A conceptual approach with an architectural solution as a smart city application. *2016 IEEE Annual India Conference (INDICON)*, 1–6. https://doi.org/10.1109/INDICON.2016.7839147

Biswas, K., & Muthukkumarasamy, V. (2016). *Securing Smart Cities Using Blockchain Technology*. 2016 IEEE 18th International Conference on High Performance

Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems.

Bo Chen, & Cheng, H. H. (2010). A Review of the Applications of Agent Technology in Traffic and Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems*, *11*(2), 485–497. https://doi.org/10.1109/TITS.2010.2048313

Bongaerts, R., Kwiatkowski, M., & König, T. (2017). Disruption Technology in Mobility: Customer Acceptance and Examples. Em A. Khare, B. Stewart, & R. Schatz (Eds.), *Phantom Ex Machina* (pp. 119–135). Springer International Publishing. https://doi.org/10.1007/978-3-319-44468-0_8

Boyes, H. (2016). *Cyber security risks in the Built Environment—Standards, Skills & Apprenticeships*.

Braem, B., Latre, S., Leroux, P., Demeester, P., Coenen, T., & Ballon, P. (2016). Designing a smart city playground: Real-time air quality measurements and visualization in the City of Things testbed. *Smart Cities Conference (ISC2), 2016 IEEE International*, 1–2.

Brandão, A., Mamede, H. S., & Gonçalves, R. (2018a). A Smart City's Model Secured by Blockchain. Em J. Mejia, M. Muñoz, Á. Rocha, A. Peña, & M. Pérez-Cisneros (Eds.), *Trends and Applications in Software Engineering* (Vol. 865, pp. 249–260). Springer International Publishing. https://doi.org/10.1007/978-3-030-01171-0_23

Brandão, A., Mamede, H. S., & Gonçalves, R. (2018b). Systematic Review of the Literature, Research on Blockchain Technology as Support to the Trust Model Proposed Applied to Smart Places. Em Á. Rocha, H. Adeli, L. P. Reis, & S. Costanzo (Eds.), *Trends and Advances in Information Systems and Technologies*

(Vol. 745, pp. 1163–1174). Springer International Publishing. https://doi.org/10.1007/978-3-319-77703-0_113

Brandão, A., Mamede, H. S., & Gonçalves, R. (2019). Trusted Data's Marketplace. Em Á. Rocha, H. Adeli, L. P. Reis, & S. Costanzo (Eds.), *New Knowledge in Information Systems and Technologies* (Vol. 930, pp. 515–527). Springer International Publishing. https://doi.org/10.1007/978-3-030-16181-1_49

Brown, B. C. (2005). *Theory and Practice of Integral Sustainable Development*. *1*(2), 39.

Bumanis, N., Vitols, G., Arhipova, I., & Mozga, I. (2017, Maio 24). *Mobile ticket lifecycle management: Case study of public transport in Latvia*. 16th International Scientific Conference Engineering for Rural Development. https://doi.org/10.22616/ERDev2017.16.N015

Cachin, C. (2016). *Architecture of the Hyperledger Blockchain Fabric*. 4.

Cachin, C., Schubert, S., & Vukolić, M. (2016). Non-determinism in Byzantine Fault-Tolerant Replication. *ArXiv:1603.07351 [Cs]*. http://arxiv.org/abs/1603.07351

Cao, T.-D., Pham, T.-V., Vu, Q.-H., Truong, H.-L., Le, D.-H., & Dustdar, S. (2016). MARSA: A Marketplace for Realtime Human Sensing Data. *ACM Transactions on Internet Technology*, *16*(3), 1–21. https://doi.org/10.1145/2883611

Casino, F., Dasaklis, T. K., & Patsakis, C. (2018). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*. https://doi.org/10.1016/j.tele.2018.11.006

Castro, M., & Liskov, B. (2002). Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems*, *20*(4), 398–461. https://doi.org/10.1145/571637.571640

Castro, M., & Liskov, B. (1999). Practical Byzantine fault tolerance. *OSDI*, *99*, 173–186.

Ceballos, G. R., & Larios, V. M. (2016). A model to promote citizen driven government in a smart city: Use case at GDL smart city. *Smart Cities Conference (ISC2), 2016 IEEE International*, 1–6. http://ieeexplore.ieee.org/abstract/document/7580873/

Cekerevac, Z., Prigoda, L., & Maletic, J. (2018). *Blockchain Technology and Industrial Internet of Things in the Suplly Chains*. *6*(2), 9.

Chakrabarti, A., & Chaudhuri, A. K. (2017). *Blockchain and its Scope in Retail*. *04*(07), 4.

Chakrabarty, S., & Engels, D. W. (2016). A secure IoT architecture for Smart Cities. *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 812–813. https://doi.org/10.1109/CCNC.2016.7444889

Chen, T., Wang, H., Ning, B., Zhang, Y., Tang, T., & Li, K. (2018). Architecture Design of a Novel Train-centric CBTC System. *2018 International Conference on Intelligent Rail Transportation (ICIRT)*, 1–5. https://doi.org/10.1109/ICIRT.2018.8641603

Chen, Y., Li, H., Li, K., & Zhang, J. (2017). An improved P2P file system scheme based on IPFS and Blockchain. *2017 IEEE International Conference on Big Data (Big Data)*, 2652–2657. https://doi.org/10.1109/BigData.2017.8258226

Chen, Y.-J., Wang, L.-C., & Wang, S. (2018). *Stochastic Blockchain for IoT Data Integrity*. 14.

Chepurnoy, A., Larangeira, M., & Ojiganov, A. (2016). Rollerchain, a Blockchain With Safely Pruneable Full Blocks. *ArXiv:1603.07926 [Cs]*. http://arxiv.org/abs/1603.07926

Chilipirea, C., Petre, A.-C., Groza, L.-M., Dobre, C., & Pop, F. (2017). An integrated architecture for future studies in data processing for smart cities. *Microprocessors and Microsystems*, *52*, 335–342. https://doi.org/10.1016/j.micpro.2017.03.004

Chin, J., Callaghan, V., & Lam, I. (2017). Understanding and personalising smart city services using machine learning, The Internet-of-Things and Big Data. *2017 IEEE 26th International Symposium on Industrial Electronics (ISIE)*, 2050–2055. https://doi.org/10.1109/ISIE.2017.8001570

Cho, H. (2018). ASIC-Resistance of Multi-Hash Proof-of-Work Mechanisms for Blockchain Consensus Protocols. *IEEE Access*, *6*, 66210–66222. https://doi.org/10.1109/ACCESS.2018.2878895

Cho, S., Park, S. Y., & Lee, S. R. (2017). Blockchain Consensus Rule Based Dynamic Blind Voting for Non-Dependency Transaction. *International Journal of Grid and Distributed Computing*, *10*(12), 93–106. https://doi.org/10.14257/ijgdc.2017.10.12.09

Chowdhary, N., & Deep Kaur, P. (2016). Addressing the characteristics of mobility models in IoV for smart city. *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 1298–1303. https://doi.org/10.1109/CCAA.2016.7813919

Coccoli, M., Maresca, P., Stanganelli, L., & Guercio, A. (2015). An experience of collaboration using a PaaS for the smarter university model. *Journal of Visual Languages & Computing*, *31*, 275–282. https://doi.org/10.1016/j.jvlc.2015.10.014

Cohen, B. (2013). Smart city wheel. *Retrieved from SMART & SAFE CITY: http://www. smartcircle. org/smartcity/blog/boyd-cohen-the-smart-city-wheel*.

Colding, J., & Barthel, S. (2017). An urban ecology critique on the “Smart City” model. *Journal of Cleaner Production*, *164*, 95–101. https://doi.org/10.1016/j.jclepro.2017.06.191

Corak, B. H., Okay, F. Y., Guzel, M., Murt, S., & Ozdemir, S. (2018). Comparative Analysis of IoT Communication Protocols. *2018 International Symposium on Networks, Computers and Communications (ISNCC)*, 1–6. https://doi.org/10.1109/ISNCC.2018.8530963

Corman, F., & Meng, L. (2015). A Review of Online Dynamic Models and Algorithms for Railway Traffic Management. *IEEE Transactions on Intelligent Transportation Systems*, *16*(3), 1274–1284. https://doi.org/10.1109/TITS.2014.2358392

Cruz, N. F. da, & Marques, R. C. (2014). Scorecards for sustainable local governments. *Cities*, *39*, 165–170. https://doi.org/10.1016/j.cities.2014.01.001

Cucurull, J., & Puiggalí, J. (2016). Distributed Immutabilization of Secure Logs. Em G. Barthe, E. Markatos, & P. Samarati (Eds.), *Security and Trust Management* (Vol. 9871, pp. 122–137). Springer International Publishing. https://doi.org/10.1007/978-3-319-46598-2_9

Cybersecurity in Smart Buildings (Collaborative Industry Perspective N. 9835–19; Cybersecurity in Smart Buildings). (2015). Frost & Sullivan. https://www.switchautomation.com/wp-content/uploads/2015/12/Cybersecurity-in-Smart-Buildings_-Discussion-Paper.pdf

Dameri, R. P. (2012). Searching for Smart City definition: A comprehensive proposal. *INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY*, *11*(5), 2544–2551. https://doi.org/10.24297/ijct.v11i5.1142

Dao, D., Alistarh, D., Musat, C., & Zhang, C. (2018). DataBright: Towards a Global Exchange for Decentralized Data Ownership and Trusted Computation. *ArXiv:1802.04780 [Cs]*. http://arxiv.org/abs/1802.04780

de Aquino, B. M. M., de Lima, M. V. L., de Oliveira, J. P. C. M., & de Souza, C. T. (2018). Protocolos IPFS e IPNS como meio para o controle de botnet: Prova de conceito. *Anais do Workshop de Segurança Cibernética em Dispositivos Conectados (WSCDC-SBRC 2018), 1*.

de Jong, M., Joss, S., Schraven, D., Zhan, C., & Weijnen, M. (2015). Sustainable–smart–resilient–low carbon–eco–knowledge cities; making sense of a multitude of concepts promoting sustainable urbanization. *Journal of Cleaner Production*, *109*, 25–38. https://doi.org/10.1016/j.jclepro.2015.02.004

Deakin, M. (2011). The embedded intelligence of smart cities. *Intelligent Buildings International*, *3*(3), 189–197. https://doi.org/10.1080/17508975.2011.579340

Deakin, M., & Al Waer, H. (2011). From intelligent to smart cities. *Intelligent Buildings International*, *3*(3), 140–152. https://doi.org/10.1080/17508975.2011.586671

Decker, C., Seidel, J., & Wattenhofer, R. (2014). Bitcoin Meets Strong Consistency. *ArXiv:1412.7935 [Cs]*. http://arxiv.org/abs/1412.7935

Desouza, K. C., & Flanery, T. H. (2013). Designing, planning, and managing resilient cities: A conceptual framework. *Cities*, *35*, 89–99.

Dhungana, D., Engelbrecht, G., Parreira, J. X., Schuster, A., Tobler, R., & Valerio, D. (2016). Data-driven ecosystems in smart cities: A living example from Seestadt Aspern. *Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on*, 82–87. http://ieeexplore.ieee.org/abstract/document/7845434/

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). *Blockchain for IoT security and privacy: The case study of a smart home*. 618–623. https://doi.org/10.1109/PERCOMW.2017.7917634

Draskovic, D., & Saleh, G. (2017). *Decentralized data marketplace based on blockchain*. 16.

Duarte, F., de Carvalho Figueiredo, F., Leite, L., & Alcides Rezende, D. (2014). A Conceptual Framework for Assessing Digital Cities and the Brazilian Index of Digital Cities: Analysis of Curitiba, the First-Ranked City. *Journal of Urban Technology*, *21*(3), 37–48. https://doi.org/10.1080/10630732.2014.940709

Dustdar, S., Nastic, S., & Scekic, O. (2016). A Novel Vision of Cyber-Human Smart City. *2016 Fourth IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*, 42–47. https://doi.org/10.1109/HotWeb.2016.16

Dworkin, M. J. (2007). *Recommendation for block cipher modes of operation: The CCM mode for authentication and confidentiality* (NIST SP 800-38c; p. NIST SP 800-38c). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-38c

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research*, *5*(4), 491–497. https://doi.org/10.1016/j.jare.2014.02.006

ENISA. (2017). *Information Sharing and Analysis Centres (ISACs)*. 51. https://doi.org/10.2824/549292

Evans, J. (2017). *A Systems Approach to Predicting and Measuring Workload in Rail Traffic Management Systems*. 16.

Fazio, M., Celesti, A., Puliafito, A., & Villari, M. (2015). Big Data Storage in the Cloud for Smart Environment Monitoring. *Procedia Computer Science*, *52*, 500–506. https://doi.org/10.1016/j.procs.2015.05.023

Ferreira, M. C., Nóvoa, H., Dias, T. G., & Cunha, J. F. e. (2014). A Proposal for a Public Transport Ticketing Solution based on Customers' Mobile Devices. *Procedia - Social and Behavioral Sciences*, *111*, 232–241. https://doi.org/10.1016/j.sbspro.2014.01.056

Forbes, T. (1999). Prime clusters and Cunningham chains. *Mathematics of Computation*, *68*(228), 1739–1748. https://doi.org/10.1090/S0025-5718-99-01117-5

Fourie, C. J., & Chimusoro, O. (2018). *AN EXAMINATION OF THE RELATIONSHIP BETWEEN SUPPLY CHAIN MANAGEMENT PRACTICES AND BUSINESS PERFORMANCE: A CASE ANALYSIS OF A PASSENGER RAIL COMPANY*. 12.

Gaetani, E., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2016). *Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments*. 10.

Gallego-Lopez, C., & Essex, J. (2016). *Understanding risk and resilient infrastructure investment*. Evidence on Demand. https://doi.org/10.12774/eod_tg.july2016.gallegolopezessex3

Garcia, A. E. G. (2017). A Inteligência Competitiva e o Desenvolvimento de Capacidades Dinâmicas nas Organizações. *Revista Ibero-Americana de Estratégia*, *16*(01), 91–98. https://doi.org/10.5585/riae.v16i1.2439

Gaubatz, G., Kaps, J.-P., Ozturk, E., & Sunar, B. (2005). State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks. *Third IEEE*

International Conference on Pervasive Computing and Communications Workshops, 146–150. https://doi.org/10.1109/PERCOMW.2005.76

Ghannem, A., Hamdi, M. S., Abdelmoez, W., & Ammar, H. H. (2015). A context model development process for smart city operations. *Service Operations And Logistics, And Informatics (SOLI), 2015 IEEE International Conference on*, 122–127. http://ieeexplore.ieee.org/abstract/document/7367605/

Gharaibeh, A., Salahuddin, M. A., Hussini, S. J., Khreishah, A., Khalil, I., Guizani, M., & Al-Fuqaha, A. (2017). Smart Cities: A Survey on Data Management, Security, and Enabling Technologies. *IEEE Communications Surveys & Tutorials*, *19*(4), 2456–2501. https://doi.org/10.1109/COMST.2017.2736886

Ghosh, H. (2018). Data Marketplace as a Platform for Sharing Scientific Data. Em U. M. Munshi & N. Verma (Eds.), *Data Science Landscape* (Vol. 38, pp. 99–105). Springer Singapore. https://doi.org/10.1007/978-981-10-7515-5_7

Ghuli, P., Kumar, U. P., & Shettar, R. (2017). *A Review on Blockchain Application for Decentralized Decision of Ownership of IoT Devices*. 8.

Giang, N. K., Lea, R., Blackstock, M., & Leung, V. C. M. (2016). On Building Smart City IoT Applications: A Coordination-based Perspective. *Proceedings of the 2nd International Workshop on Smart - SmartCities '16*, 1–6. https://doi.org/10.1145/3009912.3009919

Gilad-Bachrach, R., Laine, K., Lauter, K., Rindal, P., & Rosulek, M. (2017). *Secure Data Exchange: A Marketplace in the Cloud*. 30.

Glaeser, E. L. (2006). *Why Are Smart Places Getting Smarter?* 4.

Grave, K. M. (2016). *A Case Study of Smart Cities: The Role of Stakeholder Commitment*. 221.

Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*, *37*(2), 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01

Guo, H., Wei Sim, J. Z., Veeravalli, B., & Lu, J. (2018). Protecting Train Balise Telegram Data Integrity. *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, 806–811. https://doi.org/10.1109/ITSC.2018.8569616

Gupta, S. S. (2017). *BLOCKCHAIN - The foundation behind Bitcoin*. John Wiley & Sons, Inc.

Gurník, P. (2016). Next Generation Train Control (NGTC): More Effective Railways through the Convergence of Main-line and Urban Train Control Systems. *Transportation Research Procedia*, *14*, 1855–1864. https://doi.org/10.1016/j.trpro.2016.05.152

Hammer, S. (2018). *The Blockchain Ecosystem*. 39.

Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security*, *78*, 126–142. https://doi.org/10.1016/j.cose.2018.06.004

Hankerson, D. R., Vanstone, S. A., & Menezes, A. J. (2003). *Guide to elliptic curve cryptography*. Springer.

Harrison, C., & Donnelly, I. A. (2011). A theory of smart cities. *Proceedings of the 55th Annual Meeting of the ISSS-2011, Hull, UK*, *55*. http://journals.isss.org/index.php/proceedings55th/article/view/1703

Hasan, S. S., Sultan, N. H., & Barbhuiya, F. A. (2019). Cloud Data Provenance using IPFS and Blockchain Technology. *Proceedings of the Seventh International*

Workshop on Security in Cloud Computing - SCC '19, 5–12. https://doi.org/10.1145/3327962.3331457

Hashem, I. A. T., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Gani, A., Ahmed, E., & Chiroma, H. (2016). The role of big data in smart city. *International Journal of Information Management*, *36*(5), 748–758. https://doi.org/10.1016/j.ijinfomgt.2016.05.002

Hennessy, G., Cook, J., Bean, M., & Dykes, K. (2011). Economic dynamics for smarter cities. *29th International Conference of the System Dynamics Society, Washington, DC*. http://www.systemdynamics.org/conferences/2011/proceed/papers/P1124.pdf

Hevner, A. R. (2007). *A Three Cycle View of Design Science Research*. *19*, 7.

Hussain, A., Mkpojiogu, E. O. C., & Jasin, N. (2017). *USABILITY METRICS AND METHODS FOR PUBLIC TRANSPORTATION APPLICATIONS: A SYSTEMATIC REVIEW*. *4*, 9.

Hynes, N., Dao, D., Yan, D., Cheng, R., & Song, D. (2018). A demonstration of sterling: A privacy-preserving data marketplace. *Proceedings of the VLDB Endowment*, *11*(12), 2086–2089. https://doi.org/10.14778/3229863.3236266

IET. (2012). Intelligent Buildings: Understanding and managing the security risks. *Engineering & Technology Reference*. https://doi.org/10.1049/etr.2012.9001

ISO 37120. (2014). *Sustainable development of communities—Indicators for city services and quality of life*. International Standards Organization. https://cities.dataforcities.org/resources/ISO%2037120%20Indicators.pdf?v=1510957203519

ITU-T. (2014). *Overview of key performance indicators in smart sustainable cities*. International Telecommunication Union. https://www.itu.int/en/ITU-T/focusgroups/ssc/Documents/Approved_Deliverables/TS-Overview-KPI.docx

Jabbari, A., & Kaminsky, P. (2018). *Blockchain and Supply Chain Management*. 13.

Jang, B., Park, S., Lee, J., & Hahn, S.-G. (2018). Three Hierarchical Levels of Big-Data Market Model Over Multiple Data Sources for Internet of Things. *IEEE Access*, *6*, 31269–31280. https://doi.org/10.1109/ACCESS.2018.2845105

Jaradat, M., Jarrah, M., Bousselham, A., Jararweh, Y., & Al-Ayyoub, M. (2015). The Internet of Energy: Smart Sensor Networks and Big Data Management for Smart Grid. *Procedia Computer Science*, *56*, 592–597. https://doi.org/10.1016/j.procs.2015.07.250

Jin, J., Gubbi, J., Marusic, S., & Palaniswami, M. (2014). An Information Framework for Creating a Smart City Through Internet of Things. *IEEE Internet of Things Journal*, *1*(2), 112–121. https://doi.org/10.1109/JIOT.2013.2296516

Johnson, D., Menezes, A., & Vanstone, S. (2001). The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, *1*(1), 36–63. https://doi.org/10.1007/s102070100002

Johnson, J., & Henderson, A. (2002). Conceptual models: Begin by designing what to design. *interactions*, *9*(1). https://doi.org/10.1145/503355.503366

Kano, N., Seraku, N., Takahashi, F., & Tsuji, S. (1984). Attractive quality and must-be quality. *Hinshitsu: The Journal of the Japanese Society for Quality Control*, *14*(2), 39–48.

Katuwal, G. J., Pandey, S., Hennessey, M., & Lamichhane, B. (2018). Applications of Blockchain in Healthcare: Current Landscape & Challenges. *ArXiv:1812.02776 [Cs]*. http://arxiv.org/abs/1812.02776

Kazi, S., Bagasrawala, M., Shaikh, F., & Sayyed, A. (2018). *Smart E-Ticketing System for Public Transport Bus*. 7.

Khacef, K., & Pujolle, G. (2019). Secure Peer-to-Peer Communication Based on Blockchain. Em L. Barolli, M. Takizawa, F. Xhafa, & T. Enokido (Eds.), *Web, Artificial Intelligence and Network Applications* (Vol. 927, pp. 662–672). Springer International Publishing. https://doi.org/10.1007/978-3-030-15035-8_64

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. https://doi.org/10.1016/j.future.2017.11.022

Khan, Z., Anjum, A., & Kiani, S. L. (2013). Cloud Based Big Data Analytics for Smart Future Cities. *2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing*, 381–386. https://doi.org/10.1109/UCC.2013.77

Khatoun, R., & Zeadally, S. (2016). Smart cities: Concepts, architectures, research opportunities. *Communications of the ACM*, *59*(8), 46–57.

Kim, N. H., Kang, S. M., & Hong, C. S. (2017). Mobile charger billing system using lightweight Blockchain. *2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 374–377. https://doi.org/10.1109/APNOMS.2017.8094151

King, S. (2013). *Primecoin: Cryptocurrency with Prime Number Proof-of-Work*. 6.

King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August*, *19*.

Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal*, *79*(1), 1–14. https://doi.org/10.1007/s10708-013-9516-8

Koens, T., & Poll, E. (2018). *The Drivers Behind Blockchain Adoption: The Rationality of Irrational Choices*. 12.

Kourtit, K., Macharis, C., & Nijkamp, P. (2014). *A Multi-Actor Multi-Criteria Analysis of the Performance of Global Cities*. 43.

Kraft, D. (2016). Difficulty control for blockchain-based consensus systems. *Peer-to-Peer Networking and Applications*, *9*(2), 397–413. https://doi.org/10.1007/s12083-015-0347-x

Kuechler, W., & Vaishnavi, V. (2012). *A Framework for Theory Development in Design Science Research: Multiple Perspectives*. *13*(6), 29.

Kumar, N. M., & Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IoT. *Procedia Computer Science*, *132*, 1815–1823. https://doi.org/10.1016/j.procs.2018.05.140

Kwon, J. (2014). *Tendermint: Consensus without Mining*. 11.

Latre, S., Leroux, P., Coenen, T., Braem, B., Ballon, P., & Demeester, P. (2016). City of things: An integrated and multi-technology testbed for IoT smart city experiments. *2016 IEEE International Smart Cities Conference (ISC2)*, 1–8. https://doi.org/10.1109/ISC2.2016.7580875

Lazaroiu, G. C., & Roscia, M. (2012). Definition methodology for the smart cities model. *Energy*, *47*(1), 326–332. https://doi.org/10.1016/j.energy.2012.09.028

Lee, J. H., Hancock, M. G., & Hu, M.-C. (2014). Towards an effective framework for building smart cities: Lessons from Seoul and San Francisco. *Technological*

Forecasting and Social Change, *89*, 80–99. https://doi.org/10.1016/j.techfore.2013.08.033

Lee, J. H., Phaal, R., & Lee, S.-H. (2013). An integrated service-device-technology roadmap for smart city development. *Technological Forecasting and Social Change*, *80*(2), 286–306. https://doi.org/10.1016/j.techfore.2012.09.020

Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. (2017). Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems. *IEEE Internet of Things Journal*, 1–1. https://doi.org/10.1109/JIOT.2017.2740569

Li, F., Nucciarelli, A., Roden, S., & Graham, G. (2016). How smart cities transform operations models: A new research agenda for operations management in the digital economy. *Production Planning & Control*, *27*(6), 514–528. https://doi.org/10.1080/09537287.2016.1147096

Li, J., Wang, J., Xu, N., Hu, Y., & Cui, C. (2018). Importance Degree Research of Safety Risk Management Processes of Urban Rail Transit Based on Text Mining Method. *Information*, *9*(2), 26. https://doi.org/10.3390/info9020026

Li, S., Yang, L., & Gao, Z. (2015). Coordinated cruise control for high-speed train movements based on a multi-agent model. *Transportation Research Part C: Emerging Technologies*, *56*, 281–292. https://doi.org/10.1016/j.trc.2015.04.016

Li, Y., Marier-Bienvenue, T., Perron-Brault, A., Wang, X., & Paré, G. (2018). Blockchain technology in business organizations: A scoping review. *Proceedings of the 51st Hawaii International Conference on System Sciences*.

Liang, G., Weller, S. R., Luo, F., Zhao, J., & Dong, Z. Y. (2018). Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber

Attacks. *IEEE Transactions on Smart Grid*, 1–1. https://doi.org/10.1109/TSG.2018.2819663

Lin, I.-C., & Liao, T.-C. (2017). A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, *19*(5), 653–659. https://doi.org/10.6633/IJNS.201709.19(5).01

Linder, L., Vionnet, D., Bacher, J.-P., & Hennebert, J. (2017). Big Building Data—A Big Data Platform for Smart Buildings. *Energy Procedia*, *122*, 589–594. https://doi.org/10.1016/j.egypro.2017.07.354

Liu, B., & Sun, X. (2018). Application Analysis of BIM Technology in Metro Rail Transit. *IOP Conference Series: Earth and Environmental Science*, *128*, 012028. https://doi.org/10.1088/1755-1315/128/1/012028

Lu, Q.-C., & Lin, S. (2019). Vulnerability Analysis of Urban Rail Transit Network within Multi-Modal Public Transport Networks. *Sustainability*, *11*(7), 2109. https://doi.org/10.3390/su11072109

Luo, H., Liu, C., Wu, C., & Guo, X. (2018). Urban Change Detection Based on Dempster–Shafer Theory for Multitemporal Very High-Resolution Imagery. *Remote Sensing*, *10*(7), 980. https://doi.org/10.3390/rs10070980

Mali, N., & Kanwade, P. A. (2016). "A Review on Smart City through Internet of Things (IOT). *International Journal of Advanced Research in Science Management and Technology*, *2*(6).

Mallat, N., Rossi, M., Tuunainen, V. K., & Öörni, A. (2007). An empirical investigation of mobile ticketing service adoption in public transportation. *Personal and Ubiquitous Computing*, *12*(1), 57–65. https://doi.org/10.1007/s00779-006-0126-z

Manson, N. (2006). Is operations research really research? *ORiON*, *22*(2). https://doi.org/10.5784/22-2-40

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision support systems*, *15*(4), 251–266.

Marr, B. (2018). Blockchain And The Internet Of Things: 4 Important Benefits Of Combining These Two Mega Trends. *The Forbes*, 2.

Mattila, J. (2016). *The Blockchain Phenomenon*. 27.

Mazières, D. (2015). *The Stellar Consensus Protocol:* 45.

Mazzanti, F., & Ferrari, A. (2018). Ten diverse formal models for a CBTC automatic train supervision system. *arXiv preprint arXiv:1803.10324*.

Mazzarello, M., & Ottaviani, E. (2007). A traffic management system for real-time traffic optimisation in railways. *Transportation Research Part B: Methodological*, *41*(2), 246–274. https://doi.org/10.1016/j.trb.2006.02.005

McNamee, M. (2009). *Creating Smarter Cities 2011 Storylines: IBM and Smart Cities*. 23.

Merkle, R. C. (1988). A Digital Signature Based on a Conventional Encryption Function. *A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology*, 369–378. http://dl.acm.org/citation.cfm?id=646752.704751

Mohamad Noor, M. binti, & Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer Networks*, *148*, 283–294. https://doi.org/10.1016/j.comnet.2018.11.025

Mohammadi, M., Al-Fuqaha, A., Guizani, M., & Oh, J.-S. (2018). Semisupervised Deep Reinforcement Learning in Support of IoT and Smart City Services. *IEEE Internet of Things Journal*, *5*(2), 624–635. https://doi.org/10.1109/JIOT.2017.2712560

Morandi, C., Rolando, A., & Di Vita, S. (2016). *From Smart City to Smart Region*. Springer International Publishing. https://doi.org/10.1007/978-3-319-17338-2

Moreno, M. V., Terroso-Saenz, F., Gonzalez-Vidal, A., Valdes-Vela, M., Skarmeta, A. F., Zamora, M. A., & Chang, V. (2017). Applicability of Big Data Techniques to Smart Cities Deployments. *IEEE Transactions on Industrial Informatics*, *13*(2), 800–809. https://doi.org/10.1109/TII.2016.2605581

Moreno Pires, S., Fidélis, T., & Ramos, T. B. (2014). Measuring and comparing local sustainable development through common indicators: Constraints and achievements in practice. *Cities*, *39*, 1–9. https://doi.org/10.1016/j.cities.2014.02.003

Nair, V., Pawar, A., Tidke, D. L., Pagar, V., & Wani, N. (2018). *Online Bus Tracking and Ticketing System*. 4.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. 9.

Nam, T., & Pardo, T. A. (2011). Conceptualizing smart city with dimensions of technology, people, and institutions. *Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times*, 282–291. http://dl.acm.org/citation.cfm?id=2037602

Neirotti, P., De Marco, A., Cagliano, A. C., Mangano, G., & Scorrano, F. (2014). Current trends in Smart City initiatives: Some stylised facts. *Cities*, *38*, 25–36. https://doi.org/10.1016/j.cities.2013.12.010

Ng, S. T., Xu, F. J., Yang, Y., & Lu, M. (2017). A Master Data Management Solution to Unlock the Value of Big Infrastructure Data for Smart, Sustainable and Resilient City Planning. *Procedia Engineering*, *196*, 939–947. https://doi.org/10.1016/j.proeng.2017.08.034

Niemeyer, M., Henneböhle, K., & Kuller, M. (2014). Security requirements of IoT-based smart buildings using RESTful Web Services. *Acta Polytechnica Hungarica*, 10.

Nitti, M., Pilloni, V., Giusto, D., & Popescu, V. (2017). IoT Architecture for a Sustainable Tourism Application in a Smart City Environment. *Mobile Information Systems*, *2017*, 1–9. https://doi.org/10.1155/2017/9201640

Otero-Cerdeira, L., Rodríguez-Martínez, F. J., & Gómez-Rodríguez, A. (2014). Enhancing Alignment Results in Ontology Matching for Smart Cities. *WOIS@ BIR*, 55–65. ftp://ceur-ws.org/pub/publications/CEUR-WS/Vol-1230.zip#page=60

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Pellegrino, J. L., Fanney, A. H., Bushby, S. T., Domanski, P. A., Healy, W. M., & Persily, A. K. (2010). *Measurement Science Roadmap for Net-Zero Energy Buildings* (NIST Technical Note 1660; Workshop Summary Report). National Institute of Standards and Technology. https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=905024

Petrolo, R., Loscrì, V., & Mitton, N. (2017). Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms: R. Petrolo, V. Loscrì and

N. Mitton. *Transactions on Emerging Telecommunications Technologies*, *28*(1), e2931. https://doi.org/10.1002/ett.2931

Petrolo, R., Loscrı, V., & Mitton, N. (2012). *Towards a Smart City based on Cloud of Things, a survey on the smart city vision and paradigms*. 12.

Pillmann, J., Wietfeld, C., Zarcula, A., Raugust, T., & Alonso, D. C. (2017). Novel common vehicle information model (CVIM) for future automotive vehicle big data marketplaces. *2017 IEEE Intelligent Vehicles Symposium (IV)*, 1910–1915. https://doi.org/10.1109/IVS.2017.7995984

Popescul, D., & Radu, L. D. (2016). Data Security in Smart Cities: Challenges and Solutions. *Informatica Economica*, *20*(1/2016), 29–38. https://doi.org/10.12948/issn14531305/20.1.2016.03

Prehofer, C., van Gurp, J., Stirbu, V., Satish, S., Tarkoma, S., di Flora, C., & Liimatainen, P. P. (2010). Practical Web-Based Smart Spaces. *IEEE Pervasive Computing*, *9*(3), 72–80. https://doi.org/10.1109/MPRV.2009.88

Profanter, S., Tekat, A., Dorofeev, K., & Rickert, M. (2019). OPC UA versus ROS, DDS, and MQTT: Performance Evaluation of Industry 4.0 Protocols. *Proceedings of the IEEE International Conference on Industrial Technology (ICIT).*, 8.

Psomakelis, E., Aisopos, F., Litke, A., Tserpes, K., Kardara, M., & Campo, P. M. (2016). Big IoT and Social Networking Data for Smart Cities—Algorithmic Improvements on Big Data Analysis in the Context of RADICAL City Applications: *Proceedings of the 6th International Conference on Cloud Computing and Services Science*, 396–405. https://doi.org/10.5220/0005934503960405

Purao, S. (2002). *Design Research in the Technology of Information Systems: Truth or Dare*. 37.

Qu, C., Tao, M., Zhang, J., Hong, X., & Yuan, R. (2018). Blockchain Based Credibility Verification Method for IoT Entities. *Security and Communication Networks*, *2018*, 1–11. https://doi.org/10.1155/2018/7817614

Ra, G.-J., & Lee, I.-Y. (2018). A Study on KSI-based Authentication Management and Communication for Secure Smart Home Environments. *KSII Transactions on Internet and Information Systems*, *12*(2). https://doi.org/10.3837/tiis.2018.02.021

Rabah, K. (2018). *Convergence of AI, IoT, Big Data and Blockchain: A Review*. *1*(1), 18.

Rao, J. S., & Syamala, M. (2017). Internet of Things (IoT) based Smart City Architecture and its Applications. *Mathematical Sciences*, *6*(10), 6.

Rathore, M. M., Ahmad, A., Paul, A., & Rho, S. (2016). Urban planning and building smart cities based on the Internet of Things using Big Data analytics. *Computer Networks*, *101*, 63–80. https://doi.org/10.1016/j.comnet.2015.12.023

Rathore, M. M., Paul, A., Ahmad, A., & Jeon, G. (2017). IoT-Based Big Data: From Smart City towards Next Generation Super City Planning. *International Journal on Semantic Web and Information Systems*, *13*(1), 28–47. https://doi.org/10.4018/IJSWIS.2017010103

Rey-Robert, X. (2009). *Smarter Cities – Dublin event*. 56.

Rhee, S. (2016). Catalyzing the internet of things and smart cities: Global city teams challenge. *Science of Smart City Operations and Platforms Engineering (SCOPE) in partnership with Global City Teams Challenge (GCTC)(SCOPE-GCTC), 2016 1st International Workshop on*, 1–4.

Rinaldi, S., Ferrari, P., & Flammini, A. (2017). Analisys of modular bridge platform for heterogeneous software defined networking in smart city applications. *2017 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, 1–6. https://doi.org/10.1109/I2MTC.2017.7969846

Risius, M., & Spohrer, K. (2017). A Blockchain Research Framework: What We (don't) Know, Where We Go from Here, and How We Will Get There. *Business & Information Systems Engineering*, *59*(6), 385–409. https://doi.org/10.1007/s12599-017-0506-0

Rithika, G., Harshitha, P. S., Manasa, V., & Anisha, M. P. R. (2019). *Blockchain-Foundational Technology to Change the World*. *1076*, 12.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126.

Roberts, S., Bonenberg, L., Meng, X., Moore, T., & Hill, C. (2017). *Predictive Intelligence for a Rail Traffic Management System*. 9.

Roche, S., Nabian, N., Kloeckl, K., & Ratti, C. (2012). *Are 'Smart Cities' Smart Enough?* 22.

Roman-Castro, R., Lopez, J., & Gritzalis, S. (2018). Evolution and Trends in IoT Security. *Computer*, *51*(7), 16–25. https://doi.org/10.1109/MC.2018.3011051

Ruta, M., Scioscia, F., Ieva, S., Capurso, G., Loseto, G., Gramegna, F., Pinto, A., & Sciascio, E. D. (2017). *Semantic-enhanced blockchain technology for smart cities and communities*. 2.

Sadoghi, M. (2017). *ExpoDB: An Exploratory Data Science Platform*. 1.

Samuel, S. S. I. (2016). A review of connectivity challenges in IoT-smart home. *Big Data and Smart City (ICBDSC), 2016 3rd MEC International Conference on*, 1–4.

Sánchez, L., Elicegui, I., Cuesta, J., Muñoz, L., & Lanza, J. (2013). Integration of Utilities Infrastructures in a Future Internet Enabled Smart City Framework. *Sensors*, *13*(11), 14438–14465. https://doi.org/10.3390/s131114438

Sanchez, L., Galache, J. A., Gutierrez, V., Manuel, J., Bernat, J., Gluhak, A., & Garcia, T. (2011). *SmartSantander: The meeting point between Future Internet research and experimentation and the smart cities*. 9.

Santana, E. F. Z., Chaves, A. P., Gerosa, M. A., Kon, F., & Milojicic, D. (2016). Software Platforms for Smart Cities: Concepts, Requirements, Challenges, and a Unified Reference Architecture. *ArXiv:1609.08089 [Cs]*. http://arxiv.org/abs/1609.08089

Santos, A. P. (2015). *Cidades do Futuro: Talento, Inovação e Colaboração*. 20.

Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M., & Oliveira, A. (2011). Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation. Em J. Domingue, A. Galis, A. Gavras, T. Zahariadis, D. Lambert, F. Cleary, P. Daras, S. Krco, H. Müller, M.-S. Li, H. Schaffers, V. Lotz, F. Alvarez, B. Stiller, S. Karnouskos, S. Avessta, & M. Nilsson (Eds.), *The Future Internet* (Vol. 6656, pp. 431–446). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-20898-0_31

Schelini, P. W. (2006). Teoria das inteligências fluida e cristalizada: Início e evolução. *Estudos de Psicologia (Natal)*, *11*(3), 323–332. https://doi.org/10.1590/S1413-294X2006000300010

Schleicher, J. M., Vogler, M., Dustdar, S., & Inzinger, C. (2016). Enabling a Smart City Application Ecosystem: Requirements and Architectural Aspects. *IEEE Internet Computing*, *20*(2), 58–65. https://doi.org/10.1109/MIC.2016.39

Schwartz, D., Youngs, N., & Britto, A. (2014). *The Ripple Protocol Consensus Algorithm*. 8.

Scuotto, V., Caputo, F., Villasalero, M., & Del Giudice, M. (2017). A multiple buyer – supplier relationship in the context of SMEs' digital supply chain management. *Production Planning & Control*, *28*(16), 1378–1388. https://doi.org/10.1080/09537287.2017.1375149

Sewell, J. E., & Fraser, D. J. (2019). *A Conceptual and literature review of the effectiveness BREEAM*. 12.

Shaghaghi, A., Kaafar, M. A., Buyya, R., & Jha, S. (2018). Software-Defined Network (SDN) Data Plane Security: Issues, Solutions and Future Directions. *ArXiv:1804.00262 [Cs]*. http://arxiv.org/abs/1804.00262

Shaikh, T., Ismail, S., & Stevens, J. D. (2016). Aura Minora: A user centric IOT architecture for Smart City. *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies - BDAW '16*, 1–5. https://doi.org/10.1145/3010089.3016028

Sharma, A., & Bhuriya, D. (2019). *Literature Review of Blockchain Technology*. *6*(1), 8.

Sheikh, N., Khapekar, Ku. T., Kumar, S., & Kumar, V. (2018). *Techniques of E-ticket System: A Review*. *3*(1), 4.

Shyam R., Ganesh H.B., B., Kumar S., S., Poornachandran, P., & Soman K.P. (2015). Apache Spark a Big Data Analytics Platform for Smart Grid. *Procedia Technology*, *21*, 171–178. https://doi.org/10.1016/j.protcy.2015.10.085

Singhal, S., McGreal, S., & Berry, J. (2013). Application of a hierarchical model for city competitiveness in cities of India. *Cities*, *31*, 114–122.

Smith, G., Ofe, H. A., & Sandberg, J. (2016). Digital Service Innovation from Open Data: Exploring the Value Proposition of an Open Data Marketplace. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 1277–1286. https://doi.org/10.1109/HICSS.2016.162

Söderström, O., Paasche, T., & Klauser, F. (2014). Smart cities as corporate storytelling. *City*, *18*(3), 307–320. https://doi.org/10.1080/13604813.2014.906716

Sompolinsky, Y., & Zohar, A. (2013). *Accelerating Bitcoin's Transaction Processing*. 31.

Sonawane, S. A., & Shaikh, S. A. (2017). *Implementing Smart City Concept with Various Application Using IOT Based Technique*.

Song, L., Li, Q., List, G., Deng, Y., & Lu, P. (2017). Using an AHP-ISM Based Method to Study the Vulnerability Factors of Urban Rail Transit System. *Sustainability*, *9*(6), 1065. https://doi.org/10.3390/su9061065

Sousa, J., Bessani, A., & Vukolić, M. (2017). A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform. *arXiv preprint arXiv:1709.06921*.

Spiekermann, S., & Cranor, L. F. (2009). Engineering Privacy. *IEEE Transactions on Software Engineering*, *35*(1), 67–82. https://doi.org/10.1109/TSE.2008.88

Stanford-Clark, A., & Truong, H. L. (1999). *MQTT For Sensor Networks (MQTT-SN) Protocol Specification*. 28.

Stephen, R., & Alex, A. (2018). A Review on BlockChain Security. *IOP Conference Series: Materials Science and Engineering*, *396*, 012030. https://doi.org/10.1088/1757-899X/396/1/012030

Strass, G., & Williamson, J. (2014). Five Best Practices to Improve Building Management Systems (BMS) Cyber Security. *Schneider Electric White Paper*, 11.

Streitz, N. A., Rocker, C., Prante, T., van Alphen, D., Stenzel, R., & Magerkurth, C. (2005). Designing smart artifacts for smart environments. *Computer*, *38*(3), 41–49. https://doi.org/10.1109/MC.2005.92

Suarez-Albela, M., Fernandez-Carames, T. M., Fraga-Lamas, P., & Castedo, L. (2018). A Practical Performance Comparison of ECC and RSA for Resource-Constrained IoT Devices. *2018 Global Internet of Things Summit (GIoTS)*, 1–6. https://doi.org/10.1109/GIOTS.2018.8534575

Teixeira, J., Fernandes, P., Bandeira, J. M., & Coelho, M. C. (2017). *Information Management for Smart and Sustainable Mobility*. 19.

Telles, M. J. (2017). *Um Modelo Computacional para Cidades Inteligentes Assistivas*. *10*(1), 28.

Temple, W. G., Li, Y., Tran, B. A. N., Liu, Y., & Chen, B. (2017). Railway System Failure Scenario Analysis. Em G. Havarneanu, R. Setola, H. Nassopoulos, & S. Wolthusen (Eds.), *Critical Information Infrastructures Security* (Vol. 10242, pp. 213–225). Springer International Publishing. https://doi.org/10.1007/978-3-319-71368-7_18

Travizano, M., Minnoni, M., Ajzenman, G., Sarraute, C., & Penna, N. D. (2018). *Wibson: A decentralized marketplace empowering individuals to safely monetize their personal data*. 18.

Trindade, E. P., Hinnig, M. P. F., da Costa, E. M., Marques, J. S., Bastos, R. C., & Yigitcanlar, T. (2017). Sustainable development of smart cities: A systematic review of the literature. *Journal of Open Innovation: Technology, Market, and Complexity*, *3*(1). https://doi.org/10.1186/s40852-017-0063-2

Tyrinopoulos, Y., & Aifadopoulou, G. (2008). *A complete methodology for the quality control of passenger services in the public transport business*. *38*, 16.

Uceda-Sosa, R., Srivastava, B., & Schloss, R. J. (2011). Building a highly consumable semantic model for smarter cities. *Proceedings of the AI for an Intelligent Planet on - AIIP '11*, 1–8. https://doi.org/10.1145/2018316.2018319

UGI. (2004). *Urban Governance Index (UGI): Methodology Guidelines*. UN-Habitat. http://mirror.unhabitat.org/downloads/docs/2232_55927_Addendum%20-%20Methodology%20Guidelines.doc

UN-Habitat. (2013). *STATE OF THE WORLD'S CITIES 2012/2013—Prosperity of cities*. Routledge [u.a.]. http://mirror.unhabitat.org/pmss/getElectronicVersion.aspx?nr=3387&alt=1

Vaishnavi, V. K., Vaishnavi, V. K., & Kuechler, W. (2015). *Design Science Research Methods and Patterns: Innovating Information and Communication Technology, 2nd Edition* (0 ed.). CRC Press. https://doi.org/10.1201/b18448

van Lierop, D., & El-Geneidy, A. (2016). Enjoying loyalty: The relationship between service quality, customer satisfaction, and behavioral intentions in public transit. *Research in Transportation Economics*, *59*, 50–59. https://doi.org/10.1016/j.retrec.2016.04.001

Vasin, P. (2014). *BlackCoin's Proof-of-Stake Protocol v2*. 2.

Venable, J. R. (2006). *The Role of Theory and Theorising in Design Science Research*. 18.

Venable, J. R., Pries-Heje, J., & Baskerville, R. (2017). *Choosing a Design Science Research Methodology*. 11.

Vilajosana, I., Llosa, J., Martinez, B., Domingo-Prieto, M., Angles, A., & Vilajosana, X. (2013). Bootstrapping smart cities through a self-sustainable model based on big data flows. *IEEE Communications Magazine*, *51*(6), 128–134.

Vujicic, D., Jagodic, D., & Randic, S. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*, 1–6. https://doi.org/10.1109/INFOTEH.2018.8345547

Walls, J. G., Widmeyer, G. R., & El Sawy, O. A. (1992). Building an information system design theory for vigilant EIS. *Information systems research*, *3*(1), 36–59.

Walters, D. (2011). Smart cities, smart places, smart democracy: Form-based codes, electronic governance and the role of place in making smart cities. *Intelligent Buildings International*, *3*(3), 198–218. https://doi.org/10.1080/17508975.2011.586670

Wang, Haifeng, Zhao, N., Ning, B., Tang, T., & Chai, M. (2018). Safety monitor for train-centric CBTC system. *IET Intelligent Transport Systems*, *12*(8), 931–938.

Wang, Huaiqing, Chen, K., & Xu, D. (2016). *A maturity model for blockchain adoption*. 5.

Wang, W., Hoang, D. T., Xiong, Z., Niyato, D., Wang, P., Hu, P., & Wen, Y. (2018). A Survey on Consensus Mechanisms and Mining Management in Blockchain Networks. *ArXiv:1805.02707 [Cs]*. http://arxiv.org/abs/1805.02707

Wei, Y., Huang, C., Li, J., & Xie, L. (2016). An evaluation model for urban carrying capacity: A case study of China's mega-cities. *Habitat International*, *53*, 87–96. https://doi.org/10.1016/j.habitatint.2015.10.025

Wohrer, M., & Zdun, U. (2018). Smart contracts: Security patterns in the ethereum ecosystem and solidity. *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, 2–8. https://doi.org/10.1109/IWBOSE.2018.8327565

Wolisz, H., Böse, L., Harb, H., Streblow, R., & Müller, D. (2014). *CITY DISTRICT INFORMATION MODELING AS A FOUNDATION FOR SIMULATION AND EVALUATION OF SMART CITY APPROACHES*. 9.

Wood, G. (2019). *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER*. 39.

Wust, K., & Gervais, A. (2018). Do you Need a Blockchain? *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 45–54. https://doi.org/10.1109/CVCBT.2018.00011

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., & Rimba, P. (2017). A Taxonomy of Blockchain-Based Systems for Architecture Design. *2017 IEEE International Conference on Software Architecture (ICSA)*, 243–252. https://doi.org/10.1109/ICSA.2017.33

Yan, F., Gao, C., Tang, T., & Zhou, Y. (2017). A Safety Management and Signaling System Integration Method for Communication-Based Train Control System. *Urban Rail Transit*, *3*(2), 90–99. https://doi.org/10.1007/s40864-017-0051-7

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal*, *4*(5), 1250–1258. https://doi.org/10.1109/JIOT.2017.2694844

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. *PloS one*, *11*(10), e0163477.

Yuan, Y., & Wang, F.-Y. (2016). Towards blockchain-based intelligent transportation systems. *Intelligent Transportation Systems (ITSC), 2016 IEEE 19th International Conference on*, 2663–2668.

Zamfir, V. (2015). *Introducing Casper "the Friendly Ghost"*. https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine*, *55*(1), 122–129. https://doi.org/10.1109/MCOM.2017.1600267CM

Zhang, M. (2017). DECISION SUPPORT APPROACH FOR INTEGRATED MAINTENANCE PROGRAM OF URBAN RAIL TRANSIT. *International Journal of Computing*, *16(3)*, 143–151.

Zheng, Q., Li, Y., Chen, P., & Dong, X. (2018). An Innovative IPFS-Based Storage Model for Blockchain. *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, 704–708. https://doi.org/10.1109/WI.2018.000-8

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017a). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017b). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

Zhou, K., Fu, C., & Yang, S. (2016). Big data driven smart energy management: From big data to big insights. *Renewable and Sustainable Energy Reviews*, *56*, 215–225. https://doi.org/10.1016/j.rser.2015.11.050

Zygiaris, S. (2013). Smart City Reference Model: Assisting Planners to Conceptualize the Building of Smart City Innovation Ecosystems. *Journal of the Knowledge Economy*, *4*(2), 217–231. https://doi.org/10.1007/s13132-012-0089-4

Zyskind, G., Nathan, O., & Pentland, A. «Sandy». (2015). *Decentralizing Privacy: Using Blockchain to Protect Personal Data*. 180–184. https://doi.org/10.1109/SPW.2015.27

ANEXOS

Anexos

Anexo I - Quadro comparativo de Plataformas *Blockchain*

ANEXO I

Anexo I - Quadro comparativo de Plataformas *Blockchain*

Nome	Link	Consenso	Funções principais
AWS *Blockchain*	https://aws.amazon.com/pt/*blockchain*/		Oferece uma solução através de plataformas *Blockchain*: Ethereum, Hyperledger Fabric, Quorum e Corda. Modelos AWS *blockchain* para Ethereum e para Hyperledger Fabric Pagamento pelo uso Segurança para as empresas, com os utilizadores poderem adicionar permissões para controlar o acesso aos recursos da AWS. Aceder à atividade do recurso através do AWS *CloudTrail*. Com os AWS *blockchain* Templates, os utilizadores podem implementar rapidamente redes *blockchain* seguras.
Azure BaaS *(Blockchain as a Service*)	https://azure.microsoft.com/en-in/solutions/*blockchain*/		Oferece uma solução através de plataformas *Blockchain*: Ethereum, Hyperledger Fabric, Quorum, Chain e Corda. Modelo do Azure *blockchain* para Ethereum e para Hyperledger Fabric Pagamento pelo uso. Oferece redes e infraestrutura pré-configuradas que permite aos utilizadores iniciarem imediatamente o desenvolvimento dos aplicativos descentralizados. Através de ligações internas às ferramentas do Azure podem validar e interagir com os desenvolvimentos de *blockchain* de maneira mais rápida e fácil. Plataforma na nuvem as soluções são escaláveis.
BigChainDB	https://www.bigchaindb.com/	Federação de nós com permissões de voto	Cada registo é gravado na base de dados *blockchain* sem a necessidade de árvores de Merkle. Apoio a ativos personalizados, transações, permissões e transparência. Consenso Modelo Federação (federação de nós voto). Suporta redes públicas e privadas. Não tem moeda nativa - qualquer ativo, a moeda símbolo ou pode ser emitido. Definir permissões em nível de transação. É *open source*.
BitShares	https://bitshares.org/	Consenso *Delegated Proof-of-Stake* (dPoS)	A plataforma se orgulha de velocidade supersónica transação, de baixo custo e segurança de alto nível. Uma interface *user-friendly*, com base em código *friendly* e extensível, com as características de *smart contracts* financeiros, e uma infraestrutura de testes robusto projetado para evitar *bugs*.
Chain	https://chain.com/	Consenso Federado	Plataforma *blockchain* que adequada para aplicações financeiras. Existe uma edição de desenvolvimento *open-source*. Tipo de rede com permissão Licenciamento com preços para empresas Linguagem suportados Java, Ruby, Node.js Popularidade Média, mas ativamente atualizado em GitHub GitHub Repo SDK-Java (Java) sdk-Rubi (Rubi) sdk-NodeJS (Node.js / Javascript)
Chain Core	http://core-chain.io/	Consenso Federado	Ativos digitais nativos - moedas, títulos etc. Permissões baseadas em funções para a operação, acesso e participação numa rede. Suporte para contas multi-assinatura. Consensos Federados. Suporte para *smart contracts*. Privacidade da transação
CoinList	https://coinlist.co/	Usa um consenso desnecessário de prova de trabalho (PoW).	O objetivo é definir claramente a natureza de uma Oferta Pública Inicial (*ICO- Initial Coin Offering*), portanto, minimizar a possibilidade de violar regulamentos, como os estabelecidos pela *Securities and Exchange Commission* (SEC). O filecoin é como o bitcoin, mas com armazenamento em vez de *hashers*. A nova função de Prova de Replicação cria um serviço de armazenamento útil e valioso como subproduto do processo de mineração.
Corda	https://www.corda.net	As transações confirmadas individualmente por cada um dos participantes de uma transação.	Sem transmissão global de dados através da rede. Consenso conectável (*Pluggable*). Consulta com SQL, permitindo juntar-se às bases de dados externas, as importações em massa.

Nome	Link	Consenso	Funções principais
Credits	https://credits.works/	Créditos usa uma variante da Prova de Participação (PoS)	*Framework* de desenvolvimento para a criação de livros distribuídos com permissão. O consenso baseia-se num algoritmo com poder de voto variável.
Domus Tower *Blockchain*	http://domustower.com/	Qualquer agente que tenha acesso a um *blockchain* tem autoridade 100 para escrever transações para aquela cadeia. A Autoridade é centralizado sob este modelo.	Criação de *blockchains* ligados em que os ativos de uma conta num *blockchain* deve corresponder ao passivo na conta de outro *blockchain*. Capacidade de gravar numa alta taxa de transações de forma escalável. A gravação de balanço de dupla entrada acompanha os créditos e os débitos.
Elements *blockchain* Platform	https://elementsproject.org/	Os rótulos de ativos não fazem parte do consenso do protocolo de rede e são locais apenas para cada nó. Usa-se o valor hexadecimal do ativo, que é partilhado na rede.	Ativos confidenciais - emite vários ativos com identificadores e valores estão "cegos" e auditáveis. Transações confidenciais - mantêm os montantes transferidos visíveis apenas para os participantes da transação e entidades designadas. Códigos de operação adicionais - incluem códigos de operação previamente condicionada (incluindo concatenação e subsequências, mudanças de número inteiro, e várias operações bit a bit), operação que produz um número aleatório dentro de uma gama a partir de uma semente e operação que verifica uma assinatura contra uma mensagem na pilha, em vez da própria operação de gastos. Operações de *blockchain* cruzadas para ser construída de forma descentralizada com fichas para ser movido a partir de um *blockchain* para outro. Blocos assinados - permite que os blocos podem ser assinados criptograficamente e assim pode-se verificar a sua identidade no futuro Segregado da testemunha. A transações bitcoin contêm informações sobre o efeito sobre a contabilidade e os dados que comprovam que a transação é autorizada. Usando segregação da testemunha, os IDs de transação são redefinidos para depender apenas da informação do efeito e dos blocos e comprometer-se separadamente com os dados de testemunhas, evitando a manipulação da transação. Bloqueio de Tempo Relativo que permite que uma transação seja bloqueada no tempo.
EOS	https://eos.io/	Consenso *DPoS* (*Delegated Proof-of-Stake*) e *aBFT* (Tolerância de Falha Bizantina)	Plataforma projetada para permitir que grandes corporações, bancos e governos para construir aplicações descentralizadas.
Eris	https://erisindustries.com/	Consenso de Tendermint	Depende dos tipos que se quer ligar e desligar. Além disso, irá ajudar a desenvolver diretamente um grupo de *blockchain* com permissão para determinados indivíduos. Além de ferramentas de *smart contracts*, permite analisar ação passo a passo. Este software permite que qualquer pessoa presente na plataforma possa criar e executar um aplicativo de qualquer lugar. Qualquer entidade pode utilizar os *smart contracts* para fazer negócios com Eris automaticamente. É *open source*.
Ethereum	https://www.ethereum.org/	Inicialmente PoW e evoluiu PoS na versão 2.0	Ethereum é uma plataforma aberta de *blockchain* que permite a qualquer pessoa criar e utilizar aplicações descentralizadas que funcionam com tecnologia *blockchain*. O Ethereum é adaptável e flexível. A popularidade e atividade é alta e ativamente seguido no GitHub O tipo de rede é público, usa *smart contracts* baseado na moeda Éter. Linguagens suportadas - Python, Go, C ++ GitHub repo - pyethereum (Python) gpethereum (golang) CPP-ethereum (C ++) Disponibiliza uma máquina virtual descentralizada chamada *Ethereum Virtual Machine* (EVM) para completar os *scripts* através da utilização de uma rede global de nós comuns.
Hydrachain	https://github.com/HydraChain/hydrachain	Falha bizantina protocolo de consenso tolerante	HydraChain é desenvolvimento conjunto de tecnologias BrainBot e do projeto Ethereum. O HydraChain é uma extensão da plataforma Ethereum que apoia a criação de aplicações baseadas em *blockchain* escaláveis

Nome	Link	Consenso	Funções principais
			que atendam aos requisitos organizacionais e regulamentares. Popularidade - baixa embora ativo na GitHub Tipo de rede - privada / com permissão *Open Source* Linguagens suportadas - Python, GitHub Repo - hydrachain (Python)
Hyperledger Fabric	https://github.com/hyperledger/fabric	Consenso baseado na PoS (*Proof of Stake*)	Consulta e atualização de diário (*legder*) usando pesquisas baseada em chave, de intervalo e de chave composta. Apenas consultas do histórico. As operações contêm as assinaturas dos pares a endossar. A contabilidade de um canal contém um bloco de configuração definição de políticas, listas de controle de acesso, e outras informações pertinentes. O canal de permite a criptografia venha de diferentes autoridades de certificação
Hyperledger Iroha	https://www.hyperledger.org/projects/iroha	*Sumeragi*, algoritmo de consenso tolerante a falhas bizantino fortemente inspirado pelo algoritmo *B-blockchain*	"Simples e modular" o sistema de diário (*ledger*) distribuído e com destaque no desenvolvimento de aplicações móveis.
Hyperledger Sawtooth Lake	https://sawtooth.hyperledger.org/	Prova de Tempo Decorrido	O Hyperledger é um projeto colaborativo de código aberto criado para avançar tecnologias *blockchain*, de várias industrias: finanças, banca, Internet das coisas, as cadeias de fornecimento, fabrico e tecnologia. Popularidade - alta e ativamente atualizado em GitHub Tipo de rede - tanto privada como público *Open Source* Linguagens suportadas - Python (para Sawtooth Lake)
IBM Bluemix *Blockchain*	https://console.ng.bluemix.net/catalog/services/*blockchain*/	Raft consensus	IBM também lançou sua plataforma *blockchain* que está disponível como parte do catálogo de serviços Bluemix. Usa o projeto HyperLedger e oferece instalações de segurança e infraestrutura adicionais para as empresas. Popularidade - Média, mas ativamente atualizado em GitHub Tipo de rede - Privada / com permissão Preço - plano gratuito limitado e com upgrade pago para o plano empresarial, Linguagens suportadas - GO, Javascript, ibm-*blockchain*-js (Javascript)
*IOT*A	https://www.*IoT*a.org http://*IoT*atoken.com/	consenso *IOT*A da mesma família de algoritmos de consenso como *Snowball*	*IOT*A desvia-se dos projetos de *blockchain* tipo. Altamente escalável, em que o aumento da atividade de rede diminui os tempos de liquidação da transação. Requisitos baixos em recursos, projetado para dispositivos pequenos, como sensores, para participar. Transações de taxa zero. Transferência segura de dados, em que os dados são codificados, permitindo transferência segura de dados, armazenamento e referência. Transações off-line, em que os dispositivos não precisam da conectividade sempre ativa Imune à tecnologia quântica, dado que usa assinaturas especiais, que o torna resiliente à geração de computação quântica. Popularidade Baixa, mas ativamente atualizado em GitHub Tipo de rede - pública, com permissão. Linguagens suportados Python, C, Javascript GitHub Repo *IoT*a.lib.py (Java) ccurl (C) *IoT*a.lib.js (Javascript)
KICKICO	https://www.kickico.com/	A gestão será realizada por votação, com um consenso de 51% entre os eleitores.	Plataforma *blockchain* construída usando *smart contracts* baseados em Ethereum. Oferece soluções abrangentes para ICOs, *crowdfunding*, e *crowdinvesting* usando a tecnologia *blockchain*.
Monax/Hyperledger Burrow	https://monax.io/	*Proof of Stake* (Tendermint)	Baseia o seu funcionamento, em três funções: criar, rastrear e provar. Para criar utiliza um *template* de contrato. Para rastrear utiliza fluxos de trabalho digitais e integrações, acompanha entregas e ativa ações automatizadas. Para provar utiliza relatórios sofisticados para comprovar a conformidade com os requisitos contratuais e a atividade contratual, executa o contrato digitalizado e alimenta os seus negócios com contratos embebidos, do tipo: contratos de não divulgação (*NDA-Non-Disclosure Agreements*), contratos de serviços principais (*MSA-Master Services Agreements)* ,

Nome	Link	Consenso	Funções principais
			declarações de trabalho (SOW), pedidos de alteração (*CO-Change Orders*) e Termos de Serviço (*ToS-Terms of Service*).
Multichain	https://www.multichain.com/	Consenso distribuído entre os validadores do bloco identificado. Idêntico ao de tolerância a falhas bizantina prático, com um validador por bloco.	Suporte multi-moeda nativa. Gestão de Permissão. Implantação rápida. Várias redes podem estar simultaneamente num único servidor. Parâmetro personalizado por rede (tipos de transação permitidos, tempos de confirmação, quantidades mínimas, taxa de transação e os limites de tamanho). Este software ajuda a projetar, implementar e operar diários distribuídos. Esta plataforma permite criar e implantar *blockchains* privados (com permissão *blockchains*) dentro ou entre organizações. Fornece privacidade e controlo dentro de uma rede privada *peer-to-peer*. Trata-se de uma versão melhorada do software de núcleo bitcoin para transações financeiras privadas. Popularidade - Média, mas ativa no GitHub Tipo de rede - Privado, com permissão *Open Source* Linguagens suportadas - Python, C #, JavaScript, PHP, Ruby, GitHub Repo - savior (Python); c# MultichainLib (C#); Multichain-Node (JavaScript); libphp-multichain (PHP); multichain-client (Ruby); savior (Python)
NEM	https://nem.io/	*Proof of Importance* (POI)	O objetivo da troca é fornecer uma plataforma dedicada para ICOs e comercialização de *tokens* com base NEM. Os investidores podem comprar e vender XEM, o criptomoeda NEM e têm a opção de troca.
NXT	https://nxtplatform.org/	Votar no Nxt é importante para chegar a um consenso.	A troca de ativos descentralizada, em sistemas descentralizados de voto e de governança, um *blockchain* gerível e de operações faseadas.
Open Chain	https://www.openchain.org/	Consenso particionado	Adequado para organizações que emitem e gerem ativos digitais. Segue um sistema de consenso particionado, em que cada instância Openchain só tem uma autoridade para validar as transações, dependendo dos recursos que estão sendo trocados. O sistema de conta hierárquica permite definir permissões em qualquer nível. A arquitetura cliente-servidor (centralizada) pode ser mais eficiente e confiável do que uma arquitetura *peer-to-peer*. Popularidade - Media. Ativa no GitHub Tipo de rede - Privada *Open Source* Linguagens suportadas - JavaScript GitHub Repo - openchain-js (Javascript)
Oracle	https://cloud.oracle.com/en_US/*blockchain*	Previstos na plataforma Hyperledger Fabric	Pagamento por uso. Oferece uma solução autónoma, auto segura e auto reparadora. Permite desenvolver a rede *blockchain* e as aplicações na estrutura Hyperledger Fabric. Através do Oracle Integration Cloud pode integrar aplicações locais, Oracle SaaS e aplicações de terceiros. O Enterprise Grade *blockchain* Solution fornece recursos de nível corporativo, como backup integrado, segurança aprimorada, gestão de identidade baseado em função e gestão de revogação de certificado. O *blockchain* da Oracle é fácil de implementar, pois oferece um serviço *blockchain* totalmente gerivel e pré-montado.
Quorum	https://www.goquorum.com/	Algoritmos: RAFT, como o Proof of Stake; IBFT (*Istanbul Byzantine Fault Tolerant*); ou PoA (*Proof of Authority*)	Apresenta privacidade forte em que a informação privada nunca é transmitida para os participantes da rede. Os dados privados são criptografados e partilhados entre as partes interessadas. Consensos: RAFT, IBFT (*Istanbul Byzantine Fault Tolerant*) ou. PoA (*Proof of Authority*) modelo de consensus com identidade na participação. Permissão Defina com flexibilidade como incorporar entidades e utilizadores à sua rede usando o modelo de permissões baseadas em contrato "inteligente" do Quorum. Mapear subentidades para entidades pai para adequar-se à estrutura da sua organização. Integração simples Com o quorum-cloud, você pode implantar facilmente o Quorum em diferentes ambientes de nuvem. Ou use o Docker para integração perfeita entre ambientes.

Nome	Link	Consenso	Funções principais
			Compatibilidade com as ferramentas: TruffleSuite[72], MetaMask[73], Remix[74] e OpenZeppelin[75]. *Open Source*
Stellar	https://www.stellar.org	Stellar Protocolo consenso	Stellar é infraestrutura de pagamentos distribuída que liga bancos, sistemas de pagamento e pessoas. Stellar permite a construção de carteiras móveis, ferramentas bancárias e dispositivos "inteligentes". Fornece servidores HTTP API RESTful chamado Horizon, que ligam a Stellar Core, a base da rede Stellar. *Open Source*
Symbiont Assembly	https://symbiont.io/technology/introducing-symbiont-assembly/	Bizantino tolerância a falhas	Capacidade de lidar com milhares de transações por segundo. Assembly API - JSON padrão através de HTTP.

[72] Truffle - Ferramentas para *smart contracts* - https://www.trufflesuite.com/ , acedido em 15-04-2017

[73] Metamask - Incorpora o Ethereum ao seu navegador - https://metamask.io/ , acedido em 15-04-2017

[74] Remix - Ethereum IDE - https://remix.ethereum.org/ , acedido em 15-04-2017

[75] OpenZeppelin - Framework para criar *smart contracts* seguros - https://openzeppelin.org/, acedido em 15-04-2017

PUBLICAÇÕES

Publicações

No âmbito deste trabalho foram desenvolvidos trabalhos que permitiram apresentar os seguintes três artigos, que foram aceites e publicados.

Artigo 1 - Artigo em conferência

Brandão, A., Mamede, H. S., & Gonçalves, R. (2018). Systematic Review of the Literature, Research on *blockchain* Techno*log*y as Support to the Trust Model Proposed Applied to *Smart places*. Em Á. Rocha, H. Adeli, L. P. Reis, & S. Costanzo (Eds.), *Trends and Advances in Information Systems and Technologies* (Vol. 745, pp. 1163–1174). https://doi.org/10.1007/978-3-319-77703-0_113

Artigo 2 - Artigo em conferência

Brandão, A., Mamede, H. S., & Gonçalves, R. (2019a). A *Smart city*'s Model Secured by *Blockchain*. Em J. Mejia, M. Muñoz, Á. Rocha, A. Peña, & M. Pérez-Cisneros (Eds.), *Trends and Applications in Software Engineering* (Vol. 865, pp. 249–260). https://doi.org/10.1007/978-3-030-01171-0_23

Artigo 3 - Artigo em conferência

Brandão, A., Mamede, H. S., & Gonçalves, R. (2019b). Trusted Data's Marketplace. Em Á. Rocha, H. Adeli, L. P. Reis, & S. Costanzo (Eds.), *New Knowledge in Information Systems and Technologies* (Vol. 930, pp. 515–527). https://doi.org/10.1007/978-3-030-16181-1_49