Government Information Quarterly xxx (xxxx) xxx

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Public service operational efficiency and blockchain – A case study of Companies House, UK

Ali Shahaab [a,*], Imtiaz A. Khan [a], Ross Maude [b], Chaminda Hewage [a], Yingli Wang [c]

[a] Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff CF5 2YB, UK
[b] Companies House, Cardiff CF14 3UZ, UK
[c] Cardiff Business School, Cardiff University, Cardiff CF10 3EU, UK

ARTICLE INFO

Keywords:
Blockchain
Distributed ledger technology
Public service operation
Design science
Case study

ABSTRACT

Despite the increasing interest and exploration of the use of blockchain technology in public service organisations (PSOs), academic understanding of its transformative impact on the operational excellence of PSOs remains limited. This study adopts an action design science research methodology to develop a proof of concept (POC) blockchain based application for Companies House, a government agency that is registering companies across UK. The application addresses the operational challenges of Companies House as well as issues citizens face when accessing its services. We draw from the public value framework proposed by Twizeyimana and Andersson (2019) and demonstrate the significance of the emerging blockchain technology in relation to their democratic practices based on six dimensions. We further discuss the related challenges and barriers for its implementation and evaluate the POC with the stakeholders of Companies House. We also present an illustrative case study, where we explored the appropriateness of the POC in relation to the draft legislation, "Registration of Overseas Entities and Beneficial Owners" (ROEBO) bill which proposes the introduction of a register of the beneficial owners of overseas legal entities that own real estate in the UK. Our research is one of the few studies that will provide in-depth empirical insights about the relationship between blockchain and operational excellence of PSOs.

1. Introduction

Since the publication of the Bitcoin white paper (Nakamoto, 2008), the potential of blockchain and other[1] distributed ledger technologies (DLT) has been increasingly recognised. Public sector has been at the forefront of active explorations and experimentations of blockchain technology (Karanjia et al., 2017). For instance, Georgia and Ghana have been piloting the use of blockchain technology for land registry (Eder, 2019). UAE has been capitalising on the blockchain technology to transform 50 % of government transactions into the blockchain platform since 2018 and expects to save 77 million work hours annually. One notable area of application is its Roads and Transport Authority initiative which aims to create a vehicle lifecycle management system using blockchain by tracking ownership, sale and accident history from the manufacturer to the scrap yard (Blockchain in the UAE government - The Official Portal of the UAE Government, 2021). Germany has recently launched its blockchain enabled *German Digital Health Passport* programme to record COVID-19 vaccination certificate and tests (EU Blockchain Observatory and Forum, 2021).

Despite the ongoing exploration of blockchain technology by government agencies across the globe, academic understanding of its transformative impact on the operational excellence of public sector organisations is rather limited (Ølnes, Ubacht, & Janssen, 2017; Rodríguez Bolívar & Scholl, 2019; Tan, Mahula, & Crompvoets, 2021). Our study aims to fill this void by investigating the potential impact of a blockchain based application on operational excellence of public service organisations, especially in relation to cross-organisation information interoperability and user experience improvement.

* Corresponding author.
E-mail address: ashahaab@cardiffmet.ac.uk (A. Shahaab).

[1] DLT is an umbrella term referring to the approach of distributed, decentralised database systems which are managed by various participants. Blockchains, Direct Acyclic Graphs (DAGs), Block-DAGs, Redix, Tempo and others (details are out of the scope of this manuscript) are examples of DLTs. Blockchain technology is the most well-known DLT, to a point that DLTs and Blockchains are often being referred interchangeably. Not all DLTs are blockchains, however, all blockchains are DLTs.

https://doi.org/10.1016/j.giq.2022.101759
Received 7 September 2021; Received in revised form 15 August 2022; Accepted 18 August 2022

This study adopts an action design science research methodology to develop a POC blockchain based application for Companies House, the UK's executive agency that is registering companies across UK since 1844 and currently holds over 4.7 million company records (Companies House, 2021). The application addresses the operational challenges of Companies House as well as issues citizens face when accessing its services. This study demonstrates how such an application can improve operational efficiency, control over data interoperability and effective use of data to address challenges such as fraud detection, tax evasion, data security and privacy. Given the emergent and disruptive nature of blockchain technology, we start to observe increasing efforts from scholars trying to make sense of how blockchain can be deployed in PSOs. Since most studies are conceptual in nature (Hyvärinen, Risius, & Friis, 2017; Ølnes et al., 2017; Rodríguez Bolívar & Scholl, 2019; Tan et al., 2021; Warkentin & Orgeron, 2020), thus offer limited insights as to how exactly blockchain can add value to PSOs. Of the very few studies that do offer empirical insights (Akaba, Norta, Udokwu, & Draheim, 2020; Treiblmaier & Sillaber, 2020), they do not primarily focus on the operational management of PSOs or developing a tangible technical solution (for instance Akaba et al., 2020). Our research is one of the few qualitative studies that provide in-depth empirical insights about the relationship between blockchain and operational excellence.

The rest of paper is structured as follows. Section 2 provides the background information about blockchain technology and its application in PSOs. It further discusses the distinct differences between PSOs and private organisations and introduces the public value framework that evaluates the impact of e-government initiatives. Section 3 discusses the case background and our research methodological approach. Section 4 provides a detailed account of our research findings. Section 5 evaluates the POC in relation to ROEBO bill and section 6 discusses their significance and concludes with an acknowledgement of our limitations and future research opportunities.

2. Background literature

2.1. A brief introduction about blockchain and its developments

Blockchain technology is a shared, distributed ledger of records or transactions that is open to inspection by every participant but not subject to any form of central control (Bashir, 2017). The ledger consists of blocks of timestamped data which are cryptographically linked together in such a way that each new block points to the block prior to it, making a chain like formation, appropriately named, the blockchain (Chatterjee, Shahaab, Gerdes, Martinez, & Khatiwada, 2021). This chain of blocks of data (ledger of transactions) is distributed between the nodes (computers) participating in the blockchain network so that everyone has the same copy of the ledger, adding to the security and reliability of the network. Whenever a new block of data is created, it is broadcasted to each participant in the network, where each participant then verifies and validates the block and appends it to the existing chain of blocks. At its core, blockchain aims to establish trust in a peer-to-peer fashion without enforcing a master-slave relationship between parties or involving a trusted third party (Chatterjee et al., 2021).

Essentially, anything of value can be transacted on this distributed and decentralised network, in a peer-to-peer fashion. For example, it can be cryptocurrencies like Bitcoin, virtual adorable and rare pets like CryptoKitties (*CryptoKitties | collect and breed digital cats*!, 2021), purely digital artworks (Christies, 2021), proof of existences or automated rules to create future value such as decentralised autonomous organisations (DAOs) (Buterin, 2014).

All blockchains are distributed (processing is shared across multiple, geographically distributed nodes), but not all are decentralised. The level of decentralisation (there is no single point in the network where decision is made) can be controlled based on the participation and business use cases. The three main categories of blockchains based on the access control and centralisation are public, private or consortiums and hybrid blockchains (Kaur, Nayyar, & Singh, 2020). A public-permissionless blockchain allows everyone to participate in the network, take part in the consensus process and transact on the blockchain. This public, permissionless and borderless structure allows public blockchains to be of high censorship and alteration resistant, while simultaneously allowing for decentralised governance. Public blockchains must have an economic incentive for the nodes to support the blockchain network, therefore a user must always pay a transaction fee whenever they use the public blockchain (Shahaab, Lidgey, Hewage, & Khan, 2019). Bitcoin and Ethereum (Buterin, 2014) are typical examples of public blockchains.

Private and consortium blockchains (also broadly known as permissioned blockchains) only allow a selected group to participate in the network and consensus process. Private/consortium blockchains are more suitable for organisations where certain level of trust already exists among the participants and they can rely on a trust model based on the authority of the trusted participant. Since there is a business incentive for organisations to setup a private/consortium blockchain, they do not need to be incentivised in some sort of monetary forms such as transaction fees, to support the blockchain network (A. Shahaab et al., 2019).

A hybrid blockchain setup can be achieved by using a combination of public and private blockchains. It allows users to set rules on what interactions or transactions are to be made on the permissionless ledger (public blockchain) and where to apply restriction and keep information private on a permissioned ledger (private blockchain). For example, a government agency may want to award a contract on a public blockchain for the sake of transparency but would prefer sharing information with law enforcement regarding an investigation on the private distributed ledger. Hybrid blockchain setups can be an attractive choice as they strike an ideal balance between transparency, privacy and scalability, given the current technological limitations of public blockchains. (World Economic Forum, 2020). As discussed in the following section, blockchain deployments by public service organisations tend to fall into either the permissioned or the hybrid category.

2.2. Blockchain deployment in public services

The 21st century citizens expect a simple and hassle-free interaction with their state and relevant public services. PSOs are undergoing rapid digital transformation, automating their processes to provide better and faster public services. The concept of e-government is not new but the emergence of blockchain technology adds extra value to public service provision and operation, thanks to its unique attributes in enhanced transparency, security, and immutability. Therefore, it has the potential to improve public services efficiencies and accountability, filling the increasing trust gap between individuals and governments, a long existing issue and concern for democratic governance and public administration (Bouckaert, 2012; Ali Shahaab, Maude, Hewage, & Khan, 2020a; Thijs, Hammerschmid, & Palaric, 2017; Tolbert & Mossberger, 2006).

Researchers argue that blockchain has great potential benefits for the government such as data integrity, transparency, avoidance of fraud and manipulation, reducing corruption, and enhancing trust, security, and privacy (Ølnes & Jansen, 2017). For instance, Hyvärinen et al. followed a design science approach to develop and evaluate a blockchain based system to increase transparency in the dividend flow and reduce tax fraud, from the Danish government perspective (Hyvärinen et al., 2017). Their solution assists in the verification of tax refund entitlement and facilitates information exchange among tax authorities. The United State Health and Human Services (HHS) department has built a blockchain based application *Accelerate*, to better manage a portfolio of over 100,000 contracts worth approximately USD 25 Billion, across 50 systems. The *Accelerate* project forecasts a saving of up to USD 720 Million (Clavin et al., 2020). The landscape of blockchain in public services focuses mainly in the areas of healthcare, voting, cryptocurrency, asset registry, tax filing, bank transactions and identity management

(Karanjia et al., 2017). Table 1 summarises some of the notable use cases in recent years. Please note as most active use cases in PSOs are yet to see their way into the academic literature and most are still at piloting stages, there is a high level of uncertainty associated with the current blockchain development. Therefore, we do not intend to provide a systematic literature search of the use cases, nor is it within our research remits. Rather we draw popular examples from practice in the public domain and use these popular use cases to provide useful indications on the latest developments.

Given the emergent and diverse nature of blockchain adoption in PSOs as discussed above, it is important to understand the mechanisms how blockchain may transform PSO operations. In the following section, we will firstly discuss the unique characteristics of PSO operations management when compared with private organisations and then introduce the theory of public value as our theoretical lens to guide our research.

2.3. Public service operation management and the theory of public value

Radnor and Noke point out that though public and private sectors bear similar operations management (OM) functions, there are distinct differences between them, in that public sector OM is more complex, addressing key issues of equity, transparency, and probity within a political context (Radnor & Noke, 2013). PSOs are not producing technically designed and manufactured products but rather delivering intangible services that require attention to the processes of service delivery and to relationships with a diverse group of service users, and not simply to service design (Osborne, Radnor, Kinder, & Vidal, 2015). Private service organisations are principally accountable to their owners and are driven by 'hard' financial performance indicators such as profitability. Unlike the private organisations, the key purposes of PSOs' service delivery are to fulfil the interests of society, create and sustain citizen satisfaction. Therefore financial indicators are not primary drivers that dictate how PSOs operate (Boyne, 2002; Radnor & Noke, 2013).

The notion of the *New Public Governance* further argues that PSOs need to not only internally focus on administrative efficiencies but also externally focus on service users, inter-organisational relationships, and public value (Osborne, 2010; Osborne, Radnor, & Nasi, 2013). Organisational performance in PSOs is widely recognised as more complex, multi-dimensional, typically including both internal and external focused measures such as cost, efficiency, service quality, quality of outputs, responsiveness to service needs, equity and accountability (Andrews & van de Walle, 2013; Igalla, Edelenbos, & van Meerkerk, 2020; Walker, 2013). Those goals such as equity and accountability stem from the common ownership of public organisations and from attempts to control PSOs behaviours in order to achieve collective purpose (Boyne, 2002).

Public value is a key factor that differentiates PSOs from private sector organisations, and can be regarded as citizen's collective expectations in respect to government and public services (Moore, 1995). The theory of public value was conceptualised by Moore (1995) and has since been widely explored in public administration studies (Alford & O'Flynn, 2009; Bannister & Connolly, 2014; Jos & Tompkins, 2009; Scott, Delone, & Golden, 2016; Twizeyimana & Andersson, 2019). Public value stresses that PSOs do not only limited to produce public goods but also need to actively seek to generate the outcomes that are meaningful, desirable or perceived useful by their recipients, i.e. creating 'value' (Alford & O'Flynn, 2009). Public value is dynamic as citizen's aspirations can vary over time (Panagiotopoulos, Klievink, & Cordella, 2019), and it is also contingent upon the task environment and the context of the material and social problems that arise in that environment (Alford, 2008). Therefore, public value must be evaluated in the particular context where it was created. The public value theory is also seen as vital to assess the social and political dimensions (hence should not only focus on efficiency gains) of ICT adoption in the public

Table 1
Use cases of implementation of blockchain technology in different countries and their impact.

Use case	Problem to address	Aim of Blockchain	Impact
The U.S Health & Human Services (Rivers, 2018)	Better management of $25B worth of 100,000 contracts	Streamline the procurement process of products and services from private vendors.	Improved Data sharing, transparency, Potential saving of over $720 M over time
U.S. Centers for Disease Control and Prevention (CDC) (Melendez, 2018)	How to trace health outbreaks efficiently?	Automatically collect data in secure way and audit trail of data accessed.	A more Reliable digital trail. Improved traceability and surveillance.
BenBen – Ghana (Ameyaw & de Vries, 2021) *(A similar project has been piloted in Georgia as well* (Eder, 2019)*)*	Inefficiencies in land registry	Digitised and incorruptible ledger of land ownership, lowering risk for all stakeholders in the land transaction process.	Average time to confirm land entitlement reduced from 1 year to 3 months. Real time access, collaboration
The Danish Tax Administration (Berryhill, Bourgery, & Hanson, 2020) (A similar approach has been adapted by UAE) (Blockchain in the UAE government - The Official Portal of the UAE Government, 2021)	How to provide trusted information about vehicles' history?	Automatic Tax collection on vehicle sales and reduce fraud in vehicles' life cycle by providing immutable log of vehicle's lifespan.	Minimize existing operation costs by eliminating manual processes. Data consistency, security and integrity.
Pharmaceutical drugs supply chain –government led project in India (Roy, Kumar, Mahindru, Shukla, & Sharan, 2020)	Counterfeit drugs in the pharma supply chain	Store and retrieve large amount of data associated to a drug and its movement in the supply chain, reducing possibility of tampering and allowing several stake holders to collaborate on a decentralised platform.	Reduced dependency on intermediaries and improved reputation of pharma industry. Transparency, efficiency and reliability, collaboration.
Gross Settlement – BoE led by UK Bank of England (PWC, 2019)	Current infrastructure being the single point of failure in the UK banking settlement process	Allow multiple parties to process gross settlement contracts.	Resiliency, visibility, integrity and efficiency
The Transparency Project– Colombia and WEF (World Economic Forum, 2020)	How to tackle corruption in public procurement (Public school meals for vulnerable children).	Transparent vendor bidding and selection of public procurement contracts	Public sector transparency and reduction of corruption, automation, immutable audit log, disintermediation, enhanced citizen engagement.
South Tyrol – Italy (	How to streamline the complex	Vet applications of telecom companies and	Leaner, service oriented administration, trust

(*continued on next page*)

Table 1 (*continued*)

Use case	Problem to address	Aim of Blockchain	Impact
Treiblmaier & Sillaber, 2020)	administration process around building and modifying cell towers	trace workflows, demonstrating that right level of expertise were employed.	in public institutions, efficiency, transparency

sector, which are often not accounted for in private sectors (Cordella & Bonina, 2012).

In the context of recent e-government developments, the public value is considered as the ability of e-government systems to provide improved efficiency in government, improved services to citizens, and social values such as inclusion, democracy, transparency, and participation (Twizeyimana & Andersson, 2019). Panagiotopoulos et al. (2019) point out that public value theory has been increasingly adopted in the digital government research but there is still lack of theoretical clarity on what public value means and on how digital technologies can contribute to its creation.

Past efforts that attempt to deconstruct what public value entails tend to focus on proposing key indicators, categories or attributes that reflect the various properties of public value, often in the form of taxonomies or conceptual frameworks. While there have been several typologies proposed by scholars in categorising public value, most do not focus on the operations management perspective. For instance, Beck Jorgensen and Bozeman identify 72 public values which they divide into seven constellations, including categories such as relationship between public administrators and politicians, transformation of interests to decisions, and behaviour of public sector employees, etc. (Beck Jørgensen & Bozeman, 2007). These public values are quite comprehensive, and encompass both citizens, users and politics as well as public administration. Bannister and Connolly propose a typology in the context of ICT public value that consists of three categories: duty oriented, service oriented and socially oriented and each category comprised of multiple representative values (Bannister & Connolly, 2014). In a similar vein, Rose et al. proposed a framework of four value ideals: professionalism, efficiency, service and engagement (Rose, Persson, Heeager, & Irani, 2015). Other approaches include examining the public value from ethical, democratic, professional and people perspectives as summarised by Kernaghan (Kernaghan, 2003). Of those notable works, we found that the conceptual model proposed by Twizeyimana and Andersson (2019) is most suitable for our study because of its operations orientation (Twizeyimana & Andersson, 2019).

Via the synthesis of the literature, Twizeyimana and Andersson find that to deliver the public value, e-government initiatives should aim to a) improve the efficiency of the internal functions and processes of government, e.g. connect different departments and agencies, thus making information flow faster and more easy among different agencies; b) open up new possibilities for governments to be more transparent to citizens and businesses (Twizeyimana & Andersson, 2019). The authors further propose six dimensions of the public value and categorise them based on their internal and external orientation (Table 2). Those internal and external orientation share similarity with the operational and strategic public value proposed by Liang, Qi, Zhang, and Li (2019).

Table 2
Six dimensions of the public value of e-government initiatives (Source: Twizeyimana & Andersson, 2019).

Focus	Improved administration (*Internal focused*)	Improved social value (*External focused*)
Dimensions of public value	• Improved administrative efficiency • Open government capabilities • Improved ethical behaviour and professionalism	• Improved public services • Improved trust and confidence in government • Improved social value and wellbeing

In recent years, increasing efforts were placed to ensure data integrity and efficient information exchange (i.e. interoperability) to deliver services to citizens that are effective and open to public scrutiny (Cordella & Paletti, 2019; Panayiotou & Stavrou, 2021; Rose, Persson, & Heeager, 2015; Tan et al., 2021). Furthermore, along with the increasing digitalisation, there are increased cyber threats that exploit PSOs' vulnerabilities and cause significant disruptions to service provision and operations (NCSC, 2018). For instance, cybercrimes such as *WannaCry* outbreak (a worldwide cyberattack targeting a vulnerability in the Microsoft Windows operating system by encrypting data and demanding ransom payments in Bitcoin cryptocurrency) in May 2017 has caused global damages, causing PSOs such as National Health Service, UK £92 m (BBC, 2017). This calls for innovative solutions that help to build organisational resilience and address the aforementioned multi-faceted performance challenges that PSOs are facing. Our research demonstrated how the use of blockchain technology could address such challenges via a case study of Company House, UK.

3. Research methodology

This study adopts an action design science research methodology to develop a POC blockchain based application for Companies House (CH), the UK's executive agency that is registering companies across UK. The application addresses the operational challenges of CH as well as issues citizens face when accessing its services. The main aim of the development of the blockchain application is to improve operational efficiency, control over data interoperability and effective use of data to address challenges such as fraud detection, tax evasion, data security and privacy.

3.1. Companies House perspective

One of the important roles of governments is to maintain and provide trusted information about the assets, organisations, citizens and activities that take place within. Certain agencies are tasked to collect and maintain information such as births, deaths, property transfers, formation, and activities of legal entities. These agencies play an important role in establishing trust and are of vital importance to the economic activities of a country. CH is an example of such agencies.

In the UK, all forms of legally permitted companies are incorporated and registered with CH and are required to submit specific updates during their life cycle. The majority of the data held on a company's register is public data, openly available for anyone to view. CH is required by the Companies Act 2006 to make information available to public under the exemption of paragraph 5 of schedule 2, part 1 of General Data Protection Regulation (GDPR) (ICO, 2018). As of December 2020, there were approximately 4.7 million businesses on the CH register (4.3 million active), and all active companies must submit their accounts and reports each year (Companies House, 2021). The data on the CH register is used to support millions of business decisions annually, and the register was searched more than 9 billion times in 2019 (Companies House, 2020). CH collects a lot of information about the businesses and about the persons related to those businesses. This includes the personal details like name, nationality, date of birth (only month and year are shown), business occupation correspondence and home address, etc. of the director(s) and people(s) with significant control. It also records nature of business, date of incorporation, last date of accounts confirmation, status of company, charges details and other information regarding the respective company.[2]

[2] Readers are encouraged to visit https://find-and-update.company-information.service.gov.uk/ and search for a company to see the information Companies House holds about the respective company.

CH and other government agencies have expressed several challenges that have hindered the achievement of operational efficiency. In a 2019 consultation on corporate transparency and register reforms, it was noted that the limited nature of cross checks between CH and other public services could be abused by individuals "who report one set of information to CH and different information to other agencies" (Department of Business and Energy & Industrial Strategy, 2019, p. 14). Furthermore, CH acknowledges that the current process of sharing information with specified public services is "overly bureaucratic and expensive" (Department of Business and Energy & Industrial Strategy, 2019, p. 64) and CH is exploring ways to streamline the process for sharing information with different PSOs. Here the aim is to achieve more frequent cross-checks and making it difficult for fraudulent information to be put on the register, allowing them to identify anomalies or suspicious activities.

In a recent consultation from December 2020, the UK government has noted that "file once with government" (Department of Business Energy and Industrial Strategy, 2020, p. 10) was raised by several respondents of the consultation. Suggestions included using a centralised accounts submission standard, so all government bodies receive identical information. Then prepopulating this information in the portals when it has been filed with one organisation, in order to reduce duplicate efforts. The government further admits that the options to achieve "file once with government" have not been fully explored in the past. A joint filing system between Her Majesty's Revenue and Customs (HMRC) and CH was developed but considerable differences between requirements, timings and purpose have proved to be challenging for any further significant progress (Department of Business Energy and Industrial Strategy, 2020).

Getting the right data in the right place at the right time is a fundamental driver of public service provisions and value for money in governments. The UK government agrees that if this can be achieved, it will "improve services, increase efficiency for users, reducing their costs in relation to analysing the data and reduce the risk of fraud occurring" (Department of Business Energy and Industrial Strategy, 2020, p. 11). Furthermore, it has also been observed that "developing cross-government rules, standards and processes to collect, store, record and manage company data will bring benefits for preparers and users of financial information and create efficiencies for government" (Department of Business Energy and Industrial Strategy, 2020, p. 11). The government urges to examine the feasibility of a central source for all public services to extract relevant information or "developing technology that would send the relevant information to each government organisation at the relevant time" (Department of Business Energy and Industrial Strategy, 2020, p. 11).

This recent acknowledgement of the need for having an information sharing system across public services and the drive to explore new technologies in order to have the data available "*at the right time at the right place*", has been the key driver of this case study. This is particularly important in the context of the forthcoming ROEBO bill (discussed in detail in Section 5) that aims to combat money laundering in the UK property market (London in particular) by establishing greater transparency and data interoperability across different government agencies and stakeholders like conveyancing solicitors and civil society.

To address the challenges faced by CH, a joint research project was set up between the authors' institution and CH. Action design science research methodology was adopted. We discuss our detailed research approach in the following section.

3.2. Action design science research approach

Design science research (DSR) methodology is a popular approach in information systems studies and also is being increasingly used in the operations management discipline (Peffers, Tuunanen, & Niehaves, 2018; van Aken, Chandrasekaran, & Halman, 2016; Wang, Chen, & Zghari-Sales, 2021) and public sector studies (Danneels & Viaene, 2015; De Sordi et al., 2021). A typical design science approach follows the structure of problem identification, objective definition, design and development, final demonstration and evaluation (Holmström, Ketokivi, & Hameri, 2009). The DSR paradigm is different from conventional technology adoption studies in the management and IS disciplines which seek to develop and verify theories that explain or predict human or organisational behaviour. It contains dual objectives, a) extend the boundaries of human and organisational capabilities by creating new and innovative artifacts, and b) generate newly designed products and/or process knowledge (Gregor & Hevner, 2013; Iivari, 2020). Wang et al. (2021) argue that it is important to discuss the differences between the two paradigms because "they have different purposes of inquiry and hold different views on what constitutes as academic contributions" (Wang et al., 2021, p. 4). The authors further point out that DSR can make contributions at three levels:

- Level 1. Situated implementation of artifact and practical contribution
- Level 2. Mid-range theory – knowledge as operational principles/architecture (that applies to a specific class of problem situation)
- Level 3. Well-developed abstract scientific theory (i.e. kernel theory (Iivari, 2020)) about embedded phenomena.

Action design science research (ADSR), as one of the popular research genres in DSR, reconciles and integrates the synergies between DSR and action research (Peffers et al., 2018). The intent of ADSR is not to solve the problem per se within a specific organisational context, but to generate knowledge that can be applied to the class of problems that the specific problem exemplifies (Sein, Henfridsson, Purao, Rossi, & Lindgren, 2011). Our ADSR follows an iterative research cycle as demonstrated in Fig. 1, based on the logical stages proposed by Mullarkey and Hevner (2019), Sein et al. (2011) and Wang et al. (2021); We later report our research findings following this logic in Section 4.

- Problem formulation: this involves a clear understanding of the current operations and processes within CH, identifying existing socio-technical artifacts, defining the goals and scope of the ADSR project and selecting relevant guiding theories, i.e. the theory of public value.
- Artifact development and intervention: this entails a set of iterative co-creation activities during the project lifespan with CH in order to develop the most viable blockchain architecture.

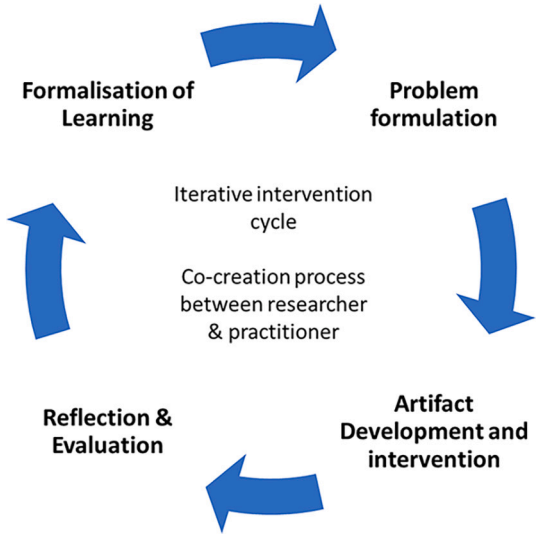


Fig. 1. The ADSR cycle (adapted from Wang et al., 2021).

- Reflection and evaluation: this is an ongoing process in concurrency with the decisions about designing, refining the artifacts and work practices, as well as surfacing anticipated and unanticipated consequences.
- Formalisation of learning: this stage formalises the learning and recognises that the research process goes beyond simply solving a problem for a particular organisation. It develops general solution concepts that can be applied to the same class of field problems.

The official research project started in 2018 and is currently in the final phase. The first author as part of the Welsh Government and European Social fund funded PhD programme was seconded to CH, where he worked with key members of CH to design and co-create the POC. The full academic research team bring their knowledge of theory and technological advances while the practitioners from CH bring practical knowledge of the organisational work practices. The two teams mutually influence each other along the research process. For example, the academic team uses the inputs from the practice team to build the IT artifact, then the practice team will interpret and help to shape its further development in the organisational context.

ADSR is a powerful method where researchers do not remain an observer outside the investigated subject but actively participate in the change of process, which removes the artificiality of splitting out single elements from an integrated system by just observing from the outside (Coughlan & Coghlan, 2002; Foster, 1972). ADSR advances research by solving real world problem and creating knowledge or theory about the action at the same time (Näslund, 2002). A weakness of action or participatory research is the potential lack of objectivity as the researchers may lose their independence due to the close association with the organisation. Through multiple data collection methods and triangulation of research findings, this negative effect can be largely reduced. This mitigation approach has been adopted by our study. Our meeting minutes, interview notes and focus group recordings have been shared with and validated by CH participants. Our main data collection methods and engagement activities include the following;

- Background research from a range of sources such as the CH's website, government reports, articles and blogs published by CH, to understand the context of the case company and its operational challenges.
- Five interviews with staff at the directorate level, to collect information regarding the aims and objectives of the institution, their vision regarding different government policies and regulations.
- Four focus group discussions, which include key members from CH's software development team, data management/analytic team, data integrity team and legal team, to clearly articulate the current state of operations, challenges with existing data management system and service provision, as well as the ideal future state enabled by blockchain.
- Regular iterative discussion and meetings (~ 14) between the academic team and CH stakeholders focusing on requirement analysis such as what architecture and algorithms to be used, and POC development and refinement.

3.3. Action design science research data analysis

Our data analysis began simultaneously with the gathering of data and continued throughout the data collection process and beyond. For instance, the PhD research created a weekly data synthesis log that summarised what he has done in the week and reflected on the progress, theoretical and practical insights gained and developed plan for further actions. Given the large amount of data we have collected, we firstly created a data repository that records the list of data collected and their key information including participants, place and time and duration, as well as a brief description of each set of data.

Our logical step for coding and analysing the data was within-dataset analysis, followed by cross-dataset analysis. We adopted an open coding process to build concepts and categories. Those individual codes were then grouped into categories. For instance, when interviews with directorate staff, key areas of concern regarding operational efficiency and service delivery were identified, for instance lack of cross organisation collaboration and information silos, the importance of legal compliance, as well as input data quality. Those are recorded as our first order codes. Our second order analysis focused on identifying recurrent themes across all five interviews and looked for differences and similarities. Similar codes were then grouped together to form categories. For instance, issues related to input data were grouped together as 'data accuracy and integrity' which later was used to evaluate the impact of blockchain in addressing this particular operational problem. A similar approach was adopted to focus group and regular project meetings analysis.

Following this, we tried to develop a sense of theoretical organisation of those themes into the two public value dimensions proposed by Twizeyimana and Andersson (2019). To improve coding reliability, we focus on consistency between researchers (or inter-rater reliability) and consistency over time with the same researcher. For the former, a minimum of two academic researchers coded the same dataset independently and then compared to resolve any deviations in understanding. For the latter, the PhD researcher would code a clean version of a dataset previously coded, and then compared to see inconsistences. As time progresses, researchers' understanding of the phenomenon improves, we often need to revisit the data and revalidate earlier coded materials, and new codes were added in where necessary, for instance cyber resilience was identified at a later stage of the project as an important contributor to the public value creation.

4. Research findings

4.1. Problem explication and requirement elicitation

Current IT infrastructure of CH introduces three key operational bottlenecks as illustrated by Fig. 2A:

- Repetition/duplication (Fig. 2A (1)): Citizens/companies have to submit nearly identical information to different PSOs. This inefficient process not only increases the cost but also creates room for error and forgery (for instance, contradicting information about turnover of a company could be provided differently to different organisations).
- Interoperability (Fig. 2A (2)): Databases of different PSOs are not in sync in terms of data schema, data format and time. Data dump (a large amount of data transferred from one system or location to another) is usually followed by manual/semi-automatic data curation, which is time consuming, error prone and often insufficient to identify forgery or trace history.
- Traceability (Fig. 2A (3)): With current database structure it is difficult to trace the changes of information of a particular entity (individual/company). Lack of provenance information makes it hard for authorities to trace/investigate individuals or companies when needed.

Following the current state mapping of the existing information architecture, the research team conducted a requirement analysis which serves as the foundation to build the blockchain protocol covering five aspects – architecture & algorithm, legal issues, data integrity, data analytics and data access. The inputs from the key members from the different teams are summarised in Table 3.

4.2. The developed blockchain application

Considering the recent government's calls for action around data transparency, sharing and integrity, a POC was developed using proxy

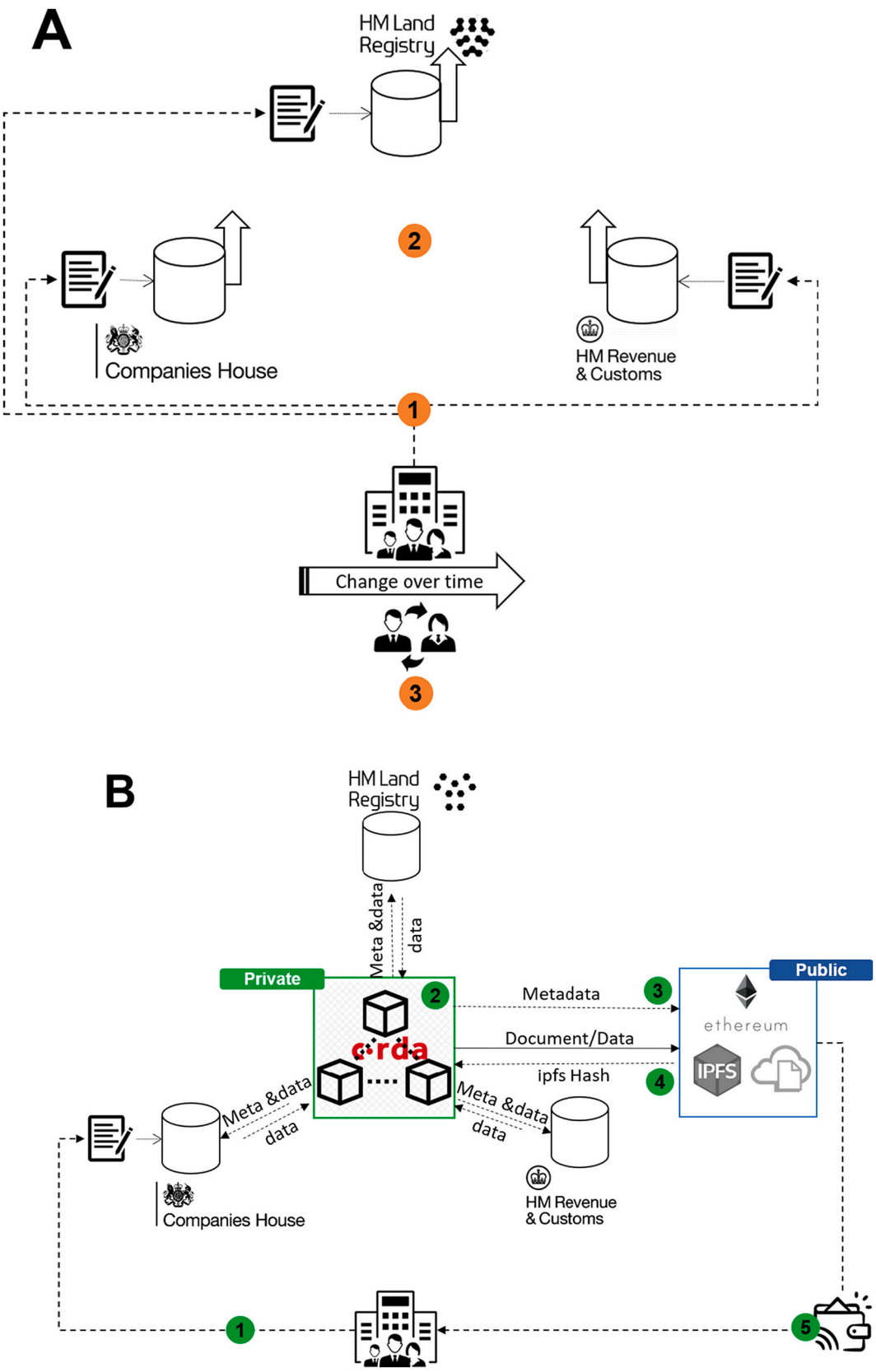


Fig. 2. Impact on operational efficiency and service delivery effectiveness by a private-public hybrid blockchain framework. (A) Illustration of the operational challenges a company and its owner faces while registering, updating its information across three public service organisations. (B) Illustration of different operational efficiencies that can be achieved through a hybrid public-private blockchain framework.

Table 3
Key issues of CH operational challenges identified by the stakeholders from the different teams within CH during the requirement analysis process.

Team	Requirement analysis
Architecture & algorithm	• Strength and bottlenecks about current database structure. • Results from the current exploration initiatives. • Scoping of different DLT architectures (public vs. private) and rationale for effective solution. • Scoping of different consensus algorithms used in DLT. • Security and privacy.
Legal	• Archiving the data within the existing legal & policy framework of CH, especially in context of GDPR. • Destroying the data (as and when required by the law) in an immutable framework like blockchain. • Process of modifying the data within legal boundaries. For example, if someone changes their gender then all historical data need to be re-written. • Strict legal definitions of terms as transactions occur on a DLT. Used "delivery" and "receipt" as example. • Process of supplying data to The National Archive. • Requirements from the UK's Registration of Overseas Entities Bill (Department of Business and Energy & Industrial Strategy, 2018).
Data Integrity	• Data quality assurance and validation process. • Process of addressing data entry mistakes on an immutable structure.
Data Analytics	• Data formats and standards in context of interoperability and analysis. • Distributed data analysis approach.
Data Access	• Alignment with different open data and inter agency data interoperability. • Alignment with Once Only Principle of European Union.

PSOs to explore the potential of using a blockchain system to address the above challenges, and demonstrate how the flow of information among different PSOs could be streamlined. Fig. 2B offers an overview of the blockchain system and Fig. 3 provides screenshots to offer further details of the developed POC. The POC operationalises and supports the 'file once with government' approach, while simultaneously provides the basis for data integrity across multiple registers and allows near real-time (~ 5 s delay) interoperability as illustrated in Figs. 2B and 3. The POC utilises a public-private hybrid blockchain where Ethereum blockchain (Buterin, 2014) is used for data integrity and public verification, whereas, Corda (Grigg, Brown, Carlyle, & Hearn, 2016), a permissioned blockchain has been used for a consortium setup, allowing for private, inter-government data sharing in an automated and real time fashion (Fig. 2B (2)). Corda DLT was carefully chosen because of its enterprise support and point-to-point communication system. Since there is no 'principal ledger' to be maintained in Corda, transactions are only shared on the *need-to-know* basis, ensuring high level of privacy. Furthermore, since Corda was primarily developed for financial institutions (Grigg et al., 2016), it has been designed to operate in highly regulated environments, which is also a primary requirement for PSOs.

The consortium consists of three UK public service nodes representing Companies House (CH), Her Majesty Revenue & Customs (HMRC) and Land Registry (LR) on Corda. The public service nodes track *states* (shared facts which can be updated by transacting on the blockchain) about legal entities registered with CH and the smart contracts[3] govern how the states evolve over time. For example, a company can only be created, updated or dissolved by CH. Similarly, a land title can only be created or transferred by the LR authority. Since Corda allows for sharing information on a *need-to-know* basis, only relevant information is shared with the related stakeholders. This allows for a distributed log of events that can take place in a company's lifespan and with a near real time update to all the relevant parties.

Ethereum blockchain is used to achieve immutability of records and allows the companies/citizens to have a digital record of the verified registry. Since public blockchains are immutable and transactions incur fees, all personal data is kept off chain on an InterPlanetary File System (IPFS). IPFS is a protocol of storing and sharing data on a distributed peer-to-peer file system, and a hash of the data (like a *fingerprint* of the data itself) is posted on to the Ethereum blockchain (Fig. 2B (3)). A hash is a deterministic, lightweight cryptographic proof for the integrity of the data which can be easily calculated and verified. IPFS addresses the content by their hashes known as content identifiers (CIDs), providing a guarantee for the integrity of the data, since slightest change to the data would result in a completely different hash. Instead of IPFS, other cloud or physical data storage systems can also be used, but these systems inherently have the vulnerability of single point of failure.

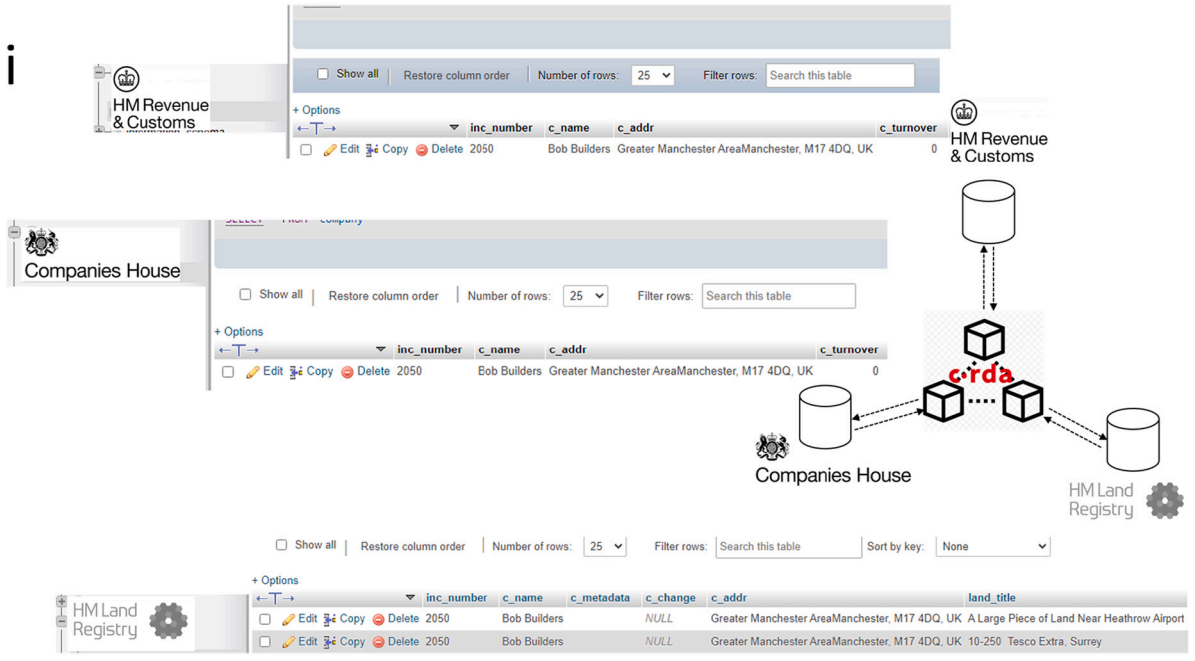
Once the transaction is confirmed on the Ethereum network, the metadata (see Fig. 2B (2)) of the transaction is broadcasted to the stakeholders on the private consortium, along with the pointer to the data stored on IPFS (Fig. 2B (4)). The metadata comprises of the information regarding the transaction added to the public blockchain for the sake of immutability and verification by PSOs or other users of the system. It includes the block information such as block number, transaction hash, block hash and the sender's address on the blockchain. The metadata also includes CID for the retrieval of data (or document) from IPFS. Since IPFS storage is decentralised (i.e. the data is stored in a distributed fashion), it is inherently difficult to tamper or hack since it is not stored on a single server or provider. Citizens also can have this hash in their digital wallet and can use it to access other services (like a mortgage/bank loan) by producing the hash as proof of the verified document (Fig. 2B (5)). This approach will substantially increase the efficiency of the *Know Your Customer* (KYC)[4] process, and will reduce bureaucratic overheads and chances of document fraud.

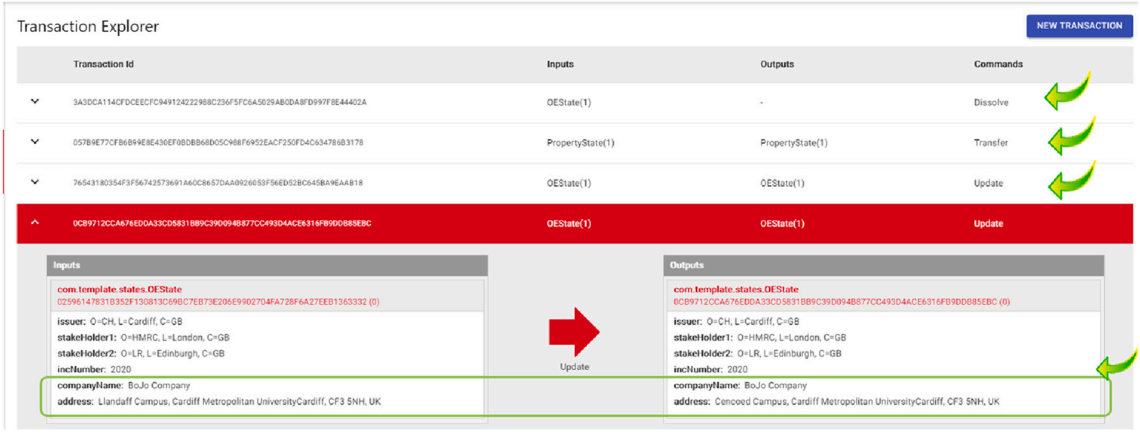
It is worth noting that the developed blockchain application is not there to replace existing native databases but is designed to integrate with the current legacy systems (shown by database icons in Fig. 2B). Here Corda works as a distributed ledger and mediator through which synchronisation and data interoperability among the native databases occurs with the help of the RPC[5] (remote procedure call) clients implemented for each PSO. The RPC client is an observer which subscribes to listen to the blockchain (similar to us subscribing to receive automatic updates from our favourite websites or applications). Any vault updates on the respective node and client-side logic is implemented to translate the events to local systems, updating legal entity's records in native databases, respectively. For example, if a legal entity updates an address with one of the PSOs, the respective PSO invokes the '*Update Legal Entity*' flow and the state of the legal entity is updated across all participating PSOs upon successful execution of the smart contract. The RPC client observer instantly retrieves the update from the respective Corda node and updates the record in the native database (see (Ali Shahaab, Khan, Maude, & Hewage, 2021) for implementation details). Therefore, any update on any of the native databases will update the Corda ledger, which then according to the smart contract will notify the appropriate database(s) that *need-to-know* about this particular update and then ultimately, the relevant database(s) will be updated accordingly. In this case study, there are some activities like change of address, that all three PSOs within the consortium *need-to-know,* yet there are other activities like the declaration of annual turnover that CH and HMRC *need-to-know* but not LR. Likewise, for land purchase or new title activity, LR and HMRC *need-to-know* but not CH.

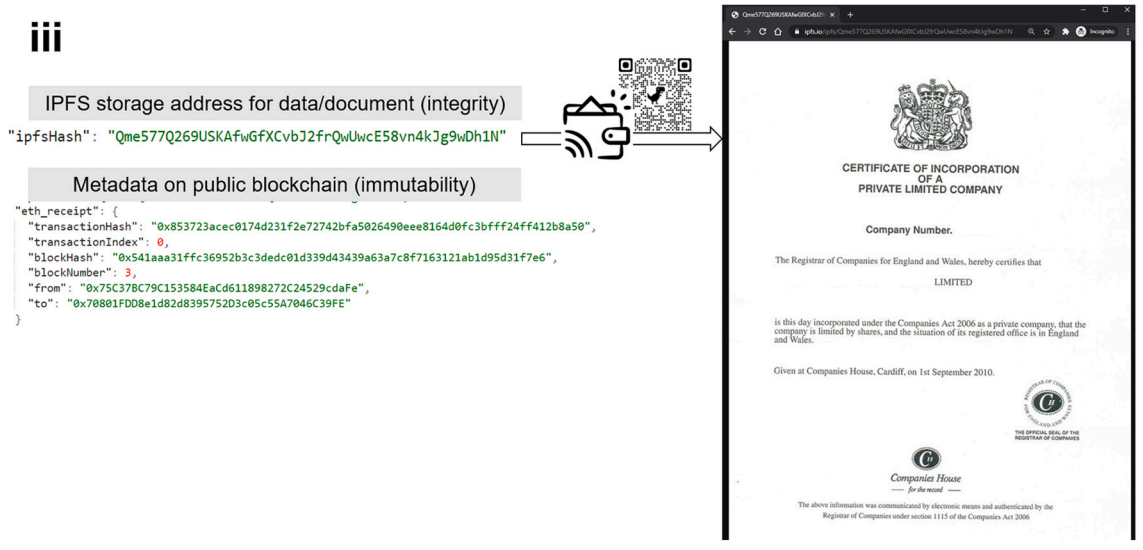
[3] A smart contract is a piece of computer program stored on the blockchain which is intended to automatically execute when predetermined conditions are met.

[4] KYC is the practice carried out by organisations to verify the identity of their clients or users in compliance with legal requirements and current laws and regulations.

[5] RPC is a software communication protocol that a program on one machine can use to request a service from a program located in another computer without knowing that it is remote.







(caption on next page)

Fig. 3. Screenshots of the proof of concept (i) Screenshot of three organisations' native databases integrated and kept in syncronisation with the private blockchain Corda. (ii) Screenshot of the Corda transaction explorer showing different activities happening over time. The expanded pane showing an update of address. (iii) Metadata from a transaction. The IPFS hash can be used to retrieve the associated data/document (in this example the Incorporation Certificate) through a common web browser. The citizen can also keep this IPFS hash in their digital wallet to make a verifiable claim to access other services like bank loan.

The point-to-point communication system of Corda enabled us to dovetail a distributed data management system with an existing siloed data management system. This continuous feedback loop system also allows for synchronisation of states across multiple public services, permitting the user to submit their details once only, with any one of the public registries (Fig. 2B (1)). Furthermore, it significantly mitigates fraud and the costs associated with identifying discrepancies across multiple registers, since all validated changes are propagated across the public services, in near real time. The detailed impact on operational efficiency and the barriers in implementations are discussed in the following sections.

4.3. Impact on operational efficiency and service delivery effectiveness

The POC has been demonstrated to the research collaborators and various stakeholders at CH and the feedback has been very encouraging. The demonstration was undertaken in a sandbox environment, simulating the legacy native databases and events recorded by CH. The system's technical capabilities are based on the physical evidence, when tested and evaluated in such sandbox environment.

CH operates a streaming API which provides access to real-time changes to the information held on companies register. Once a long running connection is established by the receiving party, the streaming API *pushes* the data to the client as it changes. The streaming API is very resource intensive and challenging to maintain. Furthermore, it only allows for one way broadcast of information to the subscribing parties. The technical team (software architects and developers) at CH believes that the "massively complex (data management) architecture" behind providing the streaming connection can be replaced by the "blockchain containing the updates which anyone could tap into". This not only allows the subscribers to obtain a transparent log of events from CH, but also enables them to access the near real-time updates across the whole network of PSOs, without having to subscribe to every single PSO for the updates.

Table 4 summarises the key stakeholders involved along the design science stages and whom we collected the feedback from. Since the design sits outside the existing data management infrastructure, it was classed as "interesting" and "will add value (Senior operations manager)" in the data sharing and update procedures. The improvements enabled by the blockchain system on the operational efficiency are categorised and discussed in the following sessions.

Table 4
Engagement of different stakeholders at different stages of the design and development of the POC.

Stake holders' role at CH	Stage- Inception	Evaluation	Development
Director Level		2 (2–3 persons/ session)	3 (2–3 persons/ session)
Senior Management	3 (2–3 persons/ session)	3 (2–3 persons/ session)	7 (2–3 persons/ session)
Software Architect		2 (3–4 persons/ session)	5 (2–3 persons/ session)
Developer	2 (3–4 persons/ session)	4 (3–4 persons/ session)	7 (3–4 persons/ session)
User	3 (7–9 persons/ session)	2 (3–5 persons/ session)	1 (3 persons/ session)

4.3.1. Data accuracy and integrity

As with private sectors, PSOs increasingly rely on data and information to manage their operations. As such, PSOs can only manage their operations effectively and deliver superior public value if the data they rely on is accurate and free from accidental and malicious alterations. CH understands that the POC will "enhance the data quality" and will be "beneficial for the users to have attested data off the blockchain". The blockchain application has unique advantages to ensure data accuracy and integrity to support PSO operation. These advantages are discussed below:

Once Only Principle: Citizens/companies only need to file or update information with one organisation and the relevant information is automatically updated to other PSOs in near real time. Missing or inaccurate data errors tend to happen when different PSOs require the same company/citizen to submit the same information (but often with a different format and via a different IT system). This leads to one of the most fundamental issues facing digital transformation – data integrity. Without data integrity, the usefulness of the data becomes diminished as any information extracted from it is not reliable for accurate decision making. The senior management at CH has noted that the developed blockchain system "reduces the time and complexities for companies/citizens to submit data and improves their digital experience when interacting with PSOs". It also supports the provision of a "single source of the truth".

The data submitted to PSOs should be validated for their accuracy and checked for accidental and malicious alterations. This is a key requirement to achieve operational efficiency by avoiding the time required for cleaning data and checking the validity by multiple PSOs. If the PSOs are not talking to each other (when they operate in their own data silos or data warehouses), a widespread fraud can take place in one public organisation without being noticed by other related government organisations.

The proposed solution has the potential to enhance the transparency and consistency of data across different PSOs through near time interoperability. It is worth noting that there is "still a need to ensure data" is accurate, before it is submitted to the blockchain. We assume that the transacting PSO (e.g. CH) would have done a validation on the data and other PSOs in the blockchain system would simply verify the transaction against the smart contract. The solution acts as a federated system, namely a single entity (company or citizen) would register with a PSO and another PSO may choose to trust the identities provided by that PSO. Thereby allowing a single entity to only submit its information once whilst its digital identity and credentials are made available to both PSOs.

The proposed solution provides the wider operability, transparency,

Table 5
A summary of how the proposed solution addresses data related concerns.

Issue	How the proposed solution addresses the concerns
Data accuracy	Data validity and accuracy can be verified by any one organisation within the consortium. Once verified and recorded by the organisation, the data is shared with other organisations through the blockchain network, and their native databases record/update the data accordingly.
Data integrity	Data integrity is maintained by the hybrid blockchain structure. Any update of data with any PSO will trigger a *state* change on the permissioned blockchain, which will be notified to other PSOs on near real time basis.
Fraud detection	Citizens or companies cannot present different data to different organisations. Since all PSOs have the same view of the data, any attempt to insert inaccurate data will be visible by all.

scalability, and efficiency across several PSOs in general. Table 5 summarises how the proposed solution addresses the key issues (Table 3) identified by CH stakeholders (Companies House, 2019).

4.3.2. Cross organisation information interoperability

The application clients of the respective nodes can subscribe to '*listening*' for certain activities on the blockchain. As soon as an activity is recorded on the node, the client listening to the blockchain instantly updates relevant information to the native databases of respective organisations. This releases the burden of manual activities such as checking, updating and exchanging information across multiple information systems from the three PSOs. Isolated IT systems or poorly integrated systems often leads to inefficient information sharing, causing delays in actions.

Data interoperability and updates across PSOs in a near real time and in a consistent manner provides a new paradigm for information sharing. In contrast to the traditional data dump (weekly/fortnightly basis), selective parameters of data sets can be shared with selective organisations in a specified format by smart contracts. This reduces the data management and integration overheads, errors, and infrastructure costs for government organisations, whilst it also removes the need for citizens to provide same information redundantly to different government organisations.

4.3.3. Records provenance and user experience improvement

As discussed in Section 4.1, hash pointers of the transactions are posted to the public blockchain (Ethereum) in an immutable manner which also forms the basis for provenance information and traceability. Provenance information accessible from the blockchain application provides the opportunity for PSOs to trace activities of companies and can be used to detect activities such as fraud and tax evasion by utilising a time series data analysis and machine learning algorithms. Effective use of data increases the value of the data and trust for the data.

Seeing the services offered from the outside in – from the citizen/companies' perspective – shifts the internal focus on efficiencies towards a more external focus on the social value and wellbeing creation. While the customer experience design has become the ultimate battleground for many private companies and brands (Bonnet & Westerman, 2021), experience design in PSOs is lagging behind, however as illustrated by our research, it offers a compelling case to transform the user experience and provide added value.

4.3.4. Cyber resilience and legal compliance

Privacy and security are key concerns for PSOs since they determine the usability and effectiveness of the system and ensure equity and legal compliance. These concerns are directly related to the operational efficacy and efficiency due to the fact that the organisations are increasingly exposed to cyber threats such as denial-of-service (DoS) (whereby a server is halted via flooding it with internet traffic) caused by an insider or external threat actors. Those cyber threats could cause severe disruption to operations and service delivery. The recent SolarWinds attack on government agencies and private companies has well demonstrated the disruptive effect on organisations. This cyberattack used SolarWinds Corp (a U.S. tech company)'s network monitoring software as a springboard to compromise a raft of U.S. government agencies (including U.S. Treasury, Justice and Commerce departments and other agencies). The attack exposed sensitive data for eight months before it was detected in December 2020 and affected nearly 18,000 organisations which use SolarWinds' network monitoring software (Abraham & Sims, 2021). It is commented by Microsoft Corp Present Brad Smit as "the largest and most sophisticated attack the world has ever seen" (Reuters, 2021).

The proposed blockchain solution is more resilient and provides more certainty for operation continuity because of its distributed, redundant nature. It has no central master database and can still synchronize and run even if a certain number of nodes are acting maliciously or fail, thus avoiding the single point of failure, a problem inherent in centralised databases. Table 5 or 6 summarises some of the major privacy and security concerns which could affect the cyber resilience and operational efficiency and how the proposed solution can minimize those risks.

Furthermore, the rights of the users around their personal data privacy can be affected if the privacy implications are not addressed. The users of the proposed solution should feel confident that their personal data is always protected, and that their privacy around Personally Identifiable Information (PII) is not at stake at any time. The data protection regulations and laws are emerging across the world since the EU enacted the GDPR regulation protecting EU citizens' personal data. Hence the proposed solution should provide the required guarantee for the protection of personal data unless this data protection is overridden by a legitimate interest or other laws (e.g., Companies Act 2006 requires that all company registration data should be open). Table 6 also highlights how data protection related issues are addressed by the proposed solution.

4.3.5. Scalability

In context of operational efficiency, the scalability refers to the expansion of the proposed blockchain framework to other public services. Here the core benefit is that the proposed blockchain framework is implemented as separate layer to the native data management environment and can be seamlessly extended to other PSOs. Furthermore, Corda DLT allows for point-to-point communication and does not require global participation from all nodes. Therefore, adding more nodes to the network does not impact the performance significantly. When a PSO decides to join the consortium, the *flows* can be updated (*Need to know*) to include the respective PSO in the transaction. For example, the Department of Work and Pension (DWP) may be interested

Table 6
Common privacy and security issues addressed by the POC.

No.	Issues	How the proposed solution addresses the issues
1	Purpose limitation	The purpose of the data can be agreed upon by the gate keepers (participating PSOs) of the proposed solution. Only the data required for inter-PSO sharing will be included.
2	Consent	Consent for data will be taken at the time of data collection. Which will be taken by each individual organisation and the privacy notice will always include the sharing of data among other public organisations for limited purposes such as fraud prevention.
3	Legitimate interest	Data can be granted access to other organisations outside the consortium if there is a valid legitimate reason. For instance, crime agencies may be able to access data in the proposed system for fraud detection. Legitimate Interests Assessment (LIA) needs to be carried out for any violation of individual rights for protecting personal data (e.g. user profiling using the proposed platform).
4	Subject data access	GDPR and other data protection legislations across the globe requires PSOs to provide subject data access. The proposed solution should also provide the access to personal data when the subjects request. This can be efficiently handled through the proposed framework since the data is visible to all gate keepers and provenance will enable subjects easy access to data.
5	Personal data change (e.g. gender change)	The personal data change is enabled in the proposed system. This is important due to individual rights for data access and change requests such as gender change. The law also requires such change to be kept in confidence, i.e. when gender change is made in a blockchain system, the system should not reveal the previous gender. The developed blockchain application can effectively solve this dilemma.

in joining the consortium to mitigate financial frauds committed by the shareholders of the companies which are filing a decent turnover, but the shareholders are fraudulently claiming state benefits. To accommodate this need, the flows can be updated to include DWP as a party in the finance related transactions. The technical solution demonstrated through this POC thereby strives to overcome the challenges of two scaling options – replication or coordinated implementation proposed by Allessie, Pignatelli, Sobolewski, and Vaccari (2019).

Linking back to the public value dimensions suggested by Twizeyimana and Andersson (2019) as discussed in Section 2.3 (Table 2), Fig. 4 summarises the aforementioned key operational benefits identified from the CH use case and illustrates how they contribute to each of the six dimensions.

In terms of the internal public value, our research findings reveal that the operational benefits offered by the POC supports two out of the three dimensions proposed by Twizeyimana and Andersson (2019), namely '*administrative efficiency*' and '*open government capabilities*'. Blockchain streamlines the information exchange in a secure environment between PSOs. The scalability will allow for a relatively easy interface between the blockchain system and the existing legacy systems. Subsequently the developed blockchain system reduces time, cost and administrative burden and removes the organisational silos. This in turn contributes positively to *administrative efficiency*. The ability to record company records with data integrity and in line with legal requirements allows CH to create the essential services the public needs, more quickly and cost effectively. Blockchain also provides a robust and secure infrastructure to support the government's ambition towards the 'Government as a Platform' service concept, enhancing the *open government capabilities*.

In terms of external public value, the blockchain system helps the government to become more joined-up, trusted and responsive to user needs, leading to *improved public services*. This, in combination with the ability to ensure data accuracy, integrity and legal compliance, builds citizens/companies' *trust and confidence in the government*. The significant user experience improvement ('file once principle') contributes directly to the *social value and wellbeing of users*.

Interestingly we did not find evidence to support the dimension of *ethical behaviour and professionalism* from an internal perspective as the literature has suggested. Given that the blockchain application prevents potential fraudulent behaviour (as discussed in Section 4.2.1), it drives ethical behaviours from the external users' perspective. Therefore, as Fig. 4 shows, we treat this dimension as ambidextrous.

4.4. Challenges and barriers in implementation

The research demonstrates that an increase in data availability and transparency via the hybrid blockchain system contributes to a more interoperable and consistent register of data across the PSOs. Ability to integrate this blockchain application as a separate layer and without perturbing existing data management ecosystems and business processes of PSOs like CH, suggests a plausible accelerated adoption lifecycle from technical, administrative, legal, and social perspectives as discussed in Section 4.2. Despite these advantages, blockchain is still an emerging technology and its deployment is not without challenges.

One of the major challenges is how to ensure the immutable and secure information record and information sharing among PSOs whilst complying with existing rules and regulations around data privacy, ownership and control? For example, GDPR introduced by European Union (The European Parliament and the Council of the European Union, 2016) has granted wide range of rights to citizens on their personal data. As European nations and beyond are adopting GDPR regulations (e.g. GDPR has been integrated to DPA 2018 as UK GDPR with a number of exceptions), PSOs of these countries are overwhelmed by how to interpret and contextualise these regulations and new rights accorded by GDPR (Tamburri, 2020). For example, the right to erasure (GDPR Art 17 commonly known as 'the right to be forgotten') where individuals' have the right to have their personal data erased, which from technical point of view, is almost impossible to adhere to and align with the immutable blockchain framework. However, this regulation is only

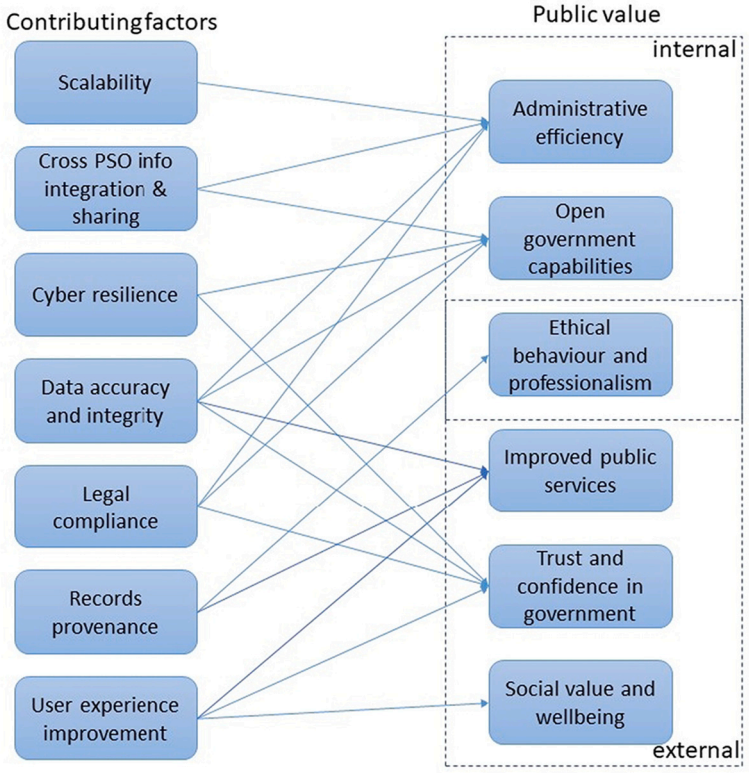


Fig. 4. A summary of how the CH blockchain POC contributes to the public value delivery.

applicable when both the personal data definition and jurisdiction conditions are met, which again is subject to interpretation. In case of CH, the organisation is obliged by the Companies Act 2006 to make information available to the public, therefore is under the exemption of paragraph 5 of schedule 2, part 1 of GDPR (ICO, 2018).

In order to future proof the blockchain framework against different data regulations and interpretations, we designed the public-private hybrid architecture where personal data is stored in the off-chain private blockchain and native databases. In other words, the personal data never leaves the premises or the jurisdiction, while only the metadata (hash of the data as well as transactions) are kept in the public blockchain, therefore maybe (depending on interpretation) considered as outside the jurisdiction. This approach can satisfy most of the rights granted by GDPR including GDPR Art 17, technically all off-chain data including the native database data can be erased. However in such a scenario, the metadata will remain on-chain but the hash will not point to anything as the pointed data can be erased.

However, in reality, CH are obliged to keep records of companies for 20 years after a company has been dissolved. From this example, it is evident that the technical solution itself is not sufficient to ensure GDPR compliance, there is a need to establish a governance framework and some data lifecycle management that is contractually binding for all participating organisations and clearly sets out each organisation's right and responsibilities. Developing such framework is perceived as "not an easy task" by the case consortium members and requires "detailed legal analysis". Therefore, PSOs are encouraged to take a proactive and responsibility centric approach, in contrast to a traditional reactive or compliance approach (Abiteboul & Stoyanovich, 2019).

Another set of complex and multi-faceted socio-technical challenges remains within the interface between government organisations (G2G), between business and government (B2G), also between governments and citizens (G2C). At G2G level despite being under the same government, inter-agency bureaucratic cooperation and communication remains opaque and sensitive to a 'turf' and reputation culture (Busuioc, 2016). Here introducing a blockchain based transparent system will require a cultural paradigm shift. Such a shift needs to be introduced in a progressive manner with appropriate incentive mechanisms.

The blockchain system also requires process changes within the consortium PSOs and among them. Resistance to changes, perceived loss of control and fear of job losses are the main perceived barriers identified during our research. Therefore, effective change management and getting employees' *buy-in* is critical to the success of the blockchain deployment. The *buy-in* and support from the senior management board is equally important for the initiative to move from the POC stages into production and wider scale deployment.

Regarding B2G, the main barrier is to ensure the data submitted by businesses is accurate before being appended to the blockchain system. Many businesses intentionally provide different information or delayed information to take advantage of the system. For example, companies may exaggerate their annual turnover to CH as compared to the actual turnover declared to HMRC. CH turnover value facilitates the companies to demonstrate the financial health and securing investments, while HMRC value is the real value for tax purpose. The in-sync operation proposed by blockchain framework introduced here can prevent such exploitation and facilitates to establish transparency and trust relationship between businesses and PSOs. However, if the original data is not accurate, then making it immutable by storing it on a blockchain does not provide any benefit and could have an adverse effect instead. Hence, ensuring data hygiene is a critical precursor to the blockchain deployment.

With regard to G2C, the traceability feature of blockchain which is regarded as the most beneficial feature, raise concerns for citizens. Since CH by law is obliged to publish a wide range of personal information about company directors (e.g. title, name, month and year of birth, address etc.) as open data via their website (which has over billion hits per year), vulnerable people like transgender people often fall victim. Recently the government was urged to change the law to protect the transgender businesspeople (Duffy, 2017). With blockchain's augmented capability to trace data, dubbed as "*Verifiable Data Audit*", such vulnerabilities will increase especially as the public can easily traceback the personal history of company directors. Although a conceptual technical solution addressing this issue has been provided (Ali Shahaab, Maude, Hewage, & Khan, 2020b), it seems inevitable that traceability will remain a major hinderance for establishing trust relationship between government and citizen. A recent example in this regard is Google's DeepMind. Despite saving the lives of thousands of kidney patients (Hern, 2017), it instigated citizen's concerns, criticism and lawsuit due to the patient's personal information tracking functionality. Therefore, the challenges and barriers of using blockchain technologies will remain precarious for the foreseeable future.

5. Registration of Overseas Entities & Beneficial Owners Bill (ROEBO)– An illustrative use case

Having presented the detailed research findings in Section 4, we present an illustrative use case in this section as a further exploration and evaluation. In 2020 international buyers purchased 49% of homes in central London (Hamptons, 2021). Most of these houses were bought under the name of overseas companies or their subsidiary company or beneficiary operating within UK. Through these property transactions "McMafia-style" money laundering occurred which also inflated the London housing price and triggered a demographic shift (Bowcott, 2019). Moreover, a large proportion of these properties remain empty as the core intention of the purchase was not always to live in these properties. Addressing this issue, UK government in 2018 drafted a legislation (i.e. ROEBO) that when passed by the parliament would enforce overseas entities to be registered with Companies House and to comply with the relevant duties. Failure to comply will result in an inability to acquire land title and therefore the selling or leasing of the property.

In order to enforce these regulations, the data needs to be shared and analysed across three UK PSOs – CH, LR & HMRC almost in a real time basis (Table 7). The data also needs to illustrate the journey of the property and its relationship with company and the beneficiaries. With the current data dump model (such analysis and intelligence gathering) remains challenging, particularly in context of tracing the journey and identifying the actual beneficiaries.

When evaluated against a hypothetical overseas company, the POC demonstrated the benefits in relation to data interoperability and sharing, data integrity and accuracy and record provenance (Table 3). These three factors enabled us to detect any fraudulent activities (e.g. declaring different turnover/income to CH & HMRC). From the

Table 7
Activities an overseas entity can take while buying, leasing or selling a property in UK and PSOs involved with these activities.

		CH	LR	HMRC
Start	Overseas entity registration	✓		✓
	Property purchase	✓	✓	✓
	Tax filing	✓		✓
Update	Address	✓	✓	✓
	Directors/ trustee board	✓		✓
	Share holder	✓		✓
	Turnover/Income	✓		✓
	Lease of property	✓	✓	✓
End	Sell of property	✓	✓	✓
	Dissolve of entity	✓	✓	✓

transactional explorer (Fig. 2 (ii)) it was easy to analyse the journey of the company/entity and their activities with different PSOs at different time points. For example, through this POC, purchase/lease/sell of a property will be known by all three PSOs due to the near real time data interoperability capacity. Using machine learning algorithms and timestamped transactions, it will be easy to detect any form of money laundering activities and the actual beneficiary. Furthermore, when evaluated against the information updating compliance, our POC enabled *once only principle* has deemed to be "easy and efficient" in contrast to current approach, where citizen need to update their information through multiple PSO websites. The management and technical team at CH have endorsed the capacity of the solution to be "beneficial for the ROEBO use case" and "is a step forward in the government's drive for the transparent and unified public services". The solution has been evaluated as "technically sound" and "easy to embed" in the current tech stack, if deployed for the ROEBO legislation.

6. Discussion and conclusion

6.1. Academic contribution

While there has been an increasing exploration of the use of blockchain technology in PSOs (Saberi, Kouhizadeh, Sarkis, & Shen, 2019; Wang et al., 2021), academic understanding of its transformative impact on the operational excellence of PSOs remains limited (Batubara, Ubacht, & Janssen, 2018; Ølnes et al., 2017). Our research is one of the few studies that provides in-depth empirical insights about the relationship between blockchain and operational efficiency and effectiveness of PSOs. We thus make strategic contributions to both the operations management and e-government literature and lay the foundation for researchers from both disciplines to explore this emerging technology further in context of PSOs. In line with the discussions in Section 3.2, we further articulate our ADSR contributions at three levels:

Level 1 contribution: introducing a hybrid blockchain architecture compatible with traditional data management system.

A primary contribution of the research is the demonstration of the ability to seamlessly integrate the hybrid blockchain outer layer with the legacy tech stack of the PSOs, with no disruption to the existing data management systems in place. Since the hybrid blockchain layer sits outside the existing technical infrastructure of the PSOs, it can be easily integrated with any legacy database systems via the help of the RPC clients from the respective PSOs. The ability to integrate a disruptive technology like DLTs without significant changes to the current data management architectures and culture will encourage PSOs to adopt DLTs into their tech stacks, as opposed to the idea of a complete transformation, which requires expensive reorganization of data management technologies, regulations, and culture This would naturally induce reluctancy and may provoke the opposition to the idea of complete or substantial transformation (Büttgen et al., 2021). Since the proposed outer layer-based approach does not disrupt any existing data management systems and culture, its adoption comes at a much cheaper cost, both in terms of capital costs and costs associated with staff training and new policy creation and implementation. Our research has also demonstrated the value of data interoperability across participating PSOs and thereby addressing the compelling need of digital PSOs workplace – "*availability of data at the right time, at the right place*". Last but not the least, the capability to trace the journey of legal entities automatically has had a decisive benefit over existing data management, especially where traceability is difficult to achieve and involves high cost and possibilities of error. Efficient and cost-effective traceability will facilitate fraud detection and auditing.

Level 2 contribution: identifying how blockchain contributes to the public value delivery.

We developed a blockchain application that promotes distributed information sharing within and between PSOs and shows how it enables the delivery of better public value. Our study concurs with a recent study of the first blockchain e-government use case in China reported by Hou (2017) that the blockchain technology improves the quality of government service by providing greater transparency and accessibility of government information and by facilitating information sharing across different organisations (Hou, 2017). Yet the use case discussed by Hou was on an individual digital identity and credit system and the author did not report any details about how the blockchain system works and the claimed benefits are rather conceptual and somewhat speculative.

Olnes et al. (Ølnes et al., 2017) in their editorial note, point out that the benefits of blockchain in government is often exaggerated in the literature and there is a need for a much deeper understanding about the positive effects as well as the limitations of the use of blockchain application. Our study responds to such a call for research. We draw from the public value framework proposed by Twizeyimana and Andersson (2019) and demonstrate via the case study of CH. In particular the significance of the emerging blockchain technology in relation to democratic practices from six dimensions. Fig. 4 is the conceptual framework we have proposed to reveal how the adoption of blockchain could lead to increased public value. The theoretical insights and relationships presented in Fig. 4 are grounded in our empirical research and can be used to interpret the emerging blockchain deployment phenomena among PSOs and to further investigate how blockchain needs to be deployed to deliver public value. We also shed further insights about the related challenges and barriers for its implementation.

Level 3 contribution: refining the public value framework.

Our study refines and extends the public value framework proposed by Twizeyimana and Andersson (2019) in the context of a blockchain enabled public service network. Our research validates the utility of the public value framework in investigating the potential impact of an emerging and disruptive technology such as blockchain on operational excellence of PSOs. While our findings support that the use of blockchain for distributed information sharing could lead to both internal and external public value generation, our research disagrees with Twizeyimana and Andersson and the wider literature on the nature of 'ethical behaviour and professionalism'. Twizeyimana and Andersson consider this public value dimension as internal public value, whereas our research found that it could be an external public value too, given that the blockchain application prevents potential fraudulent behaviour from external stakeholders. Namely the use of blockchain could not only encourage professional and ethical behaviours within a PSO but also prevent the users of public services from behaving unethically or illegally. Therefore, we argue this dimension of *ethical behaviour and professionalism'* is ambidextrous, thus refining the public value framework in the context of e-government and operations management. Consequently, we contribute to the public value theory debates and discussions in the extant academic literature, particularly in the areas of value generative mechanism, namely, *how* public value can be enhanced via the innovative use of blockchain technology.

Practical implications of our research offers several valuable insights to PSO practitioners and will prepare them for the potential uptake and exploitation of this disruptive technology. They could use the conceptual framework (Fig. 4) as a guideline to develop an effective digital transformation strategy targeting core areas to maximise public value and achieve operational excellence.

Efficient interoperability and effective use of data in a cost-effective manner helps to reduce complexities in public service operations and facilitate effective inter-organisational collaboration. A streamlined infrastructure based on trust and added value will encourage citizens and other stakeholders to act responsibly and increase engagement with public services. Understanding the implications of blockchain on public service operations, both positive and negative, will help senior executives to decide whether the deployment of blockchain will add value to their own organisations and be aware of the critical issues that they have to address for a successful digital transformation.

6.2. Research limitation and future research opportunities

Although our research offers valuable insights about the potential impact of a blockchain based application on operational efficiency of PSOs, our study is explorative, and is based on a single case study of CH. Therefore, our findings cannot be generalised to other blockchain use cases in government. Future research could examine a number of blockchain use cases in government to further validate and expand the original findings including the theoretical framework (Fig. 4) from our study. Given that most blockchain initiatives in government are still at their early stage, some longitudinal studies following through the development journey (i.e. from POC, small scale pilot, to full deployment and routinisation) of those initiatives will shed more valuable insights into how blockchain technology diffuses in PSOs. Such studies would help to demystify and further justify the value of blockchain in democratic practices. It is also worth noting that although we demonstrate the technical capability of the proposed blockchain solution, the challenges relating to data quality and integrity is multifaceted, including not only technical but also semantic, legal, organisational and process issues. No single technical solution can solve the complex problem of data integrity. To tackle this problem, PSOs need to deploy a systematic approach involving innovative technological solution, cross-organisational collaboration, right performance indicators and incentives to drive cultural adaptation of new technologies. Finally, as a blockchain system tends to involve a variety of organisations and stakeholders, we need to treat it as a complex socio-technical system (Büttgen et al., 2021). Multi-disciplinary research is much needed to explore how blockchain, in combination with other digital technologies, could be utilised to create new opportunities (e.g. new forms of governance, new types of service models) for PSOs to deliver social, economic, environmental and cultural values.

Funding details

This Research has been supported by Knowledge Economy Skills Scholarships (Scholarship # CMK219) a major pan-Wales operation supported by European Social Funds through the Welsh Government. The Scholarship was also partly funded by Companies House, UK.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Ali Shahaab, Imtiaz A. Khan, Ross Maude, Yingli Wang & Chaminda Hewage.

Acknowledgement

We would like to extend our sincere gratitude to all the staff and senior management board from Company House who participated and supported our research. We would also like to thank Dr. Fiona Carroll for proofreading the manuscript.

References

Abiteboul, S., & Stoyanovich, J. (2019). Transparency, fairness, data protection, neutrality: Data management challenges in the face of new regulation. *Journal of Data and Information Quality, 11*(3), 1–9. https://doi.org/10.1145/3310231

Abraham, C., & Sims, R. (2021). A comprehensive approach to cyber resilience. *MIT Sloan Management Review, 62*(3), 1–4.

Akaba, T. I., Norta, A., Udokwu, C., & Draheim, D. (2020). A framework for the adoption of blockchain-based e-procurement systems in the public sector: A case study of Nigeria. In *, 12066 LNCS. Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)* (pp. 3–14). https://doi.org/10.1007/978-3-030-44999-5_1

van Aken, J., Chandrasekaran, A., & Halman, J. (2016). Conducting and publishing design science research: Inaugural essay of the design science department of the journal of operations management. *Journal of Operations Management, 47–48*, 1–8. https://doi.org/10.1016/j.jom.2016.06.004

Alford, J. (2008). The limits to traditional public administration, or rescuing public value from misrepresentation: Debate. *Australian Journal of Public Administration, 67*(3), 357–366. https://doi.org/10.1111/j.1467-8500.2008.00593.x

Alford, J., & O'Flynn, J. (2009). Making sense of public value: Concepts, critiques and emergent meanings. *International Journal of Public Administration, 32*(3–4), 171–191. https://doi.org/10.1080/01900690902732731

Allessie, D., Pignatelli, F., Sobolewski, M., & Vaccari, L. (2019). *Blockchain for digital government: An assessment of pioneering implementations in public services*. https://doi.org/10.2760/942739

Ameyaw, P., & de Vries, W. (2021). Toward smart land management: Land acquisition and the associated challenges in Ghana. A look into a blockchain digital land registry for prospects. *Land, 10*(3), 239. https://doi.org/10.3390/land10030239

Andrews, R., & van de Walle, S. (2013). New public management and citizens' perceptions of local service efficiency, responsiveness, equity and effectiveness. *Public Management Review, 15*(5), 762–783. https://doi.org/10.1080/14719037.2012.725757

Bannister, F., & Connolly, R. (2014). ICT, public values and transformative government: A framework and programme for research. *Government Information Quarterly, 31*(1), 119–128. https://doi.org/10.1016/j.giq.2013.06.002

Bashir, I. (2017). *Mastering blockchain*. Packt Publishing Ltd.

Batubara, F. R., Ubacht, J., & Janssen, M. (2018). Challenges of blockchain technology adoption for e-government: A systematic literature review. In *ACM international conference proceeding series* (pp. 1–9). New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3209281.3209317.

BBC. (2017). NHS cyber-attack: GPs and hospitals hit by ransomware - BBC News. Retrieved April 21, 2021, from https://www.bbc.co.uk/news/health-39899646 (May 13).

Beck Jørgensen, T., & Bozeman, B. (2007). Public values: An inventory. *Administration and Society, 39*(3), 354–381. https://doi.org/10.1177/0095399707300703

Berryhill, J., Bourgery, T., & Hanson, A. (2020). *Blockchains unchained: Blockchain technology and its Use in the public sector*. https://doi.org/10.1787/3c32c429-en

Blockchain in the UAE government - The Official Portal of the UAE Government. Retrieved April 20, 2021, from https://u.ae/en/about-the-uae/digital-uae/blockchain-in-the-uae-government, (2021).

Bonnet, D., & Westerman, G. (2021). The new elements of digital transformation - ProQuest. *MIT Sloan Management Review, 62*(2), 82–89.

Bouckaert, G. (2012). Trust and public administration. *Administration, 60*(1), 91–115.

Bowcott, O. (2019). UK property register "needed urgently" to stop money laundering. Retrieved July 10, 2021, from https://www.theguardian.com/business/2019/may/20/uk-foreign-property-register-needed-urgently-money-laundering.

Boyne, G. A. (2002). Public and private management: What's the difference? *Journal of Management Studies, 39*(1), 97–122. https://doi.org/10.1111/1467-6486.00284

Busuioc, E. M. (2016). Friend or foe? Inter-agency cooperation, organizational reputation, and turf. *Public Administration, 94*(1), 40–56. https://doi.org/10.1111/padm.12160

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *Etherum*, (January), 1–36. https://doi.org/10.5663/aps.v1i1.10138

Büttgen, M., Dicenta, J., Spohrer, K., Venkatesh, V., Raman, R., Hoehle, H., De Keyser, A., Verbeeck, C., Zwienenberg, T., Jørgensen, K. P., Beck, R., Rikken, O., Janssen, M., Kwee, Z., & Schär, F. (2021). Blockchain in service management and service research – Developing a research agenda and managerial implications. *Journal of Service Management Research, 5*(2), 71–102. https://doi.org/10.15358/2511-8676-2021-2-71

Chatterjee, A., Shahaab, A., Gerdes, M. W., Martinez, S., & Khatiwada, P. (2021). Leveraging technology for healthcare and retaining access to personal health data to enhance personal health and well-being. In *Recent trends in computational intelligence enabled research* (pp. 367–376). https://doi.org/10.1016/b978-0-12-822844-9.00044-x

Christies. (2021). Beeple's opus. Retrieved April 20, 2021, from https://www.christies.com/features/Monumental-collage-by-Beeple-is-first-purely-digital-artwork-NFT-to-come-to-auction-11510-7.aspx.

Clavin, J., Duan, S., Zhang, H., Janeja, V. P., Joshi, K. P., Yesha, Y., Erickson, L. C., & Li, J. D. (2020). Blockchains for government: Use cases and challenges. *Digital Government: Research and Practice, 1*(3), 1–21. https://doi.org/10.1145/3427097

Companies House. (2019). How we're reforming the Companies House register - Companies House. Retrieved December 3, 2021, from https://companieshouse.blog.gov.uk/2019/06/11/how-were-reforming-the-companies-house-register/.

Companies House. (2020). Companies House: Our vision for the next 5 years - Companies House. Retrieved January 21, 2021, from https://companieshouse.blog.gov.uk/2020/09/29/companies-house-our-vision-for-the-next-5-years/.

Companies House. (2021). Incorporated companies in the UK October to December 2020 - GOV.UK. Retrieved April 21, 2021, from https://www.gov.uk/government/statistics/incorporated-companies-in-the-uk-october-to-december-2020/incorporated-companies-in-the-uk-october-to-december-2020 (January 28).

Cordella, A., & Bonina, C. M. (2012). A public value perspective for ICT enabled public sector reforms: A theoretical reflection. *Government Information Quarterly, 29*(4), 512–520. https://doi.org/10.1016/j.giq.2012.03.004

Cordella, A., & Paletti, A. (2019). Government as a platform, orchestration, and public value creation: The Italian case. *Government Information Quarterly, 36*(4). https://doi.org/10.1016/j.giq.2019.101409

Coughlan, P., & Coghlan, D. (2002). Action research for operations management. *International Journal of Operations & Production Management, 22*(2), 220–240. https://doi.org/10.1108/01443570210417515/FULL/HTML

CryptoKitties | collect and breed digital cats! (n.d.). Retrieved April 20, 2021, from https://www.cryptokitties.co/search?orderDirection=desc, (2021).

Danneels, L., & Viaene, S. (2015). Simple rules strategy to transform government: An ADR approach. *Government Information Quarterly, 32*(4), 516–525. https://doi.org/10.1016/J.GIQ.2015.09.006

De Sordi, J. O., de Paulo, W. L., Bittencourt-Jorge, C. F., da Silveira, D. B., Dias, J. A., & de Lima, M. S. (2021). Overcompliance and reluctance to make decisions: Exploring warning systems in support of public managers. *Government Information Quarterly, 38*(3), Article 101592. https://doi.org/10.1016/J.GIQ.2021.101592

Department of Business and Energy & Industrial Strategy. (2018). *A register of beneficial owners and other legal entitites*.

Department of Business and Energy & Industrial Strategy. (2019). *Corporate Transparency and Register Reform Consultation on options to enhance the role of Companies House and increase the transparency of UK corporate entities*.

Department of Business Energy and Industrial Strategy. (2020). *Corporate Transparency and Register Reform Consultation on improving the quality and value of financial information on the UK companies register*.

Duffy, N. (2017). Government urged to change law that "outs" transgender business people. Retrieved April 30, 2021, from https://www.pinknews.co.uk/2017/11/21/government-urged-to-change-law-that-outs-transgender-business-people/.

Eder, G. (2019). Digital transformation: Blockchain and land titles. In *, 12. 2019 OECD global anti-corruption & integrity forum*.

EU Blockchain Observatory and Forum. (2021). *March trends report (market updates)*.

Foster, M. (1972). An introduction to the theory and practice of action research in work organizations. *Human Relations, 25*(6), 529–556. https://doi.org/10.1177/001872677202500605

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly: Management Information Systems, 37*(2), 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01

Grigg, I., Brown, R. G., Carlyle, J., & Hearn, M. (2016). *Corda: An introduction*. https://doi.org/10.13140/RG.2.2.30487.37284

Hamptons. (2021). International Buyers: 2020. Retrieved July 10, 2021, from https://www.hamptons.co.uk/research/articles/2102-international-buyers/.

Hern, A. (2017). Google's DeepMind plans bitcoin-style health record tracking for hospitals | DeepMind | The Guardian. Retrieved April 30, 2021, from https://www.theguardian.com/technology/2017/mar/09/google-deepmind-health-records-tracking-blockchain-nhs-hospitals.

Holmström, J., Ketokivi, M., & Hameri, A.-P. (2009). Bridging practice and theory: A design science approach. *Decision Sciences, 40*(1), 65–87. https://doi.org/10.1111/j.1540-5915.2008.00221.x

Hou, H. (2017). The application of blockchain technology in E-government in China. In *2017 26th International conference on computer communications and networks, ICCCN 2017*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICCCN.2017.8038519.

Hyvärinen, H., Risius, M., & Friis, G. (2017). A blockchain-based approach towards overcoming financial fraud in public sector services. *Business and Information Systems Engineering, 59*(6), 441–456. https://doi.org/10.1007/s12599-017-0502-4

ICO. (2018). Exemptions | ICO. Retrieved April 21, 2021, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/.

Igalla, M., Edelenbos, J., & van Meerkerk, I. (2020). What explains the performance of community-based initiatives? Testing the impact of leadership, social capital, organizational capacity, and government support. *Public Management Review, 22*(4), 602–632. https://doi.org/10.1080/14719037.2019.1604796

Iivari, J. (2020). Editorial: A critical look at theories in design science research. *Journal of the Association for Information Systems, 21*(3), 10. https://doi.org/10.17705/1jais.00610

Jos, P. H., & Tompkins, M. E. (2009). Keeping it public: Defending public service values in a customer service age. *Public Administration Review, 69*(6), 1077–1086. https://doi.org/10.1111/j.1540-6210.2009.02065.x

Karanjia, B., et al. (2017). *Blockchain in public sector. Transforming government services through exponential technologies. Deloitte*.

Kaur, A., Nayyar, A., & Singh, P. (2020). *Blockchain: A path to the future. Cryptocurrencies and blockchain technology applications*. May (pp. 25–42). https://doi.org/10.1002/9781119621201.ch2.

Kernaghan, K. (2003). Integrating values into public service: The values statement as centerpiece. *Public Administration Review, 63*(6), 711–719. https://doi.org/10.1111/1540-6210.00334

Liang, Y., Qi, G., Zhang, X., & Li, G. (2019). The effects of e-government cloud assimilation on public value creation: An empirical study of China. *Government Information Quarterly, 36*(4), Article 101397. https://doi.org/10.1016/j.giq.2019.101397

Melendez, S. (2018). How IBM and the CDC are testing blockchain to track health issues like the opioid crisis. Retrieved April 20, 2021, from https://www.fastcompany.com/90231255/how-ibm-and-the-cdc-are-testing-blockchain-to-track-health-issues-like-the-opioid-crisis (April 18).

Moore, M. (1995). *Creating public value: Strategic Management in Government*. Harvard University Press.

Mullarkey, M. T., & Hevner, A. R. (2019). An elaborated action design research process model. *European Journal of Information Systems, 28*(1), 6–20. https://doi.org/10.1080/0960085X.2018.1451811

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://doi.org/10.1007/s10838-008-9062-0

Näslund, D. (2002). Logistics needs qualitative research – Especially action research. *International Journal of Physical Distribution and Logistics Management, 32*(5), 321–338. https://doi.org/10.1108/09600030210434143/FULL/XML

NCSC. (2018). *The cyber threat to UK business - 2017/2018 report*. National Crime Agency.

Ølnes, S., & Jansen, A. (2017). Blockchain technology as s support infrastructure in e-government. In *, 10428 LNCS. Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)* (pp. 215–227). Springer Verlag. https://doi.org/10.1007/978-3-319-64677-0_18.

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly, 34*(3), 355–364. https://doi.org/10.1016/j.giq.2017.09.007

Osborne, S. P. (2010). *Delivering public services: Time for a new theory? Public management review*. Taylor and Francis Ltd.. https://doi.org/10.1080/14719030903495232

Osborne, S. P., Radnor, Z., Kinder, T., & Vidal, I. (2015). The SERVICE framework: A public-service-dominant approach to sustainable public services. *British Journal of Management, 26*(3), 424–438. https://doi.org/10.1111/1467-8551.12094

Osborne, S. P., Radnor, Z., & Nasi, G. (2013). A new theory for public service management? Toward a (public) service-dominant approach. *The American Review of Public Administration, 43*(2), 135–158. https://doi.org/10.1177/0275074012466935

Panagiotopoulos, P., Klievink, B., & Cordella, A. (2019). Public value creation in digital government. *Government Information Quarterly, 36*(4), Article 101421. https://doi.org/10.1016/J.GIQ.2019.101421

Panayiotou, N. A., & Stavrou, V. P. (2021). Government to business e-services – A systematic literature review. *Government Information Quarterly, 38*(2). https://doi.org/10.1016/j.giq.2021.101576

Peffers, K., Tuunanen, T., & Niehaves, B. (2018). Design science research genres: Introduction to the special issue on exemplars and criteria for applicable design science research. *European Journal of Information Systems, 27*(2), 129–139. https://doi.org/10.1080/0960085X.2018.1458066

PWC. (2019). Bank of England tests blockchain for gross settlement applications: Advisory case studies PwC. Retrieved April 20, 2021, from https://www.pwc.com/gx/en/about/case-studies/bank-of-england.html (June 14).

Radnor, Z. J., & Noke, H. (2013). Conceptualising and contextualising public sector operations management. In *Production planning and control*. Taylor & Francis Group. https://doi.org/10.1080/09537287.2012.666884. November 1.

Reuters. (2021). SolarWinds hack was "largest and most sophisticated attack" ever: Microsoft president | Reuters. Retrieved January 31, 2022, from https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R (February 15).

Rivers, B. (2018). Report: HHS obtains authority to operate AI, blockchain-based acquisition tool. Retrieved April 20, 2021, from https://www.executivegov.com/2018/12/report-hhs-obtains-authority-to-operate-ai-blockchain-based-acquisition-tool/ (December 12).

Rodríguez Bolívar, M. P., & Scholl, H. J. (2019). Mapping potential impact areas of Blockchain use in the public sector. *Information Polity, 24*(4), 359–378. https://doi.org/10.3233/ip-190184

Rose, J., Persson, J. S., & Heeager, L. T. (2015). How e-government managers prioritise rival value positions: The efficiency imperative. *Information Polity, 20*(1), 35–59. https://doi.org/10.3233/IP-150349

Rose, J., Persson, J. S., Heeager, L. T., & Irani, Z. (2015). Managing e-government: Value positions and relationships. *Information Systems Journal, 25*(5), 531–571. https://doi.org/10.1111/isj.12052

Roy, A., Kumar, A., Mahindru, T., Shukla, P., & Sharan, A. (2020). *Blockchain: The India strategy*.

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research, 57*(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

Scott, M., Delone, W., & Golden, W. (2016). Measuring eGovernment success: A public value approach. *European Journal of Information Systems, 25*(3), 187–208. https://doi.org/10.1057/ejis.2015.11

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action design research. *MIS Quarterly: Management Information Systems, 35*(1), 37–56. https://doi.org/10.2307/23043488

Shahaab, A., Lidgey, B., Hewage, C., & Khan, I. (2019). Applicability and appropriateness of distributed ledgers consensus protocols in public and private sectors: A systematic review. *IEEE Access, 7*, 43622–43636. https://doi.org/10.1109/ACCESS.2019.2904181

Shahaab, A., Khan, I., Maude, R., & Hewage, C. (2021). A hybrid blockchain implementation to ensure data integrity and interoperability for public service organisations. In *Proceedings - 2021 IEEE International Conference on Blockchain, Blockchain 2021* (pp. 295–305). https://doi.org/10.1109/BLOCKCHAIN53845.2021.00047

Shahaab, A., Maude, R., Hewage, C., & Khan, I. (2020a). Blockchain: A panacea for trust challenges in public services? A socio-technical perspective. *The Journal of The British Blockchain Association, 3*(2), 1–11.

Shahaab, A., Maude, R., Hewage, C., & Khan, I. (2020b). Managing gender change information on immutable blockchain in context of GDPR. *The Journal of The British Blockchain Association, 3*(1).

Tamburri, D. A. (2020). Design principles for the general data protection regulation (GDPR): A formal concept analysis and its evaluation. *Information Systems, 91*, Article 101469. https://doi.org/10.1016/j.is.2019.101469

Tan, E., Mahula, S., & Crompvoets, J. (2021). Blockchain governance in the public sector: A conceptual framework for public management. *Government Information Quarterly, 101625*. https://doi.org/10.1016/j.giq.2021.101625

The European Parliament and the Council of the European Union. (2016). *Regulation (EU) 2016/679 (GDPR), Official Journal of the European Union §* (https://doi.org/L:2016:119:TOC).

Thijs, N., Hammerschmid, G., & Palaric, E. (2017). *A comparative overview of public administration characteristics and performance in EU28*. https://doi.org/10.2767/13319

Tolbert, C. J., & Mossberger, K. (2006). The effects of E-government on trust and confidence in government. *Public Administration Review, 66*(3), 354–369. https://doi.org/10.1111/j.1540-6210.2006.00594.x

Treiblmaier, H., & Sillaber, C. (2020). *A case study of blockchain-induced digital transformation in the public sector* (pp. 227–244). Cham: Springer. https://doi.org/10.1007/978-3-030-44337-5_11

Twizeyimana, J. D., & Andersson, A. (2019). The public value of E-government – A literature review. *Government Information Quarterly, 36*(2), 167–178. https://doi.org/10.1016/j.giq.2019.01.001

Walker, R. M. (2013). Strategic management and performance in public organizations: Findings from the miles and snow framework. *Public Administration Review, 73*(5), 675–685. https://doi.org/10.1111/puar.12073

Wang, Y., Chen, C. H., & Zghari-Sales, A. (2021). Designing a blockchain enabled supply chain. *International Journal of Production Research, 59*(5), 1450–1475. https://doi.org/10.1080/00207543.2020.1824086

Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management, 52*. https://doi.org/10.1016/j.ijinfomgt.2020.102090

World Economic Forum. (2020). *Exploring blockchain technology for government transparency: Blockchain-based public procurement to reduce corruption*.

Yingli Wang is a Reader at Cardiff University in logistics and operations management. She obtained her first degree in Food Manufacturing from China in 1995, an MBA in IT with Distinction in 2003 from Coventry University and a PhD in logistics and operations management from Cardiff University in 2008. She received the James Cooper Memorial Cup in 2009, awarded by CILT for her invention of the concept of Electronic Logistics Marketplaces (ELMs). She then developed a best practice guide on ELMs for the Department of Transport.

Over the last decade, she has worked intensively with many organizations including shippers, logistics service providers and IT service providers, in the field of e-logistics, such as Tesco, ASDA, BT, Costain, Panalpina, Tata Steel, Descartes, JDA Software Group, Infor, Road Tech Computer Systems, GT Nexus, Tandem Transport, CEVA Logistics, Panalpina, ABP Ports, Portbase, to name only a few. Her research on digitalisation in logistics and supply chain has attracted funding from various funding bodies such as Engineering and Physical Sciences Research Council (EPSRC), European Regional Development Funding (ERDF), Welsh Government, Highways England and Department for Transport (DfT). The book of "E-Logistics: managing your digital supply chains for competitive advantage" that she co-edited with Dr. Steve Pettit is the first book in the marketplace that offers a comprehensive coverage of technological developments in logistics.

She has written widely on the subject and her recent practical publications include a research report and guide for Highways England on accelerating BIM adoption in the supply chain, a research foresight report for Government Office for Science on the impact of emerging technologies on future mobility, and a white paper on blockchain for supply chains for World Economic Forum (WEF). Her futuristic outlook of freight ecoystem in 100 years' time was featured in CILT's flagship magazine Logistics Focus (December issue 2019, pp.35).

One of her research priorities is blockchain/distributed ledger technology and its integrative use with other digital technologies such as artificial intelligence, internet of things and cloud computing. She is currently involved in a number of blockchain initiatives, for instance she sits as a blockchain supply chain expert for World Economic Forum's Centre for the Fourth Industrial Revolution, shaping the trajectory of blockchain deployment in supply chains towards interoperability, integrity and inclusivity. In the UK, she's been working with a number of organisations from the construction and fintech sectors exploring the deployment of blockchain for value creation. She is keen in raising awareness and sharing knowledge about blockchain in supply chain and has delivered in collabration with industrial partners a master class on blockchain at RICS Digital Built Environment Conference 2019 (London) and a webinar on blockchain's role in the circular economy for the World Built Environment Forum. She is also a founding member of Blockchain Connected Council in Wales.

Dr. Wang's research started with examining technological innovation for organisations such as logistics service providers and manufacturers, and then recently extended to explore how technological innovations could benefit a wider society, in particular by addressing the 'wicked' problems and grand challenges such as food poverty and health inequality. She works closely with a number of food orgnisations in Wales and is a key member of the South Wales Food Poverty Alliance. One of her notable contributions include the recently launched strategic document: Food Poverty in Wales: a call to action and the sucessful roll out of Wales' first Your local Pantry at Dusty Forge (a food redistribution social enterprise that tackles food poverty and ineuquality) in Cardiff.

Dr. Wang is a Chartered Member of the Chartered Institute of Logistics and Transport (CILT). Before embarking on her academic career, she worked for about 8.5 years at Nestlé China in various senior managerial roles.

Imtiaz Khan is an interdisciplinary data scientists with an aim to increase the value and veracity of big data. With a background in computational biology, his research on data science is inspired by the complexity and heterogeneity of biological data. At present his research interests include: provenance, blockchain, data modelling, data interoperability, interactive data visualisation, virtualisation and machine learning.

He is a fervent advocate of research reproducibility and data integrity. He utilises his aforementioned skills to address the irreproducibility crisis of modern science. He also works with social scientists to understand the social impact of big data and artificial intelligence.

Most importantly, he inspires next generation data scientists through his teaching at undergraduate and postgraduate levels.

Chaminda Hewage is a Reader in Data Security (Associate Professor) in Cardiff School of Technologies at Cardiff Metropolitan University, UK where he is also leading the Cybersecurity and Information Networks Research Centere (CINC). He received the B.Sc. Engineering in Electrical and Information Engineering from the Faculty of Engineering, University of Ruhuna (Sri Lanka) in 2004 (First Class Honours Degree) and the Ph.D. in Multimedia Communications from the University of Surrey (UK) in 2009. He was awarded the Gold Medal for best performance in Engineering (2014) by the University of Ruhuna for his achievements in undergraduate studies at the General Convocation held in 2004. In 2014, he received Post-Graduate Certification in HE Teaching and Learning from Kingston University – London. He is a Fellow of the Higher Education Academy (HEA), UK.

After graduation, he joined Sri Lanka Telecom (Pvt.) Ltd. (Sri Lanka) as a Telcommunication Engineer (2004). In Sep. 2005 he was awarded the Overseas Research Scholarship (ORS) by the Higher Education Funding Council of England (Universities UK) to pursue his Ph.D. at University of Surrey, UK. After completing his Ph.D. in 2008, he joined University of Surrey as a Research Fellow. In 2009, he joined WMN Research Group at Kingston University – London as a Senior Researcher. He was attached to the Computing Department at Cardiff Metropolitan University as a Senior Lecture since October 2015. He worked as the Senior Researcher in a number of national and international research projects, funded by the European Commission (e.g., FP6 Visnet II, FP7 OPTIMIX, FP7 CONCERTO, FP7 Qualinet, FP7 3DConTourNet), UK research councils, Innovate UK, and industries.

A Senior IEEE Member and he is part of international committees and expert groups, including the IEEE Multimedia Communications technical committee, where he serves as Web Manager of the 3D Rendering, Processing, and Communications Interest Group.

Ross Maude is the Director of Digital at Companies House, UK since 2018.

Ross has over 20 years' experience within the digital profession, having previously worked in the banking, telecommunications, defence, public and utilities sectors. Before joining Companies House, Ross worked as a Digital Solution Partner for a consultancy firm delivering digital transformation within the utilities industry.

Ross is is responsible for developing and implementing Companies House's DDaT strategy and leading the directorate to:

- build and operate high quality, digital and data products.
- lead a culture of inclusion and innovation to continuously improve our services.

Ali Shahaab is a PhD candidate at Cardiff Metropolitan University. His research focuses on the feasibility of Distributed Ledgers (DLTs) and Blockchain Technology to guarantee the integrity of Companies House UK data. Key areas of his research are DLTs frameworks, security, privacy and immutability aspects of DLTs and Blockchain as well as legislative and deployment challenges. He also has a passionate interest in utilising blockchain technology to solve real world issues around trust, transparency and identity. Having MSc in advanced computer science from University of St. Andrews, UK and BS in Computer Engineering from Comsats Islamabad, Pakistan, Ali has a strong grip on software systems, distributed computing, cryptography and information systems.